

**PROPOSED LAN SOLUTIONS FOR ANY ORGANIZATION
A CASE STUDY OF FUT MINNA**

BY

IKUTEGBE NAJITE ROY

98 / 7084 EE

**A PROJECT SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE AWARD OF THE DEGREE
OF BACHELOR OF ENGINEERING (B. ENG) IN
ELECTRICAL/ COMPUTER ENGINEERING**

TO

ELECTRICAL / COMPUTER DEPARTMENT

**SCHOOL OF ENGINEERING AND ENGINEERING
TECHNOLOGY**

**FEDERAL UNIVERSITY OF TECHNOLOGY MINNA,
NIGER STATE**

NOVEMBER, 2004

CERTIFICATION

This is to certify that this project was designed and the report was written by IKUTEGBE NAJITE ROY of the Department of Electrical/Computer Engineering, School of Engineering and Engineering Technology, Federal University of Technology Minna, Niger State.



Student
Ikutegbe Najite Roy

06-12-2004

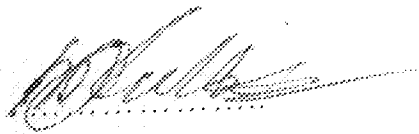
Date



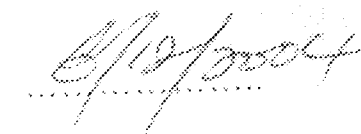
Project Supervisor
Mr. Ozomata David Ahmed

6/12/04

Date



H.O.D
Engr. M. D. Abdullahi



Date

External Supervisor

Date

DEDICATION

I hereby dedicate this project to the ALMIGHTY GOD, for mercies showered upon me all my life.

This project is also dedicated to my parents, Engineer Godspower Ikutegbe & Mrs. Dorcas Ikutegbe for their undying love and endless support.

ACKNOWLEDGEMENT

All praises be to the ALMIGHTY GOD for all his mercies; for without his protection and guidance I would not have been, neither would I have reached this stage.

With profound gratitude and deep respect I also acknowledge my darling parents Engineer Godspower Ikotegbe & Mrs. Dorcas Ikotegbe whose patience, understanding, love and financial support was – stretched way beyond elastic limit, but nevertheless has always been there for me. Thank you Dad, Thank you Mum.

I express my sincere thanks to my Supervisor Mr. Ozomata David Ahmed who by stretching me beyond my limits on this project opened up my mind academically. Thank you Sir.

I also acknowledge the contributions of my H.O.D, Engr. M. D. Abdullahi and all Academic and Non-Academic Staff of F U T Minna. Thank you all.

My thanks to Engineer Omatsola Agboghoroma in particular, who helped point out the way to go about this project.

Definitely, I must not forget to express my sincere gratitude to Engineer Timothy Ope of PAN Kaduna and all MIS staff members of PAN Kaduna for all the help they rendered.

I also acknowledge the limitless contributions of Mr. Mudi Yahaya who has always been by my side right from the moment this project was conceived until its completion. Thank you Sir.

I am grateful to my friends for their love and concern. . . Oladunjoye O. Olatayo, Edwin B. Okon . . . True definition of friends. Emeka, Azubike, Seyi, Sunny, Nasiru, Greg, Dino, Ejiro, Wale, Telvin, Paul, Fidelis, Hilary, Abia, Efe, Funsho, Abdul; you guys have not been forgotten. And to all my classmates, thank you and good luck. All my friends from F.U.T and everyone else – thank you for caring

I must not forget my brother Othniel Ikutegbe and sister Cynthia Ikutegbe. Thank you all and God bless.

Najite Roy Ikutegbe.

TABLE OF CONTENTS

TITLE PAGE	I
CERTIFICATION	II
DEDICATION	III
ACKNOWLEDGEMENT	IV
TABLE OF CONTENTS	VI
ABSTRACT	X
CHAPTER ONE	I
INTRODUCTION AND LITERATURE REVIEW	1
1.1 INTRODUCTION	1
1.2 LITERATURE REVIEW	5
CHAPTER TWO	10
NETWORK DESIGN FOR F.U.T MINNA	10
2.1 HISTORICAL BACKGROUND OF F.U.T MINNA	10
2.2 PLANNING THE NETWORK	10
2.3 LAYOUT OF CORE NETWORK BUILDINGS	13
2.4 NETWORK TOPOLOGY	17
2.4.1 THE STAR TOPOLOGY	17
2.4.1.1 ADVANTAGES	17

2.4.1.2 DISADVANTAGES	18
2.4.2 SWITCHED TOPOLOGY	18
2.5 NETWORK PROTOCOL	19
2.5.1 DEFINITION	19
2.5.2 TCP/IP (TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL)	19
2.5.3 IP ADDRESSES	20
2.5.3.1 FOUR-OCTET ADDRESS	21
2.5.4 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)	21
2.5.4.1 MANUAL OR AUTOMATIC ADDRESS ASSIGNMENT	21
2.5.4.2 ERRORS IN MANUAL ENTRY	22
2.5.4.3 IP ADDRESS	22
CHAPTER THREE	23
ADDITIONAL NETWORK FEATURES	23
3.1 NETWORK OPERATING SYSTEM	23
3.1.2 WHY WINDOWS 2000 SERVER?	24
3.2 VSAT INSTALLATION	25
3.2.1 THE OUTDOOR UNIT	25
3.2.2 INTER FACILITY LINK	27
3.2.3 THE INDOOR UNIT (IDU)	27
3.2.4 WHY VSAT?	28
3.2.5 HOW (X) VSAT SYSTEMS WORK?	29
3.2.6 PREPARING FOR SATELLITE CONNECTIVITY	30
3.3 EMAIL FACILITY	31
3.3.1 DEFINITION:	31

3.3.2 EMAIL BASICS:	32
3.3.3 FEATURES OF E-MAIL MESSAGES	32
3.3.4 MICROSOFT OUTLOOK	34
3.3.4.1 THE WHAT AND WHY OF OUTLOOK	34
CHAPTER FOUR	35
<hr/>	
HARDWARE SPECIFICATIONS & COSTING	35
4.1 HARDWARE SPECIFICATIONS	35
4.1.1 CABLING	35
4.1.1.1 UTP CAT 5E	35
THE UTP CATEGORIES:	35
4.1.1.2 FIBER-OPTIC CABLE	36
4.1.2 SERVERS	38
4.1.2.1 AN OVERVIEW OF THE HP PROLIANT ML370G4	40
4.1.3 NETWORK OPERATIONS CENTER	41
4.2 TOTAL COSTING	46
CHAPTER FIVE	47
<hr/>	
NETWORK SECURITY AND MAINTENANCE	47
5.1 NETWORK SECURITY	47
5.1.1 SELECTING A SECURITY MODEL (USER-LEVEL AND SHARE-LEVEL)	48
5.1.1.1 USER-LEVEL SECURITY	49
5.1.1.2 SHARE-LEVEL SECURITY	50
5.1.2 PASSWORD PRACTICES AND PROCEDURES	51
5.1.2.1 PASSWORD POLICIES	51

5.1.3 DATA ENCRYPTION AND PROTECTING NETWORK DATA	53
5.1.3.1 DATA ENCRYPTION	54
5.1.4 USES OF A FIREWALL	55
5.1.4.1 FIREWALL ARCHITECTURE	56
5.1.4.2 FIREWALL TYPES	58
5.1.4.3 FIREWALL FEATURES	59
5.2 DISASTER PLANNING AND PREVENTIVE MAINTENANCE	60
5.2.1 DISASTER PLANNING	60
5.2.1.1 THE NATURE OF DISASTER	60
5.2.1.2 CREATING THE DISASTER PLANNING TEAM	63
5.2.2 PREPARING FOR VIRUSES	66
5.2.2.1 UNDERSTANDING VIRUSES	67
5.2.2.2 HOW DOES A MACHINE CATCH A VIRUS?	67
5.2.2.3 PREVENTING VIRUS ATTACKS	68
5.2.3 NETWORK PREVENTIVE MAINTENANCE	70
5.2.4 ENVIRONMENTAL FACTORS THAT AFFECT COMPUTER NETWORKS	84
CHAPTER SIX	87
CONCLUSION AND RECOMMENDATION (S)	87
6.1 CONCLUSION	87
6.2 CONSTRAINTS	87
6.3 RECOMMENDATION (S)	87
REFERENCES	89

ABSTRACT

LANs provide facilities/solutions for resource sharing, security, file services, message services, print services, directory services, application services, database services, web and e-mail services, and internet access for any organization (large or small).

The Project is titled "Proposed LAN Solutions for any Organization" and therefore, it serves as a proposal for any organization that wants to implement a local area network.

This project takes a case study of F.U.T Minna. The aim of this project is to design a network architecture that would link core buildings in F U T Minna. These buildings include: The Senate Building, Student Affairs, School of Science, School of Engineering, School of Agriculture and Environmental Complex

Since these are the core network blocks, it therefore means that a Network Operations Center (NOC) or Communications room must be located within each of these structures. This room serves as the home base of all the important servers and network equipment on the network. The hardware requirements and specifications for carrying out this project as well as the costs are also well documented.

Finally, adequate information is provided on how best to secure and maintain the implemented network. This project is also an avenue for the students of the school to learn how networks work by increasing their knowledge and building their skills.

CHAPTER ONE

INTRODUCTION AND LITERATURE REVIEW

1.1 INTRODUCTION

The importance of globalization in today's world cannot be overemphasized, as the entire human endeavor is focused on it. What is the great instrument in achieving globalization? Of course, Information Technology (IT), which is the result of the confluence of communications and computing.

Two of the greatest technologies of our age are Telecommunications and Computer Engineering. Telecommunications is concerned with moving information from one point to another point or from one point to many points.

I think it is no exaggeration to say that telecommunication industry is largely taken for granted by the vast majority of people. If you were to ask the average person what the greatest technological feat of 1969 was, they would probably reply 'The first man landing on the moon'. A much more magnificent achievement was the ability of millions of people half a million kilometers away to watch what was taking place on the moon in their homes. In the last few years the revolution of computer is rather described as spontaneous as powerful computers have become even more powerful and minicomputers and microprocessors have spread to industries, education, research and the home.

However, it is interestingly surprising that these two technologies with their widely differing origins, histories and traditions should be brought together to allow computers physically separated from each other to communicate and share resources. Computer

networks are part of a general trend towards distributed computing that can be seen in multi-computer systems, in distributed databases, and in the use of intelligent terminals.

From recent studies, it has been discovered that majority of information exchange is within organizations and in particular private to the organization. Therefore, internetworking and intranetworking came to play to ensure effectiveness, efficiency, increase in performance and reliability within organizations.

The method of communication between different locations is a vital part of modern life. As we perform our daily operations in life, it is very impossible to avoid coming into contact with an application that is not fully dependent upon communication.

In communication via networking, information is captured in electronic form and needs to be communicated to computers of various type and models, using probably different operating systems.

The interconnection of systems which facilitates this communication is called networking. An example of a network from the smallest and the simplest to the largest and the most complex are two computers connected together by a cable and the internet.

Before networks came into existence, people who wanted to share information were using verbal communication, memos, and copying the information into floppy diskettes and taking it to another computer and then copying the data onto that computer which is time consuming. Therefore, Local Area Networks (LANs) implementation was aimed at increasing office efficiency through Local Area Communication. In a general survey made by a research group in November 7, 1995 the Wall Street Journal reported that nearly a quarter of about 170 large and medium scale organizations have set up intranets (i.e. collection of LANs), while another 20% have already done so (14).

A **network** is an interconnected system of computing devices that provide shared, economical access to computer services. The task of managing the access to shared services is given to a specialized type of software known as a network operating system (NOS).

A **network** consists of computers linked by means of a communication system. In a computer network, each computer is capable of communicating with every other computer, though each computer is not directly connected to every other computer through communication channel.

Once the computers are connected with each other for communication, a huge information chain is formed. This chain ensures that the information is available to the users at their appropriate time. Another advantage of Networks is that it helps an organization to make better use of the hardware and software resources. The software resources can be shared amongst the users, if the computers are connected by Network.

We need to exchange information and data. Network provides the means to exchange data amongst these computers. Network communication allows the user to work in a flexible environment.

The information age is aptly named, for we rely on information to reduce costs to produce the goods as well as to improve the overall quality.

Using computers in a professional setting without any kind of network is unthinkable these days. From the dial-up connection of a consultant's laptop to the company information distributed on an Intranet via the wide area network (WAN), networks are essential to any organization's success. Network technicians have to know the essential

ins and outs of how networks work since they can be responsible for maintaining and troubleshooting their own or a client's network.

A network is made up of two basic components: the entities that want to share information or resources and the medium that enables the entities to communicate. The entities are usually workstations and the medium is either a cable segment or a wireless medium such as an infrared signal.

Groover (1987) defined a Local Area Network as a non-public communication System that permits the various devices connected to the network to communicate with each other over a distance from several feet to several miles (Nigerian Journal of Engineering Management, Volume 3, No 3).

LANs are computer networks used to interconnect computers in localized areas like office factory or an academic institution. Each of such networks has the following:

- Workstations
- Server
- Network interface unit
- Communication channel

The past decade has been a witness to the radical evolution of data networks from their humble origins to their current forms. The original Local Area Networks (LANs) were nothing more than coaxial cabling, strung from terminal servers to desktop terminals whose users were treated to monochromatic text displayed on low-resolution cathode ray tubes (CRTs). Today, LANs have metamorphosed into high-bandwidth, high-performance, local area networks that support CPU-intensive client applications such as

live, interactive voice and videoconferencing, as well as e-mail and some of the more traditional forms of data processing.

1.2 LITERATURE REVIEW

No matter how complex computer networks are, they are all evolved from the basic need to communicate.

The very first step in modern communication was made in 1839 by Samuel F.B. who sent a message "What hath God Wrought" over a 37 mile telegraph line laid in the United States of America (from Baltimore to Washington) (1)

In 1845, Charles Wheatstone and William Cooke worked on the telegraph and it became the medium of traffic information exchange between train stations by the British railroad.

In 1876, a new technology which was based on the transmission of several telephone signals over one telegraph line and it was named telephone. This was done by Alexander Graham Bell.

The telephone and the telegraph hence came into use in the USA and the UK and the potentials of both technologies to bridge large distances were achieved.

The demand for computer communications came into existence in the mid-1950s and these early systems made use of the already existing wide communication medium, and the existing telephone network.

Digital signals used in computers were converted into analog signals for suitability by a device called the modem (modulator & demodulator).

The computer networks have been in process best described as evolution. Dr George Stibitz recorded the first computer network success as far back as 1940 when, in his experiment he sent a collection on electronic syllable over telegraph lines from a computer at Dartmouth College in New Hampshire. That event marked the birth of data communications and led to the emergence of various public and private computer communication networks over the years.

In mid 1960s an experiment was conducted by Marill and Roberts (1966) in which they connected the TX-2 computer at Lincoln Laboratories and Q-32 computer at the systems Development Corporation in such a way, that a user of one system could access the other. ARPANET (Advance Research Projects Agency Networks) owned by the U.S. Department of Defense was the first and perhaps the foremost packet switching network. A system house in Massachusetts known as BBN (Bolt, Beranek, and Newman) was awarded the contract to build the network and was developed mainly to provide resource sharing of military sites situated in the U.S, U.K and Mexico. The network became operational at the end of 1969 with four nodes.

With ARPANET, packet switching was introduced. This form of communication was based on the principle of splitting up data into small units called packets, which could be routed and carried separately through a network to be reassembled at the far end; resulting in more efficient utilization of network capacity.

TYMNET is a centrally directed packet data communications network that has been in operation since 1971. This network developed by Tymshare, started with 30 nodes consisting of various 620 microcomputers and control supervisor (with back up supervisors) using an SDS 940 computer systems (while the central supervisor provides

the network management and routing) By 1978, TYMNET has grown to 300 nodes, interconnected by leased synchronous voice grade and digital lines ranging between 2400 bps and 9600 bps.

A Canadian public packet switched Datacom Network, DATAPAC, began its operation in 1976 and first provided commercial service in June 1977. The node configuration of DATAPAC as at 1977 consists of an SL- 10 Data Network Processor manufactured by Northern telecom Ltd. Each SL- 10 is a multiprocessor consisting of a variable mixture of functional processor. Datapac include a network control center (NCC) located in Ottawa, it is connected by 9.6 kbps lines to Ottawa and Toronto lines.

The first commercial packet switching network in United States, TELENET, began operation in August 1975, and has since grown to 81 suiting nodes called the TELENET central offices (TCO'S) by 1978. The Hawaiian system is called ALOHA.

ARCNET is the forerunner of token passing networks in the United States called the Attached Resource Computer Networks and developed by Data point co-operation.

In order to overcome the problem of Interoperability and interconnectivity of the various technologies the International Standards Organization (ISO) developed an international standard for data communication. A seven-layer reference model for open system interconnection was developed by this organization to define a universal architecture for interconnecting heterogeneous computer systems.

In 1983, ARPANET was divided into two, the ARPANET carried out civil tasks and researches while MILNET carried out military tasks. Both networks were still interconnected enabling users to interchange information thus bringing about the formation of the INTERNET. Later, other networks like BITNET, CSNET, were

connected to ARPANET and MILNET. In 1986, the U S National Science Foundation (NSF) reformed the Internet by connecting networks with high performance (super) computer worldwide. Today, the internet has over 100 million people, with thousands of computers being connected everyday.

Presently, in Nigeria, most Universities are implementing Local Area Networks (LANs). This is in line with the National Universities Commission (NUC) project called Nigeria Universities Network (NUNET), which is intended to eventually connect all the universities together in a Wide Area Network (WAN).

Previous Networks carried out in this University include.

- I. Computer communication with emphasis on LAN. By Ejechi O. Kenneth 90/1641
Department of Maths/Statistics/Computer Science February 1997.
- II. The Design of Computer LAN in the School of Science and Science Education:
By Ohineme Ether Bert Otude 91/1973 Department of Physics/Computer
February 1998.
- III. Design and Simulation of Computer Network for the School of Engineering and
Engineering Technology: By Okuromade J. Adebambo 91/1869 February 1998

Therefore what is INTRANET? It is a network internal (Private) to an organization that uses Internet technology, such as Hypertext Transfer Protocol (HTTP) servers and web browser services to improve internal communications, information publishing or the application development process. It consists of computers that are connected by means of LANS.

In a survey by a business research group in the wall street journal (November 7, 1995), nearly a quarter of 170 medium and large sized organizations have set up Intranets (LANS), while another 20% have already done so. On January 22nd 1996 LAN Times Magazines pointed to a zonal research study stating that 200000 LANS were to be installed in 1966, and triple that number in 1997.

The world is becoming increasingly cyber savvy. The internet, a major computer based communication network, came online in the 1990s and has since stamped its authority in virtually every field of human endeavor. The Internet which in simplistic terms means the international network of computers is based on protocol and is used for the receipt and transmission of information in normal and encrypted formats. It has become a technology that defines relationships in our world.

From the magic of e-mail (electronic mail) to the global information reservoir on the World Wide Web (WWW), the e-commerce/business boom (i.e. B2B and B2C business), the UseNet newsgroup, listeners and other uses, the internet has become indispensable.

Pat Smith, an American Internet specialist captures it thus, 'those who use these tools will be ahead, those who do not will be left behind and may not survive'. According to a survey completed by the Internet software consortium, there were more than 56 million Internet hosts worldwide as at July 1999. Also Internet use is growing worldwide with figures of users jumping from 261 million in 1999 to projected 623 million users by the end of 2003, making the internet the medium with the fastest adoption rate in history, to connect 50 million people, in just six years of a 25 years project of Internet revolution.

CHAPTER TWO

NETWORK DESIGN FOR F.U.T MINNA

2.1 HISTORICAL BACKGROUND OF F.U.T MINNA

The Federal University of Technology, Minna is federally owned. It was established on 1st February, 1983. The objective for its establishment is to give effect to the Nation's drive for the much-needed self-reliance in Science, Engineering and especially Technology. It is a specialized University of Technology.

At take-off, the University acquired on a permanent basis, the facilities of the former Government Teachers' College Bosso which now serves as the Bosso Campus of the University. It has undergone a complete face-lift and wears a scenic outlook befitting a modern University setting.

Looking at the current increase in purchase of computer systems in various departments of F.U.T Minna, there could not have been a better time for maximizing its performance by having all of them connected on a network.

2.2 PLANNING THE NETWORK

The aim of this project is to design a network architecture that would link core buildings in F.U.T Minna. These buildings include: The Senate Building, Student Affairs, School of Science, School of Engineering, School of Agriculture and Environmental Complex.

From the university's profile, which I have carefully studied, I have noted the following structures, faculties, departments and users respectfully:

Department	Number of Users/Points
SENATE	60
STUDENT AFFAIRS	10
LIBRARY	10
SCHOOL OF SCIENCE	10
COMPUTER LAB	24
SCHOOL OF ENVIRONMENTAL	25
SCHOOL OF ENGINEERING	12
SCHOOL OF AGRICULTURE	9
TOTAL NUMBER OF USERS	160

N.B Number of Points does not necessarily mean number of offices, but it represents a network point or node for that building.

The above figures clearly state the need for a well-planned network to satisfy current and future needs.

In order to achieve this goal, the following steps were taken to break down the network to design it from the least significant user up to the main servers which will be providing all the necessary services and resources to all employees. Please note that all prices quoted in this document include labor and VAT where applicable.

STAGE I

- Layout of buildings and surrounding areas and indicate connections between buildings.
- Design and installation of the main backbone of the entire network.
- Design and installation of the network structure to accommodate all users on every floor in all the buildings and select media type and connectors.
- Design of the main computer room/ server room where critical servers will reside, and proposal of security access for these rooms.

- Detailed report of the cost involved to complete the above and provision of a time frame in which to complete this stage.

STAGE 2

- Decide on the Operating System for each department.
- Identifying each department's individual and common software/application needs, as well as selection of network software solutions which reside on the servers.
- Selecting Antivirus software for workstations and Servers.
- Deciding how many servers to be installed in total, and selection of the Network Operating System and license for every server in each department or/and floor.
- Selection of software solutions which will run on the Network Servers to enhance security, productivity, communications and help support.
- Detailed report of the cost involved to complete the above and provision of a time frame in which to complete this stage.

STAGE 3

- Hardware configuration of workstations and selection of PCs
- Multimedia computer peripherals and network printers.
- Hardware configuration and setup for each Network server.
- Redundancy. Selection of backup devices and media, stand-by servers and UPS.
- Selection of hubs, switches and chassis based hubs for each floor and building.
- Detailed report of the cost involved to complete the above and provision of a time frame in which to complete this stage.

STAGE 4

- Summary of the complete installation
- Quick reference to cost and completion time of all 4 stages.

2.3 LAYOUT OF CORE NETWORK BUILDINGS

A comprehensive layout of buildings and surrounding areas, indicating connections between buildings is shown in figure 2.1 below. Existing road network of the University premises is shown in figure 2.2.

Figure 2.1 PIII MINNA Core Network Blocks

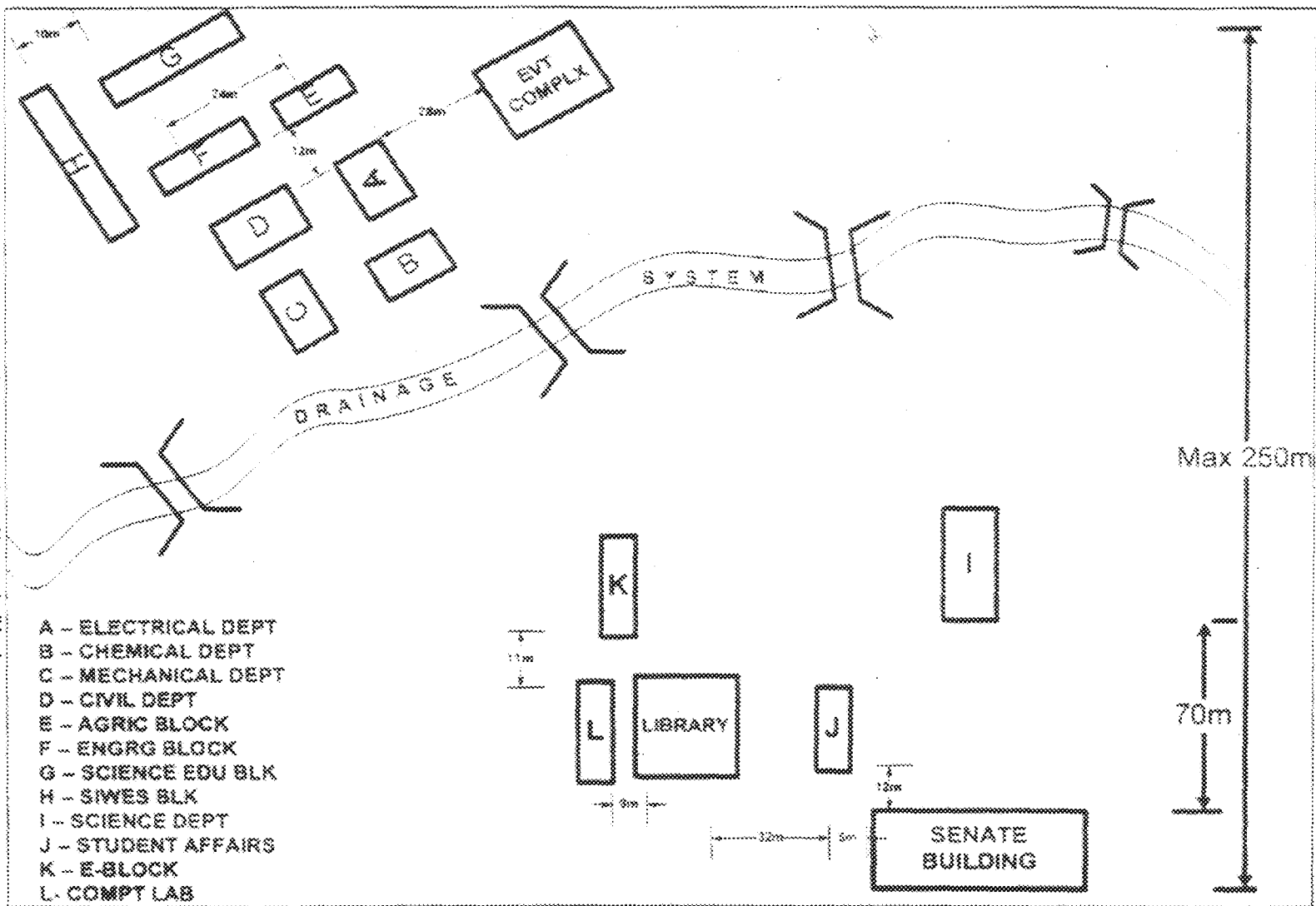
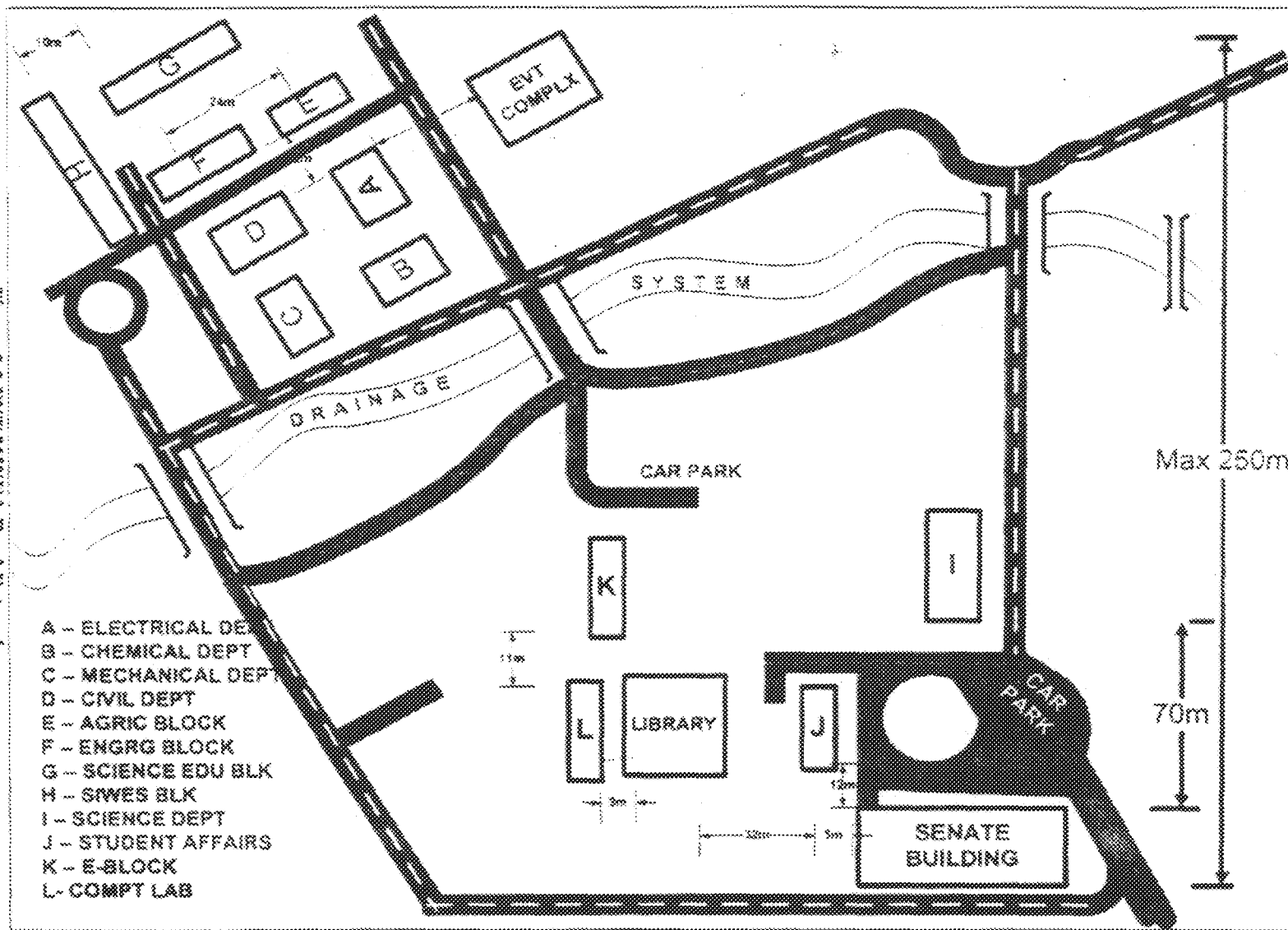


Figure 2.2 FIT MINNA Road Network



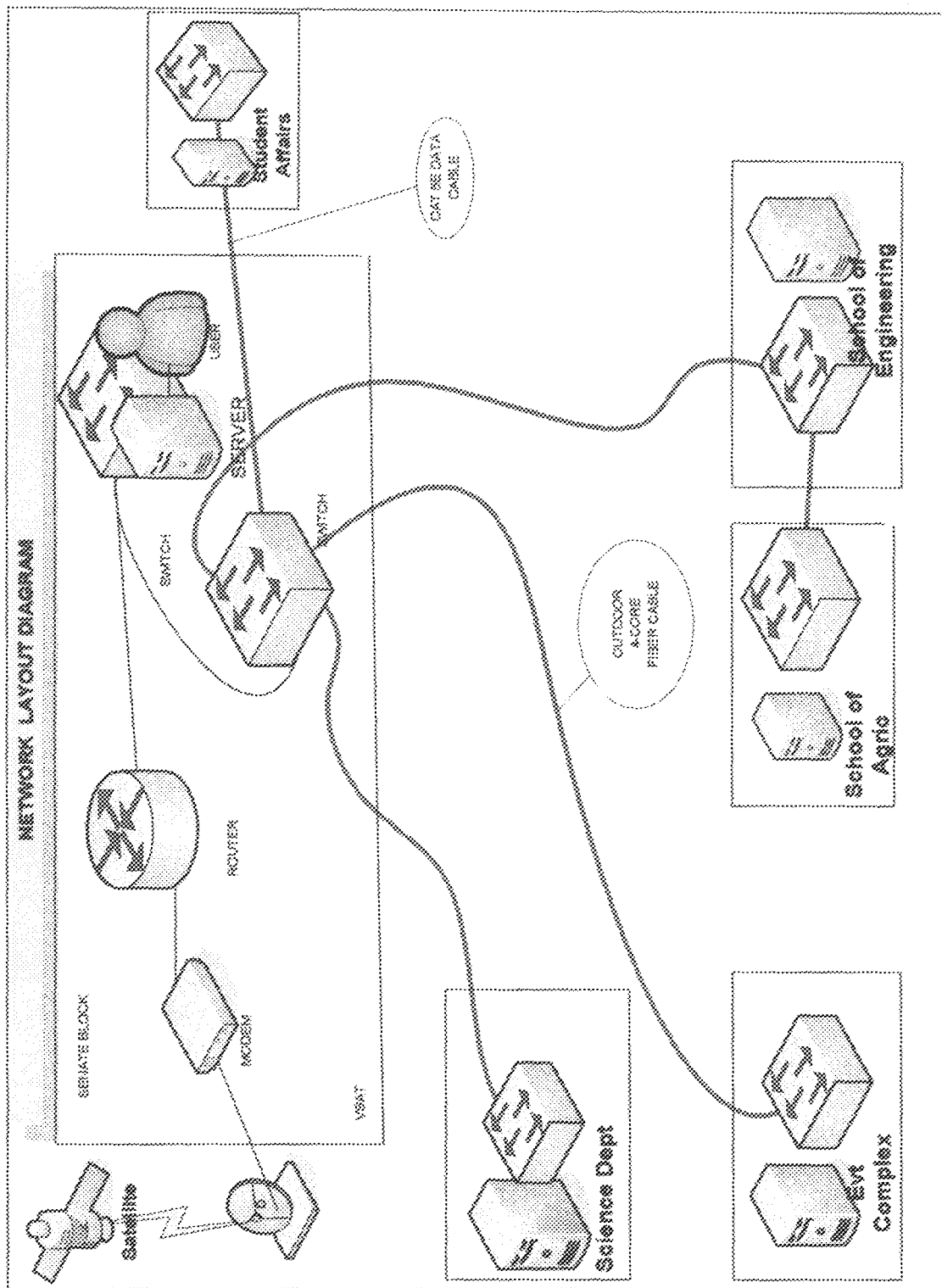


Figure 2.3 FUT MINNA Network Chart

2.4 NETWORK TOPOLOGY

A network is made up of two basic components: the entities that want to share information or resources and the medium that enables the entities to communicate. The entities are usually workstations and the medium is either a cable segment or a wireless medium such as an infrared signal.

When discussing LANs, there are two basic topics to consider: the LAN's topology (hardware connection method) and its protocol (communication control method)

There are different topologies that make up computer networks. Topology is the physical layout of computers, cables and other components on a network. Many networks are a combination of the various topologies.

2.4.1 The Star Topology

In a star topology, the logical layout of the network resembles the branches of a tree. All the nodes are connected in branches that eventually lead back to a central unit. Nodes communicate with each other through the central unit.

In star topology, all computers are connected through one central hub or switch.

2.4.1.1 Advantages

One advantage of a star topology is the centralization of cabling. With a hub, if one link fails, the remaining workstations are not affected like they are with other topologies.

Centralizing network components can make an administrator's life much easier in the long run. Centralized management and monitoring of network traffic can be vital to network success. With this type of configuration, it is also easy to add or change configurations with all the connections coming to a central point.

2.4.1.2 Disadvantages

On the flip side to this is the fact that if the hub fails, the entire network, or a good portion of the network, comes down. This is, of course, an easier fix than trying to find a break in a cable in a bus topology.

2.4.2 Switched Topology

A *switch* is a multi-port data link layer device. A switch "learns" MAC addresses and stores them in an internal lookup table. Temporary, switched paths are created between the frame's originator and its intended recipient, and the frames are forwarded along that temporary path.

The typical LAN with a switched topology features multiple connections to a switching hub. Each port, and the device it connects to, has its own dedicated bandwidth. Although originally switches forward frames based upon the MAC address, technological advances are rapidly changing this. Switches are available today that can switch cells. Switches can also be triggered by Layer 3 protocols, IP addresses, or even physical ports on the switching hub.

Switches can improve the performance of a LAN in two important ways. First, they increase the aggregate bandwidth available throughout that network. For example, a switched Ethernet hub with 8 ports contains 8 separate collision domains of 10Mbps each, for an aggregate of 80Mbps of bandwidth.

The second way that switches improve LAN performance is by reducing the number of devices that are forced to share each segment of bandwidth. Each switch-delineated collision domain is inhabited by only two devices: the networked device and the port on

the switching hub to which it connects. These are the only two devices that can compete for the 10Mbps of bandwidth on their segment.

2.5 Network protocol

In a network, some method must be used to determine which node has use of the network's communications paths, and for how long. In order for one computer to communicate with another computer, there must be a dialog in place in the form of a network protocol. The network's protocol, handles these functions.

2.5.1, Definition

A protocol is a set of rules and conventions for sending information over a network. Windows 2000 relies on TCP/IP for logon, file and print services, replication of information between domain controllers, and other common functions

2.5.2 TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP is an industry-standard suite of protocols designed for local and wide area networking. TCP/IP was developed in 1969, in a Defense Advanced Research Projects Agency (DARPA) research project on network interconnection. Formerly a military network, this global area network has exploded and is now referred to as the Internet. Windows 2000 TCP/IP enables users to connect to the Internet as well as to any machine running TCP/IP and providing TCP/IP services. The following list summarizes the advantages of the TCP/IP protocol:

- ✓ It is an industry-standard suite of protocols
- ✓ It is routable and works over most network topologies. This means that you can talk to other networks through routers.
- ✓ It is the protocol that forms the foundation of the Internet

- ✓ Installed by default in Windows 2000
- ✓ Can be used to connect dissimilar systems
- ✓ Uses Microsoft Windows Sockets interface (Winsock)
- ✓ IP addresses can be entered manually or provided automatically by a DHCP server
- ✓ It provides Dynamic Host Configuration Protocol (DHCP) support which is used for Dynamic IP addressing.
- ✓ It provides Simple Network Management Protocol (SNMP) support, which is used to troubleshoot problems on the network.
- ✓ DNS is used to resolve computer hostnames to IP addresses
- ✓ It provides Windows Internet Naming Service (WINS) support which resolves Windows NetBIOS names on the network. WINS is used to resolve a NETBIOS name to an IP address
- ✓ Subnet mask – A value that is used to distinguish the network ID portion of the IP address from the host ID
- ✓ Default gateway – A TCP/ IP address for the host (typically a router) which you would send packets for routing elsewhere on the network

To configure a TCP/IP address on a computer, you need specific TCP/IP parameters. These parameters consist of a static TCP/IP address, a subnet mask, and a default gateway (router), if you are connecting to another network.

2.5.3 IP Addresses

An IP address can be thought of as a "house" address that you might see on the side of a building. Just as every house has a street address, city, and Zip code, every computer that

uses the TCP/IP protocol has an IP address. This helps identify the computer on the network so that the computers can "talk" to one another. Each IP address can be configured for a separate subnet or network so that different computers can communicate with one another. A computer uses an IP address to identify itself on the network. An IP address is a 32-bit address that is broken up into four parts, or octets. TCP/IP's unique addressing mechanism provides for over 4.2 billion addresses. Each host is referred to by its unique 32-bit address. Because an IP address is actually a 32-bit address, a subnet mask helps separate the network from the host ID. The network ID identifies the network the computer resides on. The host ID identifies the specific computer.

2.5.3.1 Four-Octet Address

The 32-bit IP address is broken into four octets that can be represented in decimal or binary format:

11010100 00001111 10000100 01110101 (Binary representation of address)

212.15.132.117 (Dotted-decimal representation of the address)

2.5.4 Dynamic Host Configuration Protocol (DHCP)

Configuring IP addressing on a large TCP/IP-based network can be a nightmare, especially if users move machines from one subnet to another. The DHCP can help with configuration problems in these, as well as in other situations.

2.5.4.1 Manual or Automatic Address Assignment

There are two methods of assigning an IP address to a client computer. An individual can configure the client manually, or a server computer can configure the client automatically.

2.5.4.2 Errors in Manual Entry

Not only is manually entering all of this information time consuming, it is also vulnerable to human error. If the same IP address is configured for two or more computer systems, then network problems will occur and they can be difficult to trace.

2.5.4.3 IP Address

The DHCP server issues an IP address to each DHCP client system on the network.

ADDITIONAL NETWORK FEATURES

3.1 NETWORK OPERATING SYSTEM

After completing a reasonable amount of research and gathering most of the information, you will have a good picture of your "environment." It is within the concept of this environment that you can begin to envision the need for high-performance networking and the relevant network operating systems to run the applications.

All organizations have varying needs, and the right solution is often a combination of operating systems. The first step is to determine the business needs of your organization.

In medium environments, which I will define as greater than one hundred users and less than one thousand users, Windows 2000 makes sense as the desktop operating system.

From the server side, the picture gets hazier. The quantity and quality of Systems personnel often dictates software decisions in these organizations. Microsoft's premier network operating system, Windows 2000 Server, is being linked more closely to many mission-critical applications being rolled out in leading organizations. By providing integrated support for Novell and other internetworking protocols, this network operating system's graphically based ease of use is winning over customers.

First, it's important to evaluate Windows 2000 and 2000 Server separately. Windows 2000 Workstation is a very powerful, secure, stable workstation operating system. With its combination of an easy-to-use graphical user interface and a wide variety of available software programs (the library of software for Microsoft Windows is the largest on earth), a Windows 2000 Workstation can serve as a reliable desktop solution, for tasks

ranging from basic office automation (word-processing, spreadsheets, and the like) to software development to high-end computational tasks such as 3D modeling and statistical processing. Its combination of stability, performance, and flexible platform choice (particularly on the high bang-for-buck Intel platform) makes it an appealing alternative to more expensive UNIX desktop workstations (and can even exceed their performance when running on powerful hardware such as the Alpha), as well as a more advanced and more reliable alternative to other Windows and Macintosh computers. As more high-speed network implementations become available on Windows 2000 Server, the ability to augment or replace UNIX systems with Windows 2000 server becomes a more viable option.

3.1.2 Why Windows 2000 Server?

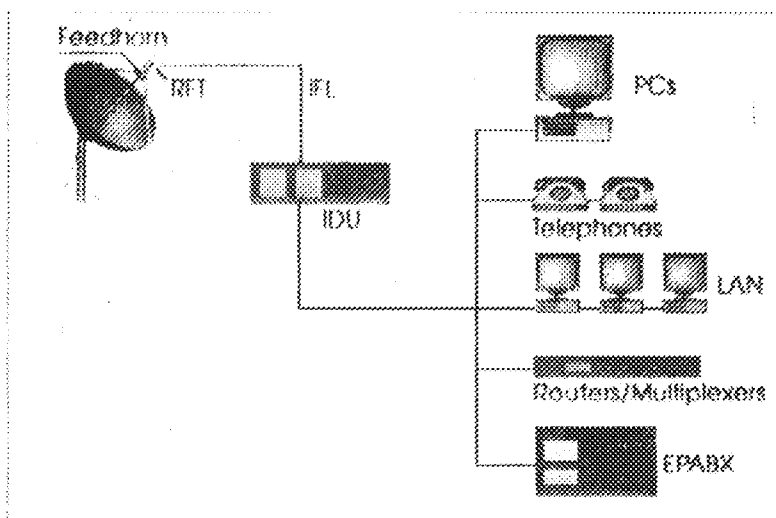
Although Windows 2000 Server's cooperation with other Network Operating Systems (NOSs) means that you don't necessarily have to make it the sole NOS for your organization, you might wonder why you would even make it one of them. NetWare has been the market leader in network software for quite some time. Is Windows 2000 Server giving NetWare a run for its money? The answer is yes, and the following sections explore a few of Windows 2000 Server's key strengths.

- ✓ Easy To Use
- ✓ Designed for High-Powered Systems
- ✓ Security
- ✓ Interoperability
- ✓ Centralized Control
- ✓ Long File Name Support

- ✓ Logging Capabilities
- ✓ UPS Service
- ✓ Software Metering
- ✓ Built-In Remote Access Services (RAS) Capability

3.2 VSAT INSTALLATION

The term Very Small Aperture Terminal (VSAT) refers to a small fixed earth station. VSATs provide the vital communication link required to set up a satellite based communication network. VSATs can support any communication requirement whether voice, data, or video conferencing.

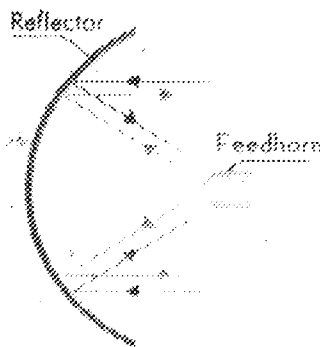


The VSAT comprises of two modules - an outdoor unit and an indoor unit.

3.2.1 The outdoor unit:

The outdoor unit is generally ground or even wall mounted. The antenna system comprises of a reflector, feedhorn and a mount. The size of a VSAT antenna varies from 1.8 meters to 3.8 meters. The feedhorn is mounted on the antenna frame at its focal point by support arms.

The Antenna is mounted where it can 'see' the satellite and where it is safe from unauthorized access. The outdoor RF unit (ORU) is mounted on the arm in front of the antenna reflector.



The FEED HORN directs the transmitted power towards the antenna dish or collects the received power from it. It consists of an array of microwave passive components. Antenna size is used to describe the ability of the antenna to amplify the signal strength.

The RFT is mounted on the antenna frame and is interconnected to the feed horn.

Also termed as outdoor electronics, RFT in turn, consist of different subsystems. These include Low Noise Amplifiers (LNA) and down converters for amplification and down conversion of the received signal respectively

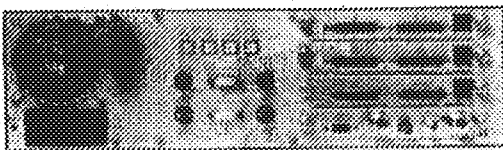
LNAs are designed to minimize the noise added to the signal during this first stage of the converter as the noise performance of this stage determines the overall noise performance of the converter unit. The noise temperature is the parameter used to describe the performance of a LNA. UpConverters and High Powered Amplifiers (HPA) are also part of the RFT and are used for upconverting and amplifying the signal before transmitting to the feedhorn. The Up/Down converters convert frequencies between intermediate frequency (Usually IF level 70 MHz) and radio frequency. For Extended C band, the downconverter receives the signal at 4,500 to 4,800 GHz and the upconverter converts it to 6.725 to 7.025 GHz. The HPA ratings for VSATs range between 1 to 40 watts.

3.2.2 Inter Facility Link:

The outdoor unit is connected through a low loss coaxial cable to the indoor unit. The typical limit of an IFL cable is about 300 feet (approx. 92 meters).

3.2.3 The indoor unit (IDU):

The indoor unit which is typically the size of a desktop computer is normally located near existing computer equipment in your office. The IDU consists of modulators which superimpose the user traffic signal on a carrier signal. This is then sent to the RFT for up-conversion, amplification and transmission. It also consists of demodulators which receive the signal from the RFT in the IF range and demodulates the same to segregate the user traffic signal from the carrier. The IDU also determines the access schemes under which the VSAT would operate. The IDU also interfaces with various end user equipment ranging from stand alone computers, LANs, routers, multiplexers, telephone instruments, EPABX as per requirement. It performs the necessary protocol conversion on the input data from the customer and equipment prior to modulation and transmission to the RFT.



An IDU is specified by the access technique, protocols handled and number of interface ports supported.

The indoor data processing unit (DPU) will typically have one or more user data ports for connection either direct to PCs or to a local area network router. The number of ports is typically 1 to 14, depending on board option. Individual user port bit rate may be set between 1200 bit/s and 128 Kilobit/s for older serial type ports or up to 100 Megabit/s for Ethernet type ports.

3.2.4 Why VSAT?

Networking of business activities, processes and divisions is essential to gain a competitive edge in any industry. VSATs are an ideal option for networking because they enable Enterprise Wide Networking with high reliability and a wide reach which extends even to remote sites.

VSATs provide an edge over terrestrial lines. They are as stated below:

REACH: You must be well aware of the limitations faced by terrestrial lines in reaching remote and other difficult locations. VSATs, on the other hand, offer you unrestricted and unlimited reach.

RELIABILITY: Uptime of up to 99.5 percent is achievable on a VSAT network. This is significantly higher than the typical leased line uptime of approximately 80 to 85 percent.

TIME: VSAT deployment takes no more than 4-6 weeks as compared to 4 to 6 months for leased lines.

NETWORK MANAGEMENT. Network monitoring and control of the entire VSAT network is much simpler than a network of leased lines, involving multiple carriers at multiple locations. A much smaller number of elements needs to be monitored in case of a VSAT network and also the number of vendors and carriers involved in between any two user terminals in a VSAT network is typically one. This results in a single point of contact for resolving all your VSAT networking issues. A VSAT NMS easily integrates end-to-end monitoring and configuration control for all network subsystems.

MAINTENANCE: A single point contact for operation, maintenance, rapid fault isolation and troubleshooting makes things very simple for a client, using VSAT services. VSATs

also enjoy a low mean time to repair (MTTR) of a few hours, which extends up to a few days in the case of leased lines. Essentially, lesser elements imply lower MTTR.

FLEXIBILITY: VSAT networks offer enormous expansion capabilities. This feature factors in changes in the business environment and traffic loads that can be easily accommodated on a technology migration path. Additional VSATs can be rapidly installed to support the network expansion to any site, no matter however remote.

COST: A comparison of costs between a VSAT network and a leased line network reveals that a VSAT network offers significant savings over a two to three years timeframe. This does not take into account the cost of downtime, inclusion of which would result in the VSAT network being much more cost-effective. Pay-by-mile concept in case of leased line sends the costs spiraling upwards. Moreover if the locations to be linked are dispersed all over the country. Compare this to VSATs where the distance has nothing to do with the cost. Additionally, in case of VSATs, the service charges depend on the bandwidth which is allocated to your network in line with your requirements; whereas with a leased line, you get a dedicated circuit in multiples of 64Kbps whether you need that amount of bandwidth or not.

3.2.5 How do VSAT systems work?

A VSAT system consists of a satellite transponder, central hub or a master earth station, and remote VSATs. The VSAT terminal has the capability to receive as well as transmit signals via the satellite to other VSATs in the network. Depending on the access technology used the signals are either sent via satellite to a central hub, which is also a monitoring center, or the signals are sent directly to VSATs with the hub being used for monitoring and control.

The network of VSATs at different locations adopts different topologies depending on the end applications traffic flow requirements. These topologies could be Star or Mesh.

Star – where a big central earth station called the hub communicates with a large number of VSATs scattered over a wide area

Mesh – implies that a group of VSATs communicate directly with other VSATs without going through the central hub

Given the topology, satellite communications systems employ several techniques to allow one satellite to relay signals to and from more than one earth station at a time without signal interference. Typically, satellites carry several transponders that operate at different frequencies, each corresponding to an earth station (or a set of stations tuned to that frequency). There are methods of access schemes to share and consequently optimize the satellite capacity. Apart from the access scheme and the network topology, the operating frequency band is also used to classify VSAT networks.

3.2.6 Preparing for Satellite Connectivity

The NUC runs a project called the Nigerian Universities Network (NUNet) that is designed to encourage universities to invest in digital communication and training. The most successful part of this project is their email gateway with ICAP. Even so, only about a dozen universities use the NUNet email system. The NUNet email system works well on occasion, but has experienced downtimes that stretch into weeks. A handful of universities who are using the NUNet email system maintain dual systems with other Internet service providers. Except for one or two institutions that use an ISP for limited email connectivity, the remaining universities operate without email.

This plan demonstrates how satellite Internet connectivity can be used throughout Nigeria and prepares Nigerian technicians for a future that looks increasingly to be satellite based. The overall notion is to provide reliable connectivity in a few universities around the country, to build redundant links between these centers, and to provide a mechanism for those at other universities to access the Internet via these "Centers of Excellence". This plan is envisaged as the first step towards full connectivity for all Nigerian universities. It is designed to provide the widest access for all institutions while a core group develops the requisite skills to foster further expansion.

Consistent with Nigeria's aspirations and the NUC's Action Plan, a fully-connected Nigerian University Network will:

1. End the intellectual isolation of Nigerian students, teachers, and researchers
2. Expand Internet access to higher education at minimal capital costs
3. Improve standards education and currency of knowledge
4. Optimize utilization of Nigeria's academic resources regardless of their physical location
5. Encourage local and worldwide academic and research collaborations

This project will also serve as a demonstration to other academic and public institutions across sub-Saharan Africa of how these satellite technologies can be best deployed to serve their communication needs.

3.3 E-MAIL FACILITY

3.3.1 Definition:

Electronic mail (email) is a quick and easy way to send a message to just one person or to hundreds of people simultaneously. In most cases, the message arrives at the person's

mail server within minutes, ready to be read. Since the first computer networks were created, email has been- and continues to be-one of the most important uses for computer networks.

3.3.2 Email Basics:

In its most basic form, an email message consists of some plain text and an address. The address identifies the recipient in a form that is recognizable by the network that forwards the mail to the recipient.

The first email messages were created with simple text editors (such as the UNIX `ed` or `vi` commands) and could be read on dumb character terminals (in other words, no fancy graphics or colors). Although mail messages can still be just as simple, today's programs for composing and reading mail offer a lot more features.

3.3.3 Features of E-mail messages

Html format:

The latest email programs enable you to create email messages in either plain text or HTML formats. By allowing HTML, you can add images, color, font changes, and text formatting. You can even include an entire webpage in an email message.

Attachments: Any type of computer file can be attached to an email message. When an attachment arrives with the message, the recipient can choose to save the attachment or open it in a program that is designed to play or display the file.

Address book:

Most email programs come with a way of storing the names and email addresses of the people you send mail to. You can also gather names together into an email group so you can send a message to a group of people at once. Some address books also enable you to

store other information about each person, such as their address, job title, phone/fax numbers and webpage location

Mail downloads:

When the computing world was mostly mainframes, mail was usually stored on the same computer where you did your work. However, with more people working on PCs, to receive email the user often sends outgoing messages and downloads incoming messages by connecting to a mail server. Many mail readers use the Post Office Protocol (POP3) or Internet Message Access Protocol (IMAP4) to get messages from the mail server.

Multiple email accounts:

Some people have several email accounts (possibly one work and one personal account). Some mail programs enable you to query several mail servers for your email

Managing messages:

Some people get so much email that managing messages they receive is a big issue. Most mail programs offer a way to save messages to your hard disk or sort them to special mail folders you create. Within folders, there are also ways to sort messages by subject, time/date received and sender.

Managing newsgroups:

Because newsgroups really just consist of a bunch of email messages grouped together, many mail message programs offer a way of reading and working with newsgroups as well as email. Some special features (such as allowing threads that follow the responses to a particular message) are included to be used for working with newsgroups.

3.3.4 Microsoft Outlook

Microsoft Outlook is an e-mail program and much more. With Outlook, you can communicate throughout your office with e-mail, but you can also schedule meetings and invite your coworkers, create task lists for yourself and others, store documents in public folders that everyone can access, and communicate over the Internet. Outlook provides accessibility and flexibility for you and your coworkers.

3.3.4.1 The What and Why of Outlook

Outlook can help you organize your work on a day-to-day basis. Using Outlook, you can do the following:

- ✓ Create task lists
- ✓ Manage your calendar
- ✓ Log phone calls and other important events in your journal
- ✓ Make notes to remind yourself of important tasks

Additionally, Outlook can help you communicate with others and share your workload.

When you and your coworkers use the combined features of Outlook and Microsoft Office, you can:

- ✓ Schedule meetings and invite coworkers
- ✓ Communicate with others using e-mail
- ✓ Import and export files
- ✓ Share data and documents through public folders
- ✓ Communicate with others over the Internet

HARDWARE SPECIFICATIONS & COSTING

4.1 HARDWARE SPECIFICATIONS

4.1.1 Cabling

Cabling is the LAN's transmission medium. LANs can be connected together using a variety of cable types. Each cable type has its own advantages and disadvantages. Transmission rates that can be supported on each of these physical media are measured in millions of bits per second (Mbps).

4.1.1.1 UTP Cat 5E

Unshielded Twisted Pair cable is most certainly by far the most popular cable around the world. UTP cable is used not only for networking but also for the traditional telephone (UTP-Cat 1). There are 6 different types of UTP categories and, depending on what you want to achieve, you would need the appropriate type of cable. UTP-CAT5 is the most popular UTP cable; it came to replace the good old coaxial cable which was not able to keep up with the constant growing need for faster and more reliable networks. The characteristics of UTP are very good and make it easy to work with, install, expand and troubleshoot

The UTP Categories:

CAT1 is typically telephone wire. This type of wire is not capable of supporting computer network traffic and is not twisted. It is also used by phone companies who provide ISDN, where the wiring between the customer's site and the phone company's network uses CAT 1 cable. CAT2, CAT3, CAT4, CAT5 and CAT6 are network wire

specifications. This type of wire can support computer network and telephone traffic. CAT2 is used mostly for token ring networks, supporting speeds up to 4 Mbps. For higher network speeds (100Mbps plus) you must use CAT5 wire, but for 10Mbps CAT3 will suffice. CAT3, CAT4 and CAT5 cable are actually 4 pairs of twisted copper wires and CAT5 has more twists per inch than CAT3 therefore can run at higher speeds and greater lengths. The "twist" effect of each pair in the cables will cause any interference presented/picked up on one cable to be cancelled out by the cable's partner which twists around the initial cable. CAT3 and CAT4 are both used for Token Ring; the only difference is CAT3 can be as long as 100 meters while CAT4 can only be 200 meters. CAT6 wire was originally designed to support gigabit Ethernet (although there are standards that will allow gigabit transmission over CAT5 wire, that's CAT 5e). It is similar to CAT5 wire, but contains a physical separator between the 4 pairs to further reduce electromagnetic interference.

4.1.1.2 Fiber-Optic Cable

Fiber-optic communications is based on the principle that light in a glass medium can carry more information over longer distances than electrical signals can carry in a copper or coaxial medium. The purity of today's glass fiber, combined with improved system electronics, enables fiber to transmit digitized light signals well beyond 100 km without amplification. With few transmission losses, low interference, and high bandwidth potential, optical fiber is an almost ideal transmission medium.

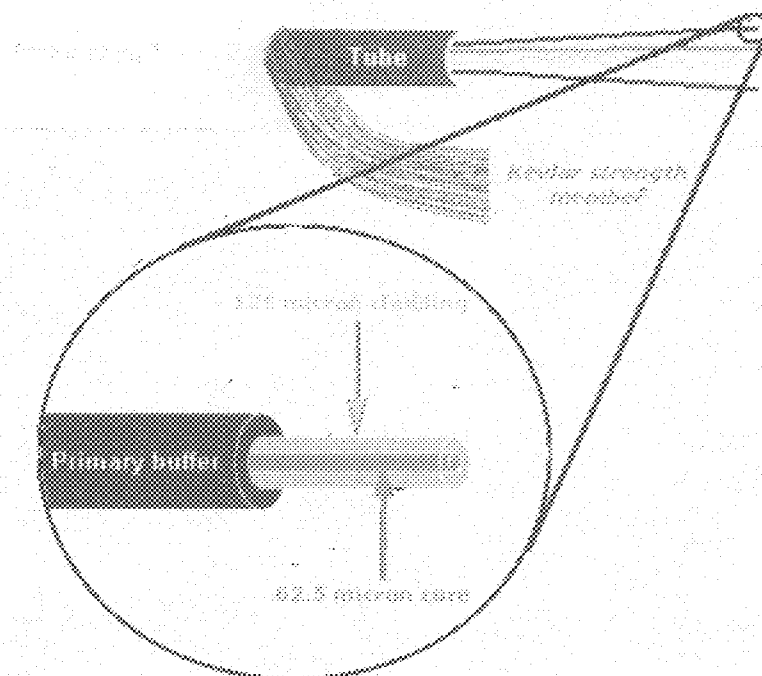
The advantages of using fiber optics

Because of the Low loss, high bandwidth properties of fiber cables, they can be used over greater distances than copper cables. In data networks this can be as much as 2km

without the use of repeaters. Their light weight and small size also make them ideal for applications where running copper cables would be impractical and, by using multiplexers, one fiber could replace hundreds of copper cables. This is pretty impressive for a tiny glass filament, but the real benefit in the data industry is its immunity to Electro Magnetic Interference (EMI), and the fact that glass is not an electrical conductor.

Because fiber is non-conductive it can be used where electrical isolation is needed, for instance, between buildings where copper cables would require cross bonding to eliminate differences in earth potentials. Fibers also pose no threat in dangerous environments such as chemical plants where a spark could trigger an explosion. Last but not least is the security aspect, it is very, very difficult to tap into a fiber cable to read the data signals.

Fibre Optic Cable



Bending Parameters

Optical fiber and cable are easy to install because it is lightweight, small in size, and flexible. Nevertheless, precautions are needed to avoid tight bends, which may cause loss of light or premature fiber failure.

4.1.2 Servers

Servers are powerful computers or processes that manage disk drives, printer services, network traffic, and other network resources. There are many different servers including: Application servers, Communications servers, Directory servers, File servers, Internet servers, Mail servers, Print servers.

Application Servers:

Application servers house applications such as programs. In an application server-based network. Instead, clients make inquiries and send up server environment is where the server house and its accompanying application. In contrast application. This scaled down version allow information to) the server.

The principal advantage of application application servers obviate the need for workstations. This saves space and

Communications Servers:

Communications servers control tele and other communication trans

function as entrances or gateways into private networks, using a wide range of networking devices (for example, modems, routers, or dedicated lines).

Communications servers provide users with quick, secure network connections. There are many such communications servers, and their functionality and cost vary considerably.

Directory Services Servers:

Directory services servers contain indexes of users, nodes, and network servers. Their chief function is to enable easy administration of large networks. Often, directory service servers provide an index of absolutely everything on the network.

Fax Servers:

Fax servers manage network fax traffic through one or more fax/modem cards. Users request faxes that have been sent or received with software on their client or workstation. In turn, the server reports (and can deliver) those faxes to the user.

File Servers:

File servers centralize data storage. The server stores files and the client requests them. Commonly used for development in software design, file servers are excellent for use in collaborative work environments.

Internet Servers:

Internet servers manage internet or intranet traffic. They allow you to create and publish web pages, sell products over the World Wide Web, and gather contacts and feedback. These servers can come in all shapes and sizes using a multitude of different software. However, internet servers are now being used in even more creative ways. For example, you can now run a microcosmic version of the internet in your organization's offices. These new networks (called intranets) run common internet protocols. Many firms are

now using intranets to offer World Wide Web-like capabilities to their local documentation and databases.

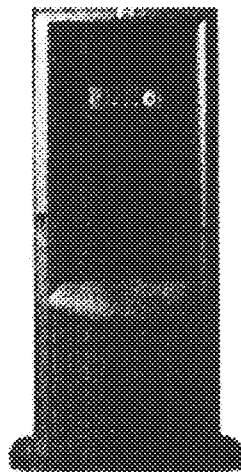
Mail Servers:

Mail servers manage email and messaging for clients. Software on the client workstation can send messages through the server to both the local network and the internet.

Print Servers:

Print servers manage networked printer peripherals, and allow anyone to print from their workstation. Today, people use print servers less than they used to. Many software companies have integrated printer management into their software, eliminating the need of a dedicated server. Furthermore, certain printers now even have print management firmware, so print servers are rarely used except in large networks.

4.1.2.1 An overview of the HP ProLiant ML370G4



HP ProLiant ML 370G4

Specs at a glance

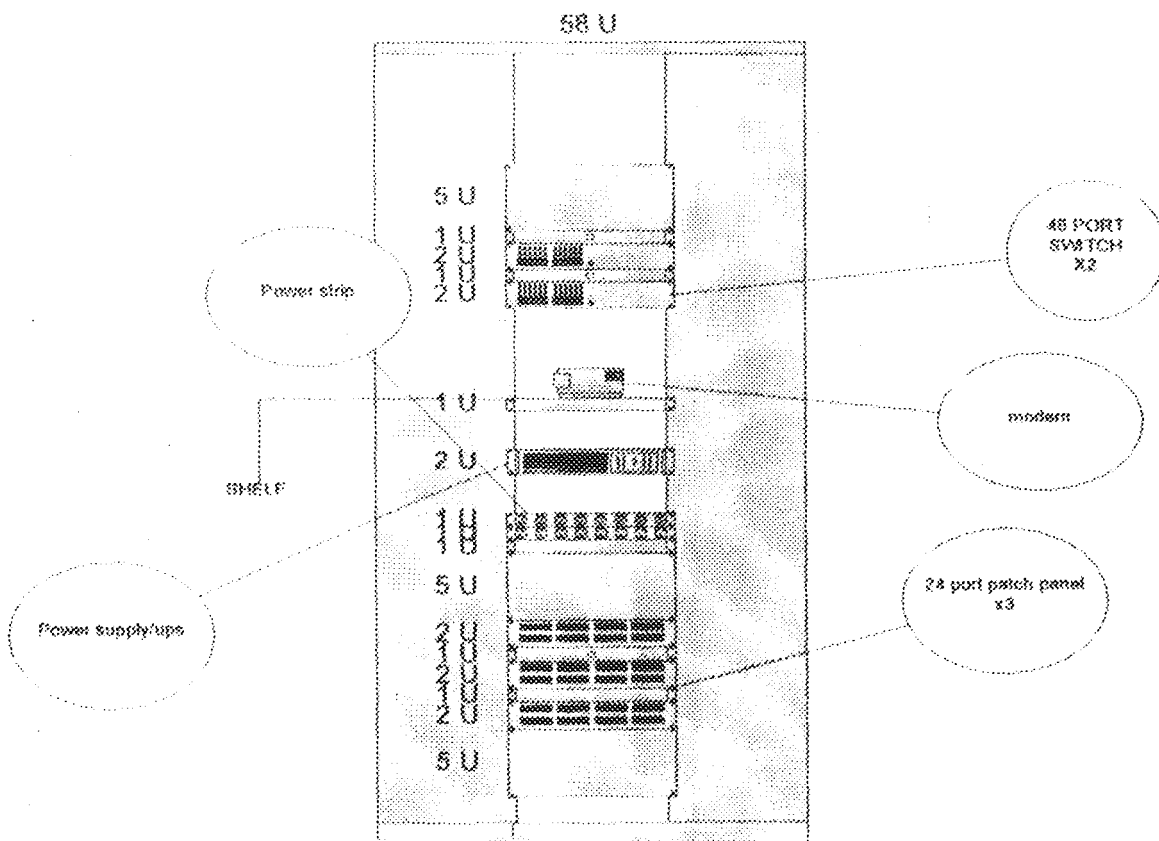
	MI 370 G4	MI 370 G4 High Performance Model
Processor	(1) Intel® Xeon™ processor at 3.4 GHz (up to 2 supported), 800 MHz FSB, 1MB Level 2 cache, Extended Memory 64 Technology (EM64T)	(2) Intel® Xeon™ processors 3.4 GHz, 800 MHz FSB, 1MB Level 2 cache, Extended Memory 64 Technology (EM64T)
Standard Memory/Max	1GB/16GB*	2GB/16GB*
Storage	U320 SCSI	Smart Array 6402 with dual channel U320 SCSI and 128 BBWC
Max Internal Drives	6 in standard drive cage	8 - includes optional 2-bay cage
Redundant Fans	Optional	Yes
Redundant Power	Optional	Yes
Tower Models	Yes (tower to rack conversion kits available)	Yes (tower to rack conversion kits available)
Rack Models	Yes, 5U	Yes, 5U

4.1.3 Network Operations Center

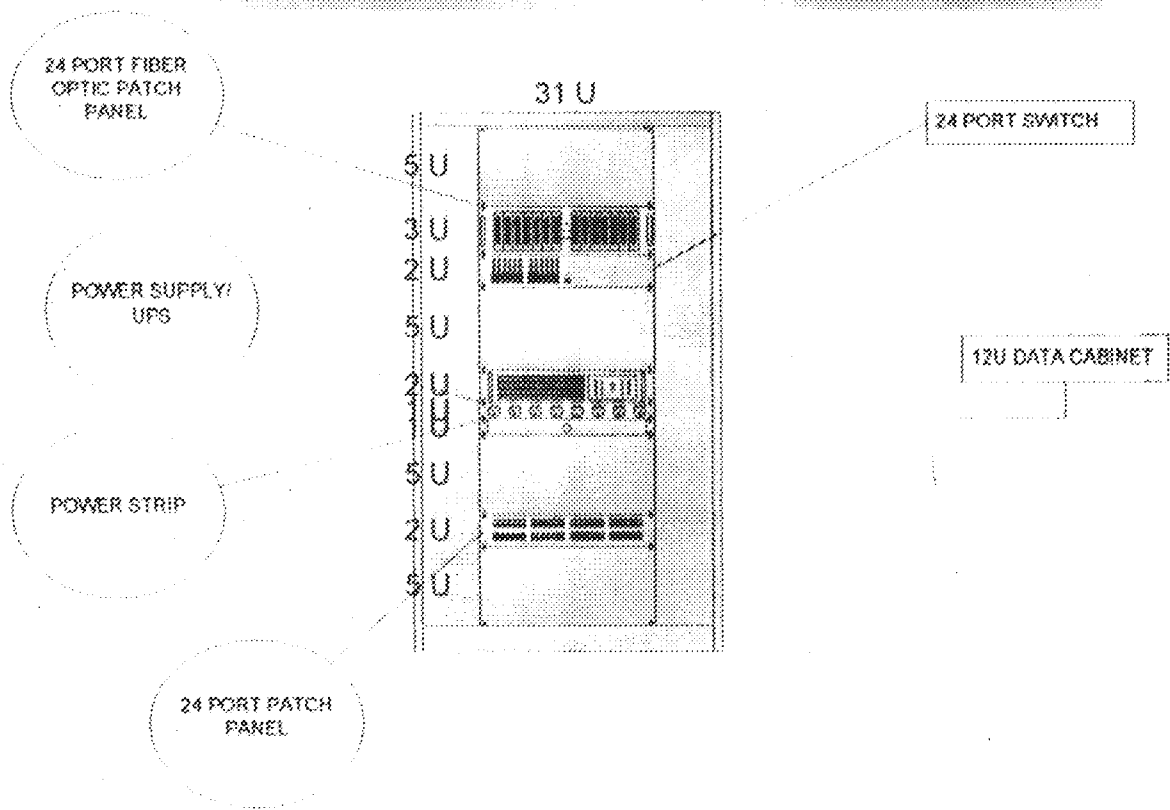
This is the main computer room for each building where critical servers will reside. This room is to house the UPS and distribution equipment. It should be housed with raised floor, suspended ceiling, 600 X 600 modular light fittings complete with reflector and fluorescent bulbs, fire protection and air conditioner. The room conditions of your NOC should be cool, dry, and temperature controlled. Computers and other electrical equipment do not like humidity, heat, or extreme cold, so you should be very careful to regulate the temperature of your NOC. This will certainly prolong the life and reliability of the systems hosted in the room. Because computer equipment is very sensitive to moisture, you need to use a form of fire suppression besides water. Putting out a fire in your NOS with a sprinkler system would ruin all of your computer equipment. There are

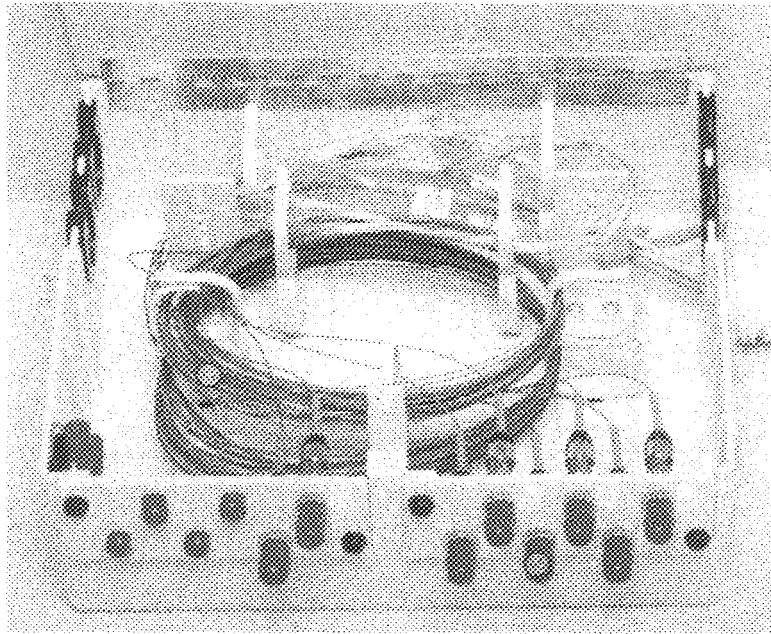
many different types of foams or Halon used to put out fires quickly and safely while minimizing the potential damage to your computer equipment. Care should be taken in choosing a Communications room/ Network Operations Center. It should be in a relatively centralized location but most of all it should be very secured from intrusion. A camera inside the room would give additional security as well.

SENATE BUILDING SERVER ROOM CABINET



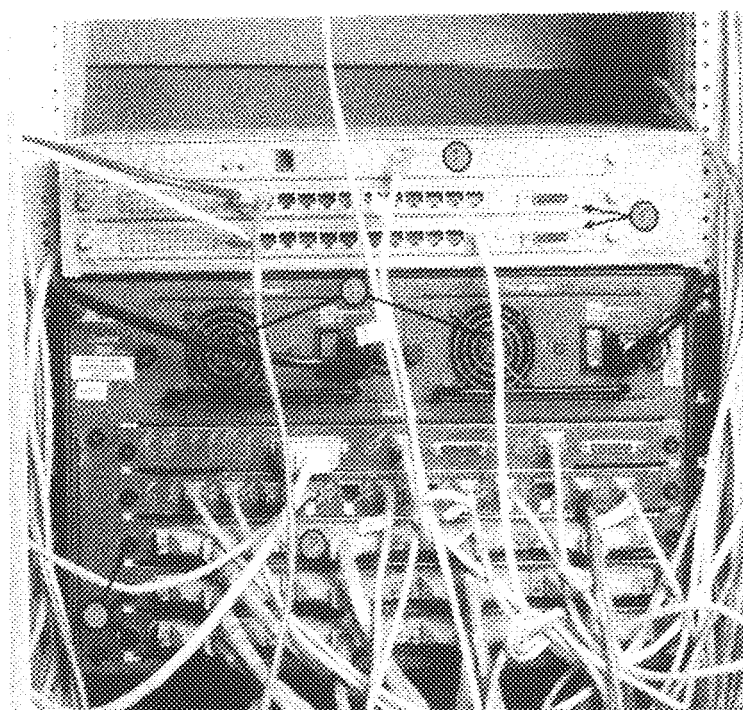
**DATA CABINET FOR
(EVT. COMPLEX, SCIENCE DEPT, SCHOOL OF
ENGINEERING, SCHOOL OF AGRIC)**



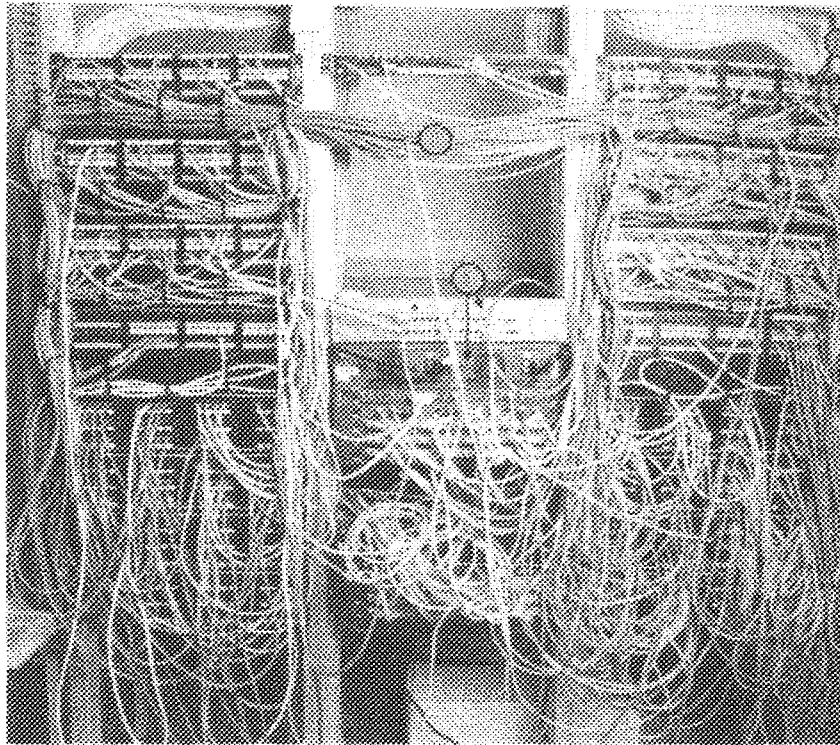


1. Fiber-Optic Cable 2. Connector Caps to prevent injury to eyes

A wall-mounted fiber-optic cable distribution box. This unit is a central station, similar to a hub that receives fiber-optic cabling from numerous sources. The distribution box is located in areas such as server rooms.



The Cisco Catalyst 5000 Ethernet switching hub, which supports 10/100 Mbps switching technology, creates "virtual circuits" between ports on the switch.



1. twisted-pair Cabling
2. Patch Panels
3. Switching Hubs

A typical Ethernet wiring closet with twisted-pair switches, hubs, and patch panels. Cables connecting the computers and devices on the network are fed into the wiring rack into their respective ports on the patch panels, which are numbered identically to the wall jacks at each network drip throughout the establishment.

4.2 TOTAL COSTING

S/N	DESCRIPTION	QTY	UNIT PRICE	EXT PRICE
1	BRAND REX 24 PORT OPTICAL PATCH PANEL	4	2500	10,000
2	48-PORT SWITCH	2	250,000	500,000
3	24-PORT SWITCH	3	200,000	600,000
4	BRAND REX 24 PORT PATCH PANEL	9	18,000	162,000
5	SATELLITE DISH/MODEM	1	3,000,000	3,000,000
6	3KVA UPS	1	250,000	250,000
7	12U DATA CABINET	3	12,000	36,000
8	42U DATA CABINET	1	65,0000	65,000
9	CAT 5E CABLE	LOT	7500	-
10	4-CORE FIBER OPTIC ARMORED CABLE	600M	1000/M	600,000
11	SINGLE FACE PLATE	LOT	800	-
12	TRANSPORT	LOT	LOT	LOT
13	MISCELLANEOUS	LOT	LOT	LOT
14	LABOUR	LOT	LOT	LOT
15	TRUNKING	LOT	LOT	LOT

NETWORK SECURITY AND MAINTENANCE

5.1 NETWORK SECURITY

The need for security in today's networks has become a requirement for any size of organization. Many different products, processes and policies can be used to maintain the information and its validity. Security is more of a mind set or way of thinking. It is important to understand that many things can be done to maintain a secure environment, but being 100% secure is not possible. The best any organization can do is to understand the security threats that may exist and how to best control and react to them.

When designing a network, it is essential to take into consideration the available options and the security impacts of each. When securing information, make sure to understand the default permissions created and how to modify those in the most secure manner. Understand the utilities available and create processes and procedures around these for users to follow. Be sure to enforce these standards, or else the tools in place provide no value. Understand what can be done to protect the individual data and how it is stored. Lastly, protect the network itself from outside intrusion.

In every network, the most important issue is security. Usually this is simple to achieve in small to medium sized businesses and quite complicated when dealing with large organizations. In this particular case, however, I am pleased to say that securing the network won't be difficult, due to the fact that servers will be located only in main computer rooms/server rooms, which will be locked to all unauthorized personnel.

Security cameras in this room are worth considering since this will provide greater protection from anyone trying to gain access to the room without permission.

As mentioned, all cables running from the central computer room will be fiber optic, which will make it impossible to tap into since the fiber as a medium is hard to break and reconnect and the cables installed in the trench will be protected from the underground conduit. Fiber-optic cable offers a high degree of security for data communications. It offers high security because it does not radiate EMI signal information that can be detected outside the conductor, it does not tap easily, and it shows a decided signal loss when it is tapped into. In addition, the diagrams for the underground cables will not be available to unauthorized personnel.

All hubs, switches and other devices critical to the network will be stored in the computer room/server room of each structure.

Connecting to the internet is quickly becoming a necessity for organizations today. Make sure that access from across this huge global network is monitored and locked down.

5.1.1 Selecting a Security Model (User-Level and Share-Level)

When you begin thinking about the security of your organization, you must first look at the security models you have in place or will use in the future. A security model is a generic term that describes methodologies used to secure a system. These can be anything from file versus share security or the underlying subsystem used by an operating system. Each model adds to the overall security architecture. Defining the model that you will use and deciding how it will be incorporated is important in any organization.

5.1.1.1 User-Level Security

One method of security that is available for use is file and directory level permissions. These permissions are based upon user or group accounts. Effectively combining these two types of permissions enables you to delineate what access a particular user will have when working in Windows 2000. You must understand the permissions available and how to apply them.

File and directory permissions are available on NTFS formatted partitions only. Other file systems available with Windows 2000, such as FAT, do not provide a mechanism to support permissions. In FAT file systems, only file attributes are available and any user can modify these.

In addition to the predefined permissions, you can custom specify certain access to a file or directory. Using individual permissions enable you to customize the files and directories to meet your security requirements. Predefined permissions use a combination of individual permissions to provide standard templates. The table below lists the predefined permissions available.

Access Permission	Description
No Access (None) (None)	Directory and File permission. This provides a user with no access at all.
List (RX) (Not Specified)	Directory permission. Enables users to display contents of directory along with permissions and attributes. This can include listing subdirectories if this permission is applied to all subdirectories as well.
Read (RX) (RX)	Directory and File permission. Enables a user to open and read files and directories and to run executable files. This also includes permissions granted by List.
Add (WX) (Not Specified)	Directory permission. Enables a user to open and add files to a directory and to create folders but they cannot view the contents of the folders.
Add & Read (RWX) (RX)	Directory permission. Enables a user to open and add files to directory. This also includes displaying directory contents and information and executing files.

Change (RWXD) (RWXD)	Directory permission. Enables users to open, modify and delete directories and files. This also includes displaying contents, navigating subdirectories, and executing and viewing files.
Full Control (All) (All)	Directory and File permission. Grants full rights to a file or directory. This gives a user all the permissions that are available by using or combining the previous items as well as the right of taking ownership of the directory or file.
Special File Access	File permission. This can be used to customize file permissions. By using this access, you are creating individual permissions rather than using the predefined permissions.
Special Directory Access	Directory permission. This can be used to customize the directory permissions. By using this access, you are creating individual permissions rather than using the predefined permissions.

Table 5.1 File and Directory Permissions Available

Individual Permission Abbreviation	Description
(R)	Read
(W)	Write
(X)	Execute
(D)	Delete
(P)	Change Permissions
(O)	Take Ownership

Table 5.2 Individual Permissions and Their Abbreviations

5.1.1.2 Share-Level Security

It is important not to become confused between share permissions which we just discussed and share-level security as they are two totally different items. Share-level security is available on client operating systems such as Windows 98 and Windows 2000. Access to a resource is determined by a password assigned to the resource and is not based on a user account or group membership. Any user that knows the share password can utilize the resource. Share-level security is easy to implement and maintain on small peer-to-peer networks; however, users must remember the password for each resource that is shared (unless password caching is in use). Access is very hard to control since

anyone who knows the password can gain access. This is one reason that user-level access is much more secure than share-level access.

5.1.2 Password Practices and Procedures

The most basic security mechanism is the password. We use passwords every day to access automated teller machines, to place calling card calls, and to access voice mail systems. Because it is such a basic concept, many implementations use this method to provide a form of security for accessing systems or resources. This widespread use is a concern, because passwords are noted as one of the poorest forms of protection available. According to the Computer Emergency Response Team (CERT), more security breaches result from poorly used passwords than from all other methods combined.

A password is a series of characters that can be used to lock down anything from an operating system to an individual file or directory. The purpose of this technique is to ensure that the user trying to access this resource is authorized to do so. If the user does not know the password, he is not allowed to access the resource. However, if a super-user account is compromised, then the other passwords stored in the same database can be at risk. In addition, someone can use one system as a starting point to reach other systems on the same network.

5.1.2.1 Password Policies

Setting up password authentication is a good start; however, it will be useless against a knowledgeable intruder without solid policies and processes defined. Each environment will be different and should be studied carefully to determine what policies would work best in that organization. Windows 2000 enables you to specify required security settings,

such as the number of characters required for a password, the number of tries before an account is locked out, and the maximum password age. Some security guidelines for creating passwords are listed below:

- ✓ Do not use your login name as your password. This includes reversing it, changing the case of the name, or any other variable.
- ✓ Do not use a familiar name such as your child's name, your spouse's name, or your pet's name.
- ✓ Do not use your first, middle, or last name. This includes any nicknames as well.
- ✓ Do not use a password of all single digits or the same letter. For example: 111111 or AAAAAAA.
- ✓ Do not use easily obtainable information about yourself, such as birth date, house number, or social security number.
- ✓ Do not use a word that can be found in a dictionary in any language.
- ✓ Use more than six characters in your password.
- ✓ Use a password with mixed-case characters. Use uppercase and lowercase randomly.
- ✓ Include non-alphanumeric characters, such as $@*.
- ✓ Do not write your password anywhere and do not give it to someone else for any reason.

In addition to these guidelines, you can implement other policies to secure your installation. Require that users change their passwords at defined intervals. In addition,

administrators need to understand that other systems can be used to compromise another installation. Most users will use the same password for multiple accounts.

Many organizations set stricter password policies for Administrator accounts than for normal user accounts, due to the security level. The higher security is due to the amount of access Administrator accounts retain. You also may want to set up two accounts for an administrator: the main account would have limited permissions for normal day-to-day activity, and the second would have full administrator access. Most installations also include a single main account with full access privileges. On a Windows 2000 Server, the account is labeled Administrator. You should rename this account to make it a little more difficult to hack into since every hacker knows that Administrator is the default name for the most powerful account in Windows 2000. Do not use this account once an administrative equivalent has been set up, unless absolutely necessary.

5.1.3 Data Encryption and Protecting Network Data

As more companies go online with the Internet, the need to protect data becomes more prevalent. The industry has strived to provide a more secure data transfer mechanism. The idea is to protect the data during a transfer and guarantee that it makes it to its recipient unread and unmodified. From this need, encryption services have grown in popularity. Multiple encryption implementations have been published and are now available to the public.

5.1.3.1 Data Encryption

Many different types of data encryption are available. Each methodology provides advantages and has a varying level of security. Encryption can be defined as the process of taking plain text data and converting it to a meaningless format that is unreadable, better known as ciphertext. Once the data has been transferred, a mechanism exists to decrypt the data back to its original format.

A key of sorts is used during the encryption and decryption process to handle the data. This key is the algorithm that the data can be compared against. Only the persons who have obtained this key can encrypt or decrypt the data. The longer the key, the more complex the encryption algorithm.

Common Encryption Programs

Due to the popularity of encryption, several vendors and organizations have written and published cryptographic programs to provide security. Each works a little different from the others and can be applied in different ways. The most popular program in circulation is PGP. In addition, Microsoft provides an application-programming interface for encryption services, called CryptoAPI.

✓ **Pretty Good Privacy**

A common implementation for encryption services is Pretty Good Privacy, or PGP. PGP is available for Windows, DOS, UNIX and Macintosh systems. It includes a full-featured tool set for encryption, digital signatures, and file compression. PGP includes multiple encryption methodologies including symmetric keys, asymmetric keys, and a random

number generator. PGP is available for anyone to use and works well with most security implementations.

✓ **CryptoAPI**

Microsoft foresaw the need to provide encryption services within applications. PGP and other implementations cannot work at the API level to provide these services to custom applications. Therefore, Microsoft created an API that enables you to add cryptographic services to your programs. This API contains a set of modules known as cryptographic service providers, or CSRs. The API is used in a very similar method as PGP; however, the encryption and decryption processes happen within the application.

5.1.4 Uses of a Firewall

As the disadvantages of non-secure networks have become more apparent in today's business world, additional forms of protection have been devised. Because it seems to be a requirement today to connect to public networks such as the Internet, some form of protection from hackers must be provided at the network level. A **firewall** protects a secure internal network from outside influence from a public insecure network. It can also be used to provide protection to a secure portion of a private network, such as Human Resources physical network.

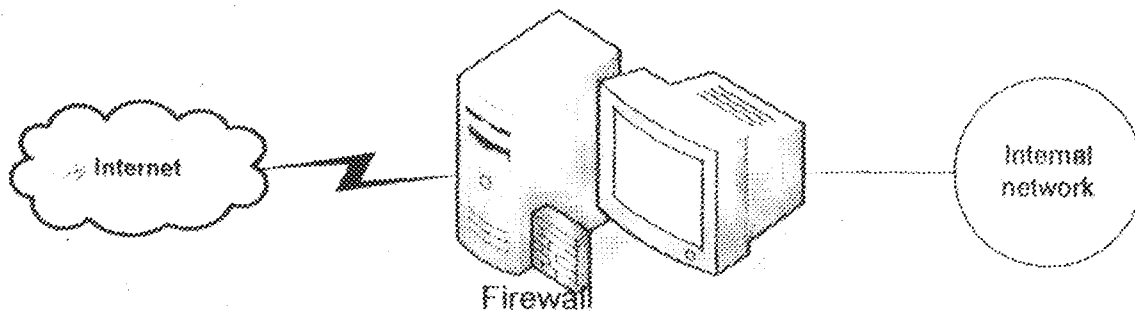
Although many vendors label products as firewalls, it is more of a network security strategy than it is a single product. A firewall is a collection of concepts used to protect one network from another. The most common implementation today is the use of a firewall between an organization's internal network and the Internet. Firewalls can be

very complex, because they provide more features than just packet filtering. They can also provide multiple layers of protection, including actually scanning the information stored in the packets for malicious data as they pass through. They use advanced techniques to monitor connections, to log potential intrusions, and to act upon these incidents.

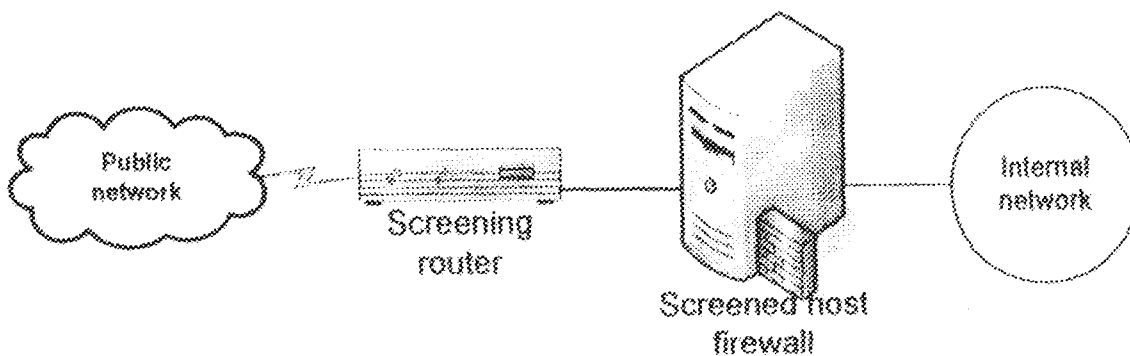
5.1.4.1 Firewall Architecture

As mentioned earlier, a firewall is a combination of techniques and technologies that are used to control the flow of data between networks. A firewall enables all traffic to pass through each network; however, it compares the traffic to a set of rules that determine how the traffic will be managed. If the traffic matches the rules for acceptable data, the traffic is passed on to the network. If the rule specifies that the data be denied, the traffic cannot continue and will be bounced back. Although some implementations may do this differently, the same basic functionality is used.

A *dual-homed firewall* consists of a single computer with two physical network interfaces. This computer acts as a gateway between two networks. The server's routing capability is disabled so that the firewall can handle traffic management. Either an application-level proxy or circuit level firewall software is run to provide data transfer capability. You must be careful not to enable routing within the network operating system or you will bypass your firewall software.

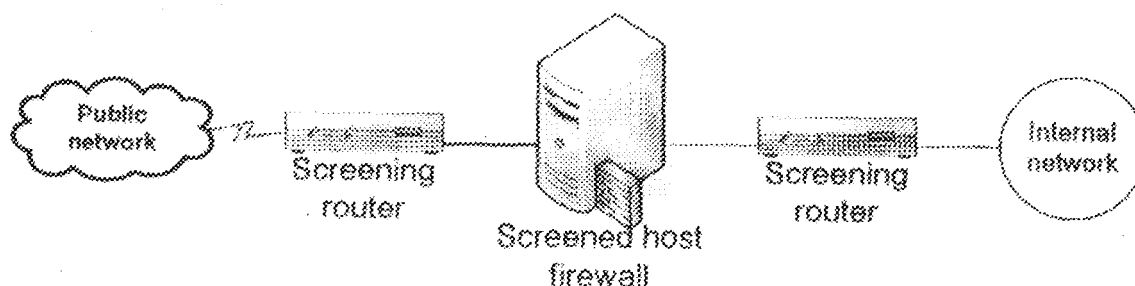


A *screened-host firewall* configuration is considered by many to be more secure than the dual-homed firewall. In this configuration, you place a screening router between the gateway host and the public network. This enables you to provide packet filtering before reaching the host computer. The host computer could then run a proxy to provide additional security to this configuration. As packets travel into the internal network, they only know of the computer host that exists.



A *screened subnet firewall* configuration takes security to the next level by further isolating the internal network from the public network. An additional screening router is placed between the internal network and the firewall proxy server. The internal router

handles local traffic while the external router handles inbound and outbound traffic to the public network. This provides two additional levels of security. First, by adding a link internally, you can protect the firewall host from an attack by an internal source. Second, it makes an external attack much more difficult because the number of links is increased.



5.1.4.2 Firewall Types

There are three types of firewalls that can be used: Packet Level firewall, Application Level firewall, and Circuit Level firewall. Each uses different security approaches, thus providing advantages over the others. One additional feature that was discussed earlier is encryption services. Most firewalls provide some sort of cryptographic services for data transfers.

With a complete understanding of the features and type of security that are needed from a firewall, you can then determine the implementation that best fits your organization.

Packet level firewall: A packet level firewall is usually a form of screening router that examines packets based upon filters that are set up at the network and transport layers. You can block incoming or outgoing transfers based upon a TCP/IP address or other rules. For example, you may choose not to enable any incoming IP connections but to enable any outgoing IP connections. You can set up rules that will enable certain types of requests to pass while others are denied. The information that rules can be based on, includes source address, destination address, session protocol type, and the source and

destination port. Because this works at only three layers, it is a very basic form of protection and is only a type of implementation. To properly provide security to another network, all seven layers must be protected by a full-featured conventional firewall.

Application level firewall: The application level firewall understands the data at the application level. Application layer firewalls operate at the application, presentation and session layers. Data at the application level can actually be understood and monitored to verify that no harmful information is included. An example of an application level firewall is an Internet proxy or mail server. Many uses are available through some form of proxy, however, these functions are usually very intensive to provide security at that level. In addition, often clients must be configured to pass through the proxy to use it. Proxy servers are also used to mask the original origin of a packet. For example, an Internet proxy will pass the request on, however, the source listed in the packet is the proxy server address. The overall server doesn't just filter the packets, it actually takes in the original and retransmits a new packet through a different network interface.

Circuit level firewall: A circuit level firewall is similar to an application proxy except that the security mechanisms are applied at the time the connection is established. From then on, the packets flow between the hosts without any further checking from the firewall. Circuit level firewalls operate at the transport layer.

5.1.4.3 Firewall Features

As firewalls have evolved, additional feature sets have grown out of or been added to these implementations. They are used to provide faster access and better security mechanisms. As encryption techniques have improved, they are being incorporated more

into firewall implementations. New management techniques and technologies such as Virtual Private Networks (VPNs) are now being included as well.

5.2 DISASTER PLANNING AND PREVENTIVE MAINTENANCE

5.2.1 DISASTER PLANNING

Disaster planning is often one of those things that gets talked about, planned, and then never accomplished. Try questioning a group of network administrators about disaster planning. Ask them, "How many of you have disaster plans in place?" and you'll see some hands up. Ask, "How many of you have written disaster plans in place?" and many of those hands will go down. Ask, "How many of you have actually tested those plans and revised the parts that didn't work?" and most hands will go down. It's also a good bet that at least one of the people whose hand is still up is lying.

No one likes to think about the possibility of the network or the file server going down in flames, but it's better to dwell on this depressing possibility beforehand than to explain afterward to the boss why you weren't prepared for data loss.

5.2.1.1 The Nature of Disaster

"Disaster" is such a dramatic word that it might sound overdone. How likely is it that disaster could touch your company? If you think of disaster only in terms of natural disasters or massive hardware failures, then disaster might not seem very close at hand. If, however, you consider disaster in terms of anything that could stop the company from functioning for an undetermined length of time, then the notion of disaster is easier to accept.

Broadly speaking, three categories of disaster could affect your organization:

- ✓ Natural disasters (events)
- ✓ Technical disasters (breakdowns)
- ✓ Human-related disasters (behavior)

These categories are not mutually exclusive. A disaster that apparently fits into one category could be slotted into another category because of its cause. For example, the slant on a power outage changes based on whether the cause is sabotage at the power company, an electrical storm, or a failed switch at your building. For the purpose of recovering from a problem, however, it really doesn't matter what caused it.

Events

Downed power lines, broken water mains, fire... Natural disasters don't have to be as dramatic as earthquakes swallowing your company headquarters. If your office shares a building or office park with others, a fire starting in a neighboring company can threaten your operation. Even a broken water main can render your office unusable and possibly destroy data.

Natural disasters don't always directly touch your office, but their effects may be felt there. An area power outage can render your office unusable, a nuisance even if every server is equipped with a UPS and able to do an automated orderly shutdown. Even if you don't experience any data loss, how can your office work if a bolt of lightning blows the power out?

Breakdown

Technological failures are often the easiest disasters to anticipate and prepare for. The simplest plan usually is redundancy — backups, hot-start servers, and alternative office sites are fine examples of how redundancy can help you overcome some breakdowns.

Breakdowns aren't limited to network equipment. In a heat wave, you can't run computers without air conditioning. Breakdowns don't have to mean that the equipment's actually broken, either. If a virus renders your network server unusable because you're afraid of spreading the contamination, the server is effectively broken, even if it boots up fine.

Behavior

Human-related disasters are probably the hardest to prepare for. If you know your geographical region, you can prepare for weather. If you know your equipment, you can prepare for hardware failures.

Technological breakdowns can, directly or indirectly, be caused or exacerbated by humans. If the backup operator hasn't been doing his or her job, then a technological problem becomes a disaster when the server's hard disk fails and you need to reload the backups. Another behavior-caused technical disaster could be unlicensed software. If the Software Publishers Association catches your company with unlicensed software on company machines, they can temporarily inconvenience your operation and levy very steep fines. It's odd to think, though it is illegal, that having too many copies of Microsoft Word 6 for Windows could destroy your company, but if a disgruntled employee calls the SPA on you (the SPA gets most of its information from tips like that), then it's a definite possibility.

5.2.1.2 Creating the Disaster Planning Team

Thus far, we've been talking about a disaster plan as though it were the creation of one person. That's not accurate at all. For a plan to be really effective, it requires several sources of input:

- ✓ The people who need to use the network
- ✓ The people who know how to fix the network
- ✓ The people who control the resources available
- ✓ The person who's in charge so that he or she can contribute an overall perspective and approve funding

How many people crowd the table – and who they are – depends on the size of your enterprise. One person in your organization might fill more than one of these jobs, but no matter how responsibilities are allocated in your enterprise you really can't create a useful plan without input from all these sources. Let's look at the role of each of these players in turn.

The Personnel Manager

The personnel manager, in this instance, means the person in charge of the staff. The disaster plan needs his perspective because he is the person who knows the most about what people are doing with the network. He should know what applications the staff uses most often, what time everyone comes in (and therefore the time that it would be nice to have everything fixed by), and in general, what everyone in the office uses the network for. This should help you prioritize if time is short and you have to figure out what to fix first. The personnel manager can help prepare the staff for disaster, too. Training is key to

surviving a problem, and the personnel manager is the most likely candidate for making sure that this training is accomplished. The personnel manager should make the following contributions to ensuring that the staffs are prepared:

- ✓ Clear, complete written job descriptions
- ✓ Regularly scheduled disaster-preparation training (including cross-training so that more than one person knows how to do each task)

The Network Administrator

The network administrator is the technical voice of the disaster planning staff. Of all the people creating the plan, he's the one most likely to know what recovery hardware and software are available, how much it all costs, and how to research other possibilities. Although the network administrator isn't likely to know everything about all company assets, he can help the business manager (whose role is described later) with details like preferred vendors and the computer needs for an alternative site.

Keeping tabs on the components of each machine on the network is another part of the network administrator's job, and this kind of information can prove valuable to the planning process. If, for example, the main server has an IDE controller, there's no point in buying a SCSI tape backup system for it unless you also purchase a host adapter. If this seems like an obvious point, think again. At one company I know of, the business manager purchased two new hard drives and controllers without first checking with the network administrator to see what slots were open in the servers those hard drives were for. When the day came to replace the hard drives, one of the servers had no VL-Bus slot available, rendering its new controller useless.

The network administrator must also work as the voice of reason. As the person who presumably has the most computing and networking knowledge, he has to explain to the others on the team why it's not practical to replicate all directories onto another server via a modem or what the current capacity limits for tape devices are. This kind of technical advice is vital to both the success of the plan and the network administrator's sanity. Much of the responsibility for developing and implementing the plan will likely rest on his shoulders.

The Business Manager

The business manager might have to act as another kind of voice of reason. As the person with the best idea of the company finances, the business manager has to take the pricing information that the network administrator provides and balance it against how much the company can spend on a disaster plan. Although it would be nice to believe that there's no limit to how much your company is prepared to spend on this worthy cause that simply isn't practical. There's no point in the company running short on operating expenses in order to over-prepare for disaster -- it's the job of the business manager to make sure that this doesn't happen. The personnel manager wants to make sure the staff is able to work and the network administrator wants to keep the network going, but the business manager is responsible for making sure that the company doesn't go broke fulfilling these goals.

Part of not going broke in the face of disaster lies in making sure that appropriate insurance covers the possibility. The business manager should bring all relevant insurance information to the meeting, including coverage data for the following:

- ✓ Casualty claims (from both employees and customers)
- ✓ Property damage claims
- ✓ Business interruption claims

The business manager can provide other information that's useful to the disaster plan. As the person in charge of purchasing, the business manager should have some kind of inventory of the company's hardware assets -- even if the network administrator knows what's in each machine, he may not have a comprehensive list. Why does this matter to a disaster recovery plan? Two reasons, actually. First, a hardware inventory makes it easier to know how old all the hardware is and prepare accordingly. Second, a hardware inventory is useful for knowing what you've got around to fix the network or individual PCs. To keep the list accessible in case of network disaster, don't keep it in a database on the server -- an erasable whiteboard or chalkboard works better -- and a copy of the complete list should be stored off-site and updated periodically.

5.2.2 PREPARING FOR VIRUSES

Since they started getting a lot of press about ten years ago, computer viruses have been a major concern for businesses. In 1991, I saw one office shut down its computer operations entirely for a day, because it was Michelangelo's "attack date," and they weren't taking any chances. (None of their machines had tested positive for the virus, incidentally, and all were stand-alones except for one on a line to their main office.)

drive. I'm not infected yet. I do a DIR and pull off the files that I need, reading them on my machine. Still no infection. I write to the files on the floppy. Not a problem.

Then, I need to reboot for some reason. With the disk in drive A and the door closed, I press Ctrl+Alt+Del to restart the computer. When the computer halts during the reboot, I notice the familiar Non-system disk message on my screen. I chastise myself and remove the disk to finish booting.

Now, I'm infected. I've made my computer access all the files on the floppy, looking for system files to boot from, so even though none of the files were bootable, the virus took hold.

I think that this dormant stage of viruses is what makes them so scary to many people. You trust a computer with your data, and the idea that it might suddenly turn on you and format your hard disk at an inappropriate time is more than a little unsettling. Let's talk about how to avoid this unsettling behavior.

5.2.2.3 Preventing Virus Attacks

The comparison between biological viruses and cybernetic ones has been made so many times that I refuse to make it again, but it's pretty accurate. If you're living in a germ-free environment, you won't get sick; if you're computing in a germ-free environment, your computers won't get sick. Let's take a look at some of the measures that real-world enterprises are using to prevent virus attacks.

Quarantine Servers. Today, when more than a few people work at home at least part of the time, it's impractical to forbid people to bring floppies to work, but you can insist on a quarantine period. Create a company policy requiring people to drop disks off for checking when they first bring them in and before sticking them into a floppy drive.

Then it's up to you to virus-scan the floppies as quickly as possible. Do it early in the day if you can so that people don't start ducking the floppy bin because of delays in getting to use their data. If you've got an extra stand-alone machine that you can use as the virus-checker, do so. If not, just run the virus checks on any machine that you know is clean. If the scanner detects a virus, clean it.

If you follow this procedure for every floppy that comes in the door of your office, you should be able to prevent most virus attacks.

Educate Users. Educating your users about virus attacks goes a long way toward preventing virus attacks upon your network. Tell them what viruses are, where they can come from, what they can do, and how the measures you're instituting will prevent infections — but only with help from them. Instituting a mandatory disk-scanning program, for example, won't help at all if no one but you understands why you're doing it.

Running Effective Virus Scans

You can perform a real wall-to-wall search for viruses on a machine if you do it right. First, before scanning a machine's hard disk, format a floppy to be a system disk and then copy your favorite virus scanner onto the floppy. Next, cold boot (turn the machine off and then back on) from the floppy to restart the machine. Then run the virus scanner. Why cold boot the machine first? Some viruses can fake a reboot unless you've actually turned the machine off.

Second, make sure that you update your virus scanner regularly. Most makers of anti-virus software run BBSs of updated virus signatures. Download these on a regular basis. Remember, there's no generic "there's a virus here" signal, most scanners work by

looking for signatures belonging to specific viruses. Even if it's a common virus, your scanner can't find it without knowing how to look for it.

5.2.3 NETWORK PREVENTIVE MAINTENANCE

A network is a collection of electrically-powered pieces of equipment, connected via cables, and running programs. In order for the network to work properly, every piece of the network must work properly. Network preventive maintenance (NPM) is concerned with anything that can be done to prevent any component of a network from failing.

A network is not just computers; therefore, NPM is not just concerned with blowing dust out of PCs. Each component of the network (cabling, servers, workstations, peripherals, and so on) has its own special usage and maintenance concerns that must be dealt with in order to provide maximum network reliability.

While proper preventive maintenance of any sort provides the opportunity to detect and correct problems before they become failures, it cannot prevent all failures. Just as no car drives forever, no network runs forever. All a good NPM program can do for your network is detect and prevent more problems than if NPM were not done. No NPM program can possibly detect and prevent all failures, and eventually any network will have to be replaced.

The NPM program itself does not determine the reliability of the system--the quality of the system is the most significant factor. A low-quality system requires more preventive maintenance than a high-quality system, and since preventive maintenance cannot detect

and prevent all failures, a low-quality system usually has more failures than a high-quality system no matter what preventive maintenance program is in place. Therefore, the results of any NPM program depend on the quality of the network itself. This means more than just hardware components--a network is a collection of hardware and software, all connected somehow. The quality of the software, connections, and how everything is assembled has to be taken into account when assessing the overall quality of a network. The best NPM program in the world is for naught if your cable plant is punched down with a pocketknife, your PC's are second-hand clones, you use only discount software or shareware, every time you install any software you do it differently, and your network documentation consists of a folder holding user's guides for some of your computers. The quality of the network is determined not only by the quality of the items you buy, but also by the quality of the effort made to install and keep track of these items.

There are three things that need to be done before you'll have a successful NPM program:

- ✓ Do it right the first time
- ✓ Duplicate it the same way every time
- ✓ Document everything

In the following sections, we discuss these concepts as they pertain to the various components of a network, and examine NPM concerns for each component.

AC POWER

Every piece of equipment on your LAN requires electrical power. Even the hubs and MAUs that do not plug into AC outlets get their power from something else that does plug into an AC outlet. There might not be much you can do about the power the utility company provides you, but that increases the importance of what you can do.

Do It Right

Until you know you have good, clean power, you always have to factor power problems into any troubleshooting situation. How can you make sure you have good, clean power? Base this information on actual tests of your power, not someone's casual assessment. Failures caused by power problems can cost you dozens of hours of troubleshooting, as well as thousands of naira

Duplicate It

Make sure all your wiring circuits are equivalent. Don't mix and match circuits of different load capacities, or put twice as many outlets on one leg as on another.

Document It

Make sure you have an up-to-date floor plan that includes the electrical wiring diagram. It should indicate where the circuit breaker panel and outlets are, and should clearly show which outlets are on which circuits.

Dos and Don'ts

Don't just assume that you have good power. Until it's been tested, assume you don't. Show your concern for your LAN server and associated equipment by having a special dedicated and isolated ground circuit installed just for them.

UPS SYSTEM

Your UPS system is supposed to protect your critical equipment and provide enough battery-powered runtime to allow it to be shut down properly during a power failure. As such, it typically spends 99.99 percent of its time doing very little, but then suddenly needs to be doing its job exactly right to prevent a very serious problem. Proper preventive maintenance for your UPS system is essential if you want to be able to rely on it.

Do It Right

Make sure your UPS system is large enough to handle the load of all the equipment you have plugged into it. Also, while we usually think of UPSs as providing power during a power failure, they should also provide complete protection from sags, spikes, surges, EMI.

Duplicate It

If you have more than one UPS, keep them the same. This means the installation and maintenance procedures are the same, reducing the chance for errors. It also means that you have 100-percent swappable units. If the UPS on your most important piece of equipment fails, you can replace it instantly with the UPS from another, less-critical piece of equipment without spending a full day reconfiguring it.

Document It

Keep copies of the original invoices, and register the units for warranty purposes. Document the expected battery life and make a note on your to-do list that informs you well in advance of this date. Document all test and monitoring results, and analyze them periodically for any trends or aberrations.

The trouble is that this kind of reaction is exactly the one that virus authors are looking for. I admire the tenacity and talent of some virus authors, but I think that writing virus programs is a totally asinine way to spend this tenacity and talent. The best way I can think of to encourage them to find another outlet for their skills is to spoil their fun. To that end, let's talk about some ways in which you can avoid virus attacks, or recover from them without much difficulty.

5.2.2.1 Understanding Viruses

Computer viruses are not supernatural. They possess no intelligence and can't possibly do you any harm unless you let them.

How would you let them? By letting an infected floppy (the most common means of infection) into your computer. A virus can only get to your system in one of two ways: during boot-up or if you run the virus's program file. Essentially, your computer must access the virus program in some way in order for it to take effect. Whether this happens by booting from the floppy – even an aborted boot usually infects your system – or by running the virus program is irrelevant. (By the way, an infected floppy doesn't have to be a boot disk to infect your machine by leaving it in drive A while rebooting. Any infected disk might do the trick).

5.2.2.2 How does a machine catch a virus?

Not everyone understands how infection works, so it's worth explaining. Suppose, for example, that I go out to a client site to fix a network. While I'm there, I borrow a floppy disk to copy some code that I want to review at home. This floppy has a boot sector virus like B1 on it, but I don't know that. I bring the floppy home, and stick it in my floppy

Dos and Don'ts

Do line up procedures and budget money to replace the batteries well in advance of their expected failure date. Test the unit regularly and document the results. Don't plug any additional equipment into an existing UPS without checking the load capacity of the UPS. Dispose of used batteries safely and properly. Higher temperatures decrease a battery's life, so don't place the UPS in an unventilated and crowded cabinet.

Cable Plant

Besides electricity, the other component of the LAN that every piece of equipment shares is the cable plant. No matter how varied or large your network, everything depends upon the connecting cabling to be working at 100-percent efficiency at all times. Cabling problems are among the most aggravating and frustrating problems to deal with, but a little preventive maintenance goes a long way in preventing cabling-related problems. Since the cabling literally just lies there, once you get it right it tends to stay right.

If you only have enough budget money to test either the AC power or the cabling, get the cabling tested first. There is less that can go wrong with AC power, and almost nothing you can do about AC power problems. On the other hand, there are many things that can go wrong with your cable plant, and there fortunately are many things you can do to fix these problems. Get your cable plant tested as soon as you can, and prepare to be surprised.

Do It Right

Make sure that your cabling has the capacity for, and is designed to work properly with, the kind of network you are running. Anything less than Category 3 (Cat 3) wiring is unacceptable for today's networks. Category 5 (Cat 5) wiring is typically installed today.

Also, all the wiring needs to be the same – a common problem is mixing different grades of wiring in a network. Maybe the original network was Cat 3, but some stations have been pulled using Cat 5, and the patch cords are a mixture of Cat 3 and Cat 5. Or maybe some silver-satin phone cabling was thrown in, just to make things interesting! (The silver-satin cables used for phone wires are never acceptable as network wiring.) According to Frank Leeds of Seitel, Leeds, and Associates, a certified cabling expert, mixing different grades of cabling creates impedance mismatches that can cause problems for your network.

The wiring itself is not the only thing that needs to be category-certified. All the connectors, punch-down blocks, patch panels, hubs, and station jacks need to have the same rating as the wiring. If you scrimp on one link in the chain, you've crippled your entire cabling system.

Of course, using all the best components won't do you any good if the wiring is not installed properly. Crossing wires, untwisting the wires too far from the connectors, or not securing connections properly can kill any cabling system. A quick survey of your wiring closets and a couple of station jacks should give you a good idea of what your whole cabling plant is like. The best thing to do, however, is to get your cable plant tested by a certified cable installation company. Each and every run of wire needs to be tested to ensure that it meets the specifications of that category level. Since this test typically includes everything from station jacks to patch panels, it eliminates the need to test each component individually and also indicates the overall quality of the installation. If the

numbers aren't up to specification, you'll have to start digging in to find out if you have substandard wall plates, poor installation, or possibly even the wrong cabling.

Duplicate It

Wire all the jacks the same way. Avoid having different station jack configurations as much as possible. This is likely to confuse you, and guaranteed to confuse your users. While it is an easy fix to make, unplugging a telephone from a data jack can be avoided. Make sure that you have specifications and part numbers for all the components of your cable plant, so that when (not if) you have to add more pulls to your plant, they can exactly match your existing pulls.

Document It

Documenting the cable plant is a classic case of "pay me now or pay me later." It is so tempting to finally get everything working, and then just walk away from it. Once it is working, it shouldn't break, so why bother documenting it? Here's why - because there is no way that your computer system and phone system will not change in the next few years. Every minute spent documenting a cable plant upon installation would have to be multiplied by ten to do the same job down the road. Besides, what better time to straighten out any problems than right after the contractor has supposedly done the job, right? Consequently, future changes are usually implemented based on assumptions that bear no relationship to reality.

Documentation should include not only a marked floor plan, but each pull should be plainly, clearly, and unambiguously marked on each station jack and its terminating end in the wiring closet.

Do's and Don'ts

Do assume that any cable plant — new or existing — that has not been tested and documented is out of compliance with specifications. If you have an untested plant, get it tested and documented immediately.

If you are installing a new plant, make sure that the installation contract includes a test for each pull. All the results should be provided to you. Once the contractor is done, plug in a server and carry a laptop around to each port to verify that it can connect to the server before accepting the job.

Just because the contractor can pull a wire from one corner of your building to another doesn't mean it will work. Ethernet typically is limited to 100 meters (about 300 feet) from hub to workstation. Make sure you know and stay within the limits of your particular wiring and networking specifications.

Hubs / MAUs

Keep hubs and MAUs dry and clean, also, make sure that you know what all the blinking lights and switches do. If you are having a system failure that you think is caused by something in the wiring, it helps to know if the light on your hub or MAU is supposed to be flashing green or solid red to indicate normal operation. Don't forget to clearly mark all units, as well as the cables interconnecting the units, with descriptive identifiers.

If you can't get any more of the old units, it's time to replace everything. Life is too short to spend it trying to track down incompatibilities between different makes and models of hubs and MAUs.

Workstations

Every time I think I've found a great preventive maintenance for workstations, I discover I'm breaking about as many units doing the preventive maintenance as the number of units I am possibly saving from premature failure.

I thought that cleaning floppy disk drives made a lot of sense until I read an article by a drive manufacturer that stated most of the cleaning solutions being used were more destructive than just letting gunk build up. I thought that blowing dust out of the insides of PCs with cans of air was a great (albeit messy) idea, until an engineer pointed out that there was a good chance of actually forcing dust and dirt into the cracks and crevices of the electrical connectors inside the computer. Heck, some monitors require special cleaning solutions even to clean the dirt off the glass! I'm almost afraid to crack a cover anymore for fear of the damage outdoing the good.

Do It Right

Buy the highest quality computers you can, because cheap ones take more support and cause more problems than more expensive ones--not every time, but far too often to bet against it.

Duplicate It

Whatever you're buying, try to buy only one make and model and always set them up the same. Or, if you have to buy more than one type, try to minimize the differences as much as possible. Always set them up the same way. I've found a very effective way to do this is to create a working model, then copy the image of the entire hard disk up to the network. Whenever I need to install a new computer, I simply wipe out its local hard disk and copy down the master image from the network after booting up from a floppy. Afterward, I need to make only the personality changes (TCP/IP addresses, LU assignments, user or computer name, and so on). Whenever I want to make a change to my workstations, I use the master image from the network as a model, and figure out the best way to make the changes to it. Of course, this only works as long as users aren't customizing their individual configurations too much.

Document It

In my opinion, the toughest thing to do on a network is to document and track the configurations of the workstations. There are so many things to track that the effort is overwhelming.

These are some of the things that you might have to take into account when planning to fix or upgrade a group of workstations: boot-up configuration (contents and specifics of CONFIG.SYS and AUTOEXEC.BAT), DOS version (and REV level), Windows version and whether all are local or not, ROM BIOS version, NIC BIOS level, whether the NIC has a BNC or UTP port or both, NIC type, available card slots, available drive bays, video card type, number of serial or parallel ports, other equipment installed (sound

cards, SCSI adapters, and so on), mouse type (PS/2 port, bus card, or serial port), free disk space, serial number, user name, user location, and station jack ID. No matter how sophisticated and complete the inventorying software is, I seem to always have to go out and document something by hand. The more you can collect automatically and electronically, though, the better off you'll be. Don't expect any package to do it all for you. I recommend using the best workstation inventorying package you can afford, but understand that you'll probably have to document something the next time you consider making wholesale changes to your workstations.

Dos and Don'ts

Don't crack a case unless you really have to. Try to keep workstations out of harm's way and never lay them flat on the floor (the dirtiest and dustiest computers are those placed flat on the floor). I prefer putting all workstations on the floor in a vertical position with just the keyboard and monitor on the desktop.

LAN Connection

Make sure that the station jack is securely fastened to the wall or partition. Loose "biscuit jacks" on the floor are unacceptable; they get kicked around and eventually will cause problems. The station cable must be the same category level as the main wiring. Never, under any circumstances, use silver-satin phone cord for a station cable. Double-check that the station cable is plugged firmly into the NIC. If the station cable shows any signs of wear (loose connectors or cuts in the shielding), replace it immediately. Using a frayed or defective station cable is an invitation for workstation failure.

Hardware

Use the best equipment you can talk the financial department into buying, and purchase as few different models as possible. Purchase everything from one manufacturer if you can (That way, you only have to create a relationship with one tech support department!) Standardize as much as you can, but realize that you'll never be able to standardize everything.

Operating Systems

Keep everyone running the same version and revision number of the operating system, even if it means removing newer versions from recently purchased computers. Better to face the devil you know than the one you don't. New versions might solve some bugs you've had to work around on the older version--but they are almost guaranteed to create new problems for which you will have to figure out solutions. Try to keep everyone using the same version; upgrade only after complete and thorough testing of the new version. Being the first one on your block to load the newest version of any program simply means you get to be first to crash and burn.

Applications

Everything that is true for operating systems is true for application programs. To make life simpler, more maintainable, and much more reliable, I advocate loading all applications on the network only. It's much easier to support and upgrade one configuration on the network, rather than a separate configuration on each workstation across the network. What might be lost in customizability and performance is certainly made up by reductions in support, maintenance costs, and downtime. Centralized

applications should invalidate anyone's argument that the network is down too often to depend on.

Servers

I'm leery of cracking the case on a workstation, and therefore I'm practically terrified to crack the case on a file server. While dropping a screw or bending a connector on a workstation might inconvenience a user for a day or so while I get the PC repaired, the same simple error on the file server will inconvenience me until I get it back up and running. This is a reason to never make any changes to the file server an hour before everyone starts work. You'll end up starting your explanation of the prolonged server problem by saying, "All we had to do was..." or "It was supposed to be a five-minute job that..." Try working early on Saturday mornings instead. That gives you all day Saturday and Sunday to recover from a failure if one occurs. Other than that, the same admonitions and advice given for workstations also apply for servers.

Printers

Printers are arguably the most complex and maintenance-hungry components of a LAN. Just the fact that these devices can pick up only one piece of paper at a time, feed it through a series of rollers and guides without tearing it to shreds, and print something intelligible on it is amazing. Laser printers not only do that, but also bounce a beam of laser light off a rotating mirror, onto a drum that circulates through a cloud of carbon particles and creates text and graphics on a piece of paper. By definition, a laser printer actually prints using smoke and mirrors! Yet I find that most, if not all printers are ignored and under-maintained. The only time they usually get any attention is when they finally fail.

Do It Right

Buy the best quality printers you can afford. Keep in mind that cheaper printers or off-brand printers can only claim to emulate the printer you know you ought to buy. "Emulate" means that an off-brand printer tries to work almost as well as the name-brand printer.

Duplicate It

Just keep things as consistent as possible, and whenever you do install more than one of the same types of printer, configure them identically.

Document It

Never, under any circumstances, loan out the user's manual for a printer. Keep it in a safe if you have to. It is almost impossible to guess, remember, or figure out how to configure a printer. If your printer has lost its settings or someone has changed them, you'll need the manual in order to know how to reconfigure it. Knowing how to reconfigure the printer is only half the battle – if you haven't documented the working configuration, you'll have to start from scratch again.

It's easy to waste half a day or more getting all the settings exactly right. Even then, invariably, someone will complain that their spreadsheets "just don't print the same anymore." In a pilfer-proof safe you should keep a user's manual and configuration listing for each printer.

Do's and Don'ts

How balanced is your printer sharing? Are all your printers being worked equally? Do you even have any idea how many pages each printer is printing per day/week/month?

Remember that every printer has a recommended duty cycle (usually described as the maximum number of pages per month) and if your printers exceed this, you're more apt to have problems. If you have one printer doing more work than others, it makes sense to rotate them in and out of the "hot spot" so you don't have a premature failure. But to find potential problems like that, you have to know how much you are printing every month.

Keep it clean! Unlike PCs, printers really thrive and appreciate being cleaned out on a regular basis. Clean off the corona wires and get any excess paper gunk out of the feed assembly; always follow the manufacturer's recommendations.

5.2.4 ENVIRONMENTAL FACTORS THAT AFFECT COMPUTER NETWORKS

Most networks have a centrally located area that can safely house all of its network appliances and servers. Within this room is a multitude of special features that can help to protect the computers and other environmentally "sensitive" equipment from failing due to extreme temperatures.

Computers, like most other electrical hardware, are affected by temperature, moisture, vibrations, and electrical interference. If the computers are exposed to these elements, they can act irregularly and sometimes fail. Luckily, there are standards that protect computer components from these situations

Cables:

Underneath the protection of most network cables lies a fragile layer of wire (or glass, in the case of fiber optic) that carries the data from one computer to another. Like most other computer components, this wire is not resistant to moisture, heat, or other electrical

interference. To protect this cable from harm, a covering is placed over the wire to protect it from breaking or accidentally becoming wet.

Cables that bring data to networks come in different forms, from copper to fiber optic. The type of cable determines the length that it can be. When a cable exceeds the recommended distance, the signal begins to fade. The table below lists the types of cables, their characteristics, and the distance they can carry a signal.

Type of Cable	Characteristic	Length
10Base T	Flexible, uses RJ-45 connector	100 meters/328 feet
10Base2	Less flexible than 10BaseT, uses a BNC connector to hook computers together. Must be terminated on one end	185 meters/607 feet
10Base5	Rigid, does not bend well around corners. Not used too often; AUI connector	1640 feet
Fiber optic	Does not do well in tight changes of redirection. Carries data extreme distances. Easily broken, fragile	2 kilometers

The Network Operations Center

The Network Operations Center (NOC) is the home base for all of the important servers on your network. The NOC enables you to centrally manage and keep a close eye on all of your networked data.

An NOC, above all else, needs to be secure and able to house all of the data and servers. Normally in a locked room, the NOC is a secured room that is equipped with different types of fire suppression (Halon, Foam), raised floors to place the cabling, and the

temperature control. A price cannot be put on the value of your data, so this room should never be compromised in any way.

Room Conditions

The room conditions of your NOC should be cool, dry, and temperature controlled. Computers and other electrical equipment do not like humidity, heat, or extreme cold, so you should be very careful to regulate the temperature of your NOC. When a computer overheats, there is no guarantee that the data on your servers can be saved.

Because computer equipment is very sensitive to moisture, you need to use a form of fire suppression besides water. Putting out a fire in your NOS with a sprinkler system would ruin all of your computer equipment. There are many different types of foams or Halon used to put out fires quickly and safely, while minimizing the potential damage to your computer equipment.

Minimizing Electrical Interference

Electromagnetic interference (EMI) can wreak great havoc on any type of computer equipment. You might be aware of certain types of speakers that are magnetically shielded to prevent electrical interference. However, magnets and computers don't mix, so this concept unfortunately doesn't mesh well. Your alternative to this is to keep all of your computer equipment away from any electrical device that may interrupt the computing power of your data.

CONCLUSION AND RECOMMENDATION (S)

6.1 CONCLUSION

This project is of high technological/technical status and economical value to any Organization once implemented fully. Looking at the current increase in purchase of computer systems in various departments of F.U.T Minna, there could not have been a better time for maximizing its performance by having all of them connected on a network.

6.2 CONSTRAINTS

I encountered slight difficulty before I could obtain the Master Plan for Bosso Campus. This caused work on the project to be delayed for quite some time.

6.3 RECOMMENDATION (S)

I strongly recommend that this project "PROPOSED LAN SOLUTIONS FOR ANY ORGANIZATION: A CASE STUDY OF F.U.T MINNA" should be fully implemented by the University Administration in the nearest future so that both Academic staff and students as well as the university community at large can benefit from the numerous gains of this Local Area Network.

The Master Plan of the F.U.T Minna Bosso Campus, and other essential documents should be provided easily for students working on projects that involve work on the campus so as not to delay their project work

I would also like to recommend that once this project has been implemented, a similar one should likewise be implemented at the F.U.T Minna Permanent Site.

REFERENCES

1. Mitch Tulloch, *Microsoft Encyclopedia of Networking*, Microsoft Corporation; 2000; ISBN 0-7356-0573-4
2. Craig Hunt, *O'Reilly™ TCP/IP Network Administration Second Edition*, O'Reilly & Associates; December 1997; ISBN 1-56592-322-7
3. *Nigerian Journal of Engineering Management*, volume 3, no 3, July-Sept 2002
4. *Fiber-Optic Technology*, ©The International Engineering Consortium; (<http://www.iec.org>)
5. Bill Wagner, Chris Negus, *The Complete Idiot's Guide to Networking Second Edition*; Que Corporation; February 1999
6. Craig Zacker, Paul Doyle; *Upgrading and Repairing Networks*; Macmillan Computer Publishing
7. Osborne/McGraw-Hill; *Network+ Certification Study Guide*; Macmillan Computer Publishing 1999; ISBN 0-07-211846-6
8. Student Affairs Department; *F.U.T Minna Handbook of Information for students*; 4th Edition.
9. Chuck Semeria; *Understanding IP Addressing: Everything You Ever Wanted To Know*; 3Com Corporation, April 26, 1996.
10. www.firewall.cx
11. www.techexams.net
12. www.vicomsoft.com
13. www.wirelessethernet.org
14. www.widernet.org/nigeriaconsult/nuc.htm