NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

LOCAL AREA NETWORK (LAN)
COMPATIBILITY ISSUES

by

RITA V. ESPIRITU

September, 1991

Thesis Advisor: Dr. Norman Schneidewind

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School; 6b. OFFICE SYMBOL (If applicable) 55	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000	7b. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000
8a. NAME OF FUNDING/SPONSORING ORGANIZATION; 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS: Program Element No; Project No; Task No; Work Unit Accession Number

11. TITLE (Include Security Classification)
LOCAL AREA NETWORK (LAN) COMPATIBILITY ISSUES

12. PERSONAL AUTHOR(S) Rita V. Espiritu

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (year, month, day)	15. PAGE COUNT
Master's Thesis	From To	September 1991	95

16. SUPPLEMENTARY NOTATION
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17. COSATI CODES

FIELD	GROUP	SUBGROUP

18. SUBJECT TERMS (continue on reverse if necessary and identify by block number)
Local Area Networks (LAN), LAN hardware and software compatibility issues, LAN Manager's Guide.

19. ABSTRACT (continue on reverse if necessary and identify by block number)
This thesis presents a research study of local area network compatibility issues. Todays high performance and successful LANs must use hardware and software that is compatible with the network technology used. Compatibility, for the purposes of this thesis, means the ability to interface without special adapters or other devices and directly relates to the ease of the rnsfer of data or programs within the network and between systems. An understanding of compatibility issues can help network users and managers diagnose and resolve connectivity problems thus saving valuble time and money that can be used toward other productive endeavors within an organization. This thesis will discuss hardware and software concepts, LAN architecture, and design issues as they relate to network compatibility. A LAN Manager's Guide covering the above issues is included as an appendix. It is written specifically for the Administrative Sciences/Information Systems (AS/IS) computer network laboratories as supplemental information for students on LANs.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS REPORT ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION Unclassified
22a. NAME OF RESPONSIBLE INDIVIDUAL Norman Schneidewind	22b. TELEPHONE (Include Area code) (408) 646-2719; 22c. OFFICE SYMBOL AS/Ss

DD FORM 1473, 84 MAR — 83 APR edition may be used until exhausted. All other editions are obsolete.

Approved for public release; distribution is unlimited.

Local Area Network (LAN) Compatibility Issues

by

Rita V. Espiritu
Lieutenant Commander, United States Navy
M.S. Naval Postgraduate School, 1991

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1991

Author: ______________________________
Rita V. Espiritu

Approved by: ______________________________
Dr. Norman Schneidewind, Thesis Advisor

____
Prof. Myung Suh, Second Reader

____
David R. Whipple, Chairman
Department of Administrative Services

ABSTRACT

This thesis presents a research study of local area network compatibility issues. Today's high performance and successful LANs must use hardware and software that is compatible with the network technology used. Compatibility, for the purposes of this research paper, means the ability to interface without special adapters or other devices and directly relates to the ease of the transfer of data or programs within the network and between systems. An understanding of compatibility issues can help network users and managers diagnose and resolve connectivity problems thus saving valuable time and money that can be used toward other productive endeavors within an organization. This thesis will discuss hardware and software concepts, LAN architecture, and design issues as they relate to network compatibility. A LAN Manager's Guide covering the above issues is included as an appendix. It is written specifically for the Administrative Sciences/Information Systems (AS/IS) computer network laboratories as supplemental information for students on LANs.

TABLE OF CONTENTS

I. INTRODUCTION

A. BACKGROUND

The Local Area Network (LAN) is a technology that has evolved to meet the needs of automating short distance communication at high speeds of operation and relatively low error rates. They are a particular form of data communications that optimize hardware and software to support the sharing of devices and information. Not only do LANs support personal computer workstations but they are also being used in conjunction with minicomputer and mainframe networks as well as wide area networks (WANs). Today, LANs have emerged as a useful technology loaded with immediate practicality and a promising future. The mere sharing of expensive resources such as laser printers and high capacity, high-speed mass storage devices among many users is a direct economic benefit to management and equates to significant savings. Businesses realize the importance of local area networks in their daily activities and recognize that networking is desirable for optimum company effectiveness.

Local area networks have expanded to global proportions and the technology has exceeded the tasks it was originally acquired to perform. In these days of fast-moving technologies, compatibility issues have become important.

Users have realized that compatibility not only results in connectivity, but also in interoperability. Starting a LAN and interconnecting it with other LANs, wide-area networks (WANs), and metropolitan-area networks (MANs) to expand its scope are complex tasks that are here to stay. Software and hardware vendors are going to great lengths to ensure compatibility with as many network products as possible. Sometimes, however, claims and intentions of vendors do not always translate into compatible machines and products, and many network users and managers end up spending numerous hours troubleshooting problems that affect the performance of the network.

Compatibility means that a hardware unit or software can perform its intended function when it is part of a larger program system, like a PC being able to perform its functions when connected to a LAN. If a PC is said to be IBM PC-compatible, that implies that the PC can run the same software and support the same add-on hardware as an IBM PC; but it may also mean that the PC can run most IBM PC-compatible software. So, there are also degrees of compatibility that must be understood. As hardware and software vendor's products claim compatibility with established products and standards, they also attain popularity in the market in that they can claim that their products can operate on older equipment as well as newer models of the same equipment. This is called backward compatibility and forward compatibility, respectively.

B. PURPOSE

The purpose of this thesis is to research and discuss LAN issues that LAN users and managers may encounter. It is the intent of this work to be a ready reference and guide to various network compatibility issues, both in hardware and software. It will assist users and managers in the resolution of difficult compatibility and connectivity issues without delving too deeply into the intricate network technology. It is also aimed at providing the reader with an understanding of compatibility issues regarding LANs. A LAN manager's guide is included as an appendix. It is written specifically as an aid for LAN managers and as a supplement in LAN courses.

C. SCOPE AND METHODOLOGY

The main thrust of this research is the investigation and identification of LAN compatibility issues with regard to available network hardware and software. An overview of network concepts and terminology will be discussed as well as its relationship to various network technologies. It is the intent of this thesis to supplement a student's knowledge of local area networks and generate interest and awareness of network compatibility issues that may be encountered by a network lab manager. The Lab Manager's Guide included in the appendix will be treated in tutorial fashion to allow for easy readability and understanding.

This research is primarily a review of current books, periodicals, and news articles on Local Area Networks, with a principal focus on network hardware and software compatibility issues.

D. ORGANIZATION OF STUDY

In order to understand compatibility issues of local area networks, some basic network issues will be discussed. A chapter on network standards is considered appropriate. This will cover determining compatibility; the different standards governing communication, media, and data transmission; the organizations involved in the development of standards such as the ISO and the IEEE; a number of network technologies and the topologies and communication protocols each technology uses. Follow-on chapters will cover various network hardware and software, describing each and discussing the relevant compatibility issues that impact a LAN's performance. Lastly, a LAN MANAGER'S GUIDE is included as an appendix.

II. NETWORK STANDARDS

A. DETERMINING COMPATIBILITY

Compatibility is defined as the capability of a peripheral, a program, or an adapter to function with or substitute for a given make or model of computer. It is also the capability of one computer to run the software of another company's computer. It should be noted though that, to be truly compatible, a program or device should operate on a given system without modification; all features should operate as intended, and a computer claiming to be compatible with another should run all the other computer's software without modification.

Standards have been set at some of the lower levels of networking, but there are still implementation incompatibilities; at higher layers, standards are still being developed. Practically every layer has some sort of incompatibility yet to be resolved. From problems with physical layer bridging to incompatibilities at the application level, myriad incompatibilities lie quietly underneath the marketing hype about "interoperability" and "true multi-vendor networking." (Schatt, 1991)

Many companies today develop software and hardware that is compatible to certain systems, the most notable of which is the clone to the IBM PC. It was a year after IBM introduced its PC that the first IBM PC-compatible computer was released. Numerous companies designed products that were to be 100 percent compatible with IBM software and accessory devices, such as displays and printers. Although these were known collectively as clones, conveying the connotation of "cheap imitation," many of the computers produced actually improved on the original, and so the term "clone" is no longer fair. (Doll, 1990)

The original IBM PC was designed to use off-the-shelf components--such as disk drives, microprocessors, and power supplies--that non-IBM companies had developed already for earlier personal computers. These same components could be assembled by anyone with requisite technical know-how. In addition, IBM purchased the PC's operating system, PC DOS, from the Microsoft Corporation, which was free to sell virtually the same system (MS- DOS) to clone manufacturers. The only part of the computer that IBM actually copyrighted was a small amount of internal programming code, which other computer companies could emulate without actually copying. (Green, 1988)

To counter the compatible market, IBM attempted to close the architecture of its personal computers by the release of the PS/2 series in 1986. The key feature in this series is its Micro Channel bus architecture, which has certain technical advantages over the method used to communicate data within previous PC's. However, the Micro Channel bus created a closed environment for PC add-on boards and accessories; the older boards and accessories do not work on a Micro Channel machine, and any company developing products for Micro Channel machines needs a license from IBM. (Green, 1988)

There are MCA clones. Most compatible makers have not emulated the Micro Channel standard, preferring instead to stick with the tried-and-true PC architecture. To take full advantage of the 32-bit bus structure of the Intel 80386 and 80486 microprocessors, these manufacturers (dubbed the "Gang of Nine") have created a bus standard called Extended Industry Standard Architecture (EISA). Computers conforming to the EISA standard can accept existing adapters while taking full advantage of these powerful new microprocessors. (Cole, 1990)

B. NETWORK ARCHITECTURE

The architecture of a computer network is the design plan of how the network's component parts work together. It is what distinguishes one network from another. It describes how the system or program is constructed, how its components fit together, and the protocols and interfaces used for communication and cooperation among modules or components of the system. In short, network architecture defines the functions and description of data formats and procedures used for communication between nodes or workstations. It combines the existing standards and protocols needed to provide the services desired to create a functioning network. It is therefore a standard; the network architecture defines the rules of a network and how the components of a network can interact. It can be broken into layers, with each layer responsible for a certain task. When these tasks are combined, they result in a service being performed by the network. (Durr, 1989)

Two different computer networks can have many components in common, but their architecture makes them different. For example, two networks can use the same kinds of cables and connectors, but still have very different architectures.

C. COMMUNICATIONS STANDARDS

The heart of networking is communication and effective communication requires a set of standards. It is important that products from different vendors are able to communicate with each other. Standards provide manufacturers a measure to follow in order to ensure compatibility between products in a multivendor network. As a result of standards, many different manufacturers can produce compatible and complementary equipment thus reducing the possibility that one or a few companies can monopolize a niche of the industry. Because many manufacturers can produce compatible equipment where standards exist, marketing is forced to emphasize quality and value-added services rather than particular protocol differences. This leads to competition and lower prices of the product for consumers. (Madron, 1990) Manufacturers often view their own implementation of communication protocols as the best solution and, over time have attempted to influence the industry.

Compliance with a standard is still a vexing issue that causes much rancor between vendors and users. As standards become more sophisticated, proving compliance becomes more costly and complex. Any ambiguities in the specifications can lead to conflicting interpretations in products.

It is important to note that standards are adopted as a result of economic self interest. Users want to have more independence from specific vendors and governments may encourage standards to foster cheaper solutions and increase efficiency, but vendors will adopt standards only when there are sufficient economic incentives. (Miller, 1991)

Fortunately, organizations have been established to help create standard industry protocols so that network devices can communicate even if they are using products from different vendors. One of these organizations is called the International Standards Organization (ISO). Another is called the Institute of Electrical and Electronics Engineers (IEEE).

1. ISO's Open Systems Interconnection (OSI) Model

The OSI model was created by the ISO as a result of a committee study on the compatibility of network equipment. The model provides the base upon which manufacturers design products and is a general reference framework for LAN standards. It is a manufacturer-independent architecture for data communication protocols. The goal is to have various systems conform to the reference model and thus be able to connect and share meaningful information.

The OSI reference model is essentially a seven-layered hierarchical model which defines specialized functions. It defines a universal architecture for interconnecting different types of computer systems. The seven layers are Physical, Data-Link, Network, Transport, Session, Presentation, and Application. Each layer defines a layer or level of function. The services that each layer supplies are defined by a range of standards, which allows for different ways of performing the same service. Compatibility of equipment can be defined within a layer, or lower-level implementations can be hidden to achieve compatibility at some higher level. Network software is written so that each layer is aware of and communicates only with the layer immediately above and below it. (Durr, 1989)

Each function or layer performs tasks necessary for different levels of communications between systems. The layers allow for the division of network tasks and make it possible for changes to be made to one or more layers without affecting any other layers of the system. (Bullette, 1991) The model provides a framework for the definition of services and protocols which fit within the boundaries established. It does not specify how functions must be performed. This level of definition requires a defined implementation (protocol) for each layer. Another description of the model is that it is a frame of reference for open systems (refers to a network model open to equipment from competing manufacturers) with implementation details being left to other standards. It does not imply any particular implementation or technology. Adherence to the reference model does not mean that one vendor's products can communicate with another vendor's products.

It is important to understand that an open system can be OSI compatible without providing the initial source or final destination of data. (Madron, 1990) In other words, an open system need not contain the higher layers of architecture. The IEEE 802 standard, for example, applies only to the lowest two layers: Data Link and Physical. This is often the source of significant confusion since, when we talk of 802.3 (commonly called Ethernet) or 802.5 (Token Ring), the discussion sometimes proceeds to commentaries on TCP/IP (Transport Control Protocol/Internet Protocol or XNS (Xerox Network Protocol) or some other "protocol." TCP/IP and XNS exist at layers beyond the Physical and Data Link (although TCP/IP and XNS are not OSI standard protocols).

The OSI model is far from complete. The initial OSI work placed major emphasis on the definition of the seven-layer model and the protocols needed for application-to-application communication. Lack of management specifications reduces the major power of OSI - unifying different systems and networking environments. (Miller, 1991)

2. IEEE 802 Standards

The IEEE has developed a set of standards describing the cabling, physical topology and access schemes of network products (i.e., IEEE 802.X standards). The standards describe the protocols used in the lower two layers of the OSI model. They **do not** go above those layers, thus using the common name of an IEEE Standard (like Token-Ring) is an **incomplete** response to the question "What network do you use?" The correct reply should also specify the network interface, including media and access protocol as well as the networking software. (Jordan, 1990) Note that the 802.x standards do not describe every popular network cabling and access protocol scheme (ARCnet , for instance, is not a perfect fit).

D. MEDIA STANDARDS

The cables and other carriers of a network's transmission signals are called media. Cabling is the physical element that connects workstations to servers, LANs, WANs, and dissimilar environments such as minicomputers and mainframes. (Liebing, 1990) The lifeblood of any data network is its cable. The most common kinds of cables are: coaxial cable (coax), which can carry high-frequency data for relatively long distances but can be expensive; twisted pair copper cables, which can be much less expensive than coax, but it lags slightly in transmission speed and maximum distance it can carry a signal; and fiber-optic cabling, which uses light instead of electricity to carry a signal. In many ways, fiber-optic cable is the ideal cable because it can carry extraordinarily high-frequency data for miles, and it is very hard to tap into without detection. It is however, expensive and less flexible, and so harder to install.

E. DATA TRANSMISSION STANDARDS

These standards relate primarily to the way in which data are transmitted on a medium. With **baseband** systems, signals are transmitted at their original frequencies (i.e., unmodulated). It transmits all signals through a single channel, one at a time. In contrast, **broadband**, often used to characterize communications based on CATV technology, transmits multiple signals at once by subdividing its transmission medium into channels. It is also characterized by a large bandwidth (a network's range of transmission frequencies) resulting in the capacity for very high data rates. Transmission speeds for broadband range from one to five mbps. The slower transmission speeds are acceptable for some installations because of the significant increase in cabling distance. Cables run can extend to as long as 50 kilometers. (Bullette, 1991) Broadband systems are modulated and in their CATV context, are analog systems.

F. LAN TECHNOLOGIES

The technology of a computer network has two main aspects: communication protocols and topology. This thesis will discuss some popular network technologies for LANs: EtherNet, Token-Ring, ARCnet, and Appletalk. The debate over the performance merits of one networking technology over another has been raging since the inception of LANs. (Liebing, 1990)

Traditionally, the debate revolves around raw transmission speed. The EtherNet camp claims that its 10Mbps transmission speed beats Token-Ring's 4Mbps and ARCnet's 2.5Mbps hands down. The IBM Token-Ring camp countered that by coming up with a 16Mbps version. They also claimed that EtherNet's CSMA/CD medium access protocol allows collisions on the wire to degrade performance considerably as more workstations are added to the network. The EtherNet proponents responded by pointing out that Token-Ring's token-passing protocol adds a significant amount of overhead, and that when a small number of workstations are passing a large amount of data across the network, time spent passing a token is time that could be better spent transferring actual data. Through it all, the ARCnet community seems quite content with their slower, simpler token-passing alternative. (Liebing, 1990)

Ultimately, the performance claims of any network architecture must be weighed against a number of other factors: ease of installation, cost per node, quality of manufacturing, efficiency of associated LAN drivers, availability of supporting hardware (repeaters, hubs, media access units, etc.), flexibility of the topology, cabling types supported, adherence to standards, and compatibility with other systems.

1. EtherNet

The original EtherNet networking scheme calls for a thick coaxial cable, which has come to be known as thick EtherNet cable. Following the classic bus topology, a single thick EtherNet trunk cable runs from one end of the network to the other. The stations are connected to the bus via transceivers and transceiver cables.

Most PC-based EtherNet networks use the thinner RG-58 coaxial cable, which has been dubbed thin EtherNet or "Cheapernet" cable. Stations are connected using a linear bus topology in which cable is strung from one station to the next. A T-connector is used to attach the cable to the network interface board at the back of each network station. EtherNet uses the CSMA/CD medium access method and provides a transmission speed of 10 megabits per second (Mbps). (Liebing, 1990)

2. IBM's Token-Ring

Its name applies a ring, however, the token ring is physically a star, logically a ring. Media repeaters can be added between two Multistation Access Units (MAU's) to increase the transmission distance. Each node acts as a repeater--receiving the serial bit from the nearest active node, processing as necessary, and sending the bit stream on down the cable to the next node in line. Only a few bit times of delay are required in each workstation for these functions. The serial transmission follows a complete ring or loop, with the sending station eventually receiving its transmitted information back after this information completes one round trip around the ring. The token is merely a specific bit sequence that circulates among the nodes, giving permission to transmit. For this reason, these networks are often described as being distributed polling environments. Each workstation is thus polled to determine if it needs access to the network. When the node is in possession of the token, it can transmit a message that is in its output buffer. Otherwise, the node is bit-repeat (and/or receive and process) mode. (Miller, 1989)

3. ARCnet

Of all the major networks, ARCNET is the most flexible in its architecture. Both star and bus topology networks, or a combination that might be described as a distributed star with branches, are possible. In addition, all three media choices: coax (RG-62/U), a single twisted pair (100 ohm impedance, 2 twists/foot, 22, 24, and 26 gauge solid or 24 and 26 gauge stranded) and duplex fiber optic cable (50, 62.5, 100, or 200 micron core) are available and can be flexibly interconnected. The only major constraint on the transmission medium is that the signal propagation delay between any two workstations must not exceed 31 microseconds. In addition, the attenuation characteristics of the different types of cable affect the number of workstations that can be attached in a bus topology. (Miller, 1989)

4. Appletalk

Appletalk is a baseband network with a bus topology. It operates over shielded twisted-pair wire, unshielded twisted-pair, or optical fiber--all at 230.8 kilobits per second. Appletalk is a proprietary network standard that does not conform to any IEEE specifications. But it uses a layered architecture, and its protocols at every layer have been published, so other vendors can develop products for it.

Appletalk networking uses an access scheme that is similar to EtherNet's CSMA/CD. Under the CSMA/CA scheme, each MAC on the network listens for a digital clock pulse that indicates another station is transmitting. Appletalk is slow because the zilog chip that runs it can be overwhelmed by clock pulses that arrive at rates faster than 230.8 kilobits per second. When data is sent any faster than that over the network, MACs are prone to not detecting the clock pulse, deciding there is no traffic, and barging into conversations. (Needleham, 1990)

G. LAN TOPOLOGY

Topology refers to the physical layout of the cable; how the network components are arranged in relation to each other. Topology also refers to the access method of sending information across the cable. It is the way in which network interface boards arbitrate with each other for access to the shared wire. (Liebing, 1990) Two methods are currently in widespread use:

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - is most commonly used on an Ethernet linear bus topology. A network board must wait until no one else is talking on the network before it can talk. Then, as the board sends the packet, it listens to what is being said. If the board does not hear itself, another board is talking at the same time. Both boards jam each other, back off for a random amount of time, then try again.

- Token passing - Token passing is used on a ring, such as IBM Token-Ring, and on a star bus, such as ARCnet. It is more complicated than CSMA/CD. The network interface boards pass a special "token" packet to each other. Possession of the packet means that a board can send a message if it wants. The trick to token-passing is adapting the passing sequence when new boards are added to the ring, and detecting when a board quits operating.

The three basic types of topology are the star, bus, and ring topologies. On the OSI model, the cabling lies below the first physical layer. One point must be made clear. The actual installation of a LAN may not truly resemble the topology used in its design. Although a network can be physically laid out in a particular network topology, it does not necessarily mean that is the route the information will flow. Topology can be either physical or logical and both are relatively independent. Both topologies can affect the network's reliability, economy and resistance to interruption.

The nodes in a LAN handle messages in one of two logical ways. Either they relay the messages from node to node in a sequential logical topology or they send the messages out to all stations simultaneously in a broadcast. EtherNet uses a broadcast topology while Token-Ring uses a sequential technique.

There are several ways of physically running the cables connecting a group of computers. In the star or hub topology, the network wires run between the network nodes and a central wiring hub, usually located in the building's wiring closet. The hub is the focal point of the star and all network traffic must pass through the hub. Each workstation is like a spoke emerging from the central hub, much like a wagon wheel.

The primary advantage of the star wiring topology is operational survivability. The wiring hub isolates the runs of network cabling. Even if a wire between a station and the wiring hub breaks or develops a bad connection, the rest of the network remains operational. It is also typically easier to install than cable running from point to point since the wire runs from the wall plates to a central point, like telephone wiring. The overall installation is neater because fewer wires run to each node. This topology makes it easier to move PCs and change connections.

A disadvantage of using the topology would be that it uses more wire and there is the cost of the wiring hub. Also, a separate cable must be run to every machine that accesses the network, and if the hub goes down, so does every station connected to it. (Derfler, 1991)

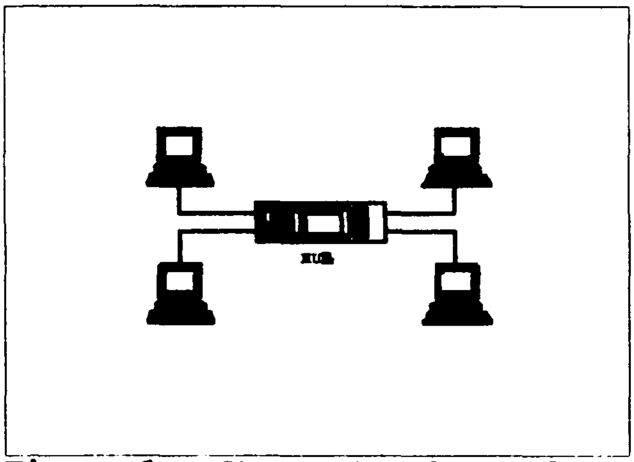


Figure 1. Star Network Topology

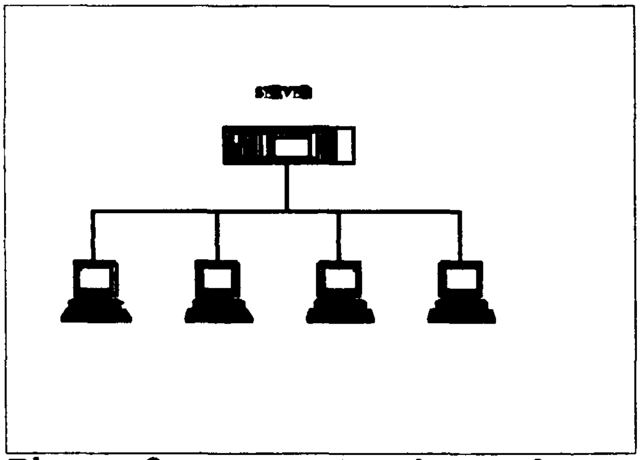


Figure 2. Bus Network Topology

The second type of topology is the bus, also called daisy chain topology. It is the simplest of the wiring schemes. (Derfler, 1991) The cable takes the shortest path from one network node to the next. The signal on the bus travels in both directions from the workstations or nodes. Unlike the ring topology, the data travels by the nodes and does not have to go through each node. Instead, a coaxial T-connector provides a tap into the cable at each network node. This topology is typically associated with EtherNet.

Because of the electrical characteristics of this topology, the following disadvantages exist: If the cable breaks at any point, the entire network fails. The cable does have many connection points, and a bad connection at any point spells failure. The cable installations are also often messy because two cables run from the CPU to the back panel of each computer and then go off along the floor in separate directions. Large networks can also saturate the bus when too many machines try to communicate on the same bus "party line." Additionally, security may be a problem since every station can "hear" all network traffic. (Derfler, 1991)

The third basic topology is the ring, where each computer is connected both to a machine "upstream" and one "downstream" from it, to form a closed loop or a ring. Each node on the cabling acts as a repeater, boosting the signal between workstations. Data travels around the ring in only one direction and passes through each node around the ring until it reaches either the destination computer, which intercepts it, or it goes back to the sender, where it stops.

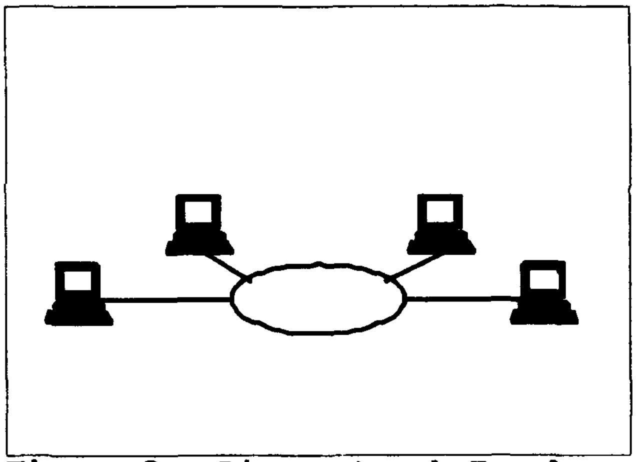


Figure 3. Ring Network Topology

IBM's Token-Ring is the most popular form of the ring topology. While it is electrically a true ring, physically it is normally wired as a star, with each computer trailing a cable to a central box called a Media Access Unit (MAU) that connects one cable to another. This kind of configuration is called a star-wired ring.

Theoretically, a break in any cable on a ring network will disable the entire network. But IBM's Token-Ring cabling system has a built-in set of back-up cable, which reroutes data back around the working part of the ring if a faulty cable is removed from the network. Token-Ring cabling is usually shielded twisted pair. (Madron, 1990)

H. COMMUNICATION PROTOCOLS

A protocol is nothing more than a formal agreement about how computers should format and acknowledge information during a communication session. (Derfler, 1991) When networking and communications products from different companies follow the same protocol, they have the ability to talk to each other, at least theoretically. Protocols define the actual steps that any device or program must take to communicate with another device or program in the network. All systems must share the same protocol type or go through a protocol conversion process to be able to exchange information. The conversion device is usually called a **gateway** and consists of both hardware and software components. Gateways always add some overhead when translating between protocols and therefore impact performance somewhat. (Bullette, 1991)

Protocols specify everything from the transmission rate to how data will be used by an application or end user. If any part of the packet is not in a format recognizable by another device, the two cannot communicate. Protocols govern format, timing, sequencing, and error control. There can be sets of protocols in some networks, with each protocol handling rules for a subset of the entire task of communication. This set of protocols is often called a "protocol suite" or a "protocol stack." (Rinzler, 1990)

In the context of the ISO seven-layer model, a protocol refers to the rules associated with a specific layer or set of layers. The protocol in any layer includes interface standards for requesting service from the layer below to the layer above. (Jordan, 1990)

Protocol rules are built into networking software, and network devices observe protocols each time they perform a task. In any network architecture, there must exist protocols that define three generic classes of functions:

- Application Services - are the highest level network functions. They enable an application program to communicate with an equivalent program on another computer.
- Transport Services - are lower-level network functions, which manage addressing and other transmission control tasks.

- Connection Services - are the lowest-level network functions. These govern the actual, physical transmission from one computer's memory onto the network, and then into the destination computer.

A poorly implemented protocol can slow data transfer, making very inefficient use of the network and degrade the performance of the network. On the other hand, a well implemented one can make communication between dissimilar networks possible. The TCP/IP protocol provides for transfer of data between computers with different architectures and operating systems. As a network grows more and more heterogeneous, matching protocols exactly is more difficult. Vendors may develop protocols that vary slightly from the published standard and from one another. This makes for incompatibility in some instances. Other vendors may develop proprietary protocols, independent of all standards, and yet others combine protocols from various standards to take advantage of the best features. (Jordan, 1990)

III. NETWORK HARDWARE

Hardware requirements for a computer that will run network operating system and application software can be complex. Systems have to run the appropriate versions of software that are compatible with the hardware (that is, network interface cards (NICs), disk controller cards, microprocessors, etc.) The best computers must be able to mix hardware and software from various vendors into a cohesive package. This is no easy feat since most software and hardware products have bugs and various incompatibilities built in, whether inadvertently or deliberately.

LAN hardware can be defined as the LAN's physical components, along with the methods used to connect those components. Cables, topologies, and network interface cards (NICs) are the primary pieces of LAN hardware. CPUs, servers, hard disks, and bus cards are other components. The selection of each component depends on the physical layout and on the performance requirements of users and applications. Because not all types of cable can support long cable runs (i.e., if long runs are necessary), the cable choices are limited. Transmission speeds, or raw bit rates, vary with NICs and should be chosen to match the needs of the application. The availability of diverse LAN hardware, interchangeable standards, and the LAN's distributed architecture, contribute to the flexibility of the LAN.

A. NETWORK INTERFACE CARDS (NICs)

NICs refer to a local area network board, also called a LAN adapter card/board. It provides intelligence and connectivity to the network cabling system, using any of a number of different wiring schemes currently available. The NIC establishes most of the LAN's hardware characteristics. (Durr, 1989) These characteristics include the cable type, topology, access scheme, and data transmission (bit) rate.

Every computer attached to a LAN uses one sort of network interface card or another. In most cases, the card fits directly into the expansion bus of the computer. In some cases, the card will be part of a separate unit to which the computer attaches through a serial or parallel connection. Dedicated workstations and servers already contain adapter cards which are built into their motherboards.

Although the NIC provides the physical connection to the network, the transfer of data from the PC to the network is not that simple. To get one byte of data from here to there, several things must happen. Buffers must be checked.

Requests must be acknowledged. Sessions must be established. Tokens must be sent. Collisions must be detected, etc.

Luckily, the work of the NIC can be broken down into eight tasks: host-card communications; buffering; packet formation; parallel-serial conversion; encoding/decoding; cable access; handshaking; and transmission/reception. These are the steps taken to get data from the memory of one computer to the memory of another computer. (LAN Magazine, Dec 88)

When choosing a NIC, such issues as performance, access method, and topology must be considered. Reliability is also an important issue. It does not matter how fast the NIC is if it does not work, causes errors, loses packets, drops the line etc. Isolating these type of network problems can be very frustrating.

Most NICs are available in either eight-bit, 16-bit or 32-bit varieties. An eight-bit card moves data from the computer's I/O bus to the cable eight-bits (one byte) at a time; a 16-bit card moves data 16 bits (two bytes) at a time. Because of the higher performance of 16-bit cards, they are most often used in the file server, whereas the slower eight-bit cards are used in workstations. (Madron, 1990)

For compatibility purposes, the 16-bit card has two edge connectors (one long and one short) so they will only fit in a 16-bit slot in the expansion bay of the computer. One must ensure that the file server has an adequate number of 16-bit slots available to accommodate the boards that must be installed. Also, many 16-bit cards can use hardware interrupts nine or above. This capability is important in avoiding hardware conflicts when the card must coexist in the same machine with other expansion cards that use the lower hardware interrupts. (Liebing, 1990)

The most common conflict between NICs and your PC occurs when the NIC tries to use the same hardware interrupt (IRQ) as another card or device in the PC, such as a mouse, internal modem or serial port. Reading the manuals of the different devices and noting which interrupts they use can prevent this conflict during installation of the NIC. Also, jumpers on the NIC will indicate which IRQs they use. Usually, if the system uses COM1 for a modem, it is using IRQ4. COM2 occupies IRQ3. Some NICs default to IRQ3, and if this is a conflict, a command could be issued telling the card which IRQ to use. The subject of interrupts is necessary to understand compatibility issues and will be discussed in detail in a separate section.

Another conflict noted is when communication errors (duplicate requests, packet collisions) occur and it is certain that cabling is not the culprit. There is a good possibility that the system is being slowed down by the NIC.

Also, if the CPU is running 50 percent, there might be a need for a new server with a 386 chip running a minimum of 25 or 33 Mhz. (Liebing, 1990)

The network operating system (NOS) communicates with the NIC through a specialized piece of software called a **communication driver** or **LAN driver**. This driver must be linked to the operating system during installation. Due to different protocols and different card designs, each NIC model may have a unique driver. Unfortunately, there is very little standardization in this area. For example, each EtherNet and Token-Ring model has a different driver. ARCnet is the exception: the ARCnet card manufacturers adhere to self-imposed design standards that make these cards and their drivers practically interchangeable. (Miller, 1989)

Different types of NICs are available depending on the type of network. The most widely used NICs are EtherNet, ARCnet, and Token-Ring.

General incompatibility problems with network boards and disk controller boards include: (Foster, 1991)

- **Bus Mastering** - Bus mastering is a fairly recent concept supported by IBM's Micro Channel Architecture (MCA) and the new EISA technology (Enhanced Industry Standard Architecture), as opposed to ISA (Industry Standard Architecture, which is known as the AT-type compatible bus).

The MCA or EISA buses are two or four times wider than that of the ISA, and increase throughput significantly. Bus mastering allows NICs to bypass the CPU and take over the bus. This enables the system throughput to be a lot faster, since the CPU no longer has to play the middleman, relaying commands from the NIC to the bus and back. They both offer a burst mode that lets data transfer from bus cards to memory (and vice versa) and take place at the speed of the processor. Bus mastering is not supported by the AT-type computers. (PC Magazine, 29 May 90)

The difficulty comes in implementing the technology uniformly; bus mastering intelligence has to be on both the board and the computer. Since the board and the computer are usually made by different manufacturers, and since bus mastering is not a universally demanded feature yet, bugs have been popping out. (Foster, 1991)

- **Configuration Option** - No two boards in the same computer can have the same memory addresses or IRQ's. Boards have a configuration option which provide the information on these unique settings. Board manufacturers provide tables to help ensure the uniqueness of the board's configuration option; the default configuration option usually works if there is only one board in the system, requiring no more effort than double checking the manufacturer's settings.

Occasionally, computers and network interface boards do not work together. Sometimes this is because the system is technologically more advanced than the board. A number of 486 computers are simply too fast for most of the boards out there. One solution to fast computers and slow boards is to slow down the computer by disabling the internal cache. This defeats the purpose in buying the machine, but at least the board will work. The better solution is to speed up the boards, and this is currently being implemented. (Foster, 1991)

- **Remote Booting** - In diskless workstations, LAN boards cannot complete the physical connection to the file server at booting time without an additional chip that supports the remote boot for a workstation. Most LAN boards are sold without this chip, although one can be purchased. Some boards, usually the fast ones, are designed exclusively for use in file servers; they do not even come with the chip. Occasionally, if the chip is on the board, the workstation does not support it.

B. FILE SERVERS

A file server is usually the fastest, most powerful computer in the network. It has more memory on the motherboard, more expansion slots so that more options can be supported, and more and larger hard disk drives than any workstation would need. Usually, it has two floppy disk drives and a switch on the back to change the wait state of the system for fast or slow software.

The file server functions as the central repository of data and/or application programs for the network. It also performs network traffic management functions and provides security for the data. It performs only information retrieval. It does not perform computations or specific record searches within a database. (Nunemacher, 1990)

The basic issues to consider in determining compatibility of file servers include the manufacturer, the CPU, the bus type, the ROM BIOS, and the amount of RAM supported. (Liebing, 1990)

There are compatibility issues between the file server and the network interface board. In a file server, there will always be at least one other board to contend with in addition to the network interface boards, and that is the disk controller board which manages the interface between the hard disk drive and the computer. The file server disk controller board is usually not interchangeable with a disk controller board in a workstation. For one thing, it is going to be more powerful. (Foster, 1991) There could be conflicts if there is more than one disk controller board in the system. In its simplest form, the hard disks would be on one channel; a disk subsystem connected to another disk controller board in the system would be on a second channel, and so on.

Most servers today are designed and used primarily for file and print service. (Needleman, 1990) Its capacity and speed are the two biggest factors in the growth and performance of many LANs. One of the ways to get more out of a server is to use a faster CPU. A 286 machine may be fine for 20-30 users, but bigger networks require more horsepower. The 486 is the server processor of choice. However, a faster processor alone, is not enough. The rest of the server system, particularly the disk drives, must be fast and large enough to keep up with the pace of the CPU. Many of today's servers can hold over a gigabyte of disk storage, and average access times are falling below 10 milliseconds.

The fastest processor and disk drives will not do much good if the data from the server trickles out to the LAN. Today's common, dumb, eight-bit network adapters are inadequate. Servers should have a 32-bit bus that can support intelligent, 32-bit disk drives controllers and LAN adapters. Bus Master adapters (boards capable of taking over the bus) offer the best performance. (Byte Magazine, June 1990)

C. MICROPROCESSORS/CENTRAL PROCESSING UNITS (CPUs)

At the heart of every server and workstation is the CPU. Every bit of data which enters or leaves the computer passes through the CPU to be processed or redirected. IBM and compatible PCs use the Intel 808x or 80x8x based processor (8088, 80286, 80386, 80486). The performance of each of these processors varies from between .5 million instructions per second (mips) to over 4 mips.

The CPU's clock speed specifies the rate at which a processor can carry out instructions. Clock speeds vary from 4.77 mhz (million cycles per second) to 33 mhz or higher. (Bullette, 1991)

A faster CPU and clock speed will yield better performance from file servers. A 386 will be faster than a 286. Also, consider the number of wait states used to match the performance of the CPU with the rest of the file server hardware. The lower the number of wait states, the faster the server. (Liebing, 1990).

D. BUS CARDS

The system bus is the circuitry which connects all of the various subsystems together. IBM compatible PCs use either of the following types: (Jordan, 1990)

- AT Style - often referred to as the Industry Standard Architecture (ISA) is found in most IBM PC AT and compatible computers. This bus accepts standard 8- or 16-bit network and disk interface cards. The standard speed is 8Mhz.

- Micro Channel Architecture (MCA) - bus design found in IBM's PS/2 model 50 or above. These PS/2 computers will accept only boards designed for MCA. MCA cards will not work in standard AT bus machines. MCA offers higher data transfer speeds than the standard AT bus.

- Extended Industry Standard Architecture (EISA) - designed as an alternative to IBM's proprietary Micro Channel Architecture. Most EISA machines are very high performance computers specially designed to be used as a network file server. They offer a higher transfer speed than the AT bus, and they have the added advantage of being able to accommodate cards designed for the AT bus as well as EISA-designed cards.

E. ROM BIOS

On a PC, the ROM BIOS (Read Only Memory Basic Input/Output System) contains basic instructions and procedures used by the CPU. The BIOS is the interface between the computer's hardware circuitry and the software (both the operating system and applications) running on the machine. Among other things, the ROM BIOS controls the computer's interaction with the monitor and the keyboard.

Compatibility problems are encountered when file servers with older ROM BIOS firmware experience difficulty (such as the inability to boot, random crashing, and APPEND errors) when running nondedicated versions of network operating systems (NETWARE). The ROM BIOS must be 100 % IBM compatible. Also, the hard disk must be included in the ROM BIOS setup tables or there will be trouble getting the file server to recognize the disk when the setup routine is run.

F. RANDOM ACCESS MEMORY (RAM)

A practical minimum for RAM is at least 2MB. The maximum amount of memory a file server can have is 16MB. Adequate memory becomes especially critical when the server must service a large number of users, or when it has more than 79MB of hard disk storage space to keep track of. Four to eight Megabytes is usually sufficient. (Liebing, 1990)

If extended or expanded memory is desired for a PC, a memory-add-on-board can be purchased. To avoid potential RAM problems, all of the RAM chips installed on a given memory board must be the same type, or at least have the same speed rating. (Liebing, 1990)

G. WORKSTATIONS

The most common workstation problems occur when other devices are added which cause a conflict with the network adapter board. Every adapter requires a unique interrupt (IRQ), direct memory access address (DMA), and input/output (I/O) base address setting. Since many devices use the same settings as the adapter, it is necessary to make changes so that each device contains nonconflicting settings.

Users who install applications in their private directories on the network may be unaware that some installation processes overwrite network drivers on the startup diskette or hard disk. These kinds of problems can be alleviated by placing write protect tabs on the diskettes or using the DOS ATTrib command to protect specific files from modification or deletion. (Bullette, 1991)

H. EMULATION BOARDS

An emulation board is a circuit board that when combined with emulation software supports the physical connection between a PC and a Mainframe system. It enables the PC, acting as an intelligent terminal to manipulate mainframe data. One of the most widely used systems of intelligent terminals is IBM's 3270 series. The 3270 terminals are used in on-line (interactive) sessions with IBM host computer.

Through emulation hardware and software, the PC workstation can perform the same functions as the 3270 terminal. In addition, the PC can store data from the host computer, modify or reformat display data, and run local applications programs that analyze the data.

All emulators do not work with all IBM compatible PCs. The emulator board should fit any slot and be used like any other circuit board. Other parts of the existing system, such as cluster controllers, may be "IBM-compatible" but not compatible enough to support a particular emulator without some modification. Compatibility is very important. Each key of the emulator-equipped PC should be evaluated. Sometimes, there is considerable variation in what a key actually does, what the documentation says the key does, and what the comparable key on a 3270 does. An advantage is emulation software that maps the keyboard to a preferred one. When evaluating the software, make certain that the software supports not only the two-way transfer but also the mainframe environment - TSO, VM/CMS, or both.

The emulator must be totally compatible with the PC and network, which means it should be possible to disconnect the coax and connector from the 3270 terminal and plug the cable directly into the emulator board on the PC. Then, the system can be started with the emulator software and be connected to the mainframe.

Another concern is that the emulator settings must not conflict with any other devices within the PC workstation, or else the system will not function properly. As long as the interrupts and I/O channels are not duplicated, other communications software can be used, including networking software.

The PC to Mainframe link is fundamental to the integration of PCs into organizations. It enables distributed resources to be accessed from any point on the network, regardless of vendor environment or machine type (mainframe, minicomputer, or PC). (Durr, 1989)

I. INTERCONNECTION HARDWARE

While bridges, routers, backbones and the like are able to provide the capability to link multiple LANs, they cannot link LANs that use incompatible technologies. If one department's LAN uses EtherNet, while another uses Token Ring, there will be a need for bridges and routers or gateways to link such dissimilar LANs. EtherNet and Token Ring both use the same logical link control (LLC) protocols (IEEE 802.2), so bridges and routers between the two must understand the LLC protocols.

Sharing the same LLC protocols often is not enough, because the LANs to be linked may be running different higher-level network software or protocol stacks, (Ex. LAN Manager, a network operating system, on Token-Ring works with a NetBeui protocol stack, while LAN Manager on EtherNet may use a version of IPX). Even though they use the same network operating system, there will be a need for more than a bridge or router that only understands LLC protocols to get these LANs to communicate. (Woram, 1990)

When two networks are being connected, the connections are made at the first identical OSI layer. For example, if layers 1 and 2 of the OSI model on the networks are different, but layers 3 and up are the same, the connection is made at layer 3 by having identical layers talk to each other within the connecting device.

Devices called repeaters achieve the lowest level of interconnection. A repeater extends the distance of a LAN. Other hardware used for interconnection are: (Jordan, 1990)

1. **Bridges**

A bridge connects two networks that use the same communication technology (e.g. Ethernet). It is the next level of interconnection after a repeater.

2. **Routers**

A router is a device that interconnects the bottom three layers of two networks.

3. **Gateways**

Gateways connect totally dissimilar networks. They may perform protocol conversion in all seven layers of the OSI model. A gateway not only performs the router's functions (determines where the packet is going), but converts the message from one packet format to another or from one data code system to another. A common use for a gateway is to connect a LAN and a SNA mainframe computer, changing protocols and retransmitting packets between two entirely different systems. When communication occurs through a gateway to a dissimilar system, some functionality usually is lost. File transfer between systems or terminal emulation at the PC currently are the extent of connection functionality.

IV. NETWORK SOFTWARE

This chapter will look at the operating system software required for each workstation to manage its hardware resources as well as some other significant network software. Operating systems have programming interfaces, software programs that make it easier for programmers to write application programs that require operating system resources. Some of these interfaces will be discussed as well as terminology associated with network software, (NetBIOS, Interrupts, TSRs etc) as to their importance to networks and issues involving compatibility.

A. OPERATING SYSTEMS (MS/PC DOS)

An operating system (OS) is a group of programs that manage all computer system resources and operations. Until the operating system is loaded and running, the computer can do nothing. The operating system's responsibilities include managing both internal memory (RAM) and the auxiliary storage resources such as a floppy disk drive or hard disk drive. It is responsible for scheduling the performance of tasks, handling input/output requests, and monitoring system security to ensure that users are authorized to view certain files and use specific programs. An operating system also includes utility programs that help the user perform key tasks such as preparing a new disk for use with a specific computer (formatting) and placing some key system files on a disk that enable the user to copy files and delete material. (Schatt, 1991)

Operating system programs facilitate communication among the computer user, the computer's hardware and software, and any peripherals. In 1981, IBM and Microsoft Corporation published MS-DOS, an operating system for the new IBM PC and all other compatible PCs that used the Intel 8088 or 8086 microprocessor. IBM also sold a version of the operating system labeled PC-DOS. Both operating systems were developed for one user performing one task at a time (single user/single tasking). The major parts of MS-DOS can be described as the supervisor, the input/output manager, the file manager, and the command processor. The supervisor is responsible for scheduling and coordinating the activities of all programs running under the operating system. The input/output manager is responsible for all information transferred to and from all peripheral devices, including printers, bar code readers, disk drives, and so on. The file manager's responsibility includes all areas of file management, such as saving, loading, deleting, copying, naming, and renaming files. The command processor checks commands from the keyboard before forwarding requests to the supervisor. It receives messages back from other parts of the operating system and translates them into language that the user can understand.

The OS in conjunction with the ROM BIOS, controls the basic input/output (I/O) functions that take place inside the computer. Input from the keyboard and other sources is handled by the OS, as is the output to the monitor, a printer, or other devices.

The disk and file management routines within the OS handle all disk I/O. These include creating, opening, closing, copying, deleting, and renaming files; reading from a file, writing to a file, and searching for files; and creating, deleting, and changing directories. The OS is also responsible for coordinating access to the CPU's computing resources and allocating memory for various applications. It provides a uniform method for initiating and terminating all other programs that run on the computer. It also has the capability to interpret and process commands typed at the file server keyboard.

Although DOS is serviceable for most network users, it has some major limitations. A DOS workstation can access only 640 kilobytes of RAM. This falls short for many programs today.

Workarounds such as expanded and extended memory serve some applications for program or data handling. However, the workaround software that allows DOS to access larger RAM is neither efficient, nor is it compatible with all software. Another limitation of DOS is the fact that it does only one task at a time. To solve this problem, IBM and Microsoft developed OS2.

OS2 does not work on old PCs (with 8088 or 8086 CPU's), but instead is intended for the newer 80286, 80386, and 80486 processors.

B. NETWORK OPERATING SYSTEM (NOS)

The NOS coordinates the LAN's hardware activity, just as DOS coordinates hardware activity in an individual PC. The NOS is often loaded after the computer's operating system. System hardware provides the data paths and platform on the network, but the NOS controls everything else. The NOS intercepts the data that is entered at the PC and passes it along the network channel, if appropriate, or passes the data back to the local PC for processing. (PC Today Magazine, Aug 90) Functionality, ease of use, performance, management, data safety, and security all depend on the NOS.

Today, interoperability between operating systems are available and improving. In 1989, network operating system companies fueled the growth of networks by announcing and delivering products conforming to open standards instead of proprietary protocols. AT&T, Digital, and 3COM led the industry in providing interoperable products for open standards. Instead of trying to lock-in and control each account with unique communication standards, they are delivering software that works according to nationally accepted standards.

Network operating systems available today are NOVELLE NetWare, IBM PC LAN Program, IBM LAN Server, 3COM 3+Open, Banyan Vines, and Apple AppleShare. (Durr, 1989)

A NOS is not one program but rather a series of programs. Some of these programs run in the PCs acting as servers of various types, and others run in PCs acting as client workstations. The networking software in servers provides and controls multiple simultaneous access to disk drives, printers, and other devices such as modems and facsimile boards. The networking software in client stations interrupts and redirects the requests for service that application programs generate and sends each of them to the appropriate server for action. (Derfler, 1991)

A NOS is the software necessary to integrate the many components of a network into a single system to which an end-user may have access. It manages the services necessary to ensure that the end-user has error-free access to network resources. Its basic function is to manage network addressing - provide the end-user the capability to establish a communications link from one node to another. Additionally, a NOS will normally provide a user interface that is supposed to reduce the trials and tribulations of using the network. Within the context of the NOS, applications such as an electronic mail system can be written which allow virtual circuits among network entities to be established without direct human intervention. (Madron, 1990)

The choice of NOS, perhaps more than any other LAN component, determines the success of the LAN. Criteria used to evaluate network operating systems include the following:

- Performance - Response time or throughput in accessing network resources.
- Functionality - This is related to each site's requirements.
- Compatible Applications - The NOS must be compatible to the software used.
- Extras - The enhancements that the NOS can support.
- Cost - Costs are measured against specific tasks and short term goals or against corporate long-term goals.

At the heart of the NOS is a concept called redirection - taking something headed in one direction and making it go in a different direction. The redirection software in each client computer makes the resources available on the network look like local DOS to the program and people using them. Commands sent from the keyboard and from programs to drives with names like D, E, and F are redirected over the network to the appropriate file servers. Similarly, programs sending output to a network printer address a local LPT port just as they normally do. The print jobs are redirected to the shared printer and queued on the PC acting as a print server until the printer is ready to take the job. (Derfler, 1991)

C. LAN DRIVERS

LAN drivers are often called communication drivers because they make communication over the physical cable possible. They provide the link between the operating system software and the network interface board, which is directly attached to the network cabling.

Information or data packets go through the network and they have a specific structure. A typical packet consists of a header and error checking codes as well as the actual data. The exact size and position of a packet's fields varies depending on the type of network (ARCnet, Token-Ring, EtherNet). Because of these differences in packet structure, network interface boards can communicate only with other boards of the same type over a certain type of cable. If the board is an EtherNet board, the driver performs actions necessary to create an Ethernet packet. The LAN driver code is also responsible for receiving packets and checking them for internal consistency.

If the driver code is slow or inefficient, the performance of the entire system suffers. Regardless of how fast and technologically advanced a network interface board is, it cannot live up to its full performance potential without a LAN driver specifically written to take advantage of the new capabilities of the hardware. For example, IBM's new 16Mbps Token-Ring boards support packet sizes up to 18KB. However, some drivers written for these boards transmit data in 1KB packets, thereby limiting the performance of the new boards. (Liebing, 1990)

D. NETWORK BASIC INPUT/OUTPUT SYSTEM (NetBIOS)

NetBIOS is an interface, not a protocol per se. It contains some critical software that functions as an interface between a program and network software on an IBM PC or compatible. It accepts commands from the program via software interrupts. Before using NetBIOS or making a NetBIOS call, the program creates and fills out a sort of electronic form called a network control block (NCB). The NCB tells the network software which of the 19 NetBIOS functions is to be performed. (Needleman, 1990)

It defines a series of commands, but not how these commands are to be communicated between two stations on a LAN. IBM did not completely explain what the NetBIOS commands do under all conditions. This may have led to incompatible NetBIOS implementations; programs that worked with one implementation would not work with another. Another common compatibility problem is user's misconception that NetBIOS is a protocol, rather than an interface. There is no guarantee that two network adapters driven by two different vendor's NetBIOS implementations will be able to exchange data reliably; in fact, the odds are that they will not. Vendors will implement NetBIOS on various protocol "stacks" (such as Novell's IPX, Xerox's XNS, TCP/IP etc). Programs written for a NetBIOS interface will generally port to various networks with no major problem. However, mixing protocol stacks on the same LAN may prevent NetBIOS programs from communicating with each other. To make two adapters communicate via NetBIOS, they have to be driven by compatible software, preferably the same release from the same vendor. (Needleman, 1990)

The NetBIOS interface provides key information on connecting together workstations, sending, and receiving information, and terminating communications. It was designed to be a low-level interface that works adequately, particularly if all workstations are using the same set of network protocols for routing information. Because it is a low-level data interface, it needs to be linked to a common protocol such as OSI or TCP/IP to ensure that network adapter cards are compatible. You can also use products that bridge together NetBIOS interfaces linked to different protocols.

The NetBIOS was a revolutionary service that supported a connection between nodes on the same network. Today, its features seem limited because the system has no implicit support for internetworking. It addresses only a small range of functionality required by sophisticated applications. (Durr, 1989)

NetBIOS is also a protocol independent session layer interface to which programmers can write for peer-to-peer communications. It provides an addressing scheme that allows nodes to be identified by a name rather than an esoteric number. These names can then be called to create a session between the nodes. Once the session is established, datagrams can be sent through the connection.

The service is very useful to communicate with another node without going through the network servers. In its native format it does not internetwork well.

E. APPLICATIONS

Applications are the real purpose for which networks exist. Without powerful, network-aware, multiuser application programs, LANs are just an expensive way for isolated users to share disk storage and printers. Putting applications on the network should be the overriding basis for all network setup and maintenance decisions. Ultimately, everything relates to what application is running and how it is set up.

A surprising number of LAN problems are related to the improper or careless installation of application software. Most network applications are fairly easy to install on the file server; others are not so easy. Then, there are always those application programs for which a network version is not yet available. (Liebing, 1990) To determine the degree of network compatibility, the following major characteristics of the application must be considered: (Liebing, 1990)

- Single-user versus Multiuser Applications - single-user applications are usually modified to run in a multiuser environment and they do not take advantage of the distributed processing capabilities inherent in multiuser applications.

- Server-Based Applications - In this type of application, the workstations become "clients" of a "server" that performs services other than the usual file services of the traditional file server. The services provided by a server-based application can either be something the workstations cannot do for themselves (usually the functions of a print server, CD- ROM server, or communications gateway involving specialized hardware not locally available to the client) or something the workstations could do for themselves but not as efficiently as the server.

- Multiple Defaults and Setup Files - A common difficulty with applications that are not very "network-aware" lies in the way they handle user preferences for defaults, configurations, and setup options. Most true multiuser applications provide a way for users to save their preferences in their personal network directories so that they do not overwrite other user's preferences.

- Network Operating System Features - The easiest applications to install are those that have a version designed specifically for a particular Network Operating System.

- License Agreements - Terms of the application's software license agreement. Multiuser software is usually sold with one of three licensing schemes: a site license, a per-server license, or a number-of-users license. A site license allows an unlimited number of users to run the application simultaneously as long as they are at the licensed site. With a per-server license, one copy of the software is loaded onto the file server. It cannot be loaded on any other server. Under a number-of-users license agreement, a user can purchase a version of the software tailored for a specific number of users.

- Fitting the Application into the Directory Structure - Some application programs require that all program files go into a single directory; with others, only certain files go into a main directory, and the rest go into nested subdirectories. This would make it easier to isolate files for back-up, and make it easier to upgrade or delete an application from the network.

- Share Critical Files as "Read-Only" - This prevents users from writing over program files. Making executable files "Read-Only" also helps prevent viruses from attaching themselves to the files. Share .EXE and .COM files should also be "Read-Only."

- Conserving Drive Mappings - certain applications require more than one search drive mapping to function properly. Often, one search drive must be mapped to the directory containing the actual program files, and another must be mapped to a directory containing specific configuration or setup files. Other programs may even require four or five search drive mappings. Also, every drive mapping users establish takes up 16 bytes of file server memory.

F. INTERRUPTS

An interrupt is a signal from a device or program that halts processing momentarily so that input/output or other operations can take place. When a program is interrupted or temporarily suspended, control is transferred to the supervisor. Interrupts use IRQ (interrupt requests) lines, registers, stacks, and parameter blocks to accomplish operations and they have priority levels, and higher-priority interrupts take precedence in processing. (Derfler, 1991) When the operation is finished, processing resumes. There are two types of interrupts: hardware interrupts and software interrupts. In a hardware interrupt, the signal is generated by a device (e.g., disk unit). In a software interrupt, the program generates a signal that suspends processing so that a specific operation can take place. (Pfaffenberger, 1990)

LAN cards/boards in a system must each be set to an IRQ that is unique to them. This is called the interrupt setting and it is the most challenging setting on the card and the cause of many network compatibility problems. I/O address conflicts and hardware interrupt conflicts are the most likely causes of a malfunctioning computer on a network. One of the problems with the PC and XT is the shortage of interrupt lines. They have only eight interrupt lines apiece, handled by one interrupt controller. The AT has two interrupt controllers working together for a total of 15 interrupts, but most LAN adapter cards have a limited selection. Examples of some interrupt functions are:

- Interrupt 3 is COM 2, the second serial port.
- Interrupt 4 is COM 1, the first serial port.
- Interrupt 5 is LPT2, the second parallel printer port.
- Interrupt 7 is LPT1, the first parallel printer port.

One must check that devices like a clone or emulation board do not use the same interrupt level as the one used on the network board (e.g., IRQ2). If this is the case, the interrupt setting on the network board will have to be changed (e.g., to IRQ7) so there is no conflict.

G. TSR (TERMINATE AND STAY RESIDENT) PROGRAMS

A TSR is a program designed to remain in the computer's random access memory (RAM) at all times so that users can activate it with a keystroke, even if another program is also in memory. TSR programs should be utilized with caution when using DOS because DOS does not operate in protected mode. DOS has no provisions for keeping one program from invading the memory space of another, and such invasions cripple the invaded program or causes a crash.

TSRs can cause software conflicts that masquerade as hardware conflicts. They are often loaded via the AUTOEXEC.BAT file, or may be loaded later on, as needed. The problem is that once a TSR terminates, it does not release its space for other purposes. This exacerbates the problem of limited RAM that is available when PCs are used on a network (due to the fact that both DOS and NOS must be resident in each PC). One solution is to use a "mark-release" approach. A "mark" program is executed prior to loading the TSR to mark the place in RAM where the TSR begins. A "release" program is executed when the TSR terminates to release the RAM occupied by the TSR.

V. CONCLUSION

The LAN industry has come a long way in finding ways to resolve compatibility issues. When local area networks first came about, compatibility did not exist. There was no such thing as multi-vendor networking or interoperability. Today, multi-vendor networking has improved. The improvement has occurred mostly in inter-LAN communication by using protocols like TCP/IP and routers and gateways. Unfortunately, many compatibility problems persist in intra-LAN communication among network boards, PC, NOS, DOS, and application software, particularly when multiple vendors are involved. The most the LAN manager can do is to be aware of potential incompatibilities and to defend against them using the methods suggested in this thesis.

APPENDIX: AS/IS LAB MANAGER'S GUIDE

LAN Manager's Guide

A Basic Reference Guide

For use on the

Administrative Sciences/Information Systems

(AS/IS) Computer Laboratories in

I-158, I-224, and I-250

September 1991

TABLE OF CONTENTS

A. INTRODUCTION

The Administrative Sciences (AS) Department of the Naval Postgraduate School has three microcomputer laboratories. They are located in Ingersoll Hall, rooms I-158, I-224, and I-250. Two of these labs (I-224 and I-250) are used as instructional laboratories. Access to the labs are restricted to students, faculty, and staff of the Naval Postgraduate School.

The purpose of this manual is to provide basic information about the setup and concepts governing the Administrative Sciences/Information Systems (AS/IS) microcomputer labs so as to aid lab managers. It is not a step-by-step guide in learning how to use these networks but rather an outline of the types of networks available, their setup, physically and logically; their capabilities; and the hardware and software used in each network. The guide is intended for use only at the Naval Postgraduate School and is tailored to the specific configurations of these labs.

B. NETWORK TECHNOLOGY

There are three different technologies used in the AS/IS laboratories: IBM Token-Ring, EtherNet, and Appletalk.

1. EtherNet

Ethernet Networks are defined by the IEEE 802.3 specification but, in practice, many variations also exist. EtherNet networks have two points in common: a contention access scheme and a linear bus topology. Ethernet runs on coaxial cabling using baseband or broadband transmissions. Ethernet can also be set up using telephone type cabling or optical fiber but the system may not entirely conform to the IEEE standard.

The original EtherNet networking scheme called for a thick coaxial cable, which has come to be known as thick EtherNet cable. Following the classic bus topology (a one-cable network tapped at any point where a workstation is required), a single thick EtherNet trunk cable runs from one end of the network to the other. The stations are connected to the bus via transceivers and associated cabling.

Most PC-based EtherNet networks use the thinner RG-58 coaxial cable, and have been dubbed "Cheapernet". Stations are connected on a bus in which cable is strung from one station to the next. A T-connector is used to attach the cable to the network interface board in each network station.

EtherNet uses the CSMA/CD medium access method. If a workstation wants to transmit, and no one else is using the cable, the station begins transmitting. If the cable is in use, the transmission is delayed until the cable is free. It provides a transmission speed of 10 megabits per second (Mbps). (EtherNet implementations range from 1Mbps to 10Mbps, although the 802.3 specification is intended to support signal rates up to 20 Mbps).

2. IBM Token-Ring

Token-Ring networks are defined by the IEEE 802.5 specification. Its name implies a ring, however, the token ring is physically a star, and electrically a ring. The LAN hardware in a Token-Ring network includes the network interface card (NIC), also called the network adapter; the data cable; the patch or adapter cable; and the Multistation Access Unit (MAU), which is a wiring concentrator that can connect as many as eight stations into the network. Repeaters can be added between two Multistation Access Units (MAU's) to increase the transmission distance. Each node acts as a repeater--receiving the serial bit stream from the nearest active upstream node, processing as necessary, and sending the bit stream on down the cable to the next node in line. Only a few bit times of delay are required in each network station for these functions. The serial transmission follows a complete ring or loop, with the sending station eventually receiving its transmitted information back after this information completes one round trip around the ring.

These networks use a token-passing scheme for network access. A station that needs to send a transmission must first gain control of the token. The token is merely a specific bit sequence that circulates among the nodes. For this reason, these networks are often described as distributed polling environments. Each workstation is thus polled to determine if it needs access to the network. When a node is in possession of the token, it can transmit a message that is in its output buffer. Otherwise, the node is in bit-repeat mode.

The wiring plans are star-wired rings, and shielded twisted pair wiring is the standard for internode connection. Current Token-Ring implementations are available in 4Mbps and 16Mbps.

3. Appletalk

Appletalk is a baseband network with a bus topology. It operates over shielded twisted-pair wire, unshielded twisted-pair, or optical fiber--all at 230.4 kilobits per second. Appletalk is a proprietary network standard that does not conform to any IEEE specifications. But it uses a layered architecture, and its protocols at every layer have been published, so other vendors can develop products for it.

Appletalk networking uses an access scheme that is similar to EtherNet's CSMA/CD--CSMA/CA. Under the CSMA/CA scheme, each MAC on the network listens for the signal that indicates another station is transmitting. If no other station is transmitting (no signals for 400 microseconds) a sending station waits an additional, random amount of time before transmitting. The sending and receiving stations will maintain control of the network medium by not allowing the medium to be quiet for more than 200 microseconds.

C. LABORATORY SETUP

The following setup describes the contents of the AS/IS labs. The table following the lab descriptions outlines the different characteristics of the AS/IS networks.

1. I-158

I-158 has six computers connected in an IBM Token-Ring network. This network has six IBM-XT computers, each with accelerator (Turbo) boards for increased speed. An IBM-AT is used as a file and print server. The printer is a laser-quality IBM 3812 Pageprinter. A Polaroid Palette film recording system is attached to one user computer which allows the creation of 35mm color slides.

Another, standalone, IBM-XT has the MAESTRO system, which gives users the capability to create computer-aided teaching programs. I-158 also has a Unix workstation--the Symmetric 375. See Figure (1) for a detailed layout.

2. I-224

This lab contains three networks: An IBM Token-Ring network with 15 attached user computers (12 AT-clones, 3 IBM-XTs); a 3COM EtherNet network with five attached computers; and an Apple-TOPS Appletalk Network with seven computers attached (six Apple Macintosh Plus' and two IBM-XTs). This Apple Talk network has APPLE-IBM connectivity.

The IBM Token-Ring network has two generic 386S and one IBM-XT computers as file and printer servers. The XT also serves as the IBM PC 3270 Emulation Gateway for 10 of the 15 user computers which are configured for terminal emulation. In addition, a 40MB Bernoulli Box is attached to one of the 386 servers. There are also an AST optical scanner, two IBM Proprinters, and one IBM Color Inkjet printer. See Figure (2) for a detailed layout.

The 3COM EtherNet network uses a 3COM 3Server[3] Server, an IBM Proprinter, and an IBM color plotter. See Figure (3) for a detailed layout.

The AppleTalk network uses an Apple Macintosh Plus as a server, which is located in a locked, vented cabinet. Apple does not provide any inherent physical security to the server unlike the IBM networks which allow locking of the keyboards. The server software used is the server version of Appleshare. In addition to the TOPS protocol, (which allows MAC-to-PC communication), the Apple network uses its own Apple protocol. The printer in the network is an Apple LaserWriter. Its cables and connectors are unique in that the network uses only Appletalk cables and connectors. See Figure (4) for a detailed layout.

3. I-250

I-250 has an IBM PC (Broadband EtherNet) network with 28 attached computers (25 IBM-XT user computers and three IBM-AT file and printer servers). It also has two IBM Proprinters, one IBM PC Graphics printer, one ceiling mounted projector for displaying the instructor's computer screen and a dual-drive Bernoulli Box with a capacity of 40Mb. See Figure (5) for a detailed layout. See below for a table outlining the characteristics in the AS/IS network labs.

AS/IS Network Labs Table: (Schneidewind, 1991).

Characteristics	IBM PC NET (I-250)	IBM Token-Ring (I-224)	3COM EtherNet (I-224)	Appletalk (I-224)
IEEE Standard	802.3	802.5	802.3	none
Access Method	- CSMA/CD - Collision detection - Jam signal	Token passing	same as IBM PC NET	CSMA/CA

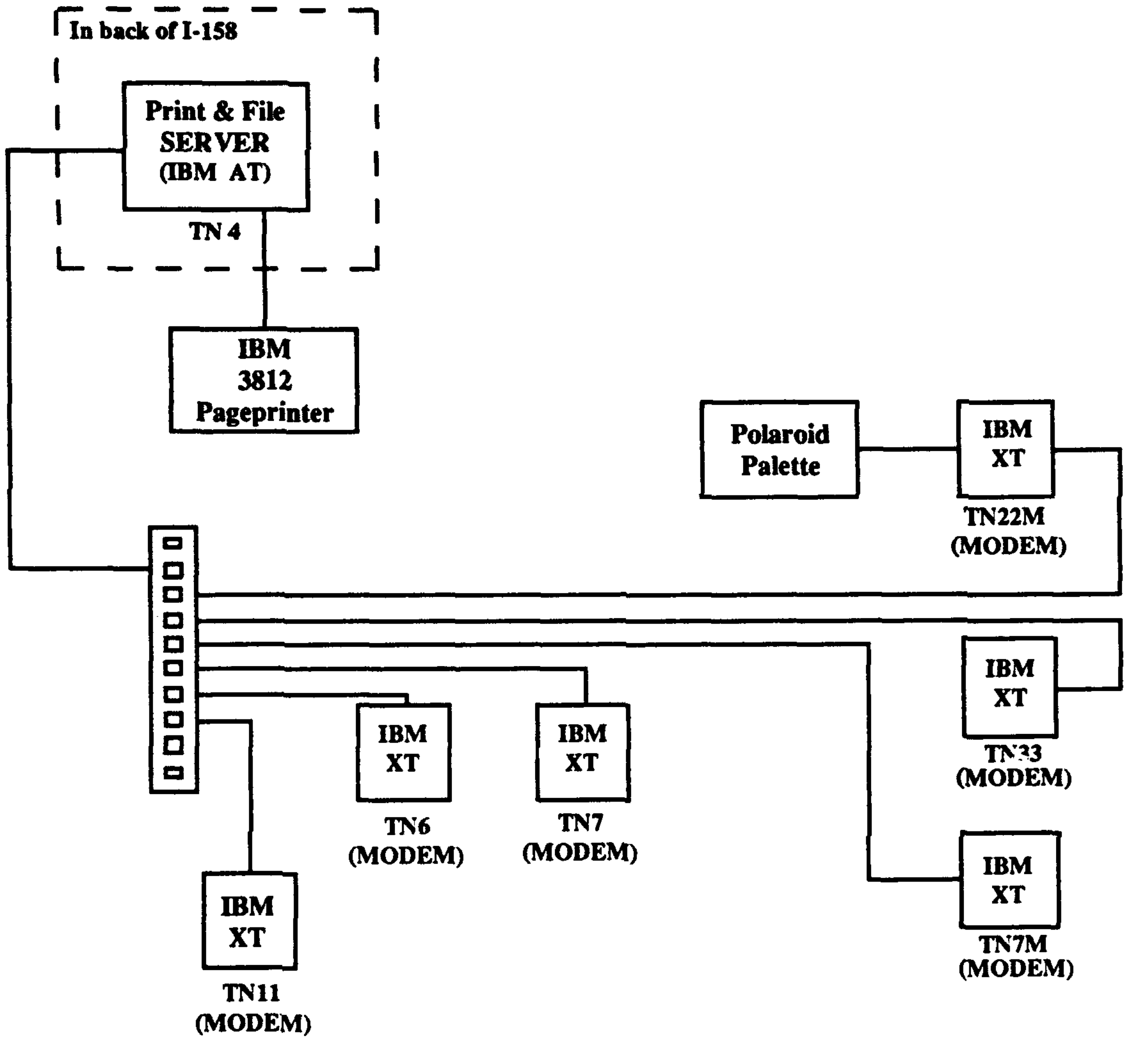
Media Type	Coax cable	Shielded Twisted pair	coax cable	Sheilded & Unshielded Twisted pair
Transmission Method	Broadband	Baseband	Baseband	Baseband
Transmission Speed	2 MBPS	4 & 16 MBPS	10 MBPS	230.4 kbps
Distance Limitation	1000 ft	- 770 m. for STP between nodes and repeaters. - 2 Km. for fiber optics bet. MAU & optical coupler	- 1000 ft for thin EtherNet - 3280 ft for thick EtherNEt	300 meters bet.nodes
Max. Number of nodes	72	- 72 for 4 Mbps - 250 for 16 Mbps	100 for thin EtherNet cable	32
Recommended Number of nodes	32	32 with 4Mbps	10 for thin EtherNet cable	6-10
Message Format	- Server message block - network message	same as IBM PC net	EtherNEt packets	Appleshare messages
User Interface	- Dir. of application BAT files - Network Function Menus - Network Commands	same as IBM PC Net	same as IBM PC Net	Appleshare hard disk icons
Performance	good performance at low loads	- High overhead at low load - good performance at medium and high loads	good performance at low loads	low power, slow

Topology	- logical bus - physical star	- logical ring - physical star	- logical bus - physical bus	-logical bus - physical bus
Other Services	- e-mail - limited file transfer (PC to PC) - full file transfer via dial-up communucation with hosts and 3270 emul.	same as IBM PC Net	- e-mail - menu system	IBM connectivity using TOPS

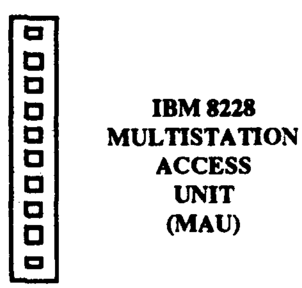
D. FILE ORGANIZATION

System and application programs are installed by the network supervisor or lab manager. A network administrator must identify who uses certain files and what type of use the files require. Although a great deal of data may be stored on the network in potentially shareable form, opening up all the data files to every user is not necessary or even desirable. Users have different uses for the files. One user may need to see a file but may not be involved in updating the information the file contains. This type of user would be given **Read-Only (R-O)** privileges. A user who actually updates the same file would require **Read/Write (R/W)** privileges. In addition, this kind of access restriction improves the integrity and the

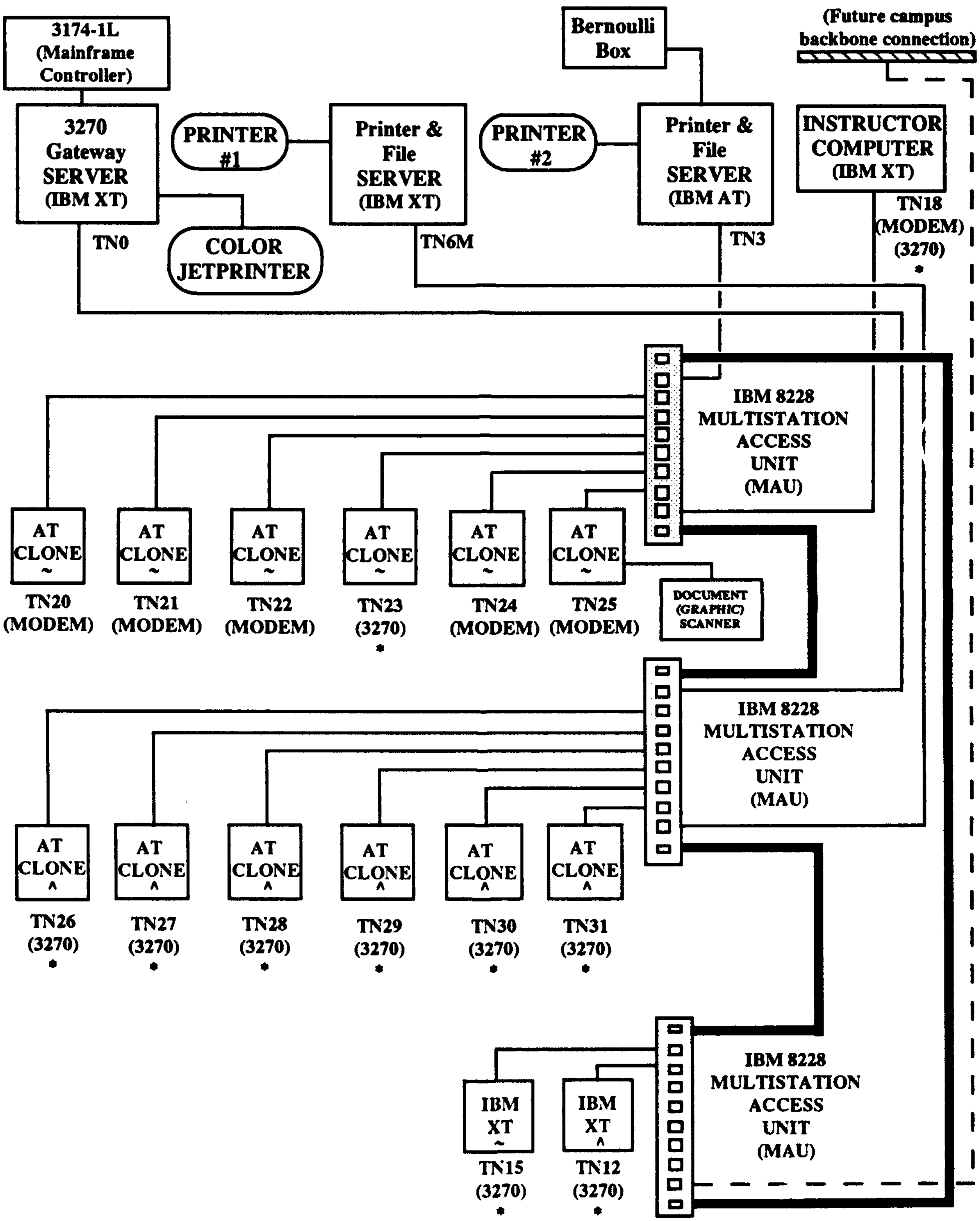
IN 158
IBM Token Ring LAN



Legend:

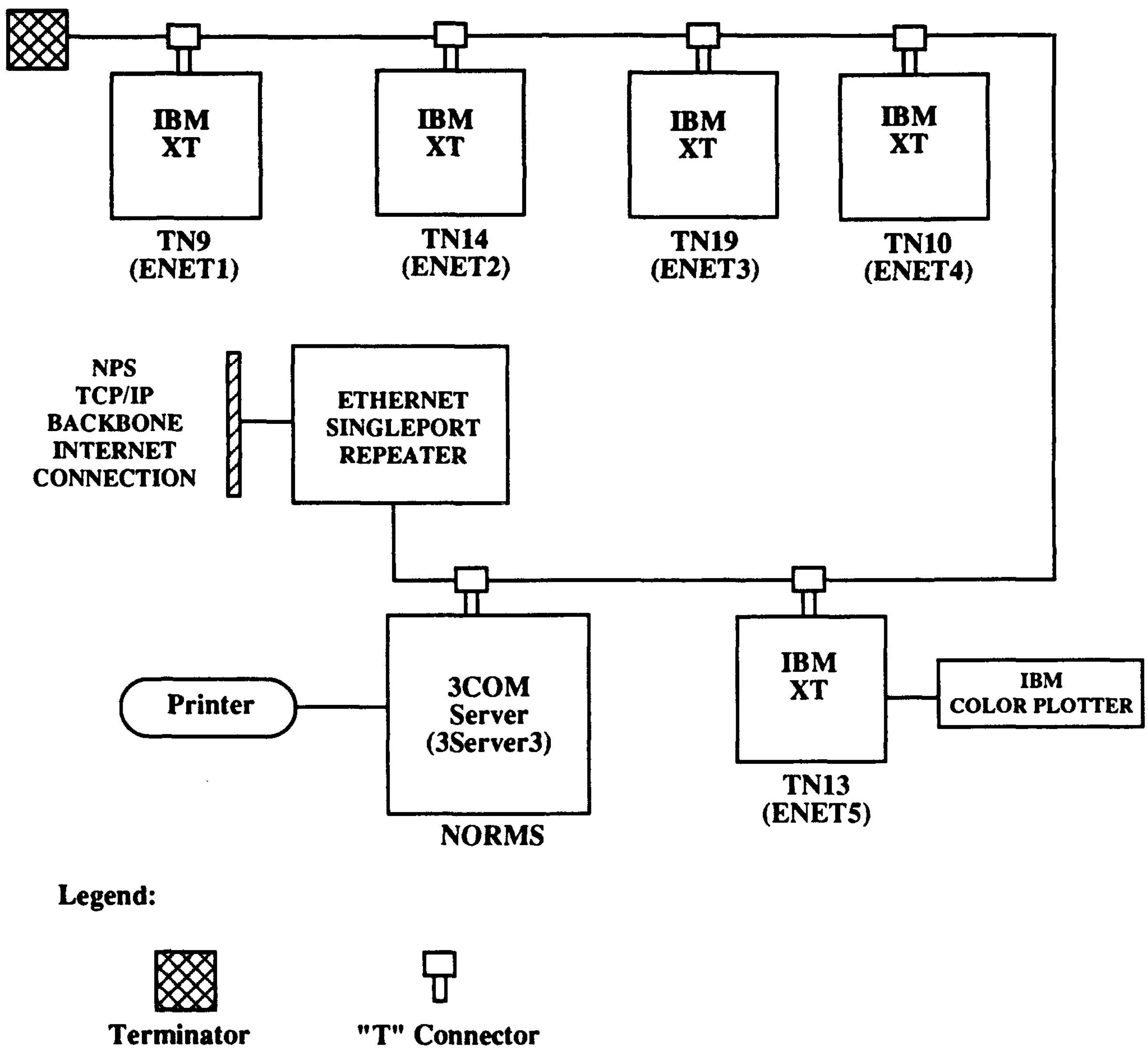


IN 224
IBM Token Ring LAN

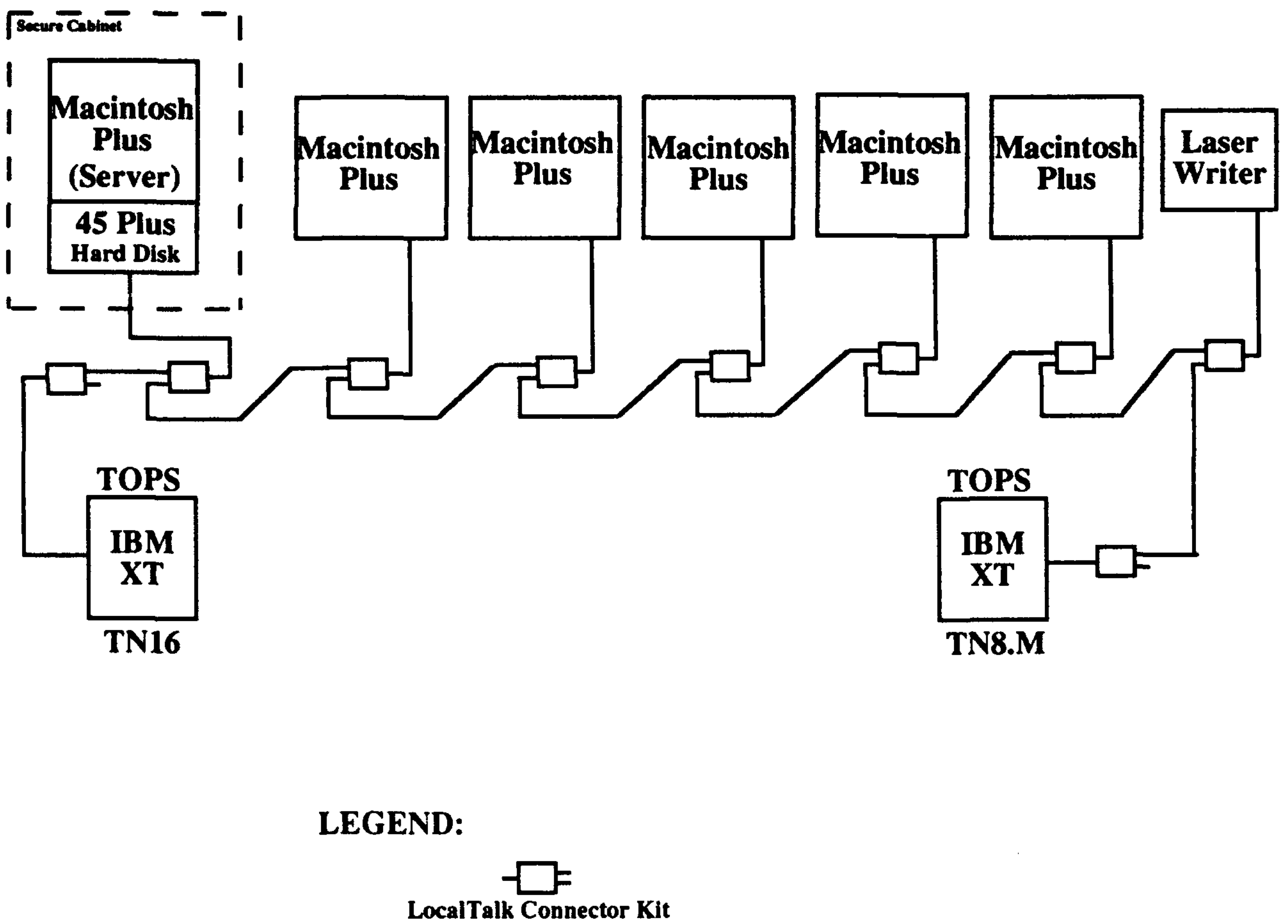


Note: This drawing, not to scale, shows the layout of the TR-LAN.
***The 3270 Emulation connection to the mainframe goes thru the Gateway server.**
~ Uses Printer #1)
^ Uses Printer #2){All users can use Color Jetprinter}

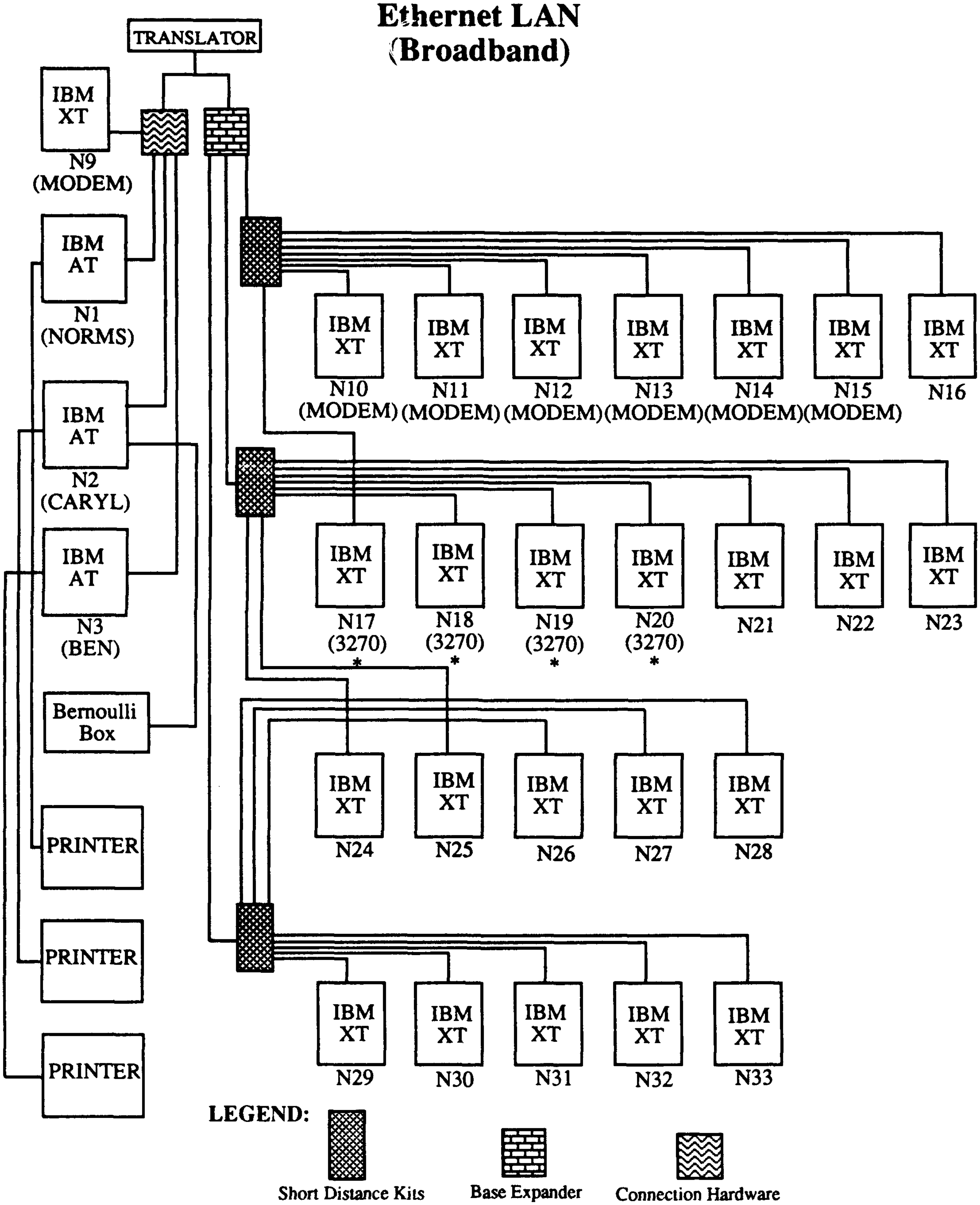
IN 224
3COM ETHERNET LAN



IN 224
Apple AppleTalk Layout



IN 250
Ethernet LAN
(Broadband)



*** The 3270 Emulation connects directly to the mainframe.**

security of the data.

Users of the AS/IS labs are generally given Read-Only privileges to application programs, which enables them to load and execute the programs, but not modify them. In these labs, however, the network supervisor has all rights to system files and keeps documentation as to file access rights.

E. SETTING UP DIRECTORIES

The structure of the AS/IS labs network directories is hierarchical. Each data storage area, or directory, is logically "below" another directory. The directory that all directories are below is called the **root** directory, represented with a backslash character (\). All other lower level directories are called subdirectories.

The user computer operating system is usually placed in its own directory, called DOS, below the root directory.

The objective for organizing a network is to give each user only as much authority as is needed to fulfill a particular job. In the AS/IS labs, all application programs are stored on the server hard disks where they are most easily controlled and supported and where they can be shared with all users. To store their created files, users save them on their own formatted 5.25 floppies.

When users log onto the network, the first thing they see is a main menu listing the different application programs and files, from which they can make a choice. This approach relieves the network manager from teaching users about paths and directories. Explicit instructions are posted beside each user computer on how to logon to the network. Users are not required to know anything at all about the network. Menu choices made by users are usually controlled by a batch file that contains a number of instructions for creating the necessary paths and loading the application. The logon process occurs automatically without the user seeing anything more than the options and the results.

F. SOFTWARE INSTALLATION

The network supervisor/lab manager ensures that the appropriate version(s) of software and related utilities are available to the users. Users will normally only use one version of a particular application. This ensures that all files created with the application will be compatible. User training and support are then simplified because they need to cover only one version of the software.

G. BATCH PROCESSING

No single tool is more important to the network user and supervisor than the batch file. They are crucial in managing and simplifying the network environment.

The AS/IS labs are controlled by batch files. A batch file is a text file containing a series of operating system commands. These files store the commands in text files and are identified by the extension BAT. The commands in the batch file execute sequentially when called upon. You can invoke several, even hundreds of instructions by simply starting the batch file with a one-word command. In the AS/IS labs, a batch file is installed that starts the network and takes you to a main menu where you can make a selection as to the application you want to use. The selections on the main menu are application batch files. The user can work with the application and is completely free to use any of its features. The AS/IS labs batch files are written so that when the user exits the application, additional system commands are executed to return the user computer to a standard network configuration. He or she is then returned to the main menu for another selection.

1. Using Batch Files to Simplify Procedures

Batch files are versatile and simplify procedures by carrying out repetitive sequences of commands. The user does not have to try to remember all the necessary commands. For example, if you frequently issue the same five commands when you start a system, you can put those commands in a batch file and give the batch file a name: for example STARTUP.BAT. When you enter the command STARTUP, the file runs and the commands are executed.

Batch files do not have to be complex chunks of programming. Most batch files are short lists of operating system commands. A typical batch file is no more than a dozen lines.

To create effective batch file systems, you must have an understanding of the user computer's operating system and the network's operating system.

The Disk Operating System (DOS) used on the networks is IBM version 3.3 except for the 3COM network in I-224 which uses IBM DOS 3.2. The Networking Operating System (NOS) used in the AS/IS labs is version 1.2 of the IBM PC LAN program.

To create a Batch File, you can use one of three different methods:

1. The COPY Command - The Copy command is quick and easy to use but is unsuitable for lengthy batch files because the command does not enable you to make corrections without completely re-creating the file. You can use COPY to copy keyboard input into a file. You must ensure, however, that

the file name you specify does not already exist. Otherwise, the old file is overwritten and lost.

2. The EDLIN program - This DOS utility supports the creation and modification of batch files. This method is always available because it is included with DOS.

3. The Word Processor - This highly flexible method is ideal for creating and documenting long batch files. Load your word processor and open a document. Type each command at the left margin on a separate line. When you are finished, save the file as an ASCII (or DOS text) file. Use any filename you want, but be sure to use the BAT extension required for all batch files.

2. The CONFIG.SYS File

The CONFIG.SYS file is not a batch file but rather a system file that performs specific tasks. The file contains values that DOS uses to configure itself in memory each time the system starts. Such values include, for example, the BUFFERS= entry (which defines the number of disk buffers DOS uses) and the FILES= entry (which specifies the number of files DOS can have open at one time). The CONFIG.SYS file is usually created the first time you install DOS. Later on, you may modify the file to suit your changing requirements. The file can include a DEVICE line, which identifies any one of a number of physical or logical attachments to the network.

Each such device requires its own device driver, which is a special program providing the required logical interface between the device and the entire system. DOS must be able to find the driver in order to load it, and the DEVICE line specifies the path (if any) to the driver.

Each time the computer is turned on, DOS installs itself in the computer's memory before executing any other commands. DOS uses the entries in the CONFIG.SYS file to customize the operating system. If this file does not exist, DOS uses default values. Only after DOS is completely installed does it check for the existence of the AUTOEXEC.BAT file.

3. The AUTOEXEC.BAT File

When DOS starts, it searches the root directory for a file called AUTOEXEC.BAT. This distinctive file AUTOmatically EXECutes a group of initializing instructions before doing anything else. This BATch file is similar to other batch files except that its filename is known to DOS and thus cannot be used for any other purpose except to startup a computer.

In the AS/IS labs, the AUTOEXEC.BAT sets up paths to the drives and directories, loads certain operating files (when needed), and establishes environmental variables, as required. It also sets parameters so that the prompt shows the current directory. Finally, it displays a screen to give users some information on starting the network, availability of printers, and what to do if a problem arises.

Using a CONFIG.SYS file and an AUTOEXEC.BAT file will go a long way toward relieving the user of having to wade through a long series of complex instructions every time the system is turned on. They also help avoid errors that might occur during the start up process.

4. DOS Environment

The DOS environment or Master DOS Environment Block is a memory block in which the system stores critical information created by the CONFIG.SYS and the AUTOEXEC.BAT files, such as the command path and definition of the system prompt. To view the current environment, type SET at the DOS prompt. The SET command changes or displays the value assigned to an environment variable. You can also use it to define replaceable parameters for use with batch files. For example, if the current environment space is too small, you can set aside more space for the environment by editing the CONFIG.SYS file.

When considering the potential sources of network problems, it is important to remember that a LAN environment includes not only the physical components such as hardware, software and cabling but also the users of the LAN. Users may often have difficulty with a network because of an incomplete understanding of basic LAN concepts. A well organized network administration avoids most of these problems by using standardized procedures and by providing information and help to the users.

Standard maintenance procedures help reduce a great number of potential network problems. LAN maintenance involves not only fixing or replacing broken parts, but includes performing regular (and sometimes menial) tasks to reduce the risk of network downtime. Simple procedures such as cleaning the heads on a tape back-up unit, hard disk optimization routines, periodic cabling inspections, and vacuuming and cleaning network components are examples of tasks which may help to prevent a large number of potential problems.

Cabling problems include network data and equipment power cables. They can be wiggled or jarred loose, and become disconnected, to cause computer or printer failures. Checking the tightness of all cable connections is a sound troubleshooting/maintenance action.

Software problems can result from improper installation or incorrect parameter settings for network services. Changes in parameter settings should only be made when a clear understanding of the desired effects are known! Software problems can also occur when certain applications are introduced to the network. Single user applications differ significantly from programs which are network aware or are specifically designed to be multiuser. Always thoroughly check the documentation to understand the potential implications. Careful testing should be performed before new applications are made available to all network users!

REFERENCES

Aaron, Bud and Aaron, Alex, Upgrading PC's Made Easy, Osborne McGraw-Hill, 1991.

Apple Computer Inc., Understanding Computer Networks, Addison-Wesley Publishing Company, 1989.

Archer, Rowland, The Practical Guide to Local Area Networks, Osborne McGraw-Hill, 1986.

Axelrod, C. Warren, Computer Productivity, John Wiley & Sons, Inc., 1982.

Berry, Paul, Operating The IBM PC Networks, Sybex, 1986.

Bertsekas, Dmitri and Gallager, Robert, Data Networks, Prentice-Hall, Inc., 1987.

Brenner, Aaron, "Getting Better," p.14 LAN Magazine, March 1989.

Bulettw, Greg and Chacon, Michael, Understanding 3 COM Networks, Wordware Publishing, Inc., 1991.

BYTE Magazine, June 1990. "Growing Pains."

Calingaert, Peter, Operating System Elements, A User Perspective, Prentice-Hall, 1982.

Cashin, Larry, "Choosing a LAN OS: Proceed with Caution," p.59, Software Magazine, March, 1990.

Cole, Gerald D., Computer Networking for Systems Programmers, John Wiley and Sons, Inc., 1990.

Costa, Linda C. and Glasgow, Mary R., "Good Software Demands Good Documentation", IEEE Professional Communication Society Conference Record, IEEE Service Center.

Davis, George R., The Local Network Handbook, McGraw Hill Publications, 1982.

Derfler Jr., Frank J., PC Magazine Guide to Connectivity, Ziff-Davis Press, 1991.

Doll, Dixon, "The Year Ahead: Changes and Challenges in Networking," Network World, 24 December, 1990.

Durr, Michael and Gibbs, Mark, Networking Personal Computers, 3rd Edition, Que Corporation, 1989.

Edelhart, Mike, Novell NETWARE Power Tools, Bantam Books, 1991.

Foster, Jennifer, The Hardware Guide for Novell NetWare, John Wiley and Sons, Inc., 1991.

Gookin, Dan, The ABC's of Upgrading Your PC, Sybex Inc., 1990.

Green, Jr. Paul E., Network Interconnection and Protocol Conversion, IEEE Press, 1988.

Guengerich, Steven, "Interoperability is Key to LAN Operating Systems," p.1, Network World, 1 October 1990.

Hader, Michael L., NETWARE Troubleshooting, Addison-Wesley Publishing Co. Inc., 1991.

Haugdahl, J. S., Inside NetBIOS, 3rd Edition, Architecture Technology Corporation, 1990.

Johnston-Turner, Mary, "Standards are Moving Targets for Harried Users," p.35, Network World, Nov 19, 1990.

Jordan, Larry and Churchill, Bruce, Communications and Networking for the IBM PC and Compatibles, 3rd Edition, Simon and Schuster, 1990.

Kibirige, Harry M., "Local Area Networks in an Online Information Retrieval Environment," National Online Meeting, Proceedings of the Ninth National Online Meeting, New York, 10-12 May, 1988.

LAN Magazine, December 1988. "LAN Interface Cards."

Liebing, Edward and Neff, Ken, NETWARE Server, Troubleshooting and Maintenance Handbook, McGraw-Hill Inc., 1990.

Liebing, Edward, Knutson, Charles D., and Day, Michael, NETWARE Workstation, Troubleshooting and Maintenance Handbook, McGraw-Hill, Inc., 1990.

Madron, Thomas W., Local Area Networks, The Next Generation, John Wiley and Sons, 1990.

Marney-Petix, Victoria C., Networking and Data Communications, Reston Publishing Co., 1986.

Martin, James, Telecommunications and the Computer, Prentice-Hall, Inc., 1990.

McConnell, John, Internetworking Computer Systems, Interconnecting Networks and Systems, Prentice-Hall, 1988.

McNamara, John E., Local Area Networks, Digital Press, 1985.

Miller, Mark A., LAN Troubleshooting Handbook, M & T Publishing, Inc., 1989

Miller, Michael A., Internetworking, M & T Books 1991.

Needleman, Raphael, InfoWorld: Understanding Networks, Simon and Schuster 1990.

Norton, Peter, Inside the IBM PC and PS/2, Simon and Schuster, Inc., 1990.

Nunemacher, Greg, LAN Primer, M & T Books, 1990.

Pfaffenberger, Bryan, Que's Computer User's Dictionary, Que Corporation, 1990.

Rimmer, Steven W., Networking with TOPS, Sybex 1990.

Rinzler, Alan and Gancher, David, The Computerland Guide to Local Area Networks, Computerland Books, 1990.

Rosch, Winn L., The Winn Rosch Hardware Bible, Simon and Schuster, Inc., 1989.

Salamone, Salvatore, "Getting From EtherNet to Token-Ring by Bridge: Beyond the LAN Boundary," p.1, Network World, 7 January, 1991.

Schatt, Stan, Linking LANS, A Micro Manager's Guide, Windcrest Books, 1991.

Schneidewind, Norman, IS 3503 Class Notes, 1991.

Stallings, William, Local Networks, An Introduction, Macmillan Publishing Co., 1984.

Stallings, William, Handbook of Computer Communications Standards, Local Network Standards, Volume 2, Macmillan Publishing Co., 1987.

Turner, Steven, "The Network Manager's Compendium of Standards," p.1, Network World, 15 April, 1991.

Van Kirk, Doug, "Troubleshoot your New Add-In Boards," p. 141, PC Computing Magazine, July, 1991.

Woodward, Jeff, The ABC's of Novell Netware, Sybex 1989.

Woram, John, The PC Configuration Handbook, 2nd Edition, Bantam Books, 1990.

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Superintendent Attn: Library, Code 0052 Naval Postgraduate School Monterey, California 93943-5000	2
3.	Commanding Officer Attn: LCDR Rita V. Espiritu NAVCOMTELSTA PSC 458, Box 7 FPO AP 96451	2
4.	Professor Norman F. Schneidewind Administrative Sciences Department Naval Postgraduate School Monterey, California 93943-5000	1
5.	Professor Myung W. Suh Administrative Sciences Department Naval Postgraduate School Monterey, California 93943-5000	1