NONRESIDENT TRAINING COURSE

October 1997

Information Systems Technician Training Series

Module 3—Network Communications

NAVEDTRA 14224

NOTICE

Any reference within this module to "Radioman" or the former "Radioman rating" should be changed to "Information Systems Technician" and the "Information Systems Technician (IT) rating". The subject matter presented relates to the occupational standards for the IT rating.

Although the words "he," "him," and "his" are used sparingly in this course to enhance communication, they are not intended to be gender driven or to affront or discriminate against anyone.

PREFACE

By enrolling in this self-study course, you have demonstrated a desire to improve yourself and the Navy. Remember, however, this self-study course is only one part of the total Navy training program. Practical experience, schools, selected reading, and your desire to succeed are also necessary to successfully round out a fully meaningful training program.

COURSE OVERVIEW: In completing this nonresident training course, you will demonstrate a knowledge of subject mattter by correctly answering questions on the following subjects: Network Administration, LAN Hardware, and Network Troubleshooting.

THE COURSE: This self-study course is organized into subject matter areas, each containing learning objectives to help you determine what you should learn along with text and illustrations to help you understand the information. The subject matter reflects day-to-day requirements and experiences of personnel in the rating or skill area. It also reflects guidance provided by Enlisted Community Managers (ECMs) and other senior personnel, technical references, instructions, etc., and either the occupational or naval standards, which are listed in the *Manual of Navy Enlisted Manpower Personnel Classifications and Occupational Standards*, NAVPERS 18068.

THE QUESTIONS: The questions that appear in this course are designed to help you understand the material in the text.

VALUE: In completing this course, you will improve your military and professional knowledge. Importantly, it can also help you study for the Navy-wide advancement in rate examination. If you are studying and discover a reference in the text to another publication for further information, look it up.

1997 Edition Prepared by
DPC(SW) Walter Shugar, Jr. and
RMCS(SW/AW) Deborah Hearn

Reissued on July 2002 to correct minor discrepancies or update information. No significant change have been made to content.

Published by
NAVAL EDUCATION AND TRAINING
PROFESSIONAL DEVELOPMENT
AND TECHNOLOGY CENTER

NAVSUP Logistics Tracking Number
0504-LP-026-8630

Sailor's Creed

"I am a United States Sailor.

I will support and defend the Constitution of the United States of America and I will obey the orders of those appointed over me.

I represent the fighting spirit of the Navy and those who have gone before me to defend freedom and democracy around the world.

I proudly serve my country's Navy combat team with honor, courage and commitment.

I am committed to excellence and the fair treatment of all."

CONTENTS

SUMMARY OF THE RADIOMAN TRAINING SERIES

MODULE 1

Administration and Security—This module covers Radioman duties relating to administering AIS and communication systems. Procedures and guidance for handling of classified information, messages, COMSEC material and equipment, and AIS requirements are discussed.

MODULE 2

Computer Systems—This module covers computer hardware startup, including peripheral operations and system modification. Other topics discussed include computer center operations, media library functions, system operations, and troubleshooting techniques. Data file processes, memory requirements, and database management are also covered.

MODULE 3

Network Communications-This module covers network administration, LAN hardware, and newtwork trobleshooting. Related areas discussed are network configuration and operations, components and connections, and communication lines and nodes.

MODULE 4

Communications Hardware—This module covers various types of communications equipment, including satellites and antennas. Subjects discussed include hardware setup procedures, COMSEC equipment requirements, distress communications equipment, troubleshooting equipment, satellite theory, and antenna selection and positioning.

MODULE 5

Communications Center Operations—This module covers center operations, including transmit message systems, voice communications, center administration, quality control, and circuit setup/restorations. Guidelines for setting EMCON and HERO conditions and cryptosecurity requirements are also discussed.

CREDITS

Trademark Credits

ARCnet is a registered trademark of Datapoint Corporation.

Ethernet is a registered trademark of Xerox Corporation.

Novell is a registered trademark of Novell, Inc.

UNIX is a registered trademark of X/Open Company Ltd.

Windows 3.11 is a registered trademark of Microsoft Corporation.

Windows 95 is a registered trademark of Microsoft Corporation.

Windows NT is a registered trademark of Microsoft Corporation.

INSTRUCTIONS FOR TAKING THE COURSE

ASSIGNMENTS

The text pages that you are to study are listed at the beginning of each assignment. Study these pages carefully before attempting to answer the questions. Pay close attention to tables and illustrations and read the learning objectives. The learning objectives state what you should be able to do after studying the material. Answering the questions correctly helps you accomplish the objectives.

SELECTING YOUR ANSWERS

Read each question carefully, then select the BEST answer. You may refer freely to the text. The answers must be the result of your own work and decisions. You are prohibited from referring to or copying the answers of others and from giving answers to anyone else taking the course.

SUBMITTING YOUR ASSIGNMENTS

To have your assignments graded, you must be enrolled in the course with the Nonresident Training Course Administration Branch at the Naval Education and Training Professional Development and Technology Center (NETPDTC). Following enrollment, there are two ways of having your assignments graded: (1) use the Internet to submit your assignments as you complete them, or (2) send all the assignments at one time by mail to NETPDTC.

Grading on the Internet: Advantages to Internet grading are:

- you may submit your answers as soon as you complete an assignment, and
- you get your results faster; usually by the next working day (approximately 24 hours).

In addition to receiving grade results for each assignment, you will receive course completion confirmation once you have completed all the assignments. To submit your assignment answers via the Internet, go to:

http://courses.cnet.navy.mil

Grading by Mail: When you submit answer sheets by mail, send all of your assignments at one time. Do NOT submit individual answer sheets for grading. Mail all of your assignments in an envelope, which you either provide yourself or obtain from your nearest Educational Services Officer (ESO). Submit answer sheets to:

COMMANDING OFFICER
NETPDTC N331
6490 SAUFLEY FIELD ROAD
PENSACOLA FL 32559-5000

Answer Sheets: All courses include one "scannable" answer sheet for each assignment. These answer sheets are preprinted with your SSN, name, assignment number, and course number. Explanations for completing the answer sheets are on the answer sheet.

Do not use answer sheet reproductions: Use only the original answer sheets that we provide—reproductions will not work with our scanning equipment and cannot be processed.

Follow the instructions for marking your answers on the answer sheet. Be sure that blocks 1, 2, and 3 are filled in correctly. This information is necessary for your course to be properly processed and for you to receive credit for your work.

COMPLETION TIME

Courses must be completed within 12 months from the date of enrollment. This includes time required to resubmit failed assignments.

PASS/FAIL ASSIGNMENT PROCEDURES

If your overall course score is 3.2 or higher, you will pass the course and will not be required to resubmit assignments. Once your assignments have been graded you will receive course completion confirmation.

If you receive less than a 3.2 on any assignment and your overall course score is below 3.2, you will be given the opportunity to resubmit failed assignments. **You may resubmit failed assignments only once.** Internet students will receive notification when they have failed an assignment--they may then resubmit failed assignments on the web site. Internet students may view and print results for failed assignments from the web site. Students who submit by mail will receive a failing result letter and a new answer sheet for resubmission of each failed assignment.

COMPLETION CONFIRMATION

After successfully completing this course, you will receive a letter of completion.

ERRATA

Errata are used to correct minor errors or delete obsolete information in a course. Errata may also be used to provide instructions to the student. If a course has an errata, it will be included as the first page(s) after the front cover. Errata for all courses can be accessed and viewed/downloaded at:

http://www.advancement.cnet.navy.mil

STUDENT FEEDBACK QUESTIONS

We value your suggestions, questions, and criticisms on our courses. If you would like to communicate with us regarding this course, we encourage you, if possible, to use e-mail. If you write or fax, please use a copy of the Student Comment form that follows this page.

For subject matter questions:

E-mail: n311.products@cnet.navy.mil
Phone: Comm: (850) 452-1501
DSN: 922-1501
FAX: (850) 452-1370
(Do not fax answer sheets.)
Address: COMMANDING OFFICER
NETPDTC N311
6490 SAUFLEY FIELD ROAD
PENSACOLA FL 32509-5237

For enrollment, shipping, grading, or completion letter questions

E-mail: fleetservices@cnet.navy.mil
Phone: Toll Free: 877-264-8583
Comm: (850) 452-1511/1181/1859
DSN: 922-1511/1181/1859
FAX: (850) 452-1370
(Do not fax answer sheets.)
Address: COMMANDING OFFICER
NETPDTC N331
6490 SAUFLEY FIELD ROAD
PENSACOLA FL 32559-5000

NAVAL RESERVE RETIREMENT CREDIT

If you are a member of the Naval Reserve, you may earn retirement points for successfully completing this course, if authorized under current directives governing retirement of Naval Reserve personnel. For Naval Reserve retirement, this course is evaluated at 3 points. (Refer to *Administrative Procedures for Naval Reservists on Inactive Duty,* BUPERSINST 1001.39, for more information about retirement points.)

Student Comments

Course Title: *Information Systems Technician Training Series*
Module 3—Network Communications

NAVEDTRA: 14224 **Date**: _____

We need some information about you:

Rate/Rank and Name: _____ SSN: _____ Command/Unit _____

Street Address: _____ City: _____ State/FPO: _____ Zip _____

Your comments, suggestions, etc.:

Privacy Act Statement: Under authority of Title 5, USC 301, information regarding your military status is requested in processing your comments and in preparing a reply. This information will not be divulged without written authorization to anyone other than those within DOD for official use in determining performance.

NETPDTC 1550/41 (Rev 4-00

CHAPTER 1

NETWORK ADMINISTRATION

Upon completing this chapter, you should be able to do the following:

- *Describe how to establish communications with remote terminals and monitor system transmissions.*
- *Describe how to start up, monitor, and terminate network processing.*
- *Explain how to change network software configurations and how to analyze network hardware configurations.*
- *Explain how to install and test software and how to perform system restorations.*
- *Explain how to evaluate network requests.*
- *Describe the procedures used to calculate network capacity.*
- *Explain how to determine communications protocols and how to design a network.*

Welcome to the wonderful world of networking. Networking has opened the world to connectivity. Networking gives an individual the capability to communicate and connect with another individual or another system in order to share resources.

The end result is to establish communications between two PC computers or two entirely different systems. The process used to reach that point can be done many ways. Once you have established connectivity and are communicating, then you will need to monitor the systems transmission to ensure the two computers are, in fact, communicating successfully. Some of the factors that will have to be taken into consideration are:

- What type of hardware will be needed
- What operating system (OS) will be used
- What applications will be needed
- What type of cabling will be used

NETWORK OPERATIONS

Networks consist of **nodes** that are interconnected by **links.** These nodes and links usually cover a relatively small geographical area, commonly known as a local area network, ranging from a few feet to a mile. Nodes are the hardware, such as computers, terminals, hard disks, printers, and so on. Links are the communications media, such as twisted-pair wire, coaxial cable, or fiber optic cable that connects the nodes.

Networks are made up of a variety of hardware, network software, connecting cables, and network interface cards combined in any number of ways. And that is perfectly OK. Quite often, we design a network using existing hardware. That is just one of the many reasons why each individual network has its own unique characteristics. The network hardware and software components determine the structure of a network, whether it is a local, metropolitan, or wide area network. Normally, the workstations (PCs) in a LAN are in close proximity to each other, usually within the same building. A metropolitan area network (MAN) consists of PCs that are basewide: one command connected with another command, or one base connected with another base, all via phone lines. A wide area network (WAN) is worldwide: one country connected with another country via satellites, etc.

A network could be made up of 13 PCs, a server with a hard disk, 3 printers, and a plotter. Another network could be made up of 6 PCs (one of which is the network server) and a laser printer. Both are networks. When you connect individual PCs together (via cable), and each PC is allowed access to the other's information and/or resources, you have created a network (see figure 1-1). By connecting PCs in this fashion, you are able to share all sorts of things. Examples are information in files; software, such as word processors, spreadsheet programs, and utilities; and peripheral devices, such as hard disks, printers, plotters, and fax machines.

A network gives you the capability of transferring data, files, programs, you name it, from one PC to another or even from one network to another. You can transfer a report or listing to any printer you desire on the network, provided you have access to the printer. How is that for flexibility? By connecting your PC into a network system, you can execute application programs stored on the server's hard disk without having to worry about disk space or keeping track of diskettes. You can exchange files and programs with other users directly without copying them onto a diskette. Can you begin to see the power and flexibility built into a network system?

COMMUNICATIONS WITH REMOTE TERMINALS

The ability to connect to the LAN through the use of remote terminals gives you great flexibility, whether it is being able to check your E-mail via a modem or check the status of the LAN by connecting to the network as a remote console. The remote capabilities will increase productivity. The network supervisor can manage the system by establishing communications through a remote terminal.

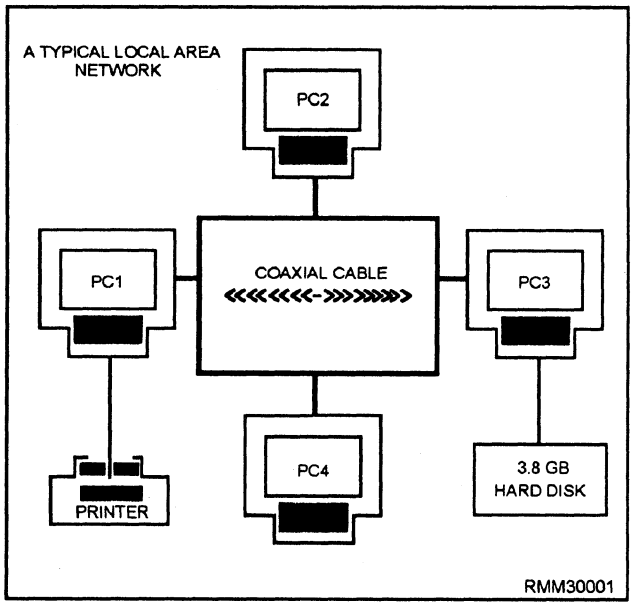

Figure 1-1.—Connecting PCs to form a local area network.

Logins from Remote Locations

Remote access refers to logins from remote locations. These login procedures are accomplished by dialing into an access server (a special modem or computer) and logging in through this server.

The network modems that can be used as remote access servers must have a network interface card (NIC) compatible with the network to which the modem is providing access. Remote connections often require special timing considerations, because many network transactions must happen within a very limited time period.

Remote Console

A networking utility that enables a network supervisor to manage a server from a workstation or from a remote location using a modem. The supervisor can give commands and accomplish tasks just as if all the commands were being given directly at the server by simulating a direct connection to the server.

NETWORK STARTUP/SHUTDOWN

Keeping the system running is the most visible aspect of system administration. You're the one they will call when the system has gone down (crashed). We will discuss the normal UNIX booting (startup) and shutdown processes. Shutting down and bringing up a UNIX system is actually very simple.

System Startup

Every time the system is booted, a series of steps must be performed before the system becomes available to users. Booting is the process of bringing a computer system up and making it ready to use.

The process begins when some instructions stored in ROM are executed which load the program boot from the boot partition into system memory. Boot loads the bootable operating system, which is also called the bootable kernel. The bootable kernel starts the init (initialization) program.

INIT.— One of the first things init does is check available memory, Next, it checks out the environment to see what hardware is present. When the kernel is

configured, it is told what types of hardware devices to expect. Init will search for and attempt to initialize each physically attached device. Any device that does not initialize or that is missing will be marked as nonexistent and the driver disabled. Even if the device is later reconnected, it will be unusable until the system is rebooted.

When all is ready, the kernel verifies the integrity of the root filesystem and then mounts it. Init does the rest of the work that is needed in preparing the system for users. This includes mounting the remaining local disk partitions (those found in the file /etc/checklist); performing some filesystem cleanup operations (fsck); turning on the major UNIX subsystems, such as accounting and the print service; starting the network; mounting remote file systems; and enabling user logins.

SYSTEM MODES.— There are two primary modes of system operation: single-user and multi-user. Single-user is a system state designed for administrative and maintenance activities which require complete and unshared control of the system. Single-user mode is sometimes called the maintenance mode. Single-user mode is entered via manual intervention during the boot process. Sometimes, however, the system will enter single-user mode if there are problems in the boot process that the system cannot handle on its own. Multi-user allows many users to all log onto the same CPU. Users can access different applications simultaneously or even the same application simultaneously. The kernel manages the different users by scheduling the use of the processing time as well as swapping programs and data in and out of memory through virtual memory to disk. The most important fact to remember is that the number of concurrent users depends on the amount of memory installed in the computer. Each user has a certain amount of memory set aside for his or her work, unless everyone is willing to tolerate slow response time from the network.

System Shutdown

While there are many occasions when shutting down or rebooting the system is appropriate, neither operation should be performed indiscriminantly. While it is generally not something to worry about, there is a degree of hardware fatigue associated with turning a computer system off and on again, and it is often better to let it run 24 hours a day than to shut it down at night.

REBOOTING.— There are only four common situations in which rebooting the system is called for:

- If you make changes to any of the system software or configuration files that are examined or executed only when the system is booted, you must reboot for these changes to take effect.
- Some devices, especially printer and modem ports, can become confused enough that resetting them is only accomplished by re-initializing the system.
- If the system has been up and running constantly for over a week, it is wise to bring the system down to single-user mode and run fsck. If any fixes are made to the root partition, the system must be rebooted.
- If the system console becomes irretrievably hung, the system must be rebooted.

SHUTTING THE SYSTEM DOWN.— There are two proper ways to shut down the operating system: shutdown and reboot. As a last resort, the system can be shut down by turning off the power to the CPU. This method is recommended only under emergency conditions because of its detrimental impact on system files and certain types of hard disk drives. These disk drives expect their floating heads to be parked prior to shutdown. Powering off the system could cause the heads to crash and cause irreparable damage to the disk.

Shutdown.— This command is the most often used method of initiating a orderly system shutdown. It is the safest, most considerate, and most thorough to initiate a halt, reboot, or return to single-user mode. The command will send messages to each user's terminal at progressively shorter intervals as the time for shutdown approaches. The messages tell the time of the shutdown.

Reboot.— This command terminates all currently executing processes except those essential to the system, then halts or reboots the system. When invoked without arguments, reboot syncs all disks before rebooting the system. The command does not send a message out to the users, unless you use the message option.

MONITOR

Some people would ask, "Why do I have to expend energy on monitoring the network when I could be doing something more productive, like file server or workstation maintenance?" There are several reasons why you should monitor your network:

- To maintain a history of the performance of your system. Studying this history could point out potential failures long before they occur.
- To provide a statistical basis for new equipment requests. Management is more likely to purchase new equipment if you can demonstrate that the current equipment will not meet the company's needs.
- To enable you to tune your network for optimum performance. This is especially true on larger networks with more than one file server. In some cases, you can provide a perceived increase in throughput by simply transferring tasks from one server to another.

Various network operating systems (NOSs) have their own utility programs to monitor what processing is taking place on their network. You can use these programs to monitor the status of your network, and some utilities give you the capability to monitor a particular job request.

REVIEW AUDIT LOGS

The main importance of reviewing audit/event logs is to monitor the security of the system. Besides, C2 Security compliance requires that the system be monitored (audited) continuously. Whether it pertains to the system – what hardware was accessed, security – identify who logged on (logged-in), or application – what software was accessed; usage must be tracked.

The term auditing refers to the process of recording events, such as file access, creations, deletions, the addition of print jobs, and so on, and using that information to detect usage violations or to confirm that network procedures are operating correctly.

A network administrator, by using the audit logs, can track what files were accessed, when they were accessed (date and time), by whom, and even what transactions were performed. Some logs even show you if the transaction was or was not successful with some type of message.

NETWORK CONFIGURATION

Equipment, the connections, and equipment settings for a network comprise the network configuration. The equipment refers to the hardware (computers, peripherals, boards, and cables), but may also include software under certain circumstances.

Because of equipment compatibility and interoperability, a system administrator needs to know considerable detail about all of the equipment that comprises the network. This information may include model numbers, memory specifications, enhancements, and so on. This information must be maintained, or conflicts between the equipment may occur. Most networking systems include a utility for recording system configuration information and updating it as the net work changes.

Record the current settings for each component as part of the configuration information. Avoid conflicts when deciding on specific settings. A conflict can arise because two boards want to use the same memory location or interrupt.

SYSTEM PARAMETERS

System parameters must be verified prior to installation and startup to avoid any conflicts. The majority of the conflicts involve system interrupts. An interrupt is a mechanism by which one computing element, such as a modem or a program, can get the attention of another elements. Interrupts may be generated by hardware or software.

Hardware Interrupt

There are 16 interrupt request lines (IRQs) for hardware interrupts in a PC environment. Each device attached to a computer can have an IRQ assigned. When the device wants service from the CPU, it signals on this line and waits.

IRQs have different priority levels, and the higher priority lines are assigned to the most important functions on the PC. By responding to IRQs according to their assigned priority, an operating system or interrupt handler can ensure that no vital activities are interrupted.

IRQ values for a device may be set through software or by manually setting them through the use of jumpers or DIP switches on the expansion board for the device. When configuring devices, it is important that you do not have two devices that use the same IRQ.

Software Interrupt

Executing programs also use interrupts to get resources needed to perform some action. There are software interrupts to access a monitor screen or disk drive, to handle a keystroke or a mouse click, and so on.

There are software interrupts for handling specific requests and for performing specific actions (for example, determining memory size). Interrupts can provide access to more functions (for example, DOS interrupt 2AH provides for network control functions).

SOFTWARE CONFIGURATIONS

All of the software that will be installed on the network will be configured for use on the system. Unfortunately, the manufacturers can't configure the software to function properly on each and every system. It will be up to you to make configuration changes to get the optimum performance from the specific software that will be loaded on the network.

These changes can include one or more of the following:

- Available memory
- Type of peripheral (e.g., disk or tape drives, printers, etc.)
- Number of users
- Access speeds
- Available disk space

Before making any changes to the software, ensure that there are adequate backups available to restore the system if problems are encountered. The most important thing to remember, when making changes, is to read the installation instructions that were supplied by the manufacturer first.

NETWORK PARAMETERS

If you think about the network, its performance is governed by both the hardware and software. The hardware has certain limitations that are set by the manufacturer and can't be changed. You can't speed up disk or memory access times, no matter what you do. The software, however, can be changed to help make the network run better.

Setting Parameters

Although the software is designed to run at the optimal rate, because each system is different there are some changes that can be made. Changes to these settings can allow the system to run even better, using all of its resources.

Some of these setting changes include:

- Adjusting memory partitions
- Drive/directory access
- Number of users

This is by no means a complete list of possible changes that can be made; refer to the operator's manual for your specific software for changes that can be made.

Modifying Parameters

The modification of the network parameters on your specific system will depend on the software being used. Each manufacturer sets up the software to run at optimal performance. There will be times that the network's performance falls off because of adding additional equipment, creating the need to change the parameters. When the parameters must be changed, always refer to the operator's manual for the specifics.

A number of parameters can be changed to improve the network's performance, including increasing the amount of memory used for disk sharing, print spooling, and printing. By increasing the buffer used for transferring files between the file server and workstations, the file server does not have to perform as many send operations and can perform other network procedures more quickly. By increasing the size of the buffer used for handling user requests, more user requests can be processed and the network can perform faster.

NETWORK PORT CONFIGURATION

A port is a connection on the back of the computer where you connect peripherals, switches, networks, or other devices. The port provides the electrical and physical interface between the device and the computer. There are two types of ports:

- **Parallel:** A hardware connection used to send or receive a lot of data over a short distance. These ports typically send eight bits of data simultaneously.
- **Serial:** A hardware connection that is used to send data one bit at a time and is very good for sending information over a long distance.

Port Address or Name

A port address is a bus or memory address that is associated with a particular hardware port. The port

will have at least enough storage allocated to handle the data being written or read at the port.

A port name can be used instead of an address to refer to a port. A name is normally easier to remember than an address. Operating systems sometimes have predefine names associated with certain ports. For example, DOS reserves COM1 and LPT1 to refer to the first serial and parallel ports, respectively.

ANALYZE CONFIGURATION

Analyzing the configuration of the network can be accomplished in two different ways. The first and simplest way happens when the computer is turned on; the operating system goes out and checks the configuration. The second way is accomplished by using an application to test whether a remote device is properly connected to the system. The use of an application is the best way to analyze the configuration.

The application tests the remote device by sending out a signal to each device and waiting for the signal to return. This process is called "pinging." The ping sent out is called an echo message, and the reply is called an echo reply message. The application sends out the echo message and, if the device is properly connected, it sends back an echo reply message. The receipt of this echo reply indicates that there is a viable connection. Some version of application software reports on how long it took to receive the echo reply and any lost replies. These reports provide information about the traffic and noise levels on the network.

SYSTEM RESOURCE LIMITS

The advantage of a network is it allows several people to share resources, both hardware and software. Hardware resources refer to printers, disk drives, CD-rom drives, scanners, and modems. Software resources include operating system, drivers, applications (word processing, database, etc.), management software, and data files. To avoid problems, such as slow response time and unavailability of resources, you must know the limits of the system resources.

Hardware Limits

The limitation involved with hardware is going to be waiting. A particular piece of peripheral equipment can be accessed by one user at a time. Only one job can be printed at a time, and only one user can be using a single modem at a time. This small inconvenience of access outweighs the cost of several different pieces of the same type (i.e., several printers or modems).

Software Limits

No matter which software package, whether application, mail, or operating system, there is a limited number of users that can use the software at one time. It is far cheaper to buy one multi-user package that allows for 25 users than to purchase 25 individual copies. But, it might run just a bit slower than an individual copy.

NETWORK SOFTWARE

Networks require the interaction of software and hardware. The system software to operate and control the network must be specifically designed for network operation. The application software/programs to solve user problems must also be specially designed to run on a network. Between the system software and the application software/programs, two pieces of software are needed. One is the telecommunications access software. It provides application programs access to the network so they can send and receive data. The other is the teleprocessing monitor, which is the interface between the telecommunications access software and the application programs. It handles the details of integrating these two. To install the system software, as with any software, follow the installation instructions supplied with the software.

SYSTEM SOFTWARE

It takes special system software to handle the unique and dynamic workloads of a network. This special software is called network system software. The network system software is sometimes referred to as the network operating system (NOS). It is different from the type of system software you normally use on your stand-alone PC. Network system software must be able to handle multiple users, multiple peripherals, network security, and be able to share information and application software, just to name a few differences. Normally, network system software runs on the network server. It includes such things as the network's operating system software, communications software, and all the programs needed to manage the sharing of information and resources on the network. Without it, there would be no way to coordinate and manage the many components of a network into a functioning whole.

Network system software provides multitasking capabilities. If the network is to serve multiple users at the same time, then the server must be able to perform tasks so fast they appear to be processed

simultaneously. An example of multitasking is to have the network server transfer a message (using a program called E-mail) from one PC to another, save a 50-page document to hard disk, and send a report to a printer, in rapid succession. Only systems with multiple processors, such as a system with two 386 or 486 microprocessors, can process information simultaneously.

Network system software provides **utility programs,** such as electronic mail (or e-mail). E-mail gives network users the ability to send messages to one another over the network. If for some reason you needed to send a message to all the network users, E-mail is capable of sending your message to multiple users. Other utility programs sort, merge, and print files.

Network system software also provides **data protection.** This includes data security/integrity and backing up of files. Data security is a must if you are to limit access to sensitive and classified information. Data integrity prevents files from being updated by more than one user at a time. There are a number of ways you can control access to information on the network. One way is to divide the shared hard disk into several different sections, similar to making logical partitions. Once the different areas have been established, you can specify how the user can access them. Generally, the different levels of access can be designated for either private, shared, or public use. They are defined as follows:

- **PRIVATE USE** Only one user is allowed to access and make changes to the data in this area. For example, all of PO1 Smith's work is located in the area \SMITH. Only PO1 Smith has access to this area, and only she can make changes.

- **SHARED USE** All users are allowed to access and make changes to the data in this area. For example, a shared area called \ADMIN could contain correspondence that can be updated by all the command's Yeomen.

- **PUBLIC USE** All users are allowed to access this area; however, they cannot make any changes to the data. For example, the area called \DIRECTIV contains all command directives. You would want your users to be able to view the data but not be able to make any changes.

Security and data protection are provided by **identification** and **password security.** When the users log on the system, they must enter their correct identification numbers along with their passwords (as a double check) to gain access to information. Another reason why data must be made secure is to prevent unintentional damage that can result when more than one user accesses and changes the same information at the same time. In a case such as this, neither user would know what the other had done, and the result would be corrupted data. To prevent this, network software often provides you with some type of **locking capability.** This locking feature prevents others from accessing the file or record when you are working on it.

To ensure a well-managed (network), the data must not only be secure, it must also be backed upon a regular basis. Files must be backed up if all the information on the network server's hard disk is to be saved in the event of a hard disk failure, a sudden power surge, or loss of power. Tape backup systems are very effective in that not only the tapes but also the tape units themselves can be stored off-site, which provides for additional security.

APPLICATION SOFTWARE

In addition to network system software, users of (network) require **application software** to carry out their specific requirements. You are familiar with many of the application software functions/packages available. They include word processing programs, database management programs, spreadsheet programs, computer aided design (CAD) programs, tutorials, and so on. Application software shared on a network is different from the software you use on your individual or stand-alone PC. It is specially designed to work on a network—to handle the demands of many users and to share resources while serving many users. It can also provide data security features, such as file or record locking and password recognition. Because network versions of application software are designed to be used by many users, a network software license agreement often costs more than a standard license.

Before leaving this section, you need to know a few other things about network software. Network system software features often vary from one network system to another. The system software can also dictate what hardware components **CAN** and **CANNOT** be used, and how the network **CAN** or **CANNOT** be configured.

SOFTWARE INSTALLATION

Before installing software on an individual's PC or on the network server, you will need to know the minimum system/hardware requirements for that

software. You will normally find this information on the side of the box and sometimes even on the back of the box the software comes in. The following requirements and recommendations will normally be listed:

Type of processor	
Required:	Recommended:
Personal or multimedia computer using 386 processor	Personal or multimedia computer using 486 or higher processor
Type or version of operating system.	
Windows 3.11®	Windows 95®
Amount of available memory required	
8 MB of memory to run applications individually	12 MB of memory to run additional applications simultaneously
Amount of available hard-disk space required	
89 MB minimum (typical)	126 MB maximum (complete)
Minimum (typical) is only the portion of the application that is needed to run the application.	
Maximum (complete) is when the entire application is loaded onto the PC.	
Video adapter	
VGA or higher-resolution	Super VGA, 256-color

Any other system/hardware requirements that may be needed will also be listed. As an example, these requirements might include: one CD-ROM drive; microphone, for voice annotation feature; a mouse or compatible pointing device; 2400 or higher baud modem (9600 baud modem recommended); headphones or speakers; and type of messaging software required to use e-mail; etc.

Once you have determined all of the above information, you will need to determine whether it will be run on a network as shared. Before you install the software, you need to read the installation instructions that come with the software application in their entirety. It is strongly suggested that you read a file normally called the "READ. ME" file, because that is where you will find the most up-to-date information (changes) that have been made to the application.

SOFTWARE TESTING

Once the software is installed on the network, it must be tested. The reason for the testing is to make sure that all aspects of the program work. There are two avenues for testing the software: an independent testing company, and end-users.

The advantage of an independent testing company is that it will use a more comprehensive and systematic testing method. Testing aimed at the generic network user is the disadvantage of the testing company.

Using end-users has both advantages and disadvantages when it comes to testing the software. An advantage is that the end-users will test all facets of the software. A disadvantage is the haphazard methods of most end-users when it comes to testing the software.

SYSTEM RESTORATION

The network is the most error-prone of the system components. Usually, multiple vendors are involved, and too few qualified personnel are available to support all the implemented networks. Due to these inherent problems with the network, system degradation is a part of operation, and getting the system back into normal operation is of great importance.

Three primary methods are used to provide service restoration after system degradation. They are as follows:

- **Redundancy.** Redundancy refers to duplicate hardware and network facility segments that are available at all times. If the primary path fails, a secondary path can continue network operation.

- **Rerouting.** Rerouting is the transmission of information along alternative paths. The end-to-end transmission initially required is still obtained.

- **Reconfiguration.** Reconfiguration is the manual or automatic reconfiguration of equipment and/or lines to achieve the original end-to-end connections. Reconfiguration may be the most costly method in time because it requires knowledgeable personnel and the appropriate switching of equipment.

These three modes of operation are short-term solutions meant to keep information moving. A better solution is to correct the degraded or failed circuit and/or equipment so normal operation is restored.

NETWORK DESIGN

The first step in designing a network is to decide whether or not a network is needed. This decision is made easier by soliciting network requests from the command. Once the decision is made to design and install a network, you need to look at the capacity and reliability of the network and the design options.

Many design options are available for designing and building a LAN. Four interrelated factors contribute to this great flexibility. They are physical layout (topology), access method (protocol), physical connection (cabling), and networking operating system (NOS). There is one additional factor to be considered when designing a network, the need for security. This need for security is met by the implementation of a firewall.

NETWORK REQUESTS

Before committing the money to install a network, you need to research the need for a network for the command. The best way to conduct this research is by using a network request. Always make sure you have all the available information to guide your planning. The following are some guidelines to use when beginning to plan for a network:

- Calculate your needs as completely as possible. This will help you decide what components and services will need to be included in the network.
- Determine what resources are available at your command for planning, implementing, and running a network.
- Determine who needs access to the network and where these people are located. This information will help determine whether a network is a necessary or feasible solution for the command's needs. It will also provide information regarding cabling requirements.
- Get to know the current usage and needs in detail. This information will also help decide whether a network is the best solution.
- Get a detailed drawing of office locations, existing wiring, and possible server locations.

After gathering and evaluating the information, the decision can be made as to whether or not a network is the way to go. If it is decided to go with a network, it is time to determine what resources are available.

CALCULATING NETWORK CAPACITY

After you've determined the available resources, use only a portion of these for your working calculations. This downsizing will protect you against the losses of these resources.

The amount by which you should decrease your estimates depends on the possible costs if your network is a failure and on how stable the resources are. A general rule to follow is to assume that your available resources will be anywhere from 10 to 50 percent less than estimated. Let's say, that you have 25 PC workstations available to connect to the network. You should plan on connecting 22 (12% less than available), which would leave you with 3 spare workstations. Another example would be: if your NOS is capable of having 250 accounts, reducing this quanity by 10% (25) will help reduce the time that the users will be waiting for the network to respond to their request.

The opposite of this rule is applied when it comes to the cost calculations. When you decide how much time and money it is going to cost, it is a good idea to add an amount or a percentage to the calculations. Projects like networks never seem to be completed on time or at cost, due to unforeseen circumstances.

LAN CONFIGURATIONS (TOPOLOGIES)

The physical arrangement of a LAN's components is called its configuration or topology. The three major types of LAN configurations, or topologies, are the **star,** the **bus,** and the **ring.** You can also create hybrid topologies by combining features of these configurations. For example, several bus networks can be joined together to form a ring of buses.

Each topology requires LAN components to be connected in a different arrangement. These components are also referred to as nodes. Remember, a node is any point on a network where data can be sent (transmitted) or received—a workstation, server, and so on.

The Star Network

In a star network, each component is connected directly to the central computer or network server, as

shown in figure 1-2. Only one cable is required from the central computer to each PC's network interface card to tie that workstation to the LAN. The star is one of the earliest types of network topologies. It uses the same approach to sending and receiving messages as our phone system. Just as a telephone call from one person to another is handled by a central switching station, all messages must go through the central computer or network server that controls the flow of data. You can easily add new workstations to the network without interrupting other nodes. This is one of the advantages of the star topology.

Another advantage of star topology is that the network administrator can give selected nodes a higher priority status than others. The central computer looks for signals from these higher priority workstations before recognizing other nodes. Also, the star topology permits centralized diagnostics (troubleshooting) of all functions. It can do this because all messages must first go through the central computer. This can prove invaluable for ensuring network security has not been breached. So much for the good news; now for the bad news, or the disadvantages of the star network. Of all the topologies, the star is the least reliable because it has a single point of failure. The network relies mainly on the central computer for all functions. If it fails, all nodes also stop functioning, resulting in failure of the entire network. This is precisely the same weakness multi-user computer systems have that rely on a central processor.

The Bus Network

The bus topology is like a data highway. That is, all components or nodes are connected to the same cable, and the far ends of this cable never meet (see figure 1-3). Bus LANs are best suited to applications involving relatively low usage of the bus coupled with the need to pass relatively short messages from one node to another. In many such networks, the workstations check whether a message is coming down the highway before sending their messages. Since all nodes share the bus, all messages must pass through the other workstations on the way to their destinations. Each node checks the address attached to the message to see if it matches its own address. Bus topologies allow individual nodes to be out of service or to be moved to new locations without disrupting service to the remaining nodes.

Unlike the star topology, where dozens of cables come together at the central computer causing logistical problems, bus cabling is simple. The bus topology is very reliable, because if any node on the bus network fails, the bus itself is **NOT** affected, and the remaining nodes can continue to operate without interruption. Many of the low-cost LANs use a bus topology and twisted-pair wire cabling.

A disadvantage of the bus topology is that generally there must be a minimum distance between workstations to avoid signal interference. Another disadvantage is that nodes must contend with each other for the use of the bus. Simultaneous transmissions by more than one node are **NOT** permitted. This problem, however, can be solved by using one of several types of systems designed to control access to the bus. They are collision detection, collision avoidance, and token passing, which we will discuss shortly. Also, there is no easy way for the network administrator to run diagnostics on the entire network. Finally, the bus network can be easily compromised by an unauthorized network user, since all messages are sent along a common data highway. For this reason, it is difficult to maintain network security.

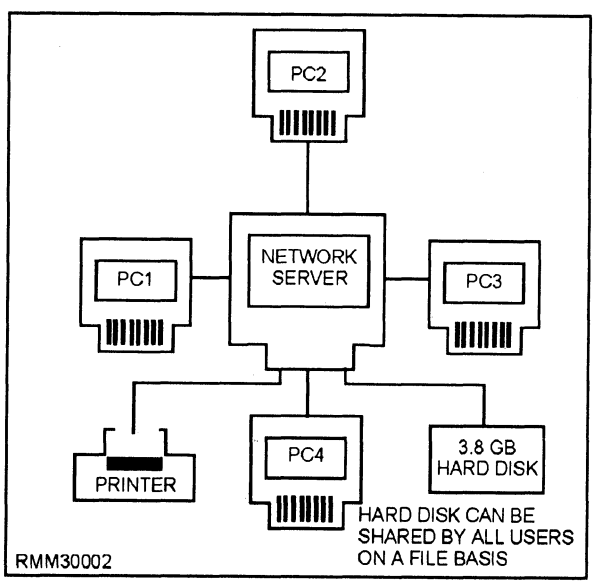

Figure 1-2.—A star network topology.

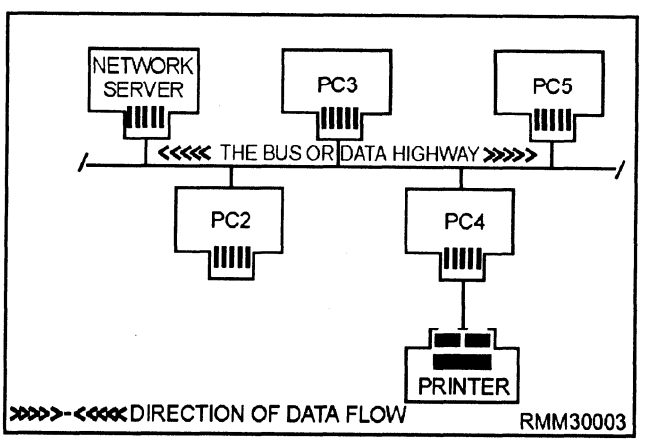

Figure 1-3.—A bus network topology.

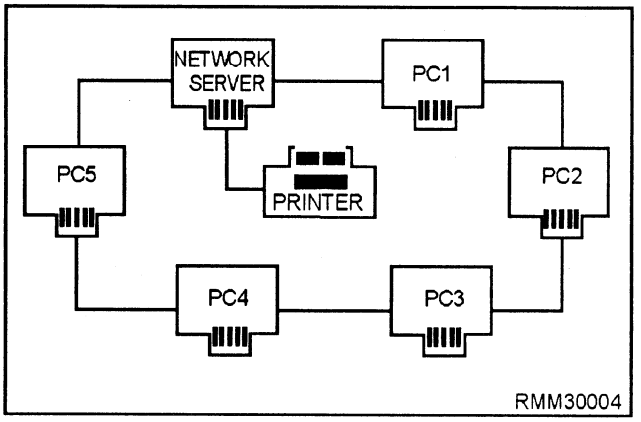

Figure 1-4.—A ring network topology.

The Ring Network

In a ring network, all of the components or nodes are connected to the main cable, and the cable forms a ring, as shown in figure 1-4. This topology allows a node to send a message to another node on the ring. However, the message must be transmitted through each node until it reaches its destination. Messages proceed from node to node in one direction only. Should anode fail on the network, data can no longer be passed around the ring unless the failed node is either physically or electronically bypassed. Using bypass software, the network can withstand the failure of a workstation by bypassing it and still be able to maintain the network's integrity. One of the major issues in a ring topology is the need for ensuring all workstations have equal access to the network.

One of the major disadvantages of ring topologies is the extreme difficulty of adding new workstations while the network is in operation. Normally, the entire network has to be brought down while a new node is added and cabling reattached. However, this particular problem can be overcome by initially setting up the network with additional connectors. These connectors enable you to add or remove nodes while the network remains intact and in operation. The addition of the connectors is accomplished with the addition of a multistation access unit (MAU). The MAU is a wiring concentrator which allows workstations to be either inserted or bypassed on the ring.

The Distributed Star (Tree) Network

The distributed star or tree topology (figure 1 -5) can provide many of the advantages of the bus and the star topologies. It connects workstations to a central point, called a hub. This hub can support several workstations or hubs which, in turn, can support other workstations. Distributed star topologies can be easily adapted to the physical arrangement of the facility site. If the site has a high concentration of workstations in a given area, the system can be configured to more closely resemble a

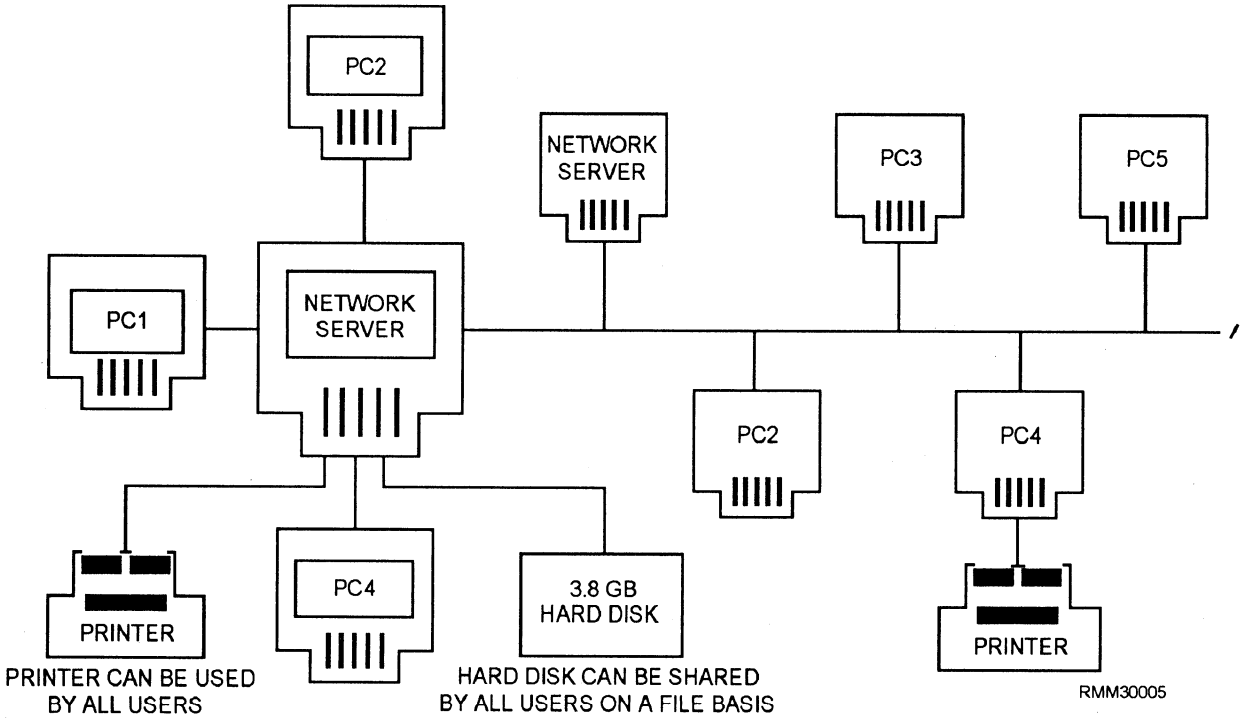

Figure 1-5.—A distributed star (tree) network topology.

star topology. If the workstations are widely dispersed, the system can use inexpensive hubs with long runs of shared cable between hubs, similar to the bus topology.

PROTOCOLS

Network protocols are an important component; they define how networks establish communications between elements, exchange information, and terminate communications. Protocols have two major operational functions. They establish the circuit for transmission (handshaking) and for the transmission itself. Transmission is conducted subject to the line dicipline. The line discipline is the sequence of operations that actually transmits and receives the data, handles the error-control procedures, handles the sequencing of message blocks, and provides for validation for information received correctly.

Two representative protocols, which control line dicipline, are: the Binary Synchronous Communications Protocol (Bisync) and the Synchronous Data Link Control (SDLC).

- **Bisync** is a half-duplex protocol that transmits strings of characters at lower speeds over dial-up circuits. Information movement is one direction at a time, with each data transfer being answered by an acknowledgement.

- **SDLC** is a control procedure that sends multiple blocks of data and returns a single acknowledgement for many blocks, thereby increasing the amount of time spent transmitting data. The bits that are put before and after the message at the transmitting end are removed at the receiving end, so only the message is presented to the user.

The hardware chosen for the network plays apart in the choice of network protocol. Most users and many of the vendors that build clone-type equipment would like to see universal interfaces. Others feel that the availability of different specifications will lead to a proprietary set of equipment, even though they favor the overall IS0 specifications (which are covered later in this chapter).

ACCESS METHODS

Another decision to be made is which access method to use. Access methods are the arrangements used to ensure that each workstation has fair and equal access to the network. The access method that will be used is governed primarily by the network's topology and protocol. The principal access methods are contention and token passing.

Contention

The contention method features Carrier Sense Multiple Access (CSMA) and Carrier Sense Multiple Access with Collision Detection (CSMA/CD). (See figure 1-6.) Access for both is on "a first-come, first-served basis. The CSMA scheme is very similar to a citizens band (CB) radio. Stations with data to send listen to the channel and wait until it is clear to transmit. With CSMA/CD, if two or more workstations transmit simultaneously, their messages will collide. As soon as a workstation detects a collision, it ceases transmission, monitors the network until it hears no other traffic, and then retransmits. Most contention networks assign a unique retry algorithm to vary the wait-and-retry period. This algorithm reduces the likelihood that after a collision, two workstations will transmit retries simultaneously.

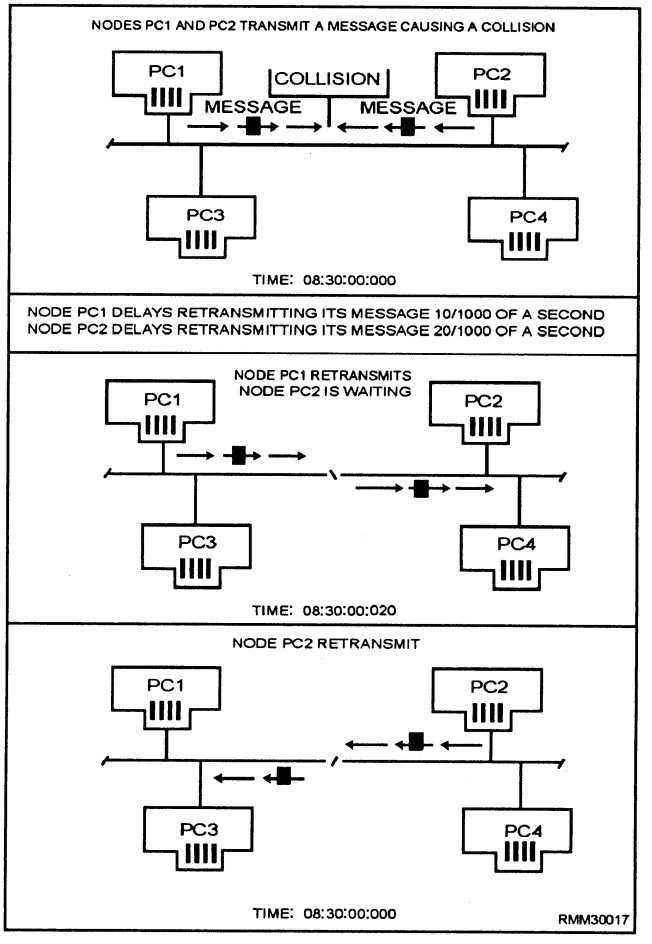

Figure 1-6.—A bus network using the CSMA/CD access method.

Token Passing

Token passing is an orderly access method (figure 1-7). Each workstation passes on the opportunity to transmit to its closest neighbor, until a station is found with a message to send. This permission to transmit is called a token. When a workstation with data to send is handed a token, part of the token is changed, indicating it is carrying a message, and then data is transmitted with the token. The token is then passed around the network, and every station checks to see if the message is intended for them. The receiving station copies the message from the token but then passes the unchanged token along the network. When the transmitting station receives the same token, it knows the message has been passed around the network. The transmitting station erases the message and puts the empty token back into circulation on the network. The amount of information that may be transmitted during possession of the token is limited so that all workstations can share the cable equally.

Network Standards

These access methods (CSMA/CD, CSMA/CA, and token passing) with their transmission medium (twisted-pair wire, coaxial cable, or fiber optic cable), are just one of several aspects (or levels) of an entire LAN structure. The topologies and network access methods just presented only establish a way to connect workstations or nodes together and how to pass along packets of data. These packets of data may be programs, data, system or personal messages, and so on. Above this hardware/software level are a number of other levels that are just as important in a LAN's design. These are the levels that define how the LAN system manages its resources, how a user like yourself is able to log onto another node's hard disk, how a common laser printer is used by all nodes, how one file is passed among many users, and so on. If order and discipline are to be maintained on the network, standards or protocols must be established and adhered to. This allows the LAN to function in an efficient and effective manner.

Over the past few years, a number of network standards or protocols have been developed by the International Standards Organization (ISO). They provide some level of uniformity among computer manufacturers and network vendors. ISO is one of several governing organizations in this field that has developed a series of protocols (rules to live by) to ensure compatibility for the many different vendors who design network hardware and software products. IS0 has defined a seven-layer architecture. These seven layers of standards, shown in figure 1-8, define a generalized architecture called the **Reference Model of open Systems Interconnection.** It is also known as the **OSI reference model** or **OSI model.** The primary purpose of the OSI model is to provide a basis for coordinating the development of standards that relate to the flexible interconnection of incompatible systems using data communications facilities.

The OSI model does **NOT** define any one vendor's particular network software as such, nor does it define detailed standards for any given software. It simply defines the broad categories of functions that each of the seven layers should perform. The OSI model can include different sets of standards at each layer that are appropriate for given situations. For example, in a very simple data communications system, one that uses a simple point-to-point link, the software at the higher-

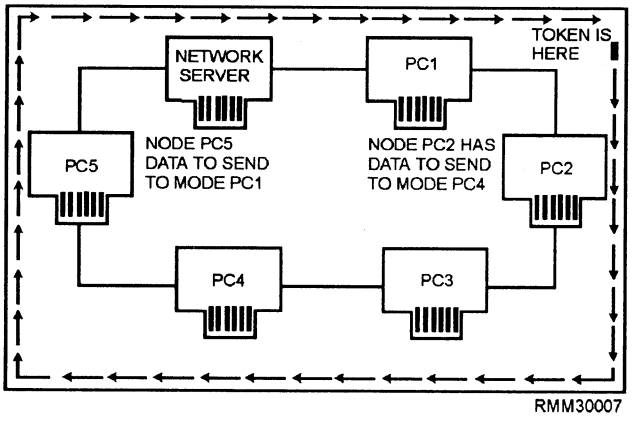

Figure 1-7.—A ring network using the token passing access method.

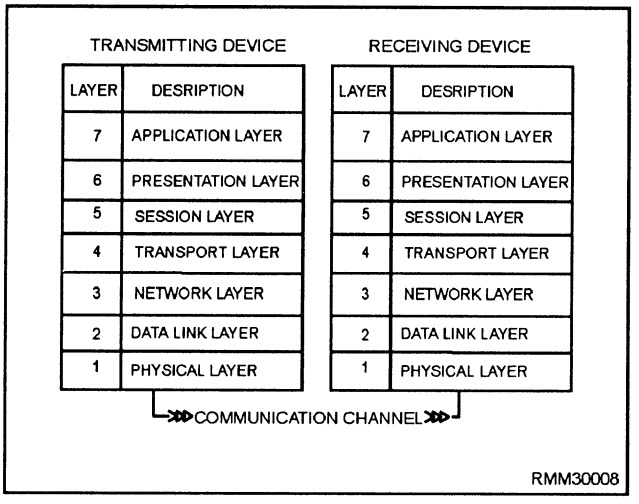

Figure 1-8.—The OSI model showing the seven software layers.

level layers (say 5, 6, and 7) might be very simple or possibly nonexistent. However, in a very complex data communications system, all seven software layers may be implemented. Although there is no requirement for any hardware or software vendor to adhere to the principles set forth in the OSI model, there is a worldwide trend in the computer industry toward acceptance and conformance to these standards.

About now, you may be asking yourself, what are these seven software layers (shown in figure 1-8), and why all the need for protocols? Don't all computers work in binary? Do they not all have operating systems? If a computer wants to communicate with another system, do you not simply connect them together using some type of cable? The answers to these questions are yes, yes, and yes; however, the commonalities seem to stop there.

Ideally, if the hardware, network software, application software, and cabling were all supplied by the same manufacturer, we would have relatively few problems to contend with when we design and implement a network. Everything would work together rather smoothly. However, a computer manufacturer's architecture can make it difficult to interconnect hardware offered by other competing manufacturers/vendors. The protocols used by communications devices are also highly complex and are often completely different from one manufacturer to another. Then, there is the network software. Network software from one LAN vendor usually won't work on a competitor's network, nor will the application programs. Even the cabling must be selected for a specific local-area network.

We could go on and on explaining the many incompatibilities that exist within these different areas, but the good news is that many hardware and software manufacturers/vendors provide interfaces. These various types of interfaces (bridges, gateways, routers, and so on) allow networks to be compatible with one another. At this point, we briefly talk about the seven software layers defined in the OSI model to give you some idea of what they are and why they are needed. To illustrate how the OSI model works, we are using the analogy of sending a letter using the U.S. postal system.

Layer l—The physical layer is concerned with the transmission of the unstructured raw bit stream over a physical meduim. It addresses the electrical, mechanical, and functional interface to the carrier. It is the physical layer that carries the signals for all the higher layers, as follows:

- Voltages and pulse encoding of bits
- Media and media interface (cables, connectors, NIC, and so on)
- Line discipline (full- or half-duplex)
- Pin assignments

In our mail analogy, the mail truck and the highway provide the services of the physical layer.

Layer 2—The data link layer provides error-free transmission of information over the physical medium. This allows the next higher layer to assume virtually error-free transmission over the link. The data link layer is responsible for getting data packaged and onto the network cable. It manages the flow of the data bit stream into and out of each network node, as follows:

- Creates and recognizes frame boundaries
- Checks received messages for integrity
- Manages channel access and flow control
- Ensures correct sequence of transmitted data

The data link layer detects, and when possible, corrects errors that occur in the physical layer without using the functions of the upper layers. It also provides flow-control techniques to ensure link-buffer capacity is not exceeded. In our analogy, the data link layer is concerned with sending the mail trucks onto the highway and making sure they arrive safely.

Layer 3—The network layer decides which physical pathway the data should take, based on network conditions, priorities of service, and other factors. Software on the network interface card must build the data packet so the network layer can recognize and route the data to the correct destination address. It relieves the upper layers of the need to know anything about the data transmission and switching technologies used to connect the systems. It is responsible for establishing, maintaining, and terminating connections across the intervening communications facility, as follows:

- Addresses messages
- Sets up the path between communicating nodes on possibly different networks
- Routes messages among networks
- Is concerned with the sequence delivery of data packets

- Controls congestion if too many packets are on the network
- Translates logical addresses or names into physical addresses
- Has accounting functions to count packets orbits sent by users to produce billing information

This layer acts in our postal service analogy, like the regional mail distribution centers throughout the country. The trucks are directed to the centers and are routed along the best path to their final destinations.

Layer 4—The transport layer ensures data units are delivered error-free, in sequence, with no losses or duplications. It relieves higher layer protocols from any concern with the transportation of data between them, as follows:

- Message segmentation—accepts data from the session layer, splits it up into smaller units, and passes the units down to the network layer
- Establishes and deletes host-to-host connections across the network
- Multiplexes several message streams onto one channel and keeps track of which message belongs to which connection
- Provides reliable end-to-end delivery with acknowledgment
- Provides end-to-end flow control and window management

The transport layer functions are provided by the mail truck dispatcher, who takes over if there is a wreck out in the system. If the network goes down, the transport layer software will look for alternate routes or perhaps save the transmitted data until the network connection is reestablished.

Layer 5—The session layer allows users on different machines to establish sessions between them. It performs the functions that enable two applications to communicate across the network, performing security, name recognition, logging, administration, and other similar functions. Unlike the network layer, this layer is dealing with the programs in each machine to establish conversations between them, as follows:

- Allows two applications processes on different machines to establish, use, and terminate a connection (or session)
- Performs synchronization between end-user tasks by placing checkpoints in the data stream so if the network fails, only the data after the last checkpoint has to be retransmitted
- Provides dialogue control (who speaks, when, how long, and so on)

The session layer in our postal agency recognizes different zip codes and reroutes letters.

Layer 6—The presentation layer formats data to be presented to the application layer. It can be viewed as the translator for the network. This layer provides a common representation for data that can be used between the application processes. The presentation layer relieves the applications from being concerned with data representation, providing syntax independence, as follows:

- Encodes data in a standard way (integers, floating point, ASCII, and so on)
- Provides data compression to reduce the number of bits that have to be transmitted
- Provides data encryption for privacy and authentication

This layer functions like a translator who translates a letter from French into English.

Layer 7—The application layer serves as the window for the application process to access the OSI environment. This layer represents the services that directly support users and application tasks. It contains a variety of commonly needed protocols for the following:

- Network virtual terminals
- File transfers
- Remote file access
- Electronic mail
- Network management

In our analogy, the application layer is the person who writes or reads the letter.

CABLING

A data communications network must have cabling to allow individual computers and other peripherals to talk to one another and share resources. And wouldn't it be easier if there were only one type available? There

would be fewer hassles when it came time to figure out such things as line speeds, line capacities, variations in line distortion, and so on. However, there area number of types, ranging in cost and capabilities. In the following paragraphs, we examine the advantages and disadvantages of twisted-wire pairs, baseband and broadband coaxial cabling, and fiber optic cabling.

Twisted-wire Pairs

Twisted-wire pairs, also known as twisted-pair wire or cable, is by far the least expensive transmission media. It consists of two insulated wires twisted around each other so that each wire faces the same amount of interference (noise) from the environment (see fig. 1-9). Unfortunately, this noise becomes part of the signal being transmitted. Twisting the wires together reduces but does not eliminate the noise.

Twisted-pair wire comes in a wide range of gauges and pairs. Wire has an American Wire Gauge (AWG) number based on its diameter. For network purposes, 22- and 24-gauge wires are the two most common types of twisted-pair media. Some local-area networks use the same inexpensive, unshielded twisted-pair cables telephone companies use. Others require a higher data grade quality. It's not uncommon to have several hundred pairs (and, in some cases, thousands) of wires placed in a single cable. Normally, each twisted-wire pair in a cable can accommodate a single phone call between two people or between hardware devices.

The advantages of using telephone wires are their relative low cost and their availability. Their disadvantages include susceptibility to signal distortion errors and the relatively low transmission rates they provide over long distances. Twisted wire can handle a data flow of up to approximately one megabit per second (Mbps) over several hundred feet. For a small local-area network with a limited number of users, twisted-pair is an ideal choice because it is both inexpensive and easy to install. A phenomenon called **crosstalk** exists in twisted-wire pairs whenever transmission occurs at a high rate of speed. Crosstalk is taking place whenever you can hear someone else's conversation in the background; say Mr. Frost telling Mrs. Christmas what a great recipe he has for southern fried chicken, or Mrs. Brush telling Mr. Smith what a large fish she caught in the Gulf of Mexico, while you're trying to carry on a conversation with your party. With voice communications this really isn't a problem; however, crosstalk can inhibit the high-speed transmission required for data communications.

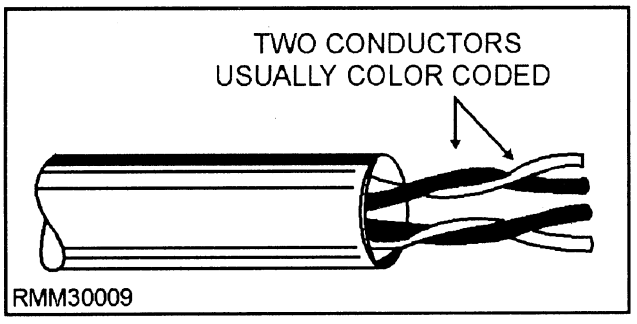

Figure 1-9.—Twisted-wire pairs (2 wire pairs shown).

Twisted-wire pairs used in data communications are either private or public lines. **Private lines** are those provided by the user. **Public lines** are those provided by a common carrier such as American Telephone and Telegraph (AT&T). Generally, public lines are used whenever distances are great or the terrain or other environmental factors prohibit the use of private lines. Public lines may be either switched lines or leased lines.

Switched lines are used whenever the amount of data to be transmitted is short in duration or when many locations must be contacted for relatively short periods of time. There is a drawback. The telephone company cannot guarantee you exactly which path or switching equipment such a connection will use. Therefore, the speed and quality of the switched connection are questionable.

Leased lines come into play when the connection time between locations A and B is long enough to cover the cost of leasing, or if higher speeds than those available with switched lines must be attained. Leased lines can also be conditioned by the telephone company to lower the error rate and increase transmission speeds. Conditioned leased lines typically operate at speeds of up to 64,000 bits per second (bps). Very-high-speed connections are also available from the common carrier. These are designated T1, T2, T3, and T4, and offer transmission rates of 1.5, 6.3, 46, and 281 million bits per second (Mbps), respectively.

Coaxial Cables

Coaxial (or coax) cable, the medium used by most cable television companies, was developed primarily because of the crosstalk in twisted-wire pairs when transmission occurs at a high rate of speed. While coax is more expensive than twisted-pair, it can transmit data significantly faster, over much longer distances, and with less electrical interference.

Coaxial cable is made up of one or two central data transmission wires composed of copper surrounded by

an insulating layer, a shielding layer, and a weather proof outer jacket, as shown in figure 1-10. It is almost as easy to install as twisted-pair, and is the preferred medium for many of the major local-area networks. Coaxial cable is used extensively in local-area networks whenever the distance involved is relatively short, generally less than 2 miles for baseband LANs and 10 miles for broadband LANs. It is used in both **baseband** and **broadband** networks. Wait a minute! You say you want to know what the terms *baseband* and *broadband* mean and how they relate to networks? Not to worry; we explain them to you a little later in the text, but for now, all you need to know is that they both deal with the way data is transmitted (in the form of electrical signals) through some type of medium.

Fiber Optic Cable

Fiber optic cable is to coaxial cable is to twisted-pair as the F-18 Hornet is to the Corvette is to the model T. It is the newest of the communication mediums, one that was spurred by the development of laser technology. Fiber optic cable (shown in fig. 1-11) consists of thousands of clear glass fiber strands, each approximately the thickness of a human hair. Transmission is made possible by the transformation of digital data into **modulated** light beams, which are sent through the cable by a laser light-emitting diode (LED) type device at incredibly fast speeds. Transmission rates available (as of 1990) range up to approximately 1 billion (or giga) bits per second (Gbps), with speeds over 2 Gbps possible. When thinking in terms of frequencies, light frequencies are extremely high. They are approximately 600,000 times that of the highest television channel. In terms of data communications, the higher the frequency of the signal, the more information it can carry. Put simply, every hairlike fiber within a fiberoptic cable has the capacity to carry many hundreds of local-area network channels simultaneously. When dealing with fiber optic cable, you will hear such terms as:

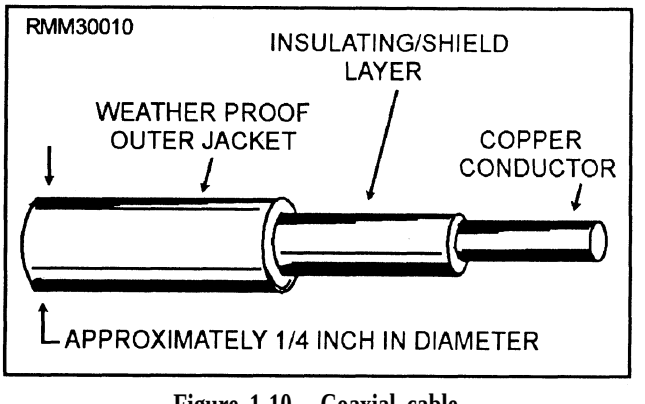

Figure 1-10.—Coaxial cable,

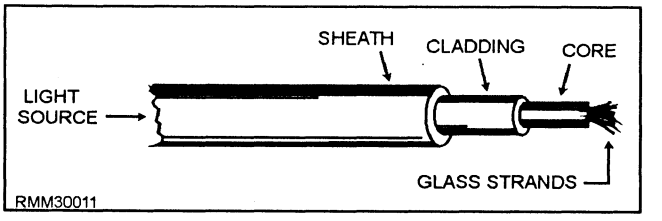

Figure 1-11.—Fiber optic cable.

- **Monomode—** Single fiber cable
- **Multimode—** Several fibers within a cable
- **Graded index—** A variation of multimode

Some of the major advantages of fiber optics over wire media include speed, size, weight, longevity, and resistance to tapping without being noticed. Since it carries no electrical current, it is immune to electrical interference of any kind, and there is no worry of it being a shock hazard.

One big disadvantage of fiber optic is the tighter restrictions on how much the cable can be bent. Other disadvantages include higher cost, and the inability to add on new workstations while other stations are active. Although it is relatively easy to splice the fiber optic cable and add new stations, the network or a portion of the network must be down while preparing the splice. On the other hand, if your activity has serious interference problems, or has a need for absolute network security, or the need to send signals several miles, then fiber optics might be the only solution.

Cable Selection

About now, you may be asking yourself, why all the fuss over transmission speeds? Why not just simply choose the cheapest transmission medium available and use it? It may not be the ideal situation, but it would get the job done, right? This is true; and with that in mind, we ask you this question. Would you put regular unleaded gasoline in your brand new car that happens to have a high-performance engine? The engine may not run as well as you would like, but it would get the job done, right? The same is true of transmission speeds and the different levels of speed within a computer system. To put it another way, the speed of transmission is very much related to the type of transmission medium used between stations in a network.

Most computer processing units (CPUs) are able to execute instructions and basic decision-making steps at a rate of several million instructions per second. Data can be transferred between the computer's memory and the cpu at these same rates of speed. The ideal network could keep up with the high speed of the cpu and be able to transfer data between the stations of the network at rates close to the rates that data is moved around within the cpu and memory. However, this is just not possible with a telephone line linked system, which is limited in the range of frequencies it can carry. When high-frequency signals are carried by wire such as twisted-pair, all sorts of electrical effects come into play. It's not sufficient to simply link computer systems with common wire. Considerable thought must be given to the electrical characteristics of the connection. The cable selection must be made during the design phase of the network to ensure that the decision is not left to be made during the installation of the network.

NETWORK OPERATING SYSTEM

A network operating system (NOS) is a software package that makes it possible to implement and control a network and enables users to use the resources and services on that network. A NOS's tasks include:

- Providing access to files and resources;
- Providing electronic mail (e-mail) services;
- Enabling nodes on the network to communicate with each other;
- Enabling processes on the network to communicate with each other;
- Responding to requests from applications and users on the network; and
- Mapping requests and paths to the appropriate places on the network.

A NOS may be server-based or peer-based. Server based NOSs are considerably more complex and powerful than NOSs for peer-to-peer networks. In a server-based network, the NOS and the server run the show, and the workstations will generally run a network shell. By contrast, in a peer-to-peer network any station can function as file server or as a client for network services.

Operating systems which have built-in networking capabilities include the following:

- UNIX®
- Windows NT®
- Novell® DOS 7

In most of these cases, the operating system's networking capabilities can be greatly enhanced through the use of utilities or other third-party programs. To learn more about these utilities or programs, check the manuals that come with the operating system.

FIREWALLS

Firewalls can be used for securing a local area network from a public network like the Internet. Firewalls are always a part of a much larger security plan. Choosing a firewall starts with a clear definition of the security goals. This includes decisions on what logging and alarms are needed, what authentication is acceptable and where security barriers are needed. Once the policy, philosophy, and service goals are defined, often only a few products on the market really fit these needs.

There are several types of firewalls that can be divided into packet filtering and application layer firewalls.

Packet Filters

Packet filters operate at a lower level than application layer firewalls. Packet filters decide whether to forward an IP packet based on the source or destination address found at the network layer. Routers typically implement this type of filtering, but since packets containing bogus IP addresses can easily be created, it's not too hard to gain access through even the most elaborate set of IP address filters. Although the router on an Internet link can filter packets, it probably wasn't designed to provide the level of control that a firewall product can. A router examines one packet at a time and forwards the packet.

Application Layer Firewall

Application layer firewalls, on the other hand, are designed specifically to control unwarranted access to your network. They can also deal with some of the trickier protocols. Application layer firewalls gain more insight into the data conversations that traverse an Internet link because they examine packets and protocols at and above the transport layer, which

controls the dialogue between communicating end nodes.

As an application gateway, the firewall typically behaves as a client on the Internet and appears as a server to users on its secure, protected side. When operating in this mode, the firewall will examine specific application protocols to decide whether connections are permissible. The range of supported application protocols varies from firewall to firewall, but most examine such popular ones as TELNET, the World Wide Web's HyperText Transfer Protocol (HTTP) or File Transfer Protocol (FTP).

Application layer firewalls offer greater protection against hacker attacks than the packet filtering firewalls. Besides providing stronger logging capabilities, many firewalls can also provide features like network address translation, authentication, and virtual private net works.

Choosing A Firewall

Once the decision is made to use firewall technology to implement an organization's security policy, the next step is to procure a firewall that provides the appropriate level of protection and is cost-effective. We cannot say what exact features a firewall should have to provide effective implementation of your policies, but we can suggest that, in general, a firewall should be able to do the following:

- Support a "deny all services except those specifically permitted" design policy, even if that is not the policy used.
- Support your security policy, not impose one.
- Accommodate new services and needs if the security policy of the organization changes.
- Contain advanced authentication measures or contain the hooks for installing advanced authentication measures.
- Employ filtering techniques to permit or deny services to specified host systems as needed.
- Use an IP filtering language that is flexible, user-friendly to program, and able to filter on as many attributes as possible, including source and destination IP address, protocol type, source and destination TCP/UDP port, and inbound and outbound interface.
- Use proxy services for services such as FTP and TELNET, so that advanced authentication measures can be employed and centralized at the firewall.

The firewall should contain the ability to concentrate and filter dial-in access. The firewall should contain mechanisms for logging traffic and suspicious activity, as well as mechanisms for log reduction so that logs are readable and understandable. If the firewall requires an operating system such as UNIX®, a secured version of the operating system should be part of the firewall, with other security tools as necessary to ensure firewall host integrity. The operating system should have all patches installed. The firewall should be developed in such a manner that its strength and correctness are verifiable. It should be simple in design so that it can be understood and maintained. The firewall and any corresponding operating system should be updated with patches and other bug fixes in a timely manner.

SUMMARY

In this chapter, we have covered some of the areas that need to be considered in the administration of a network. We have discussed network operations, the configuration of the network, network software, and network design. This is by no means all that will be required for administration, but it is a beginning.

CHAPTER 2

LAN HARDWARE

Upon completing this chapter, you should be able to do the following:

- *Explain how to install, inspect, and test network components.*
- *Describe how to make physical connections to networks.*
- *Explain the function of a network server.*

As noted in chapter 1, if the hardware, network software, application software, and cabling were all supplied by the same manufacturer, we would have relatively few problems to contend with when we design and implement a network. The answers to many hardware and software incompatibilities are found in the use of interfaces. These various types of interfaces (bridges, gateways, routers, and so on) allow networks to be compatible with one another.

NETWORK COMPONENTS

More and more, LANs are becoming part of larger networks. By connecting LANs together, any peripheral device, such as external hard disk, printer, or plotter can be shared by all users of the networks. This makes more efficient use of expensive peripherals. **Repeaters** can be used to amplify electrical signals; which, in turn, allows transmissions to travel greater distances. **Bridges** (also known as bridge servers) make it possible to interconnect like LANs; that is, two similar networks. **Routers** enable networks to communicate using the most efficient path. **Brouters** combine the functions of a bridge and a router. Gateways (also known as gateway servers) make it possible to interconnect unlike LANs; that is, two dissimilar networks.

INSTALL COMPONENTS

The installation of network components is dependent on the particular type of component, the manufacturer, and the type of cable being used. When it comes to installing one of these components, read the instructions that are supplied with the component to make sure that you install it properly.

Repeaters

Repeaters are used to amplify electrical signals carried by the network. They work at layer 1 of the OSI model—the physical layer. (The OSI model was covered in chapter 1.) The function of a repeater is to receive incoming signals (a packet of data), regenerate the signals to their original strength, and retransmit them. Repeaters are used to lengthen individual network segments to form a larger extended network. That is, repeaters allow a network to be constructed that exceeds the size limit of a single physical segment by allowing additional lengths of cable to be connected (see figure 2-l). There is a catch, however. For a repeater to be used, both network segments must be identical-same network protocols for all layers, same media access control method, and the same physical transmission technique. This means we could connect two segments that use the CSMA/CD access methods, or connect two segments that are running under the

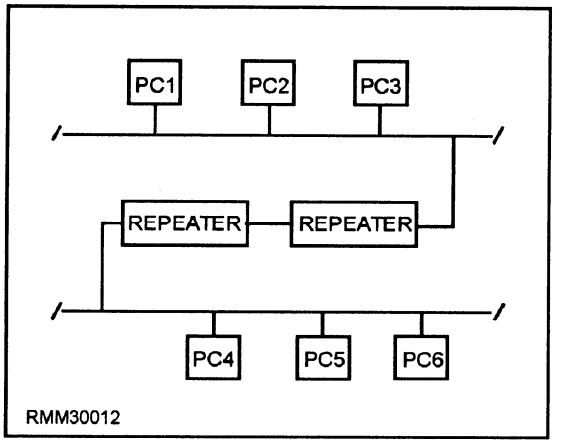

Figure 2-1.—Repeaters used to lengthen individual network segments.

token-passing access method. However, we cannot connect a CSMA/CD segment to a token-passing segment.

Bridges

Bridges handle the first two layers of the OSI model—the physical layer and the data link layer. Like repeaters, bridges connect physically-isolated networks to forma single logical network; however, a bridge has a little more intelligence and can provide some translation between dissimilar protocols. For example, our token-passing segment wants to communicate with our CSMA/CD segment. The bridge will "repackage" the message from the token-passing segment into a format that the CSMA/CD segment will understand. Then, the bridge will act as a workstation on the CSMA/CD segment and contend for access. The same thing happens in reverse. A message is sent from the CSMA/CD segment to the token-passing segment. The bridge then "repackages" the message into a format the token-passing segment is expecting and waits for the token, just like any other workstation. An important point to remember is that a bridge will pass on any message it receives. Because the bridge is not smart enough to know that unlike LANs do not understand each other, it will go ahead and send the message. Because the two LANs speak a different "language," the message will be ignored.

Routers

Routers only connect networks running similar access methods. They work at the third layer of the OSI model—the network layer. Like bridges and repeaters, routers can connect networks over different wiring media and topologies. However, unlike bridges, routers can intelligently determine the most efficient path to any destination, based on predetermined delimiters. Routers are often a better choice for interconnecting remote installations and congested networks requiring a single protocol. Let's look at this more closely.

Let's say we have a LAN made up of three token-passing segments, and each segment is connected via a bridge. For a message to go from LAN A to LAN C, it would have to travel through LAN A and LAN B before it reaches its final destination, which is LAN C. See figure 2-2, frame A. On a LAN that has large amounts of message traffic, we can see how a bridge may slow down the system. On the other hand, if the segments are separated by routers, the router on LAN A would look at the destination of the message and determine the direct route to LAN C that would be shortest route, as shown in figure 2-2, frame B.

Brouters

A brouter can work in either the second and third layers of the OSI model—the data link layer or the network layer. A brouter is a combination of a bridge and router combined. If it can't route a packet, it acts as a bridge. Brouters are particularly useful if you have two or more different networks. Working as a bridge, a brouter is protocol independent and can be used to filter local are a network traffic. Working as a router, a brouter is capable of routing packets across networks.

Gateways

Gateways work at OSI model layer 7—the application layer. A gateway functions to reconcile differences between two dissimilar networks. Messages are not only repackaged for transmission between different networks (CSMA/CD to token-passing), but the contents of the messages are converted into a format the destination can use and understand. Now our unlike LANs can talk to each other. Gateways can also provide links between microcomputer networks and mainframes.

A gateway is generally a dedicated computer with an interface card and at least some type of software for both of the environments being connected. The gateway then runs special software that provides the necessary conversion and translation services which, in turn, allow the two environments to communicate.

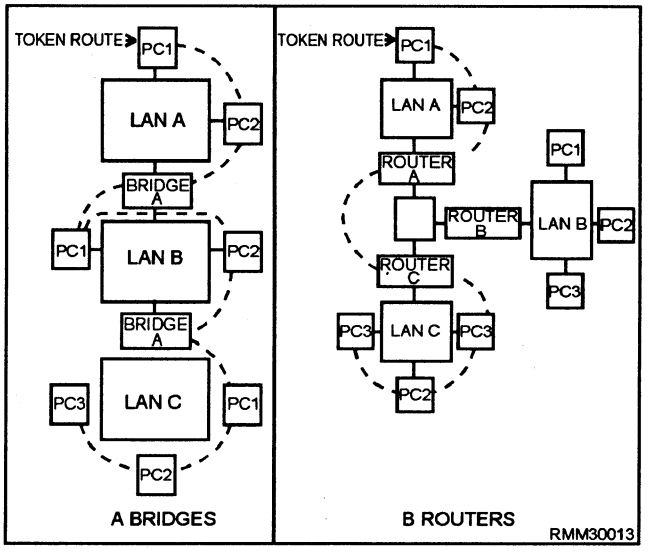

Figure 2-2.—Interconnecting LANS using (A) bridges and (B) routers.

Concentrators

The main function of a concentrator is to serve as a termination point for cable running from individual nodes in a network. The cable connects to the network or to another wire center.

A concentrator may have multiple boards or boxes mounted on a rack. Each board is essentially a hub, a wiring center for a single network's nodes. Such boards generally include light-emitting diodes (LEDs) to indicate the status of each port on the board.

Hubs

A hub is a box with a number of connectors to which multiple nodes (PCs) are attached. It serves as a common termination point that can relay signals along the appropriate paths. All hubs provide connectivity, and some even provide management capabilities. A hub usually connects nodes that have a common architecture. Although the boundary between concentrators and hubs is not always clear, hubs are generally simpler and cheaper than concentrators.

Modems

In module 2, we introduced you to modems and how they are used in a data communications environment. They translate data from digital to analog form at the sending end of the communications path and from analog to digital at the receiving end. From a conceptual standpoint, this explanation is sufficient. However, if you are going to install a modem, you need to know some of the technical aspects of modems.

MODEMS AT WORK.— Put simply, the object of a modem is to change the characteristics of a simple sine wave, referred to as a carrier signal. We know this carrier signal has several properties that can be altered to represent data. It has amplitude (height); it has frequency (a unit of time); and it has phase (a relative starting point). Modems are capable of altering one or more of these characteristics to represent data.

The job a modem performs can be divided into two discrete parts or phases at each end of the communications link. At the sending end, it converts digital bit streams (strings of 0's and 1's) into analog sine waves. This is the encoding process. Another component within the modem then changes (modulates) the analog signal so the data may be transmitted simultaneously with other data and voice traffic that has also been modulated. This process is basically reversed at the receiving end. There, the analog signal is brought back to its basic level (demodulated), and the analog sine waves are reconverted (decoded) back into their corresponding bit streams (see figure 2-3).

CODECs.— In today's digital communications lines, voice traffic is considered the outsider that digital data used to be to analog lines. Voice can enter the data communications lines only after being encoded into digital form. It then must be decoded to be audible again at the receiving end. The device used to perform the encoding and decoding functions is known as a codec. This is simply another black box conversion device that has always been in existence in a slightly different form as part of a modem.

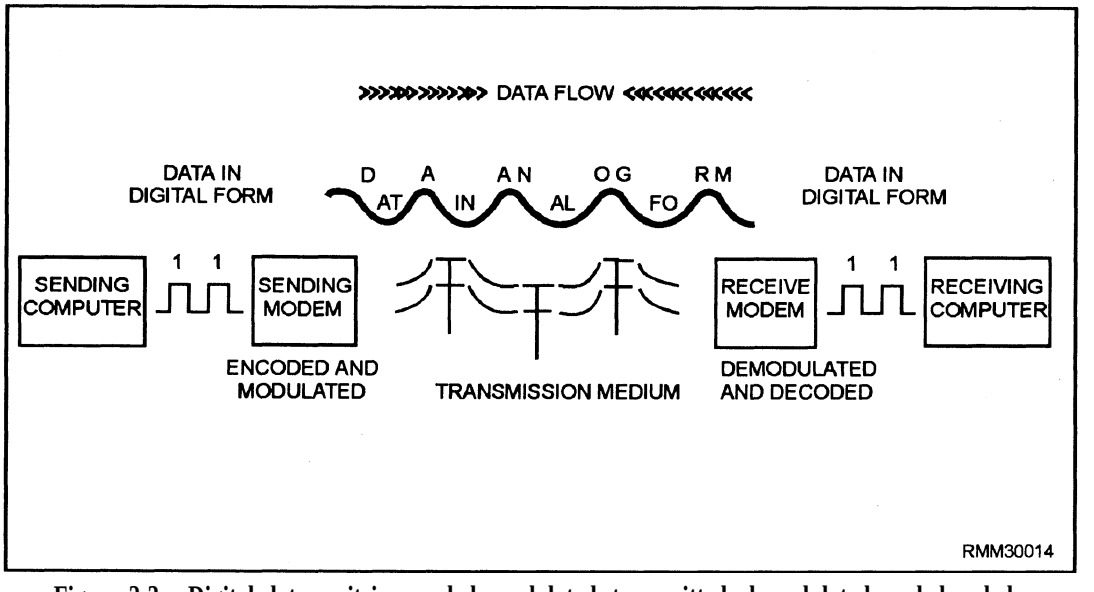

Figure 2-3.—Digital data as it is encoded, modulated, transmitted, demodulated, and decoded.

Network Interface Card and Cabling

To attach personal computers to the LAN, you must install a network interface card (NIC) into an empty expansion slot in the PC, install the appropriate software, and attach the network cable to the NIC. The other item you need to consider is what type of connector to use. But before deciding the type of connector to use, you need to know what type of cable and architecture you will be using. The cables may be twisted-pair cable, fiber optic cable, or coaxial cable.

- **Twisted-pair cable** The twisted-pair cable is easy to install and costs little on a per-foot basis. In some cases existing telephone cable may be used. Its disadvantages include limitations in capacity and speed. It is also susceptible to electrical interference unless it is shielded.

- **Fiber optic cable** Fiber optic cable is the best choice if a secure network is needed. Because the cable transmits light, the transmissions are immune to interference caused by electrical or electronic devices. Also, if your network will run through an area of heavy industrial activity or a work place with strong radio frequency interference, fiber optic cable is the most appropriate choice. Other advantages of the fiberoptic cable are that it lasts longer than other cable and can carry many more channels. Its disadvantages include its high price, poor connectivity, and low flexibility.

- **Coaxial cable** Coaxial cable, also called coax, networks have gained in popularity because of their use in cable television. The quantities of cable and connectors produced for cable television have greatly reduced the prices of these components for network users. Coaxial cable comes in various thicknesses and is designated by a number: RG-11, RG-58, RG-59, RG-62, etc. You can use either baseband or broadband transmission methods with coaxial cable.

Baseband coaxial systems, which transmit digital signals unchanged over a single channel, have several advantages. They are inexpensive, simple, easy to install, and have low maintenance. They also allow very high data transmission rates. One disadvantage is they are limited to transmitting digital signals only.

In contrast, **broadband coaxial systems** require the digital signal to be converted to an analog signal before transmission and then back to digital by modem at the receiving device. Broadband systems support data, voice, and video signals that may be transmitted simultaneously. Disadvantages of broadband systems are their higher installation costs and complex maintenance.

Connectors

The connector provides the physical link between two components. For example, a connector can link a cable and a NIC, a cable and a transceiver, or two cable segments.

Connectors differ in their shape, size, gender, connection mechanism, and function. These features influence and determine where a connector can be used. Where necessary, special adapters may be used for connections involving different connector combinations.

Connectors also differ in how sturdy they are, how easily and how often they can be attached and detached, and in how much signal loss there is at the connection point.

The type of connector needed in a particular situation depends on the components involved and, for networks, on the type of cable and architecture being used.

CONNECTOR FUNCTIONS.— A connector may be passing the signal along or absorbing it. A connector that passes a signal along may pass it unmodified or may clean and boost it. Connectors can serve a variety of purposes, including the following:

- Connect equal components, such as two segments of thin coaxial cable
- Connect almost equal components, such as thin to thick coaxial cable
- Connect unequal components, such as coaxial to twisted-pair cable
- Connect complementary components, such as a NIC to a network
- Terminate a segment

CONNECTOR SHAPES.— Specially shaped connectors are used for particular types of connections or for connections in particular locations. For example, a T-connector attaches a device to a cable segment; an elbow connector allows wiring to meet in a corner or at a wall.

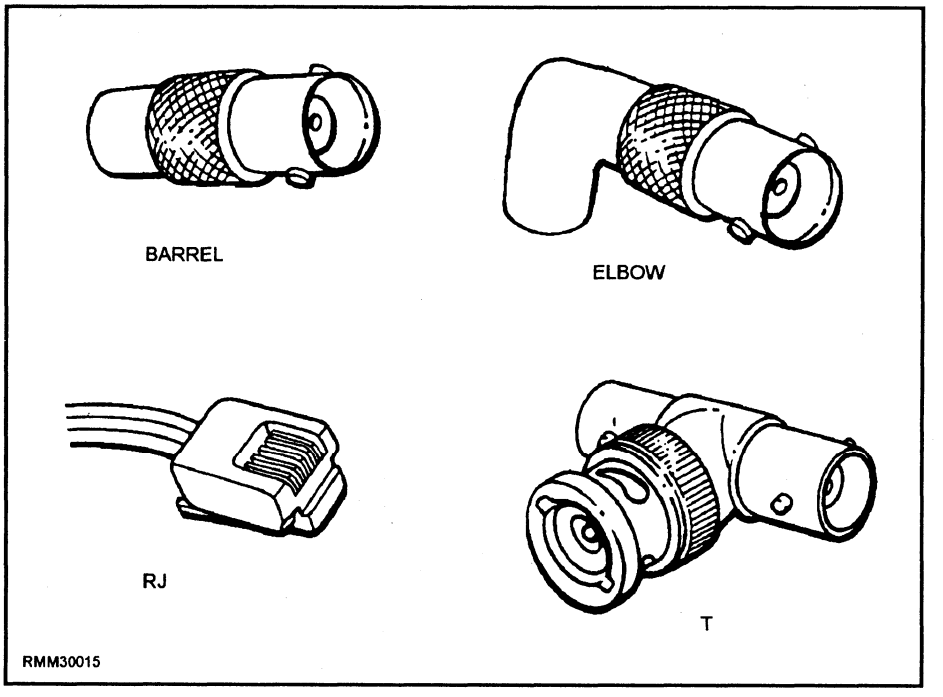

Figure 2-4.—Connector shapes.

Table 2-1.—Cable connector shapes.

SHAPE	DESCRIPTION
Barrel	Used to link two segments of cable in a straight run.
Elbow	Connector with a right-angle bend, used to connect two sections of cable in a corner or to accomplish a change of direction.
RJ	Used to connect telephones to the wall or modems.
T	Used to attach a device to a section of cable.

The connector shapes used in networking setups are listed in table 2-1. Figure 2-4 shows examples of connector shapes.

FIBER-OPTIC CONNECTORS.— Like electrical cable connectors, different types of fiber-optic connectors have different kinds of attachment mechanisms. The actual attachments between ferrule shells may be made by threading, snapping, or clicking. Table 2-2 lists the most commons types of fiber-optic connectors.

Table 2-2.—Fiber-optic connectors.

TYPE	CONNECTION METHOD	# OF MATINGS
ST (straight tip)	Barrel nut connector (BNC)	1000
SC (subscriber connector)	Pushbutton latch	1000
MIC (medium interface connector)	Pushbutton latch	1000
SMA	Threaded coupling	200

In addition to attachment mechanisms, fiber-optic connectors differ in the following ways:

- The size of the ferrule.
- Whether the connector can be keyed. This is the technique for making a connector asymmetrical, usually by adding a notch or plug, making it impossible to plug the connector in wrong.
- The number of matings the connectors can handle without producing unacceptable signal loss.

- Whether the fiber must be twisted to make the connection; multiple fibers cannot run through the same connector if it is to be twisted.

The connectors differ in the way the fiber is attached to the connector itself. You can either use epoxy to glue the fiber into the connector, or you can crimp the connector and the ferrule together using a special crimping tool.

CONNECTOR GENDERS.— Connector gender basically refers to whether a connector has plugs or sockets. The gender is important because the elements being connected must have complementary genders.

A male connector is known as a plug; the female connector is known as a jack. With a few exceptions, such as the IBM® data connectors and certain fiber-optic connectors, all connector types have distinct genders. Figure 2-5 shows examples of male and female connectors.

CONNECTOR MECHANISMS.— The connection mechanism defines how the physical contact is made to allow the signal to pass from one side of the connection to the other.

Connection mechanisms differ in how sturdy they are. For example, the pin-and-socket connection at a serial port can be wobbly without extra support from the screws on either side of the plug. On the other hand, fiber-optic connectors must be cut to precise proportions and must not allow any play in the connection.

INSPECTING COMPONENTS

The inspection of the components when they are received is limited to checking for any physical damage. This damage will include:

- Any damage to the packing material
- Damage to the case
- Hidden damage on the inside of the cabinet

The inspection that is conducted needs to be as thorough as possible, since any damage discovered must be reported to the supplier. This inspection also needs to be accomplished as soon as the equipment arrives, because the longer you wait, the less likely it becomes that the supplier will replace the equipment.

NETWORK TESTING

Network testing is changing significantly because of the growth of digital network capability. Testing in the voice network has always been considered as much of an art as a science because of the variable nature of the different impairments encountered. The digital net work has been designed with more diagnostic capability, making it much easier to identify and isolate problems. The testing is done in the carrier environment, not in the user environment.

Network Testing Methods

There are three basic approaches to network testing, as follows:

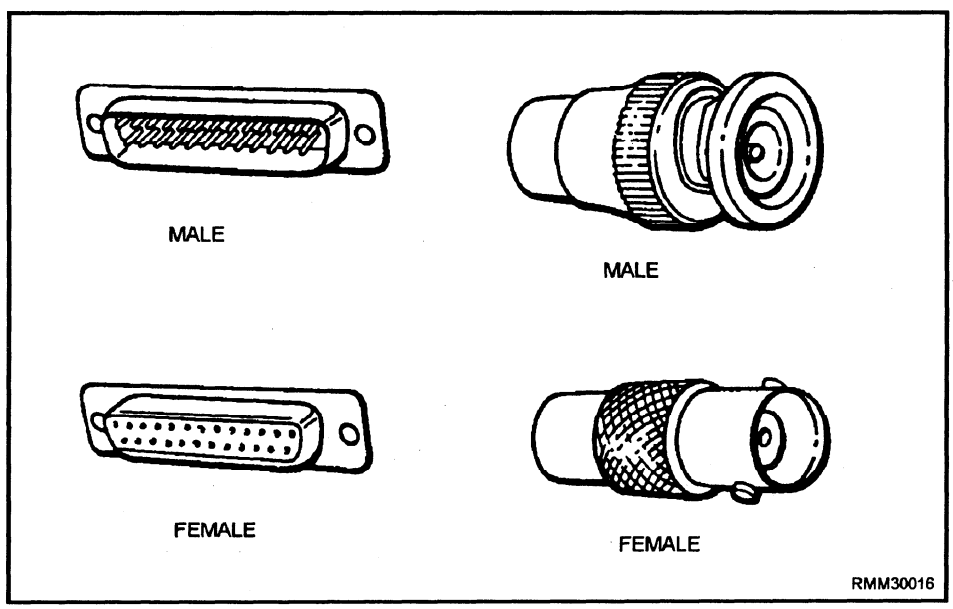

Figure 2-5.—Connector genders.

1. Rely on vendors. If you rely on a vendor for testing, you probably have a single vendor's products in your network and are, therefore, locked into that vendor. Fewer vendors today are capable of providing this complete capability.

2. Use an organization dedicated to network problem solving (third party). At one time, third-party problem solving was considered a viable alternative, but today the expertise needed is so vast and covers such a wide variety of products that it is not feasible to provide the service. The carrier providing the majority of your circuits is the best for handling your network management. However, it is difficult for the carrier to be objective, and it is usually not very cost effective.

3. Use in-house network management. In-house network control is by far the most flexible in design and operation. Network administrators typically understand their problems better than any carrier or vendor could. Network problems are not always the result of network conditions; they may actually be operational problems. A disadvantage of in-house network control is that it requires more resources, such as knowledgeable people, equipment, space, and all of the other support overhead.

Regardless of the testing method that is used, testing can be performed by both hardware tools and software programs.

Hardware Testing

The tools used are partly insurance and partly convenience devices. The greatest expense of a network comes when it is down or functioning incorrectly; it is important to be able to test components when things go wrong. Testing should also be accomplished before installing, to ensure that you do not install a faulty component. After they are installed, test components periodically to make sure they are functioning properly. Special tool are available for this purpose.

Network testers can be very expensive, while convenience tools, such as wire crimpers and voltmeters, are quite inexpensive. The amount that is spent on tools will depend on the size of the network, the importance of the network's contents, and who will be doing the maintenance on the network.

The following are several types of hardware tools:

- Manufacturing tools for creating individual components, such as crimpers and dies for attaching wires to connectors.
- Construction tools for assembling and disassembling systems; for example, screwdrivers, pliers, chip removers, and chip installers.
- Testing tools for testing individual components or for monitoring the performance of a component or system, such as voltmeters, ammeters, and line scanners.
- Safety tools for making sure components are protected against damage from electrical and other dangers; for example, static cords, electrical mats, and shorting probes.

BASIC TOOLS.— The level and range of tools you will need depends on the level of your involvement with the network. Regardless of the level, a few basic tools will almost certainly make your life easier:

- Screwdrivers, for opening machines, installing and removing expansion cards, and for attaching connectors;
- Pliers, for grasping objects;
- Wrenches or nut drivers, for tightening and loosening nuts;
- Chip removers/installers, for removing and installing computer chips; and
- Tweezers, for retrieving small parts and screws.

In addition to these tools, some people might also have wire strippers, cutters, and soldering irons that can be used to set up special-purpose circuits or wiring connectors.

If you are going to do any troubleshooting at all, you will need a voltmeter or ammeter (probably both), with an operator's manual, to test the electrical activity. Use of the manual is essential to connect the meter properly; connecting the meter wrong can cause serious damage to sensitive circuitry.

TOOLS FOR INSTALLING AND ATTACHING CABLE.— The tools used in making cables are specialized tools. They are used to attach the connectors onto the cable and then to test the cable. It is advisable to get the cables pre-made to the desired length by the manufacturer. Unfortunately, that isn't always possible.

To attach connectors to cable, you need the following tools:

- a crimping tool, for pressing the cable and connector together, and
- a die for the specified cable/connection pair, to make sure cable and connector fit properly.

Installation tool kits that include the crimping tool, die, cable, connectors, and cable ties can be purchased from manufacturers. These kits range in price from one or two hundred to several thousand dollars.

TOOLS FOR TESTING CABLES.— Voltmeters and ammeters provide readings of voltage and current, or amperage by tapping into the circuit and recording the electrical activity as it occurs. These recorded values may or may not provide the details about what is happening along the lines of the network.

Scanners are much more sophisticated testing tools. Some of the capabilities of scanners include the following:

- Check for faults in a cable.
- Test a cable's compliance with network architectures.
- Monitor performance and electrical activity, given the type of cable and architecture involved.
- Test the cable's wiring sequence.
- Generate and print a summary of the information obtained from the tests.

A powerful scanner can test for cable quality, for the quality of the connections between cable segments, or between cable and device. A less poweful scanner will be able to test for noise, crosstalk, signal attenuation, resistance, cable length, and so on.

Software Testing

Diagnostic software can be used to help anticipate or catch problems early and to help deal with the problems once they have arisen. Network versions of diagnostic software may be expensive, but they can save the system under some circumstances. For example, virus detection software can save hours of reconstruction and reloading the system. Using software to test the hard disk can identify bad disk sectors before data can be written to them and move any data from bad sectors to a safe location.

Another use of diagnostic software is performance monitoring and analysis, which involves tracking the networks behavior. This will help to identify inefficiencies and bottlenecks, so they can be elimated. While monitoring the system's performance, keep careful track of the following:

- Operating costs
- Threats to security
- User satisfaction
- User productivity

Track these areas especially during the first few weeks after the network is installed. Do not be surprised if some of these measured indicators change drastically during this period. For example, costs may drop drastically after the startup period, while user satisfaction and productivity may rise after the initial problems are resolved.

NETWORK PHYSICAL CONNECTIONS

A network connection is a linkage between network elements. Physical connections concern the cables and connectors used to create the physical layout of the network. When building a network, you must first establish the physical connections.

NETWORK BACKBONES

Backbone cable refers to the cable that forms the main trunk, or backbone, of a network. Individual nodes and other devices may be connected to this cable using special adapters and a separate stretch of cable.

Backbone cable is defined by the Electronics Industries Association/Telecommunications Industry Association-568 (EIA/TIA-568) committee as any "behind the scenes" cable; that is, cable running behind walls, in shafts, or under the ground.

The EIA/TIA-568 recognizes four types of backbone cable; they are listed in table 2-3.

The use of a backbone network to tie together a number of small access networks offers several advantages over the construction of a single large LAN. The various LANs connected to the backbone are able to operate in parallel, providing greater processing efficiency. The multiple-network approach is also more reliable, since each individual LAN can continue operating if one of the access networks, or even the backbone, fails. The backbone network must also be highly reliable, since the greater distances covered may make it difficult to locate and repair faults. The LANs that connect to the backbone must be flexible and low-cost in terms of installation and user connection.

Table 2-3.—Types of backbone cable.

Cable Type	Main	Optional
UTP	100-ohm, multipair UTP cable, to be used for voice grade communications only	
STP	150-ohm STP cable	100-ohm STP cable
Coaxial	50-ohm thick coaxial cable	75-ohm (broadband) coaxial cable
Optical Fiber	6.26/125-micron (step- or graded-index) multimode optical fiber	single-mode optical fiber

Connection to the backbone network may require a bridge, router, gateway, concentrator or hub, depending on the architectures of the various LANs and the backbone itself. The connectors used will also depend on the type of cable used for the backbone. If the backbone is coaxial cable, you would use a T-connector and barrel connectors to make the connection to another cable or a hardware device.

The backbone manages the bulk of the traffic, and it may connect several different locations, buildings, and even smaller networks. The backbone often uses a higher-speed protocol than the individual local area network (LAN) segments.

One obstacle to a successful backbone network is the high bandwidth that may be required to handle potentially heavy traffic. Because of this consideration, fiber-optic cable is the most sensible cabling for backbone networks.

NODES

The computers, or nodes, in a network may be used for workstations, servers, or both. PCs need a network interface card (NIC) installed for networking capabilities.

The NICs mediate between the computer and the network by doing the necessary processing and translation to enable users to send or receive commands and data over the network. NICs are designed to support a particular network architecture, such as Ethernet® or ARCnet®.

To connect a node directly to a backbone, you would use a drop cable for the connection. Nodes are normally connected to the backbone indirectly through a concentrator or a hub rather than with a drop cable.

The elements needed to connect a node to a network include the following:

- Cable: twisted-pair, coaxial, or fiber-optic
- Wiring centers: hubs or concentrators
- Intranetwork links: connectors, repeaters, and so on
- Internetwork links: bridges, routers, gateways, and so on

The cable provides a transmission medium, as well as the physical link between the nodes on the network. Connectors and repeaters attach cable sections to each other; connectors and transceivers attach NICs to a cable and, thereby, to the network. Transceivers enable different types of cable to be attached to each other. Terminators absorb a transmission at the end of a network, preventing the signal from traveling back in the other direction on the network. The types of intranetwork links allowed in the network depend on the type of cable used and on the network topology used.

Wiring centers serve as a focal point for network elements, and may influence the logical arrangement of nodes on the network.

Internetwork links may be bridges, routers, gateways, and soon. Such components serve to connect networks to each other. The type of internetwork link depends on whether the two networks are the same or not, and the amount of translation that is needed.

NETWORK SERVER

A server is the central computer in a network, and is responsible for managing the network. The server provides some type of network service. It may be hardware, such as a file server, or software, such as network level protocol for a transport level client.

The server provides its service to other workstations on the network or to other processes. In a server-based network, the most important hardware server is the fileserver, which controls access to the files and data stored on one or more hard disks.

A server may be dedicated or nondedicated. Dedicated servers are used only as a server, not as a workstation. Nondedicated servers are used both as a server and a workstation. Networks with a dedicated server are known as server-based networks; those with nondedicated servers are known as peer-to peer networks.

DEDICATED SERVERS

Dedicated servers cannot be used for ordinary work. In fact, access to the server is often limited to prevent any access by unauthorized users.

Most of the high-end network packages assume you are using a dedicated server. If the network has a dedicated server, it is most likely a file server.

A dedicated fileserver runs the NOS software, and workstations run smaller programs whose function is to direct user commands to the workstation's operating system or to the server. Both servers and workstations need NICs to function on the network.

NONDEDICATED SERVERS

A nondedicated server can be used as a workstation as well as a server. Using a server as a workstation has several disadvantages and is not advisable for larger networks.

The following are disadvantages of nondedicated servers as compared to dedicated servers:

- Many of the NOSs that allow the nondedicated server to run with DOS make them extremely slow and clumsy. While most dedicated servers have software that replaces DOS, such systems may also require a separate non-DOS partition on the hard disk. This allows the NOS to arrange and deal with the contents of the partition in a way that optimizes performance.
- Running applications on a DOS machine while it is also supposed to be running a network can lead to a deadly performance degradation.
- Certain tasks will tie up a DOS machine, effectively stopping the network until the task is finished.
- Adequate security is more difficult to maintain on a nondedicated server.

SUMMARY

In this chapter we discussed the different types of network components and their functions. We described cabling and the connectors used to connect the network hardware. We covered the purpose of the server and the differences between a dedicated and a nondedicated server. Remember, the driving factor for the type of hardware and cabling used is the topology of the network.

CHAPTER 3

NETWORK TROUBLESHOOTING

Upon completing this chapter, you should be able to do the following:

- *Describe how to diagnose and isolate problems with LANs.*
- *Describe how to troubleshoot network malfunctions.*
- *Explain how to test and evaluate the connection of networking system nodes.*
- *Explain how to troubleshoot communications line problems.*

With any network system, you should have a set of error procedures for personnel to follow to handle errors or malfunctions on the system. These error procedures are the steps to be taken when the system is not operating properly. They are different from the error-detection and diagnostic procedures used to isolate and correct transmission problems.

A complete set of diagnostic procedures is necessary for the system. The system procedures are used to isolate the problem to the system or subsystem level. Since the facilities of a network may not be in the local area, it is necessary to have a set of test software and equipment with replacement components available for diagnosing and correcting problems.

TROUBLESHOOTING LANS

As a communications specialist, more than likely you will be expected to know how to troubleshoot problems on LANs. As a troubleshooter, you must be able to identify a wide range of network problems relating to hardware (the data terminal equipment, the communications link, repeaters, gateways, and so on), software (network operating system, applications, and soon), and peopleware (the end user). It will be your job to identify, isolate, and resolve both the simple and complex problems.

DIAGNOSTIC TOOLS

Normally, a problem can be solved without too much difficulty with the help of diagnostic tools. The best diagnostic tool available is accurate documentation. This documentation should include:

- Workstation and server configurations
- All network related software and equipment
- Location and paths of all wiring
- Updated records of all equipment and configurations changes

With documentation in hand, along with the help of diagnostic software (a network management package or a LAN analyzer), and specialized diagnostic equipment, such as a datascope, a time domain reflectometer (TDR), or a breakout box, the job becomes routine.

Classifying the problems and taking the necessary actions to resolve them are an important part of your job as a troubleshooter. However, it is equally important to remember to log all problems according to your activity's procedures. This will identify recurring problems, provide information for long term solutions, and enhance your command's training program.

ISOLATING PROBLEMS

When isolating a problem, consider the three major areas we discussed earlier-the user, the software, and the hardware, usually in that order. The majority of all network-related problems are caused by the user's actions—operator errors. Users either do not understand how to operate their PC in a networking environment or they are unfamiliar with the application software package they are using. Most of the time you will find yourself responding to user problems and complaints. A user will call, saying such things as the following:

- My terminal/PC is hung up, and I cannot get into the system.
- My terminal/PC screen suddenly went blank.
- My temninal/PC keeps coming up with the same error message.
- My terminal/PC will not allow me to access the disk file.
- My terminal/PC will not print.

It will be your job to determine if the problem is user, software, or hardware related. Whenever you receive a call about a problem, obtain as much information as possible about the person and the problem. Ask the user's name, phone number, the terminal/PC or node identification number, the nature of the problem, and what, if anything, occurred immediately preceding the problem. In addition, you should ask the user what application he or she was trying to access or currently working with at the time the problem occured. Ask whether other users are experiencing the same or similar problem, did any error messages appear on the screen, and be sure to ask whether the PC was moved before the problem occured. Sometimes moving hardware creates problems—the connector cable may not be seated properly.

Once you have received initial information about a problem, it should help you to categorize the problem. Keep in mind most problems are the result of inexperienced users/operators. Because so many different types of errors can occur, it would be impossible for us to list them all, along with the necessary steps to resolve them. However, based on past experiences, we can provide you with some helpful hints and guidelines to follow. If the problem seems to be isolated to one user, it is probably user error; if the problem occurs with a group of users in a common geographic location, the problem is usually related to the cable; and if the problem is network wide, a close look at the network software is in order. Let us take a look at some of the more common problems that frequently occur and their solutions in connection with these three categories.

PO3 Frost has just called to report he cannot log on to the LAN. You begin solving the problem by asking some preliminary questions. You find this is the first time PO3 Frost has used the LAN and no one else in his area is experiencing any problems. At this point, you should be able to recognize the problem is more than likely the result of an inexperienced operator (user error). The logical corrective action to take is to walk PO3 Frost through the proper log-on procedures and password security requirements. He follows your instructions and successfully logs onto the LAN. PO3 Frost should have been able to log onto the LAN by following the User's Guide on LAN operations. You might want to review the guide to make sure it is current and available to all users.

A few weeks later PO3 Frost calls again and reports he has been having intermittent problems while logged on to the LAN. Sometimes while he is saving or retrieving data, his machine locks up for no apparent reason. Again, no one in his immediate work area is experiencing problems. After obtaining all the pertinent information available, you believe the problem is faulty hardware. During the save and retrieve operations, a packet is generated and sent through the network interface card, onto the cable, and to its destination. So the two most logical components to check are the cable connections and the network interface card. The diagnostic tools to use are the time domain reflectometer (TDR) to check any breaks on the cable and the diagnostics that come with the interface card. PO3 Frost runs the card diagnostics at the terminal while you check the cable continuity. The network card passes the test, but the TDR detects a continuity break near his location. A LAN technician checks the connectors at the workstation and discovers one of the connectors has worked itself loose. After replacing the connector, the cable is tested again and passes. PO3 Frost logs on to the LAN and experiences no further problems. In this example we eliminated the cable itself because no other user on the cable segment was experiencing problems. Had there been other users also experiencing intermittent failures, then the cable would have immediately been our focal point of testing, since this is the commonality between the users.

You arrive at work Tuesday morning and find a stack of messages waiting for you from users experiencing problems while trying to access the word processing program on the LAN. The only thing these users have in common is they all use the same file server. Immediately you focus your attention on the network operating system and software. You call PO3 Door to ask her a few questions before you begin troubleshooting any further. You learn PO3 Door is able to access all application programs on the LAN with the exception of the word processing program. You immediately log on to the network management program and monitor the data traffic. You discover no user has used the word processing program since

Monday at 1600. The only person authorized to use the LAN after 1600 is PO1 Brush, who is the network administrator. You call PO1 Brush and ask if any changes were made to the word processing program since yesterday. PO1 Brush states he installed a new version of the word processing program on Monday around 2200 to eliminate any work disruptions. You ask him to check the security access to this new version. You find PO1 Brush inadvertently restricted all users from accessing the new version of the word processing program after he removed the old one. He makes the necessary access changes, and everybody is once again happy and able to use the new version.

As you can see, there is a pattern to the various types of errors/problems you will encounter. The problems you will be confronted with will range from the simple to the disastrous. They may be user/operator errors, software problems, or hardware malfunctions. Knowing which is sometimes easy. Under other conditions, it may be difficult for you to determine the source of the problem. The important thing is to learn from your past experiences. Keep a list of symptoms, probable causes, and ways you can use to trace a problem to its cause. This will assist you in diagnosing and troubleshooting problems. You will also find users have a tendency to make the same mistakes again and again, especially while they are learning. You can provide them a great service by explaining some of the more common problems they are likely to encounter, the reasons for the problems, and ways to avoid having them happen to them.

NETWORK MALFUNCTIONS

Any malfunction of the network is going to result in a nonavailability of the system to the users. The diagnosis and fixing of this malfunction becomes a high priority. There are three primary culprits to network malfunctions: component and server failures, and data collisions.

COMPONENT FAILURE

Component failures are categorized in two categories: hard faults and soft faults. Hard faults are relatively easy to find, and a diagnostic program will diagnose them correctly every time. Soft faults can be difficult to find, because they occur sporadically or only under specific circumstances, rather than every time the memory location is tested. A diagnostic program tests computer hardware and peripheral devices for correct operation.

Most computers run a simple set of system checks when the computer is turned on. The PC tests are stored in read-only memory (ROM), and are known as power-on self tests (POSTs). If a POST detects an error condition, the computer will stop and display an error on the screen. Some computers will emit a beep signal to indicate the type of error.

One of the best tools to use for network malfunctions is a network analyzer. A network analyzer is a product that can be used to monitor the activity of a network and the stations on it, and to provide daily summaries or long-term trends of network usage and performance. A network analyzer can do tasks such as:

- Count or filter network traffic.
- Analyze network activity involving specified protocols or frame structures.
- Generate, display, and print statistics about network activity, either as they are being generated or in summary form.
- Send alarms to a network supervisor or network management program if any of the statistics being monitored exceeds predetermined limits.
- Do trend or pattern analyses of network activity.

Network analyzers may be software only or consist of both software and hardware. The latter may include an interface card enabling you to test the network directly. This card may include an on-board processor. Because of their greater capabilities, hardware/software analyzers are more expensive than the software only analyzers. In fact, the prices for the hardware/software analyzers can be several times as high as those for the software only versions.

SERVER FAILURE

The most obvious sign that the server has failed for some reason is that all users, except root, will not be able to logon to the system. Use the following steps as required to reestablish services:

- The first and easiest thing to try is to run the system distribution again. This will rebuild the system maps if nothing else is wrong and will allow users access to the system.
- Shutdown and reboot the system. During the boot process ensure that no failures occur on any of the nodes.

- Verify the domain name.
- Look for the maps subdirectory; it should be the same as the domain name. If it is not there, you will need to run the system initialization command.
- If the above fails, ensure that all the files to be mapped are present on the server. If any have been deleted, they will have to be restored from the latest system saves.

One of the best ways to avoid server malfunctions is to conduct maintenance on the server. It is important to set up a schedule for your server and strictly adhere to it. To check the hardware, you should do at least the following things:

- Clean the server carefully but thoroughly.
- Check cabling and connections for tightness and signs of bending or stress. Do not disconnect connectors unless necessary, since many connectors are rated for a limited number of matings.
- If possible, check the cabling with a line analyzer.
- Run thorough diagnostics on the storage medium and on other system components to identify the components that are likely to fail and to deal with these before they actually do fail.
- Check the quality of your power line by using a line tester.

The hardest part of server maintenance is finding the time to conduct the maintenance, since the network will have to be offline to conduct. In many cases, server maintenance will need to be during off peak hours, late night or early morning, when there is little or no use.

DATA COLLISIONS

A data collision is the simultaneous presence of signals from two nodes on the network. A collision can occur when two nodes each think the network is idle and both start transmitting at the same time. Both packets involved in a collision are broken into fragments and must be retransmitted.

Collision Detection

To detect for a collision, nodes check the dc voltage on the line. A voltage level of two or more times higher than expected indicates a collision, since this means there are multiple signals traveling along the backbone at the same time.

In a CSMA/CD (carrier sense multiple access with collision detection) systems, all workstations or nodes attached to the network monitor the transmission medium at all times. When a node needs to send data, it waits until the line is quiet and then transmits. If two or more nodes happen to transmit data at the same instant, a collision occurs. Each node detects the collision and then waits for a variable amount of time (as programmed in the NIC's microprocessor) before testing the bus again and retransmitting. Since each node waits for a different amount of time, say 10/1000 and 20/1000 of a second, it is very unlikely that the collision will occur a second time. The CSMA/CD detection method is further illustrated in figure 3-1.

Collision Avoidance

To avoid collisions, nodes can send special signals that indicate a line is being used for a transmission. In a

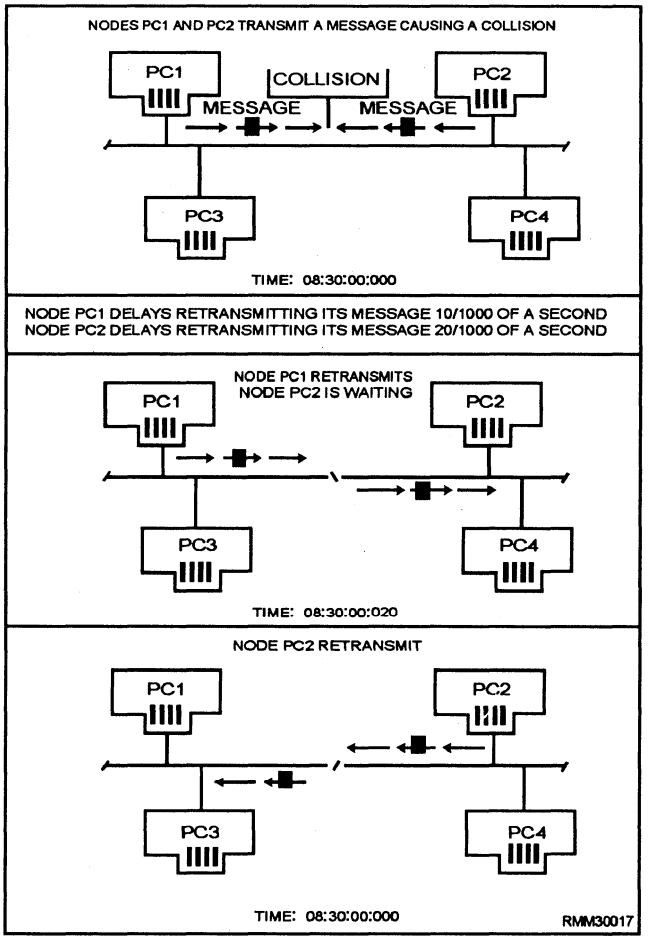

Figure 3-1.—A bus network using the CSMA/CD access method.

CSMA/CA (carrier sense multiple access with collision avoidance) system, the media-access method uses RTS (ready to send) and CTS (clear to send) signals before sending a frame onto the network. A node transmits only after the node has requested access to the line and access has been granted. Other nodes will be aware of the RTS/CTS transmission and will not try to transmit at the same time.

RTS.— A hardware signal sent from a potential transmitter to a destination to indicate that the transmitter wishes to begin a transmission. If the receiver is ready, it sends a CTS signal in return.

CTS.— A hardware signal sent from a receiver to a transmitter to indicate that the transmitter can begin sending. ACTS signal is generally sent in response to an RTS signal from the transmitter.

NETWORK SYSTEM CONNECTIONS

The testing and evaluation of network connections is accomplished with the same test equipment that is used to test network components. This equipment includes voltmeters, ammeters, volt-ohm-milliammeters, and line scanners. All of this test equipment checks the voltage, resistance, and current that passes through the cable and the connectors between the network nodes. Any increase or decrease in voltage or current or an increase in the resistance will cause communications problems for the users.

Whether the cable is pre-made or you make it, you should always test the cable before it installed into the network. This will alleviate the possibility of installing a bad cable or connector to the system. Any time that you can detect a bad connector will be to your advantage, since each connector has a limited number of connections before it has to be replaced.

COMMUNICATION LINE PROBLEMS

Communication line problems fall into three general categories: excessive noise, cabling, and backbone connections. With proper testing and precautions, these problems can be taken care of before they happen.

EXCESSIVE NOISE

Noise is the term for random electrical signals that become part of a transmission, and that serve to make the signal (information) component of the transmission more difficult to identify. Noise can take various forms, including the following:

- Impulse noise: voltage increases that last for just a short period, usually for only a few milliseconds.
- White noise: random background noise.
- Crosstalk: interference on one wire from another.

There are limits set on the allowable levels for each of these types of noise. A noise filter can be used to remove random noise from a signal.

In a transmission, signal-to-noise ratio (SNR) is the ratio between the signal and noise levels at a given point, usually at the receiving end of the transmission. The SNR value is generally expressed in dB.

The SNR can be used to determine how long a cable segment can be before the signal loss is unacceptably high. The SNR also helps to determine whether a particular type of cable will work for the intended use. Cable testers can help determine whether a particular type of cable is appropriate in a specific environment.

In general, digital signals have a much higher SNR than analog signals. Because analog signals in a broadband network must be confined to a portion of the total bandwidth, filtering and other signal-cleaning measures are necessary This confinement makes the signal more delicate and subject to distortion.

Several types of filtering maybe used to help clean a broadband transmission. The filters are distinguished by the filtering technique they use as well as by where in the transmission process they are applied.

For example, filters applied early in the transmission, prior to modulation, are known as baseband or premodulation filters. Those applied after the modulation are known as passband or postmodulation filters.

CABLING

Cables are good media for signals, but they are not perfect. The signal at the end of the cable should be as loud and clear as at the beginning, but this will not be true.

Any transmission consists of signal and noise conponents. Even a digital signal degrades when transmitted over a wire. This is because the binary information must be converted to electrical form for transmission, and because the shape of the electrical signal changes over distance.

Signal quality degrades for several reasons, including attenuation, crosstalk, and impedance.

Attenuation

Attenuation is the decrease in signal strength, measured in decibels (dB) per 100 feet. Such loss happens as the signal travels over the wire. Attenuation occurs more quickly at higher frequencies and when the cable's resistance is higher.

In networking environments, repeaters are responsible for cleaning and boosting a signal before passing it on. Many devices are repeaters without explicitly saying so. For example, each node in a token-ring network acts as a repeater. Since attenuation is sensitive to frequency, some situations require the use of equalizers to boost different-frequency signals the appropriate amount.

Crosstalk

Crosstalk is interference in the form of a signal from a neighboring cable or circuit; for example, signals on different pairs of twisted wires in a twisted pair cable may interfere with each other. A commonly used measure of this interference in twisted-pair cable is near-end crosstalk (NEXT), which is represented in dB. The higher the dB value, the less crosstalk and the better is the cable.

Additional shielding between the carrier wire and the outside world is the most common way to decrease the effects of crosstalk.

Impedance

Impedance, which is a measure of electrical resistance, is not directly a factor in a cable's performance. However, impedance can become a factor if it has different levels at different locations in a network. In order to minimize the disruptive effects of different impedances in a network, special devices, called baluns, are used to equalize impedance at the connection.

Impedance does reflect performance indirectly. The higher the impedance, the higher is the resistance; the higher the resistance, the greater is the attenuation at higher frequencies.

Line Conditioning

Line conditioning tries to eliminate the effects of certain types of distortions on the signal. It becomes more necessary as transmission speeds increase. Two types of line conditioning are available:

- C conditioning tries to minimize the effects of distortion related to signal amplitude and distortion due to envelope delay.
- D conditioning tries to minimize the effects of harmonic distortion in addition to the amplitude and envelope delay distortions handled by type C conditioning.

A line driver is a component that includes a transmitter and a receiver; it is used to extend the transmission range between devices that are connected directly to each other. In some cases a line driver can be used in place of a modem, for short distances of 10 miles or less.

To test a particular section of cable, you can use a line-testing tool. A line monitor is a low-end line-testing tool that tells you if the line is intact. A high-end line-testing tool can do very precise measurements using time domain reflectometry (TDR). A TDR is a device used to test the integrity of a section of cable before the cable is even unwound. This diagnostic method uses a signal of a known amplitude and duration, which is sent along a stretch of cable. Depending on the amount of time the signal takes to return and on the cable's nominal velocity of propagation, the TDR can determine the distance the signal traveled and whether there are any shorts or opens in the cable.

BACKBONE CONNECTIONS

In addition to the inherent problems of the cabling, backbone connections add the problems that come with the use of connectors. They have only a limited number of times that they can be connected before they have to be replaced. These connectors are used in several places along the backbone, each presenting one more place for trouble to start. Some of the places that connectors are used are:

- At the server
- At the repeater, concentrator, and the gateway
- Along the backbone for each drop or tap
- At the splice and coupler (used with fiberoptic)

Each of the connections uses a different type of connector, each with its own limitations. For example:

- A vampire tap is a connector that uses two prongs to pierce the cable to make its connection. When it is used, one of the prongs can be bent and not make a proper connection.
- An RJ connector is the same type of connector used to plug your telephone into the wall. When it is used, the plastic clip has a tendency to break off the connector, resulting in the plug not locking in place.

SUMMARY

In this chapter we discussed the how to troubleshoot communications line problems, network malfunctions, and how to test and evaluate the connection of networking system nodes. As with any troubleshooting, individual manufacturers of both hardware and software will have their own techniques to follow. What we have tried to do is give you a brief overview of the type of trouble that you can expect to run into and some basics as how to begin the troubleshooting.

APPENDIX I

GLOSSARY

A

ATTENUATION— Loss of communication signal energy.

B

BASEBAND— The frequency band occupied by individual information bearing signals before they are combined with a carrier in the modulation process.

BISYNC— Controlling of data transmission by timing signals generated at the sending and receiving stations.

BROADBAND— Transmission facilities whose bandwidth is greater than that available on voice-grade facilities.

BUS— Channel or path for transferring data and electrical signals.

C

CARRIER SENSE MULTIPLE ACCESS (CSMA)— A protocol that controls access to a network's bus.

CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE (CSMA/CA)— A protocol that requires carrier sense and in which a data station that intends to transmit sends a jam signal.

CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION (CSMA/CD)— A protocol that requires carrier sense and in which a transmitting data station that detects another signal while transmitting, stops sending, sends a jam signal, and then waits for a variable time before trying again.

CLEAR TO SEND— A hardware signal sent from a receiver to a transmitter to indicate that the transmitter can begin sending.

CROSSTALK— The disturbance caused in a circuit by an unwanted transfer of energy from another circuit.

F

FILTER— A device or program that separates data, signals, or material in accordance with specified criteria.

FIREWALL— One or more components that control the flow of network traffic between networks.

H

HANDSHAKING— The process through which the rules for exchanging data over a communications line are defined for the two devices involved.

I

IMPEDANCE— A measure of electrical resistance.

INTERNATIONAL STANDARDS ORGANIZATION (ISO)— The international agency responsible for developing standards for information exchange.

INTERRUPT REQUEST LINES— Physical connections between hardware devices and the interrupt request.

L

LINE DRIVER— A component that includes a transmitter and a receiver.

LINK— The communications media used to connect nodes.

M

MULTITASKING— A mode of operation that provides for concurrent performance of two or more tasks.

N

NETWORK INTERFACE CARD (NIC)— The expansion card that allows the workstation to communicate with the network.

NETWORK OPERATING SYSTEM (NOS)— A software package that makes it possible to implement and control a network and that enables users to make use of resources and services on that network.

NODE— The point at the end of a branch.

NOISE— Random electrical signals that become part of a transmission, and that serve to make the signal (information) component of the transmission more difficult to identify.

O

OPEN SYSTEMS INTERCONNECTION (OSI)— The networking standard for interconnecting dissimilar computer systems.

P

PROTOCOL— A formal set of conventions governing the format and control of inputs and outputs between two communicating processes.

R

READY TO SEND— A hardware signal sent from a potential transmitter to a destination to indicate that the transmitter wishes to begin a transmission.

S

SYNCHRONOUS DATA LINK CONTROL (SDLC)— Primary protocol supported under System Network Architecture (SNA).

SIGNAL-TO-NOISE RATIO (SNR)— The ratio between the signal and noise levels at a given point, usually at the receiving end of the transmission.

T

TIME DOMAIN REFLECTOMETER— A device used to test the integrity of a section of cable.

TOPOLOGY— The physical or logical layout of a LAN.

APPENDIX II

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

A

AWG— American wire gauge.

B

Bisync— Binary synchronous communications protocol.

BNC— Barrel nut connector.

bps— Bits per second.

C

CAD— Computer aided design.

CODEC— Coder/decoder.

CSMA— Carrier sense multiple access.

CSMA/CA— Carrier sense multiple access with collision avoidance.

CSMA/CD— Carrier sense multiple access with collision detection.

CTS— Clear to send.

D

dB— Decibel.

E

EIA/TIA— Electronics Industries Association/ Telecommunications Industry Association.

F

FSCK— Filesystem check.

FTP— File transfer protocol.

G

Gbps— Gigabits per second.

H

HTTP— Hypertext transfer protocol.

I

IP— Intemet protocol.

IRQ— Intermpt request line.

ISO— International Standards Organization.

L

LAN— Local area network

LED— Light-emitting diode.

M

MAN— Metropolitan area network.

MAU— Multistation access unit.

Mbps— Megabits per second.

MIC— Medium interface connector.

MODEM— Modulator-demodulator.

N

NEXT— Near-end crosstalk.

NIC— Network interface card.

NOS— Network operating system.

O

OSI— Open systems interconnection.

P

POST— Power-on self test.

R

RJ— Registered jack.

ROM— Read-only memory.

RTS— Ready to send.

S

SC— Subscriber connector.

SDLC— Synchronous data link control.

SMA— Sub-miniature assembly.

SNR— Signal-to-noise ratio.

ST— Straight tip.

STP— Shielded twisted pair.

T

TCP— Transmission control protocol.

TDR— Time domain reflectometer.

TELNET— Telecommunications network.

U

UDP— User datagram protocol.

UTP— Unshielded twisted pair.

W

WAN— Wide area network.

APPENDIX III

REFERENCES USED TO DEVELOP THE TRAMAN

Feibel, Werner, *Novell's® Complete Encyclopedia of Networking*, Sybex Inc., Alameda, CA, 1995.

Gibbs, Mark, *Absolute Beginner's Guide to Networking*, Second Edition, Sams Publishing, Indianapolis, IN 1995.

Liebing, Edward, *NetWare User's Guide*, M & T Books, New York, NY, 1993.

Lowe, Doug, *Networking For Dummies*, IDG Books Worldwide, Inc., Foster City, CA, 1994.

Martin, James, *Local Area Networks Architectures and Implementations*, Prentice Hall, Englewood Cliffs, NJ, 1989.

Ported SNAP I/II System Administration Manual TAC-3 Version, NAVMASSO Document Number 54-94-1, Navy Management System Support Office, Chesapeake, VA, 1994.

Sherman, Ken, *Data Communications User's Guide*, Third Edition, Prentice Hall, Englewood Cliffs, NJ, 1990.

INDEX

Assignment Questions

Information: The text pages that you are to study are provided at the beginning of the assignment questions.

ASSIGNMENT 1

Textbook Assignment: “Network Administration,” chapter 1, pages 1-1 through 1-19.

1-1. Networking gives an individual the capability to communicate and connect with another individual or another system in order to accomplish which of the following tasks?

1. Send messages
2. Share resources
3. Extend processing
4. Perform multiprocessing

1-2. Which of the following types of cables is NOT used for communications?

1. Coaxial
2. Fiber optic
3. Solid core
4. Twisted-pair

1-3. Login procedures that are accomplished by dialing into an access server are known by which of the following terms?

1. Dialup access
2. Distance access
3. Extended access
4. Remote access

1-4. The first thing that the initialization program checks is which of the following areas?

1. Connections
2. Memory
3. Peripherals
4. User accounts

1-5. What is the function of the kernel?

1. Establishes communications
2. Initializes the system
3. Mounts and initializes system files
4. Verifies the integrity of the root filesystem

1-6. How many primary modes of system operation are there?

1. One
2. Two
3. Three
4. Four

1-7. Rebooting the system is called for in how many common situations?

1. Five
2. Two
3. Six
4. Four

1-8. When shutting down the system, turning off the power to the CPU is recommended under which of the following times or conditions?

1. End of the day
2. End of the week
3. Normal conditions
4. Emergency conditions

1-9. Which of the following is NOT a reason why you should monitor the network?

1. To enable you to tune your network
2. To establish communications
3. To maintain a performance history
4. To provide a statistical basis for equipment purchases

1-10. The main importance of reviewing audit/event logs is which of the following functions?

1. Check system throughput
2. Monitor system degradation
3. Monitor system security
4. Verify password attempts

1-11. By using the audit logs, a network administrator can track which of the following areas?

1. Which files were accessed
2. When files were accessed
3. Who accesed certain files
4. Each of the above

1-12. How many interrupt request lines (IRQs) are there in a PC environment?

1. 14
2. 16
3. 18
4. 20

1-13. IRQ values for a device may be set through software or manually by which of the following ways?

1. DIP switches
2. Expansion slot
3. Type of cable used
4. Order in which device was installed

1-14. Network performance is governed by which of the following areas?

1. Administration
2. Hardware
3. Software
4. Both 2 and 3 above

1-15. Besides a physical interface between the device and the computer, what other type of interface does a port provide?

1. Electrical
2. Logical
3. Parallel
4. Transfer

1-16. Which of the following terms is used to describe the process used by an application to test a remote device?

1. Pinging
2. Ringing
3. Signaling
4. Sounding

1-17. The interface between the telecommunications access software and the application programs is known by which of the following terms?

1. Network operating system
2. Network system software
3. Telecommunications access software
4. Teleprocessing monitor

1-18. Electronic mail is classified as what type of software program?

1. Communications
2. Utility
3. Network access
4. Network operating

1-19. Which of the following terms describes the prevention of files from being updated by more than one user at a time?

1. Data integrity
2. Data validity
3. System access
4. System security

1-20. The different levels of access can be designated by which of the following terms?

1. Private
2. Public
3. Shared
4. Each of the above

1-21. Network software often provides some type of locking capability. This locking feature prevents which of the following actions?

1. Access to the file while it is being worked on
2. Logging onto more than one workstation at a time
3. Security violations from occurring
4. Unauthorized users from logging onto the network

1-22. Once the software is installed on the network, it must be tested.

1. True
2. False

1-23. How many methods are used to provide service restoration after system degradation?

1. Five
2. Two
3. Three
4. Four

1-24. DELETED

1-25. What is the minimum percentage to be used in calculating the available resources for the network?

1. 10
2. 15
3. 20
4. 25

1-26. How many major types of LAN configurations are there?

1. Five
2. Six
3. Three
4. Four

1-27. Which of the following topologies was the earliest type?

1. Bus
2. Ring
3. Star
4. Distributed

1-28. Which of the following topologies permits centralized diagnostics of all functions?

1. Bus
2. Ring
3. Star
4. Distributed

1-29. Which of the following topologies is used in many low-cost LANs?

1. Bus
2. Ring
3. Star
4. Distributed

1-30. Which of the following topologies normally requires the entire network be brought down to add a new node?

1. Bus
2. Ring
3. Star
4. Distributed

1-31. Which of the following topologies can be easily adapted to the physical arrangement of the facility site?

1. Bus
2. Ring
3. Star
4. Distributed

1-32. Which of the following protocols is/are used-to control line discipline?

1. Asynchronous data control
2. Binary synchronous communications
3. Synchronous data link control
4. Both 2 and 3 above

1-33. The access method that will be used is governed primarily by which of the following factors?

1. Protocol
2. Topology
3. Both 1 and 2
4. Network operating system

1-34. Using the token passing access method, what, if anything, happens when the transmitting station receives the same token?

1. The message is being sent
2. The message has been passed around the network
3. The message has been appended by another station
4. Nothing

1-35. How many layers are there in the OSI reference model?

1. Five
2. Six
3. Seven
4. Eight

1-36. The physical layer is which layer number of-the OSI reference model?

1. One
2. Two
3. Three
4. Four

1-37. Which layer provides error-free transmission of information over the physical medium?

1. Data link
2. Network
3. Physical
4. Transport

1-38. The network layer is which layer number of the OSI reference model?

1. One
2. Two
3. Three
4. Four

1-39. The transport layer is which layer number of the OSI reference model?

1. Five
2. Two
3. Three
4. Four

1-40. Which layer ensures data units are delivered error-free, in sequence, with no losses or duplications?

1. Network
2. Presentation
3. Session
4. Transport

1-41. Which layer performs the functions that enable two applications to communicate across the network?

1. Network
2. Presentation
3. Session
4. Transport

1-42. Which layer formats data to be presented to the application layer?

1. Network
2. Presentation
3. Session
4. Transport

1-43. Which layer represents the services that directly support users?

1. Application
2. Network
3. Physical
4. Session

1-44. Which of the following cable types is the least expensive?

1. Coaxial
2. Fiber optic
3. Solid core
4. Twisted-pair

1-45. For network purposes, 22- and 24-gauge wire are the most common types of which of the following types of cables?

1. Coaxial
2. Fiber optic
3. Solid core
4. Twisted-pair

1-46. Which of the following types of cable can handle a data flow of up to approximately one Mbps?

1. Coaxial
2. Fiber optic
3. Solid core
4. Twisted-pair

1-47. Coaxial cable is used extensively in LANs whenever the distance involved is relatively short, generally less than how many miles (a) for baseband and (b) for broadband?

1. (a) 1 (b) 5
2. (a) 2 (b) 5
3. (a) 2 (b) 10
4. (a) 5 (b) 10

1-48. DELETED

1-49. Why is fiber optic cable immune to electrical interference of any kind?

1. Has only one strand per cable
2. Has thick shielding
3. Carries no electrical current
4. Uses double insulation on each wire

1-50. DELETED

1-51. Firewalls can be divided into how many different categories?

1. Five
2. Two
3. Three
4. Four

1-52. What piece of hardware is typically used to implement packet filtering?

1. Bridge
2. Gateway
3. Hub
4. Router

1-53. Which of the following features can be provided by a firewall?

1. Address translation
2. Authentication
3. Virtual private networks
4. All of the above

ASSIGNMENT 2

Textbook Assignment: "LAN Hardware," chapter 2, pages 2-1 through 2-10; "Network Troubleshooting," chapter 3, pages 3-1 through 3-7.

2-1. Which of the following devices is used to amplify electrical signals carried by the network?

1. Bridge
2. Gateway
3. Repeater
4. Router

2-2. Which of the following devices is used to connect identical network segments?

1. Bridge
2. Gateway
3. Repeater
4. Router

2-3. Which of the following devices handles the first two layers of the OSI model?

1. Bridge
2. Gateway
3. Repeater
4. Router

2-4. Which of the following devices works at the third layer of the OSI model?

1. Bridge
2. Gateway
3. Repeater
4. Router

2-5. Which of the following devices works at layer seven of the OSI model?

1. Bridge
2. Gateway
3. Repeater
4. Router

2-6. Which of the following devices serves as a termination point for a cable running from individual nodes in a network?

1. Bridge
2. Concentrator
3. Gateway
4. Hub

2-7. Which of the following devices is a box with a number of connectors to which multiple nodes are attached?

1. Bridge
2. Concentrator
3. Gateway
4. Hub

2-8. Which of the following factors need to be decided on before determining the type of connector to use?

1. Architecture only
2. Cable only
3. Both architecture and cable
4. Environment

2-9. Which of the following cables is the best choice if a secure network is needed?

1. Coaxial
2. Fiber optic
3. Solid core
4. Twisted-pair

2-10. Which of the following cables is identified by a designation number of RG-11?

1. Coaxial
2. Fiber optic
3. Solid core
4. Twisted-pair

2-11. Which of the following signals is NOT supported by a broadband system?

1. Data
2. Digital
3. Video
4. Voice

2-12. What type of connector is used to link two segments of cable in a straight run?

1. Barrel
2. Elbow
3. RJ
4. T

2-13. What type of connector is used to connect telephones to the wall?

1. Barrel
2. Elbow
3. RJ
4. T

2-14. An ST connector is rated for what number of matings?

1. 200
2. 500
3. 800
4. 1000

2-15. An SC connector is rated for what number of matings?

1. 200
2. 500
3. 800
4. 1000

2-16. An SMA connector is rated for what number of matings?

1. 200
2. 500
3. 800
4. 1000

2-17. Fiber optic connectors differ from other connectors in which of the following ways?

1. Size of the ferrule
2. Keyed connector
3 The number of matings
4. All of the above

2-18. Components should be tested at all but which of the following times?

1. Before they are installed
2. During the installation
3. After they are installed
4. When things go wrong

2-19. To test electrical activity, you will need which of the following pieces of test equipment?

1. Armature
2. Calibrator
3. Conditioner
4. Voltmeter

2-20. Which of the following pieces of test equipment should be used to check for faults in a cable?

1. Calibrator
2. Conditioner
3. Scanner
4. Voltmeter

2-21. What term refers to the cable that forms the main trunk of a network?

1. Backbone
2. Main link
3. Node drop
4. Primary run

2-22. What type of cable is a 100-ohm, multipair cable used for voice grade communications?

1. Coaxial
2. Fiber optic
3. STP
4. UTP

2-23. How many types of backbone cable are there?

1. One
2. Two
3. Three
4. Four

2-24. What cable manages the bulk of the traffic on a network?

1. Backbone
2. Main link
3. Node drop
4. Primary run

2-25. What device mediates between the computer and the network by doing the necessary processing and translation to enable users to send or receive commands and data over the network?

1. Network access card
2. Network interface card
3. Network operations card
4. Network union card

2-26. Which of the following equipment is used to attach cable sections to each other?

1. Concentrators
2. Repeaters
3. Terminators
4. Transceivers

2-27. Which of the following equipment is used to absorb a transmission at the end of a network?

1. Concentrators
2. Repeaters
3. Terminators
4. Transceivers

2-28. Which of the following is NOT a category of network problems?

1. Commware
2. Hardware
3. Peopleware
4. Software

2-29. Which of the following is NOT a specialized diagnostic tool?

1. Breakout box
2. Datascope
3. Time domain reflectometer
4. Voltmeter

2-30. Which of the following areas cause the majority of all network-related problems?

1. Cabling failures
2. Operating system failures
3. Power outages
4. User actions

2-31. To determine the problem, which of the following information should be gathered?

1. Nature of the problem
2. Node identification number
3. User’s name
4. All of the above

2-32. How many primary culprits are there to network malfunctions?

1. Five
2. Two
3. Three
4. Four

2-33. Component failures are categorized into which of the following types of faults?

1. Hard and soft
2. Hard and permanent
3. Soft and temporary
4. Permanent and temporary

2-34. PC tests are stored in ROM, are known by which of following terms?

1. Boot test
2. Pre-startup test
3. Power-on self test
4. Start test

2-35. Which of the following pieces of test equipment is the best tool to use for network malfunctions?

1. Line conditioner
2. Network analyzer
3. Time domain reflectometer
4. Voltmeter

2-36. When a network malfunction is detected, the alarm is sent to which of the following persons?

1. Department head
2. Network supervisor
3. Security officer
4. User

2-37. To reestablish services, which of the following steps is the first and easiest to try?

1. Run the system distribution
2. Run the system initialization command
3. Shutdown and reboot the system
4. Verify the domain name

2-38. Which of the following terms is used to describe what occurs when two nodes start transmitting at the same time?

1. Collision
2. Derail
3. Jam
4. Wreck

2-39. When a node needs to send data, it waits until the line is quiet and then transmits. This protocol is known by what term?

1. CSMA/CA
2. CSMA/CB
3. CSMA/CD
4. CSMA/CE

2-40. In a CSMA/CA system, the media-access method uses which of the following signals before sending a frame onto the network?

1. NTS and CTS
2. RTS and CTS
3. WTS and NTS
4. WTS and RTS

2-41. Which of the following terms is described as a hardware signal sent from a potential transmitter to a destination to indicate that the transmitter wishes to begin a transmission?

1. BTS
2. NTS
3. RTS
4. WTS

2-42. Whether the cable is pre-made or you make it, it should always be tested before it is installed.

1. True
2. False

2-43. Communication line problems fall into how many different categories?

1. Five
2. Two
3. Three
4. Four

2-44. Which of the following terms is not a form of noise?

1. Blocktalk
2. Crosstalk
3. Impulse
4. White

2-45. Which of the following ratios is used to determine how long a cable segment can be before the signal loss is unacceptably high?

1. NER
2. NNR
3. SER
4. SNR

2-46. Filters applied early in the transmission are known by which of the following terms?

1. Baseband
2. Broadband
3. Passband
4. Preband

2-47. Which of the following terms is used to describe the decrease in signal strength measured in decibels per 100 feet?

1. Crosstalk
2. Impedance
3. Attenuation
4. Degradation

2-48. A commonly used measure of interference in twisted-pair cable is referred to by which of the following names?

1. Front-end crosstalk
2. Inter-end crosstalk
3. Mid-to-end crosstalk
4. Near-end crosstalk

2-49. Which of the followinq terms is a measure of electrical resistance?

1. Crosstalk
2. Impedance
3. Attenuation
4. Degradation

2-50. How many types of line conditioning are available?

1. Five
2. Two
3. Three
4. Four

2-51. Which of the following equipment is used to extend the transmission range between devices that are connected directly to each other?

1. Line conditioner
2. Line driver
3. Network analyzer
4. Time domain reflectometer