NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

IMPLEMENTATION CONSIDERATIONS TO CONNECT AN IBM TOKEN RING LAN TO THE DDN USING TCP/IP PROTOCOL

by

Greg S. Rassatt

March, 1990

Thesis Advisor: Norman F. Schneidewind

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION: UNCLASSIFIED

1b. RESTRICTIVE MARKINGS:

2a. SECURITY CLASSIFICATION AUTHORITY:

2b. DECLASSIFICATION/DOWNGRADING SCHEDULE:

3. DISTRIBUTION/AVAILABILITY OF REPORT: Approved for public release; distribution is unlimited.

4. PERFORMING ORGANIZATION REPORT NUMBER(S):

5. MONITORING ORGANIZATION REPORT NUMBER(S):

6a. NAME OF PERFORMING ORGANIZATION: Naval Postgraduate School

6b. OFFICE SYMBOL *(If applicable)*: Code AS

7a. NAME OF MONITORING ORGANIZATION: Naval Postgraduate School

6c. ADDRESS *(City, State, and ZIP Code)*: Monterey, CA 93943-5000

7b. ADDRESS *(City, State, and ZIP Code)*: Monterey, CA 93943-5000

8a. NAME OF FUNDING/SPONSORING ORGANIZATION:

8b. OFFICE SYMBOL *(If applicable)*:

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER:

8c. ADDRESS *(City, State, and ZIP Code)*:

10. SOURCE OF FUNDING NUMBERS

Program Element No	Project No	Task No	Work Unit Accession Number

11. TITLE *(Include Security Classification)*: IMPLEMENTATION CONSIDERATIONS TO CONNECT AN IBM TOKEN RING LAN TO THE DDN USING TCP/IP PROTOCOL (U)

12. PERSONAL AUTHOR(S) Rassatt, Greg S.

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT *(year, month, day)*	15 PAGE COUNT
Master's Thesis	From To	March 1990	69

16. SUPPLEMENTARY NOTATION

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

17. COSATI CODES

FIELD	GROUP	SUBGROUP

18. SUBJECT TERMS *(continue on reverse if necessary and identify by block number)*

DDN, DoD, Gateway, GOSIP, Internet, ISO, Local Area Networks, LAN, Naval Postgraduate School, OSI, Protocols, Software, Standards, TCP/IP, Token Ring

19. ABSTRACT *(continue on reverse if necessary and identify by block number)*

The Naval Postgraduate School in Monterey, California provides graduate education to commissioned officers and selected Department of Defense (DoD) personnel in a wide variety of subjects important to the military. One of these subjects is computer networks--specifically the DoD Defense Data Network (DDN) which plays a critical role in data transmission. Understanding the DDN and how to use it is immediately applicable and important to the students in their military careers. There is also faculty research in the development and use of the DDN. In addition, the DDN provides excellent electronic mail and a wealth of bulletin board and information services for a variety of users. The Administrative Sciences department is expanding its LAN-to-DDN connectivity so as to offer services common to most LANs as well as direct access to the DDN. The department has an IBM Token Ring network for this educational environment. This paper reviews the issues a network manager must consider to provide LAN-to-DDN connectivity. Particularly the DDN, token ring networks, the campus backbone network, protocols, TCP/IP software and design issues a manager should consider in making this connectivity occur.

Thesis

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT: [X] UNCLASSIFIED/UNLIMITED [ ] SAME AS REPORT [ ] DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION: Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL: Prof. Norman F. Schneidewind

22b. TELEPHONE *(Include Area code)*: 408-646-2768

22c. OFFICE SYMBOL: AS/Ss

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

SECURITY CLASSIFICATION OF THIS PAGE Unclassified

Approved for public release; distribution is unlimited.

Implementation Considerations to Connect an IBM Token Ring LAN to the DDN Using TCP/IP Protocol

by

Greg S. Rassatt
Captain, United States Army
B.S., United States Military Academy, 1981

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
March 1990

Author: Greg S. Rassatt

Approved by: Norman F. Schneidewind, Thesis Advisor

Leon R. Sahlman, Second Reader

David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

The Naval Postgraduate School in Monterey, California provides graduate education to commissioned officers and selected Department of Defense (DoD) personnel in a wide variety of subjects important to the military. One of these subjects is computer networks--specifically the DoD Defense Data Network (DDN) which plays a critical role in data transmission. Understanding the DDN and how to use it is immediately applicable and important to the students in their military careers. There is also faculty research in the development and use of the DDN. In addition, the DDN provides excellent electronic mail and a wealth of bulletin board and information services for a variety of users. The Administrative Sciences department is expanding its LAN-to-DDN connectivity so as to offer services common to most LANs as well as direct access to the DDN. The department has an IBM Token Ring network for this educational environment. This paper reviews the issues a network manager must consider to provide LAN-to-DDN connectivity. Particularly the DDN, token ring networks, the campus backbone network, protocols, TCP/IP software and design issues a manager should consider in making this connectivity occur.

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

A. BACKGROUND

The Naval Postgraduate School (NPS) in Monterey, California, provides advanced education of commissioned officers. More specifically one of its goals is "To enhance continually the contribution of the content of the academic programs to the Navy and the Department of the Defense." (Naval Postgraduate School, 1988, p. 6) Of the subjects taught, one area of increasing importance to military operations is the field of computers and computer communication.

Officers will continue to use a variety of microcomputers during their military career. The Administrative Sciences (AS) department is one of several academic departments which supports microcomputers. It does this by providing five Local Area Networks (LANs) for student and faculty use. One of these networks, an IBM Token Ring, provides a hands-on approach for student education. This network (hereafter called TR-LAN) has all the challenges, trade-offs, and problems that are typical of network management. This paper will review how the TR-LAN will fit into the NPS long range plan of connecting all campus networks. Also, this paper will discuss the exact make-up of the TR-LAN, its future goal of connecting to the Defense Data Network (DDN), and the installation of TCP/IP protocol to make this DDN connection possible.

B. OBJECTIVES

When a network manager decides to add a new capability to a small network there are four possible approaches to take. The first is to define a set of desired functions and submit this as a request for bids among vendors. When there is a limited amount of technical experience available this may be the best method to use. The second approach is to have the network staff determine the goals and prepare a list of issues to ask vendors. Then with the vendor responses, determine the best software to purchase. This approach may also include reconfiguring the network especially if it is not possible to expand the system. A third method depends on the capabilities of the staff. If the LAN staff has sufficient knowledge and experience, it can determine the specifications and order the system. The last approach is to simply write all the software code yourself to accomplish the new capability. This is undoubtedly the most work but would provide an excellent learning experience if there is enough time. Whichever method is used, it is important to survey the user and give the user a strong say in specifying requirements.

This paper will use the second approach to solve the TR-LAN software problem. In particular, it will determine and discuss the problems and trade-offs involved in *providing a connection* between the TR-LAN and the DDN. The focal point will be the Transmission Control Protocol/Internetwork Protocol (TCP/IP) software. An analysis of what is available in TCP/IP software will illustrate the trade-offs that must be made to make this connectivity occur. An underlying theme of this analysis, therefore, will be to find a TCP/IP software product which will work on the existing TR-LAN configuration. The goal is to find a software product that satisfies all needs, is easy to install and maintain, and is easy to use.

C. PROCEDURE

An explanation of several terms and systems is necessary to appreciate the analysis of this problem. The first chapter will be devoted to the DDN and describe the importance of the DDN to the military community. In the next chapter an explanation of the TR-LAN and token rings will illustrate the existing network configuration. This explanation will lead into the following chapter on the interconnection of networks. This chapter will take a close look at the future NPS network and how the TR-LAN will connect to the campus backbone. These beginning chapters provide the basis for evaluating the TCP/IP software--the topic of the fourth chapter. This analysis will cover a variety of key issues important to software selection. Finally, a summary of the issues covered in the paper provide a guideline for the network manager to solve the TR-LAN-to-DDN connection problem. This thesis will make the reader more aware of the issues involved in evaluating TCP/IP software.

II. WHY THE DEFENSE DATA NETWORK

A. CHAPTER INTRODUCTION

Communication is a critical ingredient for a successful military mission. Users need a highly reliable system which can perform a variety of functions. A user needs to understand the capabilities of the Defense Data Network to gain full appreciation of its benefits. This chapter will explain the origin of the DDN and how it operates. Then an explanation will follow on how to access the DDN. This will lead into a discussion of what a DDN host must be able to do and the DDN pricing structure.

B. WHAT IS THE DDN

The DDN is a variety of networks that include the unclassified MILNET, and ARPANET networks.

> The ARPANET was built in 1969 as an experiment by the Defense Advanced Research Projects Agency (DARPA)...to demonstrate that computers, made by different manufacturers, of different sizes, and with different operating systems could communicate with each other across a network. (NIC 50001, 1985, p. 8)

This experiment was successful but it needed to have a common protocol for all the systems. In 1982 "...Transmission Control Protocol (TCP) and Internetwork Protocol (IP) were designated official DoD network communication protocols by the Office of the Secretary of Defense (OSD)." (NIC 50002, 1989, p. 3) Then in 1984 ARPANET split to form "...a military research and development network (ARPANET) and a military operational communications network (MILNET)." (NIC 50001, 1985, p. 8) These networks work well and set a standard for many other networks to follow.

"The MILNET has approximately 160 PSNs including 24 in Europe and 11 in the Pacific and Far East." (Comer, 1988, p. 23) These Packet Switched Nodes (PSNs) are made by and under the care of Bolt, Beranek, and Newman, Incorporated. The PSNs operate by breaking a message into smaller units called packets. These packets are relayed individually to their destination by the best routes available. At the destination, the PSN reassembles the packets in their correct sequence. Most PSN ports use an 1822 interface protocol which offers reliable, flow-controlled delivery. In the future, however, more ports are likely to use the CCITT X.25 PSN interface protocol. (Comer, 1988, pp. 23-24)

The DDN is a highly reliable system for both classified and unclassified messages. It provides the capability to transfer files, send and receive messages, log on to a host in a different location, transfer graphic images, and do a variety of smaller functions helpful to the user. The DDN also includes survivability measures to ensure it can survive along with the activities it supports. In addition, the DDN provides security through link (direct hardware connections) and source to destination (end-to-end) encryption measures. This ability provides secure, reliable, and survivable message traffic which is important to the military and the network managers who use it.

> The modern military commander must not be deprived of automation and communications in the heat of battle. While some degree of manual back-up is necessary and even desirable, it is fundamental that the forces operate best when the capabilities at their disposal are the ones they are familiar with through training and exercises. (Cerf, 1983, p. 296)

The Naval Postgraduate School graduates will use or rely on DDN message traffic some time in their career. Therefore it is helpful that students be comfortable with operating in the DDN environment and be familiar with the services it provides. The direct connection of the TR-LAN to the DDN will provide an excellent training mechanism to the students. A small sampling of what the DDN has to offer includes: the Network Information Center (NIC)--which provides a help facility and a WHOIS function to locate other registered users; a listing of other hosts, Request For Comments (RFC)--which is a data base of professional notes and a variety of NIC documents.

C. METHODS TO ACCESS THE DDN

Access to the DDN occurs three ways: through a Terminal Access Controller (TAC), through a host, or through a gateway. To use a TAC a user must dial one of many TAC phone numbers located near most government facilities. The nearest TAC location to the NPS is adjacent to the Packet Switch Node on the campus. The PSN and TAC are in the NPS Computer Center. "A TAC allows a variety of terminals to communicate with any host on the network without going through an intervening host." (NIC 50001, 1985, p. 15) The user must have both a user-ID and an access code or password to gain access to the TAC. The NIC provides a TAC access card upon request. A TAC is very useful when a user is travelling. Through the TAC a user can operate a host located anywhere on the DDN. The user first dials the closest TAC phone number to his or her location. Then, with the proper codes, he or she can log into a host back at the home station.

Access to the DDN through a host is also quite simple. The mainframe computer at NPS is a host to the DDN. Therefore once a student properly accesses the mainframe, there is immediate access to the DDN. Only a DDN link command is necessary and the network is available. The mainframe makes the connection through a Series 1 Front End Processor. The Series 1 provides the electrical and timing interface of message packages to the Packet Switch Node.

To access the DDN through a gateway the user inputs a gateway address with the message. This traffic then hops from the user, to the gateway, to the DDN backbone. This connection is transparent--that is the user is unaware that this hop connection exists. Therefore the user has access to the DDN to conduct message traffic or to log into another host.

The desired goal is to use the TR-LAN as a host with direct access to the DDN. This will occur with a router connection between the TR-LAN and the PSN. This type of connection would mean the user would only need to be knowledgeable of the commands on a personal computer. The TR-LAN as a host reduces the variety of system software, operating systems, and procedures the user has to remember. In this configuration the NPS user would need to understand only the DOS and network operating systems for the TR-LAN.

When connecting to another host there could be other operating systems to learn. (Note: The Network Information Center on-line information lists 82 operating systems on various DDN hosts). A familiar DDN operating system is the TOPS-20 as seen at both NIC and the University of Southern California. Using the TR-LAN host, however, the user can concentrate on fewer commands and appreciate the full capability of the DDN. The new connectivity will also decrease the delays caused by either the slow interaction of the mainframe (on busy days) or because of the slow speed of a modem.

D. ROLES OF A DDN HOST

A DDN host has several responsibilities. In illustration this section will briefly cover: protocols, the Host Administrator, Internet addresses, routing tables, and name servers.

1. Protocols

A host provides the network protocols necessary to operate on the DDN. A protocol is "A formal description of message formats and the rules two or more machines must follow to exchange these messages." (Comer, 1988, p. 346) There are a variety of PSNs and hosts throughout the DDN. Therefore to limit possible confusion and potential problems hosts must follow the policy that "...protocol implementations for use in the DoD environment MUST comply with the MIL-STD versions of the protocol specifications." (NIC 50002, 1989, p. 6) This ensures that each host handles the message traffic in the same manner.

With the installation of the proper protocols the TR-LAN is a candidate to be a host on the DDN.

> PCs can be attached to the DDN in several ways, including as hosts. At present, however, most personal computers on the DDN are not hosts, i.e., they have not implemented the network protocols and are not attached directly to a PSN. (NIC 50001, 1985, p. 20)

A PC acting as a host is not common in the DDN. This is because most hosts are usually mainframes or a workstation such as a SUN workstation operating with UNIX.

2. Host Administrator

Besides providing the correct protocols a host must provide 24 hour-a-day access. This is now not a problem because the servers are continually in operation. When a host needs to shut down for repair, however, the Host Administrator should inform the Network Monitoring Center (NMC). Each host has a Host Administrator to serve as a technical and administrative contact for that host. The Host Administrator will also provide policies and determine which users can access the network. The Host Administrator will follow the guidelines set by the DDN Program Management Office

(PMO). The Host Administrator will also work with the NIC, the NMC, and a Node Site Coordinator (representing the PSN to which the TR-LAN attaches). (NIC 50001, 1985, p. 50)

3. Internet Address

A host needs an address to communicate on the DDN. The Host Administrator will provide each user with an internet address. This will allow students to communicate with other users and to send and receive data. Students can receive data 24 hours a day using the server mailbox. The addresses for the TR-LAN will follow a standard naming convention. This convention declares that addresses follow the format of "user-ID at host.subdomain.domain."

A potential address of the TR-LAN is easier to visualize when describing the largest organization to the smallest. To illustrate, all military groups have a domain name of MIL. Therefore the NPS domain name is MIL. Within the military, NPS falls under the Navy (hence the subdomain is NAVY). Within the Navy, the NPS Network has an additional subdomain of NPS. Next, within NPS each department will have its own subdomain. The Computer Center now uses CC hence the Administrative Sciences department could possibly use AS. Lastly, as a host operating in the AS department the TR-LAN could use the name TRLAN. Therefore a user, TomJ, operating on this hypothetical network would have an address of "TomJ at TRLAN.AS.NPS.NAVY.MIL."

4. Routing Table

A routing table matches a unique internet address to each name. The MILNET uses the address 26.X.X.X (four groups of eight bits) and ARPANET uses 10.X.X.X. These are class A addresses because the first number of the four number group is below 128.

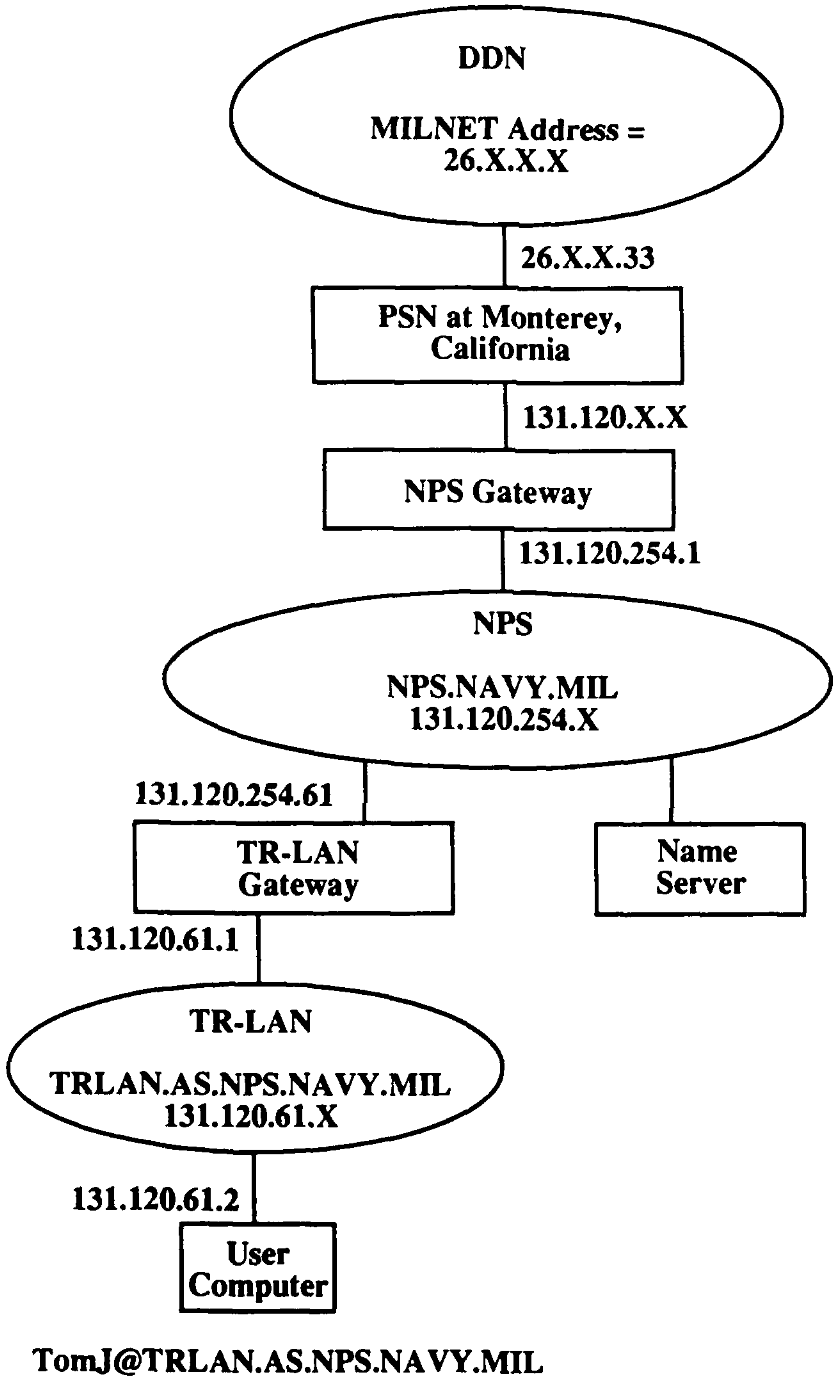
> Networks assigned class A addresses partition the 32 bits into an 8-bit network portion and a 24-bit host portion. Class B addresses partition the 32 bits into 16-bit network and host portions, while class C partitions the address into a 24-bit network portion and an 8-bit host portion. (Comer, 1988, p. 194)

The NPS network is a class B address (the first number is within 128-191). It uses 131.120.X.X to identify itself to the Internet. For example the NPS campus backbone may use 131.120.254.X. This subnet addressing allows up to 254 NPS networks which can then use eight bits (the last position in the group of four numbers) for assigning addresses to hosts. Using this technique, each NPS network could have up to 254 hosts (eight bits represent 256 addresses but this addressing does not use the numbers zero and 255). A possible address for one network in the Administrative Sciences department is 131.120.61.X with the "X" representing room for addressing up to 254 hosts. Therefore two possible TR-LAN addresses are 131.120.61.1 for the gateway and 131.120.61.2 for a user computer.

Routing tables list network names, net addresses, and routes to travel to get to a desired address. Gateways are the primary users of routing tables in the Internet. The gateways must know the network identification of the highest level networks. Therefore MILNET only needs to know the NPS internal class B address (131.120.X.X). The NPS Gateway must know the local networks (such as the various NPS networks). The TR-LAN would store several names and addresses. When declaring a unlisted name, the TR-LAN will refer to the NPS name server for the address. Refer to Figure 2.1 to see how the address plan and routing could occur from the TR-LAN to the DDN.

5. Name Server

In support of routing tables, a name server lists all the addresses and names of various networks. The Host Administrator updates the name server for all its users



Note: This diagram shows a user's hypothetical network address on the TR-LAN and how the message will flow to the DDN.

Figure 2.1 NPS Internet Address Example

with access to the DDN. The Host Administrator also registers users in the NIC WHOIS data base. This data base acts as a white pages listing of all registered users. The NPS Computer Sciences department controls the NPS primary name server. The Naval Ocean System Center (NOSC) in San Diego, California, has the NPS back-up or secondary name server.

> When a name is provided by a user for translation to an address, the host will first examine its local cache, and if the name is not found there, will communicate with an appropriate name server to obtain the information, which it may then insert into its cache for future reference. (Clark, 1982, p. 3)

Keeping the name server current, however, is a challenge when trying to stay abreast of changing users such as students. One approach to minimize registration requirements is to register students on the NPS name server as temporary users. The user registration would then only be done at NPS. Another approach is to register a generic name such as "Group1" on the NPS name server. Several students would share this generic name and use it mainly for a learning device.

E. FUTURE CONSIDERATIONS REGARDING THE DDN

The "Usage Sensitive Billing (USB)" cost structure which begins in FY 1990 will charge each DDN access port about $1,000 a month plus a usage fee. In the case where multiple hosts share one PSN access port, a monitoring device will need to measure and separate types of traffic to the PSN. This information will allow a fair breakdown of the total bill received per PSN port. The USB intentions are to: induce subscribers to select the needed number of access lines, provide incentives for efficient use of the system, distribute costs to those who use it, and provide reliable information on the use of DDN. (McNamara, 1986, p. 37) This will encourage NPS to have only one DDN access port (now the Computer Sciences department and the Computer Center each have separate

PSN port numbers). The effect of this pricing structure on individual hosts in a large organization such as NPS is not clear. The TR-LAN connection to the DDN would remain the same but there would be a concern for how or if departments must pay for their usage. Any pricing decision will probably affect the TR-LAN as a host but to what extent is unclear.

F. CHAPTER SUMMARY

The DDN is a vast network with many capabilities. The ability to access this network in a variety of ways is convenient for the user. The TR-LAN can now access the DDN two ways. Operating as a host, however, will provide a learning tool which will greatly increase the students understanding of the DDN. The planned improvements in the campus network will eventually allow the user to practice all three of the DDN access methods. These improvements will also decrease the NPS DDN usage cost through the use of a single PSN port.

III. A DESCRIPTION OF THE IBM TOKEN RING LAN

A. CHAPTER INTRODUCTION

There are a variety of network topologies used at NPS. The Administrative Sciences department alone uses ethernet baseband, ethernet broadband, token ring, and AppleTalk. The capabilities of the token ring, however, make this the best choice for an expected large number of users. Another consideration when establishing a network is whether to use dedicated servers or peer-to-peer communication among computers. The networks in the AS department all use dedicated servers. This chapter will look at what comprises a token ring and the dedicated server configuration of the TR-LAN. This will be followed by a closer look at network management as it concerns the addition of new software.

B. WHAT IS A TOKEN RING LAN

A token ring network provides to the user a transparent means of resource sharing and node communication. It accomplishes this by using the token ring. The token ring is one of the oldest ring control techniques. It was originally proposed in 1969 and is the most popular ring access technique in the United States. (Stallings, 1988, p. 355) A token ring works by transmitting a token around the network in a circular fashion. A station must be able to receive the token to be part of the network. A station which desires to transmit must wait to capture a free token. The token plus message (busy token) circulates, delivers the message, returns to the sending station (which purges the message), and is emitted as a free token for the next station.

The token ring has the advantage of having an upper bound on access delay. Carrier Sense Multiple Access with Collision Detection or CSMA/CD topology uses contention and does not have an upper bound. This means that no matter how many messages are transmitted, the token ring user can expect a reasonable maximum delay (versus CSMA/CD message traffic on ethernet networks which could have an undetermined delay time). The token ring, however, has a higher traffic delay under light traffic compared with CSMA/CD. Nevertheless, the user realizes a dependable service.

1. Token Ring Layers

Industry standards control the token ring operation. The Institute of Electrical and Electronics Engineers (IEEE) issued local area network standards (IEEE 802) to promote uniformity within LAN topologies. Later the American National Standards Institute endorsed these standards. The IEEE 802 standards are in the form of a three layer communications architecture. The Open Systems Interconnect (OSI) seven layer model--a standard for internetwork communication--illustrates how these IEEE 802 standards fit into the communication protocols. The OSI Layer two, Data Link Layer, is equivalent to the upper two layers of the IEEE 802 standards. The top-most of these two layers is the Logical Link Control (LLC) Standard 802.2. This layer is similar in operation to the OSI Data Link Layer. It provides a service for moving frames of data from one station on the LAN to another. The IEEE LLC layer also provides error control, flow control, and an interface to higher level protocols.

The lower of the upper two IEEE 802 standard layers, the Medium Access Control (MAC), is unique to LAN environments. The MAC supports three different standards: CSMA/CD (IEEE Standard 802.3), Token Bus (IEEE Standard 802.4), and

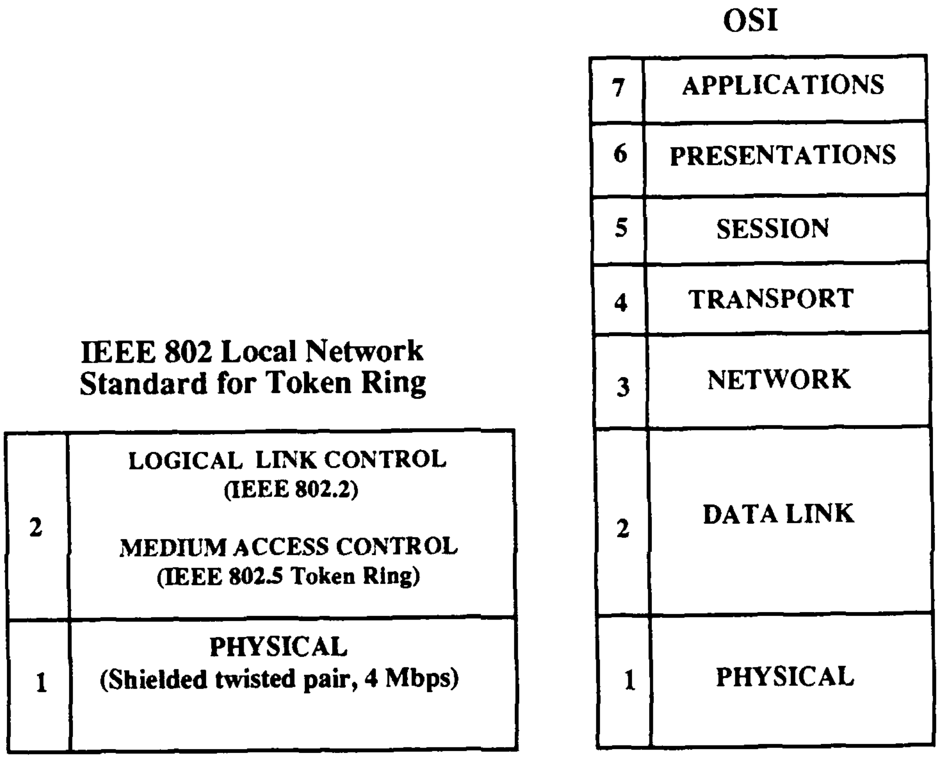
Token Ring (IEEE Standard 802.5). The OSI Layer one, Physical Layer, represents the similarly named Physical Layer in the IEEE 802 standards. The Physical Layer, for example, states that a token ring can use shielded twisted pair at four Mbps. This layer refers to the encoding and decoding of signals, and the bit transmission and reception. (Stallings, 1988, pp. 370-371, 437-445) Refer to Figure 3.1 for a mapping between the IEEE standards and the OSI seven layer model.

2. Token Ring Physical Configuration

The cable supporting the TR-LAN is a Power Limited Circuit Cable, Class 2 (verified to IBM specifications). There are two shielded twisted pairs, each 22 gauge. Each cable contains four solid-copper conductors wrapped in white plastic insulation. The conductors arranged as two pairs, each pair twisted in a spiral and wrapped in a thin plastic sheath. Two of these wires bring the signal in and two wires take the signal out. This results in a transmission speed of four Mbps. A unique plastic connector provides the connection to the Multistation Access Unit (MAU) or for cable extensions. (Berry, 1988, p. 228)

Another attribute seen in the token ring is the physical star connection of computers. The computers are attached to a MAU which provides a physical star connection while maintaining the logical ring. One advantage of this type of configuration is the ease of adding or deleting computers. A connection or disconnection during operation does not effect the network. A computer does not have to be powered up because relays in the MAU bypass the inactive computer.

The TR-LAN transmits messages in a baseband mode. Characteristics of baseband include the use of digital (unmodulated) signalling and simplicity of installation and maintenance. The entire bandwidth capacity of the cable carries the signal. A



Note: The above diagrams show the mapping between the IEEE standards and the seven layer Open System Interconnect model.

Figure 3.1 IEEE & OSI Communication Architectures

problem, however, is the inability to support some types of communication such as video and voice. Because of its flexibility, the baseband is nonetheless quite efficient for the token ring.

C. MANAGEMENT OF THE TR-LAN

Managing a network is frequently a challenge. The manager must often search for a balance to satisfy desires. The following section illustrates the diversity of this network.

1. Configuration of the TR-LAN

The TR-LAN is a 15 user computer network supported by three servers. These computers all have network interface adapter cards. The adapter "...has its own memory, its own microprocessor, its own communications controller for managing access to the network, and its own serial interface controller." (Berry, 1988, p. 326) The specifications for the equipment in this network include: three servers, two of which are IBM PC XT with a 640K Random Access Memory (RAM), and a 10 Mb or 30 Mb hard disk; and an IBM PC AT with a coprocessor, 1Mb RAM, and a 20 Mb hard disk. Note that one of the XT servers acts as a gateway in support of the IBM PC 3270 Emulation. There are also two dot matrix printers (IBM PROPRINTER) connected to two of the servers. User computers consist of: twelve 10 MHz Standard 286 AT clones with 640K RAM, 20 Mb hard disk, NEC color monitors; and three IBM PC XTs with 640K RAM, 20 Mb hard disk and color/graphic monitors. Additionally there are six telephone connections (six computers have a modem adapter card) supporting SIM/PC and SMARTCOM II, five channels to the 3174-1L connector in support of the IBM PC 3270

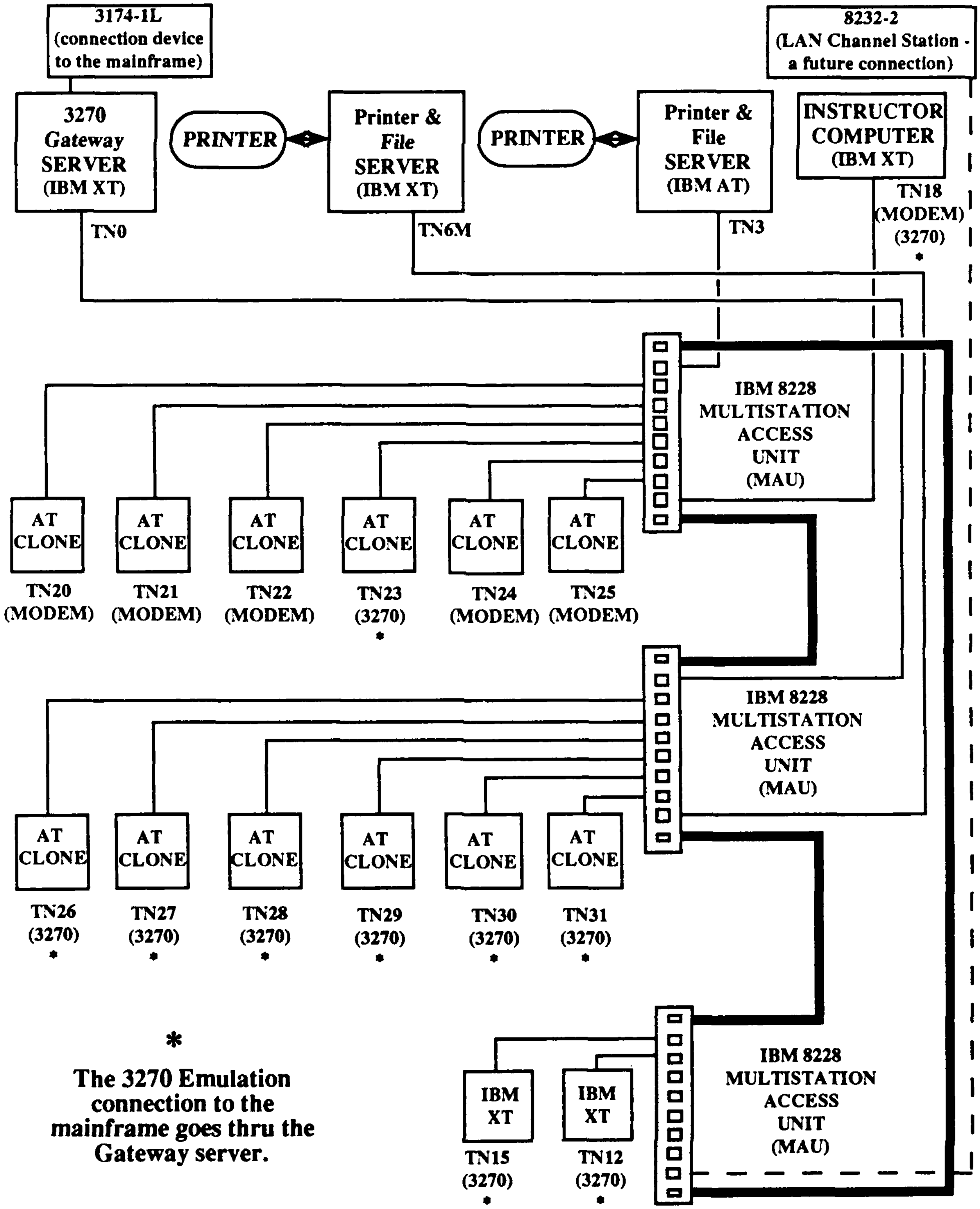
Emulation, and three IBM 8228 Multistation Access Units. There is also a plan to connect to the IBM 8232-2 LAN Channel Station in the computer center.

There are three disk drives at every computer on the TR-LAN. These include two floppy disk drives (A and B) and a hard disk drive (C). The configuration of these drives is as follows: the A drives support 5-1/4 inch floppy diskettes. The AT clones have a high density drive (1.2Mb), and the IBM XT computers have a standard drive (360K). The B drives support standard drive (360K) 5-1/4 inch floppy diskettes. Because of the requirements of the network and disk operating systems and the token ring, the original 640K RAM available in each of the 15 user computers decreases by 170K RAM. This leaves only 470K for application software. The RAM available is a restriction of the IBM PC LAN Network operating system and DOS. Actually several IBM PC LAN Network functions--such as electronic mail--are not available to the user in order to maximize the available RAM for applications.

The TR-LAN has two methods of connecting to external networks. One connection is through telephone lines using the SIM/PC or SMARTCOM II software packages. The other connection is an IBM PC 3270 Emulation Program using a direct coax cable from the gateway server to a 3174-1L controller at the IBM mainframe computer. This cable connection allows the user to operate on the mainframe and transfer files to and from the user computer. Conflicts with the user computer's interrupts, however, restricts the user computer to connect to either a modem or the 3270 Emulation, but not both. Refer to Figure 3.2 to see a drawing of the TR-LAN.

2. Providing a Wide Variety of Services

The TR-LAN provides several software programs in support of eleven different classes taught at NPS. As of this writing the following software is available on the TR-



Note: This drawing, not to scale, shows the layout of the TR-LAN.

Figure 3.2 IBM Token Ring LAN

LAN: 1DIR (a directory program), LOTUS 1-2-3 (spreadsheet program), 3270 Emulation to the IBM mainframe, SIM/PC and SMARTCOM II (communication software), WordPerfect 5.0 and 4.2 (word processing), and a Virus check program to inspect floppy diskettes. The IBM PC LAN Network operating system provides the resource allocation and sharing and manages the computers in the network. It operates with a PC DOS operating system.

3. User Friendliness

The TR-LAN does not have a full-time lab assistant in the room during operation. Only three people support the AS department networks: a Professor who is in charge of all the AS laboratories, a network administrator, and a student who acts as a part-time lab assistant. Because of this, TR-LAN security and self sufficient operation are very important.

A goal is to provide a user friendly environment which does not require explanation by a staff member for the user to understand. The students who are familiar with networks or have a class which works on the TR-LAN normally have little difficulty. Students who just use the network for its capabilities, however, may have little or no training and rely on a simple user interface. Providing programs which do all the required commands is one method to keep the network easy to use. When a user enters the network with the command "start <username>" a series of commands (batch files) perform all the network access commands. After a correct logon, the user sees a display of software to select. This selection of software is actually another group of batch files which do all the necessary processing to provide the user easy access to the application programs.

4. Provide Software Programs Through the Server

There is a continuous attempt by the lab staff to provide in the TR-LAN the most current software. To keep maintenance and installation simple all software is kept in the server and sent to the client or user computer upon request. This means any future software changes or modifications will occur only on the server. Vendors are aware of the benefits of providing this service so they provide a "License" (for a fee) to operate one software package on a network server. This fee is proportional to the number of computers connected to the server.

Locking their keyboards restricts all access to the servers thus protecting the network and application files from tampering. The keyboards are accessible only by the lab staff. There is a drawback to this approach, however. A staff person must re-boot the server whenever a problem--such as a power failure--occurs. This could cause the network to be inoperative an entire evening or weekend. This inconvenience, however, is better than allowing user access to the server which would have unpredictable results.

D. CONSIDERATIONS WHEN ADDING NEW SOFTWARE PROGRAMS

A careful evaluation of new software occurs before installation on the TR-LAN. This is especially true for software that affects communicating within a LAN or between several LANs.

> The more a local network is designed to increase the effectiveness of intra-local network communication, the more the cost of the interface to a long-distance network increases and the more the effectiveness of inter-local network communication decreases. (Schneidewind, 1983, p.17)

The TR-LAN must balance between an efficient interface to the DDN and an efficient network supporting a variety of user requirements. It is important to avoid losing present capabilities by any future installation of TCP/IP software.

The existing system is now easy to maintain and easy to operate. It is not desirable to add any new software package that would disrupt this system. As a result any new software should operate from the server, on a IBM PC LAN Network operating system, using a token ring topology.

E. CHAPTER SUMMARY

This chapter reviewed the make-up of a token ring topology and several network manager concerns. The configuration of the TR-LAN is capable of changing, but it is not desirable to make special adaptations for every new software purchase. Finding software which does not require any network changes, however, is not always easy. Another concern, the subject of the following chapter, is how to connect to the campus backbone and the DDN.

IV. CONNECTING THROUGH THE NPS NETWORK TO THE DDN

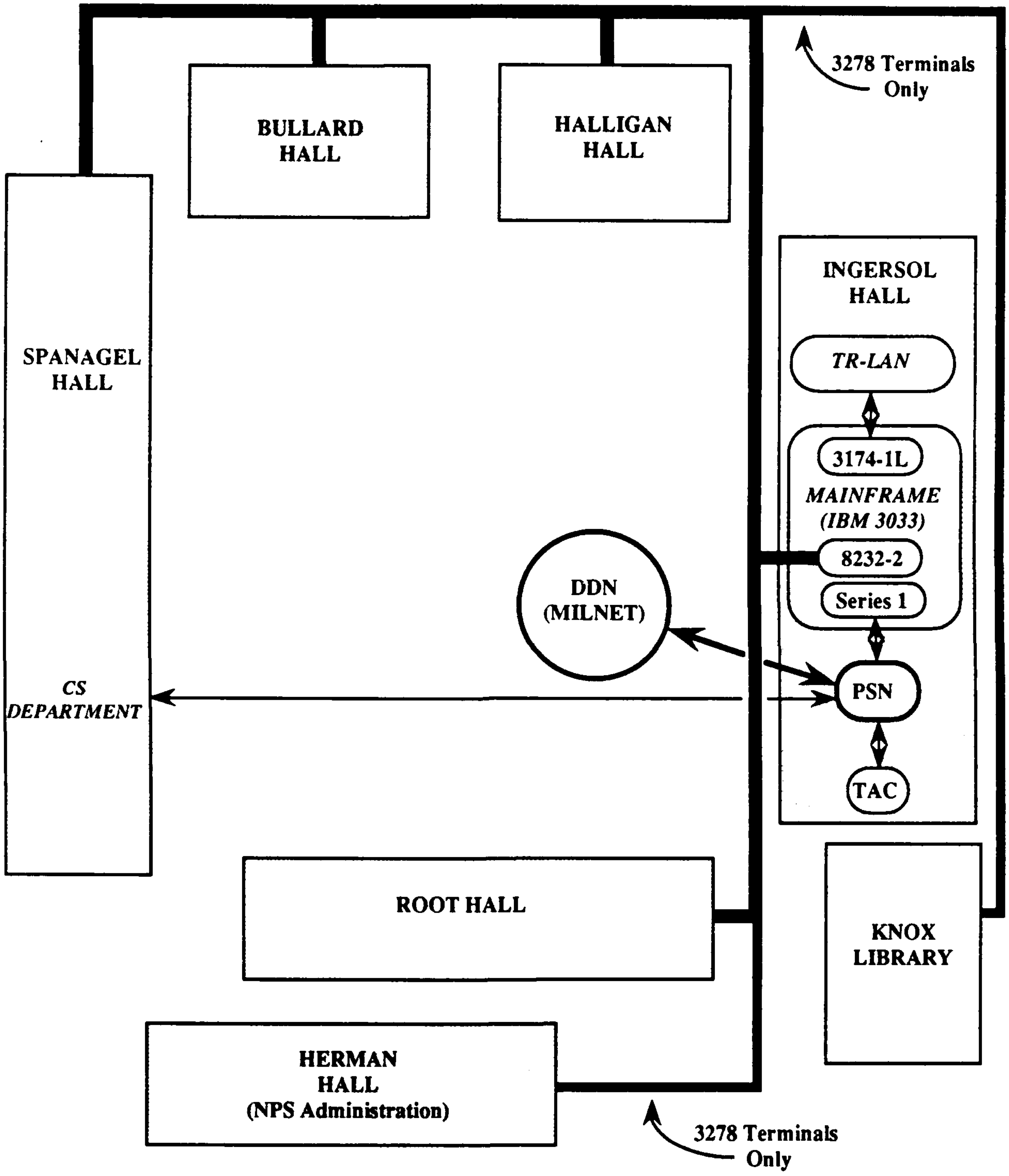
A. CHAPTER INTRODUCTION

The easiest method to physically connect to the Defense Data Network is to just install a cable between the TR-LAN and the Packet Switch Node. This, however, is neither economical nor practical. Connecting will require the consideration of the future campus communication plans. Also, it will require permission from the Defense Communication Agency. This chapter will look at how the TR-LAN can both make this connection and communicate with other NPS networks.

B. NPS NETWORK CONFIGURATION

The Naval Postgraduate School has a thick ethernet cable providing the backbone network to the campus. This cable connects the five main academic buildings, part of the administration building, and the library. The administration building and the library, however, only have 3278 terminal capability to the mainframe. The backbone network also has a connection to the NPS mainframe computer via a 8232-2 LAN Channel Station. The TR-LAN has a connection to the campus backbone only because the TR-LAN connects to the mainframe computer. Refer to Figure 4.1 to see a drawing of the current NPS configuration. In the future, however, plans to enhance the NPS backbone network should allow the TR-LAN direct connection to the campus backbone.

A potential future enhancement plan for NPS is to connect the campus buildings with routers. The routers will operate at the network layer of the ISO seven layer model. This arrangement will also offer an upgrade capability to the Fiber Distributed Data Interface (FDDI) standard. Future campus plans indicate a strong desire to operate on



Note: This drawing shows the thick ethernet cable communication backbone of the NPS campus.

Figure 4.1 NPS Present Communications

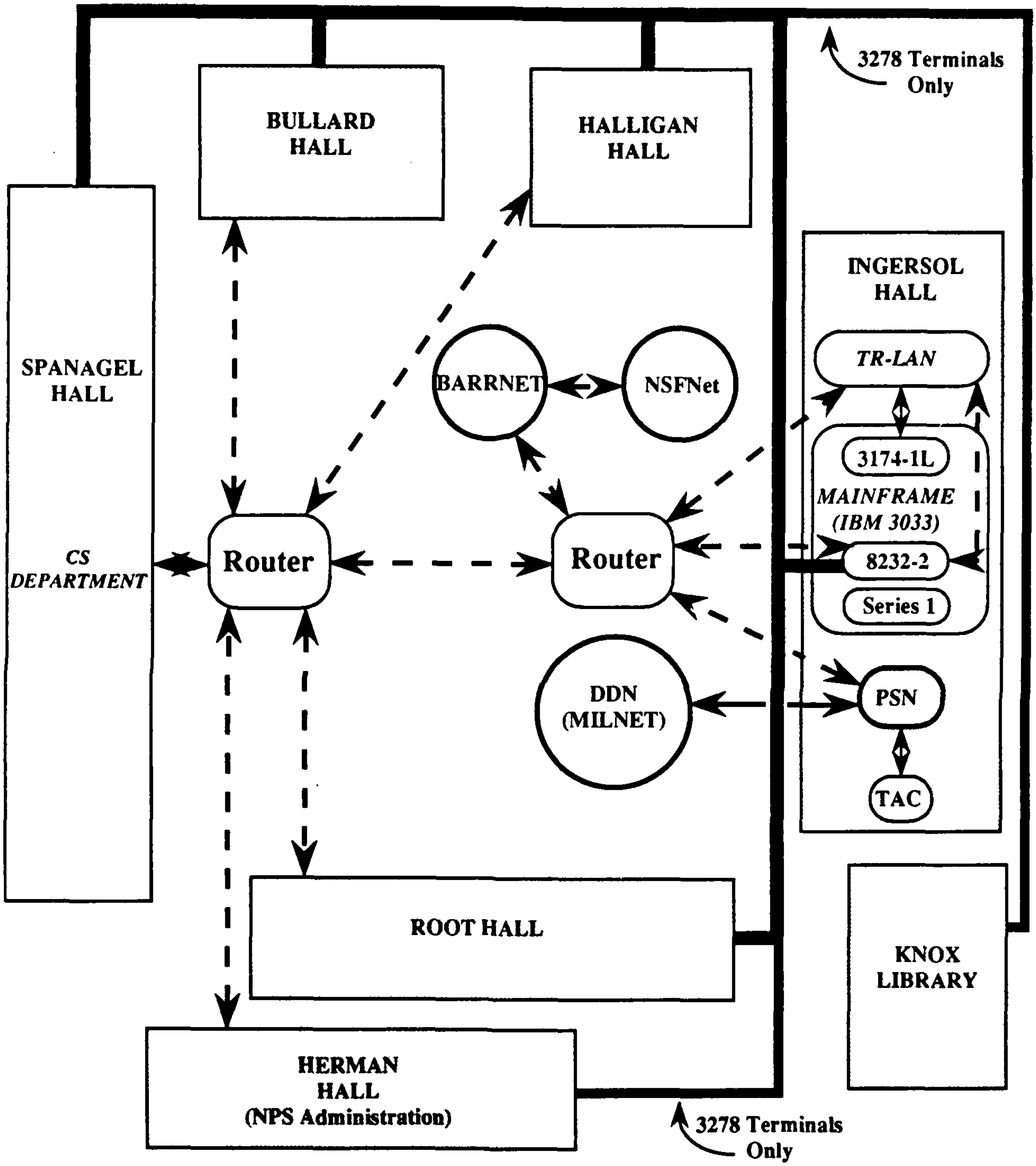
the FDDI.

The FDDI exploits the high speeds of fiber-optic ring by adapting as much of the IEEE 802.5 standards as possible. The main difference is that the token is never busy (taken by a node). Instead nodes attach messages to the end of the circulating transmission token and retrieve their transmitted message on the next token pass. It is possible for several messages to attach one behind another in this manner. With the fiber optic connections, the routers can be spaced up to two kilometers apart. This type of communication plan will provide a backbone communication system to unite diverse networks into a single system. This could include connecting to the Bay Area Regional Research Network (BARRNET) and the National Science Foundation Network (NSFnet).

The TR-LAN can attach to the NPS backbone by connecting to the 8232-2 Lan Channel Station. In the future, however, the TR-LAN could also connect to the NPS backbone through a router. This would provide the TR-LAN with the capability to exploit the router connections. In particular the TR-LAN would benefit from the future campus plan to connect a router directly to the PSN. Refer to Figure 4.2 for a drawing of a possible future NPS communications.

C. NPS CONNECTION TO THE DDN

There are two separate connections from NPS to PSN ports. The CS department has one connection using a dedicated line from Spanagel Hall to the PSN. The Computer Center has the other connection starting at the mainframe computer, to a Series 1 front-end processor, then to the PSN. These two PSN port connections cause a double charge to the NPS because of the Usage Sensitive Billing pricing structure. To save money future NPS communication goals include reducing to one port. The router is one



Note: This drawing shows a possible future router connection (illustrated using dashed lines) of the NPS campus. These routers will also provide a connection to the BARRNET communication network and leave NPS with only one port connection to the PSN.

Figure 4.2 Possible Future NPS Communications

device which could accept the two inputs from CS and CC and route the traffic to one PSN port. This router connection would also allow the TR-LAN a similar direct input to the PSN. Refer back to Figures 4.1 and 4.2 to see the planned changes in the way the NPS connects to the PSN.

D. CURRENT TR-LAN TO DDN CONNECTIONS

The TR-LAN now provides access to the DDN using two techniques--the TAC or indirectly using the mainframe host. It accomplishes these connections using either communication software and a modem or through 3270 Emulation. To connect to the DDN through the TAC a student selects a communication package (i.e., SMARTCOM II) on the TR-LAN. These packages provide the connection to the TAC access line in Monterey. This procedure, however, requires a student to have an account on a host such as the Information Sciences Institute (ISI) at the University of Southern California. It also requires the student to be familiar with commands needed to operate a personal computer, the communication software, and the host.

Users have two ways of connecting to the mainframe host to gain access to the DDN. One connection is through modems using communication software. This program allows the personal computer to act as a terminal on the mainframe. The other connection is through a 3270 Emulation package directly to the mainframe. The TR-LAN has a cable which connects directly to the mainframe computer (via a 3174-1L connection device). To use either of these connections, however, still requires the student to be familiar with personal computer commands, the communication and emulation packages, and the mainframe.

The third method to access the DDN, through a gateway, is not yet available on the TR-LAN. To access the DDN through a gateway the TR-LAN will need TCP/IP software and a connection to the IBM 8232-2 LAN Channel Station. The 8232-2 provides connectivity between an IBM System/370 and a non-SNA LAN environment. The TCP/IP provides the protocols and addressing to bypass the mainframe and enter the DDN backbone.

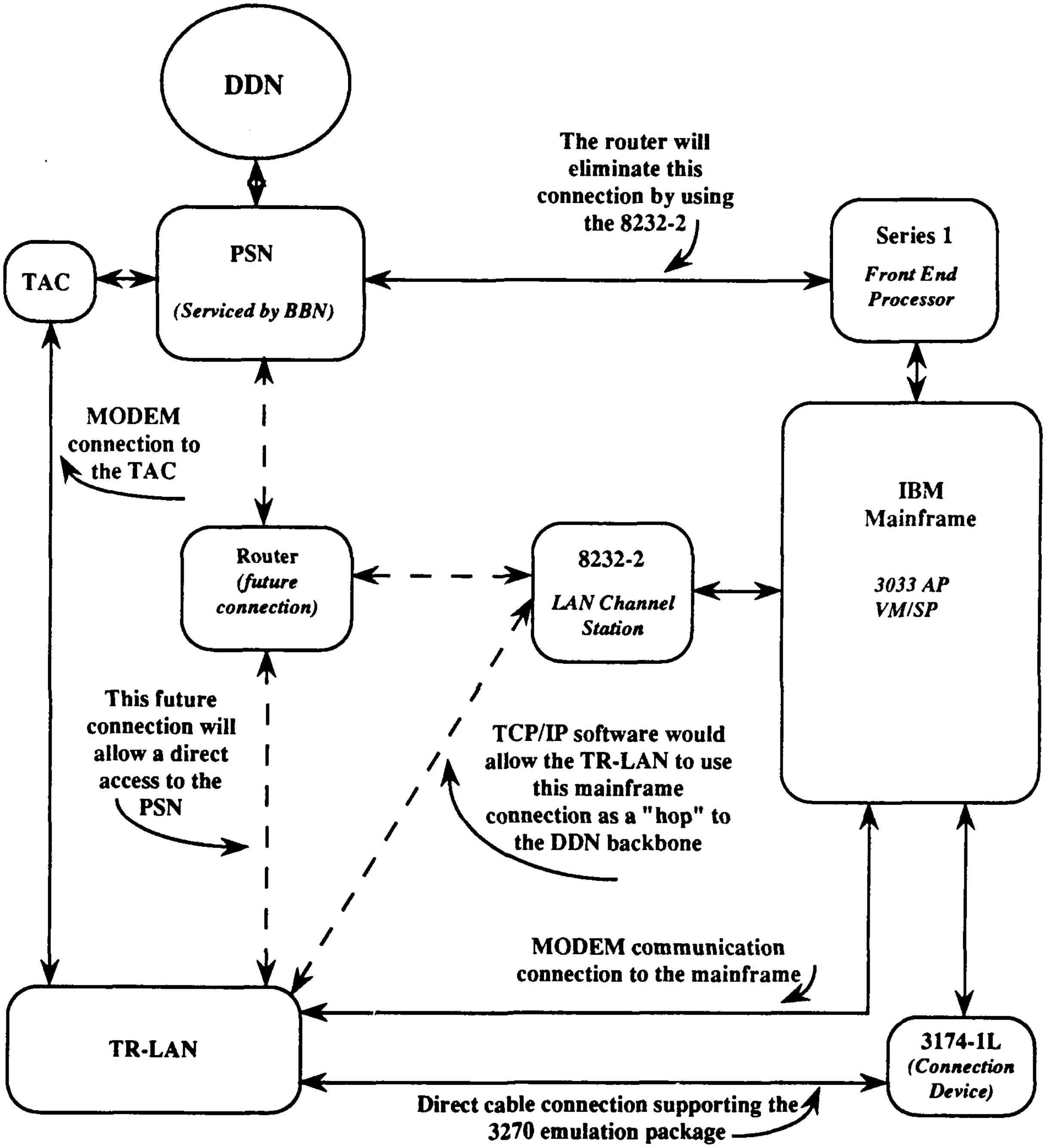
E. PHYSICAL CONNECTION FROM THE TR-LAN TO THE PSN

The location of the TR-LAN is on the second floor, north end, of Ingersol Hall. The location of the PSN is on the first floor, middle of the same building. Physically these two systems are not far from each other. A coaxial cable and a shielded twisted pair cable now spans these two systems. The coaxial cable, however, will not work in a token ring system. The coaxial cable will support networks such as ethernet. Therefore it is necessary to use the twisted pair to connect the TR-LAN. Initially the connection will go to an 8232-2 and later switch to the router. These connections will provide the TR-LAN with an access to the campus backbone and eventually a direct connection to the PSN. Refer to Figure 4.3 for an illustration of this connection.

F. SECURITY CONSIDERATIONS ON THE DDN

Host Administrators control access to the DDN using guidance from the DDN Program Management Office.

> Only users engaged in U.S. government business or applicable research, or directly involved in providing operations or system support for government-owned or government-sponsored computer communications equipment may use the DDN. (NIC 50001, 1985, p. 11)



Note: The methods the TR-LAN can (will) communicate on the DDN include:
1. Through the mainframe host (notice there are two ways to reach the mainframe).
2. Through the TAC and logging on to another host.
(3.) Using the future TCP/IP software to the 8232-2 as a "hop" to bypass the mainframe and enter the DDN backbone.
(4.) Using the future router as a direct connection (TR-LAN acting as a host) to the PSN.

Figure 4.3 Methods To Access The DDN

Host Administrators must not permit unauthorized access to the DDN. "Hosts that permit this type of access will be disconnected from the network." (NIC 50001, 1985, p. 11) The Administrative Sciences networks do not allow unauthorized access. The TR-LAN is in a physically secure room and the registration of students receiving the door lock combination helps to control access. The Host Administrator can further enforce DDN guidelines by making it clear to all users that:

> *Unauthorized use of the DDN is illegal.* Persons who break into government networks or use government computer resources without authorization will be prosecuted. (NIC 50001, 1985, p.11)

Perhaps another method to restrict usage to authorized personnel is through user input of a password before accessing the server TCP/IP directory.

G. CHAPTER SUMMARY

The TR-LAN is one network among many at NPS. To connect this network to the DDN requires a plan which considers the entire NPS communication system. This chapter reviewed the present and a possible future NPS connection plan to include how the TR-LAN can connect to the DDN. Besides making the TR-LAN-to-DDN connection, the network manager must also consider the security issues and authorization to access the DDN.

V. THE NEED FOR TCP/IP SOFTWARE

A. CHAPTER INTRODUCTION

The first three chapters provide a background to better understand the issues when purchasing new software. Knowing more about the DDN, the TR-LAN, and the future NPS communication plan will improve the TCP/IP software selection process. This chapter will look at TCP/IP, protocols, and what to look for and questions to ask when purchasing TCP/IP software.

B. WHAT IS TCP/IP

The addition of a TCP/IP software package to the TR-LAN is an important step *towards direct* communication to the DDN. The TCP/IP software enables communication between computers with different operating systems and architectures. A function of the TCP is to bundle and unbundle packets, manage the transmission of packets, sequence packets, and check for errors. The function of the IP is to keep track of node Internet addresses, determine routes for outgoing packets, and recognize incoming packets. These packets are known as IP datagrams.

The IP datagram is similar to the data frame on a physical network. There are header and data areas with the header containing source and destination addresses. The difference between an IP datagram and a frame, however, is the datagram contains Internetwork addresses. (Comer, 1988, p. 67)

Every network has an upperbound on the byte size of data per frame or datagram. To accommodate networks which have a small datagram limit, the Internet divides these packets into fragments. Each of these fragments will have a header similar to the packet header. (Comer, 1988, p. 68-69)

The DoD chose TCP/IP because it met the needs of military communication.

> Therefore, in December 1978 the DoD decreed that these two standards, the TCP and IP, would become official DoD protocol standards. The reason for this action was that both protocols had been devised to meet the essential military requirements of security, survivability, and reliability. (Selvaggi, 1983, p. 323, 324)

As a result these protocols have had several years of use and improvement. The impressive capabilities of these two protocols have made DDN quite successful. A brief description of the layers TCP/IP supports will help make these protocols easier to understand: (Comer, 1988, pp. 107-109)

1. Process/Application Layer

At this layer the users invoke applications programs to access the Internet. The FTP (MIL-STD-1780) is a simple application for transfer of ASCII, EBCDIC, and binary files. The TELNET (MIL-STD-1782) provides simple asynchronous terminal capacity and terminal emulation. The SMTP (MIL-STD-1781) provides a simple electronic mail facility.

2. Transport (Host-to-Host) Layer

The TCP (MIL-STD-1778) provides reliable end-to-end data transfer service and communication from one application to another. The data transmission is in a packet-switched environment.

3. Internet Layer

The IP (MIL-STD-1777) provides connectionless service for end systems to communicate across one or more networks and machine-to-machine communication. It is the standard for sending an IP datagram through the Internet.

The Internet Protocol is the lynch pin of the internet system. It is this protocol that insulates applications programs from needing to know specifics about the networks. (NIC 50005, 1985, p. 2-39)

4. Network Interface (Access) Layer

This layer accepts the internet protocol datagram and transmits them over a specific network. Another name is the Data Link Layer. This layer works with a variety of medium access methods (the TR-LAN uses the token ring).

5. Hardware Layer

This is the physical equipment which makes everything happen.

C. TCP/IP VERSUS OSI

Both Administrative Sciences (AS) and the Computer Center (CC) are evaluating TCP/IP software for network interconnection. These and other departments selected TCP/IP because it is required in order to interoperate with other hosts in the DDN. In addition, TCP/IP is very popular in the non-DDN community. All its capabilities (such as file transfer) provide communication between NPS departments where DDN access is not necessary. However, compatibility with OSI protocols has been mandated to begin in 1990. Therefore it is important that the software selected has an easy upgrade to OSI.

The National Institute of Standards and Technology (NIST) fostered the adoption of OSI protocols in the federal government. To organize the rapidly changing technology the NIST provided a Federal Information Processing Standard (FIPS) called the Government OSI Profile (GOSIP). GOSIP is an attempt to define a common set of data communications protocols. Starting in August 1990 federal agencies will need to cite standards set forth by GOSIP in all procurements of network products. There will undoubtedly be a coexistence of TCP/IP and OSI while this slow change to OSI occurs.

OSI equivalents to the TCP/IP include: FTAM for FTP, CCITT's X.400 or ISO's MOTIS for SMTP, TP 4 for TCP, INTERNET for IP, and possibly ISO's VTP for TELNET. "The main advantage of switching from TCP/IP to OSI is that the availability of commercial off-the-shelf products will reduce the costs of interoperability...." (Masud, 1989, p. 28) Message traffic is also much easier to send when everyone uses the same common protocols.

Although the OSI model sounds encouraging, there is a concern about compatibility. "If two sites each use the OSI model, there is no guarantee that they will be able to communicate with each other." (Tanenbaum, 1988, p. 36) This may be a result of the flexibility of various standards. To invest in a system which may not have compatibility with other locations could be disastrous.

> One of the problems with network standards as defined by IEEE, ISO, and CCITT is that they permit many options. If different vendors implement different options, connectivity cannot be achieved even though all vendors adhere to the standards. (Martin, 1989, p. 141)

Several organizations are making special efforts to use similar OSI protocols at various levels. One example is the Corporation for Open Systems (COS). This is a nonprofit organization of over 60 industry and government agencies. The goal of COS is to achieve a global conformance approach to OSI.

Another example of groups working to standardize OSI is the Manufacturing Automation Protocol (MAP) and the Technical and Office Protocols (TOP). The MAP, formed by General Motors, and TOP, sponsored by Boeing Company, "...worked closely together to ensure they would be fully compatible in the middle, and upper layers." (Tanenbaum, 1988, p. 38) Although their work is quite commendable, this need for a special effort is what turns a variety of potential users away. Many consumers desire a system that will work immediately with little effort.

A quick change to a new protocol, however, is unlikely.

> Few people who manage active networks will jump quickly from a tested and proven network to one that is still evolving. TCP/IP has a long and bright future, and best of all, it works well today. (Derfler, 1989, p. 261)

The TR-LAN will use TCP/IP because of the protocol's past success. There are many tools and software products which work well with TCP/IP. In addition, there is much documentation supporting the TCP/IP. The desire to avoid difficulties with a new protocol (such as OSI) outweighs the desire to be on the forefront of technology. Refer to Figure 5.1 to see the comparison among IEEE Standards, OSI, and DoD.

D. WHERE TO INSTALL TCP/IP

> There are two ways networked PCs can use TCP/IP. The first is to load a TCP/IP software module into every machine on the network. The second configuration uses one machine on the network as a gateway.... (Derfler, 1989, p. 248)

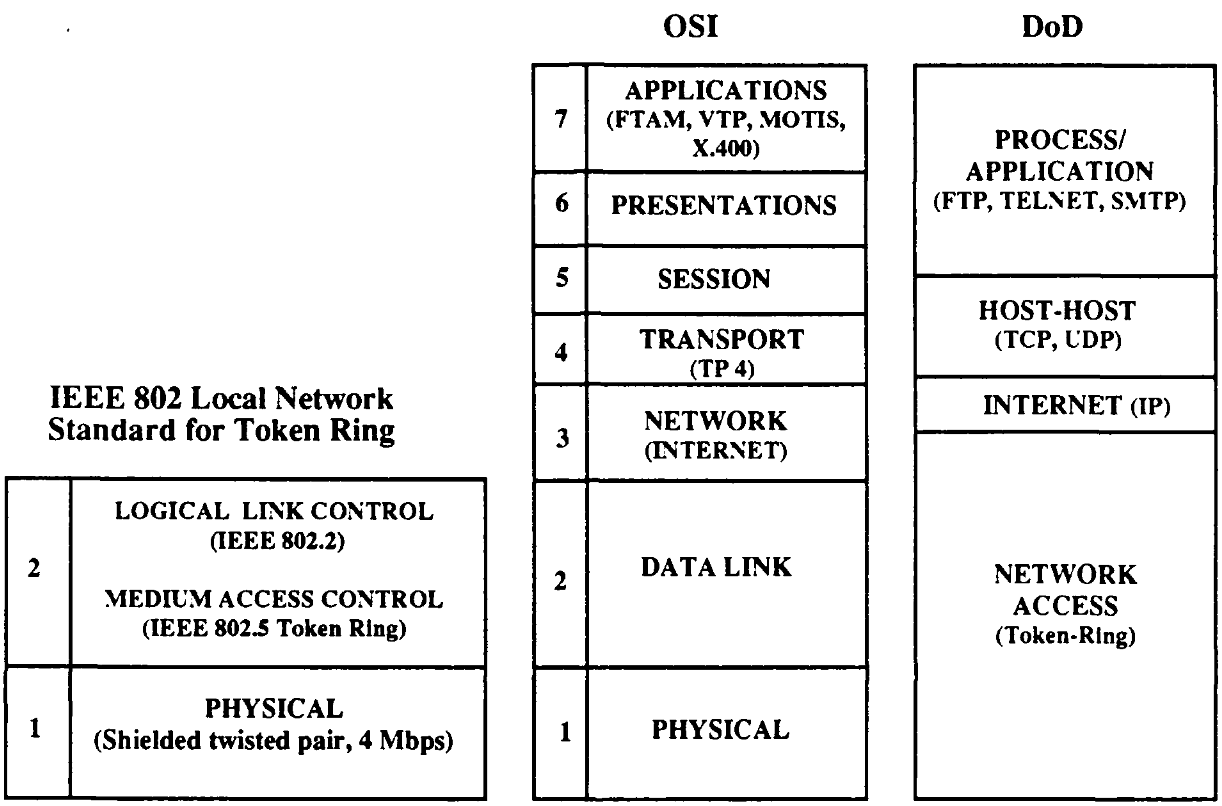
The TR-LAN would ideally use the second method. The server would both act as a gateway and share TCP/IP protocols with the user stations. This requires storing a program on the server and sharing it with the user computer only when the user desires to use TCP/IP. When the user computer requests and receives access to TCP/IP the computer is operating as a client and interacting with the server.

> Server processes await requests and perform an action based on the request. The action may include sending a response. Clients usually formulate a request, send it to the server, and then await a reply. (Comer, 1988, p. 213)

Refer to Figure 5.2 to see the protocol connections among the user, server, and the DDN.

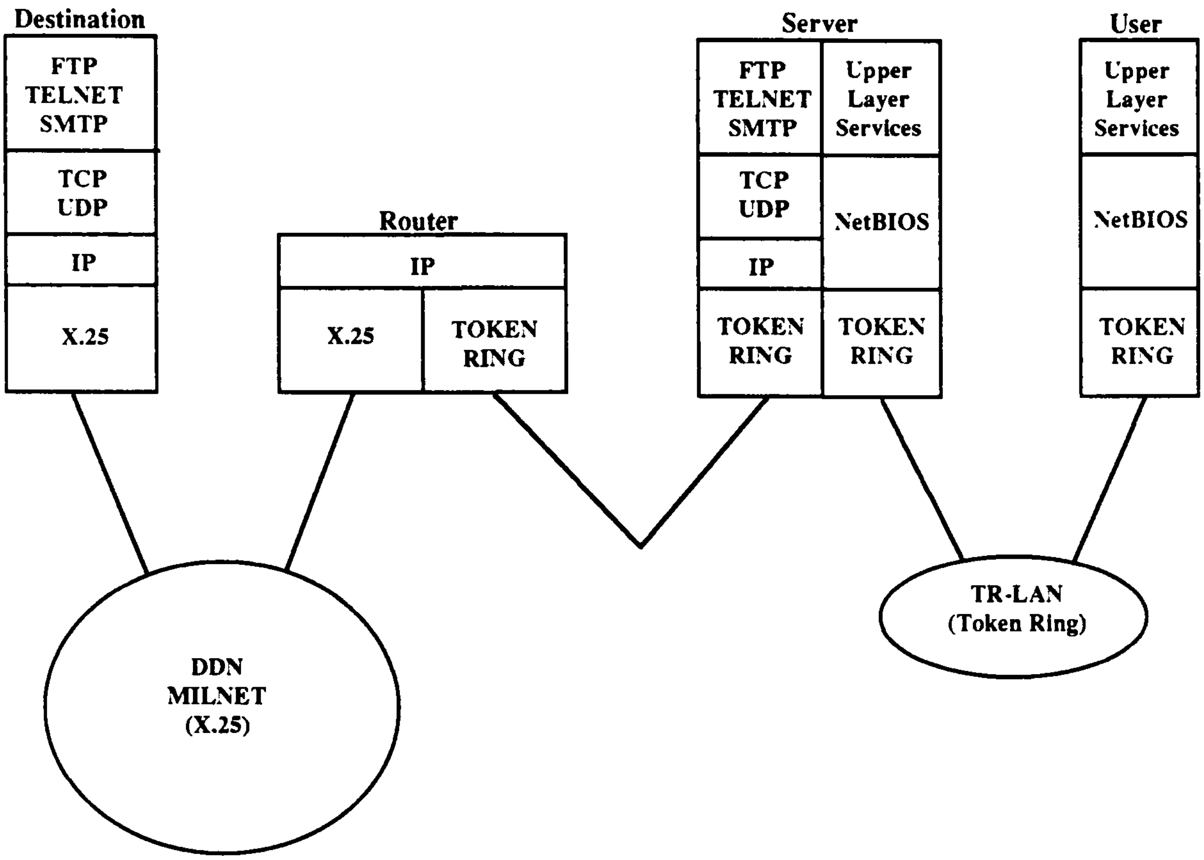
E. CONCERNS WITH VENDOR PRODUCTS

Obtaining unbiased information from vendors is often quite difficult. Not until installing the software do the small unforseen problems emerge. The 4th Interoperability



Note: This illustration shows the relationship among the IEEE Standard, OSI Layers, and the DoD communication (TCP/IP) architecture.

Figure 5.1 IEEE & OSI & DoD Communication Architectures



Note: This drawing illustrates the protocols required to provide the communication connection.

Figure 5.2 Protocols

Conference and Exhibition (INTEROP 89) in San Jose, California, provided an opportunity to question several different vendors on their products. These vendors offered a variety of solutions to the interoperability problem. The network manager, therefore, must beforehand identify items of concern. Then a trade-off can be made between what the network manager desires and the various TCP/IP software products available. The following sections will look at several of these trade-offs.

1. Token Ring Application

There are relatively few TCP/IP products available for the token ring. Although the token ring is quite popular, a variety of vendors are only in the testing phase or are not offering TCP/IP for the token ring. Vendors have many more products available for ethernet. Hence the network manager must be sure the TCP/IP software works on the token ring.

2. Interface With the Network's NetBIOS

The TR-LAN operates on an IBM PC LAN network operating system. The NetBIOS in this configuration is not compatible with some vendors' TCP/IP. "NetBIOS is a standard which specifies a means of creating virtual circuits and of transmitting and receiving point-to-point, multicast, and broadcast datagrams." (McLaughlin, 1989, p. 1) The problem of NetBIOS incompatibility is not unique to this evaluation of TCP/IP software. In other evaluations of TCP/IP software, similar problems occurred.

> Unfortunately, our tests show that the NetBIOS interfaces marketed by some of these companies do not play well together. We got a few of the NetBIOS products to exchange messages between different vendors' implementations, but only with a great deal of trial and error. (Derfler, 1989, p. 249)

Hence the network manager must be sure that the TCP/IP software selected is able to work on the IBM PC LAN Network operating system.

3. Handling IP Datagrams

Ideally the TCP/IP software would be able to send IP datagrams on the network. Depending on the size of the datagram, however, there may be a problem. The network operating system restriction on the maximum packet size may be too small. Additionally, the TCP/IP software may not be able to fragment the datagram. Therefore the network manager must verify with the TCP/IP vendor that the TR-LAN can handle the size of the IP datagram.

4. Putting TCP/IP in a Server

The desire is to use one copy of TCP/IP in the server rather than a copy in each user computer. The server would serve two functions. It would provide the TCP/IP software to the user stations upon request and it would act as a gateway to the Internet. When discussing this configuration with some vendors, however, there were four potential problems described.

The first problem was a concern about how to provide the TCP/IP software package to the user computer. Some vendors stated that the user computer must initially boot-up with TCP/IP. Then a server could send a protocol (such as FTP) to the user computer. This would require several undesirable changes on the TR-LAN. The second problem which some vendors mentioned was the lack of multitasking in DOS. There was also a concern about the limited RAM available on DOS computers. These vendors preferred to work with a larger server such as a SUN workstation operating with Unix.

The third problem mentioned was some TCP/IP software products offer protocols only in a client mode. Hence other software would operate the protocol as a server. This is not desirable because of the added problem of making a second software product work. The last problem was that some TCP/IP products were unable to provide Internet addresses to multiple users while operating in a server. The software could provide only one address. Again this is not desirable for the TR-LAN. These four potential problems would all have to be solved.

5. Use of Memory

A concern when purchasing any software is how much RAM it will need. The personal computer does not have much Random Access Memory available for applications. The TR-LAN computers have approximately 470K RAM available. This size, however, was adequate for the packages observed at INTEROP 89. If a network manager is looking for a product with many capabilities, however, the available RAM could easily become a problem.

If the size of the computer RAM is too small, an option for the network manager is to use a TCP/IP product which puts some functions in the network interface adapter board. The TCP/IP software will "...off-load a major part of the program to the board, leaving both memory time and processor time virtually untouched in the host system." (Derfler, 1989, p. 252) The end result is a TCP/IP product which uses less RAM. Not too many TCP/IP products, however, provide this capability.

6. TCP/IP Protocol Options

The variety of protocols offered in different TCP/IP products can be confusing. The LAN manager must decide what functions are important. This section will look at the required, recommended, and elective protocols as stated by the Internet Activities Board Official Protocol Standards, RFC 1130.

There are few protocols which must operate in all systems. The concern for the TR-LAN is to provide the protocols necessary for a host.

> It is expected that general purpose hosts will implement at least IP (including ICMP), TCP and UDP, Telnet, FTP, SMTP, Mail, and the Domain Name System (DNS). (Postel, 1989, p. 2)

The IP and ICMP protocols provide the network services between the third layer and fourth layers of the seven layer OSI model. The TCP and UDP protocols provide for the transport functions or layer four of the OSI model. The remainder of the protocols represent the fifth through seventh layers of the OSI model.

The protocols required for the host will provide the TR-LAN with some basic functions such as: send and receive files (the protocol FTP provides this), and act as a remote terminal (the protocol TELNET provides this). Acting as a remote terminal using TELNET provides to the user a "virtual" terminal. The computer acts as a terminal to whatever host it connects to. Ideally the user desires a full screen interaction with the host. In particular the cursor should be able to freely move about and inputs made in any location on the screen. This is especially desireable when working with graphics. On some operating systems, however, the user may view an entire screen but only have one line for input. This restriction is both annoying and sometimes difficult to work with.

Another protocol provided by the host is message service.

> An important use of computer networks is the support of electronic mail. In fact, one could attribute the success of the DARPA packet-switching research in large part to the availability of electronic mail facilities. (NIC 50005, 1985, p. 2-42)

A message service will operate on the SMTP protocol but there are other protocols available to do this service. One such protocol is the POP2.

> The intention of the Post Office Protocol Version 2 (POP2 is to allow a user's workstation to access mail from a mailbox server. It is expected that mail will be posted from the workstation to the mailbox server via the Simple Mail Transfer Protocol (SMTP). (Postel, 1985, p. 1, 2)

Vendors approach the ability to handle messages differently. Again there is a concern among some vendors that a computer acting as a mailbox needs to be the size of a Sun workstation. The network manager will need to ask the vendor how the TCP/IP software handles message service.

There are several categories of protocols defined by RFC 1130. This RFC assists the network manager by listing protocols beneficial to operating on the DDN. It also limits its recommendation to protocols which passed an evaluation criteria. The following protocol comments are from this RFC.

a. Required Protocols

The required protocols are Internet Protocol (IP) and Internet Control Message Protocol (ICMP). ICMP is a protocol for processing internet damage errors. These protocols are further explained by RFCs 791, 792, 919, 922, and 950. In addition, several other RFCs are necessary. These include RFC numbers 1009, 1010, 1122, and 1123. Note that "Protocol standards may be proposed by anyone in the Internet community, by writing and submitting an RFC." (Postel, 1989, p. 1) These protocols then go through various testing stages before they become required, recommended, or an elective.

b. Recommended Protocols

The recommended protocols include: Internet Group Multicast Protocol (RFC 1054)--specifies extensions required of a host to support multicasting or sending messages to a group of hosts; User Datagram Protocol (RFC 768)--provides a procedure to send messages to other programs with a minimum of mechanisms but no guarantee of delivery; Transmission Control Protocol (RFC 793); Domain Name System (RFC 1034 and 1035)--specifies domain style names; Telnet Protocol (RFC 854); File Transfer

Protocol (RFC 959); Simple Mail Transfer Protocol (RFC 821); Format of Electronic Mail Messages (RFC 822)--specifies a syntax for text messages; Content Type Header Field (RFC 1049)--specifies a message header which will show body content; Exterior Gateway Protocol (RFC 904)--used by gateways to advertise addresses in that system and Echo Protocol (RFC 862)--sends back to originating source the data received. The network manager will need to decide if these protocols are necessary.

c. *Elective Protocols*

The elective protocols include: NetBIOS service protocols (RFC 1001 and 1002)--defines a proposed standard to support NetBIOS; Discard Protocol (RFC 863)--throws away data it receives; Character Generator Protocol (RFC 864)--sends data without regard to the input; Quote of the Day Protocol (RFC 865)--sends a short message without regard to the input; Active Users Protocol (RFC 866)--sends a list of current active users on the host; Daytime Protocol (RFC 867)--sends a current date and time and Time Server Protocol (RFC 868)--sends time in seconds since midnight, 1 January, 1900. Another elective protocol specific to the TR-LAN is the Internet Protocol on IEEE 802 (RFC 1042). This protocol specifies a standard method to encapsulate IP and Address Resolution Protocols datagrams. Again, the network manager must decide if these protocols are worth their cost.

d. *Other Protocols*

A variety of other protocols exist. These protocols, however, are in the drafting stage, proposal stage, experimental stage or are historic (not likely to ever become a standard). Some of these protocols appear in the vendor's TCP/IP software. An example of two common protocols available is Finger and Ping. Finger displays information about users of a foreign host and Ping sends an echo request to a foreign host and displays the foreign host's response. Both of these protocols are useful and are a possible requirement of a network manager. The Internet Advisory Board keeps the entire protocol list updated. The network manager should review this list before a TCP/IP software purchase.

7. Acceptance by DDN

The network manager must also be careful which of the many TCP/IP software products will operate correctly on the DDN. A Defense Communication Agency certification which identifies the DDN approved software would be ideal, but this is not yet available.

> Currently, X.25 (up to level 3) is the only protocol being tested. There are plans to test TCP/IP and related application software at DCEC (the Defense Communications Engineering Center). (NIC 50002, 1989, p. 7)

An option available to the LAN manager is to ask the vendor if the TCP/IP software conforms with the industry protocol standards. A way to check this is through a program administered by the National Institute of Standards and Technology (NIST). The NIST provides a service to accredit independent laboratories to test manufacturers' products. This program is the National Voluntary Laboratory Accreditation Program (NVLAP). The network manager, therefore, can use the service of a NVLAP accredited laboratory by requesting that the vendor have the TCP/IP software tested. The network manager can also send the TCP/IP software to a laboratory for testing (for a fee).

There are two other methods the network manager can use to verify the proficiency of the protocols. According to the NIC on-line information service, the company of Bolt, Beranek, and Newman has authorization to provide the testing of TCP, IP, FTP, SMTP, and TELNET. The other approach is to put in writing that the software conform to its specifications.

> If a manufacturer claims that it is providing a 'standard' (whatever that is, 802.3, 802.4, or 802.5, for example), write a clause into the purchasing terms and conditions specifying that the equipment must work with other 'standard' implementations. (Madron, 1988, p. 212)

Whatever method chosen, the goal is to purchase a TCP/IP software product which works properly with the DDN.

8. Testing the TCP/IP

When the software selection narrows to a few products, the next step is to test the software. A variety of vendors will provide their software free for test evaluation. This is especially helpful if the test determines to reject the software. A rejection would occur if there is a need for major system changes in order for the software to operate. The network manager should use an off-net location for testing. A recommended approach is to use the same software and hardware configuration as the TR-LAN but on a smaller scale (perhaps only one server with two or three user computer stations). The testing of the TCP/IP software would then look for any problems. This approach would not affect the operation of the TR-LAN and would provide the necessary evaluation.

The goal is to use a test bed which does not have to remain operational. When TCP/IP software passes this test, the next step is to test the network with another system on the DDN. The test network could connect to the TR-LAN to make this test. Another test would be from the TR-LAN to the mainframe computer. In the future the TR-LAN will connect to the IBM 8232-2 LAN Channel Station. This will provide a means of transmission from the TR-LAN to the mainframe computer. In addition, this connection will allow the TR-LAN to access the DDN by using the mainframe as a gateway. Refer to Figure 5.3 for a checklist of issues to consider when evaluating TCP/IP software products.

	Yes	No
- Can it operate on the Token Ring?		
- Can it operate on IBM's NetBIOS?		
- Can it send IP datagrams on the LAN?		
- Can it send TCP/IP protocols from server to user computer?		
- Will it work on a PC server?		
- Does it provide both server and client capabilities (FTP, TELNET, SMTP)?		
- Can it provide Internet addressing to multiple user computers?		
- Will it work on the available RAM?		
- Does it provide all the required protocols?		
IP?		
ICMP?		
- Does it provide the recommended protocols?		
IGMP?		
UDP?		
TCP?		
DNS?		
TELNET?		
FTP?		
SMTP?		
Formats E-Mail?		
Content type of Header?		
EGP?		
Echo?		
- Does it provide full screen interaction on TELNET?		
- Can the mail service operate on a PC?		
- Does it provide the desired elective protocols?		
______?		
______?		
______?		
______?		
- Does it have DCA Certification?		
- Will the vendor provide the software for an on-site test evaluation?		
- Will it be easy to convert to OSI?		
- Other issues of concern: ______?		
______?		
______?		
______?		
______?		

Note: This checklist will provide the network manager with an initial set of questions to query vendors.

Figure 5.3 TCP/IP Software Evaluation Checklist

If the TR-LAN-to-mainframe computer test is successful, then the last test is the direct TR-LAN-to-DDN connection. Assuming the router is in operation, this connection will provide a direct connection to the PSN. When the TR-LAN successfully passes this test, the TR-LAN is then ready to operate as a host to the DDN.

F. CHAPTER SUMMARY

The selection of a software product is often not as easy as it seems. Often many trade-offs occur before deciding upon which software to purchase. This chapter reviewed TCP/IP and discussed several areas a network manager must consider before purchasing TCP/IP software. It emphasized the importance of maintaining the current network configuration. There was also an evaluation of which protocols will accomplish the job and which are just nice to have. Additionally, the manager will look at what protocols, if any, are certified by DCA. Despite a careful selection, however, there is still a need to test the software because of the many unforseen problems which can occur. It is best to find these problems on a test network instead of the actual system.

VI. SUMMARY

A. CONNECTING THE TR-LAN TO THE DDN

This paper outlined a variety of issues necessary to consider when configuring an IBM Token Ring LAN as a DDN host. A brief look at the key issues will summarize the thesis.

1. Benefit of Understanding the DDN

The Naval Postgraduate School educates hundreds of commissioned officers a year. The officer's understanding of the Defense Data Network is one of the many important subjects necessary to the future success of the military. The Administrative Sciences department provides five networks in support of the student education. One of these networks, the TR-LAN, can improve student education by a direct connection to the DDN. This direct connection will allow the TR-LAN to act as a host with local TCP/IP access, higher speed, and as a result better illustrate to the students the capability of the DDN.

2. IBM Token Ring LAN

The IBM Token Ring network is a proven LAN technology which provides a variety of advantages to the user. The token ring has a deterministic response time. This is an advantage over a technology such as ethernet which, with many users, can operate very slowly. The token ring user, therefore, can depend on reliable service despite the number of users. The TR-LAN's dependability is an important reason for its selection as the network to access the DDN. The TR-LAN now offers a variety of software products to users. This environment is also an excellent representation of hardware common to the military.

3. NPS to DDN Connection

The Naval Postgraduate School is making plans to enhance its campus computer network. The proposals include a desire to upgrade to FDDI. The future plan also provides for only one access to the PSN ports--a saving of money. These NPS plans are quite helpful to the TR-LAN goals. The planned installation of routers is ideal for connecting the TR-LAN to the DDN. By keeping abreast of the NPS plans, the network manager will be able to capitalize on all the improvements made to the campus network. It is apparent that the Administrative Sciences department is making great strides to be as up-to-date as possible with network technology.

4. Rank Objectives

The variety of capabilities a network can provide is almost endless. Because of a limited staff, however, any new software added must be easy to install, maintain, and use. The network manager must rank the concerns which are the most important to the users. There are several key issues to consider because all desires cannot be achieved simultaneously. The network manager must decide how important it is to keep the present equipment and configuration.

If the decision is to keep the present configuration intact, the TCP/IP software must be capable of operating on a token ring network, on the NetBIOS of an IBM PC LAN Network operating system, on a personal computer server, with both server and client capabilities, and within the RAM memory constraints of the user computers. Also, with the TR-LAN acting as a host, TCP/IP protocols will be required. An analysis of instructional needs will indicate additional protocols to request. As a minimum, however, the TR-LAN should have the protocols required for a host and the capability to provide several of the most common functions such as FTP, TELNET, and SMTP. These protocols should be in accordance with the military standards and certified by DCA when possible.

5. Do TCP/IP Software Testing

The test of TCP/IP software would begin in an off-net location to avoid the possibility of closing down the network. When the test is successful then the next step is to test with another system. One possible test is TR-LAN to mainframe communication. When this test is successful, the final test is to the DDN.

B. OPERATING AS A HOST

Using the TR-LAN as a host to the DDN requires a considerable amount of planning and preparation. The network manager can refer to the variety of issues covered in this paper when evaluating TCP/IP software. Then, with TR-LAN-to-DDN connectivity, students will be able to experience and appreciate the power of the DDN with a network which uses hardware and protocols common in the military. Later, when the need arises, these students can use this tr ing to enhance their military performance.

GLOSSARY

ARPANET	=	The Advanced Research Projects Agency Network. A member of the DDN. A packet-switched network.
AS	=	Administrative Sciences. A NPS academic department.
ASCII	=	American Standard Code for Information Interchange. A seven-bit-plus parity code.
AT	=	Introduced in 1984, this is a personal computer based on the Intel 80286 microprocessor. A registered trademark of the IBM Corporation.
Backbone	=	A common channel that connects dispersed networks.
Bandwidth	=	The difference in herz (cycles per second) between the highest and lowest frequencies of a frequency spectrum.
BARRNET	=	Bay Area Regional Research Network. Located in San Francisco, California.
Baseband	=	Network communication system that transmits data at its original frequencies.
BBN	=	Bolt, Beranek, and Newman, Incorporated. A company from Cambridge, Massachusetts which makes and supports the PSN.
Bps	=	Bits per second.
Broadband	=	A type of network which uses modulated communication and frequency division multiplexing.
Cache	=	A special memory faster and smaller than conventional RAM for holding frequently referred to data.
CC	=	Computer Center. Located in Ingersol Hall at the NPS.
CCITT	=	Consultative Committee on International Telegraph and Telephone. A standards-making organization for world-wide telecommunications.
COS	=	Corporation for Open Systems. Their purpose is to evaluate network standards.

CPU	=	Central Processing Unit.
CSMA/CD	=	Carrier-Sense Multiple Access with Collision Detection. A network access control method.
DARPA	=	Defense Advanced Research Projects Agency. A member of the DoD. Sets policy for the ARPANET.
Datagram	=	A self-contained package of data that includes routing information.
DCA	=	The Defense Communications Agency. A government agency responsible for the DDN.
DCEC	=	Defense Communications Engineering Center.
DDN	=	The Defense Data Network. A packet-switching network.
DNS	=	Domain Name System. The Internet name hierarchy.
DoD	=	The Department of Defense.
DOS	=	Disk Operating System.
EBCDIC	=	Extended Binary Coded Decimal Interchange Code. Based on the coding system using eight bit bytes.
EGA	=	Enhanced Graphics Adapter. Produces an array of 640 by 350 pixels.
EGP	=	Exterior Gateway Protocol. The service gateways use to determine what gateways they can reach.
Ethernet	=	Popular network topology, invented by Xerox which uses CSMA/CD.
FDDI	=	Fiber Distributed Data Interface. A high speed transmission fiber optic, token ring network.
FIPS	=	Federal Information Processing Standards.
FTAM	=	File Transfer, Access, and Management. An OSI standard for network file exchange and management services.
FTP	=	File Transfer Protocol. Used to transfer files on the DDN.
FY	=	Fiscal Year.
Gateway	=	A device which connects two dissimilar networks.

GOSIP	=	Government Open Systems Interconnection Profile. A government profile that outlines a policy for converting to OSI.
IBM	=	International Business Machines.
ICMP	=	Internet Control Message Protocol. Messages exchanged by IP modules to report errors and control messages.
IEEE	=	Institute of Electrical and Electronics Engineers.
IGMP	=	Internet Group Multicast Protocol.
IN	=	Ingersol Hall. An academic building at NPS.
internet	=	Collection of packet switching networks interconnected by gateways.
Internet	=	Cooperative network including ARPANET, MILNET, and NSFnet using TCP/IP.
IP	=	Internet Protocol. A DoD standard.
IP Datagram	=	Packet of information on the Internet including source, destination, and data.
ISO	=	*International Standards Organization.* Establishes international standards for computer network architecture.
LAN	=	Local Area Network. A data communication network operating at a high speed over short distances.
LLC	=	Logical Link Control. A part of the IEEE 802 local network standards.
LOTUS 1-2-3	=	A spreadsheet software program by Lotus Development Corporation.
MAC	=	Medium Access Control. A part of the IEEE 802 local network standards.
MAP	=	Manufacturing Automation Protocol. Sponsored by General Motors Corporation and based on OSI.
MAU	=	Multistation Access Unit. A wiring concentrator on a token ring network.
Mbps	=	Megabits per second. Million of bits per second.
MHz	=	Megaherz. One million herz (cycles per second).

Microprocessor = The central processing unit of a microcomputer.

MIL = Military.

MILNET = Military Network. An unclassified network which is a part of DDN.

MODEM = MODulator/DEModuiator. Modulates and demodulates signals transmitted over a communication facility.

MOTIS = Message-Oriented Text Interchange System.

MS DOS = Microsoft Disk Operating System.

NEC = NEC Home Electronics (U.S.A.) Incorporated.

NetBIOS = Network Basic Input Output System. Standard interface to networks on IBM PCs and clones.

NIC = Network Information Center. Located at Stanford Research International in Menlo Park, California.

NIST = National Institute of Standards and Technology. Formerly known as the National Bureau of Standards.

NMC = Network Monitoring Center.

NOSC = Naval Ocean Systems Center. Located in San Diego, California. Provides the NPS back-up name server.

NPS = Naval Postgraduate School. Located in Monterey, California.

NSFnet = National Science Foundation Network.

NVLAP = National Voluntary Laboratory Accreditation Program.

OSD = Office of the Secretary of Defense.

OSI = Open Systems Interconnection. The ISO's seven layer model.

PC = Personal Computer.

PMO = Program Management Office.

POP2 = Post Office Protocol, Version 2.

Protocol = Description of message formats and rules machines must use to exchange messages.

PSN = Packet Switch Node. A packet switch formerly called IMP in the DDN.

RAM = Random Access Memory. A semiconductor memory device.

RFC = Request For Comment. The name of a series of notes available from the NIC.

Router = A device that makes decisions about which path network traffic will follow.

SIM/PC = A communications software package by Simware, Incorporated. Provides for a PC terminal emulation of a 3278 keyboard for access to IBM mainframes.

SMTP = Simple Mail Transfer Protocol. A DoD electronic mail protocol.

SMARTCOM II = A communications software package by Hayes Microcomputer Products, Incorporated. Manages remote communication for microcomputers to include access to the mainframe computer.

SNA = System Network Architecture. Architecture and class of network products offered by IBM.

STD = Standard.

SUN = SUN Microsystems, Incorporated.

TAC = Terminal Access Controller. A computer that provides dial-up terminal access to the DDN.

TCP = Transmission Control Protocol.

TCP/IP = Transmission Control Protocol / Internetwork Protocol. DoD protocols.

TELNET = Telecommunications Network Protocol. A DoD standard for remote terminal access.

TOP = Technical and Office Protocol. Initiated by Boeing Corporation and based on OSI Standards.

Topology = The physical layout of computers in a network.

TP 4 = Transportation Protocol Class 4. An OSI standard internetwork protocol.

TR-LAN	=	The IBM Token Ring LAN in Ingersol Hall, room 224.
UDP	=	User Datagram Protocol. Provides datagram service to application programs.
UNIX	=	An operating system with a registered trademark of AT&T.
USB	=	Usage Sensitive Billing.
VTP	=	Virtual Terminal Protocol. An ISO standard.
WHOIS	=	Program to access NIC's database of registered users.
WordPerfect	=	Word processing Program Versions 4.2 and 5.0 by WordPerfect Corporation.
XT	=	Introduced in 1983, this is a personal computer based on the Intel 8088 microprocessor. A registered trademark of IBM Corporation.
X.25	=	A network access standard for connecting stations to packet-switched networks specified by CCITT.
X.400	=	Family of standards for Message Handling Systems, developed by CCITT.
1DIR	=	File management and menuing system by Bourbaki Inc.
3174-1L	=	IBM device for connecting remote terminals to mainframes.
3270	=	IBM PC 3270 Emulation Program Version 3.00. Provides for a PC terminal emulation of a 3278 terminal for access to an IBM mainframe computer.
3278	=	Terminal which provides access to the IBM System/370 mainframe computer.
8232-2	=	IBM 8232-2 LAN Channel Station Model 2. A device for communicating between an IBM System/370 and various networks.

LIST OF REFERENCES

Berry, Paul, Operating the IBM PC Networks, SYBEX Inc., 1986.

Cerf, Vinton G., and Lyons, Robert E., "Military Requirements for Packet-Switched Networks and their Implications for Protocol Standardization," Computer Networks, vol 7, no. 5, October 1983.

Clark, David D., "Name, Addresses, Ports, and Routes," Request For Comments 814, July, 1982.

Comer, Douglas E., Internetworking with TCP/IP: Principles, Protocols, and Architecture, Prentice-Hall, Inc., 1988.

Defense Communications Agency, NIC 50001, DDN New Users Guide, by Stephen C. Dennet and others, 1985.

Defense Communications Agency, NIC 50002, DDN Protocol Implementations and Vendors Guide, editors Nancy Dorio and others, February 1989.

Defense Communications Agency, NIC 50005, DDN Protocol Handbook, vol 2, December 1985.

Derfler Jr., Frank J., "TCP/IP for Multiplatform Networking," PC Magazine, vol 8, no. 12, June 27, 1989.

Madron, Thomas W., Local Area Networks, The Second Generation, John Wiley & Sons, Inc., 1988.

Martin, James, Local Area Networks Architectures and Implementations, Prentice-Hall, 1989.

Masud, S. A., "DoD to Require OSI Before FIPS Goes into Effect," Government Computer News, vol 8, no. 1, January 9, 1989.

McLaughlin, III, L., "A Standard for the Transmission of IP Datagrams over NetBIOS Networks," Request For Comments 1088, February, 1989.

McNamara, Kathryn, "Defense Data Networks Usage Sensitive Billing," M. S. Thesis, Naval Postgraduate School, Monterey, California, June 1986.

Naval Postgraduate School, Course Catalog Academic Year 1989, U.S. Government Printing Office, 1988.

Postel, Jon, "Internet Activities Board Official Protocol Standards," Request For Comment 1130, October 1989.

Postel, Jon, and others, "Post Office Protocol - Version 2," Request For Comment 937, February 1985.

Schneidewind, Norman F., "Interconnecting Local Networks to Long-Distance Networks," Computer, vol 16, no. 9, August 1983.

Selvaggi, Philip S., "The Department of Defense Data Protocol Standardization Program," Computer Networks, vol 7, no. 5, October 1983.

Stallings, William, Data and Computer Communications, 2d ed., Macmillan Publishing Company, 1988.

Tanenbaum, Andrew S., Computer Networks, 2d ed., Prentice-Hall, Inc., 1988.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Department Chairman, Code AS Naval Postgraduate School Monterey, California 93943-5000	1
4.	Computer Technology Code 37 Naval Postgraduate School Monterey, California 93943-5000	1
5.	Prof. Norman F. Schneidewind, Code AS/Ss Administrative Sciences Department Naval Postgraduate School Monterey, California 93943-5000	1
6.	Mr. Leon R. Sahlman, Code AS/Sl Administrative Sciences Department Naval Postgraduate School Monterey, California 93943-5000	1
7.	United States Military Academy Department of Electrical Engineering and Computer Science ATTN: CPT Greg S. Rassatt West Point, New York 10996-1787	2
8.	Prof. Barry Frew, Code 014 Director of Computer & Information Services Naval Postgraduate School Monterey, California 93943-5000	2