2

NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

ARCHITECTURE SELECTION
FOR
DEPLOYABLE LOCAL AREA NETWORKS

by

David Patrick Hunninghake
and
Bradley Keith Ashley

March, 1990

Thesis Advisor: T.A. Schwendtner

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

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 39

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 NO.

11. TITLE *(Include Security Classification)*
ARCHITECTURE SELECTION FOR DEPLOYABLE LOCAL AREA NETWORKS (UNCLASSIFIED)

12. PERSONAL AUTHOR(S)
Hunninghake, David P. and Ashley, Bradley K.

13a. TYPE OF REPORT
Master's Thesis

13b. TIME COVERED
FROM ________ TO ______

14. DATE OF REPORT *(Year, Month, Day)*
1990 March

15. PAGE COUNT
115

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

17. COSATI CODES

FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
Local Area Networks

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*
The United States Air Forces' Headquarters Tactical Air Command (TAC) Communications-Computers staff provides guidance to TAC functional users on the procurement and use of Local Area Networks (LANs) in a deployed environment. Deployable systems may be defined as those systems designed to be transported away from their normal base for semi-fixed or mobile tactical missions. Major deployed LAN concerns include issues related to transmission media, protocols, topology, and transportability/survivability. The objectives of this thesis are to: (1) review the basics of LAN technology, (2) identify unique requirements of deployed LANs, (3) make recommendations for the proper selection of deployable LAN architectures.

This thesis presents many of the complex and interrelated technical factors of LANs such as media, topology, and protocols. Selecting the proper LAN architecture cannot be done by using a simple algorithm. Many factors must be evaluated, as a whole, by an expert in the technology. There is no single answer to all military deployed LAN requirements; however, some general recommendations can be made. The most important recommendation made is to rely on a LAN expert from design through fielding of a deployable LAN.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL
Thomas A. Schwendtner, Capt, USAF

22b. TELEPHONE *(Include Area Code)*
(408) 646-2772

22c. OFFICE SYMBOL
EC/SC

DD Form 1473, JUN 86 *Previous editions are obsolete.*

Approved for public release; distribution is unlimited.

Architecture Selection for Deployable Local Area Networks

by

David P. Hunninghake
Captain, United States Air Force
B.S., Washburn University

and

Bradley K. Ashley
Captain, United States Air Force
B.S., University of Georgia
M.S., Golden Gate University

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL

March 1990

Author: David P. Hunninghake
David P. Hunninghake

Author: Bradley K. Ashley
Bradley K. Ashley

Approved by: Thomas A. Schwendtner
T.A. Schwendtner, Thesis Advisor

Tung Bui
Tung Bui, Second Reader

Carl R. Jones, Chairman
Command, Control, and Communications Academic Group

ABSTRACT

The United States Air Forces' Headquarters Tactical Air Command (TAC) Communications-Computers staff provides guidance to TAC functional users on the procurement and use of Local Area Networks (LANs) in a deployed environment. Deployable systems may be defined as those systems designed to be transported away from their normal base for semi-fixed or mobile tactical missions. Major deployed LAN concerns include issues related to transmission media, protocols, topology, and transportability/survivability. The objectives of this thesis are to: (1) review the basics of LAN technology, (2) identify unique requirements of deployed LANs, (3) make recommendations for the proper selection of deployable LAN architectures.

This thesis presents many of the complex and interrelated technical factors of LANs such as media, topology, and protocols. Selecting the proper LAN architecture cannot be done by using a simple algorithm. Many factors must be evaluated, as a whole, by an expert in the technology. There is no single answer to all military deployed LAN requirements; however, some general recommendations can be made. The most important recommendation made is to rely on a LAN expert from design through fielding of a deployable LAN.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

Special thanks deserve to be given to the following people and organizations for their time, inputs, and encouragement during this research effort:

Doug Butler, Captain, USAF

Mr. Jerry Blair, Idaho National Engineering Lab (INEL)

1912th Communications Group LAN Office, Langley Air Force Base

Tom Schwendtner, Captain, USAF, NPS Faculty

Mr. Tung Bui, NPS Faculty

Headquarters Tactical Air Command/SCL/SCX/SCU Offices

The original concept for this thesis and a great deal of support and encouragement throughout its accomplishment came from Colonel George Naddra, USAF (HQ Tactical Air Command/SCL). We thank him for his never ending words of wisdom, confidence, and support.

We are extremely grateful to our wives Patti Hunninghake and Jody Ashley for all their support, advice, and encouragements. We could not have done it without you.

I. INTRODUCTION

A. HISTORY

Dependence on computers and networks to perform tasks, make critical calculations, store, and manipulate data has become a reality in today's Air Force. Deployable systems may be defined as those systems designed to be transported away from their normal base for semi-fixed or mobile tactical missions. This thesis focuses on the deployable network concerns of Tactical Air Command (TAC), an Air Force Major Command.

TAC should have standards for deployed LANs before further expansion of their use occurs. TAC deployments cover large geographical regions with many operating locations and units worldwide. This thesis is the first in-depth study focusing primarily on TAC's requirements for deployable LANs.

Many TAC functional users have grown to rely on their computers and networks while in-garrison (office environment). These users include wing operations, command and control, logistics, and intelligence units. Several of these areas plan to utilize LANs in a deployed environment. These computer systems usually perform very specific tasks for a small number of users. These systems rely on local information transfer between deployed sites or from such sites to fixed locations. Computer networks cannot be allowed to be the weak link in the command and control necessary to accomplish the mission. Transportability, immunity to dust, temperature extremes, humidity, and chemical agents must all be carefully considered when selecting a LAN for a deployed environment.

Networks can be force multipliers or an Achilles' heel if proper planning and correct system selection are not accomplished. When deciding which network architecture is best for TAC, user requirements, as well as technical, physical, and economic factors are involved. This thesis will discuss the many important aspects of LANs, the TAC users' requirements, and recommend a standard architecture that is best suited for TAC deployed users.

B. THE RESEARCH QUESTION

In this thesis, the authors will discuss aspects of local area networks necessary to make informed decisions when selecting a LAN for use in a deployed environment. The authors will identify general requirements of all deployed LANs, as well as the concerns associated with selecting a deployable LAN architecture. Various standard LAN architectures will be discussed regarding performance under varying conditions, such as increased number of users and increased traffic load.

C. SCOPE OF STUDY

The study for this thesis effort is confined to the requirements of TAC deployed LAN users. Specific commercial packages are not addressed. However, general LAN characteristics are discussed in detail. Advantages, disadvantages of various LAN characteristics, deployability concerns, and the performance of various LAN standards under changing conditions are discussed for many aspects of LANs.

D. SUMMARY OF FINDINGS

There is no single magical answer to all military deployed LAN requirements; however, the following is a summary of some general conclusions and recommendations. Many of the military's current problems of standardization will be simplified by the ongoing transition from DoD protocols to International Standards Organization (ISO) and Institute of Electrical and Electronics Engineers (IEEE) standards. The combination of using industry standards and the use of gateways will give all military LANs the potential to be interconnected.

Careful planning and analysis of today's and tomorrow's requirements must also be considered. The military must consider size, weight, security, and interference immunity to be critical factors necessary in tomorrow's battlefield transmission media. Each of these factors suggest fiber optics will be the deployed LAN medium choice for the future. A system which works well in the fixed office environment may not be optimal for the deployed environment.

Redundancy and lack of single point of failure are critical in the design of deployable LANs. The token ring is the least sensitive protocol to workload, message size, and the number of nodes on the network. However, double rings should be used to take care of potential reliability problems.

A qualified LAN/computer/communications expert must be intimately involved with the project at every stage. Significant savings can be attained by designing the system smart from the beginning. The single magical LAN which meets everyone's needs will always elude us. Users' needs vary a great deal from system to system. General purpose or all encompassing LANs are not efficient solutions to varying deployed situations. The answer to this problem is for operations staffs to rely on the LAN expertise available to assist in transforming user requirements into the proper system design parameters. The communications/computer support staffs have the expertise to assist users in making the proper LAN decisions.

E. ORGANIZATION OF STUDY

Chapter II defines the Tactical Air Command (TAC) users' missions and deployed LAN environments. Various deployability concerns are defined and discussed. Further technical detail is provided in Chapter III and the appendices.

Chapter III provides a general overview of LANs. Various aspects of LAN technology are discussed in detail such as: transmission media, signalling techniques, topology, network access/protocols, gateways, bridges, and standards for communication protocols. This chapter provides a review of terms and concepts that are used throughout the remainder of the thesis. Further details on these subjects are presented in Appendices A and B.

Chapter IV provides a detailed analysis of how LANs perform under multiple varying conditions. The standardized protocols are also discussed with respect to how they perform under various loads.

Chapter V summarizes key issues of concern for LAN users. It also presents general recommendations for TAC LAN users and planners when selecting a LAN for deployments.

Appendix A presents general background material on LAN media. Appendix B presents details on several of the more widely used LAN standards.

II. TACTICAL AIR COMMAND REQUIREMENTS

A. MISSIONS

The mission of TAC is to organize, train, equip, and maintain combat-ready forces capable of rapid deployment and employment and to ensure that strategic air defense forces are ready to meet the challenges of peacetime air sovereignty and wartime air defense. TAC active, reserve, and national guard forces comprise more than 4,000 aircraft and over 188,000 people. Joint service responsibilities include providing the Air Force component of the US Atlantic Command, US Central Command, and US Southern Command. The TAC commander is dual-hatted as Major Command Commander and as Commander in Chief, US Air Forces Atlantic. The TAC Commander is responsible for readiness and related deployment planning for assigned or programmed forces to reinforce unified commands and NATO. (Air Force Magazine, pp. 90-91, May 1989)

The Tactical Air Control Center (TACC) provides the TAC commander and his senior staff with the capability to supervise and manage the activities of assigned or attached forces, and to monitor the actions of both friendly and enemy forces. As a top echelon command and control node, the TACC requires the use of a LAN for deployed support. The TACC has many functions. The flight management function formalizes the air mission schedule and monitors the progress of each mission. Any deviation from the scheduled mission must be relayed to the appropriate organizations. The battle management functions are those actions taken in direct response to the presence of enemy forces. Timely and accurate dissemination of information regarding the tactical situation is critical to ensure proper employment of tactical air assets. The systems management function includes the management of the airspace, all communications, and timely exchange of command and control information. The command and control information includes tasking orders, orders of battle, scrambles, and alerts. (TAC Regulation 55-45, p.4-1)

The role of LANs in providing effective command and control has increased in the deployed arena over the past several years. Tactical LANs provide essential connectivity between nodes transferring critical data necessary to represent the status of the current tactical battle. Nodes perform functions such as collection, processing, and dissemination of intelligence data, logistics support, flight management, battle management and systems management. These functions require guaranteed access to the network and assured delivery of large volumes of data in a timely manner.

B. ENVIRONMENT

The warfare environment of the future will have flexible, highly mobile air and ground forces linked with effective command and control structures. Physical threats include:

- guided bombs, missiles
- gravity bombs
- nuclear weapons
- chemical weapons
- biological weapons.

Electronic threats include:

- jammers
- deceivers, chaff
- electromagnetic pulse (EMP).

Due to these threats, future tactical systems must be transportable, secure, interoperable, reliable, flexible, mobile, and modular.

Deployed LANs in TAC do not typically operate on the move in vans or trucks. They are usually housed in expandable shelters at semi-fixed tactical locations to support air commanders in central command and control nodes. TAC LANs are required to deploy into rugged and hostile environments worldwide. LANs provide the high data rates, easy use, and functionality necessary to simplify the increasingly complex air support missions of TAC deployed units.

C. DEPLOYABILITY CONCERNS

1. Survivability

Survivability refers to the ability of the LAN to continue to operate during the adverse atmospheric and physical conditions associated with military deployments. Combat operations require rugged survivable electronic components that can easily be moved from one location to another. When a fault occurs, rapid detection, isolation, and repair are imperative. Single points of failure should be avoided whenever possible. (TAC Pamphlet 700-12, p. 6)

2. Capacity

Capacity is the amount of data that a medium can transmit at any one time and is related to the available bandwidth. (Lundquist, p. 9) Routine capacity requirements may be low. However, during deployment and as activity increases, the necessary channel capacity may greatly increase. If this is the case, worst case capacity requirements must be used when selecting a deployable LAN.

3. Connectivity

Connectivity is concerned with the ease of assembling the LAN in the deployed environment. Special training, procedures, and tools required must be considered. Connectivity also refers to the ability of the LAN to connect to other LANs. Bridges and gateways have been developed to facilitate connectivity. (TAC Pamphlet 700-12, p. 6)

4. Flexibility

Flexibility is the feature of a network allowing easy modification to its configuration or applications (Lundquist, p. 53). Flexibility is required to meet changing situations and diversified operations with a minimum of disruption or delay. Flexibility is critical because of the uncertain fluid situation of the deployed environment. Networks must be capable of adjusting to threats and provide prioritized transmission for users. Flexibility is obtained through careful system design and standardization. (TAC Pamphlet 700-12, p. 6)

5. Mobility

Mobility is a quality or capability required of military forces which permits them to move from place to place while retaining the ability to fulfill their primary mission. (JCS Pub 1, p. 217) The system must be easy to transport, set up, and use or mobility efforts will be greatly hindered. (TAC Pamphlet 700-12, p. 6)

6. Supportability

Supportability refers to wartime maintenance, spares, and support concepts for deployed LANs. The use of standard Air Force and off-the-shelf components makes the maintenance and spares problem much easier to handle. (TAC Pamphlet 700-12, p. 6) Supportability is the degree to which systems' design characteristics and planned logistic resources, including manpower, meet system peacetime readiness and wartime utilization requirements. The number of parts must be kept to a minimum and systems should have built in diagnostic and test equipment whenever possible. Systems must be designed to minimize maintenance. An increase in maintainability creates a decrease in vulnerability and therefore an increase in deployability of the system. Stubby pencil backup capabilities must not be discarded when relying on computers for critical tasks.

7. Security

Security is a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. (JCS Pub 1, p. 327-328) Network security must address both physical and internal security.

Physical security involves TEMPEST shielding to guard against electrical emanations. It concerns the interception of data transmitted over the medium; therefore, concerns the possible need for encryption devices. Although encryption makes interpretation difficult, it will not prevent the destruction of data by an intruder. (Brown, p. 16) Additionally, security is concerned with how easy the transmitted signal may be jammed.

Internal security involves the need for passwords and audit trails to keep track of systems access. Internal security is necessary to prevent unauthorized access and use of the network, as well as misdelivery of messages. (Ware, p. 65) The long range Air Force goal of securing all voice and data transmissions must be considered. (TAC Pamphlet 700-12, p. 6)

8. Cost

Cost is becoming an ever increasing influence on the selection of any DoD system. In today's fiscally constrained environment, tradeoffs must be made with regards to all components of a LAN. It may be necessary to do without a workstation in order to provide the channel capacity necessary to perform the mission. (Freund, p. 18) Cost includes procurement, training, operating, and maintenance expenses directly related to the LAN.

D. TOPICS OF CONCERN FOR LAN DECISION MAKERS

Local area networking is a multi-faceted technology. Unfortunately, the military decision makers that design, procure, and implement LANs often have a limited knowledge of the subject and must rely on the technical advise provided by their staffs as well as contractors. The intent of this section and this thesis is not to turn that decision maker into a technical expert. One intent is to expose the decision maker to the technology, terms, and concepts of LANs. Another intent is to arm the decision maker with critical topics of concern which must be satisfactorily addressed by the technical staffs.

These topics of concern vary widely and are not limited to:

- type of data to be exchanged
- number of nodes
- traffic loads
- topology
- medium
- protocol
- geographical size of LAN
- interfaces to other LANs and WANs
- deployability concerns

An exhaustive list of questions that must be answered cannot be assembled due to the variability in users' requirements, mission, and application of deployed LANs. Alternatively, the authors describe major topics of concern. These topics cannot be weighted and placed in a formula which calculates the correct LAN for the users requirements. However, each must be addressed in the initial concept and system design stages. The answers to these topics of concern will help to further specify the design for the LAN which best fits the requirements.

Decision makers who have the responsibility to procure a deployable LAN must ensure that a thorough analysis has been performed to determine the expected type of data to be transmitted over the network. The first and foremost issue to resolve is to determine the expected type of data to be transmitted over the network. This must be specified before the network analysis, design, and selection process can begin. The network could be designed under a worst case scenario with a large number of data transfers and high user activity. This approach is not efficient and can result in unnecessary overhead and delays.

Various types of data passed on a deployed LAN include:

- large file transfers (status reports)
- database queries (air tasking order generation)
- message traffic between users (operations orders)
- external sensor data (intelligence reports and summaries)

How often the data is transmitted, the time criticality of the data, and data prioritization must also be specified. If data is only occasionally transmitted over the network then it may not be necessary to incur the additional overhead of token based protocols. If high traffic loads are expected, then it is necessary to determine the criticality; of timely data transfer. Only token passing protocols can guarantee an upper bound on delay before data is transmitted. This is also related to the issue of data prioritization. For example, if message prioritization is required, a token based scheme is the only viable solution to the LAN architecture.

Other key questions must also be answered:

- What is the expected number of nodes on the LAN and how will they be organized?
- What will be the average and peak traffic loads?
- Will the traffic load be such that it is necessary to guarantee a user eventual access?
- What topology, medium, and protocol best fit the requirements?
- Will the architecture satisfy the required data rate?
- What is the required geographical size of the LAN?
- Will the LAN interface to other LANs or WANs?
- Have all the deployability issues such as survivability, security, and mobility been addressed?
- What is the anticipated growth of the LAN and how much of this is compensated for in the initial design?
- In what type of environment will the LAN operate and what shelters will be required?
- What was the basis for any previous decisions concerning these issues?

The decision maker must ask these types of questions to ensure the technical staffs have successfully analyzed and addressed all pertinent aspects of LANs and considered the mission of the unit. Naturally, the decision maker should not blindly follow advice; but, should query the technicians and build confidence in their analysis and recommendations. A simple decision tree cannot be constructed to determine the optimal design for a particular application due to the complexity and variability associated with designing a new deployable LAN for an application that has never before been automated or networked.

Determining the appropriate architecture for a deployed LAN requires a basic understanding of LAN technology and components. The next chapter identifies the key LAN components and discusses the current technology. This understanding will facilitate the decision process.

III. LAN TECHNOLOGY BACKGROUND

A. LOCAL AREA NETWORK OVERVIEW

Local Area Networks (LANs) are defined as a collection of computers and peripherals connected by shared communications media and are not limited to point-to-point communication. LANs cover a limited geographic area (usually less than six kilometers) and allow sharing of resources and exchange of information via the communications medium (TAC Pamphlet 700-12, pp. 1-10). LANs have been in use since the mid 1970s and were first deployed by the Air Force in the 1980s. LANs are functionally dependent on the attached devices, the communications medium used, the topology of the network, and the communication protocol being used. The medium is typically wideband, allowing very high data rates of 1-100 Megabits per second (Mbps). Another typical feature of LANs is that they are usually owned and controlled by a single organization. This allows decisions to be made based on the organization's requirements.

Generally, LANs follow the following functional guidelines:

- Ability to transmit data between two nodes without the use of complex routing algorithms and intermediate nodes to store-and-forward data.
- Provide communication between nodes separated by as much as six kilometers at a data rate of at least one Mbps.
- Easy modification after installation considers the addition and deletion of nodes while limiting the impact on the operation of the network.
- Nodes should be connected to the network in such a way that if one fails, the network as a whole is not affected; however, the function provided by the failing node may be lost temporarily.

- The network should be constructed to allow interface to other similar or different networks through the use of appropriate translation equipment.
- Features should be provided to facilitate network maintenance, diagnostics, and service.

One of today's fastest growing areas of communications and computer technology is the local networking of computer terminals and their peripherals. A LAN is a means of communication which connects automated data processing equipment and peripherals in a specific area. Networking allows the sharing of data, software applications, and peripheral devices such as printers and plotters. Offices throughout the civilian and military communities use local area networks to improve the utilization efficiency of data and equipment resources. Networks may also be linked to larger computers or other networks to share their resources. Software maintenance costs are lower because there is generally one central copy of application programs.

The Institute of Electrical and Electronics Engineers (IEEE) describe LANs in the following way:

> LANs are distinguished from other types of data networks in that they are optimized for a moderate size geographic area such as a single office building, a warehouse, or a campus. The network can generally depend on a communications channel of moderate to high data rate, low delay, and low error rate. The network is generally owned and used by a single organization. This is in contrast to Wide Area Networks (WANs) which interconnect facilities in different parts of the country or are used as a public utility. (IEEE Standard 802.1)

As can be seen from this description, LANs are difficult to define succinctly; thus, LANs are generally described by their characteristics. The following list of characteristics help to further describe LANs:

- high data rates
- limited geographical areas
- ownership by a single organization
- access by several devices
- relatively low costs
- low error rates
- high bandwidth
- ability to connect dissimilar equipment (Smith, p. 4; Malakie, p. 5; Gee p. 4)

To standardize network architectures and protocols, the International Standards Organization (ISO) has developed a seven level reference model. This model is formally known as the Reference Model of Open Systems Interconnection (OSI). The seven layers are: physical, data link, network, transport, session, presentation, and application. LANs deal primarily with the physical and data link layers. Figure 3.1 illustrates the layers of the ISO model and identifies those layers associated with LANs.

The physical layer consists of the physical connection system including specifications for connectors, pin assignments of cabling, noise issues, collision detection, and voltage levels. Electrical, physical, and mechanical characteristics are addressed in this layer.

The layer above the physical layer is the data link layer. The data link layer segments data for each channel into groups called frames. Frames include control information, source and destination identifiers, and the data to be transmitted. This

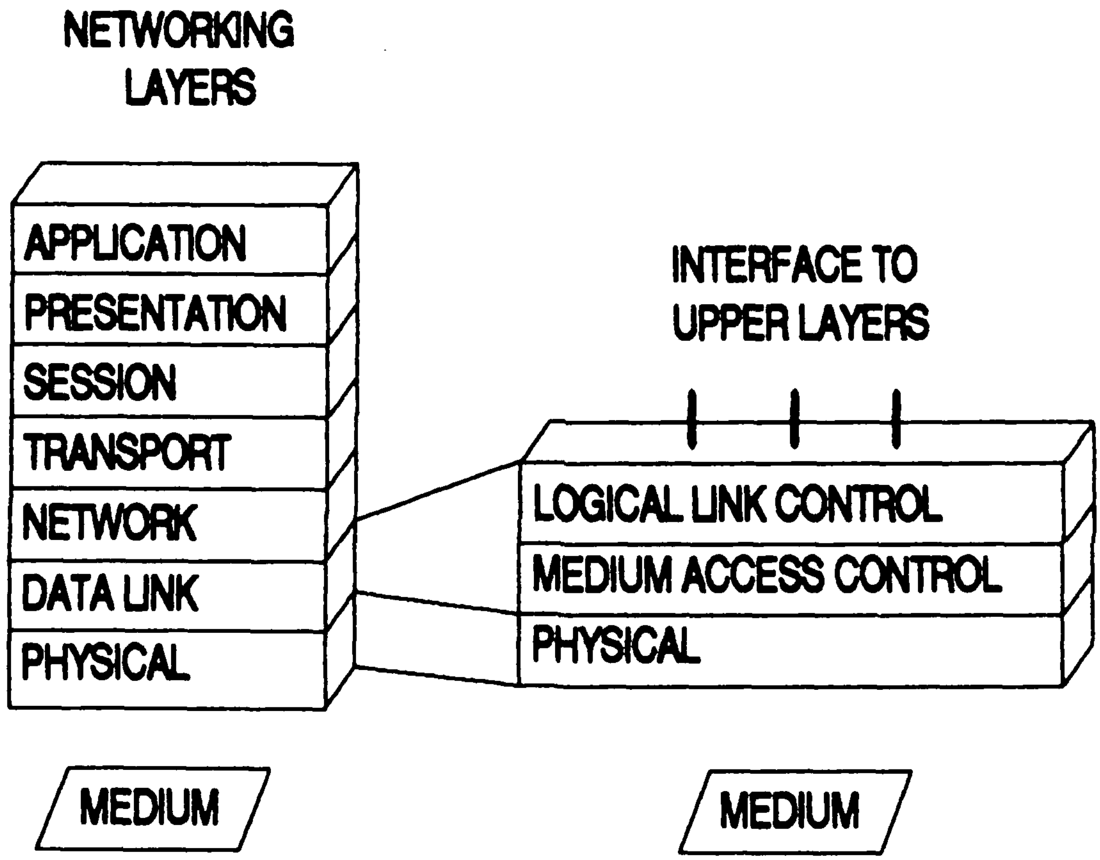


Figure 3.1 Networking and LAN Layers

Source: (Kummerle, 1987, p. 9)

layer performs many of the transmission errors and enhances service quality. Retransmission of damaged frames is also handled by this layer.

The network layer moves data from device to device along the network. Here, frames are put together to form packets and are given routing and switching information needed for their proper delivery. Required connections are established and maintained during transmission.

In the transport layer, packets are put together to form messages. This layer is responsible for message flow, routing, congestion control, and message integrity. This layer multiplexes data and puts it onto the network.

The session layer sets up and terminates communications between devices on the network and sets up synchronization between end user tasks.

The presentation layer handles code conversions and format translations to ensure that different equipment receives information in a form that can be understood. The presentation layer negotiates varying syntax of dissimilar machines allowing end users to process and exchange information of different formats.

The application layer consists of the software that interacts with the user's applications software and is directly related to the exchange of information between end users. File transfer, mail services, passwords, network security, and terminal support are examples. (Gee, pp. 77-79; Stack, pp. 260-261)

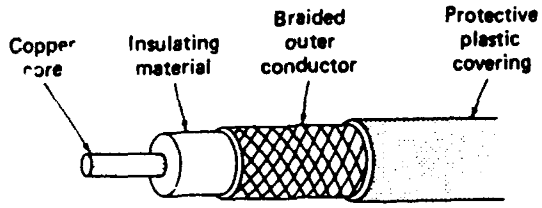
LANs have many important aspects which determine their cost and performance: medium, signalling techniques, topology, network access/protocols, gateways, bridges. These have been used to develop a set of LAN standards accepted by industry.

B. TRANSMISSION MEDIA

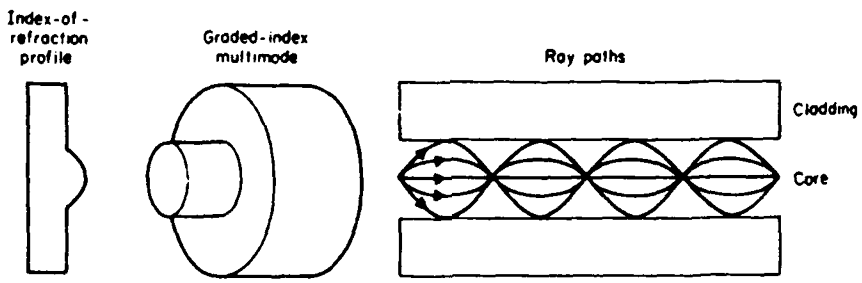
Medium is the physical communications backbone capable of carrying electromagnetic information between network transmitters and receivers. The major types of media used in LANs are: twisted pair, coaxial cable, optical fiber, radio, and various directional radiation techniques. Figure 3.2 shows examples of various cable media. Choosing the proper medium for the requirement is a technical decision which must be carefully addressed. The medium is the ultimate limiting factor on the amount of data that can be transmitted over the network. User requirements determine the choice of medium, not the other way around.

The chosen transmission medium must be rugged, capable of enduring rough handling, and withstanding the elements of nature while remaining reliable and providing the necessary data rate. The medium must be immune to noise, have low loss, and a low error rate. A critical consideration for proper medium selection is cost, including cost per channel mile, connector costs, repeater costs, operations, and maintenance costs (Roberts, Whitty, p. 9.1). The medium selected must meet present and future data rate and performance requirements. Future growth requirements must be considered early in the design process or the LAN will quickly become obsolete. The objective is to meet all valid requirements and remain cost effective (Grandalski, pp. 59-62; Stallings February 1984, pp. 7-8; Lundquist, pp. 27-29; Gee, pp. 48-51). Table 3.1 is a summary of the features for the four most common cable media. Tapping refers to the ease of connecting additional nodes to the network. Security is related to emanation of signals as they pass through the medium. Major characteristics, advantages, and disadvantages of the most common media used for LANs are provided in Appendix A.

A



B



C

Figure 3.2 Media: (A) Twisted Pair, (B) Coaxial Cable, (C) Fiber Optics

Source (Tanenbaum, p. 58; Jacobs, p. 8.2)

TABLE 3.1: COMMON LAN MEDIA COMPARISON

	TWISTED PAIR	BASEBAND COAXIAL	BROADBAND COAXIAL	FIBER OPTICS
MAXIMUM DATA RATE (Mbps)	1	10	5/channel	2000
MAXIMUM BANDWIDTH (MHz)	.300	400	400	565
MAXIMUM REPEATERLESS DISTANCE (Km)	3	10	50	10
IMMUNITY TO NOISE	Low	Low to Medium	Medium to High	High
EASE OF TAPPING	Very easy	Moderately easy	Moderately difficult	Difficult
SECURITY	Not secure	Not secure	Not secure	Very secure
AVERAGE $ COST/FOOT	0.05-0.25	0.50-3.00	0.35-1.00	0.25

C. SIGNALING TECHNIQUES

Signaling techniques are the methods used to communicate between devices. The majority of today's LANs utilize coaxial cable as their communications medium. Data transmission along coaxial cable is carried out in one of two ways: baseband (digital) or broadband (analog). If data on the network is represented by a discrete set of signal levels, it is called baseband modulation. If the data is represented by the amplitude, frequency, or phase of an analog carrier signal, it is called broadband modulation.

In making the decision between baseband or broadband, system designers must make trade-offs between user requirements, simplicity, speed, and cost (Krutsch, pp. 105-112; Gee pp. 43-46; Ware, pp. 12-14). Further details on the differences, advantages, and disadvantages of broadband and baseband transmission can be found in Appendix A.

D. TOPOLOGY

Topology is the structure, consisting of paths and switches, that provides the communications interconnection among nodes of a network. Various network topologies can be centralized or distributed. Centralized networks are those in which all nodes connect to a single controlling node. In distributed networks, each node is connected to other nodes and not to a central node.

There are two basic categories of topologies: unconstrained and controlled. Unconstrained topologies are typically associated with long-haul communications networks (Wide Area Networks or WANs) which are point-to-point links; therefore, they require a routing algorithm to instruct individual nodes how to forward data not intended for them. Controlled topologies eliminate the need for complex routing algorithms. With controlled topologies, nodes are configured in a specified pattern to support the functional guidelines stated earlier.

Topology selection affects all other aspects of the LAN; thus, several considerations must be made when evaluating topologies for specific requirements. The choice of transmission medium and topology cannot be made independently. The two must be considered together because certain medium better lend themselves to certain topologies. Diagnostics, troubleshooting, bandwidth, and expansion capabilities are just a few of the major topology concerns. (Kieffer, pp. 23-31; Stallings March 1984, pp. 6-8; Lundquist, pp. 21-26; Gee, pp. 11-30; Yeh, Jeng, Wu, pp. 7-11)

Star, bus, ring, tree, mesh, and fully connected topologies are depicted in Figure 3.3. Further details are also provided below.

1. Star

Star networks have all terminals connected to a central controlling node which becomes a single point of failure. If the central node fails, the network cannot function. If this node does not have the processing and storage capacity to handle the amount of service requests from the other nodes, a bottleneck will form and the responsiveness of the network will rapidly degrade. This configuration is typical of a mainframe computer with many individually wired terminals. The central node acts as a switchboard between all connected terminals.

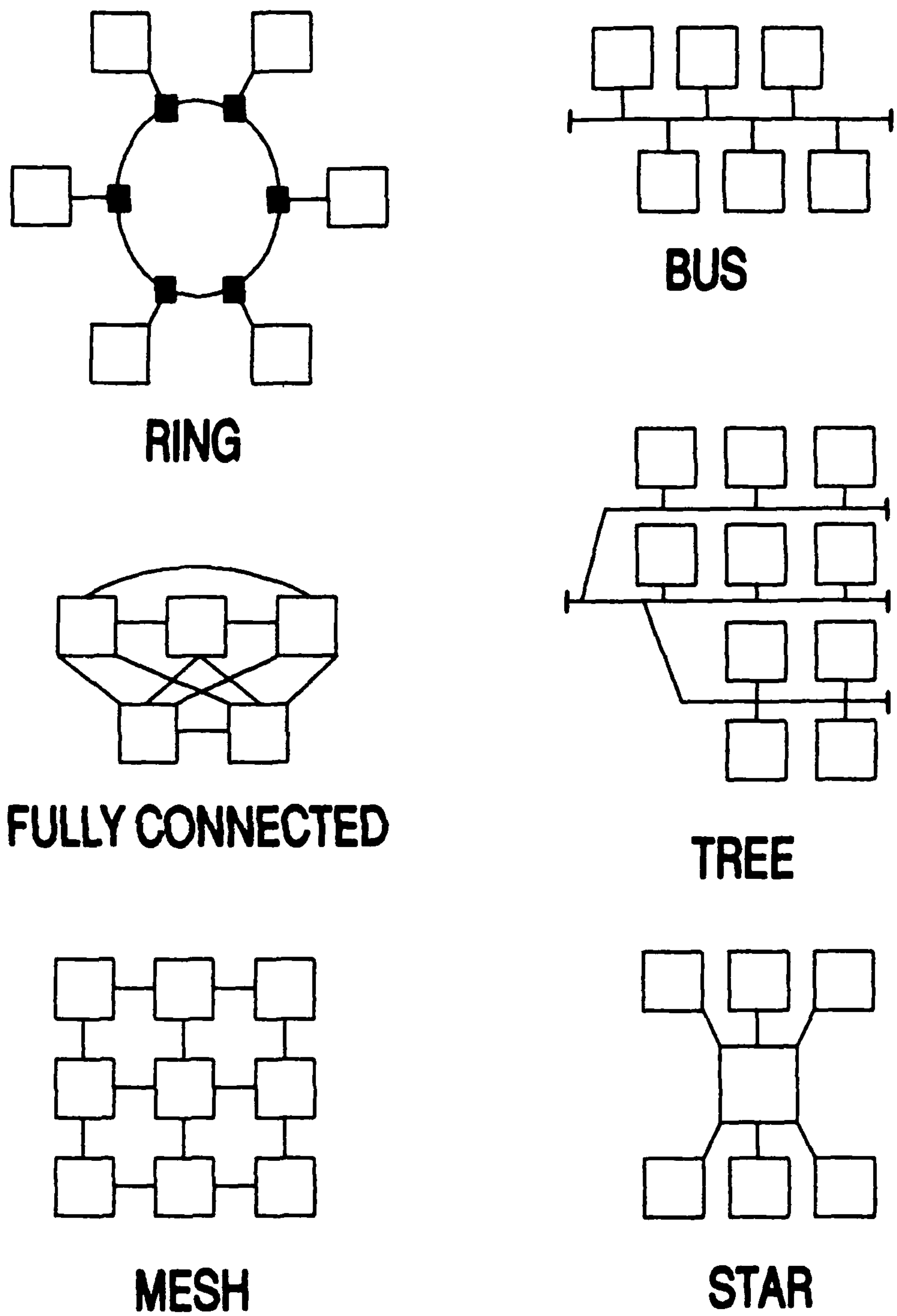


Figure 3.3 Common LAN Topologies

In a star topology, messages can be transmitted from the central node to any or all of the attached nodes, from an attached node to the central node, or from one attached node to another via the central node. In the latter case, a simple routing algorithm is necessary for the central node. Backup central nodes are recommended whenever possible to lessen the effect of a failure of the control node.

Advantages of the star topology are:

- easy troubleshooting
- suited to "dumb" terminals
- high security is possible
- centrally-controlled addressing
- each spoke on the star is independent of the rest

Disadvantages of the star topology are:

- lower data rates
- cables may be expensive
- expensive, large central node required
- very vulnerable to central node failure
- individual or shared ports required for each terminal (Gee, pp. 13-19; Stallings 1983, pp. 12-13)

2. Bus/Tree

The bus or tree is the most commonly used topology. All nodes share a common circuit which has two distinct ends. The ends are not connected to form a loop. Bus/tree topologies utilize long multi-point cable which is typically coaxial.

Signals generally travel in both directions along the bus/tree. The bus is a simple form of the tree with no branches. Point-to-point medium such as fiber optics do not lend themselves to multidrop environments because of difficulties in tapping the cable.

In a bus topology, messages are transmitted on the bus in both directions from the originating node. The other nodes simply check the message as it passes to determine if it is intended for them. No routing algorithm is required by the bus/tree topology because messages are broadcast to all nodes and individual nodes take what is addressed to them. Bus/tree topologies are best used in light sporadic transmission environments. Contention for the bus must be carefully controlled. The bus/tree topology does not utilize a central control node. Reliability is usually higher due to the lack of a single point of failure which exists in other topologies. Tree connections are not linear. Trees branch out providing two or more paths from a particular node.

Some advantages of the bus/tree topology are:

- medium priced
- very reliable
- easy expansion
- easy installation
- simple technology
- easy to attach new devices

Some of the disadvantages of the bus/tree topology are:

- no automatic acknowledgement of receipt
- messages sometimes interfere with each other (collisions)
- contention scheme must be chosen to prevent saturation
- sophisticated interface units or modems are required for each terminal (Gee, pp. 25-30; Stallings 1983, pp. 16-17)

3. Ring or Loop

In the ring or loop topology, all nodes are connected to two other nodes in the loop. The links are usually unidirectional. Like the bus topology, messages are broadcast onto the medium and circulate around the ring with each node copying what is intended for them. Each node is connected to the ring through a repeater. The repeater is not only the node's access point, but also receives the data and forwards it along the network (Stallings 1987, p. 22). The ring is a series of point-to-point links. If the cable breaks, the entire network is disabled (Stallings 1987, p. 24). Loops have a controlling node; however, rings have no node with overall authority. Rings are best suited for a small number of nodes.

Advantages of the ring or loop topology are:

- low error rate
- high data rates
- low cable costs
- routing is simple
- automatic confirmation of receipt

- no dependence on central node in rings
- greater distances between nodes is possible because repeaters regenerate the signal at each point

Disadvantages of the ring or loop topology are:

- loop depends on controller
- difficult to lengthen ring (Gee, pp. 19-25; Stallings 1983, pp. 13-14)

4. Mesh

Mesh topologies interconnect nodes in a more complex manner not easily categorized in one of the above topologies. The most economical connections are utilized. This type of topology is more prevalent in long-haul networks, such as telephone networks, than in local area networks. Overall reliability is generally better in this topology due to redundant data paths. Mesh networks require too much cabling, are too complex to use, and are too difficult to troubleshoot in the deployed environment. (Stallings 1983, pp. 17-18)

E. NETWORK ACCESS/PROTOCOLS

Network access methods, or protocols, are the rules nodes must follow to transmit data over the network. According to Andrew S. Tanenbaum, "a protocol is a set of rules governing the format and meaning of the frames, packets, or messages that are exchanged by the peer entities within a layer", where an entity is a node connected to the network (Tanenbaum, p. 27). Protocols handle varying data rates (flow control), error detection and correction (error control), and message format (data frame). (Rand Corporation Report, p. 28) A network access protocol should accomplish the following goals:

- Initialization. A node should be allowed to enter the network upon start-up of network operations.
- Fairness. Nodes should be treated fairly regarding both the delay time to access the network and the amount of transmission time allowed once the network has been accessed.
- Priority. The protocol should provide a prioritization scheme to permit quicker access for nodes with higher priority data.
- Single node transmit. The protocol should attempt to permit only one node to transmit at a time.
- Receipt. Proper receipt of messages should be ensured by the protocol.
- Error detection. The protocol should incorporate some form of error detection to identify when messages are not received correctly.
- Recovery. The protocol should be able to recover from errors within the network.
- Expandability. The protocol should support expandability through easy addition and deletion of nodes.
- Compatibility. The protocol should support equipment from various vendors.
- Reliability. The protocol should permit the network to continue to function regardless of the failure of one or more nodes. (Myers, p. 32)

In general, protocols should possess the following properties:

- Freedom from deadlock. This guarantees that parallel programs that constitute the protocol will not all enter states wherein each is waiting for an action by another.
- Completeness. This refers to the ability of the protocol to handle all conditions that might arise.
- Freedom from saturation or starvation. Nodes should not be sent frames faster than they can be processed, or so slow the node cannot keep busy.

- Freedom from infinite loops. Protocols should not cycle through a sequence of states with no means of terminating the loop.
- Possession of self-synchronization. This refers to the ability of a protocol to attain a normal state from an error state in a finite amount of time.
- Reachability. This refers to the assurance that all states can be reached.
- Termination. The protocol contains a final state and allows the final state to be reached. (Franta, Chlamtac, p. 109-110)

Protocols are grouped into two categories. These categories are contention and token passing protocols. Contention protocols involve multiple users competing for use of a single channel, thus collisions can occur and degrade network performance. Token passing protocols also eliminate collision problems by allowing only the node holding the token to transmit.

1. Contention Protocols

Contention refers to systems with multiple users sharing a common channel in a manner which could lead to data collisions and conflict over channel access (Tanenbaum, p. 121). Collisions occur when one or more nodes attempt to transmit data onto the communication channel while it is in use by another node. These collisions generally destroy data being transmitted over the channel. Therefore, all colliding nodes involved are required to retransmit their data. There is no procedure used to determine which node can access the channel; therefore, the nodes must contend for the time (Stallings 1987, p. 39).

Several protocols have been developed for networks where channel contention is an acceptable means of operation. Typically, this type of protocol works best when the amount of data traffic and channel access are low. This is normally referred to as bursty traffic. Ease of implementation and efficiency under light traffic conditions are the greatest advantages of contention protocols. The primary disadvantage is that performance declines drastically as the load increases (Stallings 1987, p. 39). The most common of the contention protocols are ALOHA, Carrier Sense Multiple Access (CSMA), and Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

a. Aloha

ALOHA is the simplest of all contention protocols. In this protocol, a node having a message to send immediately transmits it onto the channel without regard to whether the channel is busy or idle. If a collision occurs, both colliding nodes must retransmit their messages. A collision is normally determined in one of two ways: by non-receipt of a positive acknowledgement from the destination node or by the originating node's verification of the message. (Elion, p. 57) Collisions are quite common as message traffic increases because data is arbitrarily transmitted without regard to the channel's current state.

If fixed length frames are used, a slotted version of ALOHA can be implemented to reduce the number of collisions. By using fixed length frames, time can be allocated in discrete slots. Slotted ALOHA is similar to standard ALOHA in that nodes transmit data without checking channel status; however, nodes do not transmit immediately when a message is queued. A message is not transmitted until the beginning of the next time slot. This lessens the effect of collisions by controlling when they can occur. Therefore, instead of several collisions staggered over a small period of time, all collisions will be at the beginning of a time slot. The length of the time slot is equal to the length of the data frame. This increases the likelihood that a node will successfully complete its transmission because no collisions occur before the end of the time slot.

b. Carrier Sense Multiple Access (CSMA)

The CSMA protocol attempts to eliminate the collisions which occur with the ALOHA protocol when nodes blindly transmit onto the transmission channel. Using CSMA, a node first listens to the carrier on the channel to check if data is currently being transmitted. If the channel is clear, the node will attempt to transmit. If the channel is busy, the node will wait to transmit its data. This wait is handled in one of three ways. The three variations of the CSMA protocol are 1-persistent, non-persistent and *p*-persistent. The variations refer to when a node will attempt to transmit after sensing a busy carrier.

Using 1-persistent CSMA, a node senses the channel until it becomes idle, then it immediately transmits its data. With non-persistent CSMA, the node will transmit its data immediately if the channel is idle. If the channel is busy, the node waits a random amount of time and attempts to transmit again.

P-persistent CSMA has a probability of transmission p assigned to it. In this protocol, if a node senses the channel is idle, it generates a random number. If the random number is less than or equal to p, the node will attempt to transmit its data. Otherwise, the node will wait until the next time slot, sense the channel and repeat the process. If the channel is busy, the node waits a random time and repeats the above process.

One disadvantage of 1-persistent is the possibility of multiple nodes waiting for the channel to go idle. When this occurs, the nodes may sense a clear channel within a small enough time frame that multiple nodes will transmit and collide. Non-persistent eliminates this problem because of the unlikely event that two nodes would generate the same random wait time. As data transmission loads increase, this method adds a considerable amount of delay time before a node can transmit. (Tanenbaum, p. 127) *P*-persistent CSMA attempts to minimize both collisions and idle time, and depending on the probability selected will perform better than the other variations. (Stallings 1985, p. 23)

c. *Carrier Sense Multiple Access/Collision Detection (CSMA/CD)*

Sensing the carrier before transmission reduces the possibility of many of the collisions which occur with ALOHA. However, if multiple nodes sense the channel clear at the same time, they will all attempt to transmit and collisions will occur. This cannot be avoided using contention type protocols. The problem is to reduce the amount of time wasted by these collisions. Using CSMA, nodes do not know a collision has occurred until after the message has been completely transmitted. This wasted time may be reduced by utilizing a protocol which can quickly detect collisions and terminate transmission to clear the channel as soon as possible. This protocol scheme is CSMA/CD.

The collision detection feature saves considerable time by allowing nodes to terminate their transmission soon after a collision has been detected (Tanenbaum, p. 128). This allows the channel to be cleared sooner which allows nodes to attempt to access the channel earlier. When a collision has occurred, the nodes involved wait a random amount of time before attempting to retransmit. This random wait time reduces the possibility of the same collision happening again by preventing nodes from immediately attempting to transmit when a clear channel is sensed.

The greatest concern with all contention protocols is the lack of an upper bound on the amount of time a node may have to wait before it will be able to transmit its data. This can be more than a theoretical problem during heavy load periods with many collisions occurring creating a bottleneck which entirely prevents access to some nodes. To eliminate this problem, protocols have been established that will allow all nodes an opportunity to transmit data within a known maximum amount of time. Collision free protocols have been developed to establish a known upper bound on the wait time.

d. Time Slot Protocols

One method of collision free protocol is to allocate specific contention time slots, one for each node, to allow a node to identify when it has data to transmit. This protocol is known as the Bit Mapped Protocol (BMP). When a node's contention slot passes, it will set the slot if it has something to transmit; otherwise, it lets it pass. When all the nodes have had an opportunity to set their respective slots, nodes are allowed to transmit data in order. When all have finished, the contention slots pass by the nodes again and the process is repeated.

During periods of light data traffic, there is a considerable amount of wasted time. During high loads, there is still a large delay; but, there are no collisions and the maximum wait time is known for each node. An improved version of BMP allows a node to transmit as soon as it sets its contention slot, thus reducing the amount of time a node must wait before it can transmit its data. Under heavy traffic conditions overall delay is considerably reduced.

The primary benefit of this time slotted protocol is the elimination of collisions. Each node is guaranteed an opportunity to transmit its data and there exists a definite maximum amount of time a node must wait before transmitting. Time slot protocols are also referred to as "reservation protocols" because the nodes set bits to reserve an opportunity to transmit data (Stallings 1987, p. 39).

2. Token Passing Protocols

Another group of collision free protocols are called token passing protocols. These protocols involve the transmission of a special control frame, or token, over the medium. If a node has data to transmit, it must capture the token before it can access the channel. Once the node possesses the token, it can transmit its data for no more than a maximum specified time known as the token hold time. The node must then release the token for another node to have an opportunity to transmit. There are two basic types of token passing protocols: token ring and token bus.

The token ring protocol is different from token bus in that the tokens are not addressed to a specific node. Instead, the token is simply passed to the adjacent node. If this node has data to transmit, it will hold the token, otherwise it will pass it to the next node. (Stallings 1985, p. 29) This also makes the additions of nodes easier since no addressing scheme necessary.

Token passing protocols are most desireable when there is a high number of data transfers, and several stations wishing to communicate. In this way, stations are guaranteed the opportunity to transmit. Additionally, token passing protocols permit message prioritization.

With the token bus protocol, the node currently holding the token passes it to its logical neighbor by specifically addressing that node. Logical neighbors may or may not be physically located adjacent to one another. The bus is physically a linear cable with nodes attached. The cable is a broadcast medium; therefore, each node receives data and must ignore the messages not addressed to it. When a node is added to the bus, it does not automatically become a part of the network until its logical neighbors are identified. Naturally, features exist in the protocol to handle the addition and deletion of nodes. (Tanenbaum, p. 149)

F. GATEWAYS AND BRIDGES

Gateways or bridges, depending upon the similarities and differences between the networks, are used to interconnect separate networks. Figure 3.4 illustrates how bridges and gateways are used to interconnect networks. A gateway allows the connection of different protocols or physical characteristics. Gateways allow LANs to be connected to other external LANs or communication systems. Gateways strip

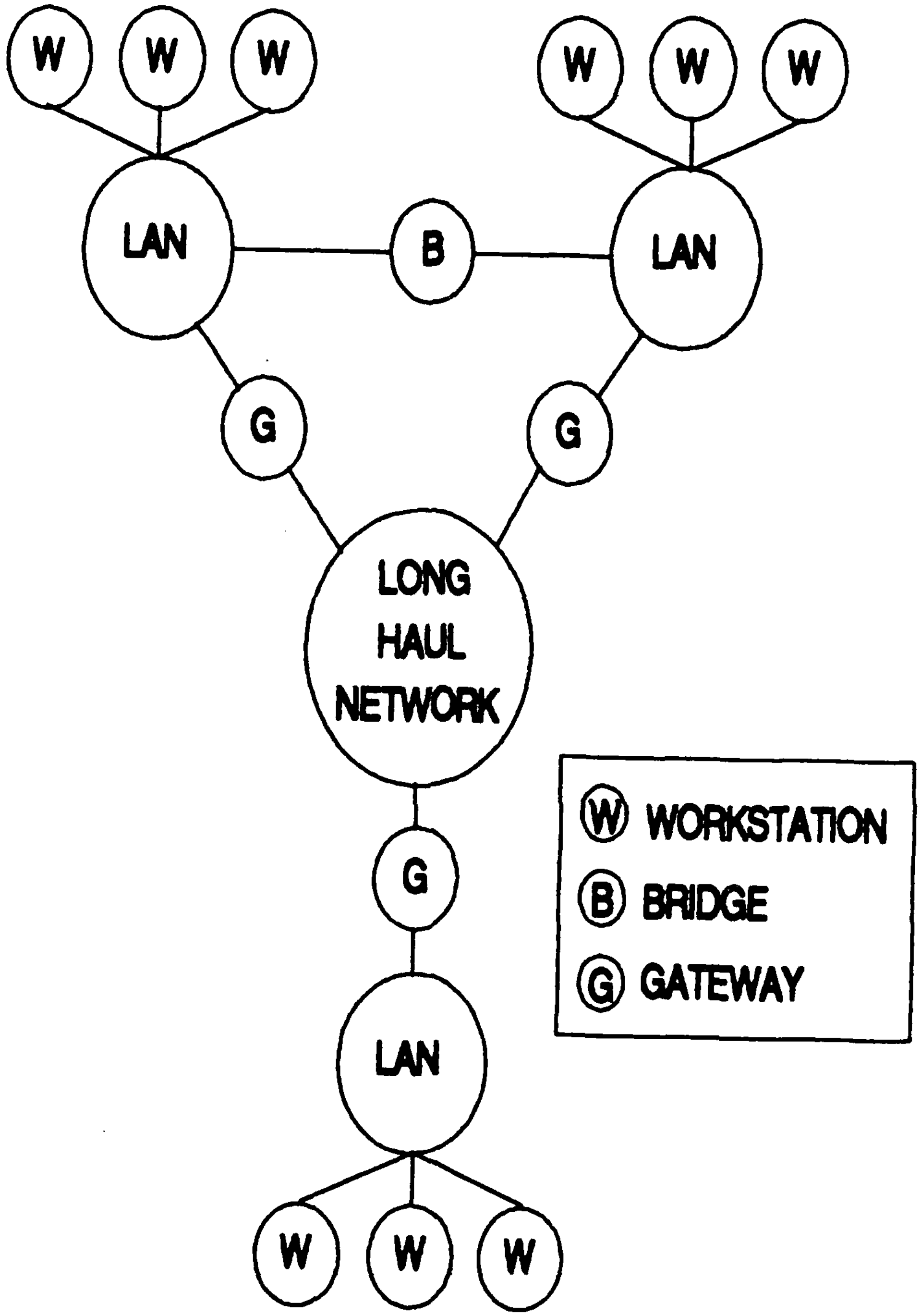


Figure 3.4 Bridges and Gateways Used to

Interconnect Various Networks

off control characters and tokens before reconfiguring the packets or data frames and delivering them to the other network. Gateways are able to translate in both directions between the differing protocols. Gateways add considerable overhead to a network because each packet must be translated for the other network. Gateways are commonly used on long distance communication networks between LANs and WANs, like the Defense Data Network (DDN). WANs include satellite links, packet switched networks, and leased long-haul communications lines.

Bridges provide long-haul communications between similar type networks. Bridges work in the physical and data link layers and perform media conversions. A bridge is a high speed switching device which handles logical routing of packets between LANs. Stations on different LANs may communicate as if both stations were on the same physical LAN. Bridges can handle differing transmission rates on the two networks it connects. It makes no changes to the content or format of the data packets. If these types of transformations are necessary, a gateway is required. Information packets are received by the bridge, stored, and then passed on to the other LAN. Local traffic is kept on the local LAN and only non-local frames are forwarded through the bridge. This aids in security concerns. Bridges can serve as a security filtering device between sub-networks.

Bridges typically add little overhead and can operate at the maximum network speed. When a frame requires forwarding, it is placed in a transmission queue and forwarded to the output LAN whenever possible. If the bridge is fed with transfer frames faster than they can be transmitted, the frame storage buffers will overflow. This will result in lost information or a request for a retransmission of the lost packets which adds to the problem of queue overflow.

Bridges provide increased reliability due to the partitioning of large LANs into several smaller LANs. If the bridge or one of the connected LANs goes down, other LANs can still operate in isolation. Clustering of similar task work stations into the smaller LANs also helps increase overall performance.

Some advantages of bridges and gateways are:

- traffic filtering
- extension of the area of a LAN
- increase the number of work stations
- connect LANs of different architecture (Malakie, pp. 33-34; Hawe pp. 55-56; Strole pp. 481-496; Ball pp. 115-117)

G. STANDARDS FOR COMMUNICATION PROTOCOLS

The need for computers to communicate continues to increase rapidly. With so many different computer systems in use, standards are essential to provide effective communications. The 1979 National Policy on Standards for the U. S. established the following definition for standards:

> A prescribed set of rules, conditions, or requirements concerning definition of terms; classification of components; specification of materials, performance, or operations; delineation of procedures; or measurement of quantity and quality in describing materials, products, systems, services, or practices (Stallings 1987, p. 31).

For LANs, standards provide the necessary guidelines to ensure the network provides an effective means of communication for the users. The following are advantages of standards:

- a standard assures there will be a large market for a particular piece of equipment or software. This encourages mass production, which results in lower costs.

- a standard allows products from multiple vendors to communicate, giving the purchaser more flexibility in equipment selection and use. (Stallings 1987, p. 31)

- if the same set of protocols are implemented on all DoD data processing equipment, then, for the functions provided by those protocols, interoperability is achieved. (Stallings 1988, p. 3)

The use of standards does have drawbacks. Two primary disadvantages of standards are:

- They usually decided upon by committee; therefore, often they are a compromise rather than the best solution.

- Standards tend to freeze technology. (Stallings 1987, p. 31)

Several organizations throughout the world are actively developing standards in efforts of improving network communications. Two key organizations are the ISO and the IEEE. ISO develops standards on a wide range of subjects; but, their primary concern is the OSI seven layer model. The IEEE is primarily concerned with LAN standards and are the most widely accepted in industry. A detailed description of the IEEE LAN standards can be found in Appendix B. Fiber Distributed Data Interface (FDDI) is another LAN standard currently under development. This standard is also detailed in Appendix B.

The IEEE standards have been developed to meet various network requirements. The most common for use in low to medium access environments is IEEE 802.3 based on the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol and uses a bus topology. This standard is good for minimal access situations. However, as traffic on the network increases, so do the number of collisions causing excessive delays. Additionally, their is no guarantee that a user will ever be granted access to the network (i.e. no upper bound on access delay). Typical data rates for 802.3 are between one and ten Mbps.

Token passing protocols are normally chosen when long periods of medium to high access is expected. IEEE has two standards to meet this situation: IEEE 802.4, Token Bus; and IEEE 802.5, Token Ring. Both protocols guarantee access to the network (i.e. there is a computable upper bound on access delay) because all stations have an opportunity to capture the token as it passes. The primary difference between the two is the topology. There are also differences in signalling techniques, the transmission medium used, and network control methods which result in performance variation. Data rates for these protocols range from one to ten Mbps for Token Bus, and one to four Mbps for Token Ring.

FDDI will be a very powerful LAN standard. It is modeled after IEEE 802.5, Token Ring, and uses optical fiber cable as the medium. This standard has all the benefits of a token passing protocol with the added feature of at least 100 Mbps data rate as well as all the other advantages of fiber optics.

The reason for different standards is the realization that different users have different network requirements. Users have different applications and varying utilization and performance requirements. Instead of creating one network to do everything, a variety of standard networks were developed to meet varying performance and utilization considerations, yet still provide common application and equipment support.

Typical applications include:

- file transfer and access protocols
- access to remote data bases
- graphics, word processing and spreadsheets
- electronic mail
- message coordination
- file sharing
- sharing of printers, plotters, and other peripherals
- connectivity to wide area networks
- process control
- digitized voice transmission (Myers, p. 30)

Finally, industry standard hardware, software, and other network accessories should be used. This increases the likelihood of future availability of parts and support. A certain level of performance and functionality must be provided to be considered a standard. Therefore, greater confidence can be placed in the products. The IEEE 802 LAN standards are recommended because of the increasing acceptance among vendors. (Jamieson, Low, p. 307)

H. SECURITY ISSUES

Security is a critical issue for deployed LANs. Every attempt must be made to prevent hostile forces from intercepting or interfering with data or otherwise inhibit the mission of the deployed unit. For network security to be effective, it must be considered in the planning stage and incorporated into the design. Add-on security packages seldom provide the necessary protection. (Jamieson, Low, pp. 306-307)

Denial of service is a critical security issue. Every precaution must be taken to eliminate areas where intentional or unintentional forces could deny users the service of the network. The choice of medium, topology, and protocol all relate to this issue.

Data transmission requirements largely dictate the type of medium necessary for the mission. However, security precautions should also be addressed. If signal emanations or electrical interference are concerns, then fiber optics should be considered. Regardless of the medium selected, measures should be taken to prevent damage to the medium. Military standard ruggedized cable should be used and external cables buried in underground ducts. (Jamieson, Low, pp. 307-308)

Another medium security issue is protection from unauthorized access. The harder the cable is to tap, the more secure it is from unauthorized access. Fiber optics currently provides the best protection because of the difficulty of tapping the cable without detection. (Jamieson, Low, p. 308)

Topology largely affects the reliability and performance of the network. Star networks are the least vulnerable to cable failures because only a single node would be isolated. However, it is the most vulnerable to node failure. If the central node fails, the network is disabled. A cable breakage on a ring or bus topology normally disrupts the entire network. However, this vulnerability can be overcome through the use of backup networks and dual cable configurations. (Jamieson, Low, p. 307)

The security implications of network protocols is less obvious than media and topology. The security concern is based on performance during various traffic loads. A network using CSMA/CD could be virtually disabled if a single node began generating large amounts of fraudulent messages. By using a token based protocol, network function would be maintained; because, a single node can only hold the transmit token for a limited time. In addition to the network protocol, software for data access control (i.e., user identification and passwords) and data encryption should be considered to prevent unauthorized access to the network and protect data integrity. (Jamieson, Low, pp. 307-314)

LAN performance varies with many factors, such as the type of applications, volume of traffic, and type of data. The selected LAN architecture must perform the best under the given set of requirements. The next chapter discusses the performance of the standard LAN architecture under a variety of conditions.

IV. PERFORMANCE FACTORS

The evaluation of LAN performance is a multifaceted endeavor involving the consideration of diverse criteria and user requirements. Key issues in selecting the proper network architecture include: throughput-delay, required data transfer rate, number of nodes, and the ability to prioritize packets. These issues must be considered among others in the "whole system" concept. The performance of various LAN architectures must be examined with respect to the requirements of the deployed LAN.

Overall efficiency and sensitivity to transmission rates, delay-throughput, numbers of stations, transmission packet lengths, and other factors have been modeled and many experiments on physical hardware have been conducted. Some of the more significant findings substantiated by several independent models and experiments conducted by various universities and industrial laboratories will be summarized in this chapter.

A. THROUGHPUT

LAN throughput varies with use; as users increase the frequency of data transfers, throughput increases. During deployed exercises or wartime, network traffic will greatly increase over normal non-combat periods. As Figure 4.1 illustrates, throughput should follow the desirable curve in order to perform as required during heavy load periods.

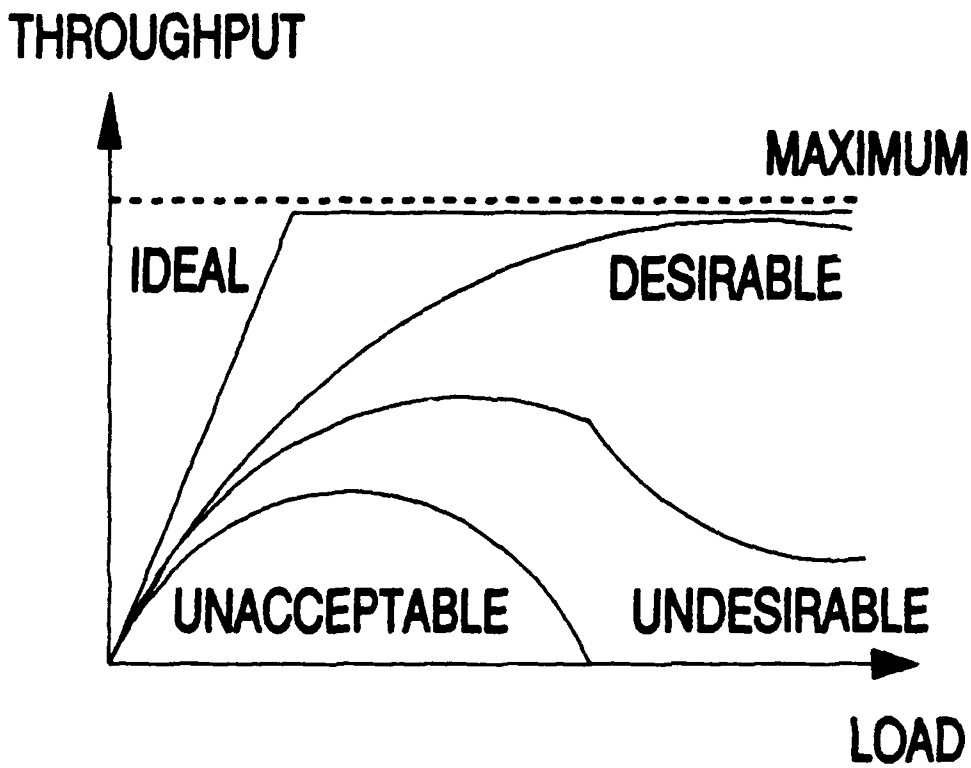


Figure 4.1 Throughput vs. Load

Source (Gee, 1983, p. 111)

Throughput, measured in bits per second, is the average number of bits passing a given point on the network per unit time. For comparison of differing LANs, throughput can be normalized by dividing it by the channel transmission rate to obtain a unitless number between zero and one which represents this quantity as a percentage of the maximum data rate. Figure 4.1 shows representative curves of throughput versus load. Once a packet is ready to be sent, it must wait in a queue to be transmitted. Access is delayed while the packet waits for a convenient time to enter. The packet then moves to the head of the queue and enters network traffic. Transmission time is found by dividing the size of the packet by the transmission rate. Typical transmission rates are four Mbps for Token Ring LANs, ten Mbps for CSMA/CD, and 100 Mbps or more for fiber optic links. After transmission, a propagation delay occurs as the packet travels through the medium. All of these factors combine to determine throughput. (Gee, pp. 110-114) Average transfer delay is the average time from the transmission of the last bit of a packet onto the network until the last bit of this packet is delivered to its destination node.

Another term frequently used in the discussion of LAN performance is utilization. For contention protocols, utilization is defined as the successful transmission time divided by the total time and is directly proportional to throughput. For token passing schemes, utilization is based on the number and size of frames transmitted, divided by this value plus the token size. Naturally, utilization varies with LAN architectures, traffic load, and number of stations.

B. PROTOCOL COMPARISONS

Protocol comparisons for in-garrison and deployed LANs are very similar. One must keep in mind that deployed LANs typically have heavy work loads during contingency and wartime scenarios. The system must be designed to keep message delays to a minimum. Varying the number of stations or the transmission rate of the network should not have a serious impact on user services.

Performance of LANs in terms of delay-throughput depends upon the protocol being utilized. Most studies include comparisons between the three most common medium access protocols: CSMA/CD, token bus, and token ring. These three protocols were covered in detail in Chapter 3, LAN Technology Background. Figure 4.2 compares these three protocols by plotting throughput versus transmission delay time. The figure shows the token bus protocol delay is less than CSMA/CD only for a system utilization greater than 87 percent. Token ring delay is lower than CSMA/CD for traffic loads greater than 35 percent.

The significant attribute of this figure is that the token bus protocol delay is higher than the token ring over the entire range which is due to the significant differences in overhead between the two protocols. (Sachs, Kan, Silvester, pp. 46-50)

Figure 4.3 also plots the three protocols' delay-throughput with an increase in transmission rate from one to ten Mbps. The token passing curves are only slightly affected; thus, having little sensitivity to the data rate parameter. The CSMA/CD curve change is due to the increase in the number of collisions as the data rate increases.

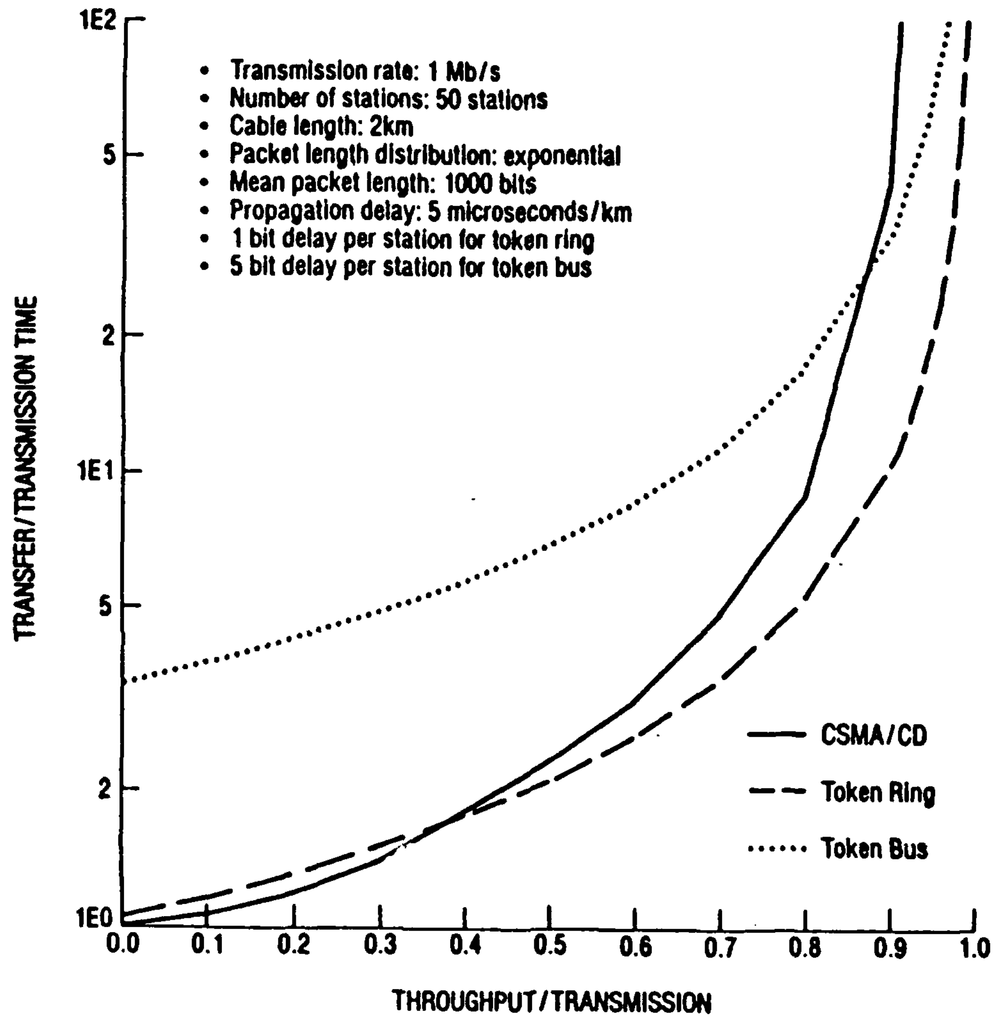


Figure 4.2 Delay Throughput at 1 Mbps

Source (Sachs, Kan, Silvester, p. 49)

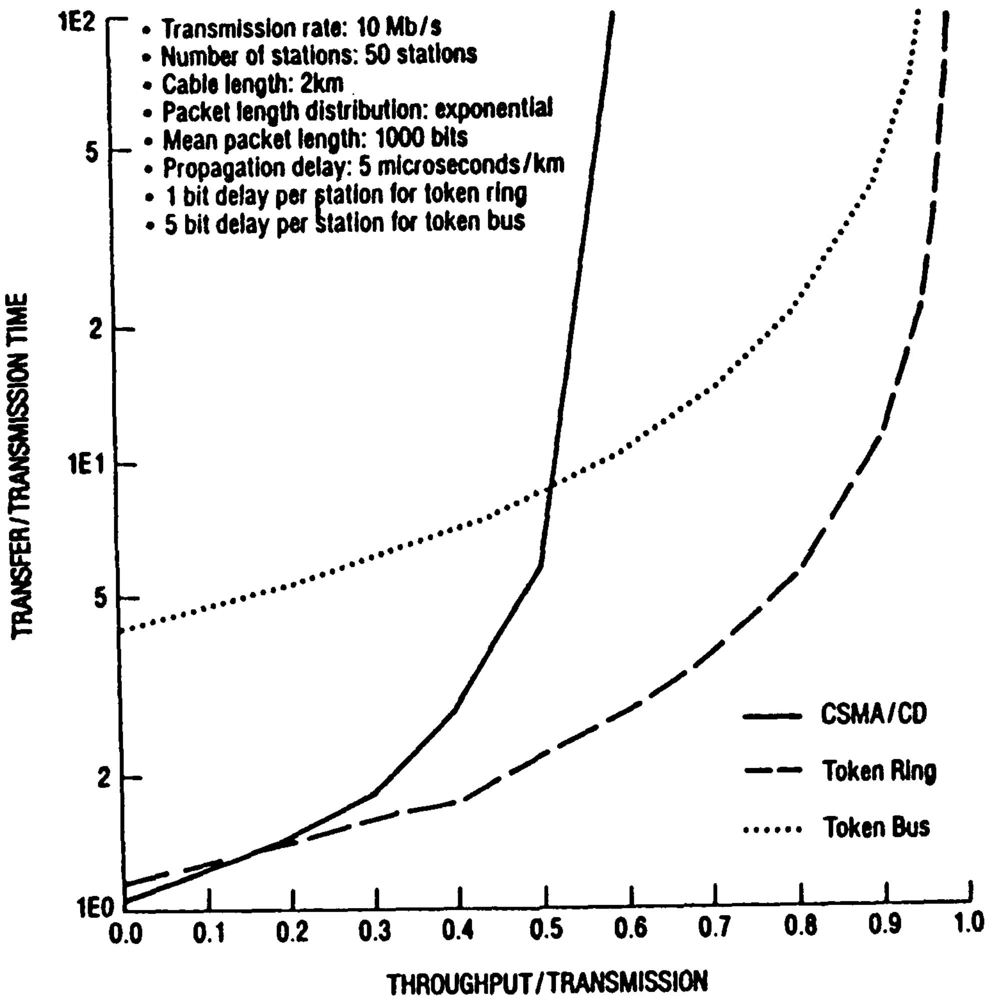


Figure 4.3 Delay Throughput at 10 Mbps

Source (Sachs, Kan, Silvester, p. 49)

Overhead includes necessary items such as address bits, synchronization bits, and unique fields for various protocols. CSMA/CD wastes time due to collisions of data packets and requires acknowledgement of receipt packets. Token bus requires similar acknowledgement packets and also has token transmission as overhead. Token ring includes waiting time for the token in its overhead. Overhead is necessary but should be kept to a minimum. Making the packet size larger adds delay for all the other stations waiting to transmit. Making the packet size smaller causes more collisions or token passing. In CSMA/CD, as the load increases, the throughput increases, and the number of collisions and retransmissions increase. Temporary bursts of data could send the network into a very high collision state. This instability is not possible in token schemes. Token rings are the least sensitive to workload. (Sachs, Kan, Silvester, pp. 46-50)

Figure 4.4 varies message length for the token schemes. Message size does not significantly affect the transfer time of the token ring. For large message lengths, the token bus performs almost as well as the token ring. For small message lengths, the token bus has a higher delay than the token ring partially because the smaller the message length, the more tokens must be passed. (Sachs, Kan, Silvester, pp. 46-50)

Figure 4.5 shows CSMA/CD delay-throughput for three different size packets. The frame transfer delay is defined as the time from generation of a frame until it traffic throughput. This is due is successfully received at its destination. The figure shows the shorter the frame length, the smaller the delay at small throughput values. At higher throughput values, smaller frame lengths require more overhead time and more collisions occur which increases the delay time. (Bux, pp. 351-371)

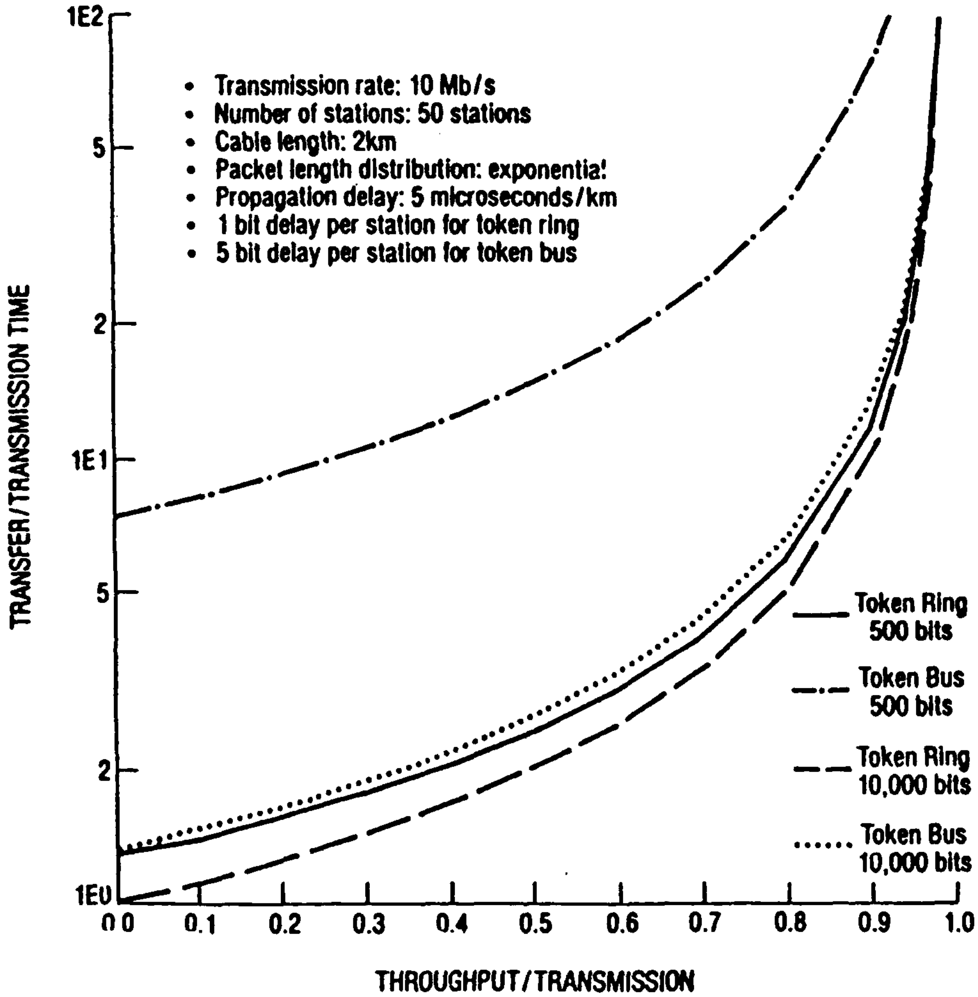


Figure 4.4 Varying Message Length at 10 Mbps

Source (Sachs, Kan, Silvester, p. 50)

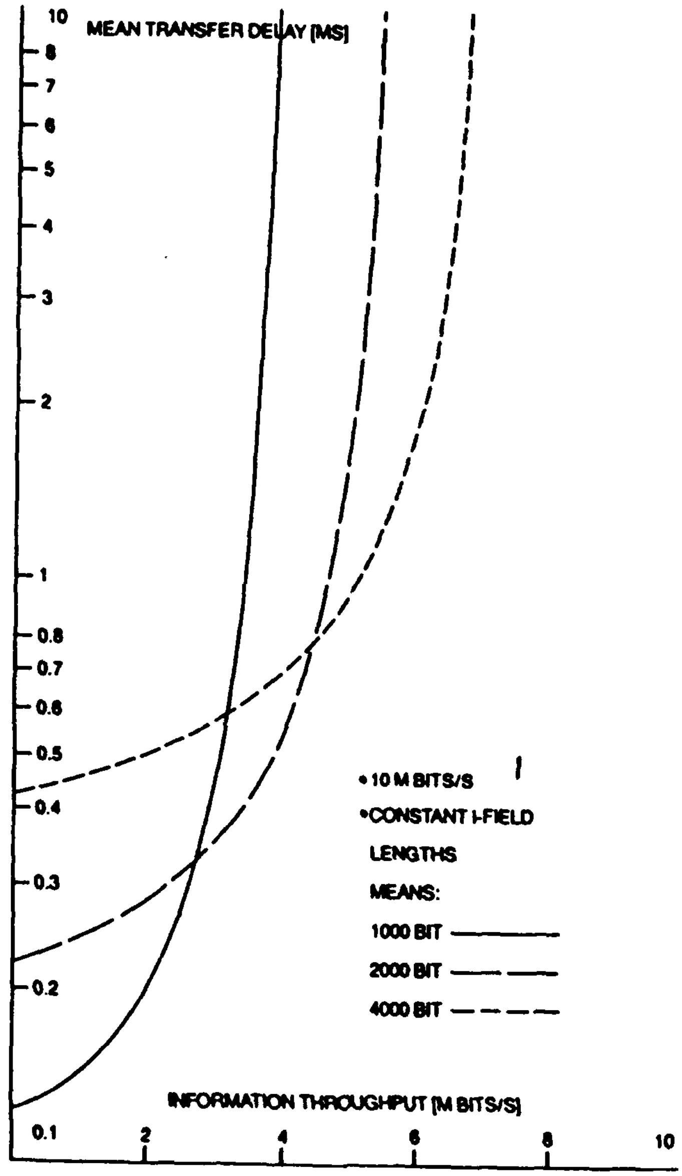


Figure 4.5 CSMA/CD Delay Throughput

Source (Bux, 1984, p. 361)

Figure 4.6 varies the number of stations on the network between five and 500 while holding the transmission rate at one Mbps. With a small number of stations, the token bus and token ring curves are very similar. With a large number of stations, the token bus has significantly lower performance while token ring is only slightly affected. This is due to the token passing along the "logical ring" on a bus which contributes significantly to the total delay with a large number of stations. The primary difference in overhead of the token ring and token bus is the time it takes to pass tokens between stations. In a ring, this time is simply the signal propagation time between the two stations (approximately five microseconds per km of cable) plus a small station delay as the signal is repeated. Buses require an explicit token frame of 152 bits to be passed to the next logical station, which may not be the physical neighbor, plus propagation delays which are significantly higher han a ring. (Sachs, Kan, Silvester, pp. 46-50)

C. RELIABILITY

Reliability, a measure of how vulnerable the system is to failures, is another important performance measure. Reliability is the ratio of the time during which the network is operating correctly to the time when it is not. Networks typically provide slower service more often than they incur total system failure. At what point this slow response becomes unacceptable depends on the end user. Topology and channel access protocols directly affect reliability. Arguably, the bus is the most reliable topology because a single node can fail without disrupting other network operations. Reliability is very crucial in deployed LANs. Support personnel and spare parts will be very limited during exercises or wartime. The criticality of the

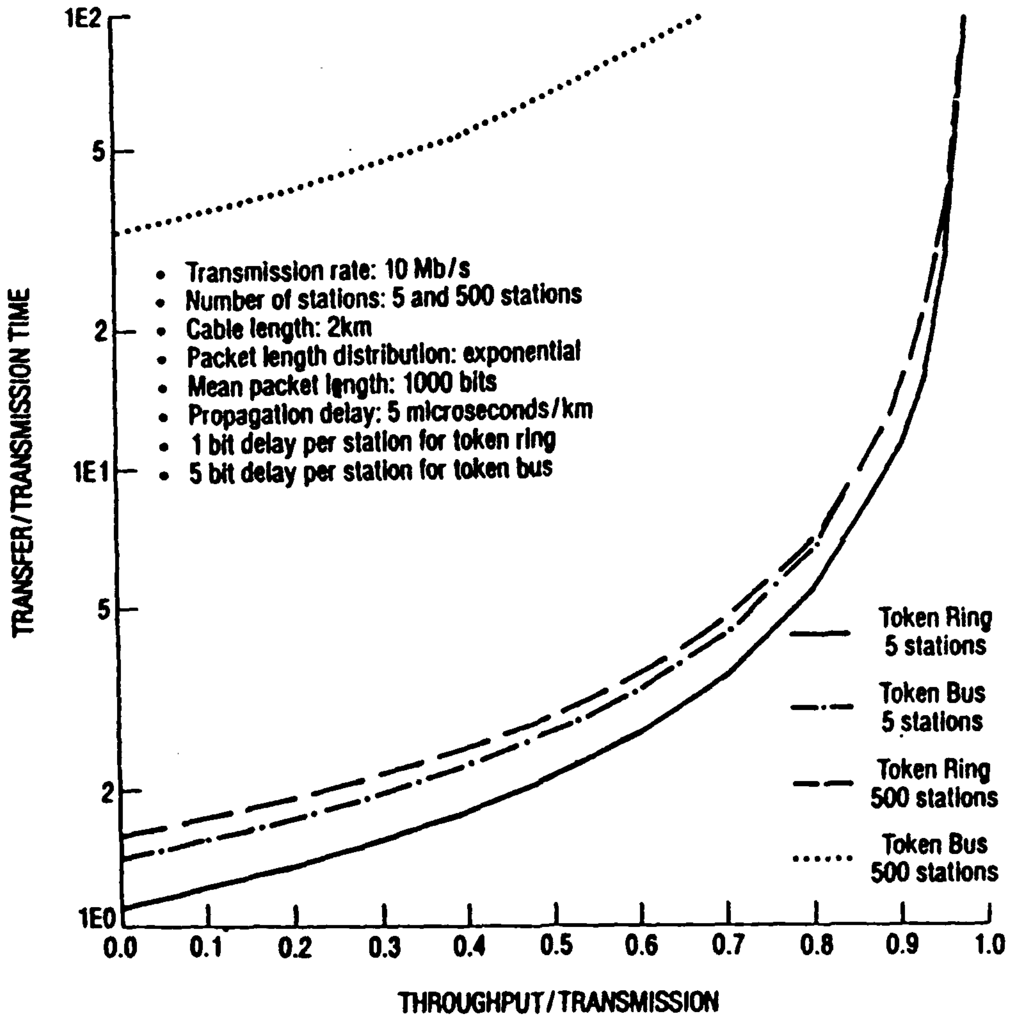


Figure 4.6 Varying the Number of Stations at 10 Mbps

Source (Sachs, Kan, Silvester, p. 50)

mission supported by deployed LANs also dictate a very high reliability must be attained. (Liu, pp. 417-426)

D. PERFORMANCE SYNOPSIS

Details on the various LAN protocols are found in Appendix B; however, this section presents a summary of them relative to performance issues.

> There have been numerous studies....of all three LANs (CSMA/CD, token ring, and token bus). The principle conclusion we can draw from these studies is that we can draw no conclusions from them. One can always find a set of parameters that makes one of the LANs look better than the others. (Tanenbaum, p. 164)

Performance is not the only consideration of LANs. Token rings have reliability problems due to network failure when a station attached to the ring fails. Redundant rings help overcome this; but, they are more costly and more difficult to set up in a deployed scenario. This chapter illustrated the fact that many measures of performance must be considered together when determining the best network for users' requirements.

As can be seen by the family of curves in this chapter, different LAN protocols are better suited for different circumstances. CSMA/CD is more applicable for low traffic LANs and token ring is more applicable for high traffic LANs. High traffic creates an increase in collisions and retransmissions unless a token scheme is used. Further details on when and why one scheme is better suited than others for some purposes are below.

1. CSMA

CSMA, CSMA/CD, and ALOHA (a simplified CSMA) all have low overheads and are applicable for low traffic load LANs. However, as the traffic load increases, the number of network accesses increases, the number of collisions increase, the number of delays increase, and the overall utilization decreases. These methods have short access delays when there is minimal traffic because there is no need to wait for a token; however, they also cannot prioritize transmissions and there is no upper bound on the access delay time as the load increases. Theoretically if the traffic load is high enough, a node may never gain access to the network. During high traffic periods, collisions become a major problem and throughput is drastically decreased. During low traffic loads, delays approach zero and throughput is usually adequate. These methods are appropriate for some LAN environments.

2. Token Schemes

As utilization increases, a token scheme is superior to CSMA/CD because there are no collisions or retransmissions. During heavy load periods, token rings are far superior to CSMA/CD especially if fiber is used. However, token rings and token bus schemes are not as efficient as CSMA/CD in low traffic environments as mentioned earlier. Due to the token passing scheme, an upper bound can be calculated for the maximum access delay. Token schemes also provide prioritization of transmissions. Message prioritization is necessary when critical messages must be transmitted and delays of several minutes cannot be tolerated. Utilization for token schemes is defined as the number of frames transmitted multiplied by the frame size.

This is then divided by the number of frames transmitted multiplied by the frame size plus the token size.

3. FDDI

FDDI has all the benefits described for the token schemes plus high throughput due to the use of fiber optics. It has an upper bound on access delays and is good for high traffic LANs or as LAN backbones. To provide increased reliability, FDDI is a dual token ring standard. FDDI has more overhead than non-token schemes, but the increased data rates more than compensate for the additional bits.

E. PERFORMANCE SUMMARY

As seen in this chapter, various LAN architectures perform differently when compared under a given set of parameters. Drastic differences exist between CSMA/CD and token ring as network access increases. CSMA/CD results in excessive delays as throughput increases. In a deployed environment, as hostilities, increase, the demand for access to the network will increase, and throughput will be strained. A token based scheme is the only architecture that guarantees access and satisfies throughput requirements.

V. CONCLUSIONS/RECOMMENDATIONS

A. PROBLEM ADDRESSED

In this thesis, the authors have: (i) described the basics of LAN technology, (ii) identified unique requirements of a deployed LAN, and (iii) discussed critical performance considerations. Recommendations for the proper selection of deployable LAN architectures are made below.

The most valuable resource deployed commanders have at their disposal is accurate information. The computer age has simplified, as well as complicated, the quest for accurate and current data. LANs can be force multipliers or an Achilles' heel if proper system design is not accomplished. As discussed in the previous four chapters, as well as in the following appendices, there are a wide variety of concerns which must be addressed when selecting a LAN. Unfortunately, there is no single magical answer to all military deployed LAN requirements. However, some general recommendations can be made.

B. RECOMMENDATIONS

1. Standards

Many of the military's current problems of standardization will be simplified by the ongoing transition from DoD protocols to ISO and IEEE standards. In the long run, industry standards are more cost efficient, more universally adaptable, and more likely to stay on the cutting edge of future technology. The combination of using industry standards and the use of gateways will give all military LANs the potential to be interconnected. Today's LANs no longer have to be restricted in design to match older existing systems' protocol or medium. Gateways provide interpretation between differing protocols and are relatively inexpensive.

2. Future Growth

In today's fiscally constrained environment, careful planning and analysis of today's and tomorrow's requirements must be considered. Even though today's requirement may be for the transmission of data between small computers, tomorrow's may include video conferencing and voice communications. Future LANs may include the requirement for commanders to have secure video teleconferencing capabilities in order to discuss alternatives for battlefield planning. Extra transmission channel capacity and the ability to expand the overall size and capabilities of the LAN must be addressed in the design stage. For the majority of LANs, allow at least a 50% margin for channel capacity growth.

3. Fiber Optics

The recent DoD contract award for a standard deployable fiber optic cable provides a light weight, durable, secure, and virtually noise free transmission medium for future deployed LANs. The military must consider size, weight, security, and interference immunity to be critical factors necessary in tomorrow's battlefield transmission medium. Each of these factors suggest fiber optics will be the deployed LAN medium choice of the future.

The ability of a LAN to continue to operate during the adverse atmospheric and physical conditions associated with military deployments is called survivability. The survivability of a deployed LAN can be increased by the use of fiber optic cable whenever possible, built in fault isolation devices, and avoiding single points of failure. Maintaining capacity during high activity periods is also attained by the use of fiber optic cable. Standard fiber optic cable and connectors also help alleviate potential connectivity problems. Flexibility is obtained through system design and standardization. Mobility is also increased with the lightweight fiber optic cables. They are easy to transport, set up, and use. With the many advantages of fiber optics and the decreasing costs associated with fiber, it should grow into the standard transmission medium for deployable LANs.

4. Topology and Protocols

Topology is often an overlooked aspect of LANs in conjunction with deployability concerns. A system which works well in the fixed office environment may not be optimal for the deployed environment. Redundancy and lack of single points of failure, such as the central node of a star topology, are critical in the design of deployable LANs. A double ring or mesh topology is best for providing redundant paths. Single points of failure cannot be relied upon in a deployed environment.

Protocols such as CSMA/CD or token passing protocols must be used to handle contention, collisions, and retransmissions of data packets. In most deployed LANs, prioritization of packets is a critical requirement. For example, a local commander's operations orders should not wait in a transmission queue behind the local weather report. The token ring protocol has built in prioritization capabilities and should be the protocol of choice until FDDI fully matures as a standard. As explained in Chapter IV, the token ring is the least sensitive protocol to workload, message size, and the number of nodes on the network. However, double rings should be used to take care of potential reliability problems. The additional initial expense for procurement will more than pay for itself with significantly less down time during possible hostile situations. When FDDI matures, it will have similar characteristics of the token ring protocol as well as provide a dual ring topology and permit data rates well over 100 Mbps.

Currently, draft plans exist for implementing FDDI on board ships and military aircraft. The Survivable Adaptable Fiber-Optic Embedded Network (SAFENET II) is a ruggedized version of FDDI for the U.S. Navy. It is designed to provide the necessary performance while reducing shipboard cabling weight by 75%. The Military Fiber-Optic Transmission System (MFOTS) is designed to integrate the FDDI standard into advanced avionics systems. The improved performance, reliability, and reduced weight are even more critical for avionics systems. Additionally, FDDI has been recommended for use on the U.S. Space Station. FDDI promises to be the topology and protocol of choice for tomorrow's LANs. (Moore, Oliver, pp. 40,42)

5. LAN Specialist

A critical recommendation concerns the LAN from the requirements stage through development and operations. Networking technology brings together the disciplines of computers, communications, and electrical engineering. A LAN expert must be knowledgeable in each of these ares. The knowledge in these areas is essential to be able to perform the necessary technical analysis and make informed recommendations. (Hansen, p. 562) A qualified LAN/computer/communications expert must be intimately involved with the project at every stage. The expert cannot specify mission needs, but can assist in the analysis of requirements, ensure requirements are clearly stated, and recommend an appropriate course of action. Significant savings can be attained by designing the system smart from the beginning. The correct design must be developed to most cost efficiently meet the users' needs. For example, the clustering of similar tasks onto small LANs bridged to a backbone can drastically reduce the needed throughput of the backbone. This seemingly simple idea in the operations concept could save thousands of dollars in hardware.

The single magical LAN which meets everyone's needs will always elude us. Users' needs vary a great deal from system to system. This is the reason so many different standards exist today. The answer to this problem is to rely on a communications/computer support staffs with sufficient LAN expertise to assist in transforming user requirements into the proper system design parameters. The authors hope that this document will be used by users and planners to enable them to make more educated decisions on deployable LANs.

C. CONCLUSIONS

Appropriate network planning is necessary for sound network design. The recommendations above provide general direction for LAN architecture development. However, the final decisions must consider each units' unique requirements.

Below is a summary of recommendations:

- DoD should continue to transition to ISO and IEEE LAN standards
- Allow for sufficient growth margin in channel capacity when designing deployable LANs
- Utilize fiber optics in deployable LANs due to security, channel capacity, and survivability as the discussion of fiber optics detailed
- Use a double ring or mesh topology to increase reliability and survivability
- Use a protocol which allows packet prioritization such as token ring
- Utilize FDDI as it matures
- Involve a LAN/computer/communications expert at every stage of development from requirements through operations.

APPENDIX A LAN MEDIA

There is a wide variety of media available for use with LANs. Careful analysis should be performed before the decision on medium is made. The medium is the most critical and most vulnerable component of LANs. Without the medium, the LAN cannot function. If cabling is severed or a radio transmission jammed, the LAN can be rendered useless. The most suitable LAN media are twisted pair, coaxial cable, optical fiber, radio, and directional radiation. The type most commonly used is coaxial cable, commonly called "coax". A description of each type, their respective advantages, and disadvantages are provided below.

A. TWISTED PAIR

Twisted pair is most commonly used by telephone companies. Twisted pair is very good for low frequency voice communications. It consists of two pair of copper wires spiraled together in the form of a helix to provide fairly constant electrical characteristics and help reduce noise. However, twisted pair is still very susceptible to noise and crosstalk from other nearby twisted pair because it is generally unshielded. Analog or digital signals can be processed at rates up to ten Mbps. Bus, ring, and star topologies can be implemented inexpensively using twisted pair.

Some of the advantages of twisted pair are:

- inexpensive
- physically very flexible
- well understood technology
- quick easy installation using common skills
- can run several major LAN topologies and protocols

Some of the disadvantages of twisted pair are:

- limited distance
- high error rates
- difficult to troubleshoot
- limited bandwidth and data rates
- poor performance during high traffic
- noise due to crosstalk or interference
- poor security, easy to tap, emanations intercepted (Gee, pp. 48-49; Stallings 1983, pp. 22-23)

B. COAXIAL CABLE

Coaxial cable is most commonly used by the cable television industry. It consists of a central conductor which carries the signal, concentrically surrounded by insulation, shielding, and a protective coating. The shielding is metal mesh or wrapping to protect against radio frequency interference. Coaxial cable costs more per foot than twisted pair; however, due to its ease of installation, it is the medium of choice for most of today's LANs (more than 90%). Coaxial cable is much more noise resistant than twisted pair; therefore, it can be used for longer distances and higher data rates. It can transmit over 400 Mbps and is used in ring, bus, and tree topologies. Bus and ring topologies may be implemented using baseband transmission. Bus and tree topologies may be implemented using broadband transmission. Baseband and broadband transmissions are discussed later in this section.

Some of the advantages of coaxial cable include:

- durability
- high bandwidth
- more immune to noise than copper wire-pair
- supports voice or data
- uses off the shelf connectors
- simple installation and troubleshooting
- carries signal further than twisted pair
- needs no extra physical protective measures
- better electrical characteristics than twisted pair

Some of the disadvantages of coaxial cable are:

- can be difficult to bend
- not secure
- expensive to install and maintain
- modems are required at each user station for broadband
- extra cost of taps, repeaters, amplifiers (Gee, pp. 49-50; Stallings 1983, pp. 24-26)

1. Baseband

Although coaxial cable is the most popular LAN medium, it remains to be seen whether baseband or broadband becomes dominant. Baseband, digital communications typically have data rates of one to ten Mbps. Simple interface units are used instead of modems. This method is best suited for short distances. Distances of over a few thousand feet require expensive signal repeaters or drivers to regenerate the signals.

Some of the advantages of baseband systems are:

- no modems required
- easy to install and maintain
- inexpensive to operate and maintain

Some of the disadvantages of baseband systems are:

- one channel
- limited distances
- poor noise immunity (in repeaterless applications)
- limited topology (primarily bus) (Gee, pp. 26,30; Krutsch, pp. 105-112)

2. Broadband

Broadband or analog communications signals are modulated on an analog carrier signal and can be sent on several channels along the medium. This allows several different signals to be multiplexed. An example of this is the many channels transmitted along a single coaxial cable television system. Typically, frequency division multiplexing is used to share the bandwidth available by well over 50 separate channels. Each channel can carry almost as much information as the entire baseband LAN in voice, digital, or video form. Typical bandwidth may be as high as 450 MHz.

Some of the advantages of broadband systems are:

- multiple channels
- good noise immunity
- longer distances available
- voice, data, and video sources may be multiplexed together
- can carry analog and digital information
- topological flexibility (bus and tree)
- many simultaneous independent communications paths possible

Some of the disadvantages of broadband systems are:

- difficult to install
- higher maintenance cost
- high propagation delays possible
- modems required at all terminals (Gee, pp. 26,30,45; Krutsch, pp. 105-112; Kummerle, pp. 62-66)

The advantages and disadvantages of baseband and broadband schemes must be carefully weighed when selecting the proper scheme for specific LAN requirements.

C. FIBER OPTIC CABLE

Fiber optics communications utilize the transmission of visible or infrared light rather than the traditional electrical signal as a means of communications. Since optical fiber is a dielectric, it does not conduct electricity and is unaffected by electrical interference. Today's fiber optic cables are tough, yet flexible, relatively secure, non-conductive and thus, relatively free from interference. Fiber links have error rates of less than one bit per billion transmitted. Fiber optic tensile strength is higher than copper wire and it is not affected by water or corrosion. Fiber optic cable is best suited for long-haul point-to-point communications. Fiber use in deployed systems is currently very limited but is increasing because ruggedized cable is now being produced to meet military standards.

Fiber optic cable consists of fine strands of glass, silica, or plastic called the transmitting core surrounded by a layer with lower refractivity called the cladding to make the light rays reflect down the cable. Each fiber is usually covered by an opaque material jacket which keeps stray light out of the fiber. Data is converted into light by a light emitting diode, or similar device, transmitted along the path, and finally converted back into an electrical signal on the receiving end.

Fiber has a much lower signal loss and less noise than a copper medium. Materials used to produce optical fibers are virtually immune to material shortages that copper may experience at times. Fiber cabling offers a ten to one reduction in weight over copper.

Data may be transmitted for over two kilometers between repeaters. Figure A.1 shows the relative amount of signal attenuation per kilometer of twisted pair, coaxial, and fiber optic cable relative to their operating bandwidth.

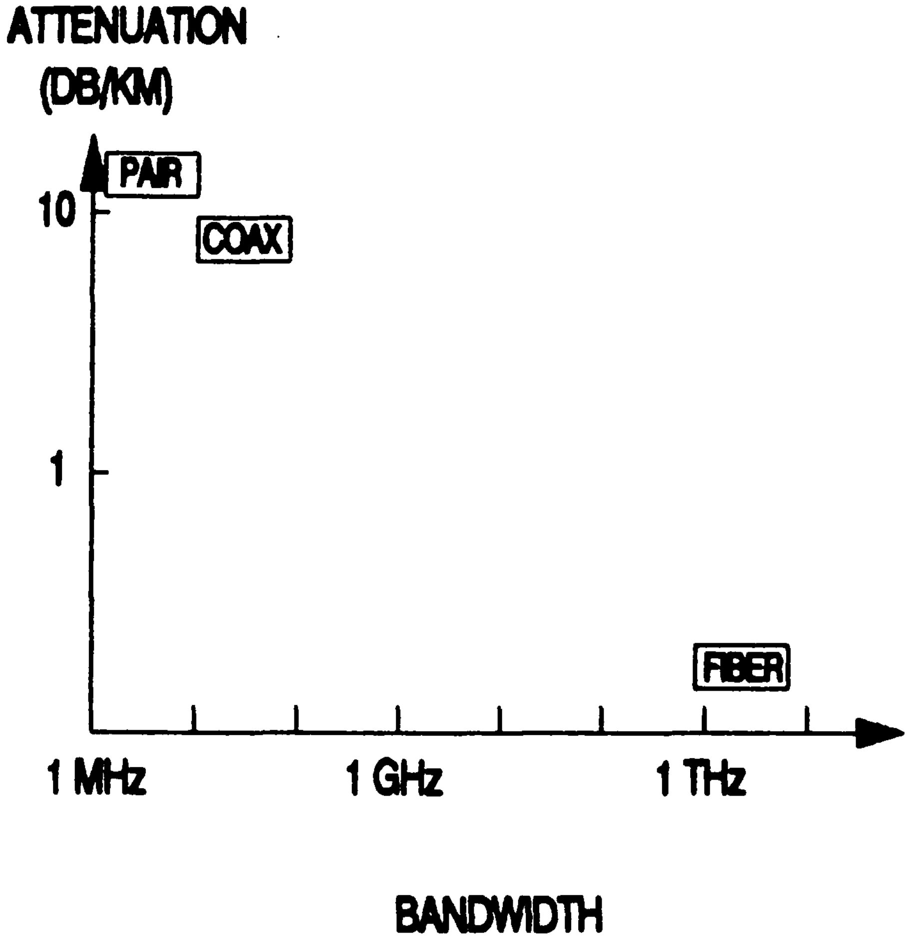


Figure A.1 Signal Attenuation vs. Bandwidth, Various Media

Source: (Henry, p. 20)

Fiber has extremely high data rates which easily exceed 100 Mbps. The potential capacity of fiber optics has not yet been tapped; ranges as high as Terra (10^{12}) bps may be possible. Fiber is most often used in ring or star topologies. The bus/tree topology is difficult to implement with fiber optics.

Some of the advantages of fiber optics are:

- small size
- lightweight
- no emanations if properly shielded
- noise immunity
- high data rate
- large bandwidth
- low attenuation loss
- immune to interference (crosstalk and jamming)
- very low bit error rate
- secure, difficult to tap
- electromagnetic pulse immunity

Some of the disadvantages of fiber optics are:

- poor flexibility (multi-strand, bundled cable)
- expensive repeaters may be necessary
- difficult to add peripherals or work stations
- skilled installation and maintenance personnel required (Gee, pp. 50-51; Stallings 1983, pp. 26-29; Glass, pp. 6-8)

D. RADIO

Transmission of data over radio frequencies is another option for LAN medium. To provide the necessary data rate for an operationally viable LAN, micro or millimeter wave radio transmissions must be used. The use of radio can greatly extend the range of a LAN without using repeaters and eliminates the time consuming process of laying heavy, bulky cable. However, the use of radio transmissions increases the risk of interception, jamming, and detection by the enemy.

Advances in microwave technology can mitigate the risks of interception and jamming. These advances are generically categorized as Low Probability of Intercept (LPI) or spread-spectrum modulation techniques. Spread-spectrum systems require a transmission bandwidth much wider than that necessary to transmit the information. By distributing the signal over a wider band, the signal appears more like random noise than data and is difficult to detect and interpret by receivers other than those intended. (Javed, pp 11.20-11.22) Specific spread-spectrum techniques include direct sequencing and frequency hopping.

Direct sequencing involves the use of a code word to hide information bits. Each information bit is multiplied by a code word, which is several bits long, and the result transmitted. A very low transmitter power is also used to make an intercepted signal appear like noise. The receiver uses the same code word to compress the signal. (Pratt, Bostian, pp. 251-256) As long as the enemy does not posses the code word, the signal cannot be correctly interpreted. To attempt to jam the signal, the enemy would have to transmit over a very wide spectrum. This decreases the power of the interference signal and, in turn, decreases the effect of the jamming signal. (Pursley, pp. 24.23-24.24)

Frequency hopping utilizes an apparently random (hence, "pseudorandom") selection of frequencies to transmit data in a very wide band (Pratt, Bostian, p. 256). Only the intended receiver knows the sequence of frequency selection. As the number of available frequencies increases, the effect of jamming decreases. Again, as long as the enemy does not have access to the frequency selection algorithm, the signal cannot be accurately interpreted. An added feature of frequency hopping is that even though a wide transmission band is required, only a small portion is utilized at any instant. Therefore, the band can be shared by other narrow band users as long as the signals do not overlap simultaneously in frequency and time and corrupt one another. (Pursley, 24.22-24.23)

Even though spread-spectrum techniques can lessen the effects of hostile jamming, the threat still exists. If the enemy can isolate any frequencies used or can jam wide frequency bands, errors can be injected. Because of this, some means of error detection and correction must be employed. Another important consideration of using spread-spectrum techniques is that necessary bandwidth to employ such techniques may not be available in the deployed area due to the crowded radio spectrum.

Another concern when evaluating microwave radio transmission as a suitable medium for a deployed environment is the atmospheric effects on the signal. The signal is attenuated as it propagates through the atmosphere. Moisture in the atmosphere also absorbs much of the signal strength. This effect can be countered by increasing transmitter power to ensure adequate signal strength for detection and correct interpretation by the receiver. (Rogers, pp 1.1-1.19)

Standard water content of the atmosphere is normally considered when determining required power for a communication system. Consideration must also be given to the added attenuation caused by rainfall, fog, and clouds. The extent of the effect is dependent on geographic location. If heavy rainfall is common in the deployed environment, the increased attenuation must be offset by providing greater transmitter power. (Schwendtner)

Terrain is another factor limiting the use of radio transmission. Microwave links for LANs need line-of-sight (LOS) transmission. Between fixed complexes, LOS can be easily accommodated. Terrain for a deployed LAN varies with each environment. Rough terrain can greatly limit the range of the LAN and in some cases provide less range than if cable had been used. (Gee, pp 51; Stallings 1983, pp. 29-32)

The use of radio transmission for LAN medium is feasible and in some circumstances very effective. Before this form of medium is chosen, careful evaluation of potential environments must be performed.

E. DIRECTIONAL RADIATION

Directional radiation technologies include atmospheric infrared, microwave, and lasers. These technologies utilize the atmosphere as a medium and are always subject to adverse atmospheric conditions. They are also all line-of-sight and are subject to physical obstruction. They have moderate noise immunity and low to medium data rates. They are typically utilized for point-to-point communications between buildings or complexes. Infrared transmitter/receiver sensors are often placed on the ceiling of a room to radiate to all terminals located within the room. This alleviates the necessity of individual cabling of many work stations in a close proximity.

Some advantages of directionally radiated media are:

- little or no cabling is required
- immune to electromagnetic interference

Some disadvantages of directionally radiated media are:

- subject to physical obstructions
- subject to atmospheric interference or jamming
- limited to point-to-point links (star or ring) (Gee, p. 50; Stallings 1983, pp. 32-34)

APPENDIX B LAN STANDARDS

A set of standards has been established by the IEEE for Local Area Networks. These standards, along with the Fiber Distributed Data Interface (FDDI), will be discussed in some detail along with the advantages and disadvantages of each.

A. IEEE 802.2 LOGICAL LINK CONTROL (LLC)

The LLC is the top layer of the LAN communication architecture. This layer primarily provides the means to exchange data between LLC users through the Medium Access Control (MAC) layer. The LLC and the MAC layers together are the LAN equivalent to the data link layer of the ISO model. The LLC provides a higher level of protocol and additional services to users. (Stallings 1987, pp. 53-55)

The LLC is primarily responsible for initiating control signals, organizing data flow, interpreting commands, determining appropriate response, and performing error control (Myers, p. 32). The LLC is most useful when communication is required between nodes on networks using different protocols (Biersack, p. 36). The LLC layer is not required for LANs; but, the MAC layer must be able to interface to it if those services are needed. By using the LLC, the underlying LAN protocol is transparent to the user. Most LAN users are connected directly to the MAC layer. For this reason, the remaining LAN standards will be addressed from this perspective.

B. IEEE 802.3 CSMA/CD

IEEE 802.3 defines the CSMA/CD MAC protocol for a bus topology using a variety of transmission media and data rates. The standard is divided into the physical layer and MAC layer specifications

The physical layer specifications are divided into two general categories: medium independent and medium dependent specifications. The medium independent specifications refer to the interface between the MAC and physical layers, the medium attachment unit, and the attachment unit interface. (Stallings 1987, p. 85) The medium dependent specifications refer to the actual LAN medium used. This part of the standard addresses such topics as signaling, media types, and data rates.

The MAC layer specification defines the services provided to the LLC or MAC level user and the MAC protocol. The MAC layer hides unnecessary details of the services and the physical medium from the user. The specification identifies the means of transmitting and receiving Protocol Data Units (PDUs) or data frames. The specification identifies CSMA/CD as the protocol for the standard and specifies the format of the data frame. (Stallings 1987, pp. 84-86)

According to the standard (Stallings 1987, p. 88), the rules for this protocol follow these steps:

1. If the medium is idle, transmit a data frame. Otherwise, go to step 2.
2. If the medium is busy, continue to listen until the medium is sensed idle and then transmit immediately.

3. If a collision is detected during transmission, transmit a brief jamming signal to assure that all stations know that there has been a collision and then cease transmission.

4. After transmitting a jamming signal, wait a random amount of time and return to step 1.

The standard also describes a parameter called a time slot. The time slot is defined as the time it takes a signal to travel from one end of the medium to the other and back. From this definition, it is obvious that this time is dependent on the medium being used.

The MAC layer specification provides a description of the format of the data frame for the IEEE 802.3 protocol. Figure B.1 shows the general format of the frame. The frame consists of eight fields. These fields are described as follows:

1. Preamble: A field consisting of seven bytes containing the bit pattern 10101010. Its purpose is to synchronize the receiver's clock with the sender's.

2. Start of Frame Delimiter (SD): One byte with the bit pattern 10101011, and serves as an indicator to the receiver that this is the start of the data frame.

3. Destination Address (DA): This field identifies the intended receiver(s) of the data frame. The destination address may be for a single station, a group of stations, or all stations. The field can be either 16 or 48 bits long and must be consistent for all stations. The length is specified at implementation time.

4. Source Address (SA): The address of the station originating the data frame. This field can also be either 16 or 48 bits long, and must match the destination address.

5. Length: A field two byte long which identifies the number of bytes in the data field.

6. Data: A field of zero to 1500 bytes long which contains the actual data to be sent to the receiver.

# OCTETS	7	1	2 OR 6	2 OR 6	2	0-1500	VARIES	4
	PRE	SD	DA	SA	LEN	DATA	PAD	FCS

PRE = PREAMBLE
SD = START DELIMITER
DA = DESTINATION ADDRESS
SA = SOURCE ADDRESS
LEN = LENGTH OF DATA FIELD
DATA = INFO TRANSMITTED
PAD = PAD FOR DATA FIELD
FCS = FRAME CHECK SEQUENCE

Figure B.1: IEEE 802.3 Data Frame Format

7. Pad: May not be required. Its purpose is to ensure the frame is long enough to allow proper collision detection. The frame must be long enough to take more than one bit slot to transmit. If the data frame is sufficiently long, the pad field is not required.

8. Frame Check Sequence (FCS): A 32 bit field used for error detection. This number is computed based on the contents of the destination and source addresses, the length, data, and pad fields. The FCS is also known as a Cyclic Redundancy Check (CRC) field. When the receiving station receives a data frame, it recomputes the CRC and compares it to the received value. If the CRCs match, then the frame is assumed to be correct. If the CRCs do not match, then an error has occurred and the originating station must retransmit the frame. (Tanenbaum, pp. 144-145; Stallings 1987, pp. 91-93)

In summary, IEEE 802.3 is typically used for low to medium network access environments. It is based on the CSMA/CD protocol and requires a bus topology. This standard is goof for minimal access situations. However, as traffic on the network increases, the number of collisions also increases causing excessive delays. Additionally, there is no guarantee a user will ever be granted access to the network. Continuous collisions could prevent a node from ever being able to successfully transmit its data.

C. IEEE 802.4 TOKEN BUS

The IEEE 802.4 standard defines the token bus MAC protocol. The standard specifies a bus topology, and allows for a variety of transmission media. It also specifies the use of analog signaling. This standard, like 802.3, provides specifications for both the physical and MAC layers. (Stallings 1987, p. 117)

The MAC layer specification defines the services provided by IEEE 802.4 to higher level users and the protocol used to communicate to other MAC layers. The token bus standard specifies that the nodes will be ordered to form a logical ring even though they are physically connected using a bus topology. Each node knows the address of the nodes logically before and after it. The next logical node may or may not be the closest physically. The last node is followed by the first. Figure B.2 shows the ordering of the nodes and the direction of data flow over the bus to form a ring. The protocol specifies that access to the medium shall be controlled through the use of a token. When a station has something to transmit, it must first capture the token before it can transmit its data. When the token passes a node, a node may capture the token and transmit data frames until it is finished or until the maximum token hold time is reached, whichever comes first. When the station is finished, or if it has no data to transmit, it passes the token on to the next node.

Message prioritization is an optional feature of the 802.4 protocol. The purpose of this feature is to provide a means for higher priority messages to be transmitted ahead of those of lesser priority. The standard allows for four different classes of data. Transmission of a given class is based on the amount of time the station has had the token. As long as the token hold time is less than a set value for a class of data, the associated class of data frames can be transmitted. Once the threshold has been exceeded, the next class is checked. This continues until all frames are transmitted or the maximum token hold time expires.

The 802.4 standard specifies eight message frame formats. One specifies the format of the token and another specifies the format of a data frame. The other six specify the control frames used for maintenance of the logical ring.

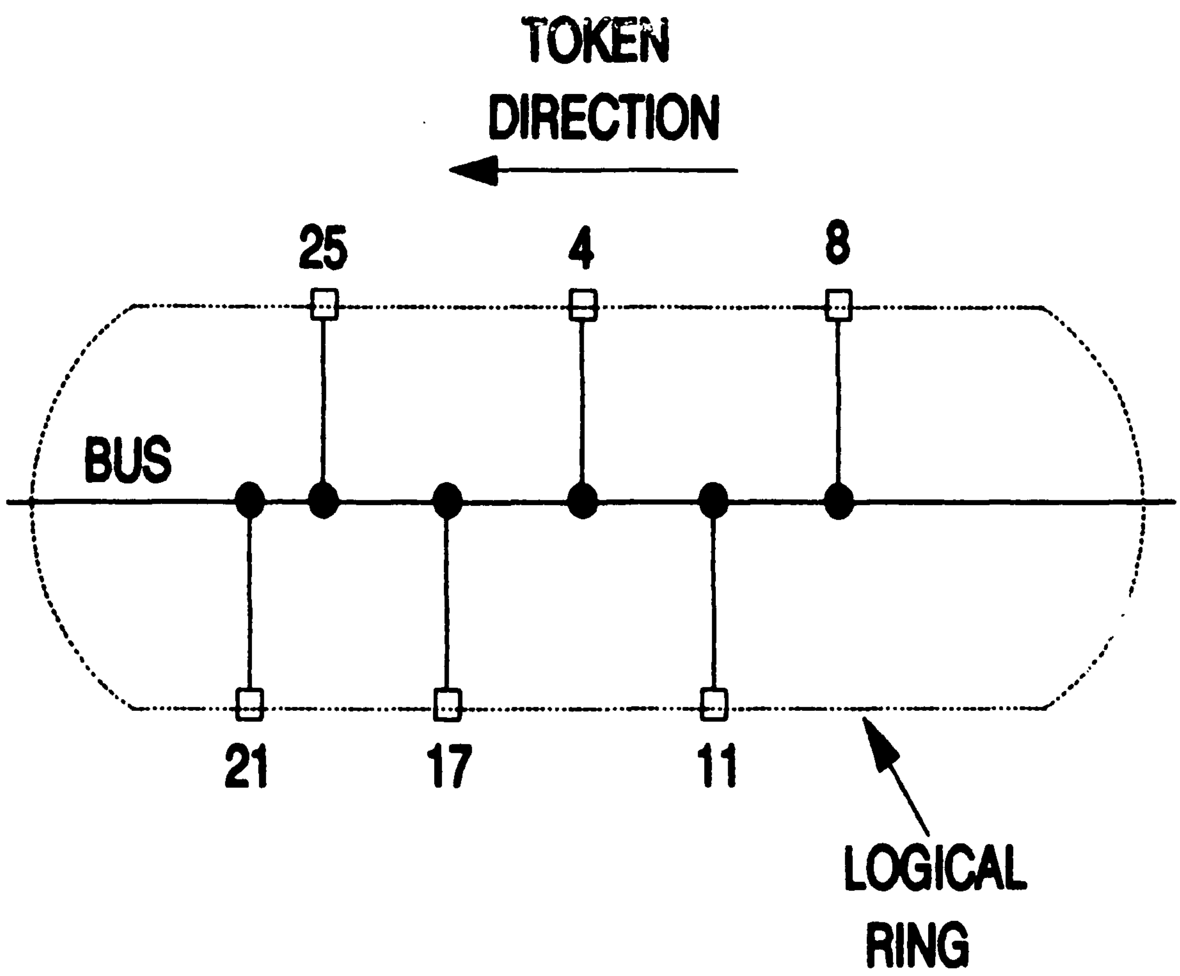


Figure B.2 IEEE 802.4 Token Bus Node Configuration

The token and data frame are shown in Figure B.3. A frame consists of the following fields:

- Preamble: This field is a series of one or more eight bit patterns used to establish synchronization with other nodes.

- Start Delimiter (SD): This field is a special eight bit pattern that indicates the actual beginning of the frame. It is distinguishable from data because of the use of a unique non-data symbol used in the pattern and is coded as follows: NN0NN000.

- Frame Control (FC): This field indicates whether the frame is a token, a data frame, or a control frame.

- Destination Address (DA): This field specifies the intended receiver(s) of the frame. It can be 16 or 48 bits in length and must be consistent throughout the network. For the token, this is the address of the successor station.

- Source Address (SA): This field holds the address of the sender of the frame. Its length must be the same as the destination address.

- Data: (Only applicable to the data frame) This frame contains the data to be transmitted to the designated receiver. It is 8182 bytes long if a 16 bit address is used, or 8174 bytes long if a 48 bit address is used (Tanenbaum, p. 151).

- Frame Check Sequence (FCS): This field is 32 bits used for error detection. This number is calculated from the contents of the FC, DA, SA ,and data fields. The FCS is also known as the Cyclic Redundancy Check (CRC) field. When the receiving station receives a data frame, it recalculates the CRC and compares it to the received value. If the CRCs match, the frame is assumed to be correct. If the CRCs do not match, an error has occurred and the originating station must retransmit the frame.

- End Delimiter (ED): This is a unique pattern used to identify the end of the frame. The pattern for this is: NN1NN1IE, where N is a non-data bit, I is the intermediate bit, and E is an error bit. If I is set to one, it indicates the final frame to be sent by the active node. If E is set to one, then one of the repeaters along the bus detected a discrepancy between the contents of the frame and the FCS. (Stallings 1987, pp. 131-133)

# OCTETS	>1	1	1	2 OR 6	2 OR 6	8182 OR 8174	4	1
	PRE	SD	FC	DA	SA	DATA	FCS	ED

DATA FRAME

PRE	SD	FC	DA	SA	FCS	ED

TOKEN

PRE = PREAMBLE
SD = START DELIMITER
FC = FRAME CONTROL
    DATA = 01MMMPPP
    TOKEN = 00000100
DA = DESTINATION ADDRESS
SA = SOURCE ADDRESS
DATA = INFO TRANSMITTED
FCS = FRAME CHECK SEQUENCE
ED = ENDING DELIMITER

Figure B.3 IEEE 802.4 Data Frame and Token Formats

Token bus has the following advantages:

- Throughput increases with data rate and levels off as the medium saturates
- All nodes get an opportunity to access the medium
- Message prioritization is possible
- An upper bound on a nodes' wait time before transmit is known; therefore, it is more adept for use with real time applications.

Token bus has the following disadvantages:

- highly complex protocol algorithm
- high overhead resulting in considerable delay time during light load. The delay for a node to transmit is due to the wait for all other stations to pass the token before it can transmit.

D. IEEE 802.5 TOKEN RING

The IEEE 802.5 standard defines the token ring MAC protocol using a ring topology. The physical layer is based on the use of shielded twisted pair and Differential Manchester signal encoding. The standard specifies the services and capabilities of the physical and MAC layers. The physical specifications are separated into medium independent and medium dependent portions. The medium independent portion of the standard has the following specification:

- one or four Mbps data rates;
- differential Manchester technique for signal encoding for data and non-data symbols;
- one bit-time delay at each node, where bit-time is computed as the reciprocal of the data rate (i.e., One Mbps data rate gives 1×10^{-6} bit-time). (Stallings 1987, p. 170)

The bit-time is a key issue when determining the length of the ring. The ring must be long enough for the entire token to be placed on the network before returning to the node transmitting the token. Since the token is 24 bits long, the amount of time before the signal returns to the originating node must be greater than 24 x 10^{-6} seconds for a one Mbps data rate, or 6 x 10^{-6} seconds for a four Mbps data rate. This implies the sum of the propagation delay for the medium and the accumulated one bit delays for each node must be greater than 24 x 10^{-6} seconds or 6 x 10^{-6} seconds depending on the transmission rate used.

The medium dependent portion of the standard simply specifies the use of two 150-ohm shielded twisted pair wires for the transmission medium. (Stallings 1987, p. 172)

The MAC layer protocol is based on the use of a token frame. The token circulates around the ring until it is captured by a node with data to transmit. Once a node captures the token, no other node can transmit until the token has been released. The token is released when the possessing node has transmitted all data frames or the specified Token Hold Time (THT) has elapsed. When the token has been replaced on the ring, the next node will have the opportunity to capture it and transmit data. If the next node has no data to transmit, the token is simply passed on. (Stallings 1987, p. 150)

IEEE 802.5 specified the following fields for the data frame which is depicted in Figure B.4. (Stallings 1987, pp. 153-154).

- Start Delimiter (SD): This field indicates the start of a token or data frame. It is an eight bit field coded as follows: JK0JK000. J and K are non-data symbols and are used to distinguish between this field and data fields. The actual representation of the symbols depends on how the signals are encoded on the medium.

- Access Control (AC): This is an eight bit field consisting of three priority, one token, one monitor, and three reservation bits. The priority and reservation bits are used to facilitate message prioritization. Further explanation of the priority scheme will be discussed later. The token bit identifies whether it is a token (0) or a data frame (1). If this bit is 0 then the next field is the ending delimiter. The monitor bit is used in ring maintenance.

- Frame Control (FC): This is an eight bit field with two bits to identify it as a MAC or LLC data frame. If it is a MAC frame, the remaining six bits are used to identify the type of MAC frame.

- Destination Address (DA): This field identifies the intended receiver of the frame. Addresses can be chosen as either 16 or 48 bits long. The length is determined prior to LAN implementation and must be consistent for all nodes on the LAN. The address scheme allows for single receiver, multiple receiver, or broadcast to all nodes.

- Source Address (SA): This field contains the address of the node originating the frame. SA must be the same length as DA.

- Information (INFO): This field contains the data to be delivered to the destination address.

- Frame Check Sequence (FCS): This field is a 32 bit cyclic redundancy check (CRC) computed from FC, DA, SA and INFO fields. The FCS is used for error detection. If DA or any intermediate node does not compute the same FCS as provided by the source node, then an error has occurred.

- Ending Delimiter (ED): This field indicates the end of the transmitted data frame or the last field of a token. The contents of the field are as follows: JK1JK1IE. J and K are non-data symbols like those in SD. The intermediate frame bit, I, is used to indicate the last or only frame (0), or more frames to follow (1). E is the error-detected bit and is set by any station detecting a discrepancy based on the FCS or detection of a premature non-data symbol.

OCTETS

1	1	1	2 OR 6	2 OR 6	> 0	4	1	1
SD	AC	FC	DA	SA	INFO	FCS	ED	FS

SD = START DELIMITER

AC = ACCESS CONTROL

FC = FRAME CONTROL

DA = DESTINATION ADDRESS

SA = SOURCE ADDRESS

INFO = INFORMATION FIELD

FCS = FRAME CHECK SEQUENCE

ED = ENDING DELIMITER

FS = FRAME STATUS

Figure B.4 IEEE 802.5 MAC Data

Frame Format

- Frame Status (FS): This field is eight bits long consisting of two duplicate four bit fields to provide redundancy external to the FCS. Of the four bits, only two are used: the address recognition bit (A) and the frame copied bit (C). (Stallings 1987, pp. 153-154)

Each node listens to the ring for frames intended for them by reading each bit before passing it on. This process introduces a one bit-time delay at each node as the frame passes. As the frame passes the node, it is checked for errors. If an error is detected the E-bit of the ED field is set to one. When a frame detects its own address in the DA field, it will attempt to copy the frame into its buffer. The node then sets the A-bit and if successfully copied, it sets the C-bit of the FS field to one. When the frame returns to the originating node, the E, A, and C-bits are checked to determine the result of the transmission. It should be noted that if transmission is not successful, the MAC layer does not attempt to retransmit the frame. The failure is reported and retransmission is determined by a higher layer.

The IEEE 802.5 standard provides a message prioritization feature through the use of the priority and reservation bits specified in the AC field. The feature is provided to allow nodes with higher priority data quicker access to the network. When prioritization is used, a node must wait until a token with a priority less than or equal to the priority of its message before it can capture the token and transmit its data. If a node cannot capture the passing token or has a message of higher priority than the current data frame, it can reserve a future token by setting the reservation bits. Before the node sets the reservation bits, it must first ensure the token has not already been reserved for a higher priority message. If a node increases the value of the priority or reservation bits, it is also responsible for lowering them to their previous values. When a node regenerates a token, it will set the priority field of the token to the higher of the previous priorities or the reserved priority. (Stallings 1987, pp. 157-162)

In summary, IEEE 802.5 is best suited for networks requiring long periods of medium to high access rates. Access to the network is guaranteed through the use of a token. Each node holds the token for a maximum specified time; therefore, the maximum possible delay for a node to transmit can be accurately computed. Additionally, IEEE 802.5 facilitates message prioritization. This permits higher priority users quick access to the network and allows critical information to be distributed in a timely manner.

E. FIBER DISTRIBUTED DATA INTERFACE

Fiber Distributed Data Interface (FDDI) is currently being developed by Accredited Standards Committee (ASC) X3T9. The FDDI standard calls for a 100 Mbps LAN using fiber optic cable as the transmission medium. FDDI is a token passing protocol which is modeled after the IEEE 802.5 Token Ring standard. This standard specifies the services and capabilities of the physical and MAC layers. The broad services are provided to allow individual units the necessary flexibility to optimize the network for their unique needs. (Ross, p. 1043)

FDDI LANs may be used as a stand-alone LAN or operate as a high speed backbone connecting several lower speed LANs. This allows low network utilization workstations to be grouped together on separate smaller LANs using, for example, CSMA/CD. The smaller LAN can then be connected to the high speed FDDI backbone to provide communication to other high speed network utilization workstations.

Figure B.5 illustrates how IEEE 802 standard LANs can be connected to the high speed FDDI through the use of gateways. This architecture allows users to be grouped together on their own LAN and still communicate to other users on the FDDI LAN. For example, workstations with low network utilization requirements could be grouped together on an 802.3 LAN and still pass information to high utilization users through a gateway when necessary. Another advantage is that a unit can connect to the FDDI LAN to take advantage of the better performance and expandability while continuing to operate on their existing LAN.

FDDI has many advantages. The use of fiber provides higher bandwidth than copper cable; therefore, a greater data rate is possible. Fiber provides protection from intentional (or hostile) and unintentional electronic interference, and is difficult to tap. Ruggedized fiber optic cable is now being produced to meet military standards for operation in grueling tactical environments. Optical fiber cable is light weight and easier to transport than copper cable. For example, tactical fiber optic cable weighs approximately 68 pounds per kilometer, compared to 26 pair copper cable weighing 10 times more. (Moore, Oliver, p. 35)

Another advantage of FDDI is that it uses a dual, counter rotating ring topology. Data propagates in opposite directions over the separate rings. One ring is primarily used for data transfer; the second is used for redundancy and ring management. This topology increases the survivability of the network because of its self-correcting properties when faults occur. Typical faults include a severed cable or a failed node. If a single line is severed, transmission continues through the remaining complete ring.

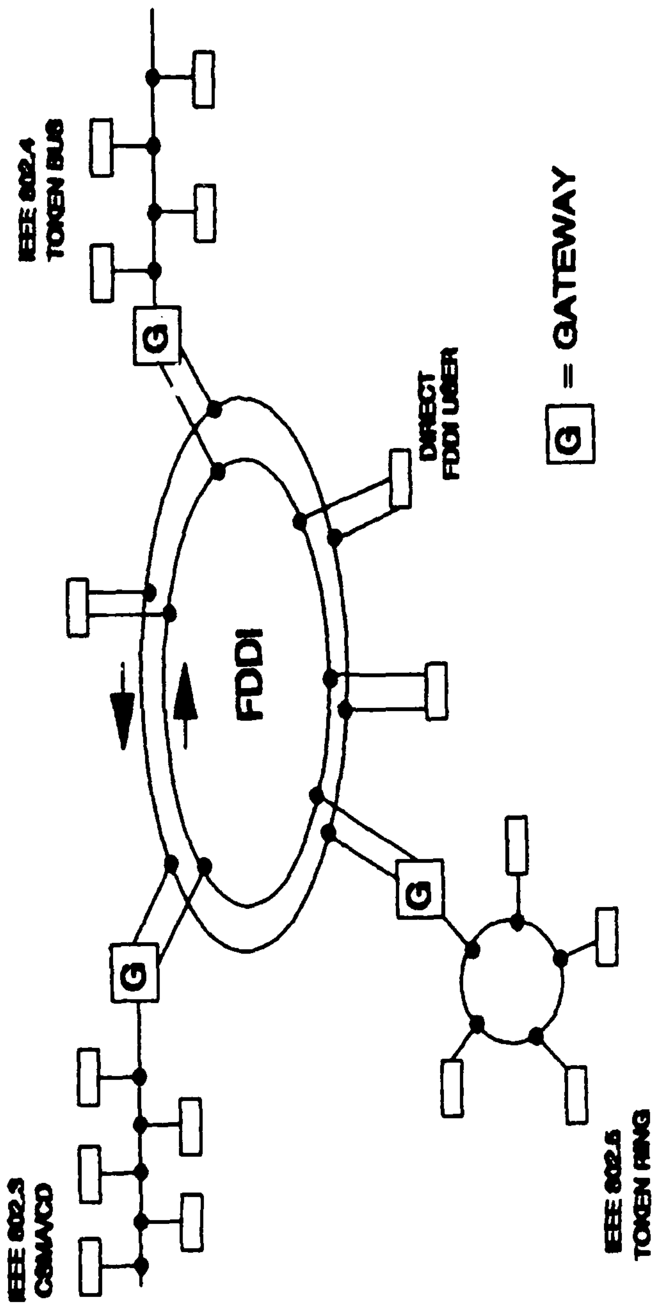


Figure B.5 Example FDDI Architecture

Figure B.6 depicts both cables being severed. In this case, the two nodes on either side of the break close the loop to form a single longer ring. Figure B.7 depicts the case of a failed node. This fault is corrected by closing the loop on either side of the failed node to form a single ring. These features allow quick detection and isolation of faults and permit uninterrupted data transmission to continue.

These self-correcting features also permit easy addition and deletion of nodes to the network without interruption of service to current users. Survivability can be increased by the strategic placement of the dual cables. There is no requirement for the cables to be positioned next to each other; therefore, they should be run using separate paths to minimize the probability of both rings being severed. (Moore, Oliver, pp. 35-36)

Another advantage of FDDI is the use of a token passing protocol. The token passing protocol provides more effective data transmission for high utilization networks. The upper bound on delay before transmission is known. The use of a token also permits the control of network access to allow higher priority users quicker access. Quick access can be critical in tactical situations.

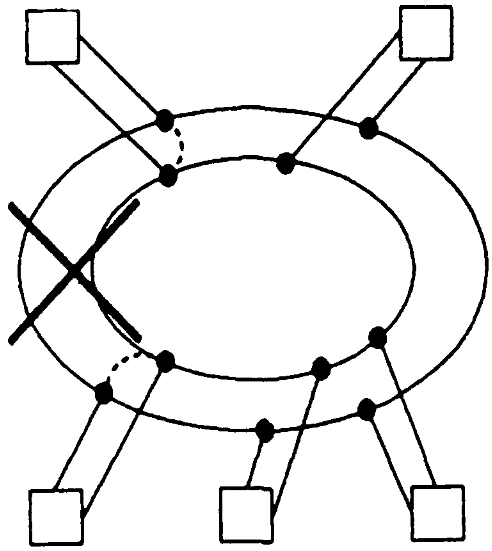


Figure B.6 Severed Cable Fault

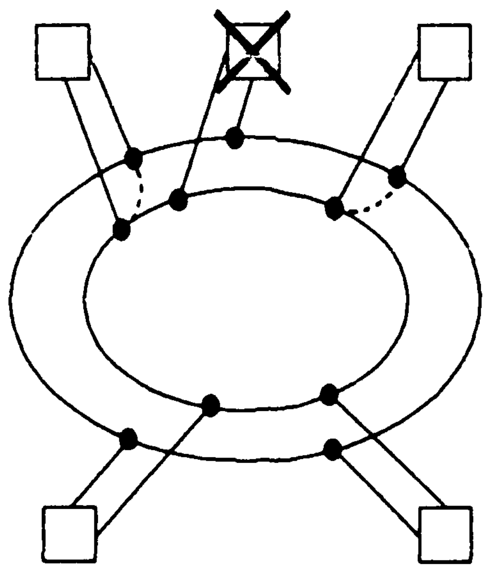


Figure B.7 Node Failure

The FDDI protocol generates both a data frame and a token. The format of the data frame can be seen in Figure B.8 and consists of the following fields:

- Preamble (PA): This field is used to synchronize each stations' clock with the frame. The preamble consists of 16 idle symbols (an idle symbol is represented as 1111, and using 4B/5B, is mapped into 11111). Since the field consists of only binary 1s, a transition will occur at the beginning of every bit interval and provide clock synchronization.

- Starting Delimiter (SD): This is a two symbol field used to indicate the start of a frame. SD is coded using non-data symbols to distinguish it from data. It is represented by the symbols JK, with a 4B/5B code of 1100010001.

- Frame Control (FC): This is a two symbol field to define the type and characteristics of the frame. The first symbol uses one bit to specify synchronous or asynchronous frame. Synchronous identifies a steady stream of traffic and asynchronous indicates bursty traffic. The next bit specifies address length (16 or 48), followed by two bits to identify whether the frame is data or control.

- Destination Address (DA): This field identifies the intended receiver(s) of the frame. Frames may be directed to a single node, a group of nodes, or broadcast for all nodes to copy and retain. FDDI, unlike other protocols, permits the use of both 16 and 48 bit addressing at the same time, and is specified in the FC field.

- Source Address (SA): This field contains the originating station address.

- Information (INFO): This field contains the information being transmitted for a data frame or any necessary control data if a control frame is being sent.

- Frame Check Sequence (FCS): This field is a 32 bit cyclic redundancy check (CRC). FDDI uses the standard CRC polynomial employed by IEEE 802 protocols. The FCS is computed from the contents of FC, DA, SA and INFO.

- Ending Delimiter (ED): This field is used to indicate the end of the frame. For data frames it consists of one non-data terminating symbol, T (4B/5B code 01101), followed by the frame status field. For the token, it contains two non-data terminating symbols, TT.

# SYMBOLS								
≥ 16	2	2	4 OR 12	4 OR 12	≥ 0	8	1	≥ 3
PA	SD	FC	DA	SA	INFO	FCS	ED	FS

PA = PREAMBLE
SD = START OF FRAME DELIMETER
FC = FRAME CONTROL
DA = DESTINATION ADDRESS
SA = SOURCE ADDRESS
INFO = INFORMATION FIELD
FCS = FRAME CHECK SEQUENCE
ED = END OF FRAME DELIMETER
FS = FRAME STATUS

Figure B.8 FDDI MAC Data Frame

- Frame Status (FS): This field contains a minimum of three status indication symbols containing the value R (reset or false) or S (set or true). These values are set by stations as they repeat the frame. The three required symbols indicate if an error was detected in the frame, if the intended receiver recognized its address, and if the receiver successfully copied the frame. Additional indicators can be included if necessary. The frame status field is terminated by the symbol T.

FDDI also accommodates message prioritization in a manner more like IEEE 802.4 than 802.5. Prioritization only applies to asynchronous traffic. If a station has synchronous data to transmit, it can capture any passing token regardless of any priorities. This is allowed because synchronous data can be handled so quickly due to the steady stream of data and the high data rate of fiber optics.

Unlike IEEE 802.5 where prioritization is handled within the token, FDDI message prioritization is controlled completely by the station. Each station has eight timer threshold values corresponding to eight priority levels for asynchronous data. When a station has asynchronous data to transmit and has captured a token, it enables a token hold timer which measures how long the station has held the token. As long as the token hold timer is less that the threshold time for a given priority, the station can continue to transmit data frame with that priority. Once the transmission of data from one priority level is completed, the next level is checked. Each level is checked and data transmitted if necessary as long as the token hold time is less than that threshold level. Once all frames are transmitted or the maximum token hold time is reached, the station generates a new token.

The characteristics of FDDI make it very suitable for tactical environments. The use of ruggedized military standard fiber optic cable provides a survivable and reliable means of data transfer while still being small, light weight, and permitting the same high data rates. FDDI has flexible configuration to permit the connection of other LANs via gateways; therefore, providing necessary expandability. Finally, it provides network traffic control through message prioritization and restricted tokens to ensure quick access for high priority users.

LIST OF REFERENCES

Air Command and Staff College, Report Number 86-0365, *A Users Guide to Local Area Network Connectivity*, by S. Brown, April 1986.

Air Force Logistics Management Center, Report, *Base-Level Mobility Local Area Network Guide*, by M. Grandalski, pp. 59-62, March 1988.

Ball, E., "LAN Bridges", *Computer Communications*, pp. 115-117, June 1988.

Biersack, E., "Performance Improvements of the IEEE 802.2 LLC Type 2 Protocol", paper presented at the 13th conference on Local Computer Networks, Computer Society Press of the IEEE, Washington D.C., October 1988.

Bux, W., "Performance Issues in Local Area Networks," *IBM Systems Journal*, pp. 351-374, 1984.

David Taylor Naval Ship Research and Development Center, Technical Report, *LAN Technology Survey*, by J. Yeh, A. Jeng, and C. Wu, pp. 7-11, February 1982.

Elion, G., and Elion, H., *Fiber Optics in Communication Systems*, p. 57, Mariel Dekker Inc, 1978.

Franta, W. R., and Chlamtac, I., *Local Networks: Motivation, Technology and Performance*, pp. 109-110, Lexington Books, 1981.

Freund, M., "Separating Myth from Reality when Designing LANs for Performance," *LAN Technology*, pp. 16-18, March 1989.

Gee, K.C., *Introduction to Local Area Computer Networks*, pp. 4, 11-30, 43-51, 77-79, 110-122, John Wiley and Sons, 1983.

Glass, B., "Fiber Optic Physics", *Networks*, pp. 6-8, October 1989.

Hansen, J. V., "Audit Considerations in Distributed Processing Systems," *Communications of the ACM*, pp. 562-569, August 1983.

Hawe, B., *Journal of Telecommunications Networks*, Volume 3, Number 2, pp. 55-56, Computer Science Press Inc, Summer 1984.

Henry P., "High Capacity Lightwave LANs", *IEEE Communication Magazine*, pp. 20-25, October 1989.

IEEE Standard 802.1: Overview, Interworking, and Systems Management, IEEE Computer Society, August 1986.

Jacobs, I., "Fiber-Optic Transmission Systems," *Electronic Communications Handbook*, Andrew F. Inglis, editor, p. 8.2, McGraw-Hill, 1988.

Jamieson, R., Low, G., "Security and Control Issues in Local Area Network Design," *Computers and Security*, Volume 8, Number 4, pp. 305-316, 1989.

Javed, A., "Signal Transmission Modes," *Electronic Communications Handbook*, Andrew F. Inglis, editor, pp. 11.20-11.24, McGraw-Hill, 1988.

JCS Publication 1, DoD Dictionary of Military and Associated Terms, pp. 217, 327-328, 1 Jun 87.

Kieffer, T., Richey, L., Christian, T., "Charting Network Topologies," *LAN Technology*, pp. 23-31, March 1989.

Krutsch, T., *Data Communications, Broadband or Baseband for Local Nets*, pp. 105-112, McGraw-Hill Inc, December 1981.

Kummerle K., *Advances in Local Area Networks*, pp. 22-24,29-32,62-66, IEEE Press, New York, 1987.

Liu M., "Performance Evaluation of Channel Access Protocols for Local Computer Networks," paper presented at the COMPCON Conference, Institute of Electrical and Electronics Engineers, pp. 417-426, Fall 1982.

Lundquist, J., *A Handbook for Local Area Networks*, pp. 9, 21-29, 53, Air University Press, 1985.

Malakie D., *Interconnecting Different Types of LANs*, pp. 5, 33-34, Master's Thesis, Naval Postgraduate School, Monterey, California, 1988.

Moore, M. V., Oliver, V. A., "FDDI: A Federal Government LAN Solution," *Telecommunication*, pp. 35-44, September 1989.

Myers, Wate, "Toward a Local Network Standard", *IEEE Micro*, pp. 28-45, August 1982.

Pratt, T., Bostian, C.W., "Multiple Access," *Satellite Communications*, pp. 251-256, John Wiley and Sons, 1986.

Pursley, M. B., "Digital Communication," *Reference Data for Engineers: Radio, Electronics, Computer, Communications*, Edward C. Jordan, editor, pp. 24.22-24.25, Howard W. Sams and Co, Inc, 1985.

RAND Corporation USAF Contract, Report Number N-1908-AF, *Technological Perspectives for Air Base Communications*, by W. Ware, October 1985.

Roberts, A. R., Whitty, M. S., "Selection of Transmission Media," *Electronic Communications Handbook*, Andrew F. Inglis, Editor, p. 9.1, McGraw-Hill, 1988.

Rogers, D. V., "Radio Wave Propagation," *Electronic Communications Handbook*, Andrew F. Inglis, editor, pp. 1.1-1.19, McGraw-Hill, 1988.

Ross, F. E., "An Overview of FDDI: The Fiber Distributed Data Interface," *IEEE Journal on Selected Areas in Communications*, Volume 7, Number 7, pp. 1043-1051, September 1989.

Sachs, S., Kan, K. and Silvester, J. A., "Performance Analysis of a Token-Bus Protocol and Comparison with Other LAN Protocols," paper presented at the Conference on Local Computer Networks, 10th, Minneapolis, Minnesota, 7-9 October 1985.

Schwendtner, T. A., Notes for EO3750 Class (Communication Systems Analysis), Naval Postgraduate School, Monterey CA, 1989 (unpublished).

Smith, D., and Webb, M., "Engineering Report on the Suitability of Ethernet in the Tactical Environment," US Air Force 1912 Computer Systems Group, 23 October 1987.

Stack, T., "Protocols for Local Area Networks", paper presented to the Trends and Applications Conference, Institute of Electrical and Electronics Engineers, May 1980.

Stallings, W., *Local Network Technology*, pp. 12-14, 16-18, 22-34, IEEE Computer Society Press, 1983.

Stallings, W., "Local Network Performance," *IEEE Communications Magazine*, pp. 27-36, February 1984.

Stallings, W., *Computing Surveys*, Vol 16, p. 6-8, Association for Computing Machinery Inc, March 1984.

Stallings, W., *Local Network Technology*, Second Edition, pp. 1-2, 23, 29, IEEE Computer Society Press, 1985.

Stallings, W., *Handbook of Computer-Communication Standards*, Vol 2, pp. 22, 24, 31, 46, 53-55, 84-86, 88-89, 91, 93, 117, 131-133, 139, 148, 150, 153-154, 157-162, 170, 172, Macmillan Publishing Company, 1987.

Stallings, W., *Handbook of Computer-Communications Standards*, Vol 3, p. 3, Macmillan Publishing Company, 1988.

Strole, N., "A Local Communications Network Based on Interconnected Token-Access Rings," *IBM Journal of Research and Development*, Vol 27 Number 5, pp. 481-496, September 1983.

"Tactical Air Command", No Author, Air Force Magazine, pp. 90-91, Air Force Association Press, May 1989.

Tanenbaum, A., *Computer Networks*, Second Edition, pp. 26-27, 121, 127-128, 144-145, 149, 151, 158, 164, Prentice-Hall Inc., 1988.

US Air Force, Headquarters Tactical Air Command Pamphlet 700-12, "Computer Network Standardization Plan," pp. 1-10, 28 June 1989.

US Air Force, Headquarters Tactical Air Command Regulation 55-45, "Tactical Air Force Headquarters and the Tactical Air Control Center," p.4-1, 26 October 1984.

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, CA 93943-5002	2
3.	Captain Greg Swain, USMC 9108 Donna Dean Drive Springfield, VA 22153	1
4.	Captain Rick Mallick, USAF HQ SAC/SCXIN Offutt AFB, NE 68113-6343	1
5.	Captain John Gibson, USAF P.O. Box 868 Morro Bay, CA 93443-0868	1
6.	Captain David Hunninghake, USAF HQ TAC/SCX Langley AFB, VA 23665	2
7.	Captain Brad Ashley, USAF HQ AF Space Command/LKW Peterson AFB, CO 80914-5000	2
8.	Captain Doug Butler, USAF Air Staff/SC Room 5B462 Pentagon, Washington D.C. 20301	1
9.	Mr. Jerry Blair Idaho National Engineering Laboratory (INEL) 391 East 13th Street Idaho Falls, ID 83404	1
10.	Colonel George Naddra, USAF HQ TAC/SCL Langley AFB, VA 23665	2

11. Professor Tung Bui — 1
Administrative Science Department
Naval Postgraduate School
Monterey, CA 93943

12. Mr. Don Lacer — 1
Code 39
Naval Postgraduate School
Monterey, CA 93943-5000

13. C3 Academic Group Code 74 — 1
Naval Postgraduate School
Monterey, CA 93943-5000

14. Joint C3 Curricular Office Code 39 — 1
Naval Postgraduate School
Monterey, CA 93943-5000

15. Director for Command, Control and Communications Systems, Joint Staff — 1
Washington, DC 20318-6000

16. AFIT/NR — 1
Wright-Patterson AFB, OH 45433-6583

17. AFIT/CIRK — 1
Wright-Patterson AFB, OH 45433-6583