NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

LOCAL AREA NETWORK STRATEGIES AND GUIDELINES FOR A PERUVIAN AIR FORCE COMPUTER CENTER

by

Miguel A. Palomino Fonseca

March, 1991

Thesis Advisor: Prof. Myung Suh

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION: Unclassiefied

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)*: 54

7a. NAME OF MONITORING ORGANIZATION: Naval Postgraduate School

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

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

8a. NAME OF FUNDING/SPONSORING ORGANIZATION:

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

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER:

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

10. SOURCE OF FUNDING NUMBERS

Program Element No.	Project No.	Task No.	Work Unit Accession Number

11. TITLE *(Include Security Classification)*: Local Area Network Strategies and Guidelines for a Peruvian Computer Center

12. PERSONAL AUTHOR(S): Miguel A. Palomino Fonseca

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT *(year, month, day)*	15. PAGE COUNT
Master's Thesis	From To	March, 1991	108

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

17. COSATI CODES

FIELD	GROUP	SUBGROUP

18. SUBJECT TERMS *(continue on reverse if necessary and identify by block number)*: LAN, Broadband and Baseband Systems, data Communication, Protocols, Transmission Media, Topologies, Access Method.

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

This thesis examines the application of local area network (LAN) technology to the Peruvian Air Force Computer Center. The current Peruvian Air Force Computer Center communication system and its problems are discussed, along with the basic concepts of data communication, protocols, and topologies. The IEEE 802.3 and IEEE 802.5 specifications are discussed in detail. This study is primarily concerned with how to design the best local area network for the Peruvian Air Force Computer Center, and proposes a local area network implementation strategy for the Peruvian Air Force Computer Center.

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

21. ABSTRACT SECURITY CLASSIFICATION: Unclassified

22a. NAME OF RESPONSIBLE INDIVIDUAL: Myung Suh

22b. TELEPHONE *(Include Area code)*: (408) 646-2637

22c. OFFICE SYMBOL: AS/SU

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

Approved for public release; distribution is unlimited.

Local Area Network Strategies and Guidelines for a Peruvian Computer Center

by

Miguel A. Palomino Fonseca
Second Lieutenant, Peru Air Force
B.S., Peruvian Air Force Academy, 1988

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1991

ABSTRACT

This thesis examines the application of local area network (LAN) technology to the Peruvian Air Force Computer Center. The current Peruvian Air Force Computer Center communication system and its problems are discussed, along with the basic concepts of data communication, protocols, and topologies. The IEEE 802.3 and IEEE 802.5 specifications are discussed in detail. This study is primarily concerned with how to design the best local area network for the Peruvian Air Force Computer Centers, and proposes a local area network implementation strategy for the Peruvian Air Force Computer Center.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

I. INTRODUCTION

A. OVERVIEW

The modern world is experiencing many variations. This is remarkable especially in the increased use of electronics and computers. Although the computer industry is young compared to other industries, it has seen great advances. The merging of computers and communication system recently has had a remarkable influence on the way computer systems are organized.

Today, the use of computers to communicate the results of user's information processing has started another revolution: telecommunications. Computer technology has advanced rapidly within the past decade and the need for communication and information exchange between computers and offices has grown rapidly in recent years.

Local area networks (LANs) have grown in popularity with the widespread use of personal computers (PCs) in offices and organizations. LANs are an effective medium for the interconnections of PCs. They provide a variety of applications, including resource sharing (such as central files and expensive peripheral) as well as information interchange via electronic mail facilities.

PCs become much more efficient when wired together in networks. Electronically sharing peripherals and information, these networked PCs are easily able to outstrip their non-networked counterparts in both productivity and creativity.

In a network each member of the organization may independently use a personal computer. One PC, with processor, file storage, high-level languages, and problem solving tools, is expensive. In a network, these resources can be shared economically. Some files must be used by several users. Members of the military organization need to share work and information. The most efficient way to do so is with a network.

In parallel with the growing need for the communication and information exchange between elements of a squadron, networks are becoming very important in national defense. The Peruvian Air Force requires rapid, accurate information transmission that will make its information systems more efficient.

B. HISTORY

The data processing industry began in 1950s. Until terminals were first wired to telephone lines for the purposes of sending data to a remote computer in the mid-1950s, the communications industry was oriented strictly toward voice communications. The development of the data processing industry opened the doors to the world of data communications.

Further technological developments resulted in time-shared computer system. A relatively large number of terminals then could be connected to a single computer, using the transmission facilities of the voice telephone network.

The late 1960s also brought the development of common-plug peripheral devices. The manufactures of the plug compatible equipment identified and exploited a market for the peripherals, including multiplexers, concentrators, and terminals that could be connected with various computers and made available to users as alternatives to a single-vendor computer system arrangement. In the early 1970s, the complexity of computer network increased when coaxial cable and communication devices (multi-drop lines, multiplexers, concentrators, and intelligent terminal devices) were used to enhance and extend communication between users and the central processing unit (CPU). [Ref.1:p.178]

C. TENDENCY TO THE FUTURE

The actual use of small, dedicated minicomputers or microcomputers at remote locations, in place of mainframe computers, are perhaps the most significant computer development for this study. Although large mainframe computers are suitable for applications involving large data bases or requiring high-speed processing, many typical user functions do not need the speed and sophistication of large computers. The result has been the increasing use of minicomputers at various user locations to replace a single large mainframe computer. In some applications microcomputers have been custom designed by the user to perform specialized functions in the most efficient manner at the remote location. [Ref.2:p.11]

A local Area Network (LAN) is a data communications system that allows communication between several independent devices (minicomputers and microcomputers). The network may support a wide variety of applications, such as file editing and transfer, electronic mail, and database management.

The shift to inter-networking can be expected to gain more momentum in the future, particularly as leaders begin to reap the benefits. The initial investment in new products, conversion, personnel training, and application redesign is not small, and many groups will not see a return for years after they take the plunge. The leaders may spend more because the path is not clearly defined and mistakes are inevitable. The followers may find conversion less expensive because the leaders will have worked out more of the kinks. At the same time, followers will have lost ground while sticking with outmoded environments.

Many organizations are making a major shift in their philosophy of computing and communications. Traditional thinking had computers in the foreground as the major factor. Concerns were focused on speed, storage, operating system, and applications software. Communication was considered later, when the needs became obvious.

The change is toward the view of computing embedded in a matrix of communication resources. Communication and interaction are treated as equals with computation. Computing elements are being selected for their inter-networking capabilities as well as for specific tasks in particular environments. These computing elements can be placed where their capabilities can be exploited to best advantage. Special purpose equipment can easily be added and shared among larger groups. The major attributes are flexibility, a careful plan, and ongoing attention to the environment as it evolves.

The shift is underway; these initial efforts represent a departure that cannot be deflected. These first efforts are creating a stage for more sophisticated generations of inter-networking approaches based on real operational experience. The main watchword at this point is potential many communications technologies, coupled with inexpensive, powerful processors, can be employed. The potential power of new approaches and perspectives is soon to be realized. At this time, the largest challenge is the strategic use of technology to create the type of interworking environment that is necessary to bring the information age closer to reality.

D. OBJECTIVES AND OUTLINE

1. PROBLEM

The primary Computer Center for the Peruvian Air Force is located in the Air Force headquarters. In addition to the primary center, there are nine other smaller computer centers at other key Air Force locations. All ten centers are listed in appendix (a). Each center works independently and has its own communication system. Development of an integrated communication system is important for the future of the organization. The ten communication systems all operates on the same basic concept. If one of the ten services were to develop an integrated communication system, the others then could use that system or a similar one.

Normally the communication between this centers is by telephone, radio, post service,etc. Increasing the use of computers for communication, integrated, rapid data exchange and accurate information processing are important goals for the modern Air Force.

Many organizations within the Air Force are seeking ways to improve knowledge sharing and document management and delivery. Considering the demanding requirements of a heterogenous computer center user population, the improving cost-effectiveness of smaller, dedicated processors for specialized tasks, and the increasing availability of computer networking facilities, the development of LANs for the ten centers should be seriously considered.

2. GOALS AND OBJECTIVES

a. Goals

This study will provide a specific outline for Peruvian A.F. Computer Center LAN development. Anticipated division acceptance of LAN systems will be discussed, along with LAN impact in the future communication. The goals of this study are:

- Determine the impact of a LAn system on the future communication, on work efficiency, and real time information sharing.
- Describe possible effects and advantages of LANs for the military in Peru.
- Determine basic guidelines and strategies for a Peruvian Air Force Computer Center.
- Determine the basic key concepts of communication networks for a future LAN implementation.

b. Objectives

In order to achieve these goals, the following objectives must be met.

- Describe the current communication system of a Peruvian Air Force Computer Center, focused on the other centers.
- Define the requirements for an effective LAN for a Peruvian A.F. Computer Center.
- Discuss how LANs can support the communication needs of the ten computer centers.
- Propose a model that could be used for a Peruvian A.F. Computer Center LANs based on the United States system.

3. OUTLINE

This chapter has provided an overview of the telecommunication network technology development since it's conception into the future. The basic concept of data communication is discussed in Chapter II. This includes such things as transmission media, LAN topologies, a brief presentation on LAN operating system, LAN components, LAN standard, transmission techniques, etc. Chapter III will address two of the IEEE LAN standards. The IEEE 802.3 standard defines CSMA/CD protocol for bus topology, which nearly identical to the Xerox Ethernet system. A second standard, IEEE 802.5, defines the Token Ring MAC protocol for ring topology. It also presents interconnection and security issues. Selection of a possible LAN for a Peruvian Air Force Computer Center system is covered in Chapter IV, along with information and networking requirements that may be used to determine whether the LAN is the appropriate technology for the Peruvian Computer Center. Chapter V provides the conclusions and recommendation based on this study.

II. ARCHITECTURE AND STANDARDS FOR LANs

A. GENERAL

LANs provide a means of communication for PCs, so that information can be exchanged between connected stations. The primary objective is to provide high-speed data transfer among a group of stations within a small area.

1. LAN DEFINITION

The driving force for the use of LANs is to increase employee productivity and efficiency and to share expensive hardwares, like printers and disks units. Productivity can be increased and expenses can be decreased by giving employees easy, fast, and shared access to computers, terminals, and other work stations in the office. Moreover, with the distribution of computing resources (PCs), it has became necessary to provide a means to connect these devices with the host computer. LANs are designed to provide these services.

Definitions of local networks are plentiful. Normally referred to simply as LANs, they are interconnected distributed communities of computer-based data terminal equipments. These equipments normally are confined to a single building or localized group of buildings. For example, a LAN may be used to interconnect a community of computer-based workstations distributed around a block of offices within a building. Alternatively, it may be used to interconnect various computer-based equipments located within a single organization.

LANs under normal circumstances are installed and maintained by one organization; hence they are also referred to as private data networks. Networks accessed by many organizations are called public data networks. There is a major difference between a communication path established using a LAN and connection made through a public data network. With a LAN, because of the relatively short distance between the various items of interconnected equipment, much higher data transmission rates are normally possible.

According to the IEEE 802 Committee, a Local Area Network is a data communication system that allows several independent devices to communicate with each other. This communication network is usually in a small geographic area (usually up to 10 Km. maximum) and allows for high speed data exchange (usually up to 10 million bits per second (Mbps) for most LANs).

While one definition has not gained prominence, most definitions include the following:

- The connections between the user devices are usually within a few hundred meters, to several thousand mts.

- The LAN transmit data (and often voice and video) between user stations and computers. [Ref.3:p.763]

- The LAN transmission capacity is usually greater than that of a wide area network. Typical bit rates range from 1 Mbits/s to 20 Mbits/s.

- The LAN channel is typically owned by the organization using the facility. The telephone company usually is not involved in channel ownership or management. However, telephone companies are moving into this arena with their own offerings. [Ref.3:p.763]

- The error rate on a LAN is considerably better than that on a wide area networked-oriented telephone channel.

2. ADVANTAGES OF LAN

Some of the advantages of a LAN are:

- Resource sharing. Expensive resources such as laser printers and mass storage can be shared among a group of interconnected system, allowing economy of resources.

- Higher availability of resources through data exchange or remote access to other networks. This increases productivity as data and message exchange becomes easier.

- Better reliability and maintainability through a centralized management and control.

- Backup of one system by another in case of failure.

3. LAN COMPONENTS

A LAN contains four major components that transport data between end users: (a) channel; (b) physical interface; (c) protocol; (d) user station (see Figure 1).

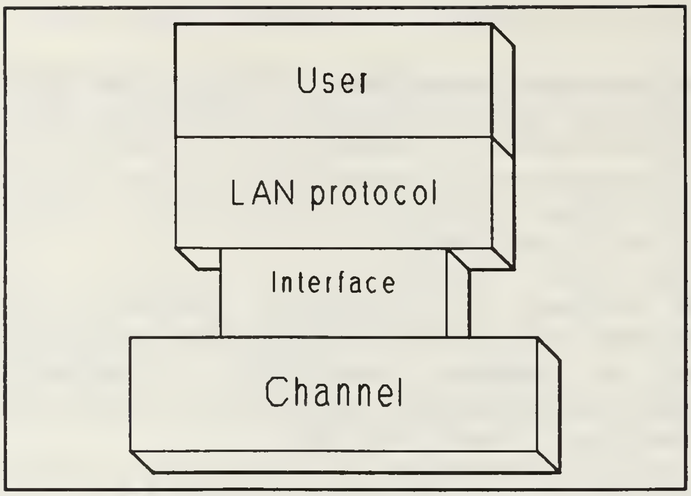

Figure 1. LAN Components [Ref.3:p.763]

a. Channel

LAN channels (media) consists of coaxial TV cable, coaxial baseband twisted pair cable, or optical fiber. Coaxial cable TV (CATV) is used on many networks because it has a large transmission capacity, a good signal-to-noise ratio, low signal radiation, and low error rates. Twisted pair cable and microwave are also found in many LANs. Baseband coaxial is another widely used transmission path, giving high capacity as well as low error rates and low noise distortion.

Thus far, optical fiber paths have seen limited application, but their positive attributes assure their increased use. The immediate use of lightwave transmission on local networks is for point-to-point, high speed connections of up 10 miles (16 Km). A transfer rate of over 100 Mbits/s can be achieved on this type of path.

Infrared schemes using line of sight transmission are also used on the LAN channel. Several vendors offer infrared equipment for local loop replacement. Up to 100 Kbit/s over one mile (1.6 Km) distances are possible with infrared schemes. [Ref.3:p.763]

b. *Physical Interface*

The interface between the path and the user station can take several forms. It may be a single cable television (CATV) tap, infrared diodes, microwave antennas, or laser emitting semiconductors for optical fibers. Some LANs provide regenerative repeaters at the interface; others use the interface as a buffer for data flow. [Ref.3:p.764]

c. *Protocol*

The protocol control logic component controls the LAN and provides for the end user's access onto the network. The LAN protocols employ methods and techniques to be discussed later in this chapter. [Ref.3:p.764]

d. *User Station*

The last major component of a LAN is the user workstation. It can be anything from a word processor to a mainframe computer. Several LAN vendors provide support for other vendors' products, and the upper layers of the ISO model are also supported by some LANs. [Ref.3:p.764]

B. OPEN SYSTEM INTERCONNECTION MODEL

The objective of the local network standards is to ensure the compatibility between equipments made by different manufactures such that data communications can take place between the devices with minimum effort on the part of the equipment users or the builders of a system containing the equipments.

The standards also increase the market for a particular product. This encourages mass production, leading to lower price in scale implementation.

In continuing efforts to accomplish this mission, a number of organization have became involved in developing LAN standards, such as ISO, ANSI, and IEEE.

Many different communications systems and equipments are used throughout the world. This has created the need for standard protocols that allow different brands of computers to communicate and to transfer data between them. The International Standards Organization (ISO) has responded to this need by standardizing a multilayered computer architecture that permits interoperability between computer systems. The ISO is an international organization for the development of standards on a wide range of subjects. A private, voluntary, nontreaty organization, ISO has been active in developing a system interconnection architecture called Open Systems Interconnection (OSI). The American National Standards Institute (ANSI) is a nonprofit, nongovernment federation of standard-making and standard-using organization. It is also the U.S.-designated voting member of the ISO. The Institute of Electrical and Electronics Engineers (IEEE) is the world's largest professional society and the leading organization in the area of standardizing LANs. Its activities are organized under a number of boards, one of which is IEEE LAN standards.

The ISO standards as we already know use what is called the OSI model. This model divides computer communication architecture into seven layers and prescribes protocols for each layer (see Figure 2). [Ref.4:p.203]

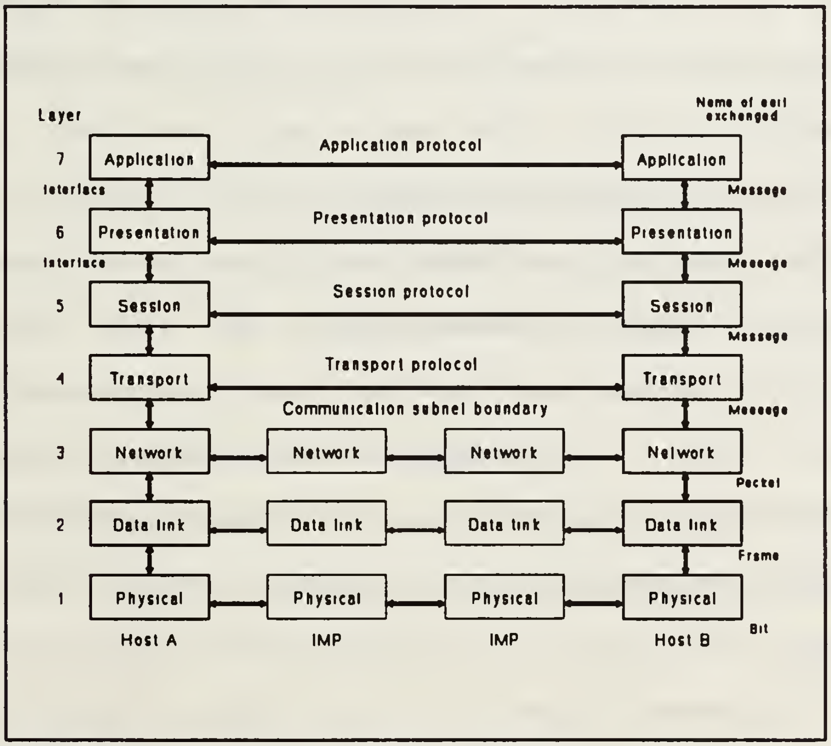

Figure 2. OSI Reference Model

Only the lowest layer provides for actual physical connections. That is, only this layer is concerned with an actual exchange of raw bits over a communication channel. In all the others only logical connections are created, with data sent from layer to layer in order to get it across to another system. The seven layers are described below.

1. Layer 1: Physical Layer

This layer defines the physical interface between devices and the rules by which bits are passed from one to another. It is used in prescribing the interface between data terminal equipment and data circuit-terminating equipment. In addition, the number of signal lines and the shape and the size of connectors are specified by the physical layer standards.

2. Layer 2: Data Link Layer

The task of the data link layer is to take raw data transmissions and transform them so they are free of transmission errors and can be used by the network layer (layer 3). This is accomplished by breaking the input data into data frames, transmitting the frames sequentially, and processing acknowledgement frames sent back by the receiver.

3. Layer 3: Network Layer

This layer basically divides data streams into packets for transfer between a host and a network and between network components. Using these protocols, messages are accepted from a source host and converted to packets. Packets then are directed toward their destinations.

4. Layer 4: Transport Layer

The basic function of the transport layer (also known as the host-to-host layer) is to accept data from the session layer (layer 5), split it up into smaller units if necessary, pass these to the network layer (layer 4), and ensure that the pieces all arrive correctly at the other end. [Ref.5:p.16-19]

5. Layer 5: Session Layer

This layer provides end-to-end procedures to establish, maintain, and terminate logical relationships between processes in higher layers. It is the user's interface into the network. Once the connection has been established, the session layer can manage the dialogue in an orderly manner, if the user has requested that service.

6. Layer 6: Presentation Layer

This layer provides a host-to-host procedure that prescribes how data formatting and data transformation will be done. The function of the presentation layer is to provide the user with certain useful but not always essential services. Among these services are cryptographic transformations and text compression.

7. Layer 7: Application Layer

This layer is concerned with the support of an end-user application process. Unlike the presentation layer, this layer is concerned with the semantics of data. The layer contains service elements to support application processes such as job management, and financial data exchange. The layer also supports the virtual terminal and virtual file concept. [Ref.3:p.285]

Essentially, the lowest three layers are concerned with the communication protocols associated with the data communications network. The upper three layers are concerned with the protocols necessary to allow two heterogeneous operating systems to interact with each other. The intermediate transport and internetwork layers support the upper protocols layers with the help of the detail workings of the lower network-dependent layers.

The function of each layer is formally specified in the form of protocol which defines the set of rules and conventions which are used by the layer in order to communicate with a peer layer in another system. Each layer provides a defined set of services to the layer immediately above it, and in turn, use the service provided by the next lower layer to transport the message units associated with the defined protocols of that layer.

C. TRANSMISSION MEDIA

The transmission medium is the path between nodes of the network. This medium provides physical channels needed to connect stations on the network. It is one of the most crucial and complex components of a LAN. Media commonly used for LANs are twisted pair-wires, coaxial cable, and optical fibers. Microwave is now considered for wireless LANs which are still in an experimental stage.

1. TWISTED-PAIR WIRE

Twisted-pair wire is the oldest satisfactory electronic transmission technology which has a limited data rate. It consists of two insulated copper wires twisted together in a helical form and covered by a common insulated sleeve. Figure 3 illustrates a cable made of twisted-pair wires. Shielded-twisted-wire-pair cable is a special form of twisted pair that uses a higher quality protective sheath. The twisted form is used to reduce electrical interference.

It is the most common transmission medium for both analog and digital data, and it is widely used due to their adequate performance and lower cost. [Ref.1:p.66]

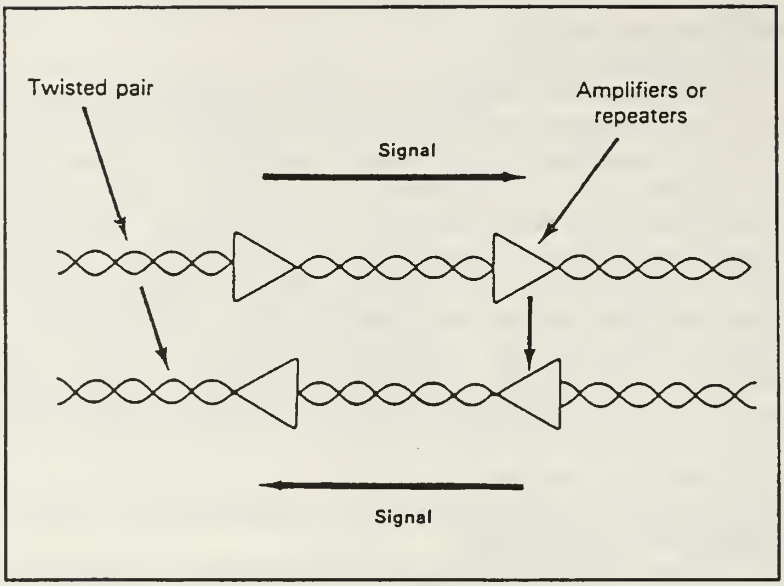

Figure 3. Twisted-Pair Cable [Ref.3:p.120]

2. COAXIAL CABLE

Coaxial cable is the most popular medium for LANs, which consist of a central copper core surrounded by 'the insulating material. The insulator is then surrounded by a cylindrical conductor covered with a protective plastic sheath. Figure 4 shows the construction of a typical coaxial cable. Two kinds of coaxial cable are widely used for LAN application. One type, a 50-ohm cable, is employed for digital signals and is called "baseband". The other type, a 75-ohm cable, is utilized for analog signaling with Frequency Division Multiplexing (FDM) and is called "broadband". The broadband which does not use FDM is sometimes referred to as "single channel broadband".

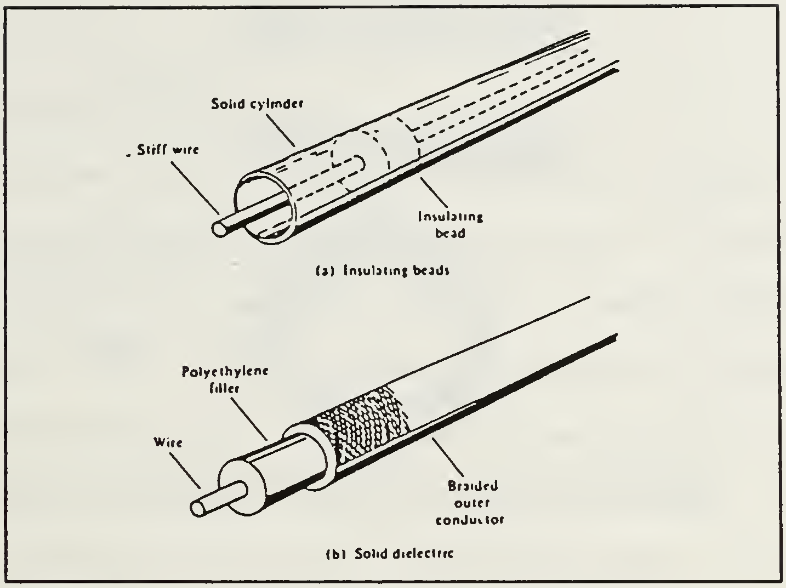

Figure 4. Coaxial Cable [Ref.6:p.51]

3. OPTICAL FIBER

The most exciting development in local area network transmission media is the use of fiber optics. This medium carries data signals in the form of modulated light beams. An optical fiber structure consists of an extremely thin fiber of glass or fused silica, called "core" surrounded by concentric layers of glass known as "cladding". The outermost layer, surrounding one fiber or a bundle of cladded fibers, is the protective sheath. The construction of a typical optical fiber is shown in Figure 5.

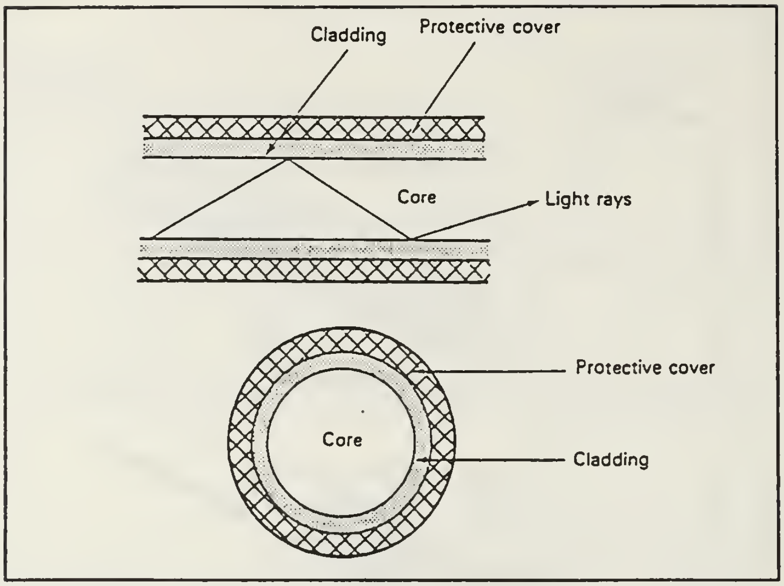

Figure 5. Optical Fiber [Ref.3:p.130]

4. MICROWAVE

More than half of the miles of circuits in the United States telephone system now are microwave circuits. Microwave systems use very high frequency radio waves. Because of their short wavelength, microwaves exhibit some of the characteristics of lightwaves; they travel in straight lines, can be reflected, and can be directed or focused by special lenses. Microwaves are accurately beamed in line-of-sight transmission from one antenna tower to another 25 to 35 miles away. The spacing sometimes varies because of the mountains or other physical obstructions. At each tower the weakened microwave signal is received, amplified, and retransmitted to the next antenna. Microwave circuits usually are not used for convetional LANs. But they are considered for use in wireless LANs. [Ref.1:p.66]

5. SATELLITE

Communication satellites provide a special form of microwave relay transmission. The satellite is essentially a microwave antenna that has been placed in earth orbit. It can relay signals over longer distances than is possible with earth microwave stations because the curvature of the earth and physical obstacles block line-of-sight microwave transmission between land-based microwave towers. In addition to the satellites, a satellite communication system requires earth stations for initiation and receipt of transmission. Communication satellites are generally geostationary. That is, the satellite appears to be stationary to the earth ground stations. A satellite receives microwave signals in a given frequency band, amplifies them, and retransmits them at a different frequency. [Ref.1:p.67]

Satellite channels will be increasingly used for the long-distance, high-volume data transmission. Use of rooftop antennas at an organization's various locations could avoid the need to use other common carrier long-distance facilities. However, satellite transmissions are not used for LANs, at present.

D. LAN TOPOLOGIES

Topology, one of the key elements in a LAN's success or failure in performing its task, refers to the manner in which network devices are geometrically arranged and connected, it also describes how the stations of the network are interconnected. The topology determines the characteristics of network in terms of reliability, expandability, and performance. The major classes of LAN topologies are mesh or tree, bus, ring, and star. Each of these methodologies has its own particular advantages and limitations in terms of reliability, expandability, and performance characteristics.

1. MESH TOPOLOGY

In the mesh topology, each device has a point-to-point link with every other device, as illustrated in Figure 6. A transmission or a message from any station can be received by all other stations and propagate throughout the medium. This is referred to as a fully connected or mesh topology. [Ref.6:p.35] Some networks employ a mesh configuration either by itself or in combination with one or more of the other configurations, thereby forming a hybrid configuration. [Ref.7:p.14]

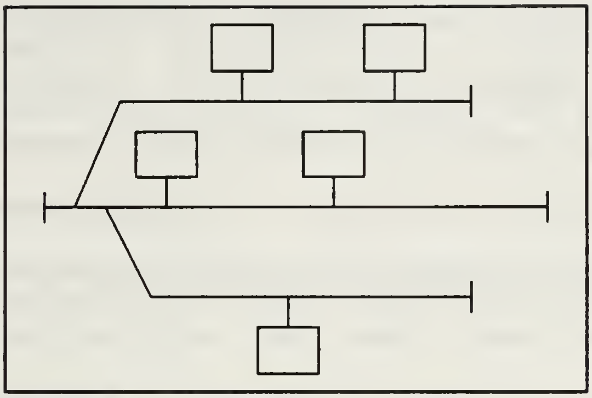

Figure 6. Tree Topology

a. Advantages

- The mesh configuration has a low response time and is robust against node or link failure.
- This topology is well suited and commonly used for a long-haul packet switched networks. [Ref.8:p.33]

b. Disadvantages

- Mesh topology is very complex.
- This topology is extremely expensive, relative to the bus and ring types, without a proportionate advantage in efficiency. [Ref.7:p.14]

2. BUS TOPOLOGY

Generally, with bus topology, a single cable runs past all the network stations. Each station is connected to the bus either directly or to the trunk line through a short drop cable. All stations continuously monitor the medium. When a message is transmitted, it propagates throughout the medium and is received by all stations. Each station determines whether to accept the message or simply ignore it based on the address contained in the message. To prevent several stations from transmitting simultaneously, some type of communication protocol, or media access control (MAC), is needed. The methods used are generally "controlled access" or "contention" technique. In a bus topology, illustrated in Figure 7, there are no routing decisions required by any of the nodes. A message flows away from the originating node in both directions to the ends of the bus. A node must be able to recognize a message intended for it. All stations share a full duplex transmission medium and receive all transmissions.

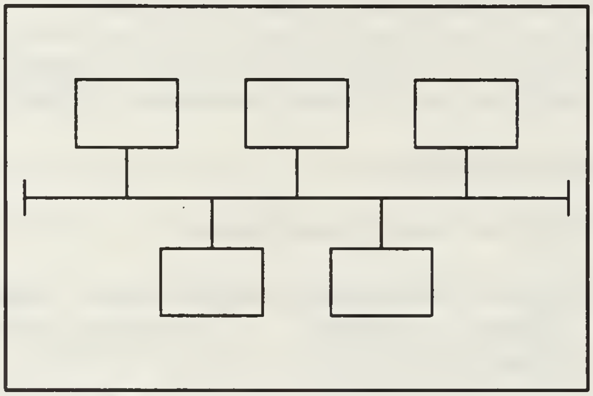

Figure 7. Bus Topology

a. *Advantages*

- Bus nodes share a single physical channel via cable taps or connectors.
- Messages placed on the bus are broadcast out to all nodes.
- Unlike nodes in a ring, bus nodes do not have to repeat and forward messages intended for other nodes. As a result, there is none of the delay and overhead associated with retransmitting messages at each intervening node.

- Bus networks are easily configured and expanded in most physical layouts, for instance a room, building, or building complex. This feature alone is often a major reason in choosing the bus topology for a local network. [Ref.8:p.38]

b. Disadvantage

- In some bus topologies, if nodes are physically too distant from each other, collision of two messages may not be detected.

3. RING TOPOLOGY

In the ring topology, expendability are linked together the same way as the bus, but it is arranged to form a loop (ring structure). With this structure, messages are transmitted from station to station around the ring. To transmit, the sending station places a message on the medium. This message then travels around the ring until it either reaches the destination station or is returned to the sender. The interface attachment on each station has the ability to determine whether to accept and process the received message based on the address contained in it. Otherwise, the station will retransmit the message to the next station until it reaches the destination address. Furthermore, the interface also has the ability to remove the message returned to the sender. Ring topology is shown in Figure 8.

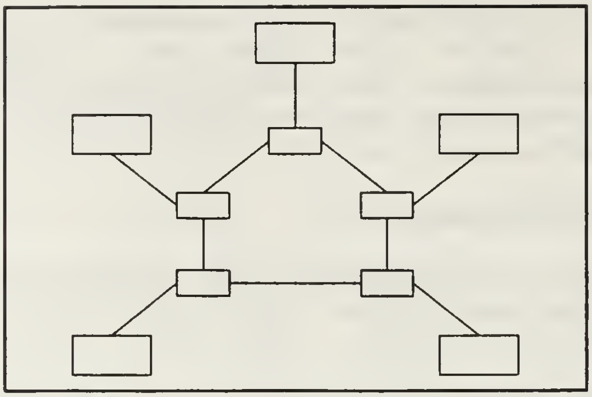

Figure 8. Ring Topology

a. Advantage

- Ring nodes can be less complex than the routing nodes in an mesh topology, since message routes are determined by the topology, i.e., messages automatically travel to the next node on the ring.

b. Disadvantages

- Rings must be physically arranged so that they are fully connected. Lines have to be placed between any new node and its two adjacent nodes each time an addition is made. Thus, it is often difficult to prewire a building for ring networks in anticipation of nodes to be added in the future.

- Failure of a node or an active component adding a new node, or any other break in the ring topology will most always cause the network to stop functioning. [Ref.8:p.36]

4. STAR TOPOLOGY

A star configuration features a central hub to which a collection of stations is directly connected. Communications between any two stations is achieved through the central hub, which is responsible for managing and controlling all the communication with active or passive devices.

With an active device, the central hub acts as a switching device. When one station wishes to communicate with another, the hub establishes a dedicated path between the two stations.

With a passive device, a power splitter is used at the hub of the star to divide the incoming signals among the stations. Star topology is illustrate in figure 9.

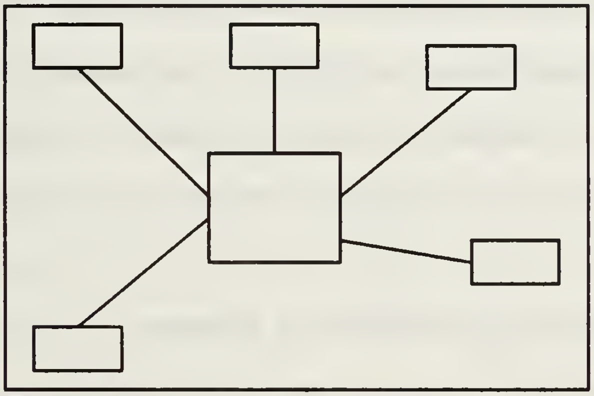

Figure 9. Star Topology

a. Advantage

- Point to point lines connect the central and outlying nodes, eliminating the need for the complex link and the control requirements of other topologies, and allowing simple and usually low cost connections to the network through the central node. [Ref.8:p.35]

b. Disadvantages

- This topology may be is extremely expensive relative to the bus and ring (without a proportionate advantage in efficiency) because it uses dedicated lines to connect each node to the network. [Ref.7:p.14]

- A basic problem with the star configuration is that the central hub failure results in the failure in the failure of the entire network.

E. NETWORK ACCESS TECHNIQUES

Terminals connected into a network must use some method of accessing that network. Different access methods are available different functions. Two basic access methods are centralized control and distributed control. The latter allows individual devices to control their own access. Several types of network access methods currently are used for LANs. These include time division multiple access (TDMA), frequency division multiple access (FDMA), carrier sense multiple access (CSMA), token passing on ring networks, and token passing on bus networks.

1. Time Division Multiple Access

TDMA allows each user, in sequence, to transmit a fixed-size message segment. Each message segment is initially stored in the computer's buffer. When the network's concentrator-commutator selects a particular buffer, the bits are read out of the buffer and on to the common channel at the network's bit rate.

TDMA systems are very efficient if the users have a continual need to transmit. However if users' transmission needs vary from time to time or if users rarely transmit, the TDMA becomes inefficient. This is because a user occupies the time slot, even when it has nothing to transmit. His time slot

is wasted. During this wasted time an additional user could have been admitted to the network. However, when the data are digital, TDMA is more "natural"; as technology improves, more systems are converting to TDMA.
[Ref.9:p.696]

2. Frequency Division Multiple Access

Under FDMA systems, each user can transmit all of the time, but each must use only a portion of the total bandwidth.

FDMA is a more popular technique than TDMA due to the technological problems arising from building very high-speed circuits required by TDMA. As is the case for TDMA, FDMA is efficient as long as each user requires the use of the network a large percentage of the time. If such is not the case, available bandwidth is being wasted since other users could have transmitted on these bandwidth. Using FDMA these extra users were denied access to the network. [Ref.9:p.696]

3. Carrier Sense Multiple Access

In a CSMA system, each user tunes a receiver to the common carrier frequency employed by all users. Before transmitting, a user (or his computer) will listen to determine if any of the other users are transmitting; if no other user is transmitting, the computer will transmit the message. All potential transmitting users generally are geographically closely clustered as are all potential receiving users. Propagation delay between transmitting users then can be ignored and there will be no data collisions.

[Ref.9:p.704] If all users are not close to another, data collisions can become a serious problem.

The ability to detect collisions and shut down the transmitter promptly is an important feature in minimizing the time on the channel lost to collisions. Some CSMA systems have this ability, and are called CSMA with collision detection (CSMA/CD). The general requirement is that, while transmitting, a controller must recognize that another station is also transmitting. There are two approaches:

- Collision detection in the transmission system. It is usually possible for the transmission system itself to recognize a collision. This allows any medium-dependent technique to be used, and is usually implemented by comparing the injected signal with the received signal. Comparing the transmitted and received signals is best done in the transceiver where there is a known relationship between the two signals. It is the controller, however, which needs to know that a collision is taking place.
- Collision detection in the controller. Alternatively, the controller itself can recognize a collision by comparing the transmitted signal with the received signal, or unilaterally attempting to recognize collisions, since they often appear as phase violations.[Ref.10:p.18]

4. Token Passing Access

A token is a predetermined bit pattern that travels through the network from station to station. Possession of the token enables a station to transmit signals to the network communication channel. If that station has nothing to communicate, the token is passed to the next station.

Token passing techniques differ depending on network topology. In a ring network, consecutive nodes must be physically adjacent to one another, with the token passed between the nodes through the physically communications ring. In a bus network, a "logical ring" may be created, and the consecutive nodes on the ring need not to be physically adjacent. [Ref.11:p.58]

F. TRANSMISSION TECHNIQUES

1. GENERAL

LANs are available as either broadband or baseband. A broadband network is characterized by the use of analog technology. It uses a high frequency modem (greater than 4 KHz.) to introduce carrier signals onto the transmission channel. The carrier signals are then modified (modulated) by a user's digital signal. Because of the analog nature of the network, broadband systems are often frequency division multiplexed (FDM) to provide multiple channels (e.g.,data, video, audio) on one path. (FDM is not mandatory, and a LAN with a single analog channel is called single channel broadband.) Broadband systems are so named because the analog carrier signals operate in the high frequency radio range (typically, in the 5 to 400 MHz range). They operate with widely used CATV 75-ohm coaxial cable. [Ref.3:p.764]

2. BROADBAND SYSTEM

The broadband LAN is unidirectional, that is, the signal travels in one direction. It is not economically feasible to construct amplifiers that operate in both directions, so the broadband LAN uses two separate channels to provide an inbound and outbound channel. Two configurations can be used to obtain the inbound and outbound channels: dual cable and split channel.

A dual cable configuration uses two separate cables, one for the inbound channel and one for the outbound channel. A headend connects the two cables and the connected station uses the same frequency to send and receive.

The split channel configuration uses two different frequencies for the inbound and outbound transmissions on one cable. The headend is responsible for converting the inbound frequencies to the outbound frequencies. It can be either and analog device (changes and amplifies signals) or a digital device (regenerates the digital signals).

Split channel configurations use various schemes to divide the frequency spectrum. Three common approaches are subsplit, midsplit, and highsplit multiplexing [STAL87]:

Direction	Subsplit	Midsplit	Highsplit
inbound	5-30 MHz	5-116 MHz	5-174 MHz
outbound	54-400 MHz	168-400 MHz	232-400 MHz

A split system is some percent less expensive than a dual cable system [HOPK79], and it is convenient if only one cable is installed in a building. However, the dual cable system has over twice the capacity (bandwidth) of the split system, and it does not need a headend frequency translator. [Ref.3:p.765]

3. BASEBAND SYSTEM

The baseband network uses digital technology. A line driver introduces voltage shifts onto the channel to represent binary 1s and 0s. The channel then acts as a transport mechanism for the digital voltage pulses.

Baseband networks do not use analog carriers or FDM techniques. However, multiple access to the medium can be provided by a time division multiplexer (TDM) or by other protocols.

Baseband systems are bidirectional and use one cable. The technology is limited in distance (0.6 mile/1 Km is typical), because the digital pulse attenuates severely over longer distances.

Baseband LANs can use either coaxial cable or twisted pair. The coaxial scheme usually is implemented with 50 ohm cable (in contrast to broadband CATV 75 ohm cable) because it works well on multipoint lines and under conditions where low-frequency noise is present.

Baseband coaxial systems are configured with the following constraints (according to the Ethernet specification):

- Cable length of 500 m.
- Stations attached with distances in between in multiples of 2.5 m.
- A maximum of 100 taps per cable.
- Cable length can be extended by replacing the terminators with digital repeaters.

Twisted pair baseband systems are attractive because they are simple to install, and are relatively inexpensive. But they do not have the capacity of coaxial systems. An unshielded twisted pair configuration often permits the use of existing wire inside a building (for example, telephone wiring). Shielded twisted pair, while more expensive, provides considerably more capacity and supports more drops on the channel. [Ref.3:p.765-766]

The following table provides the reader a summary with the trade-offs of broadband and baseband systems.

TABLE 1. COMPARISON OF BROADBAND AND BASEBAND LANs

Comparison of Broadband and Baseband LANs		
	Broadband	Baseband
Advantages	Distance Capacity Multimedia (voice,TV) Flexible config.	Cost Simplicity
Disadvantages	RF modem costs Propagation delay (split channel or dual capability) Complexity	Capacity One channel One media Distance

III. DESIGN ISSUES OF LANs

A. COMPARATIVE EVALUATION OF DIFFERENT LANs

1. GENERAL

The objective of the local network standards was stated in Chapter II. Out of a number of organizations involved in developing LAN standards, it is essential to mention the Institute of Electrical and Electronics Engineers, known as the IEEE 802 committee.

The IEEE 802 has defined a network architecture oriented specifically to LAN implementation called the IEEE 802 standard family. The standard was developed to enable equipments of a variety of manufacturers to interface with each other. It is in complete conformance with layers one and two of the ISO-OSI model shown in Figure 10.

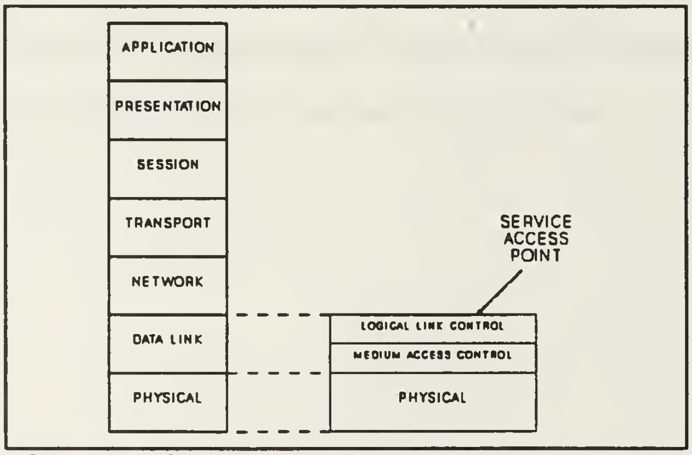

Figure 10. IEEE 802 Reference Model Relationship to OSI Model

The architecture of the 802 standard is in the form of three-layer communication: The physical layer encompasses basically the same features as the physical layer in the ISO model; while the media access control and logical link control sublayer correspond to the data link layer.

a. Physical Layer

The physical layer encompasses basically the same features in both the IEEE and ISO model. It is concerned with transmitting bits over the transmission medium and detail device attachment. This includes encoding the data into the proper form for transmission, type of signaling, and timing control of the devices. The IEEE 802 has standardized basicly on three transmission media explained previously.

b. Media Access Control Sublayer

Media access control is concerned mainly with controlling the use of the physical medium, since devices on the LAN share the cabling system and other transmission facilities. The IEEE 802 chose CSMA/CD, Token Ring, and Token Bus access control methods for standardization.

c. Logical Link Control Sublayer

The logical link control is responsible for medium independent data link functions. It provides an interface for the upper layers to access the LAN device. The standard also defined the interface between the LLC sublayer and MAC sublayer.

The IEEE 802 Committee is currently organized into the following subcommittees: [Ref.12:p.57]

- 802.1: High Level Interface
- 802.2: Logical Link Control
- 802.3: CSMA/CD Networks
- 802.4: Token Bus Network
- 802.5: Token Ring Network
- 802.6: Metropolitan Area Network
- 802.7: Broadband Technical Advisory Group
- 802.8: Fiber Optic Technical Advisory Group
- 802.9: Integrated Data and Voice Networks

The High Level Interface subcommittee deals with issues related to network architecture, internetworking, and network management for local networks.

The initial work on LLC, CSMA/CD, token bus, an token ring was completed and joint ANSI/IEEE standards were issued in 1985. Some minor changes and additions were made and a revised set of standards were issued in 1987. Work continues on additional options and features in each of the four subcommittees. [Ref.12:p.58]

The work on metropolitan area networks (MANs) is just beginning to make progress. The subcommittee is attempting to develop a small number of reasonable alternatives for further study. However, the FDDI standard, described that satisfies many of requirements for a MAN.

The purpose of 802.7 and 802.8 is to provide technical guidance to the other subcommittees on broadband and optical fiber technology, respectively. The 802.7 subcommittee is producing a recommended practices document for broadband cabling systems. The 802.8 subcommittee is investigating the use of optical fiber as an alternative transmission medium for 802.3, 802.4, and 802.5. It is also considering installation recommendations and a tutorial on fiber optic standards and related information. [Ref.12:p.58]

The newest subcommittee, for Integrated Data and Voice Networks, was chartered in November of 1986. It is developing a standard for interfacing desktop devices to both 802 LANs and to Integrated Services Digital Networks (ISDNs), utilizing twisted-pair wiring to carry both voice and data.

The acceptance of the IEEE 802 standards has been remarkably widespread. The National Bureau of Standards, which issues Federal Information Processing Standards for U.S. government procurements, has adopted the LLC and CSMA/CD standards as FIPS 107. The others (802.4 and 802.5) will probably follow. The International Organization for Standardization (ISO) has adopted the 1987 version of 802.2 through 802.5 as international standards 8802/2 through 8802/5. The effect of these standardization activities is to encourage both vendors and customers to employ 802-based LANs.

Applying the knowledge of the IEEE 802 Local Network Standards Committee, it is necessary to make a comparative evaluation of the different network access methods such as CSMA/CD and the Token Ring.

2. IEEE 802.3 CSMA/CD

a. Overview

The IEEE standard 802.3 defines the CSMA/CD access control method initially developed by Xerox Corporation. CSMA/CD is the most commonly used access method for LANs employing bus topology. This protocol is sometimes described as "listen while talk". A station that has data to transmit first senses the medium. If the medium is quiet, the station begins transmitting. Otherwise, it waits for a random period of time before trying to transmit.

The following section presents an overview of the IEEE standard 802.3. In addition, a simplified version of the standard protocol using a system of communicating machines is also presented.

b. MAC Service Specification

This section specifies the services provided by the MAC sublayer to the LLC sublayer. The service specification of the interface between the LLC sublayer and the MAC sublayer is defined by three service primitives: MA_DATA.request, MA_DATA.confirm, and MA_DATA.indication.

The service provided by the MAC sublayer allows the LLC sublayer to exchange the LLC data units.

MA_DATA.request initiates the transfer of data from the local LLC sublayer entity to one or more peer LLC entities. The primitive is generated by the LLC sublayer entity whenever the data needs to be transferred.

The receipt, in turn, will cause the MAC entity to append all specific fields of the particular media access method, and pass them to the lower layer.

MA_DATA.confirm provides a response to the LLC sublayer regarding the success or failure of the request. This primitive is generated as a response to the request from the local LLC sublayer entity. The receipt is unspecified.

MA_DATA.indication defines the transfer of data from the MAC sublayer entity to the one or more LLC sublayer entities to indicate the arrival of a frame to the local MAC sublayer entity. This receipt is also unspecified.

c. *Frame Structure*

The 802.3 standard defines the frame format for data communication across the network. The format is shown in the following figure.

CSMA/CD FRAME FORMAT

Preamble	SFD	DA	SA	LENGTH	LLC Data	PAD	FCS

Preamble begins the frame and is used to establish bit synchronization. The preamble pattern is an alternating sequence of 1's and 0's, with the last bit being a 0.

Start Frame Delimiter (SFD) immediately follows the preamble in the bit sequence 10101011. It indicates the start of the frame.

Destination Address (DA) specifies the station(s) for which the frame is intended. Each address field can be either 2 or 6 octets in length, depending on the vendor that implements the network. The first bit is used to identify whether the destination address is an individual or group, indicated by 0 or 1, respectively.

Source Address (SA) identifies the station that sent the frame. The first bit is reserved and set to 0. The size of the source and destination address must be the same for all stations on the network.

LENGTH is a 2 octet field that indicates the length of the data field. The field is used to determine the length of the data field when a PAD field is included in the frame.

LLC DATA contains data units supplied by the LLC sublayer.

PAD consists of octets added to ensure that the frame is long enough for proper collision detection.

FRAME CHECK SEQUENCE (FCS) ends the frame. FCS field uses a Cyclic Redundancy Check (CRC) to determine whether an error has occurred.

d. *Media Access Control*

1. CSMA/CD Operation

As mentioned above, the most commonly used MAC technique for bus topology is CSMA/CD.

With CSMA/CD, a station wishing to communicate first listens to the medium for a specified period to determine whether another station is currently transmitting a message. If no traffic is detected, the station transmits and continue to listen. If a collision is detected, the station waits for a random interval of time, and tries to transmit the message again. When two or more stations send their messages simultaneously and the result ia a collision, the transmitting stations stop transmitting. In this situation, receiving stations simply ignore the garbled transmission, while transmitting stations must wait for an indefinite period before attempting to transmit.

2. CSMA/CD Function

The IEEE 802.3 standard defines the functional capabilities of the MAC sublayer. These functions can be categorized into three functions: Data Encapsulation/Decapsulation, Media Access Management, and Data Encoding/Decoding which is concerned with transmitting and receiving data.

Data encapsulation function provides for adding information to the beginning and end of the data unit to be transmitted after receiving the frame from LLC sublayer, while data decapsulation function in the receiving station to remove the information before passing the frame up to the LLC sublayer.

Media access management is responsible for controlling the availability of the transmission medium. This includes the action regarding collision.

Data encoding performs the function of translating the bits into the proper electrical signal to be sent across the transmission medium, while data decoding translates it back into the bit stream.

e. Other considerations

1. Message Priority

Since the CSMA/CD standard is intended for operation under a light load, when response time is short, the standard does not provide for message priority. All messages are processed with the same priority.

2. Response Time

The response time of a LAN is the time a message must wait at a station before it can be transmitted. Response time is a function of a network data rate, the load presented by all stations, and the access method.

Under a light load, the CSMA/CD provides short response time, because only a few collisions occur and little time is spent in retransmission. As the load increases, response time increases, since more collisions occur at a higher load. Furthermore, when loading approaches the network's capacity, the response time gets very long and difficult to predict.

3. Error Rate

Since collisions and the resultant garbled transmissions occur regularly on CSMA/CD networks, it is difficult to measure transmission error rates on operating networks.

4. Frame Format

Frame format is one of the most important aspects to be considered in interconnecting networks. In connecting 802.3 to 802.5, a bridge must generate priority bits since 802.5 supports priority while 802.3 does not. Bit order and congestion are other considerations.

5. MAC Protocol

A CSMA/CD access controller does not have to maintain long-term information on the state of the network. There is no requirement for monitor and token management functions. This simplifies the implementation of a MAC mechanism and makes CSMA/CD products relatively inexpensive.

(a) Adding and Deleting Stations. Stations are easily added and deleted simply by activating or deactivating them. Activation allows a station to compete for the bus, and deactivation is not detectable at this level.

(b) Station Behavior. Stations simply operate as if they have exclusive ownership until a collision changes ownership. A station need only wait for the bus to be available. Once a frame is sent, the station can continue using the bus until a collision occurs.

(c) Performance. A station throughput does not depend on the total number of stations; it depends only on the activity of any other station when a transmission is attempted. As loading increases, throughput begins to decrease, with collisions causing delays in completing operations. CSMA/CD operation is unpredictable over short time intervals, so it is not possible to predict or guarantee a certain level of performance. CSMA/CD imposes a minimum time frame requirement to ensure accurate collision detection. Increasing the transmission speed of the bus may not improve throughput in all cases. Only a change in the size of the frame can have an effect, and it may not always be possible to make such an alteration.

3. IEEE 802.5 TOKEN RING

a. Overview

Token Ring is one of the most popular ring access techniques. It is the basis of IBM's main architecture for Local Area Networking, and is one of the access methods selected for standardization by the IEEE 802 committee.

The IEEE 802.5 standard defines the token ring access control method, and describes the services provided by the MAC sublayer to the network management and LLC sublayer. The IEEE 802.5 standard also defines a physical layer based on the shielded twisted pair and differential Manchester encoding. The following section presents an overview of the IEEE 802.5 standard.

b. Token Ring Protocol

The Token Ring network structure consists of serially connected stations using a physical ring topology. Each node is connected to two other nodes: an upstream node from which the data is received, and a downstream node from which the data will be transmitted. Information is passed sequentially in one direction from one station to the next and each station acts as a repeater to forward the data.

Among the Token Ring's attractive features is the fact that is not really a broadcast medium, but a collection of individual point-to-point links that happen to form a circle. A ring is also almost entirely digital. The Token Ring protocols handles maintenance using a monitor that each token has.

The token ring technique is based on the use of a particular bit pattern called a token, which circulates around the ring when all stations are idle. Any station wishing to transmit must possess a token. Upon receiving, the station modifies one bit in a token to transform it into the start of a frame sequence. The station then appends appropriate data needed to construct a frame, and transmits for a specified time.

The data units travel from station around the ring. Each station, while repeating the incoming signal, checks to ensure that the frame's DA field matches the individual address. After the station has completed transmission of its frame and the transmitted frame has returned to the station that originally sent it, the station removes the data unit from the network and initiates a new token to be passed on to the next station so that other stations can transmit their data.

c. *Frame Format*

This section specifies the format generated by the IEEE 802 committee for the token ring access control method. The format of the transmission frame and the special formats for the token and abort sequence are presented.

The first special format is for the token. It contains an access control field and starting and ending delimiter. It is a means by which the right to transmit is passed from one station to another. The format is shown in the figure below:

Starting Delimiter	Access Control	Ending Delimiter

The other special format, called abort sequence, is used to terminate the transmission of a frame prematurely. The abort sequence may occur anywhere in the bit stream. The format is shown in the figure below:

Starting Delimiter	Ending Delimiter

The transmission frame format is shown in the figure below. It is used for transmitting both the MAC and LLC messages to the destination station(s).

TOKEN RING FRAME FORMAT

SD	AC	FC	DA	SA	INFO	FCS	ED	FS

The following are descriptions of the individual fields in the transmission frame, token, and abort sequence formats:

- Starting delimiter (SD): consists of signal patterns to indicate the start of a frame; it also includes nondata values to ensure distinguishability from data.

- Access control (AC): consists of a priority bit to indicate the priority of the token; a token bit to identify whether the frame is token or data; A monitor bit to monitor the persistence of the frame; and a reservation bit.

- Frame control (FC): identifies the type of frame and information frame function.

- Destination address (DA): specifies the station(s) for which the frame is intended; this can be individual, group, or broadcast.

- Source address (SA): identifies the station that sent the frame; the format and length should be the same as the DA in a given frame.

- Information(INFO): contains either a protocol data unit from the LLC sublayer or control operation information from the MAC sublayer.

- Frame-check sequence (FCS): is a 32-bit cyclic redundancy check modified by division of the FC, DA, SA, and INFO fields.

- Ending delimiter (ED): contains nondata values to indicate the end of the frame; it also includes an "I" bit to identify whether it is the last frame of the transmission and an "E" bit for error detection.

- Frame status (FS): contains an address-recognized bit (A) and a frame-copied bit (C) to indicate whether a frame was successfully received by a destination station.

d. Service Specification

The IEEE 802.5 standard specifies the services at the interface between the MAC and the LLC sublayer, the physical layer and MAC sublayer, the MAC sublayer and network management, and the physical layer and network management.

a. The primitives required for the interface between the LLC and MAC sublayer are as follows:

- MA_DATA.request

- MA_DATA.indication

- MA_DATA.confirmation

These services provided by the MAC sublayer allow the local LLC sublayer entity to exchange LLC data units with peer LLC sublayer entities.

b. The services available to the MAC sublayer from the physical layer allow the local MAC sublayer entity to exchange MAC data units with peer MAC sublayer entities. The interface between the MAC sublayer and physical layer is defined in terms of the following primitives:

- PH_DATA.request defines the transfer of data from a local MAC sublayer entity to the physical layer for transmission.
- PH_DATA.indication defines the transfer of data from the physical layer to the MAC sublayer.
- PH_DATA.confirmation provides the response by the physical layer to the MAC sublayer, signifying the acceptance of the PH_DATA.request.

c. The following primitives allow local network management to request services from the physical layer. They thus permit local network management to control the operation of the physical layer.

- PH_CONTROL.request is used to request the physical layer to insert itself into or remove itself from the ring.
- PH_CONTROL.indication is used by the physical layer to inform network management of errors and significant status changes.

d. The services provided at the interface between network management and the MAC sublayer are used by network management to monitor and control the operation of the MAC sublayer. These services are:

- MA_INITIALIZE_PROTOCOL.request is used to reset the MAC sublayer and change MAC operational parameters.
- MA_INITIALIZE_PROTOCOL.conformation is used by the MAC sublayer to indicate the success or failure of the request.
- MA_CONTROL.request is used by network management to control the operation of the MAC sublayer.
- MA_STATUS.indication is used by the MAC sublayer to report errors and significant status changes.
- MA_NMT_DATA.request is the primitive that defines the transfer of data from a local NMT entity to the local MAC entity.
- MA_NMT_DATA.indication defines the transfer of data from the MAC sublayer entity to the network management entity.
- MA_NMT_DATA.confirmation is the primitive sent by the MAC sublayer to indicate the success or failure of the requested data. The station that transmits a data unit is responsible for removing the token from the ring while transmitting, and sending a free token to the next station.

e. Physical Layer

The IEEE 802.5 standard defines physical layer specification, including data symbol encoding and decoding, symbol timing, and reliability.

The physical layer encodes and transmits the four symbols presented by the MAC sublayer using a form known as differential Manchester encoding. The symbols presented are binary zero (0), binary one (1), nondata_J (J), and nondata_K (K). The latency buffer is provided by the active monitor with two distinct functions: assured minimum latency and phase jitters condensation.

The standard also specifies the functional, electrical, and mechanical characteristics for baseband transmission using two 150-ohm shielded twisted pair wires. It supports the use of a data rate of 1 or 4 Mbits/s with a tolerance of 0.01%.

f. Other considerations

1. Message Priority

The token ring provides up to eight separate priorities of data link traffic. A station can preempt the token and reserve it next, regardless of its physical position on the ring relative to the current token-holder. Preemptions are nested by the order of the priority so that proper succession is maintained.

The nature of the ring permits each station to examine the special frame fields while the frame is being regenerated for further delivery. The access control fields have reservation and priority fields to manage prioritized frames. The reservation field is used in frames carrying data, while the priority field circulates with the token.

2. Response Time

Unlike the response time of CSMA/CD, which is short at light load and increases as the load increases, the response time for a token ring is longer at high load, since a station must wait for the token to come around before transmitting. The increase in response time is proportional to the load, which is both efficient and fair.

3. Frame Format

In connecting 802.5 to 802.3, several problems must be considered. The 802.5 frames carry a priority bit that an 802.3 frame does not have. As a result, if two 802.5 LANs communicate via an 802.3 LAN, the priority bit will be discarded. A bridge must reformat the frame. The 802.5 frame has A and C bits in the frame status byte. Another consideration is whether the frame is too long.

4. Measuring Error Rate

Since a Token Ring network sends data only when other stations are not transmitting, the number of garbled data messages is good measure of the error rate. A high error rate is an indication of either an incipient failure in a station or a defective cable.

5. MAC Protocol

A token ring access controller is more complex than a CSMA/CD controller. Creating and operating a token-passing protocol requires transmission capacity and time delays for protocol exchanges. Token maintenance represents an additional expense, because the functions are replicated in each MAC interface. A Token Ring has only one active monitor, although other monitors must be available to take over in case of failure.

(a) Adding/Deleting Stations.- For the purpose of adding and deleting stations, a Token Ring requires only a test for a duplicate address before joining the ring.

(b) Station Behavior.- Stations are well-behaved and fair, in that they surrender the token after a certain time. Predictable response times can be attained because of this stability and predictability. Parameters such as the token-holding time can be adjusted to tune the performance.

(c) Performance.- Token-passing performance is a function of the number of active participants. Passing the token through each station increases the delay and reduces the throughput for every station. As loading increases, token-passing performance remains very stable. If each station uses its full time interval with each token, the behavior is the same as time division multiplexing. The operation remains fair in that each station can receive a guaranteed portion of the capacity.

In the ring, the token returns after traversing the ring and all intervening systems. The minimum waiting time is the propagation delay and the processing delay of all other systems. The maximum delay adds the time intervals that all other systems use for their own transfer to the minimum delay.

B. INTERCONNECTION ISSUES

1. GENERAL

Rapid advances in network and communication technology have increased the need for connecting LANs to cover a wider area. Interconnecting LANs allows information to be passed between widely separated locations without restricting local needs. Furthermore, the ability to reach other users or stations means extending network capabilities far beyond the single network.

Along with the advantages that advanced technology has offered, the proliferation of LANs in industry has resulted in an interoperability dilemma for network users and designers. Network designers are faced with the heterogeneity of networks, just as they were previously faced with the heterogeneity of computers within a single network. The issues of internetworking thus become more important.

2. MAJOR CONSIDERATION

Most of the internetworking general problems are related to the parameters that specify the nature of LANs. Network uses different physical medium to carry data signal for transmission; topology which shows the way network devices are interconnected; and access control methods to control access to the transmission medium.

Some other common problems encountered in interconnecting LANs are shown below:

a. *Frame Format*

Each LAN uses a different frame format. As a result, any copying between different LANs requires reformatting, which takes CPU time, requires a new check sum calculation, and introduces the possibility of undetected errors due to bad bits in the bridge's memory. To see how frame format differs, compare the two frame formats for Token Ring and CSMA/CD shown in section A.

b. *Speed*

Networks allow a variety of speeds. As a result, both software and hardware need to manage the difference in speeds. Each of the IEEE 802 standards uses different speeds. The 802.3 (CSMA/CD) allows 1 to 10 Mbps, while the 802.5 standard calls for 1, 4, or 16 Mbps. In practice, 802.3 is 10 Mbps, and 802.5 is 4 Mbps.

c. *Frame Length*

All three 802 LANs have different maximum frame lengths. This must be considered, since splitting the frame into pieces is out of the question in the data link layer. All protocols assume that the frames arrive, or that they do not.

d. *Buffer Parameters*

Buffers are another important consideration in connecting LANs, since they can improve the performance of the LAN if allocated properly. The buffer is assumed to have a capacity that can hold the largest frame transmitted on the ring and only one frame is transmitted before the token is given up. They store data that is in transit and send it to the processor when the processor is ready to read the data or accept data when the processor is ready to write. They also assist in data transfer from one machine to another. Buffers requires space in the computer memory. This often results in a trade-off between space for buffers or space for application programs because of memory limitations. Consequently, the size of the buffer is a major consideration.

3. GATEWAY

Networks can be connected in a number of ways via a device (or pair of devices) generically called a "gateway". This device provides an interface between networks for establishing long-distance communication between stations on the network. Gateway functions may be implemented with a separate equipment connected to two or more networks, as well with additional modules in an already existing equipment.

Three common types of gateways are bridges, routers, and protocol converters. Each approach to network interconnection raises several issues, depending upon the complexity of the job and how similar the networks are. Some ways in which networks can differ are: frame, packet, message size, addressing scheme, connection or connectionless, timeout system, status reporting, and network access mechanism. Repeaters are discussed for a comparision purpose.

a. *Repeaters*

When merely extending the local distance limitations inherent in LANs, relatively simple devices are used. The simplest device for interconnecting LANs is the repeater, which operates at the lowest level of the OSI reference model, the physical layer. For this reason, repeaters can only be used to link LANs having the same physical-level protocols. They do not control or route information, nor do they generally hace management capabilities. [Ref.13:p.197]

The function of the repeater is merely to generate a signal, thereby maintaining the level of the signal across the LAN. Failure to maintain the signal level in this way will result in the signal becoming distorted. Bad data may go undetected, or throughput may be substantially reduced by forcing retransmissions.

Repeaters pass all the information on a LAN whether or not it needs to be transmitted; hence, repeaters are most often used to interconnect LANs that are close together, within the same building, for example. The IEEE 802.3 design guidelines for Ethernet LANs specify that the span between the two farthest users, including the cable connecting each user to the LAN, cannot exceed 500 meters. Even with repeaters, the typical Ethernet LAN application requires that the entire path not exceed 2500 meters end-to-end, the limit established for the proper operation of the Ethernet collision detection mechanism.

In conclusion repeaters are low-level devices that amplify only electrical signals and are needed to extend cable length. Repeaters simply copy individual bits between similar networks. It is the simplest and the least expensive of interconnection devices.

b. Bridges

The bridge is a protocol-independent interconnection device that operates at the DLL of the OSI reference model. To be more specific, bridges interconnect at the MAC sublayer of OSI's DLL . By working below at the MAC layer, the bridge will interconnect LANs that use the homogeneous MAV protocols.

As long as the bridge operates at the MAC layer, it does not need to perform protocol conversion. The bridge monitors all traffic on the subnets that it links. In reading every packet, it looks only for MAC layer source and destination address to determine where the message is going. On this basis alone, the bridge determines the subnet the message is coming from and the subnet to which it is going. [Ref.13:p.202]

In summary, the bridge is used to connect similar networks but it is more intelligent then repeaters. Bridges accept an entire frame and then forward it to a different subnet. Bridges work in the physical and data link layers.

c. Routers

A router is similar to a bridge in that both provide filtering and bridging functions across the network. However, while bridges operate at the physical and DLLs of the OSI reference model, routers join LANs at the network layer; specially, at the internet sublayer. When interconnecting a LAN and a WAN, routers convert LAN protocols into wide area packet network protocols, and perform the process in reverse at the remote location. They may be deployed in mesh as well as point-to-point networks and can be used in combination with bridges. In fact, hybrid products called "brouters" have emerged in recent years that combine the functions of a bridge and a router in a single unit. [Ref.13:p.209]

Routers differ from bridges in other ways. They generally offer more embedded intelligence, and consequently more sophisticated network management and traffic control capabilities than bridges. In terms of functional sophistication, a router falls between a protocol converter and a bridge. Perhaps the biggest distinction between a router and a bridge is that a bridge delivers messages on a "best effort" basis, which may result in lost data unless the host computer protocol provides protection. In contrast, a router has the potential for flow control and more comprehensive error protection.

d. Protocol Converters

Protocol converters are found in the transport layer and above. The gateway converts the protocol used in one network to that used in another by replacing messages received from one network with the same protocol semantics sent to another.

C. SECURITY ISSUES

Many organizations depend on the integrity of their systems and data in order to transact their business. A massive disruption can occur if the integrity of either is compromised through accidental or malicious means. The number of potential attackers can be very large. Some attackers may be sophisticated, patient programs on other systems that attempt to compromise a system by generating many possible access codes. Other attacks can come from recording actual traffic and extracting access control information that can be used in the future. Even attacks that fail can compromise a system by adding to its processing burden and affecting the performance of legitimate applications.

Systems in an interworking environment must increase their own security and must agree on certain conventions of encoding and procedure if they are to survive these attacks.

Administrative procedures for protecting critical access codes must also be implemented.

Security protocols are needed to validate the identity and privileges of remote users, to authenticate transferred information, and to distribute new access codes. One important service is the distribution of accurate, environment-wide time references that can be used to detect bogus traffic captured at an earlier time. Modifications to portions of the OSI architecture may be necessary to increase the security of operations.

For example, the Transport layer may include additional additional control information fields for conveying additional security information. Connection establishment may include separate encryption of parameters that specify the users in order to protect the identity of the partners. Application entity titles and access control codes may also be encrypted to afford another level of security.

Better security is attained if data encryption and decryption are left to the application users themselves. Lower layers cannot be compromised when the specific key is known only to the users. Drawbacks to this approach are the additional application overhead and the difficulty of using hardware encryption devices above the Data Link level of operation. [Ref.17:p.197]

The internetwork environment may have interconnected subnetworks with different levels of security services.

Additional protocol control information is needed so that the gateways can choose appropriate neighboring gateways and subnets when they are routing internet traffic. Transport layers must also apply appropriate security measures to assure the end-to-end integrity of communication. Both layers use the same encoded security parameter, which defines a security level such as top secret, secret, confidential, or unclassified.

Security within an OSI environment is a large task that affects each computer system and every network. Many products and protocols must be specified, implemented, and certified before much progress can be made.

IV. SELECTION OF A LAN FOR PERUVIAN A.F. COMPUTER CENTER

A. INTRODUCTION

This chapter discusses, firstly, the LAN design issues such as transmission medium, topology, transmission techniques, and access control methods; secondly it discusses the requirements that must be met by any Peruvian Air Force computer center LAN system.

B. SELECTION PROCESS

The main design issues of LANs are: transmission medium, topology, transmission techniques, and access control methods. Table 2 presents options for each of these design issues.

TABLE 2. DESIGN ISSUES OF LANs

Transmission Medium	Topology	Transmission Techniques	Access Methods
Coaxial cable	bus	baseband	CSMA/CD
Twisted-pair wire	tree	broadband	token ring
Fiber optic	ring		TDM
	star		

1. TOPOLOGY

The choice of topology depends on reliability, expandability, and performance factors. The choice is part of the overall task of designing a local network.

The bus/tree topology appears to be the most flexible one. It is able to handle a wide range of requirements, in terms of the number of devices, data rates, and data types. Because the bus is a passive medium, it would appear highly reliable. [Ref.14:p.57] Bus nodes share a single physical channel via cable taps or connectors. Bus networks are easily configured and expanded in most physical layouts, for instance, in a room, building, or building complex. This reason alone is often a major reason in choosing the bus topology for a local network.

The choice of transmission medium and the choice of topology are not independent. Table 3 shows the commonly observed relationship between medium and topology. [Ref.14:p.68]

TABLE 3. RELATIONSHIP BETWEEN MEDIUM AND TOPOLOGY

Medium	Topology			
	Bus	Tree	Ring	Star
Twisted-pair	*		*	*
Baseband coaxial	*		*	
Broadband coaxial	*	*		
Optical fiber			*	

After comparing the topologies, the bus topology would be favored by the Peruvian Air Force for easy expansion.

2. TRANSMISSION MEDIUM

The media used in local area networks include twisted-pair wire, coaxial cable, and optical fiber. Table 4 summarizes some of the important characteristics of the various media. [Ref.14:p.61]

TABLE 4. CHARACTERISTICS OF THE MEDIA

Medium	Signaling Technique	Maximum data rate (Mbps)	Maximum range at Max.data rate(Km)	Practical number of devices
Twisted-pair	Digital	1-2	a few Km	10's
Coaxial cable (50 ohm)	Digital	10	a few Km	100's
Coaxial cable (75 ohm)	Digital	50	1	10's
	Analog with FDM	20	10's	1000's
	Single chn. Analog	50	1	10's
Optical Fiber	Analog	100	1	100's

Types of information that can be transmitted over LAN are data and imagery. We need to transmit voice and video in near future. Figure 11 shows the product selection tree to help determine the best medium for a given environment.

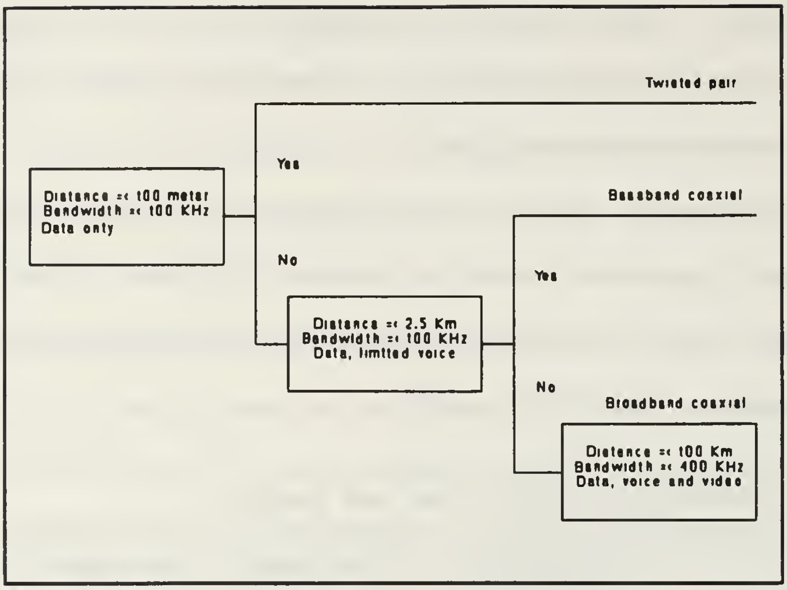

Figure 11. Selection Tree for Medium [Ref.15:p.174]

To decide which medium to select for a LAN, we move from left to right across the selection tree checking the distance, bandwidth, and applications supported by twisted-pair, baseband, and broadband. The optical fiber is currently best only for point-to-point communication. We chose a broadband coaxial cable, which offers sufficient bandwidth to support data, voice, and video. Baseband coaxial cable has only data and some limited voice capability.

Comparing the characteristics of transmission media and requirements of a LAN, we select broadband coaxial cable as the most appropriate for a Peruvian Air Force computer center.

3. TRANSMISSION TECHNIQUES

There are two transmission techniques, baseband and broadband. The argument or trade-off between the broadband and baseband is cost versus bandwidth/data rate.

Baseband employs much more lower bandwidth-usually no more than 50 Mhz and the bandwidth is taken up by transmitting one signal. The bandwidth of broadband signals is usually far greater than that of baseband. It is often the order of 300 Mhz or more. The primary advantage of the broadband system is its handling of video transmission. Broadband systems usually have their available bandwidth broken up into a number of channels. Each of these channels has the potential for transmitting image, data, voice, and text.

The aim of broadband systems is to provide a LAN with the capability of handling large numbers of devices over distances up to ten miles and to carry data, image, and voice transmissions. Baseband systems are generally regarded as being insufficient for continuous video or voice applications. Yet, baseband system are much less expensive and more available today. Table 5 shows the advantages and disadvantages of the two techniques. [Ref.14:p.87]

TABLE 5. BASEBAND VS BROADBAND

Advantages	Disadvantages
BASEBAND	
Cheaper (no modem)	Single channel
Simpler technology	Limited capacity
Easy to install	Limited distance Grounding concerns
BROADBAND	
High capacity	Modem cost
Multiple traffic types	Installation and maintenance complexity

Comparing the characteristics of baseband and broadband systems and considering requirements for a LAN, such as high capacity and multiple data types, we select broadband as a transmission technique for the LAN at the Peruvian Air Force computer centers.

4. CHANNEL ACCESS TECHNIQUES

The decision tree for access method is shown in Figure 9. The dedicated access method is not appropriate because it wastes resources and is inflexible for most office and data processing environments. Both controlled and random access are techniques which permit sharing of a high bandwidth medium by a multiplicity of contending users.

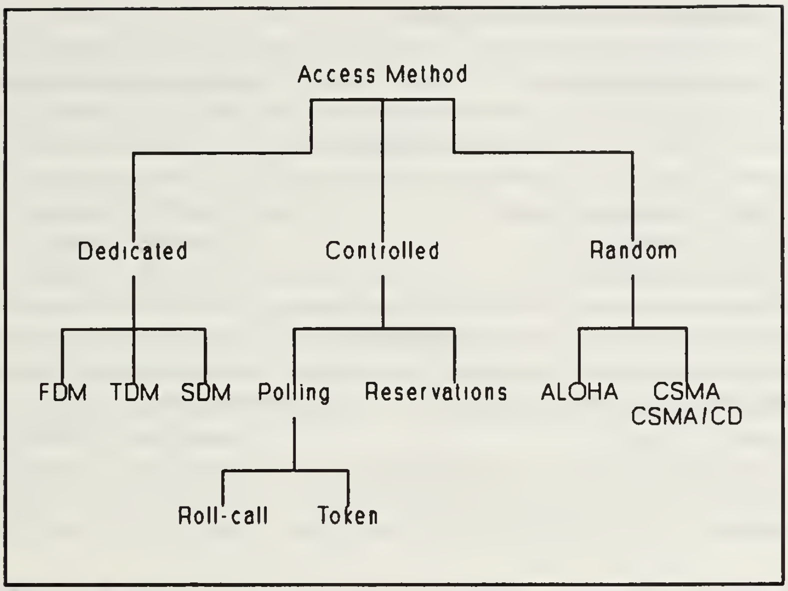

Figure 12. Decision Tree for Access Method [Ref.18:p.28]

In controlled access, contention is reduced by polling or use of reservation. Roll-call polling assumes the centralized controller interrogates each subscriber separately and allocates the channel accordingly.

There is a correlation between network topology and access method. At present, CSMA/CD and token bus are two of the principal contenders for medium access control technique on a bus/tree topology. The advantages and disadvantages of CSMA/CD versus token bus is shown in Table 6. [Ref.14:p.125]

TABLE 6. CSMA/CD VS TOKEN BUS

ADVANTAGES	DISADVANTAGES
CSMA/CD	
Good performance and low to medium load	Poor performance under heavy load
TOKEN BUS	
Good performance under heavy load	Inefficient under low to medium delay

Token passing is more suitable for LANs with heavy traffic (for example, file transfers) and CSMA/CD is appropriate for a large number of bursty users (for example, in a office and interactive data processing environment). Comparing these two access techniques, we select CSMA/CD as an access method which is suitable to the environment of Peruvian Air Force computer centers.

C. IMPLEMENTATION PROCESS

In the previous section, we selected a broadband LAN. Broadband transmission is performed in the VHF band by employing RF modulation. It can support multiple frequency division multiplexing (FDM) channels for data, voice, and video. That is, a broadband network carries mixed media services.

Coaxial cable (75 ohm) is used as the transmission medium because of its capacity, available bandwidth of 300 to 400 Mhz, high speed data transmission rates and very low bit error rate.

Note that RF transmission requires separation of transmit/receive signals either via two separate cables, or by splitting the bandwidth of a single cable and translating transmit/receive signals at a headend. The question of whether to use single or dual cable distribution, remains to be answered. Two different cable schemes single cable and dual cable are shown in Figure 13.

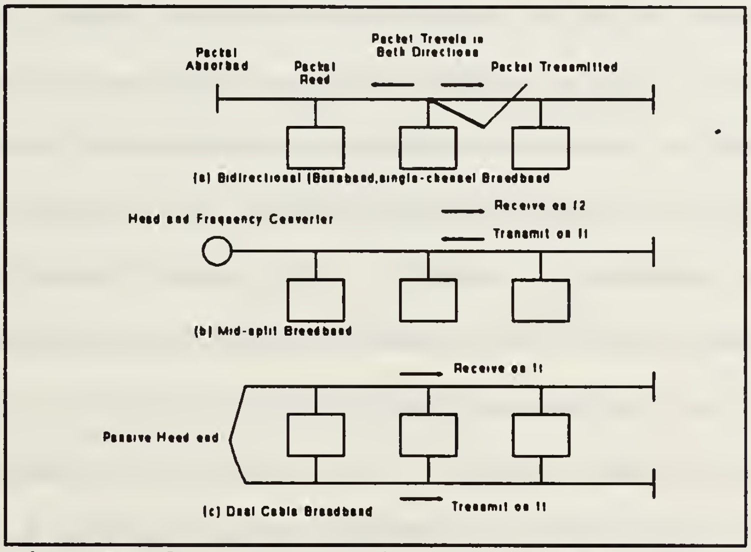

Figure 13. Transmission Techniques [Ref.14:p.81]

A dual cable network uses one cable for inbound carriers and the other for outbound carriers. The split cable is represented by a single cable that loops at the headend, thus creating two separate paths, inbound and outbound. Single cable uses frequency-spectrum split to achieve bidirectional communication.

Dual cable networks are less cost effective than single cable networks because they require twice the amount of hardware, to support the inbound and outbound cables. The single cable networks have half the number of components of the dual cables. Studies indicate an average of only 35 percent of the total available bandwidth is currently being used in broadband local networks.

There are exceptions, but generally only a fraction of the available bandwidth is needed in each direction to meet the requirements for most local networks for data, voice, video, and control. Single cable networks fit better, especially if the network is to be installed in an existing facility. Single cable networks can be represented as a branching tree, which simplifies network design and also facilities network maintenance. Dual cable became a problem, since the loop must be maintained throughout the network.

Based on the benefits of mid-split configurations as explained above, the mid-split format using a single cable broadband system is selected. [Ref.3:p.765]

The components of a single cable broadband system are cable (75 ohm coaxial cable) with 75 ohm terminator for all end-points, amplifiers, directional couplers, and controllers. Cables used in broadband LANs are of three types: trunk, distribution, and drop cable. [Ref.14:p.83] Trunk cables are used for larger systems. Distribution cables are used for shorter distances. Drop cables are used to connect stations to the LAN. For single cable systems, amplifiers must be bidirectional, passing and amplifying lower frequencies in one direction and higher frequencies in the other.

Directional couplers or taps divide an input into two outputs and combine two inputs into one output. Splitters are used to branch the cable. The broadband tap is a passive directional coupler that provides a mechanical interface between the trunk and the drop cable. The maximum length between the tap and the modem is 50m.

In the military environment, network redundancy is desirable in order to provide a back up to crucial network services in case the primary network is damaged. In a mid-split network, two cables are installed side by side, providing the redundant communication path.

Using the basic components of a broadband cable system, the layout of a computer center LAN can be drawn as in Figure 14.

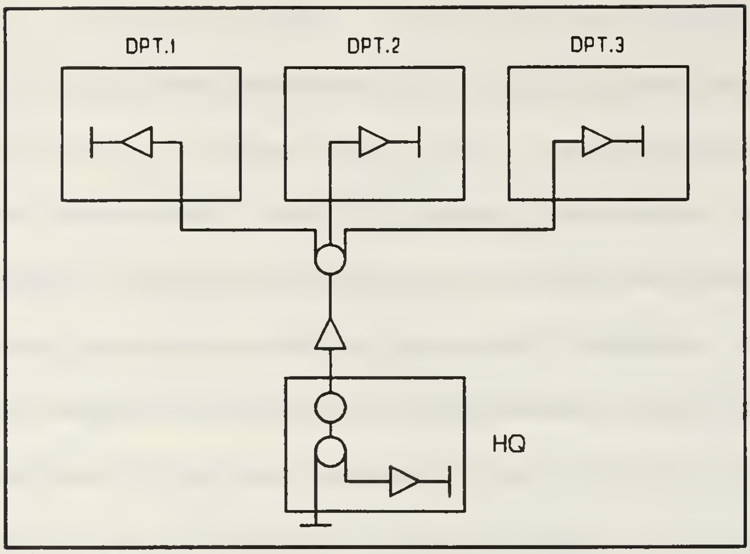

Figure 14. Layout of the System

D. REQUIREMENTS

The scarcity of both manpower and monetary resources in the Peruvian Air Force demands the use of computers for the planning and implementation of programs. Computers will also raise executive efficiency and improve the working environment The following requirements must be met for any computer center LAN system in the Peruvian Air Force.

1. BUDGET

Funds must be allocated based on performance and on need; money cannot be spent if not available. Many budget issues arise when installing LAN equipments. These include:

- What is the minimum require cost?
- Who will support the system?
- Who will pay for the training?
- Who will pay for maintenance and spare parts?

Funds must be carefully allocated, controlled, and utilized by an able staff which has computer expertise, if possible. Poor distribution and use of funds have caused many failures. In addition, once purchased, the equipment is plant property and must be accounted for accordingly.

2. TRAINING AND MAINTENANCE

The Peruvian Air Force Academy is responsible for training students in data communication concepts. The Peruvian Capacitation School and the Electronic Communication School are responsible for training users in the operation of LANs. Many sources of help are available. These include:

- Individuals who set up the training program.
- Vendors of computer equipment used in training.
- Commercial training consultants.
- Experienced personal from the command or from neighboring commands.

Maintenance is not usually a major problem with small computing systems. If these systems are operated properly in a relatively clean, cool environment, few problems should be encountered. However, protection against brown-outs and power fluctuations is important. Also, the user must protect the Air Force warranty rights, and careful inspection of service and operating requirements is necessary to protect those rights. Maintenance requires the following:

- Maintenance training for unit personnel.
- One-time purchase request that includes appropriate warranties.
- Preventive maintenance as part of each day's routine work, such as head cleaning and enclosure dusting.

The option of leasing equipments should be considered due to the rapidly changing nature of computer technology and periodic upgrades to existing systems are advised.

3. SECURITY

The computer center LAN will be used to help manage such things as documents, record rosters, security rosters, training records, and many other types of personnel information. The LAN multiplies the problems of affording appropriate levels of protection for personal and intelligence information. Data on a network medium is not automatically safe from enemies and intruders. Several safeguards must be used to ensure security. Special database software which affords passwording and file security may have to be acquired. Restricting access to a LAN to particular persons may be necessary. Appropriate physical security of backup tapes, diskette media, and the like must be provided.

LANs used in the military environments should provide different security levels, based on subscriber needs. For multilevel subscribers, communication should be restricted according to the Peruvian Air Force regulations security policy constraints. Basically these regulations of security are divided as shown below:

- Unclassified
- Confidential
- Restricted
- Secret
- Top secret.

4. RELIABILITY

One of the characteristics of a LAN must be low error rate, since reliability is one of the most important requirements for data communication. The transmission medium and access methods associated with different topologies will produce different levels of reliability. Thus the error detection technique must be tested and considered before installing a LAN system. If the receiver of data cannot read or believe it, the system is useless.

5. EFFICIENCY

Economies of scale play an important role in any computer system. Economic efficiency means allocating resources in the best manner among the various types of work stations, printers, and computer peripherals that make up the system. The simplest possible techniques are the best.

Computer and data communication functions can be applied to various aspects of social and economic life. The best systems are modular, ensuring that they will not require replacement all at once and can be kept modern as some peripherals change. Due to the rapid pace of technological change in the computer and communication industries, data processing and information sharing techniques change rapidly. The throughput of a LAN is directly related to the access method, processing capacity, and transmission medium at each network node. A high speed data rate is desirable, and the systems must be compatible for interconnection with long distance networks, if possible.

6. PERFORMANCE

Many studies have determined that the single most important factor in determining network performance is the type of access method employed. For optimum LAN performance, it is necessary to investigate and make comparisons between the most commonly used multiple access control protocols which can be used to control network access. Each of the three topologies should be examined to determine which provides the best performance, as part of the process of deciding which LAN is most appropriate for use.

Both bus and ring topologies are good for LANs, as discussed in Chapter II. Some topologies that utilize the CSMA/CD method perform better for applications where short-burst traffic is characteristic, while token-passing access method provides relatively better performance when the network has a heavy load.

Figures 15 to 20 provide the maximum data rates and throughput rates for different medium access methods and different topologies. [Ref.19:p.364-367] Several assumptions are made for these comparisons:

- There are two delay regimes, low delay and high delay.
- Ring topology uses only token passing access for control and all nodes are equidistant apart.
- Bus topologies can use token passing or CSMA access method.
- There are 100 nodes. At low delay one node is on line and sending traffic. At high delay 100 nodes are on line and sending traffic.
- All frames consist of a header and a trailer with a total of 96 control bits.
- The total bit count for a frame is 500, 1000, or 2000 bits including control and data bits.

The following conclusions can be drawn by examining the plots:

- Token ring is the least sensitive to workload.
- Token ring offers short delay under light load.
- Token ring offers controlled delay under heavier loads.
- Token bus has the greatest delay under light load.
- Token bus cannot handle as much traffic as a ring under heavy load. [Ref.16:p.154]
- CSMA offers very low delay under light load.
- CSMA is quite sensitive to the heavy work load.

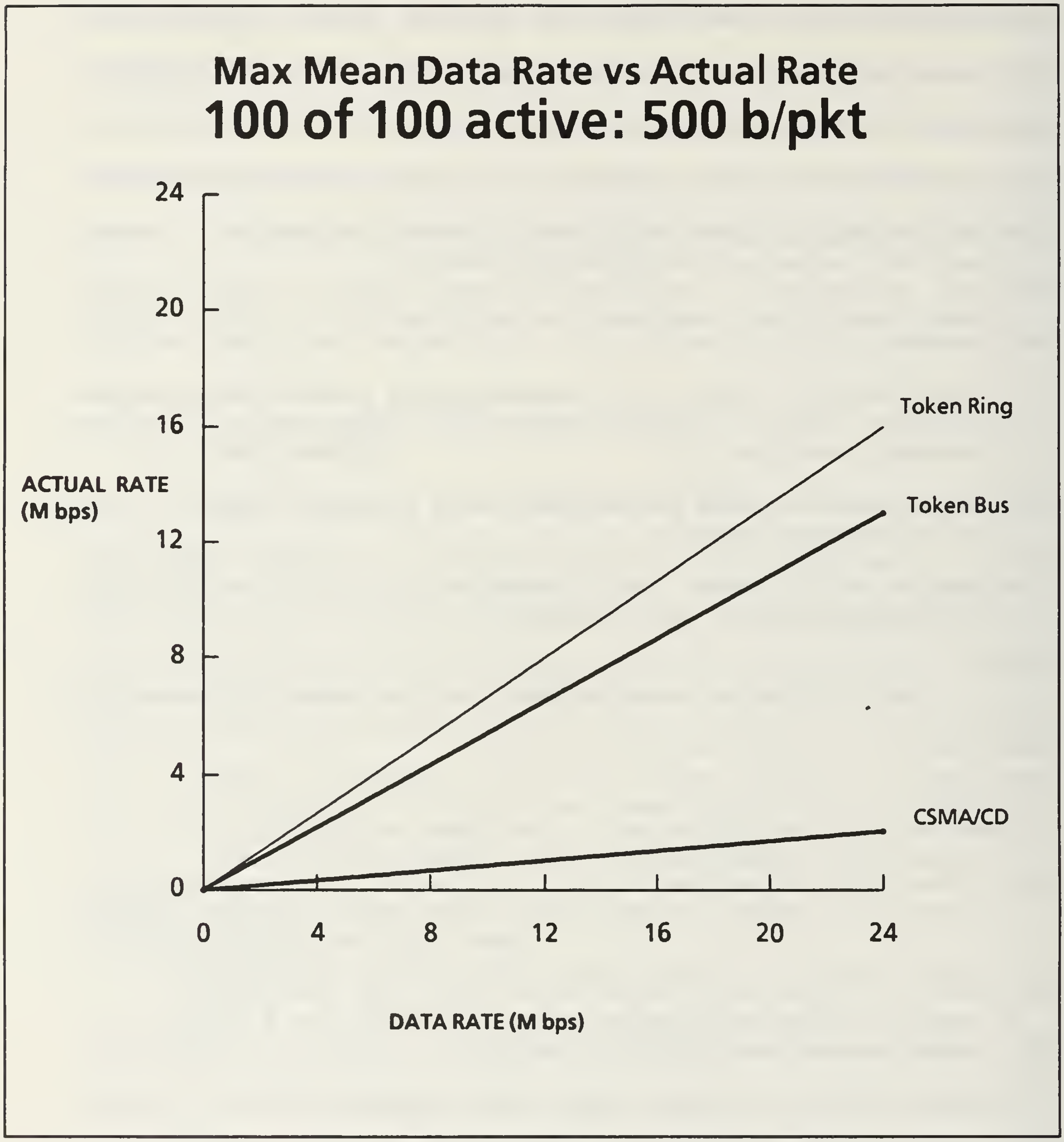

Figure 15.
Comparison of Token Ring, Token Bus, and CSMA/CD Topologies When all Nodes are Actives, at 500 Bits per Packet

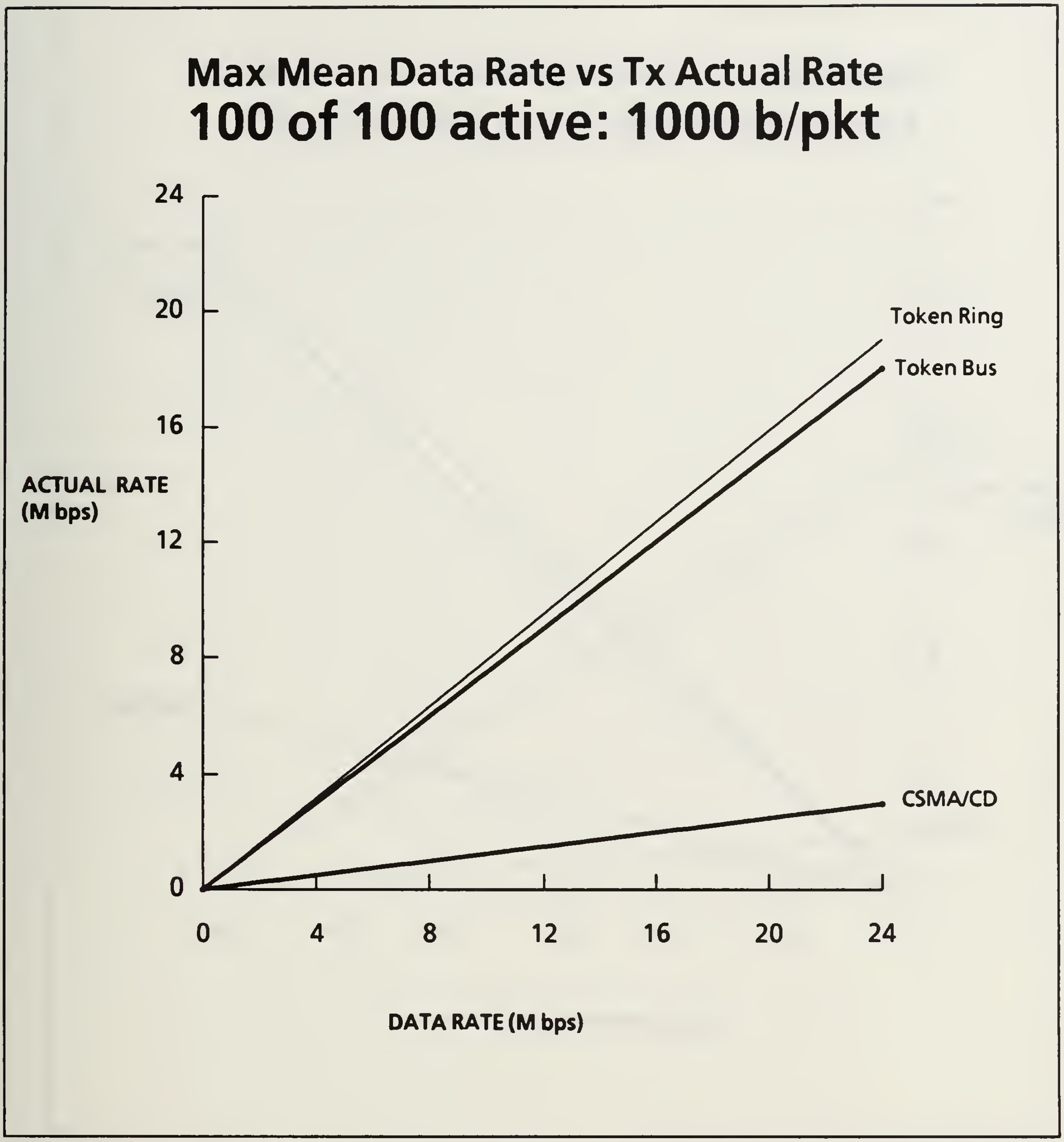

Figure 16.
Comparison of Token Ring, Token Bus, and CSMA/CD Topologies When all Nodes are Actives, at 1000 Bits per Packet

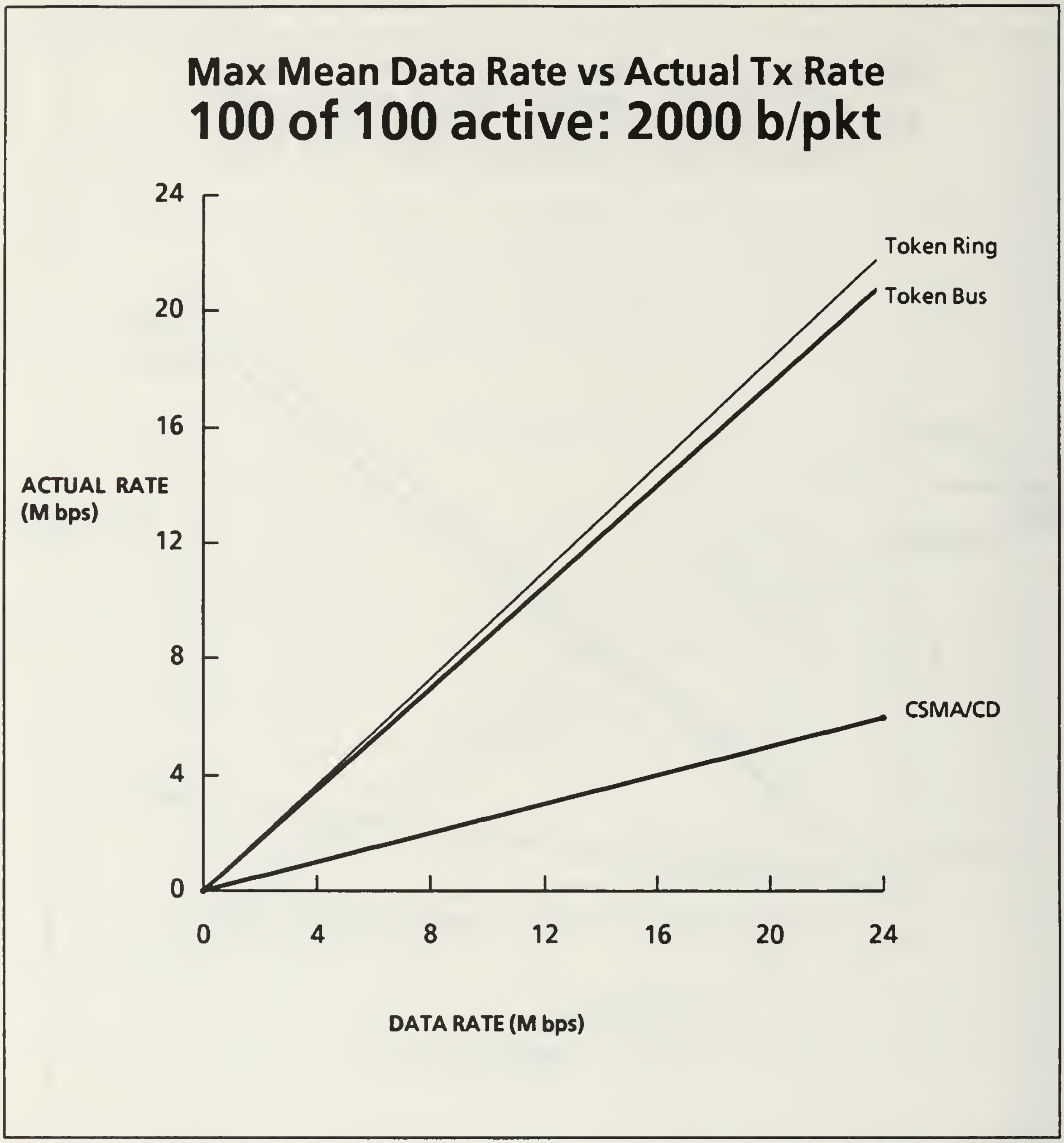

Figure 17.
Comparison of Token Ring, Token Bus, and CSMA/CD Topologies When all Nodes are Actives, at 2000 Bits per Packet

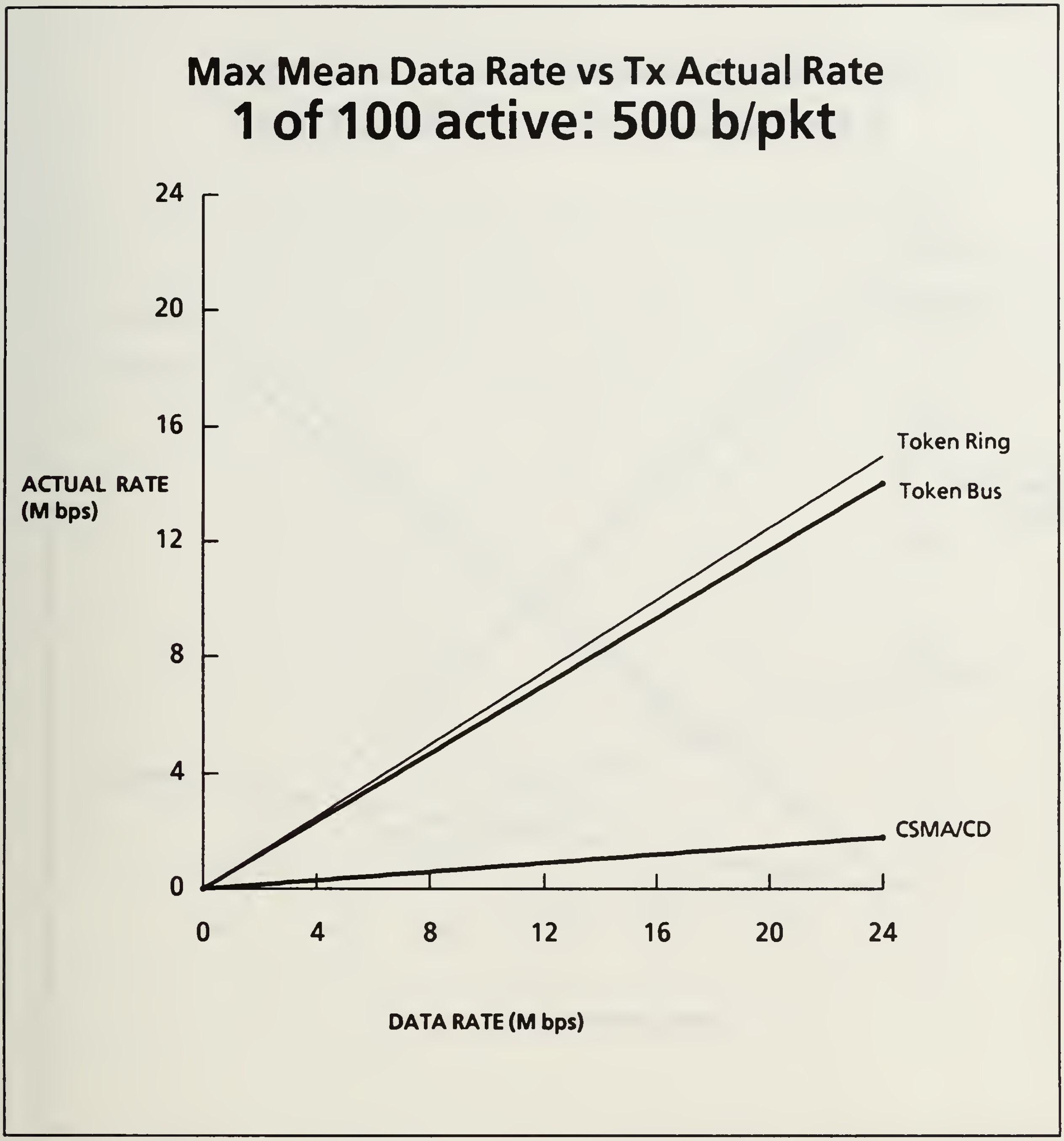

Figure 18.
Comparison of Token Ring, Token Bus, and CSMA/CD Topologies When Only One Node Out of 100 is Active, at 500 Bits per Packet

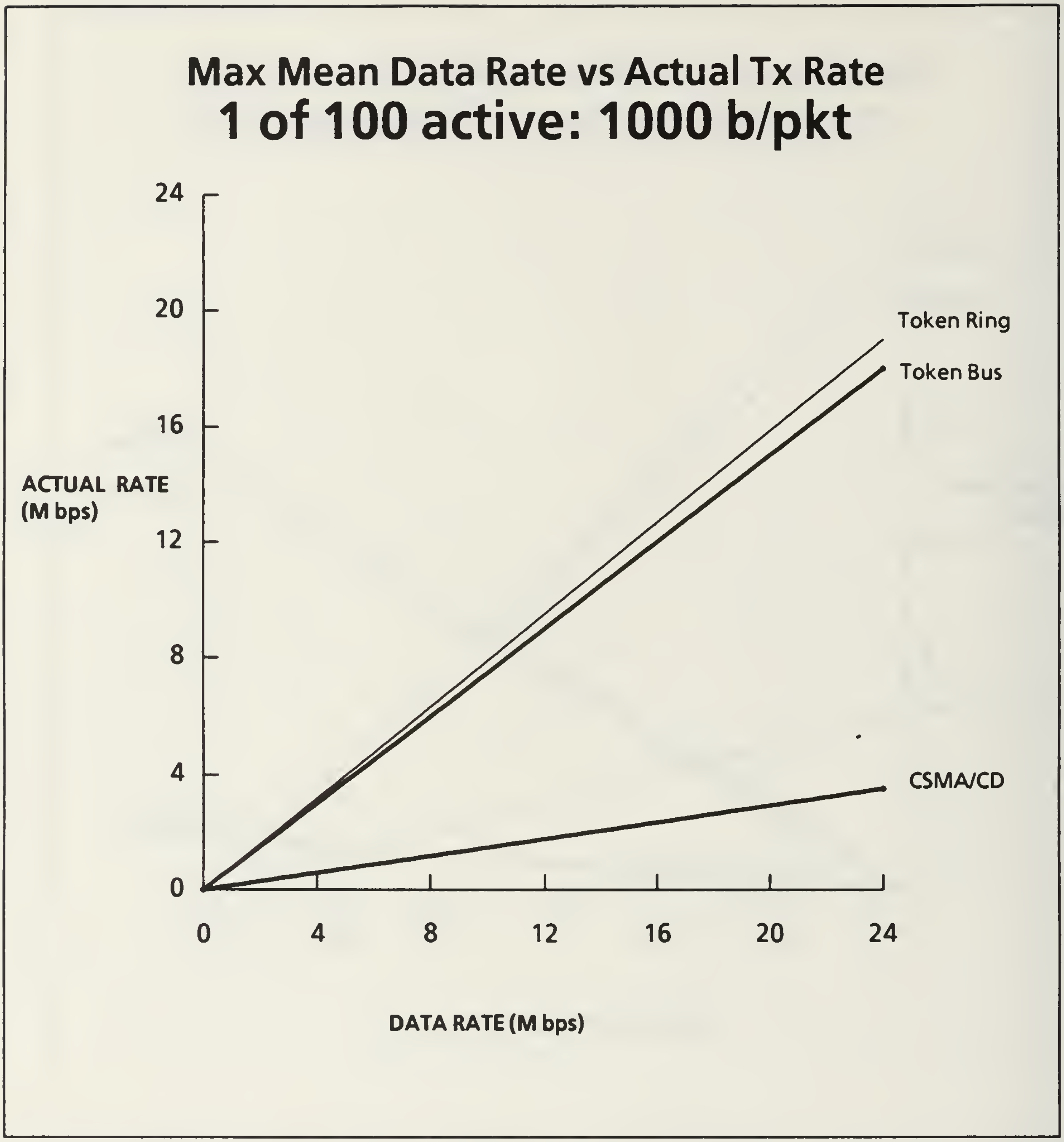

Figure 19.
Comparison of Token Ring, Token Bus, and CSMA/CD Topologies, One Node Out of 100 Active, at 1000 Bits per Packet

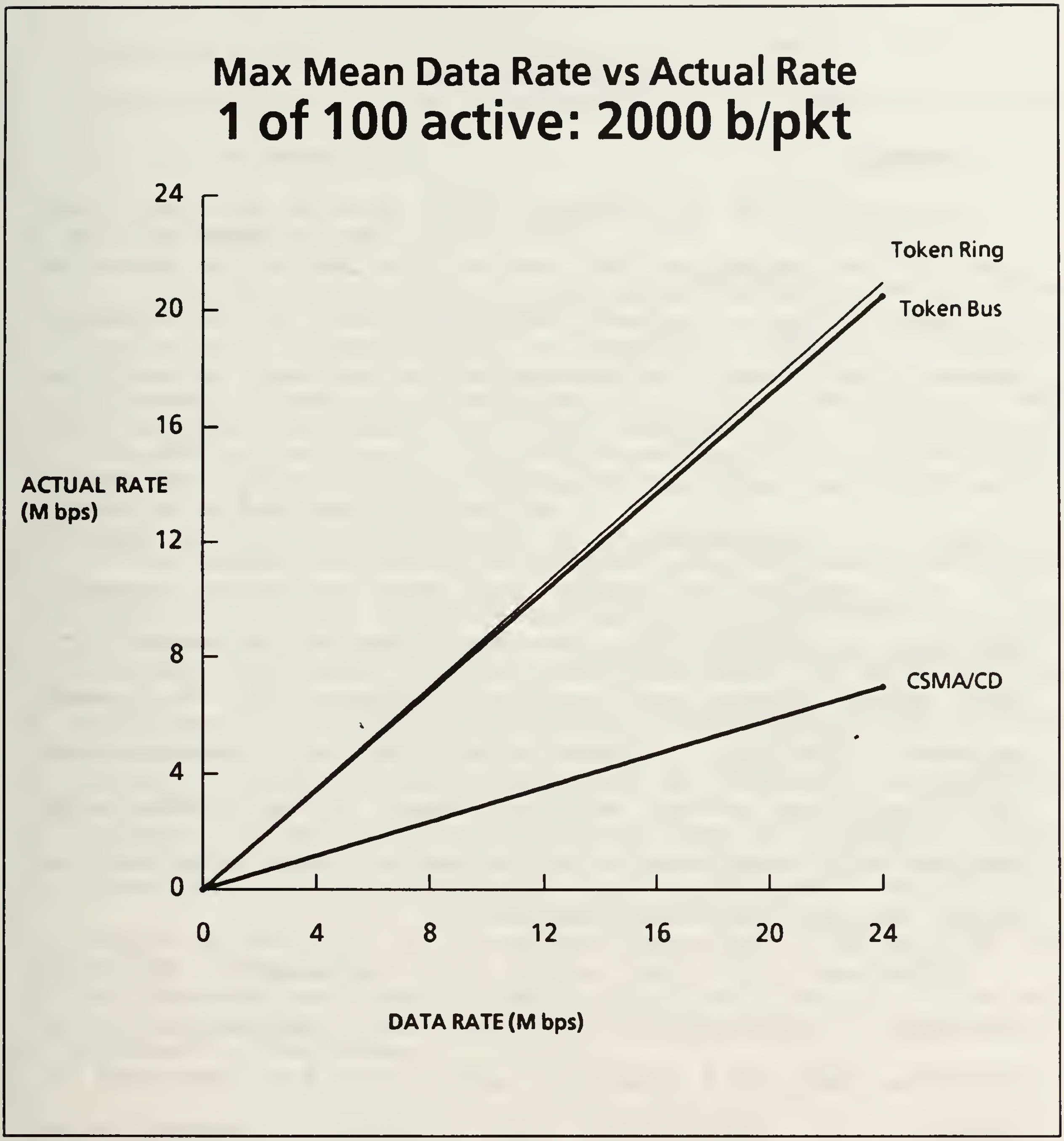

Figure 20.
Comparison of Token Ring, Token Bus, and CSMA/CD Topologies, One Node Out of 100 Active, at 2000 Bits per Packet

V. CONCLUSIONS

A. SUMMARY

The purpose of this study was to provide the basic key elements and guidelines for designing a LAN in the Peruvian Air force computer centers. The first part of this thesis reviewed the overall telecommunication systems, defined the problems of the Peruvian Air Force computer centers, and specified the goals and objectives of the study. The basic concepts of data communication have been discussed in Chapter II. Two popular LAN models and some practical computer standards and architectures have been provided in Chapter III. Major design issues were examined in Chapter IV. The issues included topology, transmission medium, transmission techniques, and access methods. These design issues were compared with requirements and selection trees were used to select the best LAN configuration.

Computers will be useful for integrating military knowledge in the Peruvian Air Force. The requirements for an effective LAN for a computer center have been provided in Chapter IV. Introducing new computer communication technologies and computer equipments to the Peruvian Air Force so that the resulting system meet critical Peruvian Air Force goals is a very important agenda for the future.

It is expected that this study serves as a guideline for constructing the LAN to connect system elements. The actual implementation and the construction of the LAN is a subject for future research.

B. RECOMMENDATIONS

Computer system and networks should be developed to be as simple and uncomplicated as possible. Since the use of different brands of computers introduces complexities and compability problems for interconnecting WANs and LANs, this should be avoided if possible.

Different network access methods associated with different topologies result in different levels of performance in LAN systems. Therefore, before installing LANs, the Peruvian Air Force must decide what kind of performance is required for the future. Security factors also must be seriously considered, Budgets, reliability, and efficiency must be considered. Once installed, the air force must plan to test and evaluate the resulting security of the system. Reports of the results can be discussed and used to improve the Peruvian Air Force LAN systems in the future.

APPENDIX A

CINFA.- Centro de Informatica de la Fuerza Aerea

DIGEC.- Direccion General de Economia

EMGRA.- Estado Mayor General

ALAR2.- Ala Aerea No.2

SEBAT.- Servicio de Abastecimiento

SEMAN.- Servicio de Mntenimiento

EOFAP.- Escuela de Oficiales de la Fuerza Aerea del Peru

HCDA.- Hospital Central de Aeronautica

ESFAP.- Escuela Superior de la Fuerza Aerea del Peru

DIGAF.- Direccion General de Aero Fotografia

LIST OF REFERENCES

1. Loomis, M.E.S, Data Communications, Prentice-Hall Inc., 1983.
2. McGlynn, D.R., Distributed Processing and Data Communication, John Wiley and Sons, Inc., 1978.
3. Black, Uyless D., Data Networks, Printice-Hall Inc., 1989.
4. Halsall, F., Introduction to Data Communications, Addison-Wesley Publishing Company, 1985.
5. Tanenbaum, A.s., Computer Networks, Printice-Hall Inc., 1981.
6. Stallings, W., Data and Computer Communications, Macmillan Publishing Company, New York, 1985.
7. Well, J.D., IBM's Token-ring LAN; A Base-level Communications Solution, student report, Air Command and Staff College, Maxwell AFB., Alabama 1984.
8. Goles, D., Introduction to Local Area Networks, Digital Equipment Corportation, Marynard, Mass., 1984.
9. Taub, H., and Schilling, D.L., Principles of Communications Systems, McGraw-Hill Book Company, 1986.
10. Goos, G., and others, Local Area Networks: Advanced Course, Springer-Verlog, Berlin, 1985.
11. Luczak, E.C., Global Bus Computer Communication Techniques, Computer Networking Symposium, IEEE, MD, 1978.

12. Stallings, William, Local Area Network Technology, IEEE Computer Society Press Publishing Company, California 1990.

13. Muller, N.J., Davidson, R.P., LANs to WANs: Network Management in the 1990s, Artech House, Inc., 1990.

14. Stallings, William, Local Networks: An Introduction, Macmillan Publishing Company, 1984.

15. Dahod, A.M., Local Network Standards: Data Communication, March 1983.

16. Lundquist, C.Q., Handbook for Local Area Network, Computer, June 1985.

17. McConnel, John, Internetworking Computer Systems Prentice-Hall, Inc., 1988.

18. Lissack, T., Maglaris, B. and Frisch, I.T., Digital Switching in Local Area Network, IEEE Communication Megazine, May 1983.

19. Stallings, William, Data and Computer Communications, Second Edition, Macmillan Publishing Company, 1988.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2.	Library, code 52 Naval Postgraduate School Monterey, CA 93943-5002	2
3.	Comando de Instruccion de la Fuerza Aerea del Peru Cuartel General de la Fuerza Aerea Peruana Lima, Republica del Peru	1
4.	Centro de Informatica de la Fuerza Aerea del Peru Cuartel General de la Fuerza Aerea Peruana Lima, Republica del Peru	3
5.	Escuela de Oficiales de la Fuerza Aerea Peruana Biblioteca del Grupo del Instruccion Base Aerea "Las Palmas", Surco Lima, Republica del Peru	2
6.	Escuela de Capacitamiento (ESCAP) de la Fuerza Aerea del Peru, Surco Lima, Republica del Peru	1
7.	Escuela Superior de la Fuerza Aerea del Peru (ESFAP) Cuartel General de la Fuerza Aerea del Peru Lima, Republica del Peru	2