1986

Local area networks :

Mark G. Stickler
Lehigh University

LOCAL AREA NETWORKS:
METHODS OF DETERMINING THEIR NEEDS
AND MODELING THEM FOR DESIGN
AND PERFORMANCE ANALYSIS

by

Mark G. Stickler

A Thesis

Presented to the Graduate Committee

of Lehigh University

in Candidacy for the Degree of

Master of Science

in

Electrical Engineering

Lehigh University

1986

This thesis is accepted and approved in partial fulfillment of the requirements for the degree of Master of Science.

5/19/86
(date)

Professor in Charge

Chairman of Department

TABLE OF CONTENTS

ABSTRACT

This thesis describes a methodology for assessing needs of local area networks (LAN's) and for modeling of those needs in a simulation analysis. This thesis is primarily concerned with proposing a way of determining a suitable LAN architecture for a particular manufacturing enviornment. Fundamental concepts of LAN's are discussed. An overview of the General Motors Manufacturing Automation Protocol (MAP) is presented. This is followed by discussion of methodologies. The reader who already has a thorough understanding of LAN's and/or MAP may skip to the methodology section.

INTRODUCTION

Currently there is a great deal of activity in the area of computer networks and in local area networks (LAN's) in particular. One environment in which LAN's show tremendous usefulness is manufacturing. The importance of communication between so called "islands of automation" of today's factories cannot be over stated. This importance has been universally recognized by people involved in creating the "factory of the future". But what has not been universally recognized is a methodology for determining communication needs of a given factory. An efficient method is needed for modeling a LAN and for simulation to determine if factory communication needs are met. This paper describes a needs methodology and a modeling technique.

Because LAN concepts are relatively new, not everyone involved in factory automation is familiar with fundamentals. This thesis first provides an explanation of LAN architecture fundamentals including design and performance issues. After the reader is comfortable with

the fundamentals of LAN's then the latest version of the General Motors Manufacturing Automation Protocol (MAP) will be summarized. The reader will gain a working knowledge of important LAN features in the manufacturing enviornment. This helps in understanding particular needs of factory LAN's. After needs are established the next step is to apply them to a given factory and to determine the best LAN solution for that factory. This requires a methodology of capturing a factory's communications needs. This thesis will explain a methodology developed at Lehigh University for capturing and characterizing information flow requirements. Once communication needs have been deterimined then it is necessary to accurately model needs in a simulation study. A methodology is presented for building a simulation model suitable for efficient design and performance analysis. This is followed by a presentation of some of the important issues in the areas of analysis and performance including methods of determining key performance characteristics of LAN's.

The next logical step would be a detailed explaination of simulation packages which lend themselves to LAN applications, along with a discussion of the experiences and results of an actual simulation analysis and LAN design. Unfortunatly, due to time contraints, this author

was unable to pursue these activities. It is hoped that this thesis may spark interest in this timely subject and encourage further research to be directed toward both the concepts presented here and the ones which time prohibited.

Chapter One

Overview of Local Area Network Architecture

1.0 Introduction

The concept of local area networks (LAN's) is a relatively new one and is still in the developmental stage. However, many of the basic aspects of communications systems which fit into the LAN catagory have been set down in various sources. There are a number of definitions used to define the catagory of communications networks known as LAN's all of which are correct, but the general definition used here will be that which Stallings [1] uses:

> A communications network that provides interconnection of a variety of data communicating devices within a small area. Typically privately owned with high data rates and low error rates.1

What this generally entails is a network covering several kilometers and limited to a small group of

1. Stallings, Local Networks, pg. 2

buildings such as a corporate or university campus, a factory, or simply an office building. As for the various data communication devices, this can include almost any device which uses information in its operation. This might be something as simple as a printer or as complex as a mainframe computer, what is important is that it be able interface to the network through some means. The idea of being privately owned goes along with the limited size of the network, whereas long haul or wide area networks generally involve many different entities as users. Finally, the data and error rates involved with LAN's will be discussed in detail later on in this chapter.

1.1 Advantages and Disadvantages of LAN's

Before any of the details of LAN's are presented it is important to understand the motivation behind implementing one. This is best shown by presenting some of the advantages and disadvantages of local networks. Stallings [1] has summerized them in the following manner:

Advantages:

1. System evolution: incremental changes with contained impact
2. Reliabilty/availablity/survivabilty: multiple inter-

connected systems disperse functions and provide backup capabilities

3. Resource sharing: of expensive peripherals, hosts, data
4. Multivendor support: customer not locked into a single vendor
5. Improved reponse/performance
6. User needs single terminal to access multiple system
7. Flexibility of equipment location
8. Integration of data processing and office automation.

Disadvantages:

1. Interoperability is not guaranteed: software, data
2. A distributed data base raises problems of integrity, security/privacy
3. Creeping escalation: more equipment will be procured than is actually needed
4. Loss of control: more difficult to manage and enforce standards.

Most of the points in the above list should be self evident. It should also be apparent that the advantages of LAN's outway the disadvantages in most cases, otherwise it would be hard to justify a LAN implementation. In addition, it should be noted that some of the above points, such as the enforcement of standards, are more important than others. The standards issue is a major

force behind the MAP movement discussed later.

1.2 LAN Architecture

The fundamental concept of LAN's, and any other type of communications network for that matter, is the division of the overall architecture into a layered model. The most universally accepted model is the ISO-OSI 7 layer model which structurally defines the communications tasks in a hierarchically layered set. Zimmerman described the procees used by ISO to arrive at their model in the following manner:

"1. A layer should be created where a different layer of abstraction is needed.

2. Each layer should perform a well defined function.

3. The function for each layer should be choosen with an eye toward defining internationally standardized protocols.

4. The layer boundaries should be choosen to minimize the information flow across the interfaces.

5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy." 2

With this in mind the ISO arrived at its OSI seven

2. Tannenbaum, Computer Networks, pg. 15.

layer model. A brief discription of each of these layers follows starting with the lowest layer and continuing in ascending order. This is only intended to refresh the reader's memory. If a detailed explaination is desired it can be found in Tanenbaum [2] and in other references.

The Physical Layer (lowest) is concerned with the transmission of bits over the physical link. It includes the electrical, mechanical, functional and procedural characteristics of the interface. Examples include RS-232-C and X.21.

Next the Data Link Layer provides the means for a reliable channel, through error detection and frame acknowledgement. It also sets up, maintains, and shuts down the link. Examples include Bi-Synch and HDLC.

The Network Layer (third) is in charge of routing and flow control to facilitate communication across the network. It can also provide datagram or virtual circuit communication for packet (systems) or circuit switching for non-packet systems. The most prominent example is X.25.

The Transport Layer (fourth) is commonly referred to as the first end-to-end layer because it provides reliable transfer of data between devices. It ensures data is delivered error free, in sequence, with no loss or

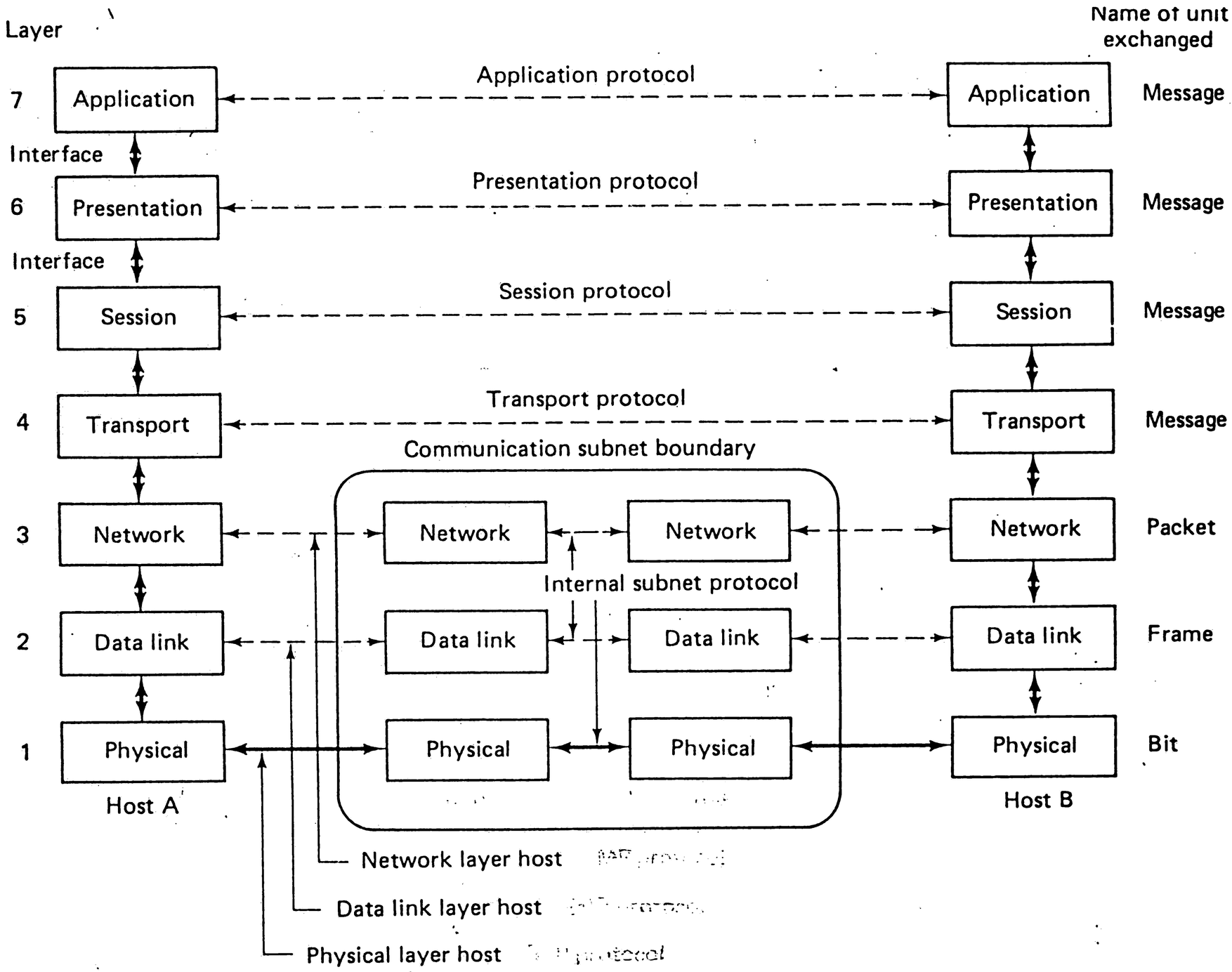

Layer
Name of unit exchanged
7
Application
Application protocol
Application
Message
Interface
6
Presentation
Presentation protocol
Presentation
Message
Interface
5
Session
Session protocol
Session
Message
4
Transport
Transport protocol
Transport
Message
Communication subnet boundary
3
Network
Network
Network
Internal subnet protocol
Network
Packet
2
Data link
Data link
Data link
Data link
Frame
1
Physical
Physical
Physical
Physical
Bit
Host A
Host B
Network layer host
Data link layer host
Physical layer host

Figure 1.1

duplication.

The Session Layer (fifth) is in charge of set up and use of a session or connection. It provides duplex type, quarantining, and recovery mechanisms.

The Presentation Layer (sixth) generally handles manipulation of data before transmission and after reception. This includes such tasks as encryption, compression, and formatting.

Finally, the Application Layer is concerned with application dependent services. They include vendor programs such as transaction servers, network management, file transfer, and electronic mail.

The above brief refresher may help the reader in the following sections. These sections concentrate on LAN design issues and discuss advantages and disadvantages related to particular LAN implementations.

1.3 Topology

The topology of a network is the actual physical configuration of nodes and their connecting links. It is possible for a physical topology to behave differently internally on the logical level, i.e., the physical bus,logical ring configuration. But the concept of the network's topology is nevertheless limited to the physical

layout. There are three common topologies for LAN's. They are the star, the ring, and the bus. In the following discussion of these topologies the term point-to-point refers to a single link between exactly two stations and the term multipoint refers to a bus-like link in which one or more stations have access to the channel.

In the star configuration each station is connected by a point-to-point link to a common hub which is the central switch. This requires the use of circuit switching (discussed later). Any station wishing to communicate with another must request a connection through the central switch to the destination. This centralized control relieves the burden on individual stations but can result in total network failure if the hub goes down.

The ring topology is configured as the name implies with a set of repeaters connected by point-to-point links in a closed loop. Stations are connected to bufferless repeaters, which accept data on their in-link and retransmit it on their out-link as fast as it is received. Packet switching (discussed later) is used and control is necessarily decentralized.

Lastly, in the bus topology the communications network itself is the transmission medium thus negating the need for switches or repeaters. All stations connect

to the bus in a multipoint fashion. This is also known as a broadcast system since a station simply transmits a message which propagates the entire length of the network, enabling the messgae to be received by all stations. Only one station can transmit at a time, necessitating a method of access control (usually distributed). As with the ring topology, packet switching is typical. The tree topology is simply a generalized form of the bus where you have a branched cable with no loops.

It should be noted that each of these configurations has advantages and disadvantages. The pros and cons of centralized control have already been described in the star topology. The ring is capable of the highest data rates, but if a single link is broken the entire ring is disabled. The bus also has this problem, but to a lesser extent in that only the stations downstream of the break will be cut-off from communications with those which are upstream.

1.4 Transmission Media

There are three prevalent types of transmission media in use for local networks today. They are twisted pair wire, coaxial cable, and fiber optic cable. Each has unique attributes which make it more suitable for

certain applications. These are explained more fully in the following paragraphs. It should be noted that if any terms such as those dealing with multiplexing and modulation techniques are not understood, explainations exist in Tanenbaum [2], Chorafas [3] & [4], and Stallings [1].

Twisted pair wire is the most common medium and is used for both analog and digital data. It consists of two insulated wires arranged in a spiral pattern. Under analog conditions, amplifiers are required every 5 to 6 kilometers (km), while digital transmission necessitates the use of repeaters every 2 to 8 km. One of the most common use for twisted pair is for analog voice transmission using Frequency Division Multiplexing (FDM) with up to 24 channels. When transmitting a digital signal a modem is needed. It possible with a modem to achieve speeds of up to 9600 bps when using Phase Shift Keying (PSK). A good illustrative example of one of these systems is Bell's T1 Carrier which is presented in detail in Tanenbaum [2]. Twisted pair is commonly used for point-to-point, but can also be used for multipoint configurations, however with fewer stations and lower performance than coaxial cable. Its geographical scope can easily cover up to 15 km in several buildings. Noise immunity can be achieved through the use of proper shielding and different

twist lengths of the cables in the bundle. Immunity is best when the wave length is much greater than the twist length. Twisted pair can have better noise immunity than coaxial cable at lower frequencies, but performance falls off above 10 to 100Khz. Lastly, it is the cheapest medium of the three, but installation costs approach that of the other two.

The most veratile of the transmission media for LAN's is coaxial cable. It consists of two conductors - one in the middle of the other. Two types are common: 50 ohms which is used only for digital transmission of up to 10 Mbps (baseband), and 75 ohms which is CATV technology allowing either analog (up to 400Mhz and many channels using FDM) or digital (requiring modulation (ASK, FSK, PSK) and capable of data rates up to 20Mps) transmission. Coax can be used for both point-to-point and multipoint systems. Baseband 50 ohm cable can support hundreds of stations per segment linked by repeaters. Broadband 75 ohm, on the other hand, can handle thousands of stations providing data rates are kept below 50Mbps. The geographical scope of baseband is more limited than broadband (a few km vs. 10's of km) due to the fact that most of the energy in a digital signal lies in low frequencies where most noise also lies. An analog signal

can be placed on a high frequency carrier. In a very high speed system geographic scope is limited to 1km. As previously mentioned, noise of coax immunity is superior to twisted pair at higher frequencies but in general immunity is application dependent. Finally, the installed cost of coax falls between twisted pair and fiber optics.

The newest of the transmission media is fiber optic cable which is a thin, flexible, medium capable of conducting an optical ray. The source of this optical ray can be either a Light Emitting Diode (LED) or an Injection Laser Diode (ILD). The ILD is more efficient and can sustain greater data rates than the LED but is more expensive. The receiving end uses either a PIN (intrinsic layer between the P and N layers) diode or an Avalanche Photo Diode (APD). They are both basically photon counters. The PIN is less expensive and less sensitive. For modulation of digital signals a form of ASK (Amplitude Shift Keying) known as Intensity modulation is employed. Network connectivity in fiber optic systems is generally point-to-point. Multipoint, howerver, while more expensive, could in principle handle more stations than other media due to lower attenuation and greater bandwidth potential. It is possible to have single segments of up to 6 to 8 km before the use of a repeater is required. Noise immunity is almost perfect because fiber optic cable is

unaffected by electromagnetic interference. Although fiber optic cable is currently the most expensive per foot, costs are expected to drop in the future, and installation is presently cheaper.

The above are the three most common transmission media used in LAN's today and most likely the LAN's of the near future. It is important to note that other media do exist, such as the air itself for radio and infrared links, but these are unlikely to be as important in the factory enviornment for a variety of reasons. The types of topologies which lend themselves to the different transmission media is generally dependent on connectivity and is presented by Stallings [1] in the following table.

MEDIUM	TOPOLOGY			
	Bus	Tree	Ring	Star
Twisted Pair	X		X	X
Baseband Coaxial	X		X	
Broadband Coaxial	X	X		
Optical Fiber			X	

1.5 Baseband vs. Broadband

At this point it is appropiate to mention a few facts about baseband and broadband signaling in respect to local area networks. Baseband refers to a single channel method of using a medium. Only one line of commumication exists

on the network between all devices. Baseband will range between 0 and 10 Mbps, but the 1 to 2.5 Mbps range is more typical. Quite often, baseband is used for sending digital signals. Broadband on the otherhand transmits analog signals and operates at 0 to 400 MHz, Due to noise problems broadband is generally limited in LAN's to under 10 Mhz. Since broadband uses analog signaling and has a wide bandwidth, frequencies can be subdivided into carriers, enabling many different channels to be present on a single cable. This involves frequency division mutliplexing (FDM) where the signals are placed on a certain carrier frequency and then modulated by some technique. Other forms of multiplexing exist such as time division multiplexing (TDM) which is used in the previously mentioned Bell T1 channel. For more information on baseband and broadband with respect to LAN's see Chorafas [3] and Stallings [1].

1.6 Communication Switching Techniques

There are three accepted methods of switching used in LAN's. Two of these are commonly implemented in real applications (Circuit Switching and Packet Switching) while the third (Message Switching) is virtually never

used. All Three methods are described in this section with emphasis placed on the first two methods.

In Circuit Switching a dedicated path through nodes of the network is established between two end stations for the duration of the communication session between them. This is accomplished through three phases: 1) the circuit is set up after a request is sent and acknowledged. Routing information is used to determine the best available path. 2) data is transferred, typically in full duplex, over the circuit between the two end stations. 3) the circuit is deallocated when both stations are completely finished transmitting. It is apparent that this can be inefficient because channel capacity is dedicated even when transmission is temporarily suspended between the two stations. The channel is always there for the stations until deallocation.

Message Switching does not use a dedicated circuit. It simply attaches the destination address to the message and sends it out onto the network where it is passed from node to node until arriving at the desired receiving station. Each node receives the entire message, temporarily stores it, then forwards it to the next node along the route. This method shares with packet switching many of the same advantages over circuit switching. These

advantages will be presented when Packet Switching is discussed. Message Switching's disadvantages include the fact that it is not suitable for either real time or interactive traffic and it is unable to provide voice communication.

Packet Switching is similiar to Message Switching except messages are broken into fixed-length packets and then sent, one at a time, over the network. There are two methods of Packet Switching available. The first is datagram or connectionless service. In this method each packet is treated independently and is possibly routed differently necessitating numbered packets to insure correct resequencing should they arrive out of order. The second method of Packet Switching is virtual circuit or connected service. In this method a logical path is first set up between the stations as in circuit switching but it is not dedicated, enabling numerous such virtual circuits to exist simultaneously. Each node on the established route knows where to direct the packets so there are no routing decisions to be made after the initial route is established. Virtual circuit service may provide sequencing, error control, and flow control. This is in contrast with datagram which has no call up phase, and is more flexible and reliable.

There are quite a few advantages shared by Message Switching and Packet Switching (over Circuit Switching). Some of the more important ones are given here. Line efficiency is greater since channels can be shared rather than dedicated. Simultaneous availibility of sender and receiver is not required do to buffering at nodes. Heavy traffic causes blocked calls in Circuit Switching but only delays in delivery in Packet (and Message) Switching. Message Switching allows easy broadcast to many stations simultaneously and can establish priorities for messages. Error control and recovery procedures on a message basis can be built into the network. Messages sent to inoperative terminals may be intercepted and either stored or rerouted to other terminals. These advantages contribute to the fact that Packet Switching is the dominate choice for LAN's. Message Switching offers the same above advantages but is slower and therefore less desirable.

Some important concepts may be concluded from the above discussion. For light, intermittant loads, Circuit Switching is the most cost effective. The public telephone system, although not a LAN, can be used via dial-up lines. For heavy sustained loads a leased Circuit Switched line is most cost effective. Packet Switching (efficient line utilization) is a good choice when there

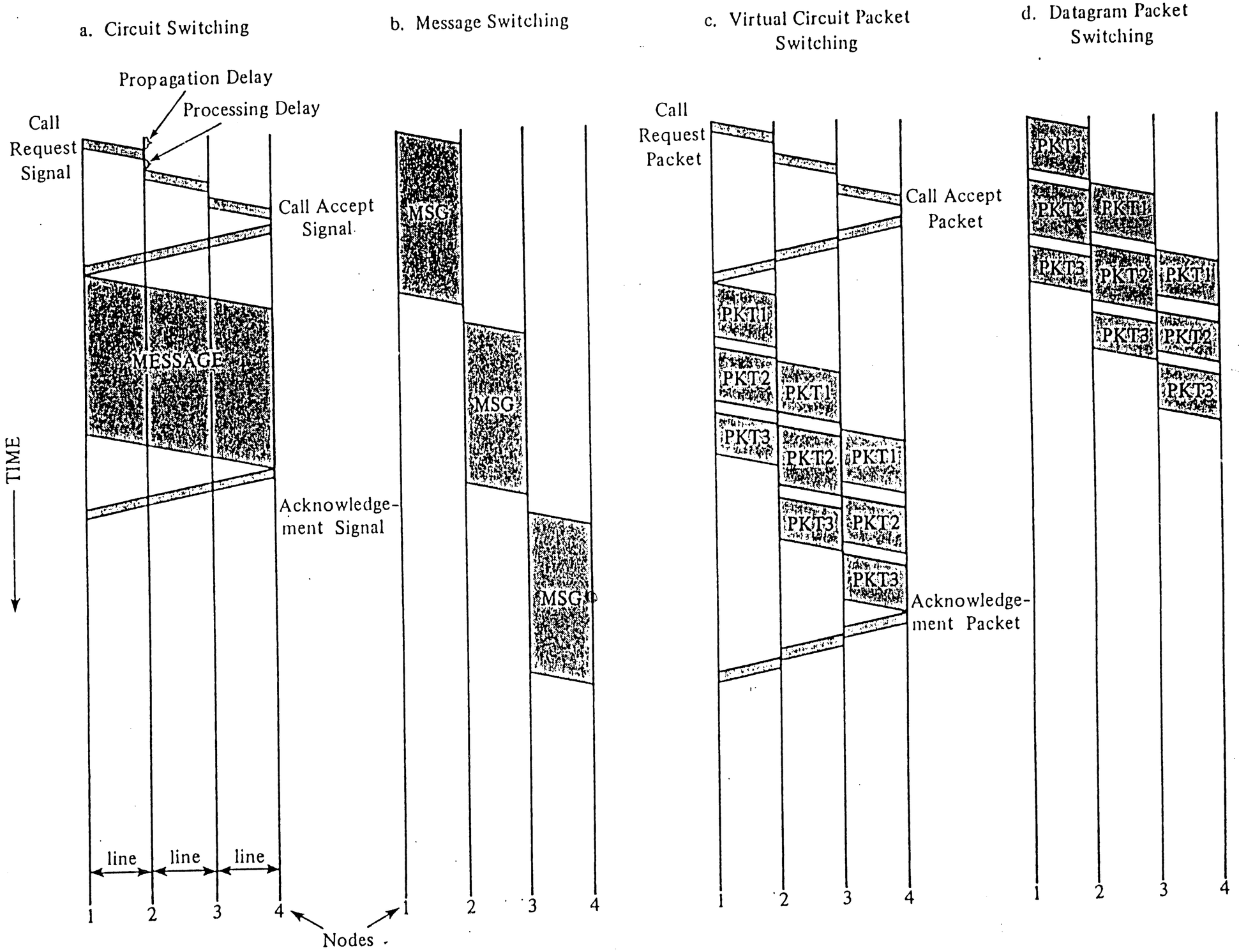

a. Circuit Switching
b. Message Switching
c. Virtual Circuit Packet Switching
d. Datagram Packet Switching
Propagation Delay
Processing Delay
Call Request Signal
Call Accept Signal
MESSAGE
Acknowledge-ment Signal
TIME
MSG
MSG
MSG
Call Request Packet
Call Accept Packet
PKT1
PKT2
PKT3
Acknowledge-ment Packet
line
line
line
1
2
3
4
Nodes

Figure 1.2

is a collection of devices that must exchange a moderate to heavy amount of data (typical LAN description). Datagram Packet Switching is good for short messages and provides a high degree of flexibility. Virtual circuit Packet Switching is good for longer exchanges and for its attribute of relieving intermediate stations of routing burden.

1.7 Classes of Local Area Networks

A description of LAN basic architecture has been presented. It is also helpful to break LAN's down into classes before presenting more of the basic concepts of LAN's. Stallings [1] divides LAN's into three classes: Local Networks, High-Speed Local Networks, and Computerized Branch Exchanges. Each of these is elaborated upon in the following paragraphs.

The Local Network is the most common class and is generally referred to interchangably with the idea of a general purpose LAN. It typically supports mini's, mainframes, terminals and other peripherals by carrying data, voice, video, and graphics. Local Networks commonly have a bus or tree topology, connected by coaxial cable or twisted pair wire with data rates from 1 to 20 Mbps. The

IEEE 802 Committee provides standards for this class of LAN. The Local Network is probably the most prevelent class due to the wide variety of devices and traffic types it supports at a relatively low cost.

High-Speed Local Networks (HSLN), as a class, are designed to provide high end-to-end throughput between expensive, high-speed devices such as mainframes and mass storage devices, usually within a computer room. They are commonly implemented on a bus topology using CATV coaxial cable with data rates up to 50Mbps. Both the distance and number of devices is limited. Due to their usual high price they are not practical for mini's, micro's, and inexpensive peripherals. HSLN's are almost exclusively used for file and bulk transfer, automatic backup, and load leveling. Standards are provided by the ANSI (American National Standard Intitute) in their ANS X3T9.5 Committee document.

Computerized Branch Exchange (CBX) (the third class) is a digital on-premise PBX designed to handle both voice and data. It is typically a star or hierarchical star configuration. It sometimes uses twisted pair wire to connect end points to the central switch, but also uses high-speed trunks of coaxial cable or fiber optic to connect satelite switching units to a central switching unit. CBX's are well suited to voice traffic and both

terminal-to-host and terminal-to-terminal data traffic. Circuit Switching is used so data rates to individual end points are typically low, but bandwidth is guaranteed and there is essentially no network delay once a connection has been made.

So you can see there is a choice in the class of LAN which one implements. Once the class is choosen there is yet another group of choices to be made within that class, at each layer of the architecture. With all these choices to be made it is apparent that a methodolgy is needed to help in the decision process. This is the topic of a later chapter.

1.8 Protocols

Protocol is one of the most important concepts of communications networks. A protocol contains syntax (data format and signal levels); semantics (control information for coordination and error handling); and timing (for speed matching and sequencing).[3] There is a protocol for each architectural layer of any communications network. Protocols usually present themselves in the form of headers attached to the front of the message (and possibly

3. Stallings, pg. 37

trailers attached to the end) at each layer as we descend the hierarchy of the sending station. Protocols are examined and stripped off as the message ascends the layers of the receiver. Some of the more important and common protocols are presented and explained in this section.

The protocols for the data link layer are concerned with the transmission of frames of data between two adjacent stations. Their fundemental requirements include flow control and error control. Their functions can include datagram or virtual circuit service, multiplexing techniques, and multicast (broadcast) capabilities. Probably the most popular data link protocol is High-level Data Link Control (HDLC), which has most of the capabilties mentioned above. If the reader is interested in details of HDLC discussions can be found in Chorafas [4] and Tanenbaum [2].

The concept of medium access control is extremely important to such areas of LAN concern as performance and design. It is, as the name implies, the method by which a station gains control of the network medium. Medium access control is topology dependent. The following subsections describe medium access control for the two main LAN toplogies.

1.8.1 Medium Access Control for Buses

The most popular method of medium access control for the bus configuration in the office enviornment is Carrier Sense Mutiple Access with Collision Detection (CSMA/CD) This popularity is due to its adoption by Ethernet and TOP. Its most attractive feature is its simplicity. There is some similaruty to the approach used on amature or C.B. radio. The basic rules dictate that a station listen to the medium prior to transmitting. If the line is free it can begin transmitting immediately, otherwise it must wait. If another station also transmits, either simultaneously or before the message propagates to it, a collision will occurr. This is detected by having the transmitting stations listen while they are sending data. If a collision does occur then all transmitting stations stop sending data and then output a jamming signal so that the collision occurrance is made known throughout the network. Then a backoff algorithim (usually exponential) is used so that each station waits a different amount of time before attempting to retransmit. They continue to do this until successful. Each time they are unsuccessful the algorithim produces a longer wait period. Because packets must travel the length of the bus they must be greater than twice the length of the longest propagation delay to

ensure collision detection (if the two station located farthest apart transmit almost simulataneously). This minimum packet length can cause wasted bandwidth if the message is shorter than the minimum, but the greatest disadvantage of CSMA/CD is its poor performance under heavy loads as contention for the medium causes excessive collisions.

The alternative to CSMA/CD is the token bus method of medium access control. This is the chosen standard for MAP. The bus is logically a ring and a token is passed around it according to a predefined order. When a station gets a free token it can set it to busy and attach a message to it or it can pass it on to the next station. It can keep control of the token as long as it likes. Functions required for this method to work are: 1) a ring initialization process which is a cooperative decentralized algorithem to assign position, 2) a process for adding stations to the ring which allows the periodic self-insertion of non-participating stations onto the ring, 3) a deletion from the ring process which enables stations to delete themselves from the ring by splicing their successor and predaccessor logical together, 4) a recovery mechinism for any of the possible errors (broken ring, no station thinks it is their turn, two or more

stations think it is their turn, and duplicate addresses). These functions and associated rules obviously make the token bus more complicated but it is capable of greater throughput than CSMA/CD under any conditions.

1.8.2 Medium Access for Rings

The ring topology makes it possible for three different methods of medium access control. They are register insertion, slotted ring, and token ring. Each of these is explained in this section.

The register insertion method of medium access control for rings is not implemented very often but helps present some of the factors to be taken into consideration with an access method for rings. The underlying concept here involves the use of a shift register at each node (size equal to the maximum frame length) to temporarilly store and check the address of the frames which circulate past it before reinserting them onto the ring. There is also the need for a buffer for frames which are produced by that node. The node can either keep messages addressed to it and send an acknowledgement of receipt to the sender, or make a copy of the message and place the original back on the ring for the sender to remove, thus also providing a means of acknowledgement. To output a

frame the node simply waits until the line is idle and then shifts the message out onto the ring while simultaneously shifting in any frames which arrive after it begins transmitting. The register insertion method obviously utilizes bandwidth well. In addition it allows variable frame lengths (as long as they are shorter than the shift register). This helps improve throughput since messgages which are shorter than the maximum frame length don't have to be stuffed with dummy bits to achieve some minimum frame length. Multiple frames may be permitted on the ring. Disadvantages include the fact that each message, regardless of destination, must be completely shifted in and its address must be checked. Also, if a messages address is in error, it could remain on the ring indefinatly if provision is not made for removal.

The slotted ring approach dictates that a number of fixed length slots continuously circulate around the ring carrying a lead bit to indicate whether a slot is empty or full. The rules which apply to this method are summarized as follows. All stations must be initially empty. A station wishing to transmit data must break it up into fixed length frames equal to the slot sizes and then wait for an empty slot to arrive. It can then set the lead bit to indicate that the slot is full and insert the frame into the slot. A station cannot transmit another frame

until the last one has returned. The slot also contains two response bits which can be set on the fly by the addressed station to indicate either acceptance, rejection, or busy. The source marks that slot empty and then must wait for the next empty slot to retransmit the previous frame or to transmit a new one. The advantages of this method include its simplicity, its fairness, and improved reliability due to less interaction at each node. The disadvantages are the waste of bandwidth because each frame contains more control bits than data bits (see Stallings [1] for details of frame makeup) and bandwidth loss when only one node is transmitting but must wait for more than one complete revolution of a slot around the ring before its next transmission.

Lastly, the token ring, which was recently adopted by IBM for personnal computer LAN's, seems to be the emerging choice of medium access control for rings. It is much like the token bus method except that a token is passed around a physical ring rather then a logical one. The token provides access to the ring and is marked either free or busy. If a station desires to transmit a frame it waits for the free token and then marks it busy and attaches its frame. The frame then circulates around the entire ring and is finally purged by the transmitter who can either

immediately attach another frame or set the token to free. The advantages of this method are that it is fair, it can provide priority to certain stations, and can provide guaranteed bandwidth services. The biggest disadvantage is the requirements of token maintenance (see token bus). There are two approaches to token maintenance which may be used. They are covered below.

The first approach to token maintenance is the use of decentralized control. There are two timers, a long no-token timer (NTT) and a shorter valid frame timer (VFT). If a station has a frame to transmit and has not seen a token for NTT it assumes the token is lost, purges the ring, and issues a new token. It also keeps track of the amount of time since the last valid frame or token and if it exceeds VFT, it to purges the ring and issues a new token.[4]

The second approach to token maintenance is through the use of centralized monitoring of the token's vital statistics. Here a station is designated as the active token monitor and purges the ring if it does not see the token before the greatest ring propagation time. It also checks to see if there is a busy token which does not have an attached message and therefore was not freed. It will

4. Stallings, pg. 132

set the token to free so normal operation can resume. Finally, there can also be provision for making another station the token monitor in the case of failure of the primary station.

1.9 The Network Interface Unit

Before this chapter on fundamentals can be conluded and the discussions on broader LAN aspects can begin, one last basic concept must be presented. This is the concept of the actual network interfacing device known commonly as the Network Interface Unit (NIU). It is defined as an intelligent device that implements the local network's protocols and provides an interface capability for attached devices. NIU's collectively control the access to and communications across the network.[5] The functions which are performed by the NIU include: 1) the acceptance of data from attached devices, 2) buffering data until medium access is achieved, 3) transmitting data in addressed packets, 4) scanning each packet on the medium for its own address, 5) reading packets into buffers, and 6) transmitting data to the attached device at the proper rate. In other words, the NIU handles all the lower level

5. Ibid pg. 203

network needs for any device wishing to communicate on the network.

The basic architecture of the NIU can be broken down as follows. The physical link is generally a predefined standard such as RS 232-C. Internally it is usally a microprocessor based device which acts as a communications controller to provide data transmission service to one or more attached devices. It transforms the protocol and data rate of the subscriber to that of the local network.

There are three possible uses for the NIU/Device interface. The first and most common is as an implementaion for layers one and two of the ISO model. Here each NIU is attached to the medium and they all communicate with each other to implement the LAN. Another use is for the NIU to function as a gateway to connect two systems that use different protocols. Usually layers one thru three are implemented (converted) by the gateways to a common protocol (i.e., X.25) and routed to the destination with the upper layers intact. Finally, NIU's can also function as front-end network processors (FNP's) which provide communication management services to an attached information processor. In contrast to gateways whcih convert protocols, the FNP replaces protocols that might be found in attached devices. Most logically the FNP

takes care of the lower four layers.

1.10 Summary

Some of the fundamental concepts of LAN's should now be apparent to the reader. Due to limited space and the thrust of later parts of this thesis not all fundamental concepts of local area networks have been presented. Rather, fundamentals have been covered that are important to the next chapter, which discusses some of the more far reaching concepts of LAN's, as well as those important to all the remaining chapters. The reader should now be able to continue without extensive reference to other sources.

CHAPTER TWO

LOCAL AREA NETWORK ISSUES

2.0 INTRODUCTION

Before examining features of local area networks which distinguish factory LAN needs from office environment needs some more important LAN issues need to be discussed. LAN performance issues, internetworking, and important design considerations are the major topic of this chapter. Coverage of each major topic is limited to affects on Packet Switched networks.

2.1 Local Network Performance

The key performance related characteristics of LAN's are the fact that there is a shared access medium, requiring a medium access control protocol, and the fact that packet switching is used. Five major parameters or measures of performance and their common mnemonic follow:

1. D: Delay that occurs between the time a packet or frame

is ready for transmission from a node, and the completion of a successful transmission.

2. S: Throughput of the local network; the total data rate being transmitted between nodes.

3. U: Utilization of the network medium; the fraction of total capacity being used.

4. G: Offered load to the local network; the total rate of data being presented to the network for transmission.

5. I: Input load; the rate of data generated by individual stations attached to the local network.

The first three are measures of performance and the last two are parameters which can be applied to produce the measures. The results are often presented in graphical form for analysis. The most widely used is the amount of throughput for varying offered loads (S vs. G).

The affects of propagation delay and transmission rate can have a strong bearing on performance. In fact, the bandwidth multiplied by the distance of the communications path is the single most important factor in determining network performance. This is due to a parameter which can be denoted "a" which is the ratio of the length of the medium and the typical frame length; "a"

puts an upper bound on utilization because it is inversely related. In order to make "a" as low as possible it is desirable to increase frame size as much as possible without wasting bandwidth due to unnecessarily large frames.

Factors which affect performance independent of attached devices are as follows. First there are factors which determine the parameter "a": bandwidth, propagation delay, and frame length discussed above. Next are the protocols selected for the various levels including: transmission medium, data link protocol, and, most importantly, the medium access control discussed below. Finally, there are two independent factors which the analyst can vary to determine maximum performance: offered load, and the number of attached stations.

2.1.1 Performance of Protocols

In order to achieve maximum performance the analyst must establish bounds of performance and then apply them to the various LAN protocols. Three regions of operation can be established based on the magnitude of the offered load: 1) low delay where capacity is more than adequate to handle offered load, 2) high delay in which the network becomes a bottleneck with relatively more time spent

controlling access to the network and less time spent on actual data transmission, 3) unbounded delay where the offered load exceeds total capacity of the system. Region Three is clearly to be avoided, and Region Two is generally to be avoided as well because it implies an inefficient use of the network. Ideally, the designer should try to require the network to operate below the boundary between the first and second regions.

It is useful to apply some of this knowledge in comparing protocols presented in the first chapter of this thesis. First token passing and CSMA/CD will be compared for both the token ring and the token bus. Next different forms of contention protocols will be contrasted with each other. Finally, performance characteristics for three types of ring access protocols will be compared.

2.1.1.1 Performance of Contention vs. Token Passing

When comparing the performances of token passing and CSMA/CD, certain conclusions may be drawn: 1) for a given set of parameters, the smaller the mean frame length, the greater the difference in the maximum delay between token passing and CSMA/CD; this reflects the strong dependence of CSMA/CD on the parameter "a". 2) token passing on the ring topology is the least sensitive to work load, 3)

CSMA/CD offers the shortest delay under light loads, while it is the most sensitive to work load under heavy load conditions.

2.1.1.2 Performance of Different Contention Protocols

Prevelent classes of contention protocols are the Aloha method and CSMA/CD. The Aloha method is made up of the pure Aloha and the slotted Aloha types. The CSMA/CD class which can be broken into persistent, nonpersistent, and slotted CSMA/CD. For detailed explanations of these five types of contention protocols see Tanenbaum [2] or Stallings [1]. In general all schemes of CSMA/CD have dramatically improved performance over Aloha methods. Also, in general, the more sophisticated the CSMA/CD technique, the better it will perform.

2.1.1.3 Performance of Different Ring Protocols

In the previous chapter we covered three common types of ring access protocols; register insertion, slotted ring, and token ring. It is not an easy, clear cut matter to compare them because the results depend critically on a number of parameters unique to each protocol. However, in general it can be said that token ring has superior delay characteristics to slotted ring because the ratio of

overhead bits to data bits in the small slots of a slotted ring is very high and the time needed to pass empty slots around the ring (to guarantee fair bandwidth) is great. Several positive performance characteristics of slotted rings are the fact that expected delay for a message is proportional to length (shorter packets get better performance than longer ones) and overall mean delay is independent of packet length distribution. Finally, register insertion seems to have the best utilization since more than one message can be transmitted simultaneously, but propagation time around the ring can be great (due to the reading and buffering of messages at every station). Also, propagation time is not constant because it is traffic dependent.

The work of Stuck and Arthurs [5] contains a great deal more information about performance of computer networks as well as discussions on modeling and simulation of networks. Stallings [1] also contains an indepth presentation of LAN performance.

2.2 Internetworking

It is often desirable to connect several smaller LAN's into a larger one. In this case the original smaller

LAN's are then known as subnetworks or simply segments. One approach, known as homogeneous internetworking, is the internetworking of several similar subnetwork segments. The other possibility, hybrid internetworked LAN's, is the connection of dissimilar LAN segments to form a larger network. Both approaches are covered below. Then principles of internetworking facilities are covered in detail

2.2.1 Homogeneous Internetworking

The simplest type of internetworking is the homogeneous local network in which two or more similar LAN segments are used. Such networks exhibit the same interface to attached devices and generally use the same internal protocol for medium access. The device which is used to connect the segments is called a bridge. It usually consists of two Network Interface Units linked together. A bridge between two networks, A and B, should perform the following functions:

1. Read all frames transmitted on A, and accept those addressed to B.

2. Using the medium access protocol for B, retransmit the frames onto B.

3. Do the same for B-to-A traffic.

When designing a bridge, there are several considerations. The bridge must not change content or format of the frames received. Also the bridge should not encapsulate frames with a header, but it can be implemented using another protocol. The bridge should contain enough buffer space to meet peak demands when frames arrive faster than they can be retransmitted. Addressing and routing information for connecting networks and any cascaded networks are needed. A bridge may connect more than two networks.

There are numerous reasons for using bridges. They improve reliability because the network can be divided into segments. If a problem occurs in one segment it will not bring the entire network down. Performance can be enhanced by breaking the network into subnetworks in such a way that the majority of traffic is intrasegment. In this way it behaves as a group of smaller networks with fewer stations per network. As shown earlier, the fewer the stations the better the performance. Security can be increased. This will be explained later in this chapter. Convenience comes into play if you have two networks which may be difficult to link together with the present medium. Using bridges they can be linked with a different medium.

A good example is two buildings separated by a highway which could use a microwave link with bridges to connect two coaxial based LAN's. Finally, geographic scope can be increased by using bridges to connect widely separated LAN's.

2.2.2 Hybrid Internetworking

Hybrid internetworking involves the connection of dissimilar classes of LAN's. It is possible and often advantageous to connect several different classes of local networks (LAN, HSLN and CBX) into one internetwork through the use of a bridge or a gateway.[1]

There are some good examples that illustrate the advantages of hybrid local networks. One strategy is to connect all of the telephones, low speed terminals, and microcomputer to a CBX. This takes advantage of the low attachment cost for devices that do not have high data rate requirements. Then minicomputers and high-speed peripherals could be connected to a LAN. Finally, mainframes and mass storage devices could be attached to a HSLN. To bring all these subnetworks together, the CBX

1. Stallings, pg. 295.

could attach directly to the LAN via one or more NIU ports. Devices could request an NIU connection and then access the LAN. For interactive traffic between the LAN and the HSLN it would be best to connect the LAN to the mainframe front end processor since it is designed for this type of traffic. Finally, for file transfer between the LAN and HSLN a direct NIU-to-NIU connection could be used. This is just one example of how hybrid internetworking could be used to implement a large and powerful LAN at the lowest possible cost.[2]

2.2.3 Principles of Internetworking Facilities

There are a few requirements which must be observed when designing an internetworking facility (four types will be presented below) including the obvious requirement to provide a link between the subnetworks. At the very least provision must be made for the bottom two layers of the OSI model. Routing and delivery of data between processes on different subnetworks must be available. There should also be provisions for accounting services which maintain status information and keep track of the use of the various networks and gateways. The

2. Stallings, pg. 296.

internetworking facility must provide all of the above services in such a way that there is no requirement to make modifications of architecture for any attached subnetworks. This means that the internetworking facility design must accommodate the following possible differences among subnetworks: addressing schemes, maximum packet sizes, network interfaces, time-outs, error recovery, status reporting, routing techniques, access control, and Packet Switching service (datagram vs. virtual circuit). With all of these requirements it is obvious that a gateway can be a complicated and costly device.

The key issue in designing a gateways is the architectural approach. Factors determining architecture are the nature of the interface and the the, nature of the transmission medium.

The nature of the interface depends on whether it is at the DCE (Data Communication Equipment) level or the DTE (Data Terminal Equipment) level. Tanenbaum [2] gives detailed explanations of both cases. If the interface is at the DCE level it implies that the network has a common network layer interface (i.e., X.25). This means there is a standardized format for all packets entering and leaving each subnetwork. If implemented correctly, the gateway is transparent and no changes need be made to host software.

Alternatively, if the interface is at the DTE level, there will have to be some form of protocol translation. This is usually implemented in software and will clearly increase the complexity of the gateway design.

The nature of the transmission service can be either end-to-end or network by network. In end-to-end service it is assumed that all networks offer at least a partially reliable (some packets may be lost or out of order, but some do get through) datagram service. Transmission across multiple networks requires a common end-to-end protocol, providing reliable end-to-end service. If, on the other hand, the network by network approach is taken there must be a reliable service within each network. The networks are then strung together and interfaced with some type of protocol package (see below).

From the above discussion a table can be constructed to summarize the possible architectural approaches:

	DCE Level	DTE Level
End-to-end	Bridge	Internet protocol
Network by network	X.75	Protocol translator

The simple bridge was discussed earlier and warrants no further attention. Internet protocol (IP) is a layer which fits between the third and fourth layers of the ISO model and provides datagram service between hosts. MAP

calls for such a sublayer in its Network Layer. The IP layer receives packets and encapsulates them with a header, specifying a global network address, before sending them out onto the LAN. The protocol translator is a special purpose software package and is beyond the scope of this paper. Lastly, the X.75 standard is designed as an extension to X.25 and specifies a protocol for exchange of packets between networks to allow a series of internetwork X.25 virtual circuits to be strung together. It is transparent to hosts on different networks. Stallings [1] provides the following table to compare the features of IP and X.75:

Internet protocol	X.75
DTE gateway	DCE gateway
Datagram service	Virtual circuit service
Gateway must know IP and two network access interfaces	Gateway must maintain state information about all virtual circuits
Adaptive routing	Fixed routing
All hosts must have IP layer and may need common layer 4	All networks must be X.25

2.3 Local Network Design Issues

In this section three major design issues will be

discussed. The first is Network Control. It is the group of operations which keep the network running smoothly. The next design issue is the combination of reliability, availability, and survivability, all of which are measures of system functionality. The last design issue is network security or the protection of network resources.

2.3.1 Network Control

Network Control is the most important and complex issue of network design. The manager of the network must be able to configure the network, monitor its status, react to failures or overloads, and plan intelligently for future growth.[3]

Network management is a broad concept. It encompasses many tasks. The more vital of these tasks are listed below:

1. Operations Management: responsible for the day-to-day operation of the network including monitoring status of all aspects of the network

2. Administration: deals with managing the use of the network including system generation, assigning user

3. Stallings, pg. 319.

passwords, managing resources, file access, and billing

3. Maintenance: assures that the network continues to work properly. This involves detecting and reporting problems, isolating to determine cause, and resolving problems.

4. Configuration Management: effective management of the system life cycle and providing for an evolving configuration.

5. Documentation/training function: responsible for education functions as well as development and maintenance of documentation.

6. Data Base Management: provides the capability for a network managed data base.

7. Planning: responsible for on-going requirements analysis and configuration change planning.

The Network Control Center (NCC) can support the first three items above. As was done with LAN performance, the NCC will only be discussed in terms of packet switched LAN's. The NCC typically attaches to the network via an NIU and consists of a dedicated microcomputer. NCC functions involve observation, active control, or a

combination of the two. These functions fall into categories of configuration, monitoring, and fault isolation.

The configuration function sets up either a connectionless (datagram) or connected (virtual circuit) session between NIU's. It is also in charge of directory management which maintains name/address tables so users can request stations by name. The NCC can control the operation of the NIU's to implement features such as start/stop and parameter set-up for simple security systems.

The monitoring function can be broken down further into more primitive functions. The first, and most important, is performance monitoring, involving gathering statistics about network traffic and timing. Performance analysis is also a part of performance monitoring and consists of software for reducing and presenting the data. Synthetic traffic generation can also be used to observe the network under controlled load. There are many more important aspects of performance monitoring including simulation and model validation, location of problems, and answering questions for an array of network performance aspects. The second primitive function of the monitoring function is network status. This is the job of keeping

track of which NIU's are currently active and the connections that exist. The last primitive of monitoring is accounting. It enables the NCC to keep track of billing on a device or user basis.

The fault isolation function of the NCC is also important. The NCC can continuously monitor the network to detect faults and, to the extent possible, narrow them down to a single network component or a small group of components. The NCC to periodically poll each NIU, requesting it to return a status packet. Another approach is to have each NIU be required to periodically and automatically (without poll) emit a status packet.

The discussion in this section is related to network control. To be exact, it should be called communications network control because it is NOT computer network control. Communications network control is the capability to control the operation of a computer network. Computer network control on the other hand encompasses activities at all seven layers of the ISO model. These activities include enabling/disabling network objects (paths, virtual circuits, nodes, communication links), gathering statistics on objects, inquiring current status of objects, and running tests through the network. Although they may overlap, the responsibilities of communications and computer network control are distinct. It is possible,

at least in a homogeneous network, to merge them. But for now, it is likely the network manager will need two NCC's and two operator interfaces.[4]

2.3.2 Reliability, Availability, Survivability

There are three probabilistic measures of LAN performance. They are reliability, availability, and survivability. They help describe how the system performs under ordinary or extraordinary conditions. Each is defined below in terms from Stallings [1]. Some examples are presented in respect to different LAN components.

The probability that a system will perform its specified function for a specified time under specified conditions is called reliability. Component failure is expressed by mean time between failure. The reliability of the system depends on the reliability of its individual components plus the system organization. For example some components may be redundant, such that the failure of one component does not affect system operation. Or the system configuration may be such that the loss of a component reduces capability, but the system still functions.

Availability is the probability that a system or

4. Stallings, pg. 325.

component is available at a given time. Availability of a function or service depends on both the availability of system components and the expected load on the system. Survivability, on the other hand, is the probability that a function or service is available after a specified subset of the components or systems become unavailable.

There are two categories of components which may fail or malfunction and affecting the network reliability, availability, or survivability. The first is failure of attached devices. This is not of concern here because it only results in the loss of service provided by that device and does not affect network performance. The other category of component failure is that of any of the actual LAN components. Examples of component failure and ways of preventing this failure are discussed below.

In broadband networks there are generally a great number of devices dispersed over a large area, due to its tremendous capacity and flexibility. This means the loss of the network could be catastrophic. There are four areas in which any possible malfunction must be overcome as described in the following paragraphs.

Headends used in a broadband LAN can be: 1) a simple piece of cable joining the two sections of the main cable, known as a passive headend; this is as reliable as the

rest of the transmission medium (discussed below), 2) a frequency converter (active component) used in a midsplit system to convert the incoming signal in the lower band of frequencies to outgoing signals in the higher band. Failure of this component would disable the entire system. One solution is to keep a "hot" back up frequency converter to override the primary one in case of failure.

The transmission media would cause at least partial system failure if it were to be damaged. A back up cable could be supplied but it is almost imperative that it be located close to the primary cable, making it likely that if one is damaged so will be the other. An alternative would be to have addressable taps which can be polled to determine where the break is. Subsequently that part of the cable downstream of the break could be shut down resulting in only partial loss of the network. To make this method as effective as possible the network topology should contain many branches or it should be partitioned into many bridge connected segments.

A typical network interface unit (NIU) failure will only result in the loss of the attached device. But it is possible that an NIU logic failure could cause excessive transmission, channel jamming, transmission of distorted signals, or interference with CSMA protocols by a receiver failure. Here, addressable taps could also be used to

determine and shut down the faulty NIU. The taps could be contacted on an out of band frequency to to avoid the jammed frequency. More benign failures could be detected by having the NCC poll the NIU's or by requiring them to send status information periodically.

The network control center (NCC) has lesser availability concerns so it is reasonable to take no measures to improve its reliability. However, a "hot" back up in the same spirit as the active headend could be used. It would have to be connected via an independent NIU. It would monitor the channel and shut down the primary NCC's NIU if it detects a fault, thus taking over as primary NCC. It is also useful to have a back up NIU for each NCC in case of NIU failure.

Baseband bus networks entail fewer availability problems because they contain no active components (amplifiers or headends) except repeaters on larger networks. For repeaters, failure is less likely and it can confined to one segment. To insure this confinement, repeaters should contain enough intelligence to know not to transmit on a segment which is being jammed. Also, double cables can be used. The NIU and NCC problems are the same as in a broadband system and can be handled in the same way.

As discussed earlier, the loss of a single link in a ring network can disable the entire network. There are two possible ways of addressing this problem. The first would be to use ring wiring concentrators to make it easy to isolate the problem. Then a bypass relay could be closed to remove the problem. The impact of ring failure can be reduced by configuring the network as multiple small rings connected by bridges.

2.3.3 Network Security

Stallings [1] defines network security as "the protection of network resources against unauthorized disclosure, modification, utilization, restriction, or destruction."[5] The subject is broad and encompasses physical and administrative controls as well as automated ones. The following discussion is limited to access control, encryption, and multilevel security.

Access control is used to ensure that those only authorized have access to the system and its individual resources. This means access to and modification of particular portions of data are limited to authorized individuals and programs. Access may be controlled by user

5. Stallings, pg. 326.

or by data authentication.

Access control by user is also referred to as authentication. It is usually implemented via a password during a logon procedure. This is the only cost effective method available at this time. Because a LAN uses a multiaccess medium it is possible to listen in on the logon procedure. This can be remedied by encryption or by the diffecult process of allowing only the NIU which is addressed to read the message. The authentication process can be centralized or distributed. If centralized, the network can provide logon service which can be thought of as being associated with the NCC. If distributed, it treats the network as a transparent communication link, and the usual logon procedure is carried out by the destination host.

In data authentication, through the authentication procedure the user can be identified together with a profile that specifies permissible operations and file accesses. The operating system may enforce rules based on user profile. The data base management system, however, should control to specific portions of records. This can be done with an access matrix which cross matches the user with the data they are permitted to access.

The next area of security to be discussed is

encryption. This can be used as a countermeasure to eavesdropping achieved by tapping into the medium or programming an NIU to accept packets not addressed to it. There are many encryption schemes. Most involve the use of a cipher which is an encryption algorithm that is parameterized by a key. When encrypted text arrives it can be transformed back to the original text if the destination NIU knows the cipher and the key. If the keys are managed properly then the risk of the code being broken is low.

The last area of security to be presented is multilevel security. It is sometimes possible and also advantageous to protect resources on the bases of security levels. The requirements for multilevel security can be fully stated in two parts: 1) No read up is allowed. This means a subject can only read an object of less or equal security level. 2) No write down is permitted. This means a subject can only write into an object of greater or equal security level.

2.4 Summary

This chapter has presented three topics of local area networks. The first was performance. This is the most

important issue of LAN's. Because of this importance there should be an easy and efficient way to evaluate the performance of many different LAN designs. This can be done through the use of a computer model which can simulate a LAN's performance. Chapter five of this thesis presents a methodolgy for modeling local area networks. The topic of internetworking was presented next. It deals with linking together homogeneous and heterogeneous LAN's to form a larger, often more capable LAN. In such environments as the factory floor where some operations must take place in real time while others may not, it is necessary to internetwork several different types of LAN. More on this topic is presented in the next chapter which deals with MAP. The last topic discussed was the broad area of LAN design issues, presenting some of the many factors which should be taken into account when designing a local area network.

Chapter Three

OVERVIEW OF MAP

3.0 Introduction

Material in this chapter is based on the General Motors Manufacturing Automation Protocol Version 2.1 [6]. This chapter is a brief summation of the current definition of this evolving specification. For a complete description of MAP see the above reference.

The impetus behind the creation of the Manufacturing Automation Protocol (MAP) is to provide standards for factory local area networks. These networks are made up of computers and intelligent devices supplied by a myriad of vendors. Standardization will make it possible for any vendor specific device to communicate with ease with any other vendor specific device.

Currently and in the past, plant floor computer systems at some General Motors facilities had to allocate fifty percent of their costs to networking. This was the result of using different vendors' programmable devices

each requiring its own proprietary communications protocol and interface. MAP was developed to address this problem and to establish a uniform set of standards to be used in manufacturing facilities. Success of MAP requires that a strong effort be made to encourage vendors to adopt these standards.

The scope of the MAP project was to define standards for LAN's which can provide service to terminals, computing resources, and programmable devices within a manufacturing complex. The architecture also allows for the internetworking of multiple LAN's and for connection to Wide Area Networks (WAN's) or digital PBX's for long distance communication.

3.1 MAP Network Architecture

Because the ISO model for OSI has wide acceptance by the international community, a specific goal of MAP is to adhere to it as much as possible. This section will discuss the model and other architectural aspects of LAN's as they apply to the MAP specification. The reader can refer to Chapters One and Two of this thesis for more information on some of the basic concepts of LAN's as

applied to MAP in this Chapter.

3.1.1 MAP Topology

All devices in the plant must be able to connect to the MAP network. This means the physical cable must be accessible from every location in the plant. Because network performance decreases as the number of devices connected to it increases, it is best to break the LAN into smaller segments with fewer devices per segment. Design and performance criteria can be met when the total network is implemented as a set of subnetworks. This requires the use of bridges, gateways, and routers. Each is defined to the MAP specification in the following sections.

3.1.1.1 MAP Bridges

A bridge is a transparent device used to link segments of a single LAN. The data link protocols are generally the same for all segments. By comparison to a baseband repeater which provides transparent network expansion at the Physical Layer, the bridge provides this expansion at the Data Link Layer. A bridge can be used to extend a network beyond the design specifications for a single segment or to physically isolate the segments from

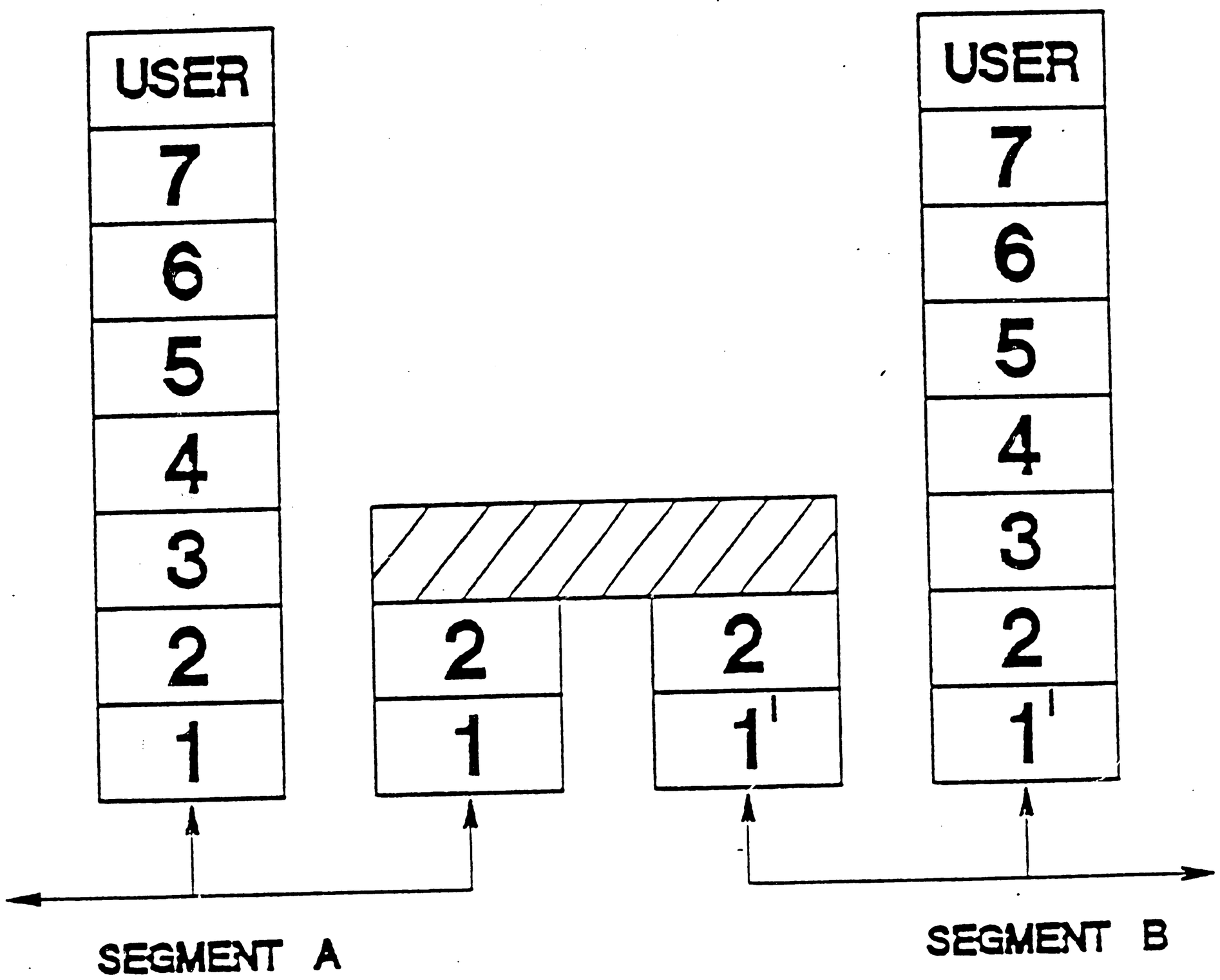


Figure 3.1

BRIDGE ARCHITECTURE

each other. The MAP representation of a bridge is shown in Figure 3.1.

Some features of bridges include: transparency, link ability of different media, capability of speed matching across itself, capability of message store and forward, provision of data link protocols with broadcast (multicast) capability, and elimination of need for an address, (but one is required for network management). Goals for bridges are different than their features but do tend to overlap. Goals include: protocol transparency, technological independence, low overhead, and high performance.

The MAP specification puts constraints on bridge design. Bridges must provide a non-routing, tree topology. This does not mean that individual segments may not be rings or buses. Bridges must have a unique address at the Data Link Layer for network management (discussed later) and they must have a datagram interface as opposed to a virtual circuit interface. Bridges may be used to connect identical network types or to couple networks with dissimilar media.

3.1.1.2 MAP Gateways

Gateways are devices which connect different network

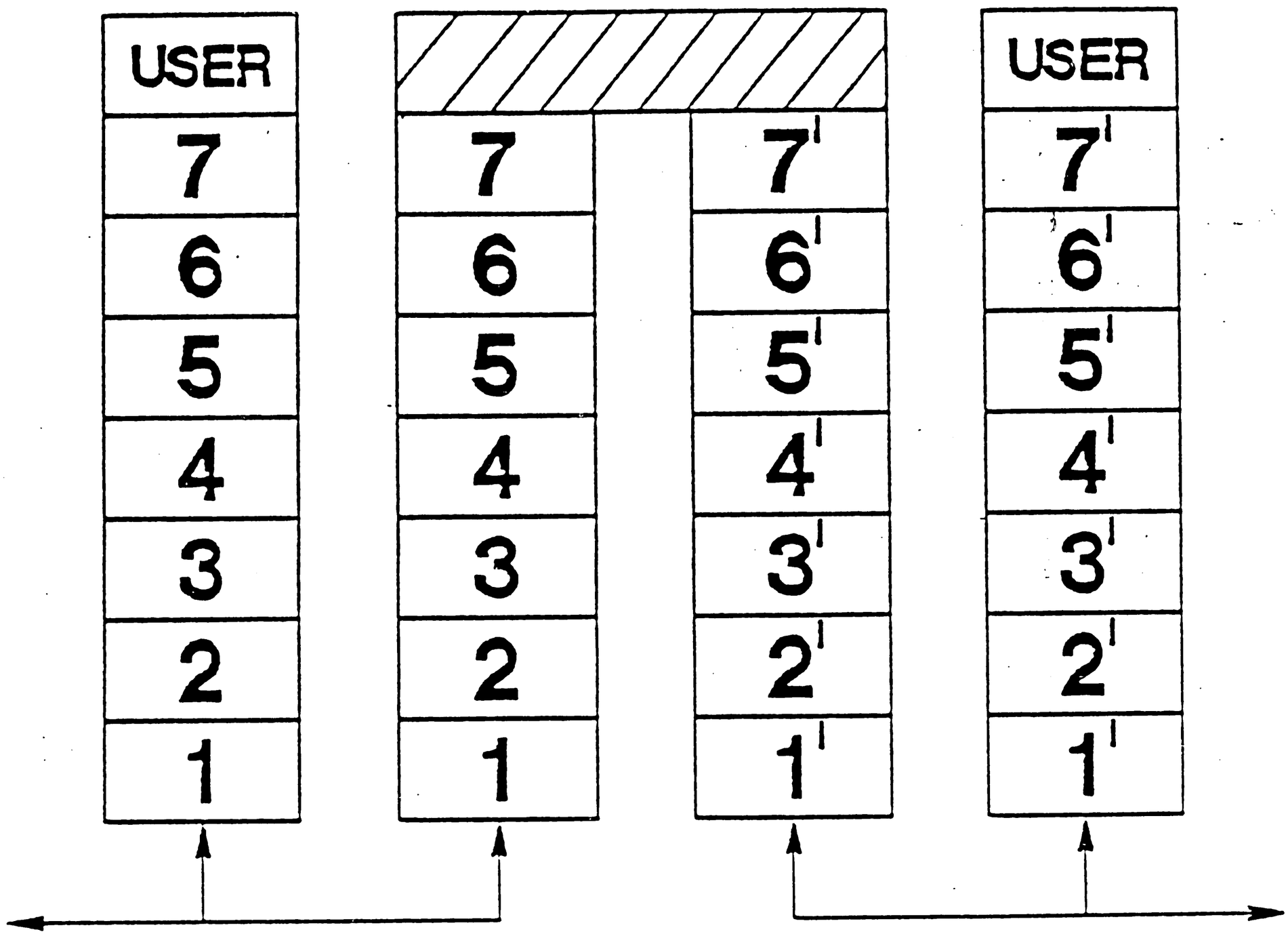


Figure 3.2

GATEWAY ARCHITECTURE

architectures by performing protocol translation. The primary difference between a bridge and a gateway is that the latter utilizes all seven layers of the OSI model whereas the bridge only uses layers one and two. A gateway can also provide connection from LAN's to longhaul networks or WAN's of any type. A MAP gateway is shown in Figure 3.2.

There are several distinctive characteristics of gateways. Unlike bridges, gateways are not transparent. Gateways do perform message store and forward, but they are also required to support flow control resolution. They must provide a virtual circuit interface as opposed to a datagram interface. Gateways are connected at the application level. They support network management for multiple networks. As mentioned above, they must perform protocol translation. Finally, since gateways connect networks with different address structures, they must have different addresses on each attached network.

3.1.1.3 MAP Routers

Routers are commonly used to connect several networks together at a common point. In this configuration the router provides path selection and alternate routing based on destination network layer addresses and status of

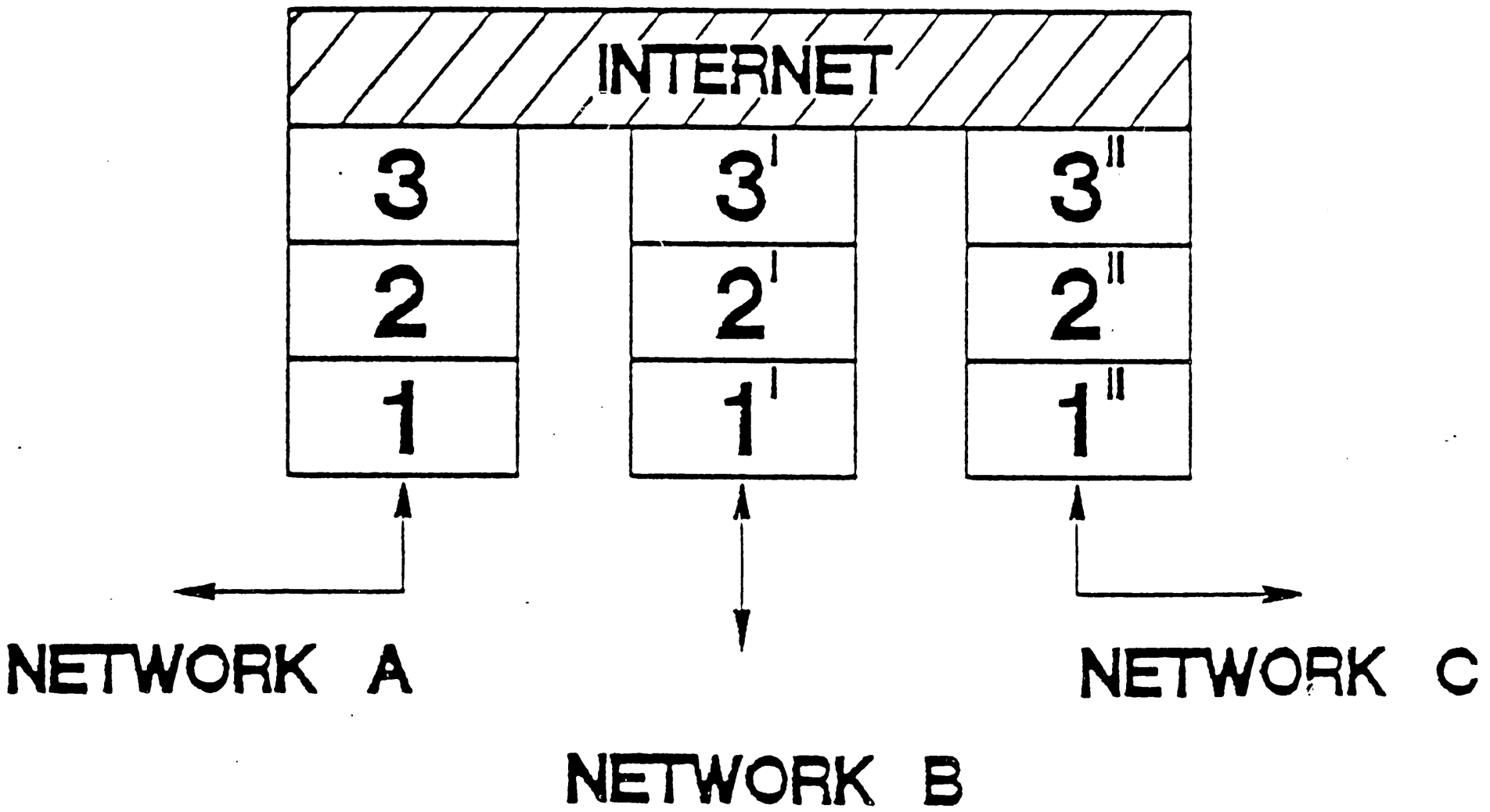


Figure 3.3

ROUTER ARCHITECTURE

connected networks. A router has one common network address for all attached networks. This requires all networks to have common address schemes. Figure 3.3 depicts the MAP definition of a router.

3.1.1.4 MAP Catanet Environment

The final concept for this topology section is what MAP refers to as the Catanet Environment. This is simply the resulting topology when interconnecting a group of networks through the use of bridges, gateways, and routers. An example is shown in Figure 3.4.

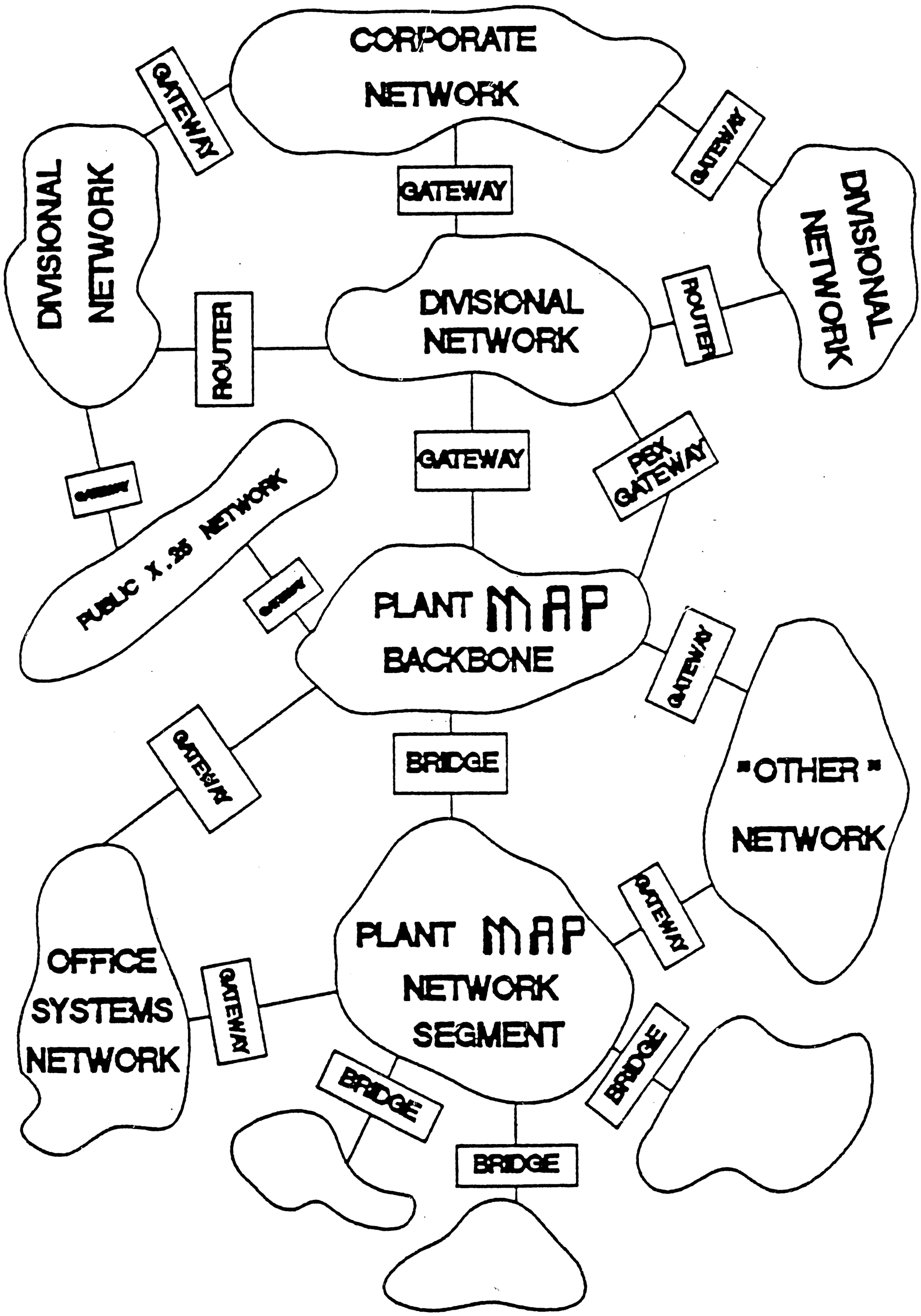
3.1.2 MAP Layer Specifications

In this description of the layer specifications of MAP, each layer's specification will be presented by first explaining the direction General Motors expects its LAN designers and vendors to take to implement that layer and then the rational for GM's choice will be covered. It is assumed the reader has a good understanding of the OSI model and each of its layers.

3.1.2.1 The Physical Layer

The direction for this layer suggests that the

Figure 3.4



EXAMPLE OF A CATANET

standard MAP network will consist of a backbone network with gateways, bridges, and routers connecting to other MAP networks and possibly non-MAP networks. The actual topology will be left to the individual plant requirements, but the bus topology is favored for the backbone itself. Broadband coaxial cable is recommended as the standard media. It should be installed and operated according to CATV industry standards. This means with a mid-split provision for two-way data flow. The mechanical and electrical specifications for interfacing to the network are detailed in the IEEE 802.4 standard for token bus broadband. For MAP the two channel 10Mbps option is required.

The rational for the above choices lies in the fact that although MAP is intended to be media independent, the initial installations will use a broadband backbone for a variety of reasons. Broadband allows multiple networks to exist on the same media simultaneously. Therefore, wiring modification will be minimized while effecting a smooth and orderly transition to MAP. Also, broadband can handle the high data rates required by LAN's in addition to voice and video. Broadband is part of the IEEE 802.4 token bus standard and other IEEE standards. Finally, GM has already made an initial investment to install broadband in some

facilities.

3.1.2.2 The Data Link Layer

Specifications for the Data Link Layer include two protocol selections. The first choice is the media access control and the second is the data link control. Token passing on a bus configuration (IEEE 802.4) has been chosen as the media access control making it a physical bus topology with a logical ring configuration for the purpose of token passing. The selected data link control is HDLC (High-level Data Link Control) which is the IEEE 802.2 standard for logical link control. It is a multipoint peer-to-peer protocol which can provide connected or connectionless service. Connected (virtual circuit) service establishes a data link connection, provides error recovery, includes flow control, and provides message sequence acknowledgment. Connectionless (datagram) service does not do any of the above things. However it is the choice of MAP because these functions are implemented at higher layers. In addition to these specifications, MAP uses a 48 bit address field which is large enough to specific both network segment and device address.

The reason for choosing the token passing media access method is four fold. First, it is the only media access protocol supported on broadband by IEEE 802. Second, many of the programmable devices to be used on MAP are already somewhat token bus based. Third, token passing supports a priority scheme. Last, and most important, unless a physical failure occurs, high priority messages will be delivered within a specified time limit. This means it is deterministic, which is a requirement for real time application such as those in the manufacturing environment.

The rational the MAP Committee used for selecting the IEEE 802.2 logical link control (HDLC) standard for layer two is also based on four reasons. It can support data transfer at very high data rates. It can be used on multiple media. It will provide connectionless service. If widely accepted, VLSI chips will emerge and substantially reduce the cost of utilizing devices.

3.1.2.3 The Network Layer

The Network Layer for the MAP specification is primarily concerned with end-to-end routing. It accomplishes this by using a global routing function. There is presently a provision for a local routing

function to exist within a subnetwork if it is needed for historical or migration purposes. This type of two level routing technique is supported by IEEE, NBS, and ISO.

Conceptually, the MAP Committee has broken the Network Layer down into four sublayers. They are, in defending order, the Internet Sublayer (layer 3.4), the Harmonization Sublayer (layer 3.3), the Intranetwork Sublayer (layer 3.2), and the Link Access Interface Sublayer (layer 3.1). The details of each of these sublayers are presented in the following discussion.

The Internet Sublayer contains the internetworking routing information for end node-to-end node information flow exchange. This allows MAP datagrams to traverse multiple LAN's without regard for the routing methodology of each particular LAN. The complete specification for this protocol is beyond the scope of this paper. For further reference see MAP Specification Version 2.1 [6].

The sublayer below the Internet is the Harmonization. It provides enhancements to lower layers and sublayers as necessary. These enhancements provide uniform support services to the Internet Sublayer. It adapts the global routing sublayer requirements to the local routing sublayer services. This sublayer is dependent upon the particular application and in some cases need not exist.

If the Intranetwork Sublayer (layer 3.2) is present then the Harmonization Sublayer must also be present. It will then be responsible for mapping internetwork addresses into intranetwork addresses and vice versa.

The next sublayer of the Network Layer is the Intranetwork Sublayer. It contains the intranetwork (local) routing protocol(s). This means that it is responsible for all routing and switching of messages to, from, or through a node within the immediate LAN (the set of interconnected nodes communicating with a common protocol). This may be an X.25 packet switched network or a vendor proprietary LAN. In the ideal MAP network this sublayer would be null because the protocol selected for layer 3.4 should be able to handle this function. The Intranetwork Sublayer would be the best place to interface to WAN's.

The Link Access Interface (layer 3.1) provides the necessary interface to the Data Link Layer. This sublayer has a complete protocol implementation if it provides conversion between types of data link services. If for example the Intranetwork and Harmonization sublayers provide connectionless (datagram) service and the data link service is connection (virtual circuit) oriented, then the Link Access Interface Sublayer will be a full protocol with data link connections established between

entities of this sublayer.

The combined functionality of these four sublayers is to convert global address information into routing information, maintain message routing tables and/or algorithms, establish and terminate network connections, and switch each incoming message to a proper outgoing path. As would be expected these are generally the operations which are associated with a complete Network Layer. Associated with these sublayers are Application Layer routines and address/routing data bases which provide support for translating global addresses into the required routing information. These data bases are part of what could be called directory services.

Within any given network, it is not necessary for a local network routing sublayer to exist if the MAP standard Internet, Data Link, and Physical layers are available and compatible between adjacent nodes. The Internet Sublayer was specified to satisfy two needs. The first need is the implementation of routing within a single vendor's network. This would be for historical or migration purposes. The second need is the routing of messages between networks via external communications facilities. These are explained below.

For communication with a network of one vendor, the

Harmonization Sublayer may be reduced to simply translating the destination address to/from the addresses of the global and local networks. Following this, the vendor specific protocol may be used to route the message. From the Internet logic point of view, the local routing sublayer provides a multi-drop, peer communications data link service. For communications between two networks, such services as Telenet, Tymenet, and Accunet also provide multi-drop, peer communications data link services to the Internet Sublayer.

The last topic to be discussed concerning the Network Layer is address structure and routing. The MAP Committee has selected the address structure utilized by the Data Communications Protocol for providing Connectionless Mode Network Service (CLNS). This is the same as the address structure used in the ISO-8348 DAD2 Specification which is followed so that "Destination and Source Address" parameters may be defined according to the CLNS protocol. These are NSAP (Network Service Address Protocol) addresses as defined in the Internal Organization of the Network Layer (IONL). This means that the syntax and semantics which describe NSAP are also described in ISO-8348 DAD2. For further reference to these protocols and specifications please see the appendices of the MAP Specification version 2.1 [6]. As for routing, while

address encoding is not required to contain or imply any routing information, General Motors has decided that the underlying address structure to be chosen will imply and/or describe hierarchical routing information to be used by intermediate systems. This will be the specification until an accepted national or international standard is available.

3.1.2.4 The Transport Layer

The NBS, in its overview of the transport services, states that "the transport protocol exists to provide one fundamental service, the reliable, transparent transfer of data between transport users."[1] The transport user is the Session Layer. The MAP standard for the Transport Layer (layer 4) is the ISO compatible subset of the NBS. This is known as the Class 4 Transport Protocol (NBS-Class 4). It is the largest and most complex class of transport. It provides flow control, the ability to multiplex user transmission to the network, error detection and recovery by checking for out-of-sequence, lost, and damaged packets (checksum is optional). The main reason for selecting Class 4 is the fact that it has a great deal of support

1. MAP Task Force, pg. 3.48.

among U.S. computer manufacturers. This is due to the fact that it is the only transport protocol which supports datagram oriented networks and also because the control it offers would seem to support a wide variety of network sublayers.

The ISO and NBS standards for Class 4 are very similar. However, there are three fundamental observable differences between ISO and NBS. The NBS version supports datagram service while the ISO does not. This means that NBS allows a transport user to transfer data to a correspondent user without establishing a transport connection. The NBS version provides the "graceful close" of a connection service. This is redundant with the Session Protocol but ISO still does not provide it. Finally, the NBS supports "The Status of Connections" feature while ISO does not.

The services of the Transport Layer can be thought of as fitting into two general types. First there is the transport connection management type which allows a transport user to create and maintain the data path to a correspondent transport user. The second type is the data transfer services which provides the means for exchanging data between the transport users. The actual services provided by each of these transport service types are

discussed below.

Connection management is composed of four services: 1) the Establishment Service provides for the establishment of connections, 2) the Close Service provides for graceful termination of service, 3) the Disconnect Service also terminates a connection, but with the possible loss of data (an abort service), 4) the Status Service provides a mechanism for the user to be informed about the attributes and status of a transport connection.

The data transfer service type of the Transport Layer provides three services. The first is simply called Data Service and allows the user to transfer data to a correspondent user on a connection (a "normal data" service). The second is the Expedited Data Service which allows for transfer of a limited amount of data outside of a normal stream (an "urgent data" service). The third service provided by data transfer is the Unit Data Service. It allows for the transfer of data to a correspondent user without the need to first establish and later terminate a transport connection.

3.1.2.5 The Session Layer

The Session Layer is still in the process of being

defined for the MAP Specification. At this time the proposed standard for layer five of the OSI model will follow the ISO Session Standard which achieved International Standard status in 1984. Only two way simultaneous (full-duplex) communication will be implemented on MAP at this time. The minimum subset of the ISO Session International Standard for MAP connectivity is specified by the Kernal functional unit and the Duplex functional unit.

3.1.2.6 The Presentation Layer

Currently there is no specification for the Presentation Layer in the MAP Specification Version 2.1. No Presentation Protocol Control Information will be present.

3.1.2.7 The Application Layer

The direction to be taken for the Application Layer is the use of Common Application Service Elements (CASE) for programs that desire to communicate with programmable devices. A CASE makes available two groups of services. The first is a service for application associations

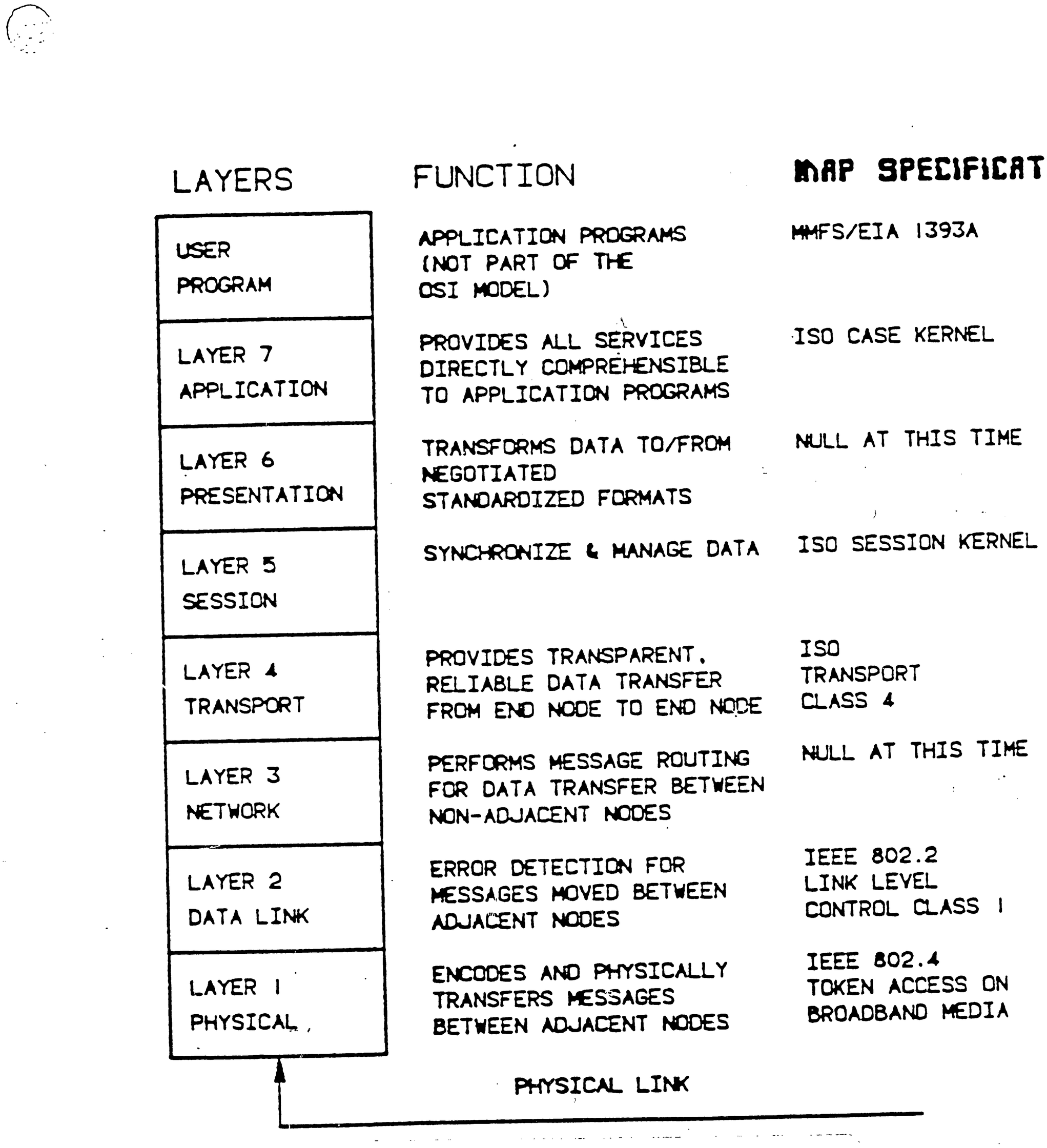


Figure 3.5

MAP SPECIFICATION SUMMARY BY LAYER

control, performed within the service elements of the Application Layer. The second is a service for information transfer and dialog control, both passed through from lower layers. Association control services enable the CASE user to establish an application association with a peer in another open system and to terminate an application association by an orderly release or by an abrupt termination (abort).

The Manufacturing Message Service makes use of the services available from CASE. It provides peer-to-peer data exchange services at the Application Layer. It provides many functions including: context management, variable access, event management, file transfer, job scheduling, operator communications, and device status. Manufacturing Message Service along with FTAM (File Transfer Access and Management) ISO DP 8571 are part of the MAP definition for layer seven of the OSI model. More information can be found on these protocols in the appendices of the MAP Specification Version 2.1 [6].

3.2 MAP Network Management

In Chapter Two of this thesis one of the topics introduced was Network Management. This section concerned

with MAP's concept of Network Management. It specifies MAP Network Management requirements that must be met by the various devices connected to the LAN. This section is an overview of guide lines suggested by the MAP committee for implementing a Network Management Facility.

3.2.1 Network Management Requirements

The requirements for the Network Management Facility of a multivendor LAN are different than those of the past required for vendor proprietary networks. There is a set of criteria that should be followed when designing a MAP Network Management Facility. These are listed below:

1. Conceptually, the network management control responsibility is decentralized.

2. The Network Manager assists each system in its own management. (i.e., distribution of the management function).

3. Network Management activities should occur infrequently and on an exception basis.

4. Isolated failures should not affect the Network Manager's operation.

5. Network Management support will vary on nodes of the

network as a function of node type (i.e. host, gateway, router, or bridge), processing power, memory capacity, and amount of local management intelligence.

6. Most importantly, the Network Management Facility developed must be modeled consistently with the OSI management architecture. Initially, MAP will adhere to this conceptual network management model and will utilize IEEE 802.1 recommendations with the intent to migrate toward the eventual ISO Standard.

3.2.2 Scope, Assumptions and Constraints

In the present MAP specification, the scope of the above management definition only pertains to layers three through seven. At some future date the management facilities for layers one and two are expected to be implemented separately using an independent manager. In addition, it is assumed that the responsibility of the Network Manager ends at any gateways connecting to a non-MAP network. As for constraints, the management architecture implies that most of the management functions will be taking place at the seventh layer through the use of messages. These messages are currently limited to ten

types and will be based on those defined in the IEEE 802.1 Standard.

3.2.3 Architectural Framework

Two views can be taken of the architectural framework for the Network Management Facility. The designer can look at it from either the external or internal point of view. These two perspectives are presented below.

When looking at the management architecture from an external point of view we see that network management is responsible for gathering information on the usage of the network media by the attached network devices. This ensures correct operation of the network and provides management reports. Information can be processed for the various types of users, assisting in planning, operations, and maintenance. An explanation of the use of each of these types of data follows.

Planning data is used by managers in network design for modeling and simulations. Operations data is used by planners and operators in conducting performance monitoring, configuration management, and network access management. Maintenance data is used by technicians to perform functions such as problem detection and diagnosis,

installation and check out, and preventive maintenance.

The Network Management internal view concentrates on the inner workings of what MAP refers to as the Management Applications Processor. This is the actual hardware and software that performs the functionality required by a Network Manager. It can be a centralized node or Network Manager responsibilities can be distributed over the network. Four functions are required of the initial Management Applications Processor implementation. They are covered below.

Configuration Management's function is to determine and control the state of the system. This encompasses the logical and physical configuration of the system. Performance Management is in charge of performance control and assessment of the nodes and the network operation. Event Processing sees to the generation and interpretation of notification of unsolicited significant occurrences. Fault Management provides diagnosis of failures using tests initiated on the network by the manager. The reader should be able to draw parallels from the MAP specification for Network Management architecture presented in the last four paragraphs and those presented for LAN's in general in Chapter Two.

3.2.4 Management Application Requirements

In the MAP specification, the requirements for each of the four internal view management applications is described in terms of its inputs, outputs, and processing. For the purpose of the MAP Network Manager, each management application is defined as the set of functions, data, messages, and parameters used to: collect, control, store, and present information. These are described below.

Configuration Management is the set of functions, data, messages, and parameters used to: 1) collect information about the system state, 2) control the system state, 3) store the system state and state histories, 4) present the system state.

Performance Management is the set of functions, data, messages, and parameters used to: 1) collect system statistics, 2) control the collection of system statistics, 3) store the system statistics and their histories, 4) present the system statistics.

The Event Processor is the set of functions, data, messages, and parameters used to: 1) collect information about system changes, 2) control reporting of the system changes, 3) store system state changes and their histories, 4) present system state changes.

Fault Management is the set of functions, data,

messages, and parameters used to: 1) verify the system state, 2) isolate any faults, 3) correct any faults.

3.3 The MAP Migration Path

MAP has yet to be wholly defined. In addition, some of the standards chosen by MAP have just been approved or are under development at the national level. It may be some time before equipment manufactures implement the hardware and software to meet these new standards. For these reasons there needs to be some recommendations for a migration path to be taken by both LAN designers and equipment vendors.

Implementation of the MAP standard in terms of compatible network products will occur over a period of time. Through activities with several computer manufacturers, General Motors currently has full network capabilities developed for only a few specific machines. Implementation of this capability, referred to as "network node capability", will evolve to more computing hardware in the future. It is planned that node capability will eventually be offered in the majority of manufacturing computers, allowing wide interconnection on a MAP

backbone.[2]

In the mean, time the MAP Committee has made a list of interim recommendations to all General Motors vendors. These recommendations were designed to fit the best possible solution for the majority of the vendors. The recommendations also use the criteria of the availability of existing hardware and software.

The interim recommendation for backbone media is broadband coaxial cable. This is due to the fact that it can appear as many independent communication channels or as a multipoint link. Existing systems (in GM facilities) do not need to be altered to use broadband cable. MAP recommended IEEE 802 protocols include operation on broadband cable.

The attachement link (NIU) is required for devices which do not provide full MAP functionality in order for them to connect to MAP gateways. The architecture for these links is necessarily application dependent.

Attachment protocols are dependent on the connected equipment and the communications options available. In cases where protocol options exist, the MAP Task Force recommends HDLC-NRM and HDLC-ABM with the Manufacturing Message Standard along with RS-449/422 or, as a second

2. MAP Task Force, pg. 5.1.

choice, RS-232C.

High-level Data Link Control-Normal Response Mode (HDLC-NRM) is the interim MAP standard for multi-drop applications. This interim choice will be eliminated when IEEE 802.4 hardware becomes readily available. HDLC-NRM is a polling protocol with a master/slave relationship. It is a half duplex, multi-drop protocol. It was selected for quite a few reasons: 1) its a well documented and well accepted standard, 2) hardware is currently available for implementing a portion of the standard (framing, CRC generation/checking, bit stuffing/unstuffing, etc), 3) it can be easily implemented with microprocessors without consuming more than two kilobytes of code, 4) because most interim communications in the typical GM plant are now vertical along a hierarchical path they lend themselves to a master/slave relationship, 5) half-duplex is simple in terms of protocol, trouble shooting, and implementation (single channel), and 6) multi-point reduces wiring costs.

High-level Data Link Control-Asynchronous Balanced Mode (HDLC-ABM) is the interim MAP standard for point-to-point applications. It is a non-polling protocol which allows secondary stations to initiate transmission and allows full-duplex where needed for greater performance throughput. The reasons for choosing HDLC-ABM for point-

to-point applications include: 1) it is a well documented and well accepted standard, 2) hardware is currently available for implementing a portion of the standard (framing, CRC generation/checking, bit stuffing/unstuffing, etc.), 3) it can be implemented with minimal processor resources (only two kilobytes of code required), 4) it is directly applicable to broadband coaxial point-to-point connections and provides a viable short term attachment link protocols, 5) in critical subnetworks where a single failure could disable an NRM network, ABM is a better alternative.

3.4 Summary

The driving force behind MAP is the need for compatibility of communications to integrate the many different factory floor devices in todays plants. Because many vendors supply these factory floor devices, it is the goal of MAP to provide an environment for multiple vendors to participate on a standard communications network.[3]

The current MAP specification provides for definition of layers one and two of the OSI model by the IEEE 802.4 and 802.2 standards respectively. Layer four is

3. MAP Task Force, pg. 1.2.

specified by the NBS standard. The MAP specifications of the other layers are in various stages of development. Progress has been made. Today the user can specify MAP and purchase compatible systems that will provide connectivity and guaranteed data transfer.

CHAPTER FOUR

A METHODOLOGY FOR NETWORKING NEEDS ANALYSIS

4.0 Introduction

So far this thesis has presented an overview of the fundamental concepts of local area networks and a summary of the latest MAP Specifications. This chapter deals with a methodology of capturing the information flows of a factory so they may be analyzed to determine the network needs of that factory. Once a methodology for determining local network needs has been applied and results analyzed the designer can then use knowledge of LAN's to determine and specify the best network architecture for the factory.

4.1 Description of Methodology

The methodology for capturing factory network needs described in this chapter was recently developed at Lehigh University. A requirement existed to identify and specify the network needs for an actual manufacturing facility. Lehigh staff recognized a need for a methodology to

capture network needs of this specific factory. A methodology was developed and given the name "Manufacturing Systems Analysis and Design Methodology".

The Lehigh methodology was developed by drawing upon such notable structured analysis techniques as the ICAM Definition Language (IDEF) and the Yourdon Methodology. Detailed information on these two methodologies can be found in most structured analysis texts. The Manufacturing Systems Analysis and Design Methodology can be used to model existing and future manufacturing facilities. These models do not characterize a network design (a network modeling methodology will be presented in the next chapter), rather they are used to critique the manufacturing environment in question with respect to procedural improvements, and the thoughtful application of advanced manufacturing technologies.[1]

According to the report defining the Lehigh Network Needs Methodology [7] the purpose of this methodology is to characterize a manufacturing facility with respect to basic communications needs, opportunities, and restrictions. This methodology focuses on three distinct areas of manufacturing communications: 1) the information flows of the shop floor and supporting operations, 2) shop

1. Lehigh Network Needs Report, pg. 2.

floor equipment profiles, and 3) existing electronic communications. The information which must be gathered can be collected by an interviewing process in which all key personnel involved with the shop floor and its supporting facilities are questioned. The methodology itself is supported by two closely coupled tools which allow the collected information to be organized, reviewed, verified, and analyzed. The first tool is the Information Flow Diagram. This tool permits information flow data to be properly organized and provides graphic representation of complex inter-relationships. The second tool is a supporting data base structure which can be used to store all collected data and to provide capabilities for user friendly statistical analysis.[2]

These two tools can be used in analysis to identify dominate relationships regarding existing and potential network usage. The result of such analysis includes not only goals and objectives for the networking effort to which it will be applied, but also a quantitative base from which to begin formulation of the detailed communications architecture.

2. Lehigh Network Needs Report, pg. 2.

4.2 The Data Collection Process

The first step of the Manufacturing Systems Analysis and Design Methodology is to collect all the necessary data describing the communication needs of the factory floor and its supporting facilities. This data is collected using a special form to describe information flow, a form to classify shop floor devices, and a form to document existing communications. An interviewing process is used to collect information from key people involved with the factory. Also, present electronic communications are documented.

4.2.1 Information Flow

Whether or not there is an existing communications network in a manufacturing facility there is still a great deal of information exchanged between different areas of the shop floor and with supporting facilities. It is important to capture information flows and to determine amounts of data the future communications network will have to support between different areas of the facility. The Lehigh methodology does this through the use of a form which helps identify and characterize information flows directly or indirectly supporting the

factory floor.

The Network Needs Methodology first focuses on describing critical shop floor and supporting operations. This Information Flow description includes:

-- Information flow name

-- A brief description of the information flow and its use

-- Type of information flow

-- Media used to support the information flow

-- Source or originator of information flow

-- Destination of the information flow

-- Information flow size

-- Transmission time and rate (if appropriate)

-- Frequency of transmission

-- Criticality of the information flow. The levels of criticality are defined below.

- High: vital to proper shop floor operation

- Medium: important to shop floor operation

- Low: minimum adverse impact to shop floor operation.

An example of a completed Information Flow Form is shown on the following page.

INFORMATION FLOW QUESTIONNAIRE

DF NAME: _____ PLANT: F T

DESCRIPTION/USE: _____

TYPE: *Batch* *Interactive* *Real-time* *Monitor* *Corrective*

MEDIA: *Paper* *Diskette* *Wire* *Voice* *Magnetic-tape* *Other*

ACR: _____ SOURCE: _____

ACR: _____ DESTINATION: _____

SIZE: _____

CONVERTS TO: _____ *Bytes* *Kilobytes* % USED: ___

TRANSMISSION TIME: _____ *Second* *Minute* *Hour*
Day *Week*

RATE: _____ BAUD

FREQUENCY: _____ PER: *Second* *Minute* *Hour*
Day *Week* *Year*

CRITICALITY: *Low* *Medium* *High*

INITIALS: _____

S/N: ___ _____

INFORMATION SOURCE(S): _____
_____

4.2.2 Device Classification

The factory floor of a particular manufacturing facility is made up of devices which now communicate or will communicate when the new network is installed. It is important to classify these devices according to their communication needs and capabilities. This device classification information can be brought together to determine what type of network should be installed and to anticipate difficulties that may arise with respect to equipment at installation time. The Device Classification includes:

-- Device name

-- A brief description of the device and its use

-- Device vendor

-- Number of similar devices within the facility

-- Level of electrical noise environment seen by the device

-- Type of device controller used

-- Device controller vendor

-- Existing mode of device communication

-- Desired mode of device communication.

An example of a completed Device Classification Form is shown on the following page.

DEVICE CLASSIFICATION QUESTIONNAIRE

ACR: _____ NAME: _____ PLANT: F T

DESCRIPTION/USE: _____

ACR: _____ VENDOR: _____

QUANTITY: _____ ELECTRICAL NOISE: *Low* *Medium* *High*

CONTROL: *Hardwire* *Logic-controller(programmable)*

Personal-computer *Minicomputer* *Dataprocessor*

ACR: _____ VENDOR: _____

EXISTING COMMUNICATIONS: *Paper* *Wire* *Voice* *Magnetic-tape* *Other*

DESIRED COMMUNICATIONS: *Paper* *Wire* *Voice* *Magnetic-tape* *Other*

DESIRED CONNECTIVITY: _____

INITIALS: _____

S/N: _____

INFORMATION SOURCE(S): _____

_____

4.2.3 Existing Communications

Because there is a great deal of information flow in manufacturing facility there usually is some form of existing communications system for the factory floor. Here we are only interested in the existing digital communications environment. It is this environment in which the target communications architecture must be implemented. In general, a communications network is realized through a migration path which may be completed during several different phases. For this reason, as the target architecture is implemented over time it will have to coexist with and in some cases gradually replace a portion of the existing communications infrastructure. This makes it important to capture the existing communications description. This description includes:

-- Name of communications system

-- Communications system vendor

-- System capacity and current utilization

-- Protocol used

-- Medium used

-- System topology.

An example of a completed Existing Communications Form is shown on the following page.

EXISTING COMMUNICATIONS QUESTIONNAIRE

ACR: _____ NAME: _____ PLANT: F T

ACR: _____ VENDOR: _____

CAPACITY: _____ % LOADING: _____

ACR: _____ PROTOCOL: _____

ACR: _____ MEDIUM: _____

ACR: _____ TOPOLOGY: _____

NOTES:

INITIALS: _____

S/N: _____

INFORMATION SOURCE(S): _____

_____

4.3 Information Flow Diagrams

Use of Information Flow Diagrams is closely coupled with the above forms in organizing, reviewing, verifying, and analyzing information gathered about needs of a manufacturing facility network. Information Flow Diagrams, are discussed in this section.

This diagramming tool has three primary purposes with respect to network needs analysis: 1) to provide the analyst with a tool that graphically assists in unraveling the large amounts of inter-related data that has been collected; 2) to provide the analyst and other reviewers a concise tool with which to review, reconcile and verify the resulting information model; 3) to graphically assist in identification of key areas of interest requiring in-depth data base analysis.[3]

The Information Flow Diagram depicts information flows between different entities of the facility by a top down decompositional approach. There are three distinct types of graphic elements used in these diagrams. The first are internal entities, which are usually organizational and reside in the structure under analysis.

3. Lehigh Network Needs Report, pg. 5.

The second are external entities. They interact with the structure under analysis but do not reside within it. Finally, there are the in-coming and out-going aggregate information flows which interconnect the internal and external entities. Each of these aggregated information flows is identified by a number so that its constituent information flows can be retrieved from the data base and analyzed.

The process used to construct these diagrams is hierarchical. First a high level representation of the manufacturing environment is constructed. An example is depicted in Figure 4.1. Then, proceeding in a top down fashion, the high level representation is decomposed into its supporting detail. This can be seen in Figure 4.2. Here the constituent internal entities of a high level entity are described graphically. All of the information flows within the higher level entity are numbered and depicted. Any flows which are a constituent of a higher level aggregate information flow are also numbered with that flow's number in parentheses. The last decomposition process depicts the inter-entity communications. Each of the entities being examined is broken into its constituent parts and these parts are enclosed in dashed lines. This shows how each high level entity communicates

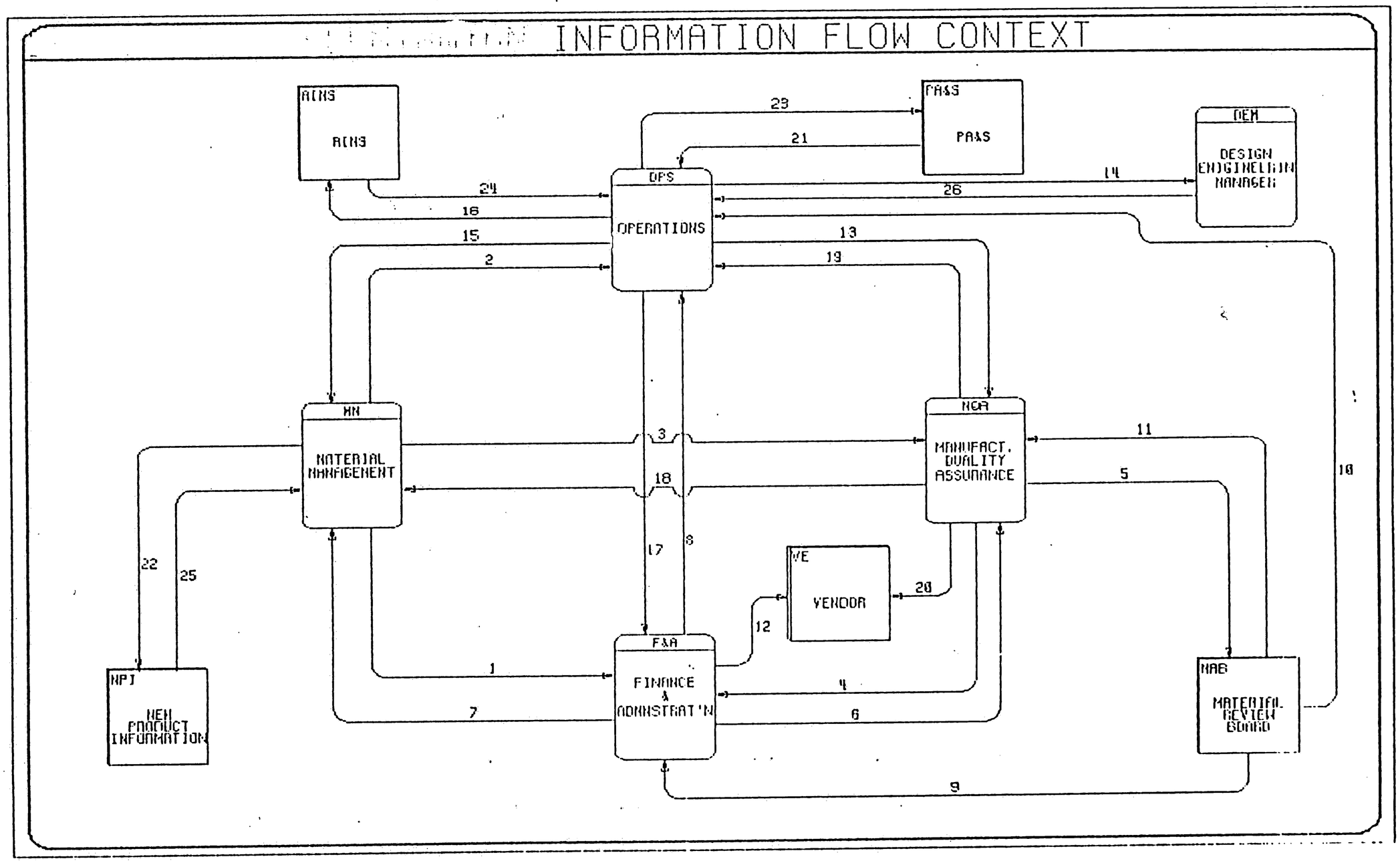

INFORMATION FLOW CONTEXT
RENS
RENS
PA&S
PA&S
DEM
DESIGN ENGINEERING MANAGER
OPS
OPERATIONS
MM
MATERIAL MANAGEMENT
MQA
MANUFACT. QUALITY ASSURANCE
VE
VENDOR
F&A
FINANCE & ADMINSTRAT'N
NPI
NEW PRODUCT INFORMATION
MAB
MATERIAL REVIEW BOARD
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

Figure 4.1

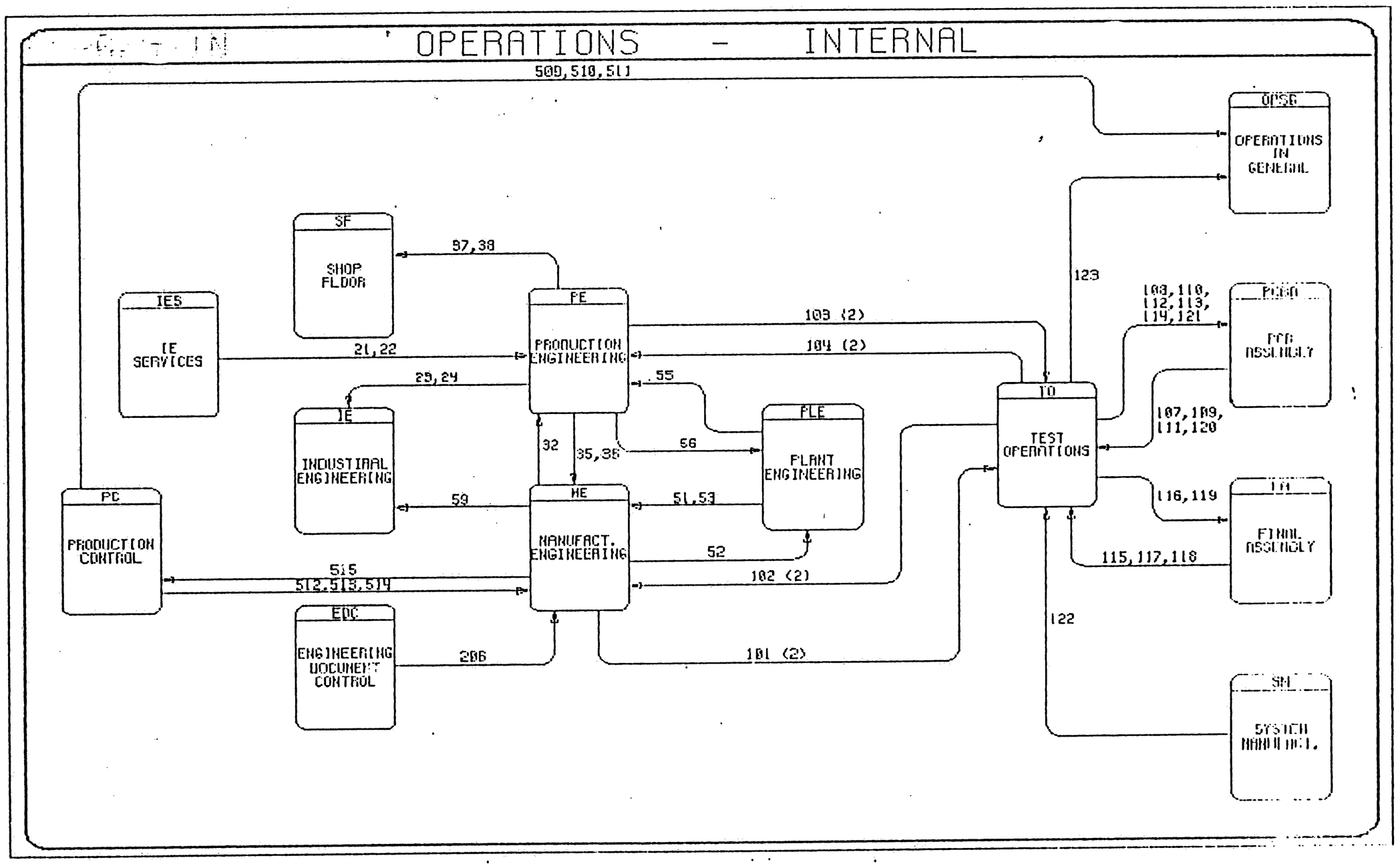

OPERATIONS - INTERNAL
500,510,511
OPSG
OPERATIONS IN GENERAL
SF
SHOP FLOOR
37,38
IES
IE SERVICES
21,22
PE
PRODUCTION ENGINEERING
103 (2)
104 (2)
123
100,110, 112,113, 114,121
PCBA
PCB ASSEMBLY
25,24
.55
TO
TEST OPERATIONS
107,109, 111,120
IE
INDUSTRIAL ENGINEERING
32
35,36
56
PLE
PLANT ENGINEERING
PC
PRODUCTION CONTROL
59
ME
MANUFACT. ENGINEERING
51,53
116,119
FA
FINAL ASSEMBLY
52
115,117,118
515
512,513,514
102 (2)
EDC
ENGINEERING DOCUMENT CONTROL
206
122
101 (2)
SML
SYSTEM MANUFACT.

Figure 4.2

with others via their internal entities. An example is shown in Figure 4.3.

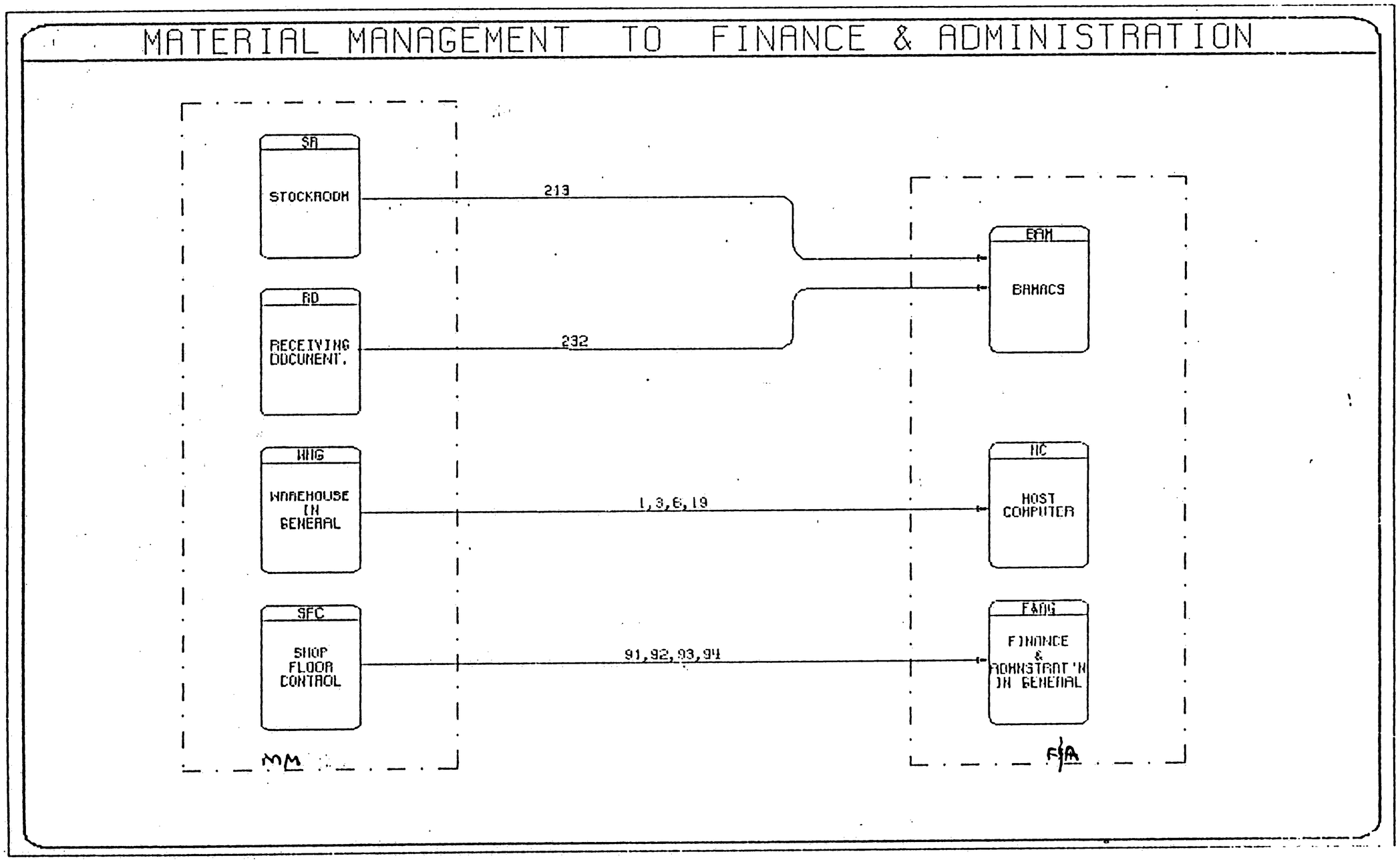
These information flow diagrams can be used for detailed analysis of the communication requirements of an existing manufacturing facility. The use of this tool can be helpful in the systematic analysis of the existing communications model. In addition, because of the close coupling of this tool with the data base (discussed next) it can be useful in developing a network architecture and migration path.

4.4 The Data Base

The interviewing process (of key personnel) results in a collection of forms detailing aspects of information flows, device classifications, and existing communications. The amount of data contained in these forms can be quite large and intractable. The use of a powerful data base management tool can be very helpful in storing and manipulating this data for analysis. The Network Needs Methodology developed at Lehigh employs a data base as the single repository for all data collected. This data base is referred to as the "Communications Model Data Base".

The data base chosen should provide strong

Figure 4.3—


MATERIAL MANAGEMENT TO FINANCE & ADMINISTRATION
SR
STOCKROOM
213
BAM
BAMACS
RD
RECEIVING DOCUMENT.
232
WHG
WAREHOUSE IN GENERAL
1,3,6,19
HC
HOST COMPUTER
SFC
SHOP FLOOR CONTROL
91,92,93,94
FAAG
FINANCE & ADMNSTRAT'N IN GENERAL
MM
F/A

statistical capabilities as well as organizational, analytical, and summary graphics. It is also helpful to have cross tabulation capabilities which provide percentage and summary functions. Figure 4.4 shows some of the possible comparisons which can be made with a powerful data base.

The data base tool coupled with the information flow diagrams can be used to answer a tremendous variety of questions about the current and desired communications of a particular manufacturing facility. This provides a model of the networking needs which in turn can be used to formulate the design of a suitable network architecture for a given factory environment. The next chapter of this thesis will present a methodology for modeling the selected network architecture to determine if it can fit the required needs.

4.5 Interrogation of the Network Needs Model

When the information flow diagrams have been completed and the data base is filled with the information collected and reconciled (to get rid of any erroneous entries) it is then possible to interrogate the Network Needs Model. This interrogation can provide answers to a

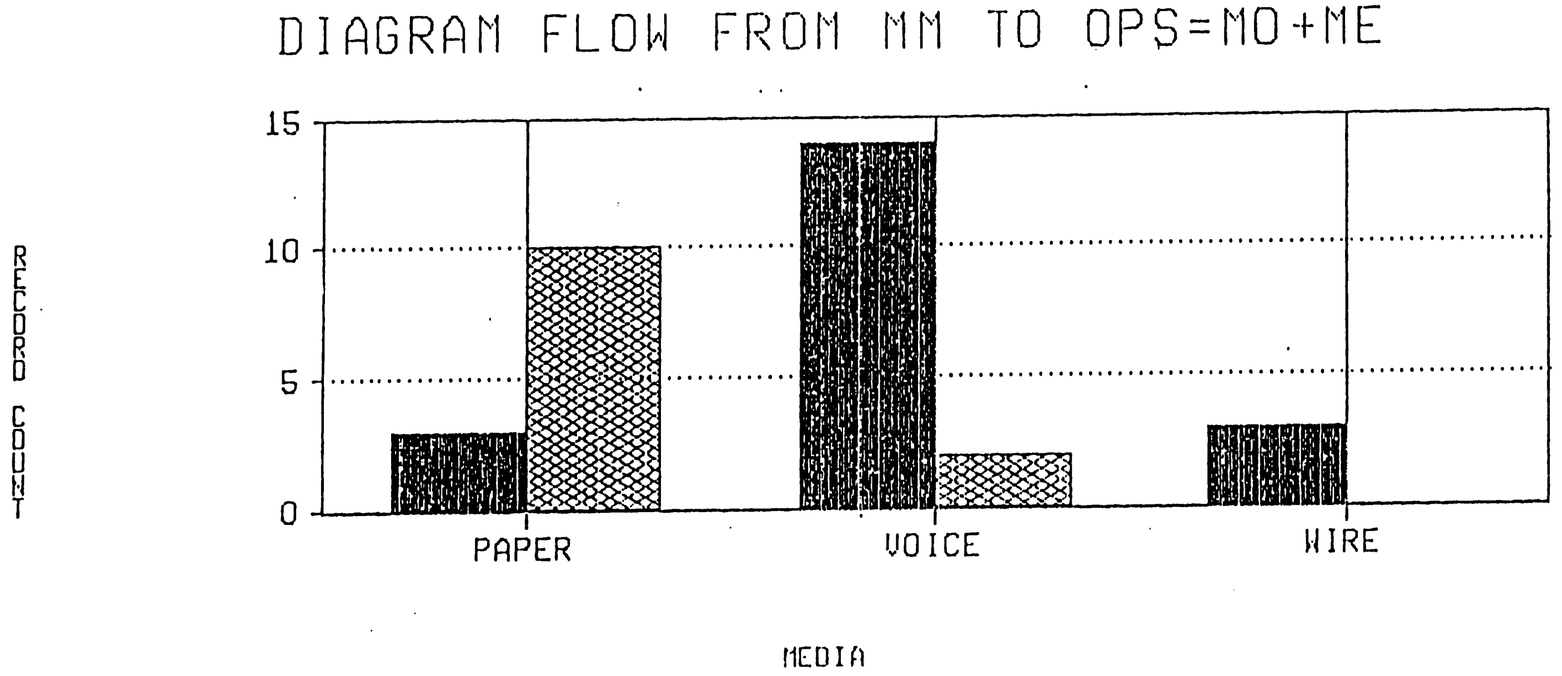


DIAGRAM FLOW FROM MM TO OPS=MO+ME
RECORD COUNT
15
10
5
0
PAPER
VOICE
WIRE
MEDIA

Figure 4.4-

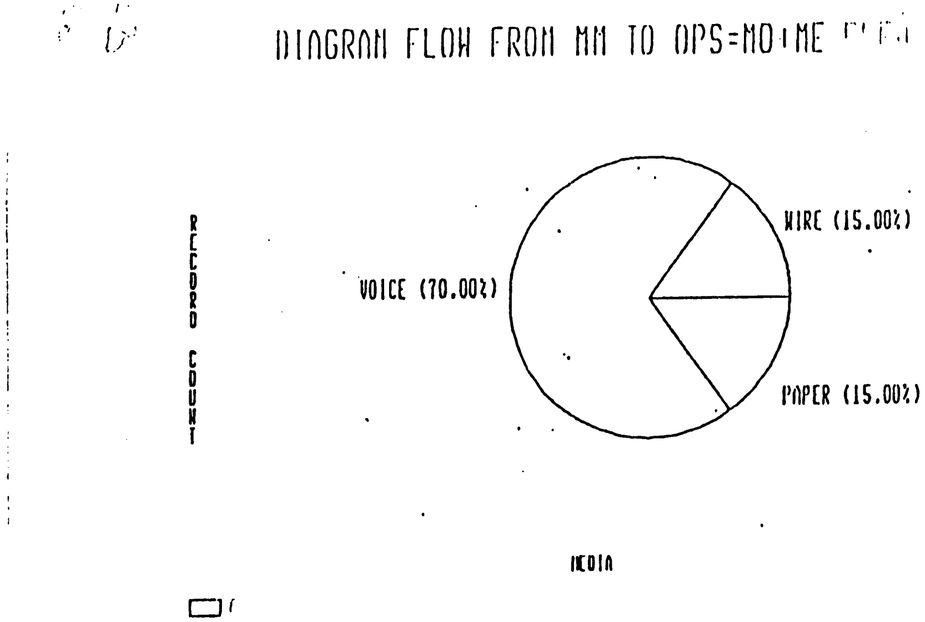


DIAGRAM FLOW FROM MM TO OPS=MO+ME
RECORD COUNT
VOICE (70.00%)
WIRE (15.00%)
PAPER (15.00%)
MEDIA

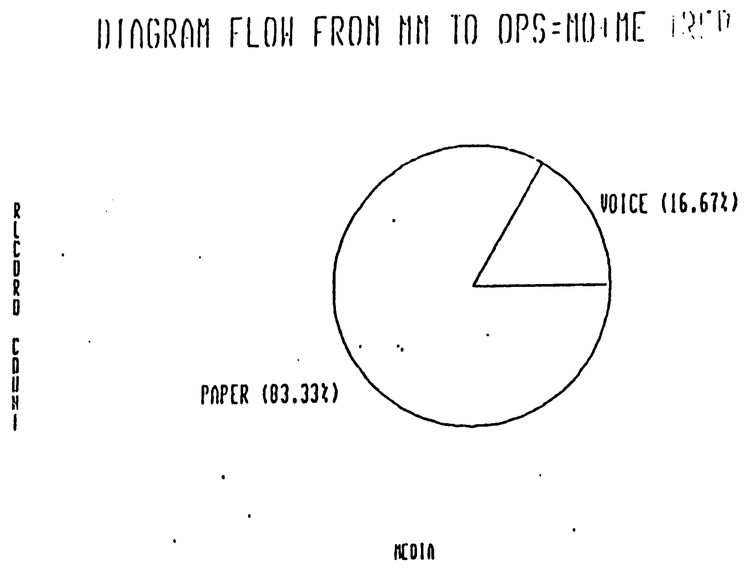


DIAGRAM FLOW FROM MM TO OPS=MO+ME
RECORD COUNT
VOICE (16.67%)
PAPER (83.33%)
MEDIA

vast array of questions relating to the current and desired communications capabilities and requirements. If a powerful data base management tool was selected, there should be no problem in quickly obtaining answers to many analysis questions. This section presents some of the most relevant questions to ask and how their answers should be interpreted. These questions are grouped by the area of manufacturing communications to which they are related, namely Information Flow Analysis, Device Classification Analysis, and Existing Communications Analysis.

4.5.1 Information Flow Analysis

Information Flow Analysis deals with statistical analysis of the various information flows within, in and out of the factory floor and its supporting facilities. This section presents some of the fundamental questions which should be answered in this analysis.

The most fundamental question to be asked here is "what is the total volume of information (usually in bits) which flows through the present communication system (not necessarily a network) over some period of time (usually daily)"? The answer to this question will determine the capacity or bandwidth which will be required to support present information flow. It should be easy to vary time

period and determine when peak loads will be on the network to insure network capacity will meet requirements. Finally, it will be possible to determine the bandwidth requirements for certain segments of the network. This makes it possible to determine the information flows which take place directly between two factory floor entities. This enables the network designer to specify network segment bandwidth requirements.

Another question the network analyst may be interested in is "what proportion of the traffic on the network will be of a highly critical nature"? This question can be just as easily answered for any of the three levels of criticality. This question can also be applied to different segments of the network, helping the analyst to determine which information flows absolutely have to be handled by the network.

A final fundamental question which should be addressed concerning information flows is "what volume of information flow presently takes place on each existing communications medium". This will show how much data is being carried on the desired communications medium versus the amount being transferred through different types of undesirable, existing communications media. This knowledge will assist in choosing a migration path towards the final communications network implementation. Some examples of

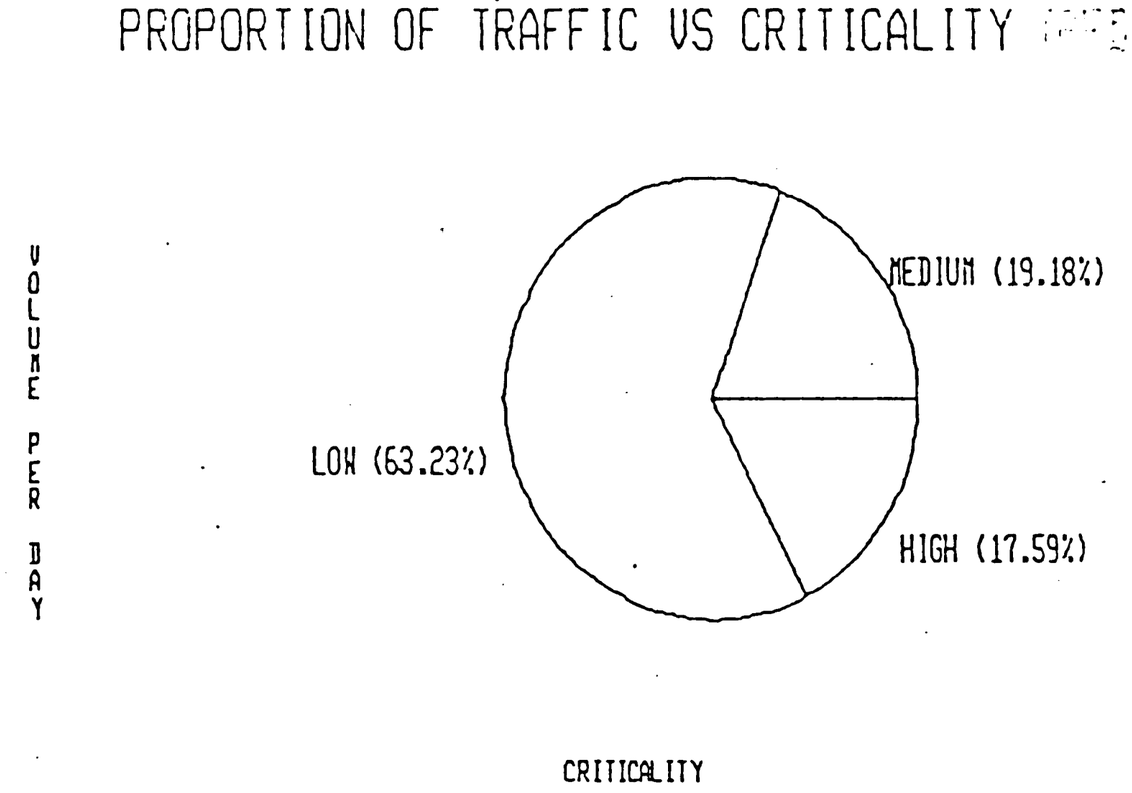
data base graphs and cross tabulations answering these questions are shown in the following pages.

4.5.2 Device Classification Analysis

The manufacturing facility in question will undoubtedly have a large collection of different devices being used on the factory floor. These devices will not only differ in type but also in vendor. If the networking goal is to enable all of these different devices to communicate then their present communications capabilities will be of great interest to the analyst who is assessing network needs. As the MAP standard moves toward completion and gains wider acceptability this problem will become smaller, but until then questions addressed in this section are very important.

The first question which will probably come to mind here is "what percentage of the devices use each of the existing communications media"? This will determine which medium is currently most prevalent. Then the percentage of devices not using the desired communications medium could be determined to give an idea of the amount of changes required to implement a desired network design.

Another statistic of interest is the percentage of


PROPORTION OF TRAFFIC VS CRITICALITY
MEDIUM (19.18%)
LOW (63.23%)
HIGH (17.59%)
CRITICALITY

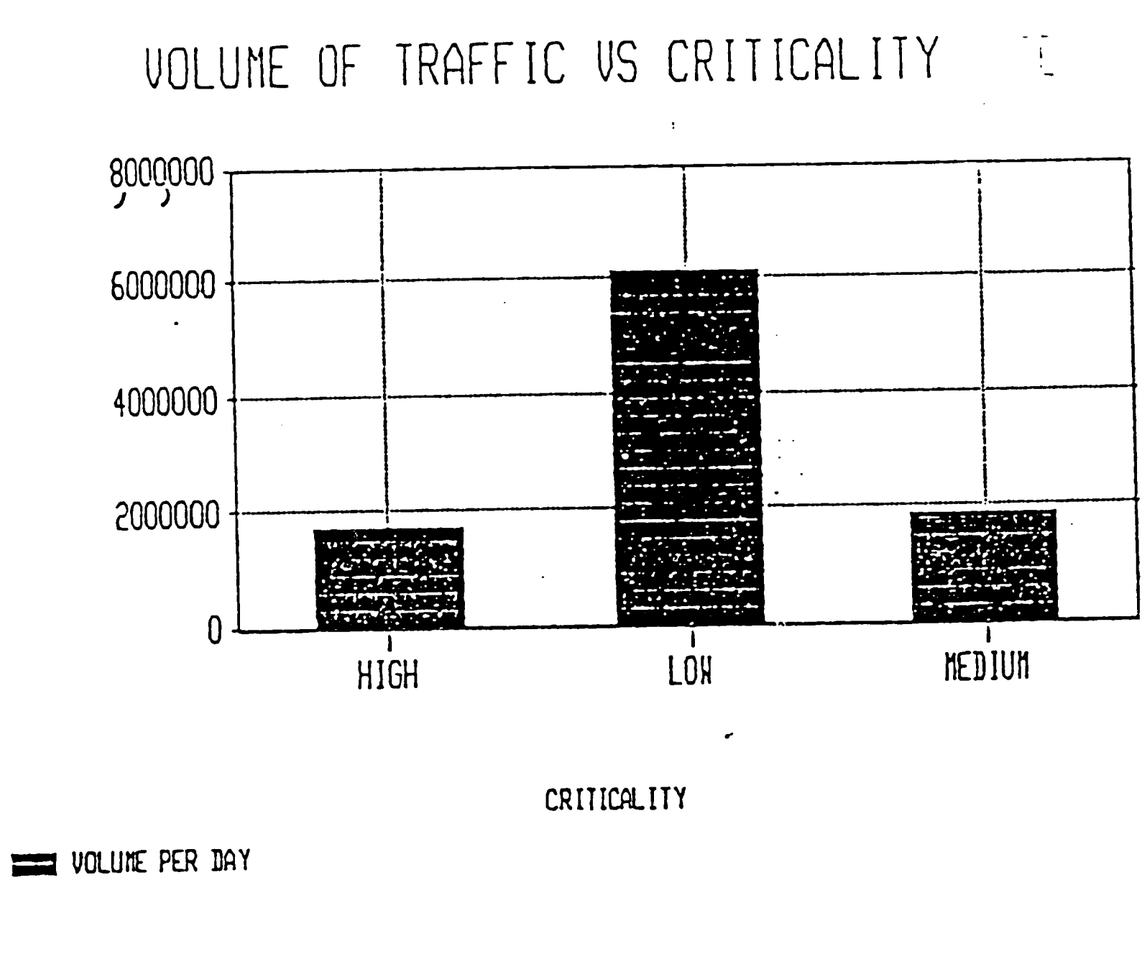

VOLUME OF TRAFFIC VS CRITICALITY
VOLUME PER DAY
8000000
6000000
4000000
2000000
0
HIGH
LOW
MEDIUM
CRITICALITY
VOLUME PER DAY

Figure 4.5

devices in each of the electrical noise environments present on the factory floor. The Network Needs Methodology recognizes three categories of electrical noise which may exist in a manufacturing facility. They are simply low, medium, and high. The level of noise in which a device must operate can affect the choice of communications medium.

Finally, there is a group of questions which may be addressed concerning the number or percentage of devices which are the same type, have the same vendor, use the same control device, etc. These questions simply help the analyst get a feel for the amounts of different devices which must be networked. The following pages contain some examples of answers to these questions obtained using a data base tool.

4.5.3 Existing Communications Analysis

The last type of analysis which must be performed in the Network Needs Methodology deals with the existing communications infrastructure. The data base should contain information on all types of digital communications presently in place at the manufacturing facility. This information includes the vendor, capacity, percent of loading, protocol, medium, and topology of each of the

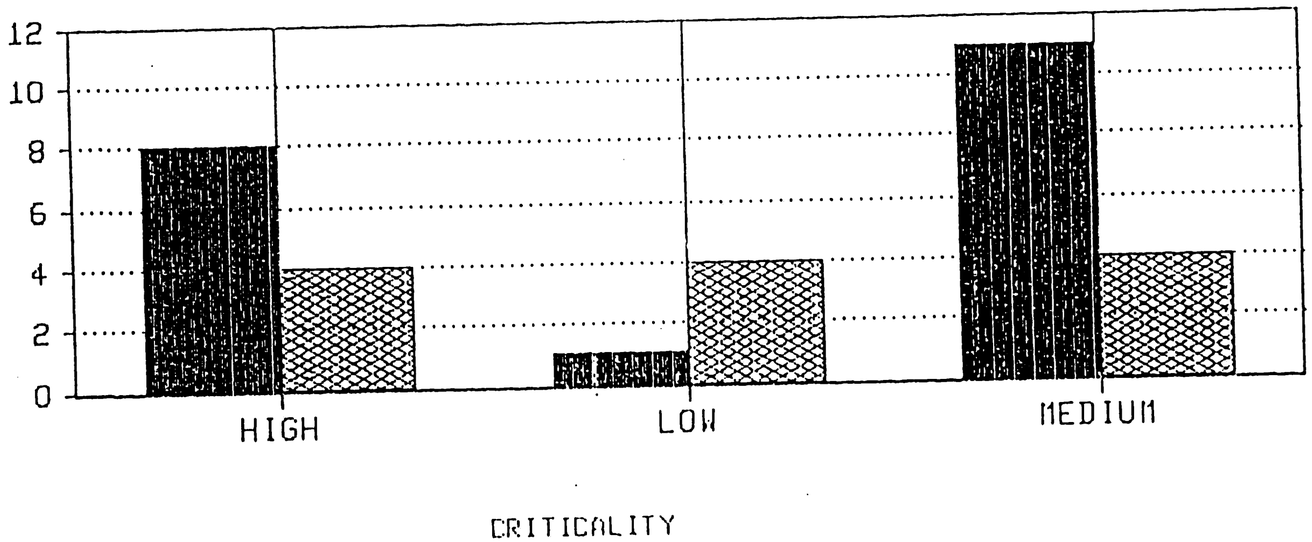


DIAGRAM FLOW FROM MM TO OPS=MO+ME
12
10
8
6
4
2
0
RECORD COUNT
HIGH
LOW
MEDIUM
CRITICALITY

FIGURE 4.6

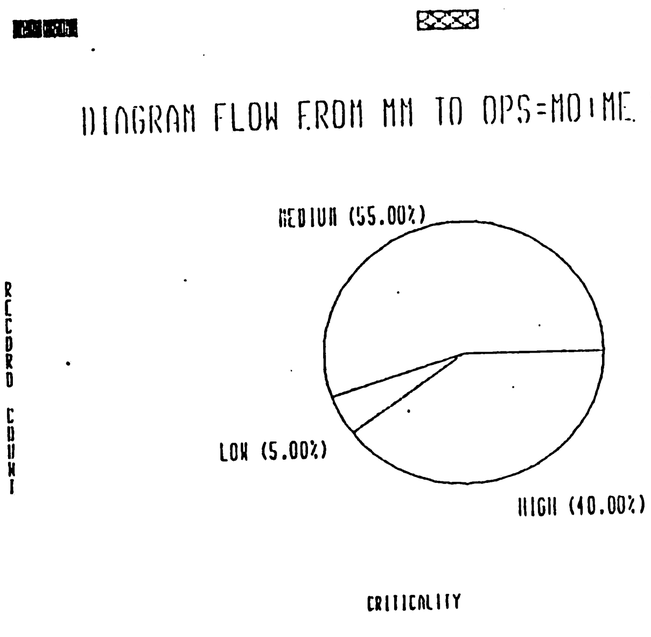


DIAGRAM FLOW FROM MM TO OPS=MO+ME
MEDIUM (55.00%)
LOW (5.00%)
HIGH (40.00%)
RECORD COUNT
CRITICALITY

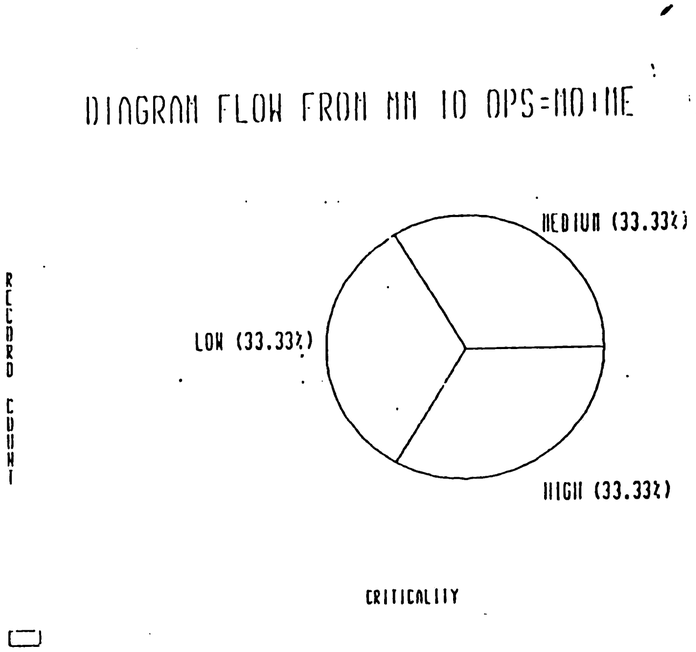


DIAGRAM FLOW FROM MM TO OPS=MO+ME
MEDIUM (33.33%)
LOW (33.33%)
HIGH (33.33%)
RECORD COUNT
CRITICALITY

named networking facilities currently in place. The importance of this information lies in the contribution it will make in choosing a final network architecture and the migration path taken to achieve it.

The obvious questions concern percentage or total amount of each of the existing communications equipment. If the analyst sees there is already a broadband backbone in place, it would be wise to stick with this since the initial investment has been made. In addition, if the majority of the communication taking place is using a certain protocol it would make sense to stick with it because the network trouble shooters most likely have a thorough understanding of it. Also, the hardware and software for implementing the protocol will already be in place on a majority of the devices. Common sense governs most of the decision made in this analysis.

4.6 Summary

This chapter presented a methodology for assessing the network needs of a manufacturing facility. Developed at Lehigh University, and called the "Manufacturing Systems Analysis and Design Methodology" (MSADM), it is based on popular structured analysis techniques. This discussion focused on the Network Needs Methodology

portion of MSADM. Through the use of extensive data collection, organization, and analysis it is possible to define network needs for a factory floor and its supporting entities. Once needs are known it is possible to begin design of tentative network architectures for the facility. Following this, it is best to model the network design so it may be thoroughly tested prior to implementation. The following chapter presents a methodology for the efficient modeling of local area networks.

CHAPTER FIVE

A LAN MODELING METHODOLOGY

5.0 Introduction

When a LAN designer first comes up with an architecture for a particular network application the next step should not be implementation. It is far wiser to extensively test a model of the LAN's architecture to make sure it meets performance requirements then it is to wait and test the implemented network. This chapter will first discuss concepts and reasons for modeling local area networks. Then a methodology is presented for constructing a simulation model which is suitable for efficient design and performance analysis.

5.1 Modeling and Monitoring a LAN

It has been suggested that issues of LAN design can

be classified as either configuration issues or protocol issues. Also, networks consist of four basic elements for which performance is dependent, both individually and in mutual interactions. These elements are the transmission medium, the control mechanism, the interface, and the protocols. It has also been suggested that network traffic properties such as message sizes, rates, and their distribution have a great affect on network performance; and further, that performance is not only strongly dependent on the traffic but also upon the mutual interaction of traffic, the configuration, and the protocols. Chapter Two pointed out some of these aspects when discussing network performance. This chapter will explain how these issues, elements, and properties of LAN's can be built into a model.[1]

Models can and have been of critical importance in design, implementation, and tuning of LAN's. Models can be used to verify and explore the anticipated performance of a tentative LAN design through simulation prior to actual implementation. The process doesn't stop after implementation however. Modeling can also be used to fine tune and enhance a LAN which is already up and running. In actuallity the process should be cyclic, involving

1. Watson, pg. 31.

feedback in a design-measure-model-design, etc., iterative process. Feedback is provided by monitoring and measuring the implemented LAN. Measurements are fed into the model, making effective design possible. As flaws are detected or enhancements discovered during simulation, beneficial modifications are made to the original design and model. The whole process is repeated and is hopefully quickly and economically convergent. Without this cyclic process it is nearly impossible to achieve an efficient and successful LAN design. This may be summed up by saying: " if you don't (can't) model it how can you understand it, and if you don't (can't) measure (monitor) it how do you know it is working correctly".[2]

5.1.1 Measuring

Predominate ways of measuring performance of an actual LAN implementation are: 1) install software in each node to monitor and record the node's network activity, or 2) directly monitor and make measurements on the network medium. Advantages and disadvantages of each of these methods are discussed below.

If software is installed in all of the hosts it is

2. Watson, pg. 33.

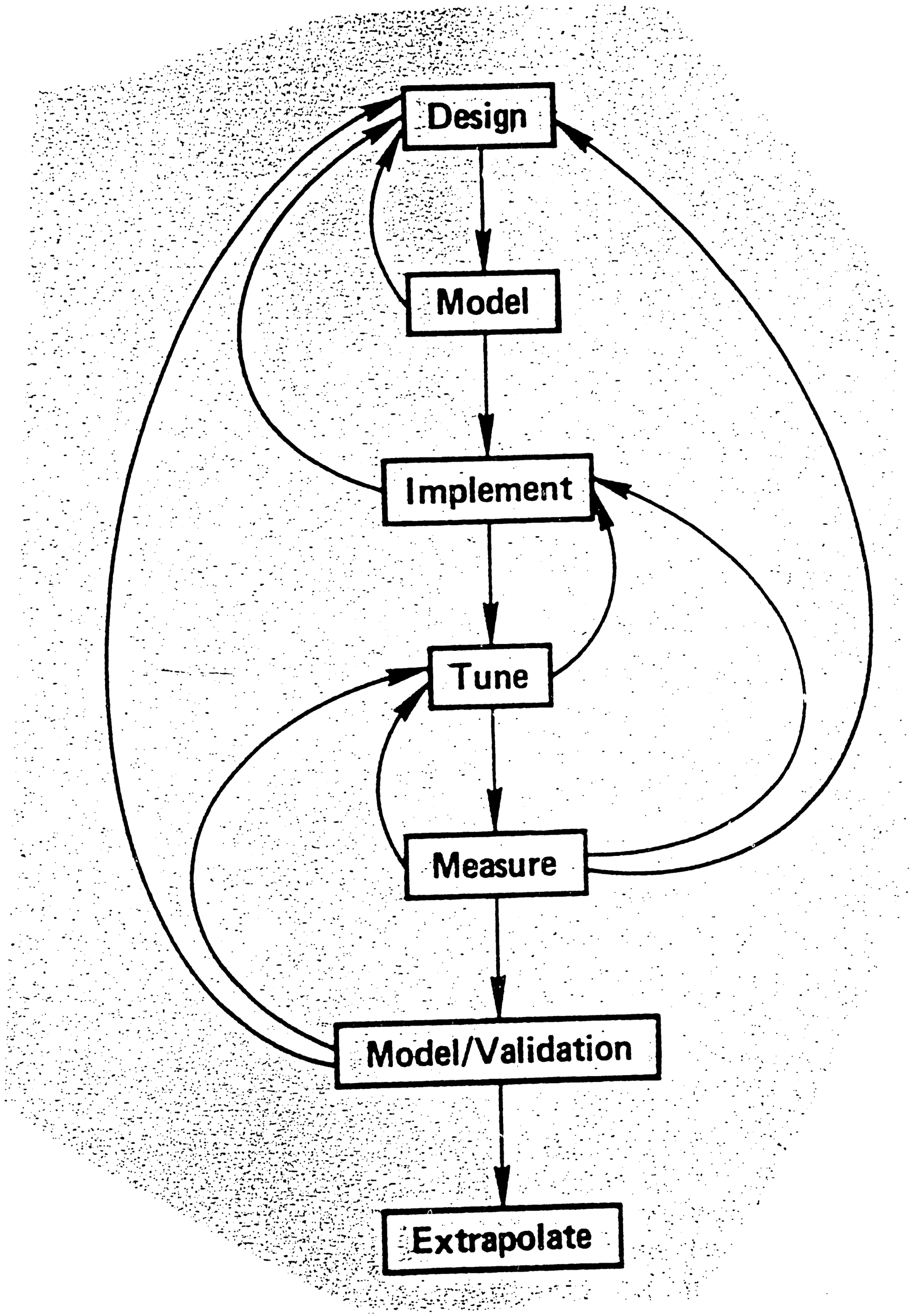

Design
Model
Implement
Tune
Measure
Model/Validation
Extrapolate

Figure 5.0

easy to determine network message queues, node-to-node transmission delays, and network throughput on a per node basis. However, timming problems arise. It is almost impossible to synchronize software across the network such that all measurement periods cover the exact same period of real time. Also, if the network itself is used for continuous collection of the measurements at a central site then network performance will be affected by load due to the monitoring process. Finally, such complex monitoring software could become quite expensive.

The direct approach of monitoring the transmission medium is clearly going to be cheaper than the software method and will provide precise measurement of throughput over arbitrarily small or large periods of time. Disadvantages of the direct method stem from the fact that message queue length is indeterminable. For this reason transmission delay can only be inferred and then only during periods of low loads (no message queues).

5.1.2 Model Validation

The importance of having a correct model should be obvious. It is therefore necessary to have a method of validating a model. Requirements every LAN model

validation process should meet (according to Watson [8]) are discussed below.

The model validation process should be able to determine that sequence and timing for frames of the lowest level protocol exchanged in a simple two adapter (NIU) configuration are exactly duplicated in sequence, and statistically and acceptably approximated in timing.

The model should also be able to predict network performance in a three node, two data path configuration with one path high speed while the other is lower speed. This is known as the message switch configuration and is helpful because of its sensitivity to adapter buffer management and to certain aspects of lowest level protocols. Specifically, the high data transfer path will operate at its maximum rate, while the slow path will attempt to transmit at various lower rates. Simulation results show that the fast and slow paths interfere with each other under these circumstances.

Finally, the validation process should ensure that the model can measure and model the sequence and timing of the exchanged frames in a four node, two path configuration. Again, the goal is to verify that the model exactly duplicates the sequence of exchanged frames and suitably approximates their timings.

The above model validation process shares many of the

problems existing in performance monitoring methods. In order to validate the model, the LAN being modeled must be subjected to experiments in which it is controlled in some precise way that can be duplicated by the model. This usually entails modifying the operating system of hosts involved in the validation experiment so that they use the network in some computationally meaningful way. For example, it is helpful to be able to submit messages to the network which have nice distributions in size and arrival time. Finally, not only must the experimenter control the presented load precisely, he/she must also have some way of measuring the network's response to load with equal precision. This can be done with software or with direct transmission medium monitoring.

5.1.3 Extrapolation

Extrapolation in the context of LAN's deals with determining realms of performance which can only be reached by means of computer simulation. Extrapolation has been the traditional use of simulation. It helps in the design of future LAN's that may be able to achieve these realms of performance.

Extrapolation can also be used directly in modeling

and simulation. The layered nature of network functionality, in both hardware and protocols, lends itself to an incremental model construction technique. That is, once there is confidence in modeling and simulation of lower layers, it is possible to add on layers of higher functionality. This can lead to a highly complex model which can consume large amounts of computer resources in simulation. Extrapolation can be used to replace lower layers with simpler components that imitate (simulate) actual behavior. This can be done by characterizing lower layers using data derived from monitoring studies. This will be illustrated in greater detail in the following modeling methodology section.[3]

5.2 A Methodology for Building a Simulation Model for LAN's

This section describes in detail the LAN modeling methodology developed by I. Chlamtac and R. Jain at Digital Equipment Corporation [9] who saw the need for a method of building LAN models for simulation which would provide efficient design and performance analysis. This

3. Watson, pg. 53.

modeling method should be able to efficiently capture the wide spectrum of software and hardware alternatives and to allow the developer to freely replace system components with minimal programming effort. The method Chlamtac and Jain came up with achieved this modeling flexibility without introducing run time penalty into the resulting simulation programs.

A complete LAN design with multiple segments can require a very complex model. The modeling methodology must provide the ability to configure systems from their basic components in order to build an efficient and flexible software tool. It should also be possible to move the components freely within the system to evaluate alternative designs.

To provide for separate modeling of various software and hardware components, the network should be decomposed vertically along the protocol layers, and for each layer horizontally to separate the software specifications from the hardware used for implementation. The network is viewed as a hierarchy of several layers each consisting of independently modeled functional components - protocols, nodes, and resources. To synthesize an actual system, these components are interleaved (at compile time) within a generic system framework where they communicate via

predefined or user provided services.[4]

The system design builds on modeling flexibility. The design process is divided into several phases where each one concentrates on a different functional or physical system aspect. Each phase or cycle of a phase is repeated until satisfactory finetuning is achieved. In a typical phase, the corresponding network model configuration represents only some network components in full detail, while others are left as rough I/O specifications. This concept was presented in the previous section. Chlamtac and Jain liken it to scanning a large system with a magnifying glass and concentrating each time on only a small and manageable area without losing the effect of the total design on the magnified area.

From the viewpoint of modeling and simulation, the need for modeling, verifying, and running a vast simulation program is replaced by building and executing a larger number of smaller programs each requiring only a fraction of the computer resources. The iterative hierarchical design process and the associated modeling methodology above are described in the following sections. Also, an example of this methodology is presented by explaining the steps of modeling an Ethernet LAN design.

4. Chlamtac & Jain, pg. 58.

5.2.1 Hierarchical System Design

Three principle steps can be identified in the system design process. The first is the identification of the system requirements. A methodology for this was presented in the previous chapter. The second is the formation of design alternatives. This is the job of the LAN designer. The third step is the comparative analysis of alternative designs. This is the impetus for using models. The total process is usually iterative, leading eventually from a coarse system conception to a detailed design that meets performance goals at minimal cost. This process is described below.

In a distributed system like a LAN, the design task complexity and the inherent layered system structure often lead the designer to a fragmented view of the network, treating each protocol layer conceptually as an independent component. This lack of system integration in the design process is also contributed to by the unavailability of software performance tools. Using a conventional one piece system modeling approach leads to programs whose size and complexity make them impractical. To allow for an overall system design in which the total effect of protocol and device choices can be accounted

for, the design model should also be hierarchical to reflect the modeled layered network architecture. This can be done by combining the design requirements in a top down design and the performance needs in a bottom up modeling approach.[5] This is explained below.

First the network requirements are identified at the highest level, and are gradually translated into specific protocol requirements as one moves toward the lowest protocol layer. Then detailed performance modeling begins at the bottom layers and works up using the results of performance evaluation of the model's lower adjacent protocol (if one exists) as the input for the present layer. Its design constraints are dictated by the next higher protocol layer's system requirements. When a satisfactory design is achieved, the full protocol description is collapsed into an I/O specification, and the next protocol layer is entered. This way, detailed models of each protocol layer and its associated nodes and resources are only required one at a time, while all of the lower layers are lumped together as input. The tool used for predicting the input may be analytic, simulation, or a hybrid of the two as long as it is flexible enough to allow for changing the level of modeling detail of all

5. Chlamtac & Jain, pg. 58.

network components and has ease in representing alternative designs. Figure 5.1 depicts this process.

5.2.2 The Modeling Methodology

A local area network is generally described in terms of its architecture, implementation, and topology. The modeling tool developed by Chlamtac and Jain [9] builds network systems by combining network components representing specific protocols, nodes, etc., in a general framework such that the required architecture is obtained. Once a model of a given network is specified the simulation efficiency becomes comparable to that of conventional simulation models. Flexibility is gained by dynamically characterizing distinct systems as collections of interleaved components. The result is a tool suitable for evaluation of architectural as well as performance issues in LAN's.[6]

A network consists of nodes which execute processes governed by communication protocols. These protocols network resources allocated by device specific rules. Components are characterized in a model as:

6. Chlamtac & Jain, pg. 59.

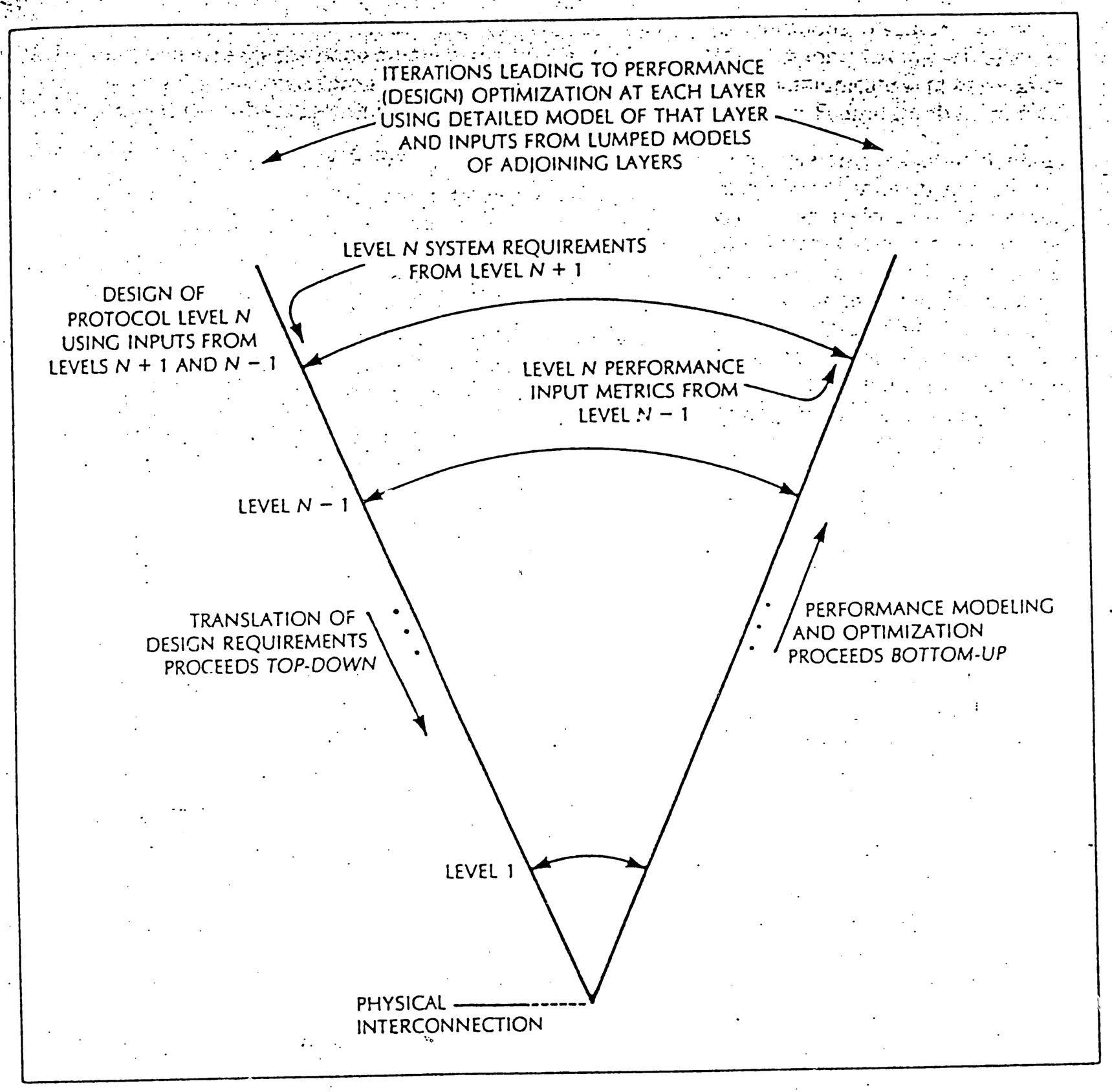

ITERATIONS LEADING TO PERFORMANCE (DESIGN) OPTIMIZATION AT EACH LAYER USING DETAILED MODEL OF THAT LAYER AND INPUTS FROM LUMPED MODELS OF ADJOINING LAYERS
LEVEL N SYSTEM REQUIREMENTS FROM LEVEL N + 1
DESIGN OF PROTOCOL LEVEL N USING INPUTS FROM LEVELS N + 1 AND N − 1
LEVEL N PERFORMANCE INPUT METRICS FROM LEVEL N − 1
LEVEL N − 1
TRANSLATION OF DESIGN REQUIREMENTS PROCEEDS TOP-DOWN
PERFORMANCE MODELING AND OPTIMIZATION PROCEEDS BOTTOM-UP
LEVEL 1
PHYSICAL INTERCONNECTION

Figure 5.1

-- Network: nodes and topology (for point-to-point networks given by links)

-- Nodes: protocols, allocated resources and resource association rules

-- Topology: physical network configuration

-- Protocols: rules for various aspects of using the network

-- Resources: processors, memories, and channels.

The network consists of logical and physical components modeled separately but executing in an interleaved manner within a generic network framework. The network model consists of procedures and structures that specify and interconnect various network elements, and manage the dialog between them to build a characterization of a specific network system. The procedures consist of a node manager, protocol manager, and a resource manager, which define node behavior, specify the protocols to be used, and the node and network resources respectively. The structures consist of data structures which store objects representing dynamically generated processes and describe node and network configurations. The framework is characterized by:

Protocol Manager (is protocol specific):

-- specifies the protocols for execution

-- specifies protocol interfaces

-- handles communication processes

-- generates resource requests

-- presents common node manager interface.

Resource Manager (is device specific):

-- controls resource utilization

-- interprets and executes resource requests

-- collects resource related statistics

-- presents common node manger interface.

Node Manager (is node specific):

-- specifies node resources

-- specifies node protocols

-- interfaces between the resource and protocol managers.

Network Configuration (is network specific):

-- specifies the number and type of nodes

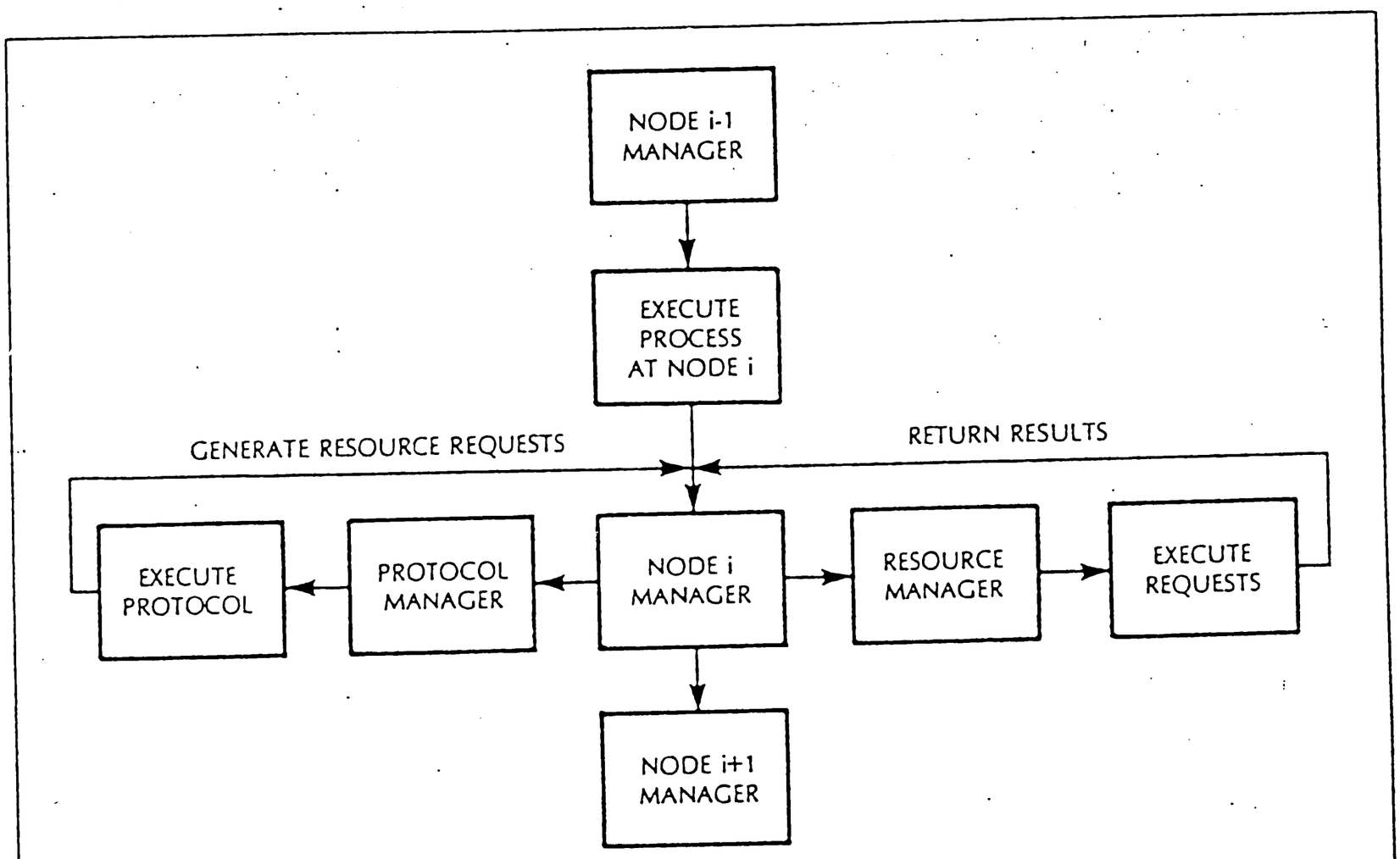
-- gives their relations (topology).

The simulator is fed the above specifications and uses abstractions natural to communications networks to create different classes of networks and node objects. To create the objects, the simulator uses protocol, resource, and network topology specifications that are modeled independently of each other. Objects communicate with each other via node managers. The control flow is process

oriented. This can be seen in Figure 5.2.

In the network configuration phase, node objects are created. Every class of node object specifies its protocols and resources to be used in executing functions required by the simulated network. A given process related request is originated at the end of the network and then flows through the network adhering to the protocol rules specified at each node it passes while consuming the node's resources. At a node that becomes active (one that reacts to a communication request) the node manager assumes control and chooses the correct protocol(s) to be engaged. As in a real system, a protocol must have available resources to execute a request. These requests are passed as parameters to the node manager which engages the resource manager routine and records them for statistical purposes.

After the request execution, the manager returns values such as the time spent executing a given request and the availability of the resource. Using these values, the node manager can permit the protocol manager to continue execution or schedule its renewal after some (un)conditional delay. After the execution of the appropriate protocol has been completed, the node manager invokes the manager of the next network node as needed.



Comment: Nodes i-1, i, i+1, . . . execute network processes in the order determined by the protocols. A typical process can be transmitting a terminal connection request from the terminal (node i−1) via an intermediate node; to the host computer (node i+1). The node manager in each case identifies the request and evokes the required level of protocol, as determined by the protocol manager. The node manager relinquishes control of the process after all its protocols have executed (i.e., acted upon the process requests by evoking the various node resources), and the control is passed to the next node, if any.

Flow of control in the model.

Figure 5.2

From the information on LAN's which has been presented so far in this thesis, several advantages of this methodology for modeling computer networks should become apparent. With respect to modeling ease and flexibility, this approach requires modeling only N + M + K network components to produce N * M * K possible network configurations. This is based on a network with N protocol layers of M variants, and K classes of nodes. The equations above are derived from the fact that changes such as the replacement of a protocol module, inclusion of a new type of device, or the protocol migration between nodes only require the change of one of these independently modeled components. This decomposition of the model into independent protocol and resource models is convenient because protocol specification and existing resource models can be directly incorporated into the simulator with interfacing taken care of by the various managers. A final advantage of this methodology results from the fact that the approach provides modeling flexibility without penalty to run time efficiency. This efficiency is achieved at both the network configuration and model execution phases of model implementation.[7]

The network is configured during the compilation

7. Chlamtac & Jain. pg. 61.

stage. Procedures and managers representing a given network configuration are linked before the model program is executed. Execution is unique in that unlike existing simulators, it enables routines representing various model components to use a standard way of communication. These points are explained below.

By providing compatibility between different protocol and resource model components through their managers, all recognizing a basic set of primitive operations, the above standard communication protocol is achieved. For example, a given resource does not need a special code to handle requests for each one of the protocols using it. This means that adding new protocols doesn't increase the amount of code to be written and executed beyond the code needed for the new protocol description. Otherwise, the amount of code for resource management would increase as alternative protocols were investigated. Also, for this method, all procedures are able to directly pass parameters between themselves with the exact procedure chosen to model a component in a given simulation run being transparent. If this were not the case, each time a different protocol is invoked the right code segment for it would have to be located and eventually the simulator program would spend most of its time locating code

segments.[8]

Each manager provides an easily accessible handle on statistics associated with its attached network component. This saves time because the statistics for each component can be collected from a single point of reference in the program in a way analogous to an actual network where test data is associated with a node, a protocol, or a resource.

This methodology is helpful in gaining a better understanding of the behavior of the modeled system because decomposition into protocols and resources reflects the two main aspects of a computer network's behavior. One is the correctness of its protocols and the other is the utilization of its resources. The ability to collect statistics and to monitor each component through its respective manager makes the simulator very useful in analyzing the protocol properties and network performance. An example of this methodology applied to an actual LAN design is presented in the next section. This should help the reader get a firmer grasp of how it works.

8. Chlamtac & Jain, pg. 61.

5.2.3 A LAN Model Implementation

The following example demonstrates the above modeling methodology on an Ethernet LAN as presented by Chlamtac and Jain [9]. However, the type a LAN is not the important issue here. Instead the steps taken to model a LAN using this methodology are emphasized. The LAN consists of an unspecified number of nodes and uses three protocol layers. For the sake of simplicity, all nodes are considered homogeneous and are connected to a single cable. To implement the model the topology, protocols, nodes, and workload, must be specified. Each of theses items will be addressed in the following subsections.

5.2.3.1 Network Topology Implementation

The simulated network will consist of any number of nodes which can communicate directly if on the same segment or through a bridge/gateway if on different segments. The nodes are numbered uniquely and each segment is characterized by a segment vector. A segment vector contains the physical and logical addresses of all the nodes on that segment in addition to the physical distance each node from either the beginning of the cable or a specified node in the case of a ring. This makes it

possible to calculate all propagation delays. Connections between different segments can be represented by an internetwork matrix which specifies the gateway nodes connecting two segments. For communication between nodes of nonadjacent segments a routing algorithm must be used to choose the required route. This may be implemented by placing additional gateway information in the internetwork matrix. The information could specify the next gateway along a fixed route between two nonadjacent segments. Distances between nodes on different segments are computed from respective segment vectors using the internetwork matrix for correct gateway specification. The following page contains examples of segment vectors and internetwork matrices.

5.2.3.2 Node Implementation

A node is characterized by a physical location and by its specified node manager. In addition, its associated data structure and workload must be given. During a simulation run, information about the node's state is maintained. This information is partly static and contains a list of resources and protocols local to the node for the duration of the simulation, as well as the list of remote resources and protocols available to it. The use of

local or remote resources can only be obtained through the resource manager. The remainder of the information maintained by the resource manager is dynamic and is discussed below.

A resource can be either dedicated to a specific node (like a CPU) or shared between nodes (like the transmission medium). In either situation the way the resource is used depends upon the node's state when the request is made and also upon the state of the node which has the resource. In either case, dedicated or shared, the resource manager handles the rules for resource utilization. Since a resource is not node specific, the information needed for the correct resource request must be dynamically stored in each node which uses the resource. Therefore, if several nodes are using the same type of processor which is represented by a single resource manager, the resource manager can execute requests using independent node state models. In the case of a shared resource, access made to it will always be made through a node or device which is local to it. As a result, any device specific information must also be associated with the resource (in addition to state information collected by the nodes).

A good example of this is the Ethernet cable. The channel is a resource shared among all nodes connected to

it. Nodes that want access (the node managers are in charge of this) must first issue a channel allocation request. This requires two sets of information for its representation. The first set is local to each node and records the use of the channel by collecting the number of unsuccessful requests presented to the channel device. This information is needed for correct node management because it affects the choice of retransmission strategy and is also necessary for statistics collection. The second set of information for representation of a channel allocation request is device oriented and is kept at the device-resource manager. For this example this would be the cable resource manager and would consist of keeping track of all the requests which are currently pending. Device state information is necessary in order to collect information not locally available to the cable requesting nodes. This would include such things as conflicting requests. The state information is also necessary for device statistics collection such as cable utilization.

5.2.3.3 Protocol Implementation

The number and type of protocol layers which may be represented in a single model can vary dynamically without

having an affect on the node or resource description. The effect of implementing a different number of protocol layers is evident in the workload description (amount of header information in each frame). This will consequently affect the size of the frames to be transmitted in the protocol manager.

The example to be presented here will be an implementation of Ethernet's Data Link Layer. Most of the higher order protocols can be modeled by directly coding protocol specification. For the data link, direct coding would require modeling of frame transmission, reception, and other bit level functions. This kind of detail is only needed for performance purposes if just the Physical Layer characteristics were to be examined. Since for higher level protocol monitoring the frame can be handled as the basic unit of information, it is of interest to show a protocol representation of the Data Link Layer at the frame level.

The Network Layer views the data link as only a supplier and receiver of frames. It is assumed the Physical Layer is executing correct bit transmission at the request of the Data Link Layer. In this case the only resource needed to be considered is the one provided by the channel device. All other data link resource requests, such as CRC computation and testing, are assumed to take

place in zero time. This is a reasonable assumption considering the difference between frame transmission time and hardware executed frame checking. Due to the fact that we are only considering a single data link protocol here the protocol manager is very simple. The implementation of the data link for the model is shown in the flow chart on the following page. If more than one protocol version is to be used at a given level, the protocol manager's function would be to provide the node manager with the requests unique to each protocol. This would include some of the following provisions.

Static versus dynamic routing implementation requires different amounts of information in making decisions. In order to maintain total model flexibility, differences of implementation of two different protocols are resolved in the protocol managers. Similarly, differences in resource implementations are transparent to all but the associated resource managers. For example, broadband or baseband communications differences would be handled by the resource managers. This allows the nodes, protocols, and resources to be modeled independently of each other. This means different network configurations can be obtained by freely combining together devices, resources, and protocols. However, to add a new device or protocol, it is

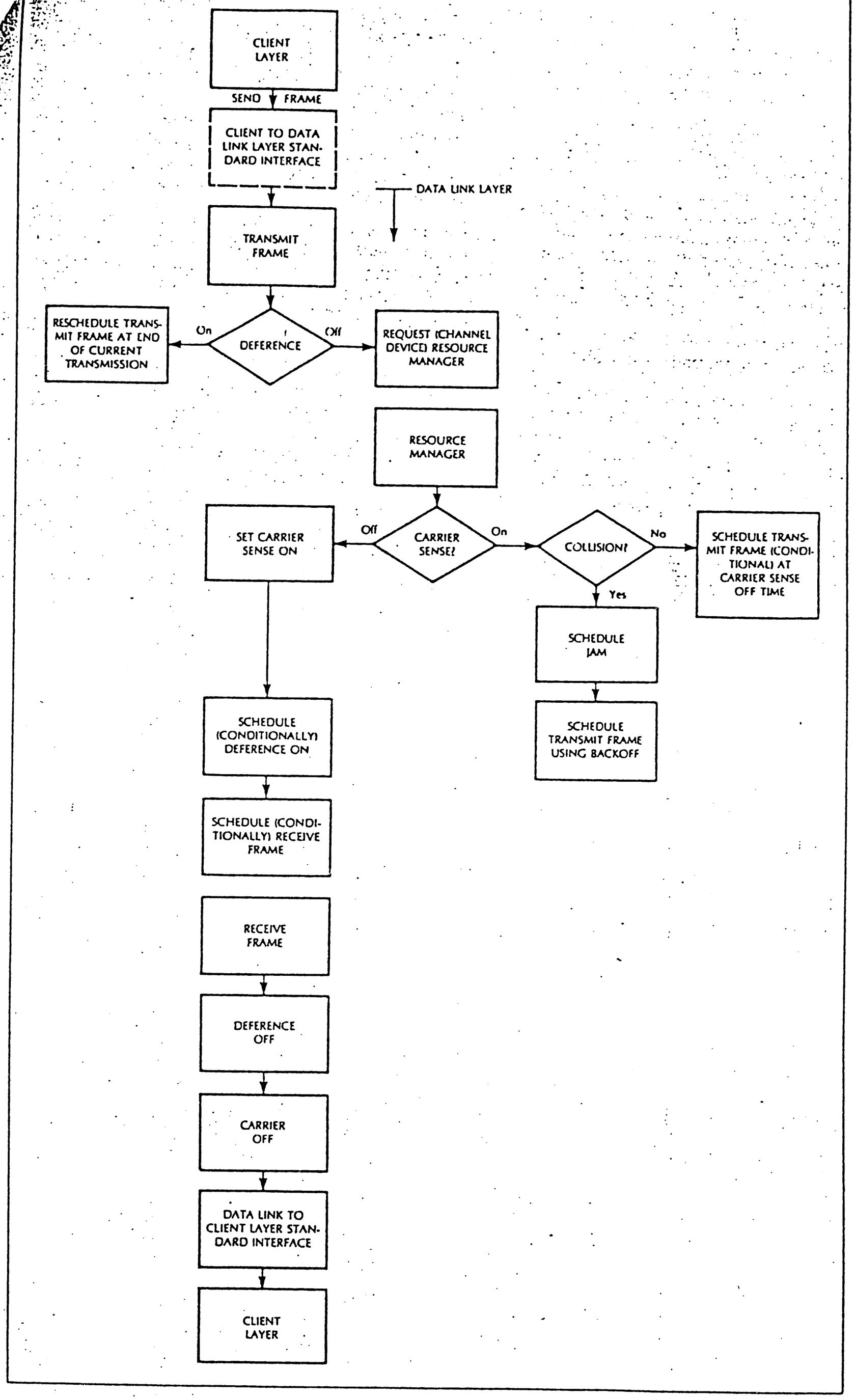

CLIENT LAYER
SEND FRAME
CLIENT TO DATA LINK LAYER STANDARD INTERFACE
DATA LINK LAYER
TRANSMIT FRAME
RESCHEDULE TRANSMIT FRAME AT END OF CURRENT TRANSMISSION
On
DEFERENCE
Off
REQUEST (CHANNEL DEVICE) RESOURCE MANAGER
RESOURCE MANAGER
SET CARRIER SENSE ON
Off
CARRIER SENSE?
On
COLLISION?
No
SCHEDULE TRANSMIT FRAME (CONDITIONAL) AT CARRIER SENSE OFF TIME
Yes
SCHEDULE JAM
SCHEDULE TRANSMIT FRAME USING BACKOFF
SCHEDULE (CONDITIONALLY) DEFERENCE ON
SCHEDULE (CONDITIONALLY) RECEIVE FRAME
RECEIVE FRAME
DEFERENCE OFF
CARRIER OFF
DATA LINK TO CLIENT LAYER STANDARD INTERFACE
CLIENT LAYER

Figure 5.4

possible a new manager may be needed.

5.2.3.4 Workload Specification

This implementation of an Ethernet model will use an open workload. This means that transactions arrive, wait for service, and then depart from the system. The transmission time will be the difference between departure and arrival. This is usually a better representation of a transaction based system, such as an airline reservation system, than a closed system. In a closed system, the user waits a random 'think time' after each request and then generates the next request. The number of requests generated depend upon the system speed. This may be an adequate representation of a program development environment, but it doesn't represent an application environment. In most applications, the time between transaction arrivals is governed by the outside world, not the system or a terminal user. The user will have a fixed typing speed which will result in queueing at the terminal if either the user or the system is slow. These considerations lead to the choice of an open system.[9]

An open system is easier to model and, more

9. Chlamtac & Jain, pg. 64.

RETAKE

The Operator has Determined that the Previous Frame is Unacceptable and Has Refilmed the Page in the Next Frame.

possible a new manager may be needed.

5.2.3.4 Workload Specification

This implementation of an Ethernet model will use an open workload. This means that transactions arrive, wait for service, and then depart from the system. The transmission time will be the difference between departure and arrival. This is usually a better representation of a transaction based system, such as an airline reservation system, than a closed system. In a closed system, the user waits a random 'think time' after each request and then generates the next request. The number of requests generated depend upon the system speed. This may be an adequate representation of a program development environment, but it doesn't represent an application environment. In most applications, the time between transaction arrivals is governed by the outside world, not the system or a terminal user. The user will have a fixed typing speed which will result in queueing at the terminal if either the user or the system is slow. These considerations lead to the choice of an open system.[9]

An open system is easier to model and, more

9. Chlamtac & Jain, pg. 64.

importantly, if the number of potential sources of the load is large compared to the number that are in queues at any given time, an open system is a very good approximation of a transaction oriented system. This is the case for Ethernet and other office LAN's as well as for several other environments. The open system used in the simulation may be modified to model closed systems by the concept of 'following transactions' which is explained below.[10]

The model should maintain three tables which completely define workload. They are: 1) the Transaction Definition Table, 2) the Terminal Definition Table, and 3) the Concentrator Definition Table. Of these, only the first is strictly part of the workload while the other two are part of the system definition. However, a combined explanation of the three tables makes the concept easier to understand. A concentrator is a node on a LAN which has one or more terminals attached to it. Each terminal is used to execute one or more different types of transactions. Thus, there is a hierarchical relationship among concentrators, terminals, and transactions.

The Transaction Definition Table specifies the characteristics of different transactions. The

10. Chlamtac & Jain, pg. 64.

Transaction definition table.

Transact. type	Terminal Input #	Terminal Input Size	Terminal Output #	Terminal Output Size	File server ID	File server Input #	File server Input Size	File server Output #	File server Output Size	CPU time ms	Print server ID	Following transaction #	Following transaction Size	Following transaction Type	Following transaction Time	Priority
MAKRES	3	36	4	80	D1	9	512	5	512	312	L2	3	1024	SHORES	9 ms	3
SHORES																
CANRES																

Terminal definition table.

Terminal type	Output rate char/sec	Input rate char/sec	Transaction Type	Transaction Rate	Transaction Type	Transaction Rate	Transaction Type	Transaction Rate
RESTTY	950	10	SHORES	6/HR	MAKRES	2/HR		
SUPTTY	30	5	CANRES	1/HR				

Concentrator definition table

Concentrator type	Model	Terminal Type	Terminal How many?	Terminal Type	Terminal How many?	Terminal Type	Terminal How many?
TRAGNT	GANDALF	RESTTY	28	SUPTTY	3		
AIRPRT							

Figure 5.5

characteristics are basically resource requirements such as the number of terminal inputs and size of the terminal inputs. If a transaction results in the generation of another transaction, it is specified in the 'following transaction' field of the transaction table. A following transaction may, in turn, also have a following transaction. This allows a sequence of events to be chained together. The time between the end of a transaction and the beginning of the following transaction is the following transaction time and is similar to the think time in a closed system. The number and sizes of resource demands can be specified as a distribution such as normal, constant, uniform, exponential, etc.

The Terminal Definition Table specifies the activities at different terminal types. A terminal can execute many different types of transactions. For each type of transaction, the rate at which transactions arrive at the terminal is specified. The terminal input rate (typing speed) and output rate (line speed) are also specified in the terminal definition table.

Finally, the Concentrator Definition Table specifies the number and types of different terminals attached to each concentrator type. Also, the model name or type of the concentrator is specified in this table. Examples of

these three tables are given on the following page.

5.2.3.5 Network Configuration

As with most modeling techniques, this methodology allows the user to either use standard library modules for network configuration and for output specification or to write their own routines for one or both of these functions. A typical use of a system involves several steps which are presented below.

The first step is network configuration. Here the user specifies the required topology by "inputting" the physical relations between nodes and the segments. Then system configuration specifies physical devices such as CPU's and buses to be used in the network. Next, protocol configuration is used to specify protocols for the simulation run. System implementation then takes place so that associations are created between devices and the protocols to create network nodes. Next, workload configuration is required to create the processes to be run in a given test of the LAN model. Finally, simulation management takes place to specify simulation control parameters, such as the length of run time, the number of messages to be monitored in the program, the required confidence interval, and the percentiles to be collected.

5.2.3.6 Simulation Methodology

For a large simulation program to become a useful tool, several requirements must be satisfied. For openers, the user interface must be friendly. In the case of a design tool, this means that in addition to easy input, users can add their own routines in a general purpose language. This should be possible without necessity of providing tools essential to simulation such as the control program, event handling routines, and statistic collection. The simulation program must also be very efficient in execution to permit within a reasonable amount of time the large numbers of runs needed to evaluate alternative protocols, to determine where functionality should reside, and to allow generation of a sufficiently large number of observations at all network components. Finally, in a complex program, the output routines must be able to efficiently hardle the large amount of data, such as calculations of distributive moments, medians percentiles, etc., without being prohibitively expensive in terms of storage requirements [11] and without excessively slowing down program execution.

11. Chlamtac & Jain, pg. 65

A simulation control program generally executes processes consisting of events. Each event is represented as a routine in a general purpose language and interfaces with other routines via standard interfaces handled by protocol, node, and resource managers. As a result, as long as users comply with interface requirements, they can substitute their own routines. To satisfy requirements of the simulation environment, the user is provided with primitives to execute, schedule, and cancel events. Each primitive completely specifies the event or routine on which the control program is to act.

Given that a simulation of networks with several hundred nodes may be required, the ability to handle large event sets efficiently is a must. The handling of events (maintaining an ordered set of events on which primitive routines can execute) is provided by an event handling algorithm that can execute efficiently even when there is a large event set. The event handling algorithm can be conveniently implemented in a general purpose language. It is not necessary for the language to have dynamic memory management. FORTRAN will work without loss of efficiency or storage penalty. This feature is obtained by storing pending events in a data structure based on queues of events.

Finally, there must also be a method of handling the large amounts of data generated. One way of doing this is by collecting all model statistics on the fly without storing observations. This can be done by some of the well known dynamic algorithms for finding moments. There are also some new heuristic algorithms to do this with percentiles. They have a small fixed storage requirement and operate dynamically. Specifics of these algorithms are beyond the scope of this thesis.

5.2.3.7 Collecting Statistics

A distributed system such as a LAN communicates by creating and processing messages. At the same time it is consuming resources. The statistics of interest can be collected by monitoring the individual messages, the sequences of messages that constitute a process, and the utilization of the various network resources. All of these tasks are accomplished naturally by the model. Every resource is accessed by a resource manager that records its use and dynamically computes the required statistics.[12]

The ability to collect statistics locally is an

12. Chlamtac & Jain, pg. 65

important aspect of a LAN model. Message (process or task) related statistics are collected by having each message carry time stamps relevant to the statistics in question. Every message is simply a collection of data necessary for protocol communication. For performance modeling, the message is augmented by a time stamp which records its progress through the network. In the program, messages are pointed to rather than moved between the node's data structures. Information representing a message changes as it moves through the network. Such things as time and additional headers are recorded as necessary and stored in common message (transaction) space. In this way, a total response time for a message or process at the data link protocol is obtained by simply accessing the pool of messages as required.

5.3 Summary

This chapter has presented a methodology for modeling LAN architecture so LAN's may be simulated prior to implementation. The advantages of modeling before implementation were discussed. These included most notable the fact that many alternative designs can be tested in order to find the best architecture for a certain

application at the minimum cost. The modeling methodology presented achieves most of the requirements necessary for a modeling technique while still providing an efficient design and performance analysis.

SUMMARY

This thesis is primarily concerned with presenting a methodology for capturing networking needs of a particular facility and modeling these needs for simulation and testing. Prior to presenting the methodology fundamentals of local area networks as required for implementation are discussed. Because of its timely thrust toward standardization of LAN specifications for the manufacturing environment, an overview of the General Motors Manufacturing Automation Protocol (MAP) is included

The first two chapters covered fundamental concepts of LAN's including descriptions of the ISO model for OSI, topology, transmission media, switching techniques, protocols, and the network interfacing unit. Also presented were some issues important to LAN's including performance, internetworking, and design issues. Discussion of these concepts and issues is intended to give the reader a better feeling for problems which should be taken into consideration when designing, testing, and implementing LAN's.

Chapter Three presents the latest results of the MAP committee's effort to define a standard for local networks in the manufacturing environment. This chapter outlines specifications set down by General Motors for future vendors supplying communications equipment. The rational for particulars of these MAP specifications is also discussed. This chapter gives the reader insight to the decision process used in choosing an architecture for a particular application.

Chapter Four presents a methodology for capturing networking requirements of a facility. This methodology was developed at Lehigh University. It employs a formalized data collection process to describe the networking communications requirements of a plant or office building. Results of this methodology can be used by a LAN designer to propose an appropiate network architecture and alternatives for given requirements.

Chapter Five continues with the next logical step in the network design process, modeling of proposed alternative designs. A methodology is presented for building models suitable for efficient design and performance analysis of LAN's. Also, reasons for constructing computer models as well as steps involved in validation are covered. The modeling methodology is shown

to allow alternative designs to be rapidly modeled for simulation.

The final step before actual implementation of the proposed LAN design is simulation of LAN models. Aspects of a good simulation program are discussed, along with features of a modeling methodology which can make analysis through simulation easier. Ideally, results of using these methdologies will produce the best LAN design at the lowest cost for a given set of communications requirements. It is hoped that research of this thesis will create an interest for further study involving actual simulations (beyond the scope of this thesis).

LIST OF REFERENCES

[1] Stallings, William, Local Networks, New York, New York: Macmillian Publishing Company, 1984.

[2] Tanenbaum, Andrew, S., Computer Networks, Englewood Cliffs, New Jersey: Prentice-Hall Inc., 1981.

[3] Chorafas, Dimitris, N., Designing and Implementing Local Area Networks, New York, New York: McGraw-Hill Book Company, 1984.

[4] Chorafas, Dimitris, N., Computer Networks, New York, New York: McGraw-Hill Book Company, 1985.

[5] Stuck, W. and Arthurs, J., A Computer and Communications Network Performance Analysis Primer, Englewood Cliffs, New Jersey: Prentice-Hall Inc., 1985.

[6] Manufacturing Automation Task Force, General Motors' Manufacturing Automation Protocol Specification Version 2.1, Detroit Michigan: General Motors Publications, 1985.

[7] Lehigh University Center for Design & Manufacturing Innovation, "Manufacturing Systems Analysis and Design Methodology Report", Lehigh University, Bethlehem, PA, April, 1986.

[8] Watson, W. B., "Modeling and Monitoring a LAN, One Experience", NBS Publication, pp. 32-55.

[9] Chlamtac, I. and Jain, R., "A Methodology for Building a Simulation Model for Efficient Design and Performance Analysis of Local Area Networks", Simulation, (February 1984), pp. 57-66.

VITA

Mark Stickler is a graduate student in the Department of Electrical Engineering and Computer Science at Lehigh University. He is concentrating in Computer Engineering and is specifically interested in Local Area Networks. He will recieve his M.S. in Electrical Engineering in June of 1986. He recieved his B.S. in Computer Engineering from Clemson University in December of 1984. He was also involved in the Cooperative Education Program as an undergraduate. During this time he worked for Motorola's Communications Division for four semesters. At the graduate level he worked as a Senior Techinical Assistant for Bell Laboratories during the summer of 1985. Mark was born November 1 st, 1962 and is the son of Mitchell G. and Janet E. Stickler.