Theses and Dissertations   1. Thesis and Dissertation Collection, all items

1991-09

Selection and specification of a data link protocol for VSAT based inter-LAN communications

Benvenutti, Eugene S., Jr.

Monterey, California. Naval Postgraduate School

https://hdl.handle.net/10945/28523

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

SELECTION AND SPECIFICATION OF A
DATA LINK PROTOCOL FOR VSAT BASED
INTER-LAN COMMUNICATIONS

by

Eugene S. Benvenutti, Jr.

September, 1991

Thesis Advisor: G.M. Lundy

Approved for public release; distribution is unlimited.

Unclassified

Security Classification of this page

<table>
<tr><td colspan="4" align="center">REPORT DOCUMENTATION PAGE</td></tr>
<tr><td colspan="2">1a Report Security Classification Unclassified</td><td colspan="2">1b Restrictive Markings</td></tr>
<tr><td colspan="2">2a Security Classification Authority</td><td colspan="2" rowspan="2">3 Distribution Availability of Report
Approved for public release; distribution is unlimited.</td></tr>
<tr><td colspan="2">2b Declassification/Downgrading Schedule</td></tr>
<tr><td colspan="2">4 Performing Organization Report Number(s)</td><td colspan="2">5 Monitoring Organization Report Number(s)</td></tr>
<tr><td>6a Name of Performing Organization
Naval Postgraduate School</td><td>6b Office Symbol
(If Applicable) 39</td><td colspan="2">7a Name of Monitoring Organization
Naval Postgraduate School</td></tr>
<tr><td colspan="2">6c Address (city, state, and ZIP code)
Monterey, CA 93943-5000</td><td colspan="2">7b Address (city, state, and ZIP code)
Monterey, CA 93943-5000</td></tr>
<tr><td>8a Name of Funding/Sponsoring Organization</td><td>8b Office Symbol
(If Applicable)</td><td colspan="2">9 Procurement Instrument Identification Number</td></tr>
<tr><td colspan="2" rowspan="2">8c Address (city, state, and ZIP code)</td><td colspan="2">10 Source of Funding Numbers</td></tr>
<tr><td colspan="2">Program Element Number | Project No | Task No | Work Unit Accession No</td></tr>
<tr><td colspan="4">11 Title (Include Security Classification) Selection and Specification of a Data Link Protocol for VSAT Based Inter-LAN Communications</td></tr>
<tr><td colspan="4">12 Personal Author(s) Benvenutti, Eugene S.</td></tr>
<tr><td>13a Type of Report
Master's Thesis</td><td>13b Time Covered
From To</td><td>14 Date of Report (year, month,day)
1991 September</td><td>15 Page Count
79</td></tr>
<tr><td colspan="4">16 Supplementary Notation The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.</td></tr>
<tr><td colspan="2">17 Cosati Codes
Field | Group | Subgroup</td><td colspan="2">18 Subject Terms (continue on reverse if necessary and identify by block number)
VSAT, LAN, Data Link Protocol, Systems of Communicating Machines, Specification</td></tr>
<tr><td colspan="4">19 Abstract (continue on reverse if necessary and identify by block number .

This thesis proposes an architecture for the development of inter-LAN communication across a VSAT network. The architecture of a VSAT node consists of the entities *node, bridge, buffer, transmitter, receiver,* and *frame assembler/disassembler*. Each of these entities contains a finite state machine, predicate/action tables, and local variables.

A selective repeat, sliding window data link protocol for the VSAT architecture, the *transmitter* and *receiver*, is formally specified using the systems of communicating machines model. A partial analysis of the specified protocol is performed using reachability diagrams.</td></tr>
<tr><td colspan="2">20 Distribution/Availability of Abstract
[X] unclassified/unlimited ☐ same as report ☐ DTIC users</td><td colspan="2">21 Abstract Security Classification
Unclassified</td></tr>
<tr><td colspan="2">22a Name of Responsible Individual
G.M. Lundy</td><td>22b Telephone (Include Area code)
(408) 646-2094</td><td>22c Office Symbol
CS/Lu</td></tr>
</table>

DD FORM 1473, 84 MAR   83 APR edition may be used until exhausted   security classification of this page

All other editions are obsolete   Unclassified

Selection and Specification of a Data Link
Protocol for VSAT Based Inter-LAN Communications

by

Eugene S. Benvenutti, Jr.
Captain, United States Marine Corps
B.S., United States Naval Academy, 1985

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(SPACE SYSTEMS OPERATIONS)

from the

NAVAL POSTGRADUATE SCHOOL
September 1991

Rudolf Panholzer, Chairman, Space Systems Academic Group

ABSTRACT

This thesis proposes an architecture for the development of inter-LAN communication across a VSAT network. The architecture of a VSAT node consists of the entities *node*, *bridge*, *buffer*, *transmitter*, *receiver*, and *frame assembler/disassembler*. Each of these entities contains a finite state machine, predicate/action tables, and local variables. Entities communicate by reading from and writing to shared variables.

A selective repeat, sliding window data link protocol for the VSAT architecture, the *transmitter* and *receiver*, is formally specified using the systems of communicating machines model. A partial analysis of the specified protocol is performed using reachability diagrams.

TABLE OF CONTENTS

I. INTRODUCTION

The past twenty five years has seen rapid changes in the technologies of computers and communications. As computers have proliferated, the need to economically connect geographically distant computing resources has increased. Terrestrial private lines have been the primary means to interconnect computers in the past. Unfortunately, these lines offer poor to moderate reliability and limited flexibility. While the costs for these lines have been rising, innovations in satellite communication technology have made data communications using low cost *very small aperture terminals* (VSAT) a viable alternative.

A. PURPOSE OF THESIS

The intent of this thesis is to develop a formal specification for communication between *local area networks* (LANs) using VSAT terminals as a bridge. The specification will cover LANs that adhere to the Institute for Electrical and Electronic Engineers (IEEE) Standard 802.3 for *carrier sense multiple access* with *collision detection* (CSMA/CD). The *Open System Interconnection* (OSI) reference model is used as a basis for examining the lowest two layers of the VSAT network. Alternatives for a data link protocol are examined and a recommendation given. A selective repeat protocol for this layer is then specified and an analysis is performed. The specification of the data link layer protocol is based upon the *system of communicating machines* (SCM) proposed by Lundy and Miller [Ref. 1]. It is expected that the VSAT bridge specified using this model may be easily modified to accommodate communications between other LAN standards, such as the token ring and token bus LANs.

B. OUTLINE OF CHAPTERS

Chapter II discusses computer networks and protocols. It uses as a framework the OSI model for communication networks. Each layer of the OSI model is briefly discussed, with the lower layers emphasized. It then looks at LANs specified by the IEEE 802 series standards.

Chapter III looks at current corporate VSAT applications and the components of a VSAT network. An architecture for the VSAT based interconnection of remote LANs is introduced. Advantages and disadvantages of VSAT based LAN internetworks are discussed.

Chapter IV examines issues relating to the data link layer of a VSAT network such the nature of network traffic, required throughput, and allowable delay. Several candidate protocols are analyzed and a recommendation made for the network of LANs.

Finally, Chapter V will specify the data link protocol using the SCM model and perform an analysis to ensure that it is free from deadlock. Conclusions and recommendations for further study will be contained in Chapter VI.

II.   COMMUNICATION NETWORKS

If two devices wish to share information or pass data, there must be a communication path between them. Sometimes it is practical to establish a direct point-to-point link between the two devices, or *hosts*, but what if we need to communicate between more than a single pair of hosts? If faced with running direct lines between more than a very few hosts the task becomes imposing. If we need to connect N hosts then the number of lines required is:

$$\frac{N(N-1)}{2}$$

Communication networks offer a way around this problem. If an application a running on a host A has data to send to an application b on host B, with access to a common network, A passes the information to the network software resident in the same machine. The network is now responsible for ensuring that this information is now sent from node to node until it reaches host B. The network software on this host then passes the data to application b. [Ref. 4:p. 193-195]

This chapter will introduce the methods of classification for communications networks. It will then examine network architectures and discuss the *Open System Interconnection* model for computer networks. Finally we will take a more detailed look at the various types of *Local Area Networks* (LANs).

A.   CLASSIFICATIONS OF NETWORKS

Communication networks may be categorized by three different criteria: their size, their shape, and their method for routing information from node to node.

1. Geographical Coverage

In classifying a network by geographical coverage we are essentially looking at its "footprint." By the size of this footprint we may classify the network as either a *Local Area Network* (LAN), *Metropolitan Area Network* (MAN), or *Wide Area Network* (WAN). Knowledge of network size may also give us insight into the technology used. For example, it would be rare indeed for a network of computers in the same building to use microwave relays as a means to exchange data!

a) *LAN*

LANs are computer networks that occupy a size on the order of a college campus or smaller. They usually use twisted pair or coaxial cable as their connecting medium, though the use of optical fiber is becoming more widespread, and offer data rates of from 1 to 100 Mbps. Because of their relatively small size and simplified routing schemes, LANs do not require all of the layers of software that larger networks do. There are several different standards for LANs. These will be discussed in a later section.

b) *MAN*

MANs are about the size of a city as the name implies. They use a combination of connecting mediums from coaxial cable to microwave relay. An example of a common MAN is a cable TV system. The only currently formalized standard for computer MANs is IEEE standard 802.6. This standard, known as *Distributed Queue Dual Bus* (DQDB), will allow network lengths of up to 50 km and data rates of 45 to 150 Mbps across an optical fiber medium.

c) *WAN*

WANs are the largest and most complex of all networks. These networks rely on satellite communication, terrestrial microwave, and long haul leased data lines as

their communication media. Data rates currently range from 50 kbps to 1.544 Mbps with data rates of 45 to 155 Mbps projected for the near future. The international telephone network is an example of a WAN. Many layers of software are needed to handle complexities such as routing, congestion, error and flow control across the WAN. Also, some WANs are an aggregation of many smaller networks. In this case an additional layer of software must handle the difficulties of moving data between the different networks, or *internetworking*. Most of these software layers are described in the OSI network architecture described later.

2.   Topology

While geographical coverage classified networks by their size, topology classifies them by their shape. If we look at the connections between nodes on a network we may see a pattern. This pattern is the topology. Topology can be described as five different "shapes": fully connected, ring, star, bus, and tree. If a network does not fit into any of these categories then it is classified as "irregular." All of these topologies except the bus are a series of point-to-point links that allow information to be routed from one node to another until it reaches its destination. The bus topology is different in that every node can talk directly to every other node through the use of a shared data "bus." Figure 1 graphically shows the six different topologies.

3.   Switching Technique

Switching classifies networks by the manner in which data is routed from the sender to the receiver. Devices at each node take data off of incoming channels and place it on the appropriate outgoing channel as determined by software algorithms. The data is thus *switched* from node to node until it reaches its destination. [Ref. 4:p. 196]

5
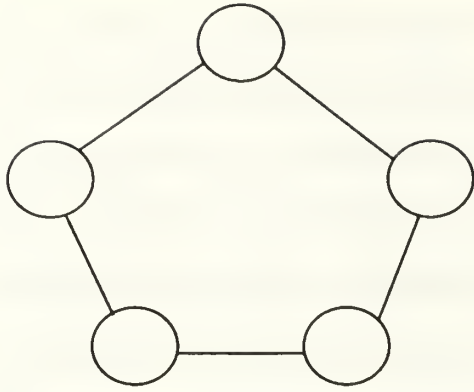
RING
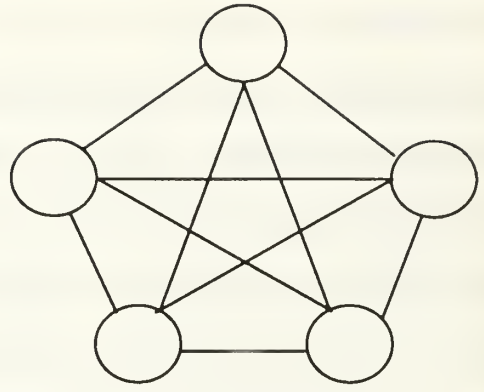
FULLY CONNECTED

STAR

IRREGULAR

BUS
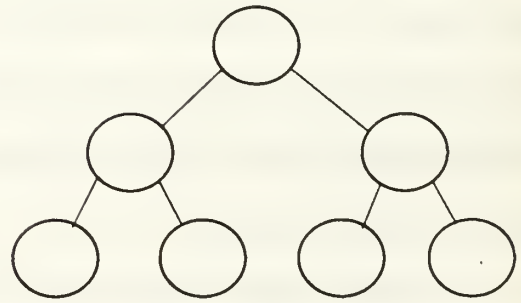
TREE

Figure 1: Network Topologies

6

a) Broadcast Networks

Broadcast networks use the simplest possible switching: data is passed directly from sending to receiving node via a shared communications medium so transmissions by one node are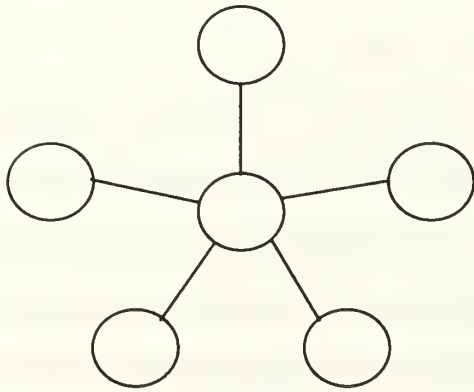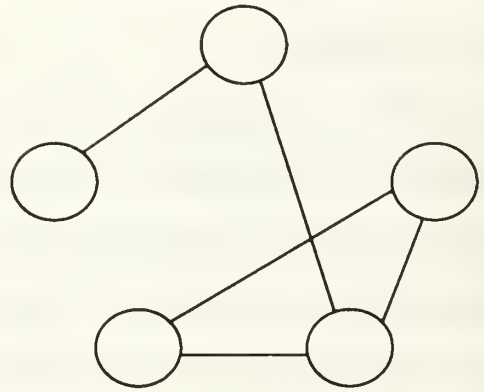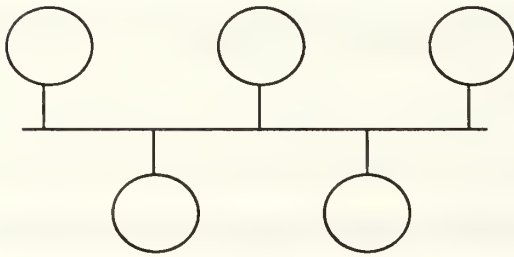 received by all. Examples of this type of network are packet radio networks, satellite networks, and LANs. [Ref. 4:p. 207]

Sharing a communication medium raises problems that must be solved by software. If two hosts transmit simultaneously, a collision occurs and neither message gets through. A method to control access to the transmission medium is necessary to minimize collision and to resolve collisions successfully when they occur. This layer of software, called the *medium access control* (MAC), resides in the data link layer of the OSI architecture and will be discussed in detail in Chapter IV.

b) Circuit Switching

Circuit switching establishes a dedicated path between two hosts that wish to communicate. Because a connection must be established prior to the transmission of data, this type of switching is known as *connection oriented*. This path is a series of links from node to node that lead from the sending node to the receiving node and is in place for the duration of data transfer session. The public phone system is an example of a circuit switched network. [Ref. 4:p. 197]

There are three distinct phases to a data transfer session on a circuit switched network. The first phase, *circuit establishment*, sets up an end-to-end circuit. The initiating station ties into its node and requests a connection to the receiving station. This node determines the next link in the chain based upon routing algorithms and availability and sends a request for a channel to that node. Once that is done the two lines are "patched" together. This proceeds until the node that the destination station is attached to is reached. If the receiver is available, the sender is notified and the *data*

7

transfer phase begins. After the exchange of data is complete, the *circuit disconnect* phase is initiated by one of the two hosts. This frees the allocated resources for use by other calls. [Ref. 4:p. 197-198]

Circuit switching is advantageous because it allows the continuous exchange of data such as voice across a network in a manner that is transparent to the user at either end, but it has some major drawbacks. First, both sender and receiver must be prepared for the data exchange. If the receiver is not ready, the sender gets a busy signal and must try again later. The time taken to set up the circuit is wasted and must be done again when the sender calls back. The second major drawback is that circuit switching wastes capacity. Even if there is no data being transmitted, the circuit is reserved for use by the two parties involved.

c) *Message Switching*

Message switching avoids wasting capacity in the manner of circuit switching. This method of switching works much like the postal system. If you wish to send a letter to a friend, you put the letter in an envelope and give it to your postman. It doesn't matter if your friend is ready to read it or even if he's home at that time. Similarly, if a station has information to send, such as a large data file, it places a network address on it and passes the entire package to the network node. The node looks at the address, consults its routing algorithm, and sends it on to the next node. No direct link is established, so this is *connectionless* service. Eventually the message will reach a node to which the destination is attached and be delivered. If traffic between two nodes on the path is heavy, the message can be rerouted or stored by a node until it can be sent. The primary disadvantage of message switching is that it is unsuitable for real-time data. [Ref. 4:p. 198-201]

8

d) Packet Switching

Packet switching performs similarly to message switching except that large messages must be broken down into smaller fixed-length packets of a few thousand bits. Each of these packets is individually addressed and transmitted. As these packets are passed to the network they may be handled in two ways. The first is referred to as *datagram packet switching*. This procedure treats each packet as an independent message that may take a different route to its destination. Because packets do not follow one behind another they may arrive at their destination in the wrong order. To enable the receiving station to reassemble the packets into a coherent message, the sending station tags each packet with a *sequence number*. Datagram service is connectionless. [Ref. 4:p. 201-202] [Ref. 3:p. 88-89]

The second approach to packet switching establishes a logical connection, or *virtual circuit*, between the sender and receiver. This method, a connection oriented service, is very similar to circuit switching in that the three phases are the same. The route must be determined and the receiver must be ready, the data must be transferred, and the connection must be terminated. The difference is that with virtual circuits, the links from node to node are not dedicated. Instead, each packet is given a label that corresponds to the virtual circuit it is using. The nodes take each packet and place it in a queue for the appropriate link. Because the circuit is established in advance, nodes are not required to make a routing decision for each packet, thus reducing their load. Also, since every packet follows the same path through the network, the receiver is ensured of getting them in the proper order. [Ref. 4:p. 202-203]

Figure 2 based on diagrams in [Ref. 3:p. 88] and [Ref. 4:p. 204] depicts the relative performance of the above switching techniques.
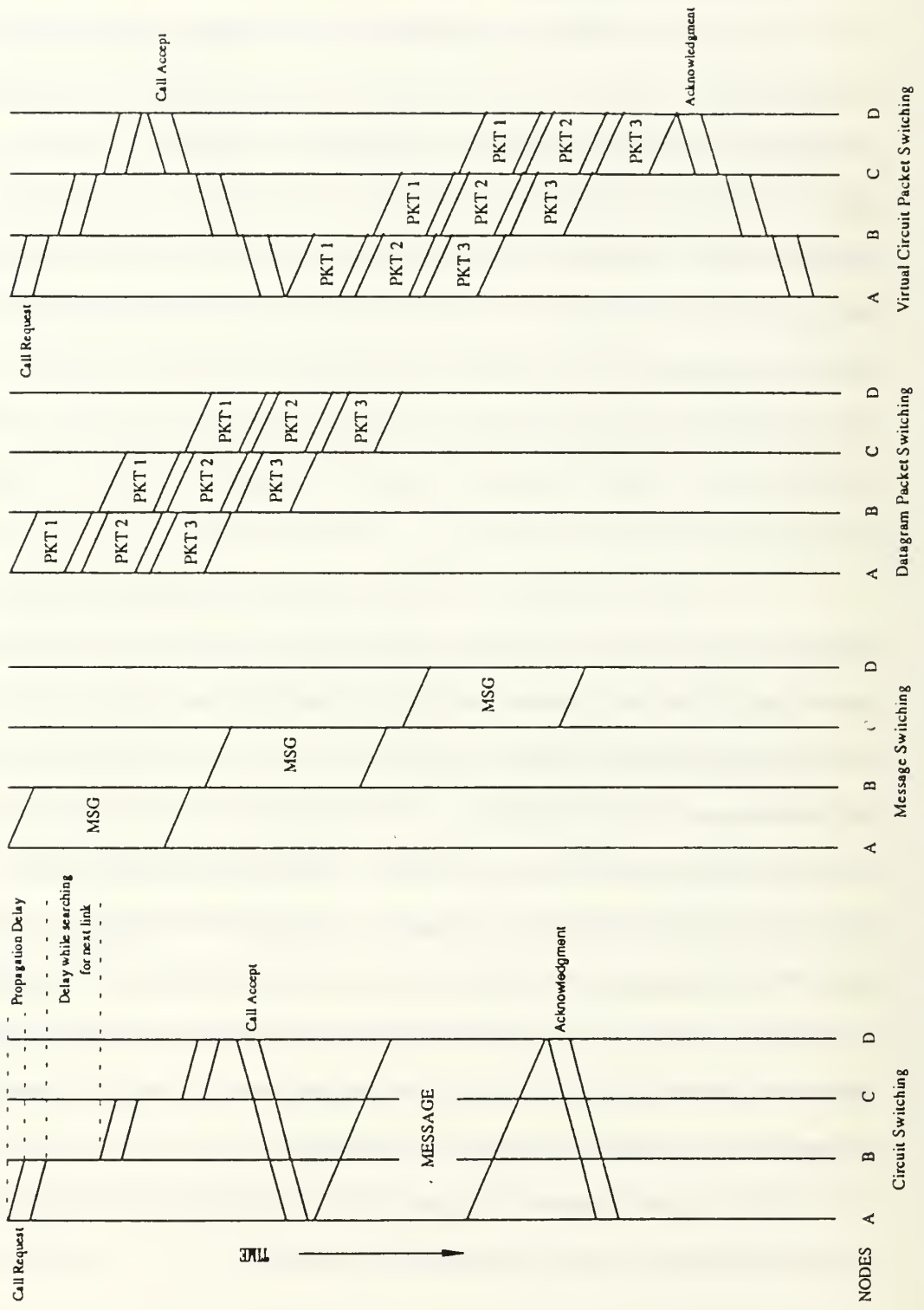
Figure 2: Event timings for switching methods. Source: [Ref. 5:p. 204]

10

B. NETWORK ARCHITECTURE

A designer faced with the task of designing and implementing a computer network from the top down would probably be overwhelmed by the magnitude of the task. Fortunately, standard architectures have been developed that greatly simplify the matter. These architectures divide the communication process into functional "layers." Each layer offers a group of "services" to the layer directly above while hiding from them the implementation details. The rules that govern the functionality of an architectural level is its *protocol*. The architecture specification provides details that allow implementers to build hardware and write programs that obey the protocol of the level for which it is meant. [Ref. 3:p. 9-11]

Physically, there is an interface between each pair of levels that allow a level to take data from the level directly above, add some control information that is particular to the protocol, and pass this to the layer directly below. This process continues until the information is in a form suitable for transmission across the physical medium. At the receiver the reverse process is carried out. Data packets come up from the layer below, protocol specific information is stripped and any necessary actions performed, and what remains is passed up the chain.

Because the implementation details of lower levels are hidden from higher levels, level *n* on machine A carries on a conversation with level *n* on machine B. These are known as peer processes. Logically, all communications are from peer to peer [Ref. 3:p. 10]. Figure 3 illustrates the relationships in a four layer architecture.

Several organizations have put forward standards for network architectures. The three most prominent of these are the *International Organization for Standardization* (ISO), the *Institute of Electrical and Electronic Engineers* (IEEE), and the United States

11
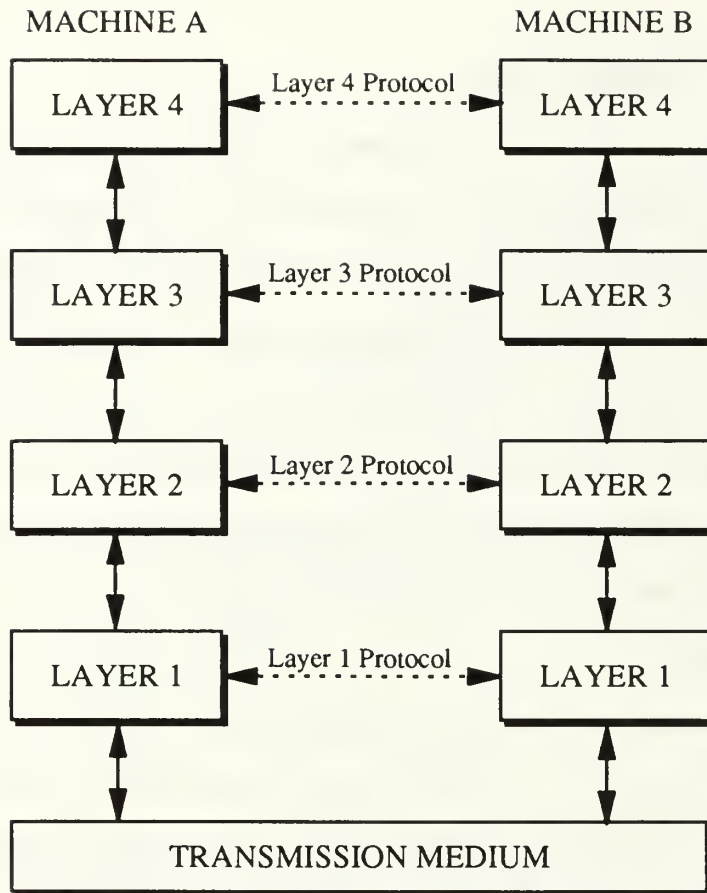
Figure 3: Relationships In A Four Layered Architecture. Source: [Ref. 2:p. 10]

Department of Defense (DoD). The IEEE standards are the de facto standards for LANs, while the OSI architecture is gaining growing recognition as an international standard. As such, we will only concern ourselves with these two.

C. THE OSI MODEL

The ISO network architecture is known as the *ISO Open Systems Interconnection Reference Model* and is commonly referred to as the OSI model. This model is a hierarchy of seven layers: physical, data link, network, transport, session, presentation, and application. The designers of this reference model created layers such that each layer

contains functions that are manifestly different in process and technology or where a different level of data abstraction exists; yet they attempted to keep the model from having too many layers and becoming unwieldy. Required interactions across boundaries were minimized as much as possible. Also, a prime consideration was to keep changes made in one layer from affecting the layers above or below it. [Ref. 4:p. 391]:

These layers function as described above with each taking "data" from the layer above, encapsulating it, and passing it on to the next layer below. Figure 4 depicts the seven layers and their interaction. The following sections will look at the lowest four levels in some detail. The upper three levels will briefly have their services described.

1.   The Physical Layer

The physical layer is responsible for moving bits from point A to point B. Typical issues dealt with at this level are bit representations and timings, modulation methods, and physical connections. The ultimate goal of this level is to ensure that there is a viable path over which bits can be passed.

2.   The Data Link Layer

This layer is responsible for taking error prone transmissions from the physical layer and making them appear error free to the layers above. To accomplish this, the data link layer forces the sender to divide information into fixed size packets. It then takes these packets and encapsulates them with header and trailer information, called a frame, that allows the data link entity in the receiving machine to determine if a packet was received correctly or in error. Implicit or explicit acknowledgments allow the sender to know what packets have been received correctly and which need to be retransmitted.

13
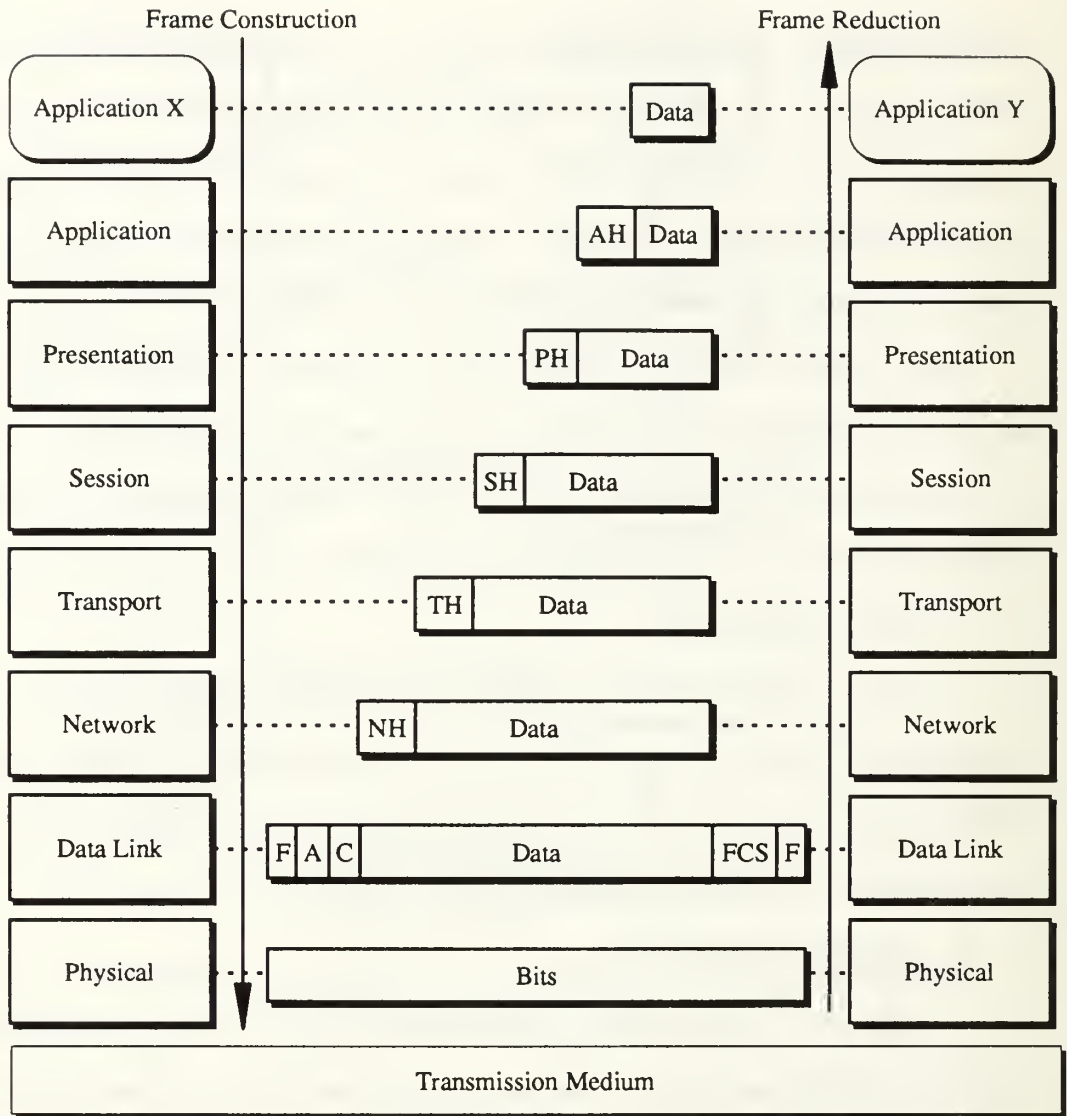
Figure 4: OSI Operation. Source: [Ref. 5:p. 391]

Another function of the data link layer is point-to-point flow control. If a sender is transmitting packets faster than the receiver can handle them, the receivers buffers quickly become full, and data frames are lost. The lost frames must be retransmitted thus adding to the quantity of packets that the receiver is trying to handle and pushing it farther behind. The data link layer is responsible for ensuring that this

does not happen. This is usually accomplished through the use of a "window" that allows a sender to have only a certain number of unacknowledged frames outstanding at any time. If a sender has transmitted a full window, then he must wait for an acknowledgment from the receiver before continuing. This allows the receiver to control the flow of data by withholding acknowledgments.

3. The Network Layer

The network layer is concerned with routing of packets, congestion control across a network, and *internetwork* issues if packets are to move from one network to another. Routing may be either predetermined through the use of tables or dynamic, adapting to the current conditions of the network. If too many packets are following similar routes, bottlenecks may occur. The network layer must ensure not only that packets avoid any existing bottlenecks, but also that the bottleneck itself is removed. Finally, this layer must resolve issues that arise when a message must pass out of the boundaries of one network and into another. These networks may use dissimilar addressing schemes and even entire different sets of protocols. The network layer must handle this transition smoothly and transparently. [Ref. 3:p. 16]

4. The Transport Layer

The transport layer is the first end-to-end protocol and creates a logical connection between sender and receiver. Each of the layers discussed thus far have operated in the various nodes of a network and have been concerned with point to point links. The transport layer resides in the hosts and is concerned with host-to-host error and flow control. It must take large data blocks passed to it by the session layer and subdivide it into smaller packets acceptable to the network layer. It may take a data stream from a single session layer entity and split it into many streams that are transported across the network concurrently and reassemble them at the other end. By

15

the same token, the transport entity may take data streams from several session entities and *multiplex* them into a single data stream for the network to transmit.

Error and flow control are placed in this layer as well as the data link layer to ensure a high quality of service to the user. Typically, the owner of a host does not own the entire network to which it is attached. If service by the network is poor, the transport layer may recover from it with little or no interruption to the higher levels. [Ref. 3:p. 370-373]

5. The Session Layer

While the transport layer is responsible for creating logical a connection, the session layer essentially provides a "user interface" to this basic service [Ref. 4:p. 522]. The basic services that are provided by this layer are session establishment and maintenance, dialog management, and recovery from failures [Ref. 4:p. 398].

6. The Presentation Layer

The presentation layer handles problems relating to the conversion, encryption, and compression of data [Ref. 3:p. 471]. It provides the syntax that is used between communicating applications [Ref. 4:p. 398]

7. The Application Layer

This layer contains the actual user initiated programs, or applications, that are run on the computer. The most common three are remote log on, file transfer, and electronic mail transfer. [Ref. 3:p. 528]

D. LOCAL AREA NETWORKS

Because of their limited scale, LAN architectures generally omit the network layer. Also, the data link layer of the OSI model has been subdivided into *medium access control* (MAC) and *logical link control* (LLC) sublayers.

LANs are logically broadcast networks. Some method for controlling access to the shared transmission medium must be established. This is accomplished in the MAC sublayer by either *contention* or by *token passing*. Contention protocols allow every node on the network to vie directly for idle time. If two or more nodes transmit simultaneously, then a *collision* is said to have occurred. A contention based MAC layer protocol should provide a fair and predictable method for minimizing these collisions and correcting them when they occur.

Token passing protocols avoid the problem of contention by allowing only one station to transmit at any time. This is accomplished by a special frame that is passed from node to node called a *token*. There is generally only one token per network and only the current holder of the token is allowed to transmit. Algorithms within the protocol must prevent one station from holding the token indefinitely.

The LLC sublayer sits on top of the MAC sublayer and provides a common interface to higher layers regardless of the MAC that lies beneath. The essence of this layer is a header field that is added to data packets that are sent down. This header gives source and destination addresses as well as control information. [Ref. 3:p. 265]

The IEEE 802 committee has put forward standards for three types of copper connected LANs. Standard 802.2 covers the LLC sublayer while 802.3 through 802.5 cover the physical layers and medium access control sublayers for *carrier sense multiple access with collision detection* (CSMA/CD), *token bus*, and *token ring* LANs. These standards have been adopted by the ISO as ISO 8802. Token ring and CSMA/CD are the predominant LANs in offices while token bus is chiefly used for real-time applications in industry. The following section will look at the MAC sublayer these three LAN standards.

1. CSMA/CD

This is by far the most common access technique for LANs. It is a broadcast network that was originally developed in the mid 1970's at Xerox as part of their Ethernet LAN and is sometimes (inaccurately) referred to by that name [Ref. 4:p. 349]. The IEEE standard describes a family of CSMA/CD systems that operate at data rates of from 1 to 10 Mbps over a variety of media [Ref. 3:p. 141].

Carrier sensing multiple access is a contention based protocol that can be summed up by the phrase "listen before talk." Anyone that has tried to talk on a HAM or CB radio knows that if you just pick up the microphone and start talking you might talk over someone else, so no clear signal gets through. If you listen to make sure that the channel is clear before you begin your transmission then you stand a better chance of having it get through. If a collision occurs, the sender will wait a random time before trying again. This minimizes the possibility that two stations will continue to collide on subsequent tries. CSMA can be summarized as a four step algorithm:

1. Sense the medium to determine if another station is transmitting.

2. If a carrier is sensed, go to step 1.

3. Otherwise, begin transmitting message and send until it is completed.

4. Determine if a collision has occurred. If so, wait a random time and go to step 1.

The problem with the pure CSMA algorithm is that a station transmits its entire message before trying to find out if a collision has occurred. If a station continues to sense the medium while it is transmitting then this waste can be avoided. If a collision is detected, the sending stations stop their transmission and sends a short "jamming signal" that allows all stations to know that there has been a collision [Ref. 4:p. 350]. The CSMA/CD algorithm is thus:

18

1. Sense the medium to determine if another station is transmitting.

2. If a carrier is sensed, go to step 1.

3. Otherwise, begin transmitting message while continuing to sense medium.

4. If a collision is detected, cease transmission of message and send jamming signal. Go to step 1.

Figure 5 illustrates the frame structure for 802.3 networks. All octets within the CSMA/CD frame, with the exception of the frame check sequence, are transmitted with their low order bits first. The first part of the frame is the *preamble* field. This is a 7 byte field of alternating 1's and 0's that allow the receiver's clock to synchronize with the incoming frame timing. The second field is the *start frame delimiter* field. This field holds the pattern 10101011 and indicates the actual start of the frame. [Ref. 6:p. 24]

The next two fields in the frame are address fields. These fields may be either 2 or 6 bytes in length and hold the *destination address* and *source address* respectively. The choice of either 16 or 48 bit address must be consistent across the network but is left as an implementation decision to the manufacturer. Figure 6 shows the format of both 16 and 48 bit address field formats. Each octet within the address fields are transmitted with the least significant bit first. In the destination field the first bit is used to indicate an individual or group address. If the bit is set to 0, then the field is an address for an individual station on the network. A 1 indicates that the address is for a group of stations on the network. If the 48 bit address is being used then the second bit indicates whether an address is administered locally or globally. Local addresses are ones for a single LAN while global addresses are those administered by the system administrator of several interconnected LANs. [Ref. 6:p. 24-26]

19

Bytes	
7	Preamble
1	SFD
2 or 6	Destinaton Address
2 or 6	Source Address
2	Length
Variable	Data
Variable	Pad
4	FCS

Fields Transmitted Top to-Bottom

LSB MSB

Bits Transmitted
Left-to-Right
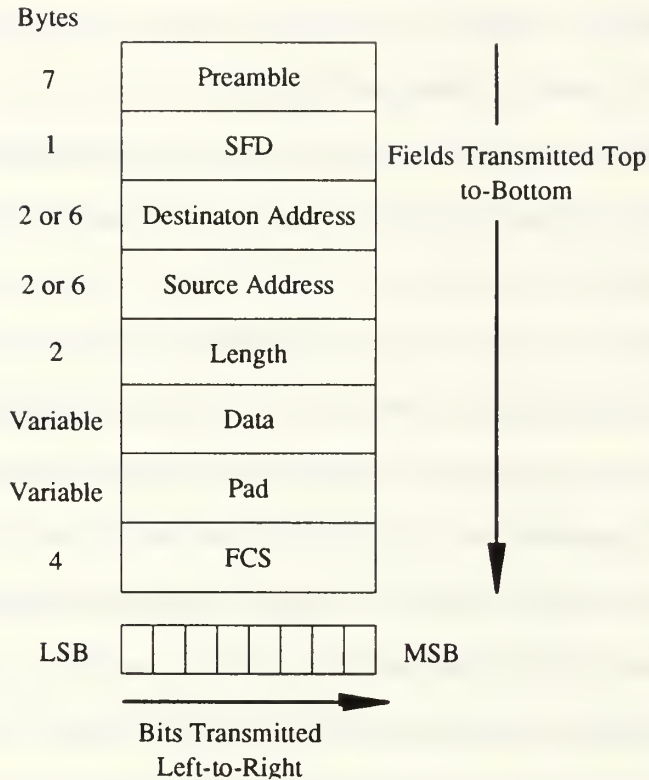
Figure 5: CSMA/CD Frame Format.
Source: [Ref. 6:p. 24]

The *length* field is a 2 bytes and its value indicates the number of bytes of data that follows in the data field. This field is transmitted with the high order octet first. [Ref. 6:p. 26]

The *data* field is where packets passed down by the LLC layer are contained. Maximum sizes for the data field are specified by the particular implementation of the CSMA/CD standard. Each implementation also specifies a minimum length for the CSMA/CD frame. If the data field is not long enough, the *pad* field is used to fill out the frame [Ref. 6:p. 26-27]. Data field lengths range from 0 to 1500 octets while the pad field may be 0 to 46. [Ref. 3:p. 144]

48 Bit Address Format
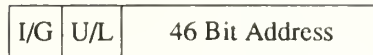
I/G	U/L	46 Bit Address

16 Bit Address Format

I/G	15 Bit Address
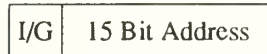
I/G = 0 Individual Address

I/G = 1 Group Address

U/L = 0 Globally Administered Address

U/L = 1 Locally Administered Address

Figure 6: CSMA/CD Address Field Format
Source: [Ref. 6:p. 25]

The final field in the CSMA/CD frame is the *frame check sequence* field. This field contains a 32 bit cyclic redundancy check (CRC) value. This value allows the receiver to check the incoming frame for bit errors. It is computed as a function of the address fields, data field, and pad field. [Ref. 6:p. 27]

2. Token Bus

CSMA/CD's performance is probabalistic so the possibility exists that, under heavy loads, a station may have to wait an arbitrarily long time before sending its traffic. The token bus protocol (IEEE 802.4) alleviates this situation by allowing stations to take turns. If there are n stations on the network and each is allowed to transmit for a maximum of time T seconds, then a station is guaranteed of being able to send data at least every nT seconds. Also, there is no method of prioritization built into the CSMA/CD protocol which makes it unsuitable for some real-time factory automation tasks. Data rates of 1, 5, and 10 Mbps are allowed. [Ref. 3:p. 148]

Token bus is a broadcast LAN in which the stations on the network form a logical ring in which each station knows its predecessor and successor. The token is

21

passed around this ring, allowing each station a chance to transmit. The protocol specifies methods for adding and deleting stations from the ring and also recovery mechanisms for multiple tokens or lost tokens. [Ref. 3:p. 148-153]

A priority scheme is specified which may be used to reserve a fraction of the network's capacity for real-time data, such as voice. Low priority packets are sent only when there is excess capacity. Priorities are defined as 6, 4, 2, and 0 with 6 being the highest. A set of timers within each station determine how much of each type of data may be transmitted while the token is held.

3. Token Ring

The token ring network (IEEE 802.5) is physically a series of point-to-point links that form a circle. As packets are transmitted by a station, they are read one bit at a time by the next station and placed onto the link to the following one. This continues until the packet has returned to the originator, who takes it off of the network. Since every station sees every message, this is logically a broadcast medium even though physically it is otherwise. The 802.5 standard allows implementations of 1Mbps and 4 Mbps.

The basic token ring MAC protocol is very simple. It operates by continuously circulating a three byte token around the ring. When a station has traffic to send it seizes this token and changes the second byte to indicate that what follows is a data frame. It then sends its data until completion. If the station needs to send more data after the first frame, then it may do so as long as its token holding time has not expired. Once it has completed its transmission it then releases a new token.

The 802.5 standard allows 8 levels of priority. The *access control* field in a token ring frame gives the priority of a token. A station may "seize" a token and begin transmitting if its data is of equal or higher priority than that in the access control field.

22

For a data frame, the access control field serves as a reservation mechanism. When a station transmits a frame, other stations may set the reservation bits in this field if their traffic is of higher priority than that already there. When the station that sent the data packet gets the access control field back and is ready to release a new token, it may set the field to the priority of the reservation. Once the station that raised the priority has finished, it releases a token that returns the priority to its original state. [Ref. 4:p. 357]

E. SCM SPECIFICATION OF CSMA/CD

While the CSMA/CD MAC protocol standard was written as Pascal procedures, Lundy and Miller [Ref. 7] have devised an easily understood model for the CSMA/CD protocol using *systems of communicating machines*(SCM). The model SCM combines finite state machines, shared and local variables, and predicate-action pairs to describe a system's states and behaviors.

Figure 7 shows the specification for a network node. State 0 is the initial state of the system. From this state a node may transmit data if the local variable *msg* is not empty and the shared variable *medium* is clear. If no collision occurs then the *OK* transition is taken, returning the node to state 0. If there is a collision then the *collision2* transition takes the node to state 3 and from there back to state 0. The receive transition, *finish*, is enabled when a message with the nodes address appears in the *medium*. Table 1 gives predicate-actions for the network node. This model of a CSMA/CD node will be used as an entity in a VSAT based LAN-LAN bridge. [Ref. 7:p. 7-10]

The CSMA/CD bus is modeled by the shared variable *medium* onto which packets consisting of *address* and *data* fields are placed. The *controller* is responsible for "cleaning" the contents of the bus periodically, thus modeling the ends where signals

23

terminate. Figure 8 is a diagram of the controller and its shared variables. The predicate-action table for the controller is given in Table 2. [Ref. 7:p. 7]
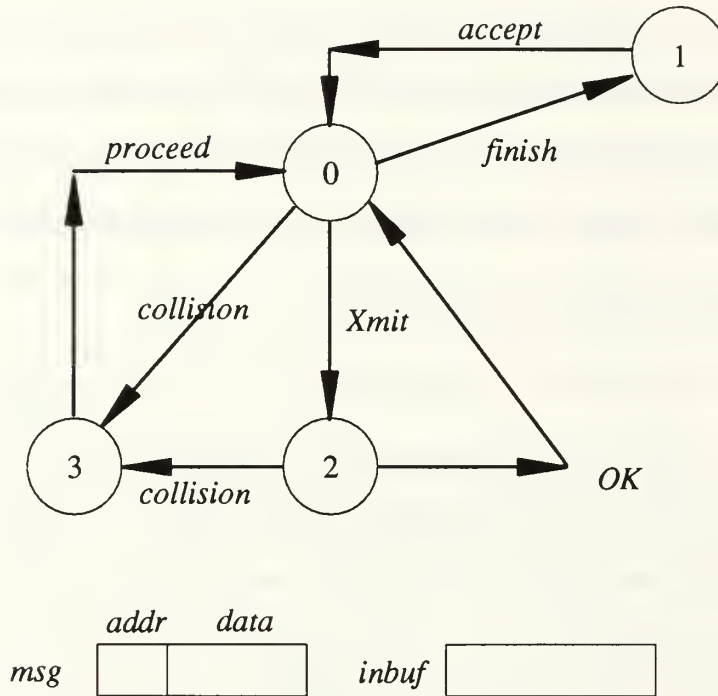
Figure 7: CSMA/CD Node and Variables
Source: [Ref. 7:p. 10]

TABLE 1: PREDICATE-ACTION TABLE FOR NODE. [Ref. 7:p. 8]

transition	predicate	action
Xmit	$msg \neq \emptyset \wedge medium = \emptyset$	$medium := msg;$ $Signal(i) := tranceive$
OK	$Signal(i) = clear$	$msg := \emptyset$
collision0	$medium = garbage$	$Signal(i) := collision$
collision2	$medium = garbage \wedge Signal(i) = clear$	$Signal(i) := collision$
proceed	$Signal(i) = clear$	
finish	$medium.addr = i \wedge Signal(i) = clear$	$inbuf := medium.data$
accept		$Signal(i) := tranceive$

24
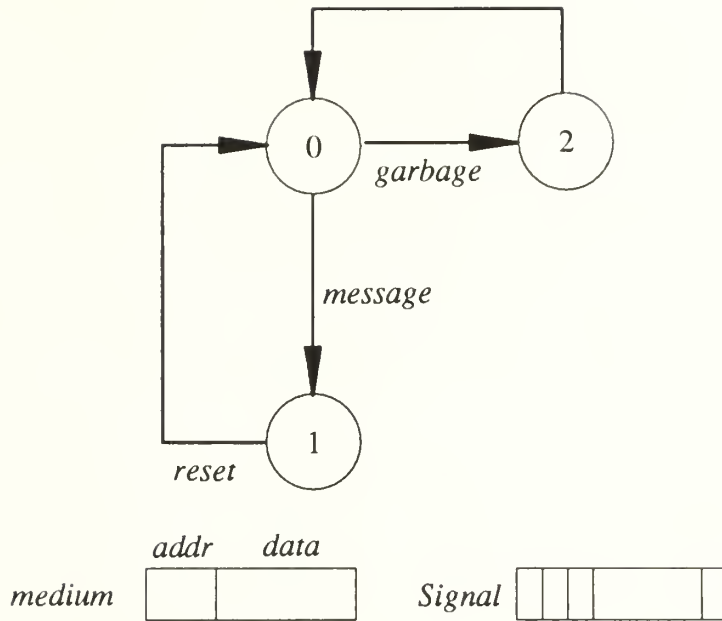
Figure 8: Controller and Shared Variables. Source: [Ref. 7:p. 10]

TABLE 2: PREDICATE-ACTION TABLE FOR CONTROLLER [Ref. 7:p. 10]

transition	predicate	action
message	*medium* ε {*garbage*,∅}	
reset	*Signal*(*medium.addr*) = *tranceive*	*medium* := ∅; *Signal*(1..*n*) := *clear*
garbage	*medium* = *garbage*	
delete	*Signal*(1..*n*) = *collision*	*Signal*(1..*n*) := *clear*; *medium* := ∅

25

III.   VSATs AND THEIR USES

This chapter introduces VSATs. It reviews the components of a VSAT network, the current uses for VSATs in corporate communications, and the advantages of VSAT-based networks. The use of VSATs as a bridge between geographically dispersed LANs is discussed and a potential system architecture for this use is proposed.

A. VSAT SYSTEM COMPONENTS

VSAT systems consist of three major components: a hub, the satellite, and the VSATs themselves. These are usually configured as a star topology network. Messages from the VSATs are sent over a channel shared either by *time division multiple access* (TDMA) or *frequency division multiple access* (FDMA). These access methods allow each VSAT to have all of the available bandwidth part of the time or part of the bandwidth all of the time. TDMA schemes are more responsive to growing and changing networks. More will be said of its different forms in Chapter IV.

Messages moving from the hub to the VSATs are transmitted over a single *time division multiplexed* (TDM) channel. The distinction between TDMA and TDM is that in the former, many stations are transmitting on a shared channel while in the latter only one station is transmitting. VSATs listen to the entire TDM data stream but "grab" only those packets addressed to it.

1. Hub

First, a hub with a large (4-8 m diameter) antenna and front end processor acts as the central network control point and as the main data processor. It is generally located at or near the central offices or corporate headquarters. Network management functions such as protocol and frame changes, frequency and time slot assignment for

26

remote stations, and addition of new stations to the network are accomplished from here. Transmissions from the hub have data rates typically in the range of 56 to 256 kbps. [Ref. 9]

Each hub is capable of handling several thousand VSATs. If a network is not very large, then this huge capacity is not needed and a VSAT network with a dedicated hub may not be economical due to the large initial investment necessary to establish the hub. In order to make VSAT networks a viable alternative for smaller networks, many VSAT vendors have established regional hubs that are shared by several corporate networks. These hubs are owned and operated by the VSAT supplier and the capabilities are "leased" by the users, alleviating the need for both the large capital investment and the cost of a staff dedicated to running the hub.

2. Satellite

The second component is a communications satellite. These satellites are in a geostationary orbit approximately 42,200 km above the equator. From this position, a global coverage beam is able to see 42% of the Earth's surface [Ref. 8:p. 3]. In order to provide high gain for the coverage areas, multiple beams may be used [Ref. 10:p. 55]. The VSAT user leases a transponder in the appropriate coverage region, or a portion of the transponder's bandwidth, from the VSAT provider. Stationkeeping and health and welfare of all systems aboard the satellite are the responsibility of the satellite's owner. To the users of VSATs, the satellite is a relay that takes in all signals on the uplink frequency, shifts them to the downlink frequency, and then retransmits them. The most notable characteristic of the satellite link is the added propagation delay. As a rule of thumb, a signal will take 0.27 seconds to propagate from the sender to the receiver along a single hop satellite link. If there are two hops between sender and receiver, such as might be the case in a star network, then the delay is 0.54 seconds. If the sender is

waiting for a response at the terminal, then he could only hope to see it at 1.08 seconds at the earliest. While this delay may not be intolerable, it would certainly be an annoyance to the user.

3. VSAT

Finally, the VSAT itself is a small (.8-2.4 m) antenna, an outdoor unit consisting of a transmitter (1-5 Watt) and receiver, and an indoor unit with a modem, encoder/decoder, multiplexer/demultiplexer, and digital data interface. The modular design allows easy upgrades of system components and ensures transportability. Because of the small antenna and low transmitter power, communications are normally limited to VSAT-to-hub or hub-to-VSAT, though systems are available that allow VSAT-to-VSAT messages. Data rates for low-end VSATs typically range from 56 to 128 kbps.

B. VSAT USES

Frequency bands used in satellite communications are generally referred to by a letter designation. This is a hold-over from World War II attempts to hide exact radar frequencies from the enemy. Through the years the letter designations were declassified, modified, and generally abused [Ref. 8:p. 181]. It is unknown whether this subterfuge confused our opponents, but it certainly causes difficulties for communication engineers since there is no recognized standard. The two frequency bands of interest to VSAT communication are the C and Ku bands. Generally, the C band of the radio frequency spectrum is considered to range from 3.7 to 6.425 GHz while the Ku band extends from 10.7 to 18 GHz [Ref. 8:p. 212].

The first VSAT networks used C-band satellites for one way point-to-multipoint communications. These early VSATs had antennas of 0.6 to 1.2 m and spread spectrum technology in order to minimize interference with terrestrial microwave and adjacent

satellites. The need for an interactive capability led to the introduction of two-way VSATs using C-band, but these systems were limited to bit rates of around 9600 bps and suffered from interference problems. Today, C-band VSATs are used by news organizations and others that are primarily concerned with broadcasting information to geographically dispersed locations [Ref. 9].

Most new VSAT data networks utilize Ku-band satellite channels. These are free from ground-based microwave interference and offer a larger available bandwidth, hence higher potential data rate. These networks have found a wide variety of uses in corporate data communications:

- Point-of-sale information is gathered and transmitted to central computers for order processing, credit authorization, and inventory control.
- Automatic teller machines are connected to the central office for transaction approval and processing.
- Terminals are connected to a central data base for use in hotel and airline reservation systems.
- Corporate teleconferencing and private phone systems.
- Broadcast of corporate training films and in-store audio/video advertisements to branches.

Table 3 lists a few current networks for both C and Ku-bands.

TABLE 3: CURRENT VSAT NETWORKS. SOURCE: [Ref. 9]

CORPORATION	# OF VSATs
Associated Press	3200
Dow Jones & Co.	2600
Farmer's Insurance	2500
Reuters	2000

C-BAND VSAT NETWORKS

CORPORATION	# of VSATs	USE
Chrysler	6000	Batch data, voice, video.
WalMart	2100	Batch data, voice, video.
Holiday Corp.	2000	Batch data, interactive reservation service.
Merrill Lynch	2000	Video, voice, outbound data.
Xerox	1500	Service for time-sharing customers.
A.L. Williams	1200	Interactive data.

Ku-BAND VSAT NETWORKS

C. ADVANTAGES OF VSAT SYSTEMS

1. Service

Service on a VSAT network can be entirely controlled by the user. Installation and testing of the new VSAT can be done by personnel in the using organization. In order to integrate a new VSAT into a network, network management must make frame changes that allow the new VSAT to access the link. This is done through commands issued from the network hub, which is run by the using organization. There is no outsideagency that must be dealt with in case there are changes that must be made to the network.

If there are any difficulties with the service, the user is dependent upon the leased line provider for tracking down and correcting the problem. Since the

deregulation of the telephone system this is increasingly difficult. The local phone system may blame the regional carrier, who can blame the next region, and so on until the other end of the line is reached. Any disputes over service and billing must be negotiated to the satisfaction of all parties. When difficulties crop up with a VSAT network there are no disputes over who is at fault. The blame rests squarely with the VSAT provider, allowing a rapid resolution.

Natural disasters such as earthquakes and unnatural ones such as a backhoe slicing through a cable can wipe out communications paths on a terrestrial network. VSAT networks are immune to this type of problem. Also, VSATs are capable of providing a lower bit error rate than that of leased data lines.

2. Network Flexibility

Modifying a terrestrial network can be both costly and time consuming. In order to add nodes, it is necessary to install leased lines to the site. The user has no direct control over the installation an setup process because he is dependent upon an outside agency for service. It is entirely possible that delays of weeks or months may be encountered before service can be initiated. Installing or moving nodes on a VSAT network is simple. All components are modular and easily transported to the site. The installation procedure is simply erecting and pointing the antenna and attaching the interface to the local network. Any necessary frame changes can be initiated from the hub.

3. Cost Comparison

Leased line pricing usually uses a 1.544 Mbps line, or T1 carrier, as a basis for cost comparison. Price for a line increases as a function of distance and required bit rate. A typical 1000 mile long T1 link costs about $10,000 per month while a 500 mile T1 link runs about $6,000. If a full 1.544 Mbps is not needed, a fractional T1 can be leased

at rates of 384, 512, and 768 kbps. A 1,000 mile long 512 kbps line will cost approximately $7,000 per month. These prices do not include the cost of any terminating equipment and circuits needed ar either end of the line. [Ref. 11:p. 357-362]

Prices on VSAT remote sites range from $6,000 to $20,000. For small networks of less than 200 remote sites, shared hubs allow many networks to utilize the same central ground station for network control. These shared hubs are owned and operated by the VSAT provider, thus the initial capital outlay costs. For larger networks, it becomes economical to operate a dedicated hub for networks of between 200-300 nodes [Ref. 9]. Table 4 shows rough cost estimates for a dedicated hub network of 325 remote sites and a shared hub with 100 sites.

D. VSATs AS A BRIDGE BETWEEN LANs

An ideal VSAT application is linking the various LANs in a widely spread organization. For even moderately sized corporate networks, VSATs can be a viable alternative to terrestrial links. Figure 9 shows a network that links two LANs in a star topology. Within this physical framework, a logical architecture that supports the communication process resides. We will look at an architecture that is specified by using the systems of communicating machines model. We will deal with CSMA/CD LANs as this is the most frequently used LAN. An SCM specification for the CSMA/CD LAN [Ref. 7], can be used as one of the components of the bridge. Because all communication between machines is done through shared variables, other LAN standards can be easily linked using the same logical architecture. Figure 10 illustrates the logical relationships between machines and variables for the two LAN network of Figure 9.

32

TABLE 4: COST ESTIMATES FOR TWO VSAT NETWORKS. SOURCE: [Ref. 9]

Dedicated Hub	Lease Rate: 2.00%		Term: 5 yr		325 Sites
Item	Unit Cost		Quantity	Cost/mo.	Cost/mo./site
VSAT					
Equipment	$10,800		325	$70,200	
Installation	$3,400		325	$22,100	
Maintenance	$65	/VSAT/mo.	325	$21,125	
HUB					
Equip. & Inst.	$1,300,000		1	$26,000	
Maintenance	$7,500	/mo.	1	$7,500	
SATELLITE	$15,150	/mo.	1	$15,150	
TOTAL				$162,075	$499
Operating Costs				$43,775	$135

Shared Hub	Lease Rate: 2.00%		Term: 5 yr		100 Sites
Item	Unit Cost		Quantity	Cost/mo.	Cost/mo./site
VSAT					
Equipment	$11,000		100	$22,000	
Installation	$3,600		100	$7,200	
Maintenance	$65	/VSAT/mo.	100	$6,500	
HUB SERVICES				$9,200	
BACKHAUL				$2,600	
TOTAL				$47,500	$475
Operating Costs				$18,300	$183

1. Logical Composition of the VSAT

The VSAT on each of the LANs is composed of six separate finite state machines along with variables that allow them to communicate. In order to function on the CSMA/CD network, there is a CSMA/CD *node*. This machine is identical to the SCM specification in Chapter II. The variables *inbuf* and *msg* are now shared with a another machine, *bridge*.
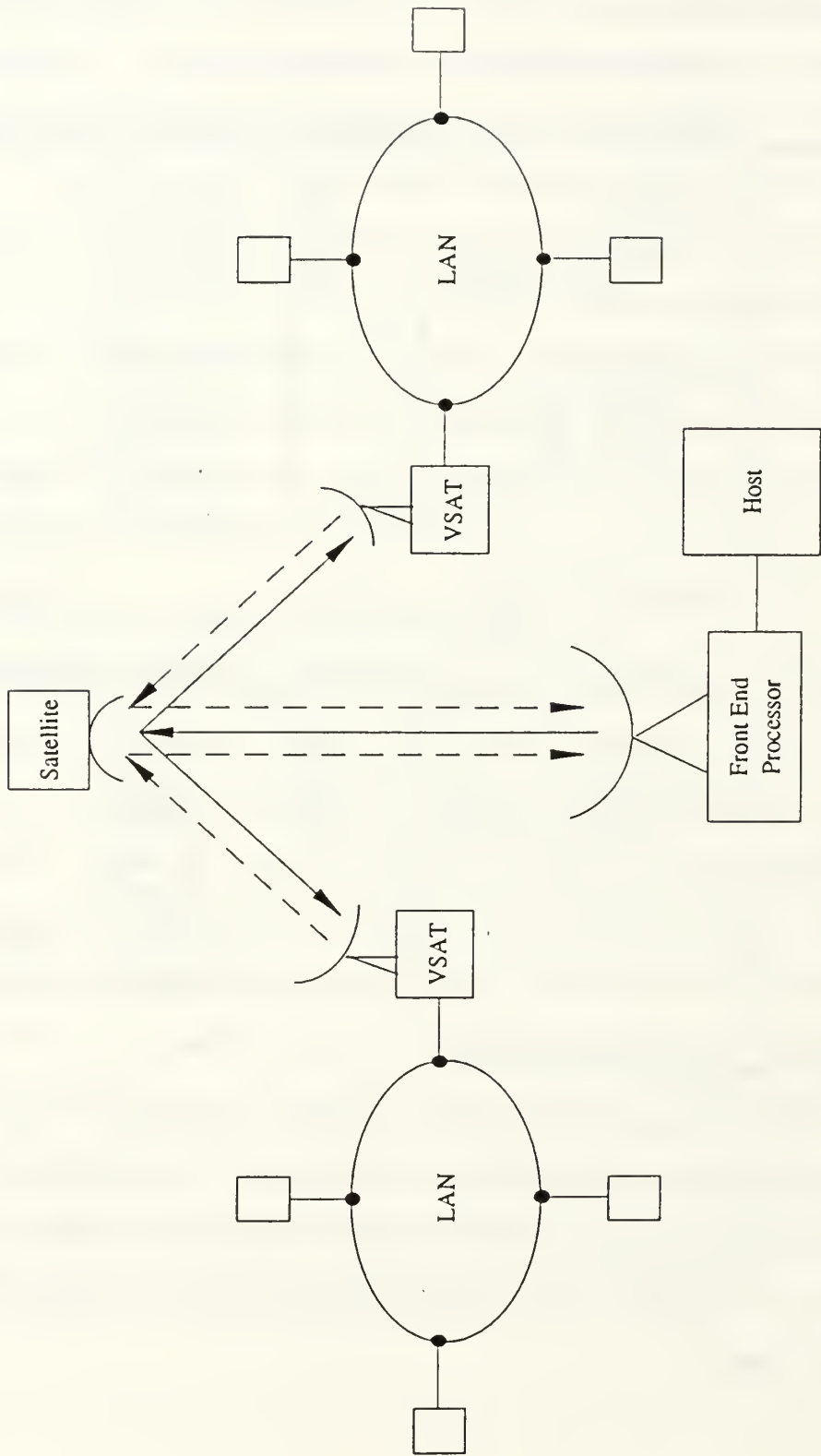
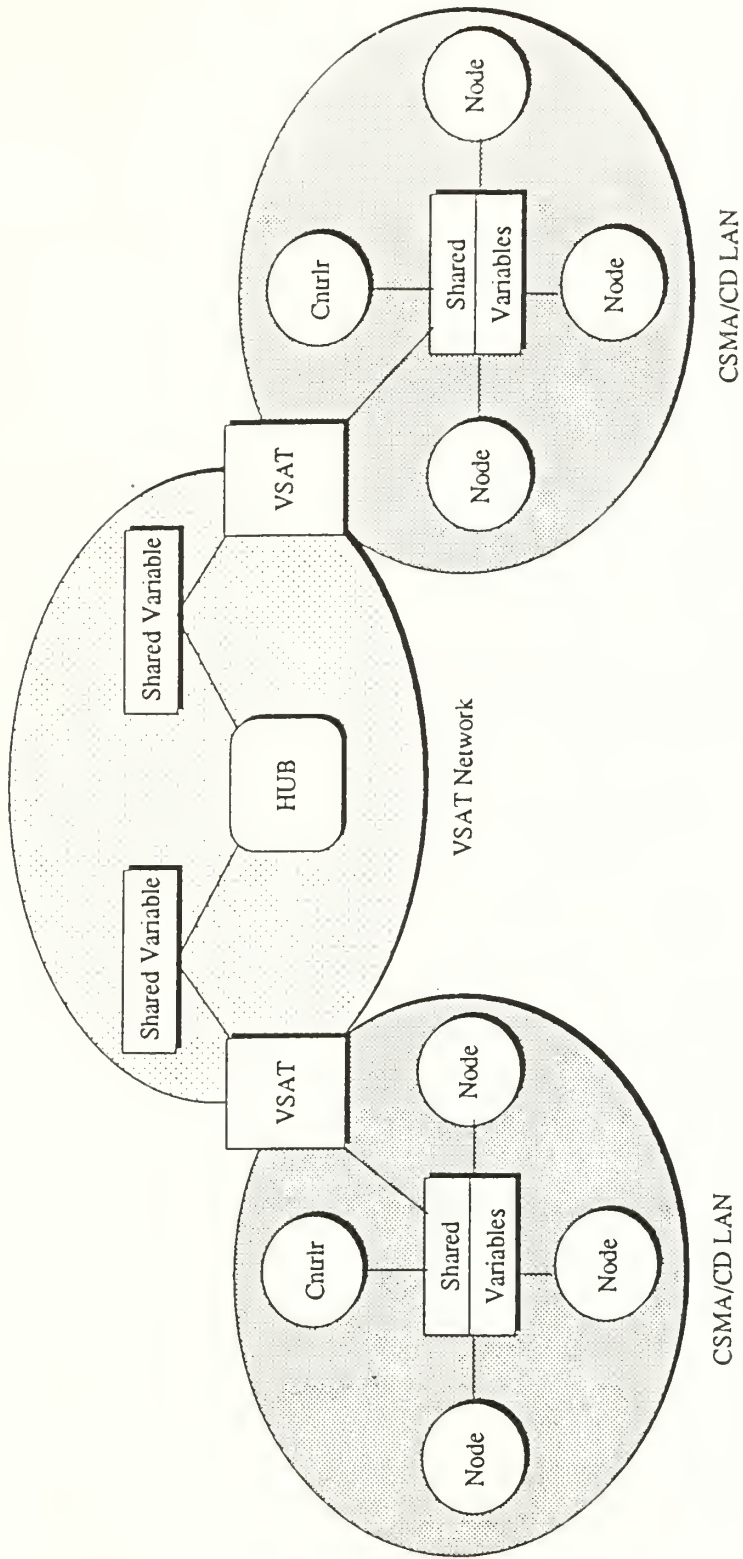Figure 9: VSAT Based LAN Internetwork.

34

Figure 10: Logical Architecture of VSAT Bridged LANs

35

The bridge is responsible for stripping any CSMA/CD MAC layer information that does not need to be sent and replacing that information on incoming traffic. It communicates with the next machine, *buffer*, via the variables *send* and *rec*. Bridge software is commonly available.

The *buffer* is responsible for managing the incoming and outgoing buffers in the VSAT. Outgoing traffic is buffered until a space is available in the queue for transmission. Incoming traffic is buffered until the bridge is ready to handle it. Since the CSMA/CD protocol does not have a built in priority scheme, this machine may be used to impose priorities on traffic. For example, network management may wish to have traffic from address A or to address X take priority over all other traffic. If this functionality is not desired, then the machine is merely the manager for a *first-in-first-out* (FIFO) queue.

The next three machines, *transmit*, *receive*, and *FAD* function together as the MAC layer protocol for the VSAT network. These machines will be specified in Chapter VI of this paper. Figure 11 displays the composition of the VSAT.

2. Logical Composition of Hub

The number of separate machines present in the hub is dependent upon the number of remote VSATs being supported. It has only one *FAD* and one set of *transmit*, *receive*, and *buffer* for every remote VSAT plus one set for the hub itself. The functioning of these machines is virtually identical to that in the VSATs. The *FAD* and *receiver* must be able to pass traffic to the appropriate *transmit/receive* pair and *buffer*, respectively. Also, a method such as polling must ensure that the *FAD* "sees" all of the *transmit/receive* machines and data is not overwritten before it can be sent.
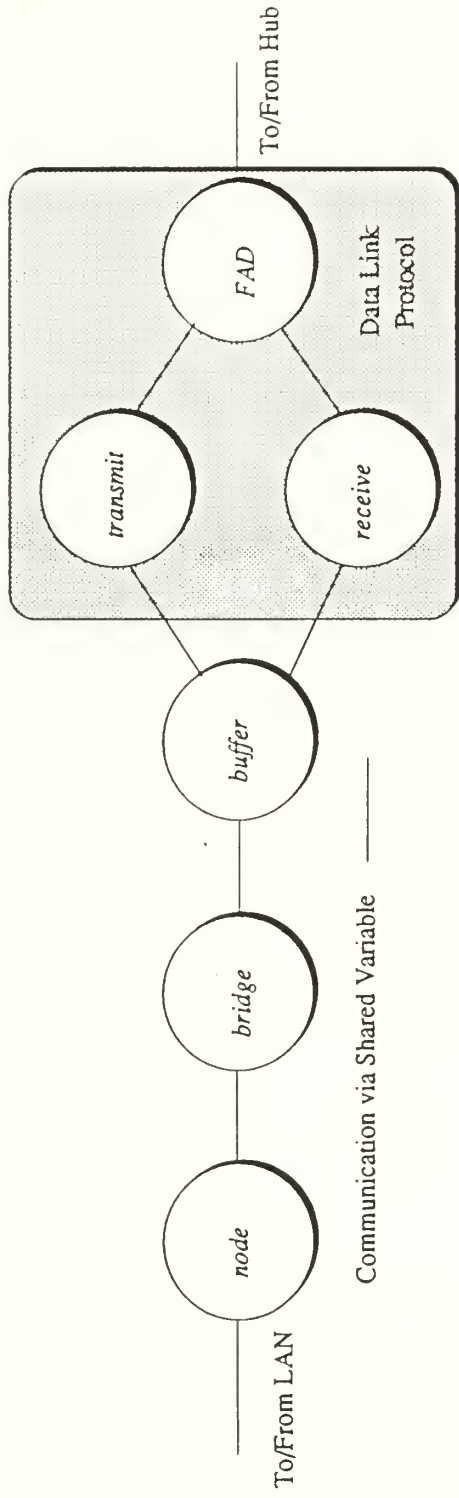
Figure 11: Logical Composition of VSAT

IV.   SELECTION OF A MEDIUM ACCESS CONTROL PROTOCOL

Medium access protocols allow many users to share a common communications channel. The protocol must fairly allocate the available resources, either passively or actively, to the users while maximizing throughput and minimizing delay. Also, network stability must be maintained at all anticipated traffic loads. If offered load reaches a saturation point, some method of recovery may be needed to force the network back into a stable operating region. Time division multiple access (TDMA) protocols will be focused on because they allow for the simplest growth path for evolving networks.

There are three general types of TDMA protocols. General TDMA assigns slots within a time frame to each ground station. *Random access protocols* allow users to transmit their message packets without any sort of coordination. *Demand assigned multiple access* (DAMA) protocols use either a distributed or centralized reservation scheme to coordinate users waiting to transmit packets.

A.   GENERAL TDMA

TDMA is a technique that allows stations on a network to transmit traffic bursts during certain slots of a periodic time frame. Slots are synchronized so that bursts from different earth stations arrive at the satellite closely spaced but without an overlap. The transponder takes one burst at a time, amplifies it, and retransmits it on the downlink. Figure 12 is a simplified view of TDMA. [Ref. 10:p. 226]

In order to fine tune the performance of a TDMA network, more than one time slot in each frame may be assigned to users that typically have large volumes of traffic to send. While this is not a dynamic process, it may be placed on a time schedule if the

38

traffic patterns between stations is predictable. For example, if a station is required to perform large data transfers every morning then it can be assigned several slots in each frame between the hours of 8 and 10 AM. During other times it would receive only one slot per frame.
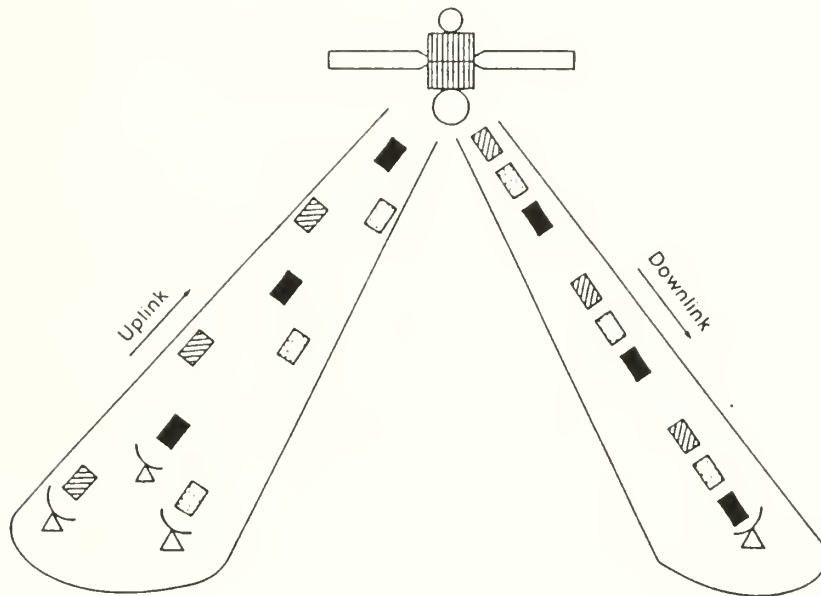
Figure 12: Time Division Multiple Access Source: [Ref. 10:p. 227]

TDMA is particularly well suited for networks in which the station loads are moderate to heavy, predictable, and vary slowly over time. Under lightly loaded conditions, TDMA wastes a large portion of the available bandwidth. A station always has at least one slot per frame assigned to it even if it has no traffic to send and another station has a large queue. Also, every time a station is added to or taken off of the network the frame structure and slot assignments must be changed. In order to better

utilize the bandwidth under such conditions random access or demand assigned techniques must be used.

B. RANDOM ACCESS PROTOCOLS

Random access protocols, sometimes referred to as contention based protocols, have no scheduled time for users to transmit nor is there a central agency controlling the timing of traffic. Each remote station is attached to one or more users who generate message packets in a random manner. As the message packets arrive at the station, they are placed in a queue and transmitted first-in-first-out. Because there is no central controller, collisions occur when data packets from two or more stations overlap in time at the receiving station. It the job of the protocol to recover from these collisions and also from errors induced due to channel noise.

In order to make the analysis of the system tractable, the following assumptions are made:

- ○ All links are equidistant.
- ○ Infinite number of users.
- ○ Packets of equal length T seconds.
- ○ Packets are generated by remote station according to a Poisson process with average arrival rate of λ packets/second.
- ○ Transmission channel is assumed to be error-free.
- ○ ACKs never suffer a collision.

Special notice should be taken of the assumption of a Poisson process. The Poisson process states that the probability of a single occurrence of an event during an interval of t seconds is given by $e^{-\lambda t}$. If a remote station is connected to more than one user, each of which is generating messages according to a Poisson process, then the

40

transmissions of the station are *not* Poisson. Also, the Poisson process assumes that the number of occurrences during one time interval is independent of the number occurring in any other interval. This is not the case for VSAT systems because the offered load g of the system is dependent on the generation rate λ and also the number of packets awaiting retransmission.

While the above assumptions clearly do not reflect the physical reality of the system, they do allow the successful prediction of an upper bound for performance. [Ref. 12:p. 47-48]

1. ALOHA

ALOHA, shown in Figure 13, is the simplest of all random access protocols. Packets are simply transmitted by the remote stations as they are created. The receiver uses an error detection scheme to see if the packet was received uncorrupted. If no error was found, an acknowledgment is sent. If errors are detected then no acknowledgment is sent and the originator will attempt to retransmit the packet after a random time-out interval. In some satellite communications systems using ALOHA, no ACK is returned by the receiving station because the sender can "hear" his transmission on the satellite downlink and determine if a collision has occurred. While this would be a better method, it is not plausible with all VSATs due to their low transmitter power and antenna gain.

If a packet is transmitted at time t, it will be received without collision as long as no other packet is transmitted during the interval t-T to t+T. The probability of success $P[suc]$ is therefore the probability that no other packets are transmitted during the interval $2T$. By the Poisson process, the probability that only one packet is generated in $2T$ seconds is given by:

$$P[suc] = e^{-2gT}$$

Where g is the offered load and must be greater than λ since not every packet is successfully transmitted on its first attempt.

The throughput S of the system is the fraction of time that useful information is transmitted. Since $P[suc]$ is the fraction of offered packets that are successful during a time period, it can be defined as S/gT. Therefore, the throughput of an ALOHA system is given by:

$$S = gTe^{-2gT}$$

This is usually normalized by the packet transmission time and takes the form:

$$S = Ge^{-2G}$$

where G is referred to as the *normalized offered load* [Ref. 12:p. 49]. Differentiating this equation and setting to zero, the maximum throughput is found to be $S = 1/(2e) \cong .18$ where $G = 1/2$.

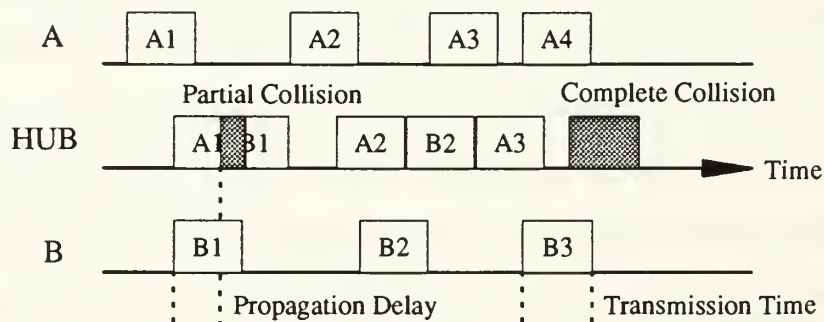
Figure 13: ALOHA

The average packet delay for ALOHA networks is the sum of the packet length T, propagation delay τ, and the expected value of the retransmission delay $E[D_r]$:

$$D_{avg} = T + \tau + E[D_r]$$

T and τ are known quantities. The value of $E[D_r]$ is dependent upon the type of retransmission scheme used.

One method for determining the amount of time to wait before retransmission is to perform a random draw from a uniform probability distribution. If the random retransmission delay is taken from a uniform distribution with K intervals of T seconds each, then the average delay before the first retransmission is $T(K+1)/2$ and the retransmission delay after r attempts is given by:

$$D = r\left[\tau + \frac{T(K+1)}{2}\right]$$

If Q_r is the probability of a success after r retransmissions, the expected value of r is:

$$E[r] = \sum_r r\, Q_r$$

and so the expected retransmission delay of a packet is:

$$E[D_r] = E[r]\left[\tau + \frac{T(K+1)}{2}\right]$$

In order to find $E[r]$, an expression for Q_r must be determined. Let q be the probability that a packet is successfully transmitted on its first attempt and q' be the probability that its is successful for one retransmission event. Q_r is therefore:

$$Q_r = (1-q)q'(1-q')^{r-1} \qquad\qquad \text{for } r \geq 1$$

Substituting this back into the series, $E[r]$ converges to:

$$E[r] = \frac{1-q}{q'}$$

Since q is the probability of a newly generated packet being successfully transmitted, it is merely the Poisson distribution e^{-2gt}. Assuming that $q \cong q'$, the expected value of r is found to be:

$$E[r] \cong e^{2gt}-1$$

The expected retransmission delay is thus:

$$E[D_r] \cong (e^{2gt}-1)\left[\tau + \frac{T(K+1)}{2}\right]$$

and therefore the average packet delay is:

$$D_{avg} \cong T + \tau + (e^{2gt}-1)\left[\tau + \frac{T(K+1)}{2}\right] \qquad\qquad K>>1$$

The actual value of D_{avg} does not change greatly for values of K between 10 and 50 so the choice of K is not critical [Ref. 10:p. 364-366]. This equation can be normalized by the packet time and becomes:

$$D_{avg} \cong 1 + a + (e^{2G}-1)\left[a + \frac{(K+1)}{2}\right] \qquad\qquad K>>1$$

2. S-ALOHA

Slotted ALOHA, Figure 14, is a modification of pure ALOHA in which packets can only be sent at discrete times called slots. The length of a slot is the packet size converted to seconds (the reciprocal of the bit rate times the number of bits in a packet). A central clock keeps all stations synchronized to ensure that packets arrive at the receiver only at the beginning of a slot. Because all packets must begin on a boundary, a packet will be successfully transmitted if it was the only packet scheduled for transmission during the previous slot. Thus:

$$S = gTe^{-gT} \qquad\qquad \text{or normalized: } S = Ge^{-G}$$

Differentiating this shows that the maximum throughput is $S = 1/e \cong .36$ and occurs when $G = 1$. [Ref. 12:p. 50]

The derivation of packet delay is similar to that for pure ALOHA except that there is an additional delay of $T/2$ before a packet may be transmitted since the sender must wait for the beginning of a slot. This applies to both the original transmission and all subsequent retransmissions. With this additional factor the average packet delay becomes:

$$D_{avg} \cong \frac{3T}{2} + \tau + (e^{2gt}-1)\left[\tau + \frac{T(K+1)}{2}\right] \qquad K>>1 \quad \text{[Ref. 10:p. 366]}$$

Normalizing by packet time we have:

$$D_{avg} \cong \frac{3}{2} + a + (e^{2G} - 1)\left[a + \frac{(K+1)}{2}\right] \qquad K \gg 1$$
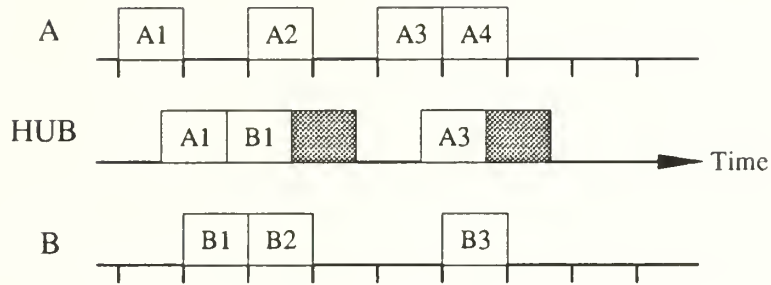
Figure 14: S-ALOHA

3. SREJ-ALOHA

Selective Reject ALOHA attempts to increase throughput on a random access channel without the implementation difficulties caused by using time slots. Variable length messages are sub-packetized and then transmitted in an unslotted manner. As collisions occur, the receiver rejects the corrupted sub-packets. These sub-packets are then retransmitted by the senders. Figure 15 shows the functioning of SREJ-ALOHA. [Ref. 13:p. 314]

Selective Reject ALOHA has a throughput that is comparable to that of S-ALOHA but without the requirement for synchronization across the network. Messages are not forced into fixed size packets for transmission. Instead, each message is divided into smaller sub-packets and then transmitted as a continuous burst. Since most collisions result in only a partial overlap, only the few sub-packets that were corrupted would need to be retransmitted.

This type of strategy has several advantages over S-ALOHA. It does not require the additional complexity of timing coordination so implementation cost could be lower. Also, the performance could possibly be better than that of S-ALOHA because it does not have the overhead caused by forcing the traffic into fixed length bursts. Actual

45

throughput of SREJ systems is in the range of .2 to .3 due to the need for acquisition preamble and header in each sub-packet. [Ref. 14:p. 37]
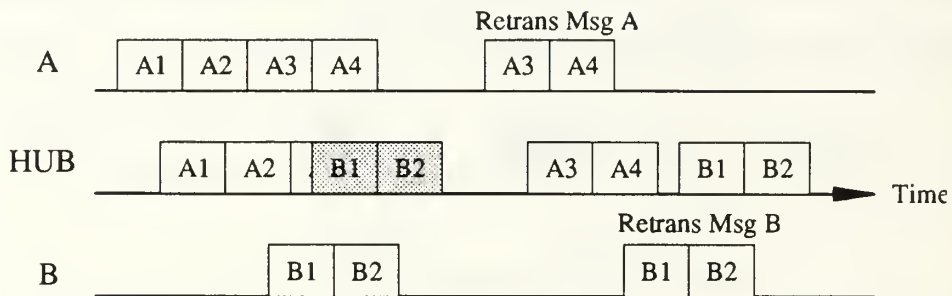

Figure 15: SREJ-ALOHA

An additional modification may be made to the SREJ-ALOHA protocol that increases its maximum useful throughput to .4 -.45 . SREJ-ALOHA/FCFS uses a time-of-arrival "first-come-first-served" method to resolve collisions. Returned acknowledgments are monitored by all stations on the network. When collisions have occurred, an interval of time is reserved exclusively for the retransmission of the corrupted packets. The message that began arriving first would be retransmitted first. For example, messages A and B each contain three sub-packets (A1, A2, A3 and B1, B2, B3) and are transmitted such that A1 arrives correctly; A2, A3, B1, and B3 overlap and are indecipherable; and B3 arrives correctly. The order and content of the returned acknowledgments would allow all stations to know that the first sub-packet of three part message A was received correctly before message B interfered. The last sub-packet of three part message B was then received. The ordering is used to set up a retransmission interval, with A first and B second, after a prespecified delay relative to a mutually observed channel event. Because all stations received the channel feedback, other stations are able to avoid transmitting during this period guaranteeing a conflict-free retransmission. [Ref. 15:p. 435-438]

46

4. Instability of ALOHA Protocols

All of the ALOHA family of protocols are unstable when faced with large variations in offered load. As G increases, so does S until the maximum is reached. Beyond this point, throughput decreases while offered load continues to increase. If S is then less than λ, the system will drift further until S eventually reaches zero.

This is true for any ALOHA system using fixed retransmission probabilities. Schemes exist to stabilize ALOHA systems by adapting the retransmission probabilities by recursive algorithms in order to reflect the state of the system. These schemes are difficult to implement and only offer to increase stable throughput to $S = 1/e$ for the pure ALOHA case. [Ref. 12:p. 70]

C. DAMA

DAMA protocols allow users to reserve slots in a time division multiple access (TDMA) frame for their use. This can be done by either requesting slots from a central host or by preemptively transmitting in slots that were empty during the previous frame. Reservation schemes minimize the contention for channel resources and greatly enhance the overall stability of the network. They offer potentially higher throughput, especially for messages, but at the cost of increased delay. Also, they require additional complexity in the system hardware, but could be worth the cost for some traffic loads.

1. Decentralized Schemes

In decentralized schemes, reservations are implicit. Successfully transmitting in some slot reserves a corresponding slot in a later frame for that stations use. These methods require a station to hear its own broadcast on the downlink. Two decentralized protocols that are suitable for VSAT networks are discussed here.

a) R-ALOHA

With R-ALOHA, a station monitors all slots in the current frame. Any slot that is empty or contains a collision is available for use in the following frame and is contended for using S-ALOHA. Successfully transmitting in that slot reserves the corresponding slot in subsequent frames for that station's use for as long as it has traffic. [Ref. 4:p. 318]

Performance of R-ALOHA can be worse than that of S-ALOHA if traffic is very bursty due to the fact that after a transmission is completed, the slot must remain empty for one frame before it can be utilized again. Fairness is also a problem with this protocol. Once a station manages to capture slots it can hold them indefinitely, monopolizing the circuit. [Ref. 4:p. 319]

b) Robert's Scheme

Robert's scheme divides the first slot of every frame into "minislots." Users contend for the minislots using S-ALOHA by sending a request packet that contains the number of slots per frame it desires. If this is successful, it determines the slots it has reserved and transmits its data. Throughput of this protocol is significantly better than that of S-ALOHA, though delay is somewhat greater. [Ref. 4:p. 320]

c) CPODA

Contention Priority Oriented Demand Assignment is similar to Robert's scheme with the differentiation of data and reservation slots. The difference here is that the boundary between the two types may be varied with system load. This ability allows the protocol to handle both stream and bursty traffic. Stations are also allowed to reserve future slots by setting flag bits in their current data slots, so heavy users will not need to contend for the next reservation minislot. Reservations can be made for a single frame or for a series of frames depending on the data type. [Ref. 3:p. 181]

While this protocol is decentralized for the scheduling of packets, some form of central control is necessary in order to change the frame structure. The controlling node would be responsible for monitoring the state of the network and adjusting the number of data and minislots to optimize throughput and/or delay.

d) ARRA

Announced Retransmission Random Access is a different twist on reservation protocols. Instead of using minislots to reserve a slot prior to transmitting data, the station transmits and then reserves a future slot for retransmission if a collision occurs. Because a packet may be transmitted without first reserving a slot, in lightly loaded networks this protocol has a much lower average delay than other reservation protocols. [Ref. 3:p. 181]

2. Centralized Schemes

These protocols use a central agency to allocate channel resources. Centralized control allows the frame structure to be dynamic so these techniques are well suited to mixtures of both stream and bursty traffic. These schemes potentially offer the highest throughput. Two techniques are commonly used for packet communication.

a) FPODA

Fixed priority oriented demand assignment is a technique that is used to connect six LANs scattered throughout the United Kingdom. Each frame begins with a series of 100 byte long *minislots* each assigned to a particular LAN. These are used to either transmit data or to make reservations. Reservations can be made for three levels of priority: priority, normal, or bulk. These reservations are used by a master control station to divide the remainder of the frame into from one to six variable length slots, again with each slot assigned to a particular station. This protocol is very effective where there is a small, fixed number of stations using the network. [Ref. 4:p. 320-322]

b) *PDAMA*

Packet-demand assigned multiple access (PDAMA) was developed for NASA's mobile satellite system, handling voice and data communications to mobile users throughout a wide area. The PDAMA frame begins with a leader control slot, transmitted by the master station, that contains acknowledgments of received reservations and slot assignments. This is followed by a guard slot of 280 ms that allows stations to determine their slant range to the satellite by transmitting a tone. The next section of the frame is a set of reservation minislots that are contended for using S-ALOHA. Reservations may be made for one slot at a time; long message mode, which allocates the entire information subframe to a station until its transmission is completed or it is preempted for higher priority traffic by the master station; or digitized voice conversations. The information subframe is of variable length and is allocated by the master station based upon a prioritized queue of all received reservations.

D. SELECTING AN ACCESS PROTOCOL

There are no hard and fast rules for selecting an access protocol for a VSAT network. The system designer must balance performance parameters such as throughput and delay against present costs and anticipated expansion plans.

The primary consideration in the selection of an access protocol is the nature of the traffic that is anticipated. If a VSAT is being used to relay transactions from an ATM, its packet sizes, message generation rates, and required minimum delay time will be substantially different than that of a VSAT network that is being used by a corporation to transmit inventory, accounting, and personnel data. This leads to some rules of thumb that can be used in the selection of an access protocol.

Networks whose primary traffic is "bursty" and which do not require high channel utilization are well suited to contention algorithms such as the ALOHA family.

Examples of this type of application would be credit card approval and bank ATMs. As long as the offered load remains low, then the probability that a collision occurs between two or more packets is small. As system load increases, then performance decreases dramatically. An additional benefit of this type of access scheme is that round trip delay is low. This is especially important in systems like the above examples where there is a customer waiting on the results.

Networks that are primarily used to pass business data such as inventory and accounting information require high channel utilization since each message is potentially thousands of packets long. For these networks, a TDMA scheme is the best choice. This allows each of the VSATs to have a guaranteed amount of access time to the uplink, eliminating the need to contend for this resource. The amount of time given to each VSAT can be equal or skewed towards the heavy users. While the allocation of channel slots is not dynamic, it is possible to vary the time slices in some predetermined fashion. In this way stations that have large amounts of data to pass at certain times of day can be given larger access blocks during those times. As new stations are added to the network, slot assignments for all stations are modified by the hub.

For networks that have a mixture of traffic types or a varying number of VSATs connected, a DAMA access scheme is needed to allow efficient channel utilization. These schemes force VSATs to reserve time slots, either implicitly or explicitly, before they transmit their data. This requirement significantly adds to the overhead on the channel. Even so, DAMA is the only alternative for non-deterministic traffic that requires high utilization.

E. MAC PROTOCOL SELECTED

A generalized TDMA protocol is recommended as the medium access method. The nature of the traffic traveling between LANs was the prime consideration in its selection. Approximately 80 percent of the traffic on a VSAT net is estimated to be bulk traffic such as electronic mail, spreadsheets, and other such documents [Ref. 10:p. 597]. Random access techniques are undesirable in this case because the length of bulk transmissions may cause many collisions, increasing delay and possibly pushing the protocol into an unstable operating region. It was also felt that transmissions from the VSATs would not be "bursty." Bursty users have long periods of time, relative to the typical message length, between transmissions. For interconnected LANs in a corporate network there would most likely be some level of offered load for a VSAT most of the time. Because the channel would be in almost constant use, DAMA protocols are unnecessary. Several other factors were also considered:

- o The network topology should be fairly stable so a protocol that automatically handles the addition/removal of stations is not needed.

- o Traffic volume should be predictable from historical data so slot assignments within the TDMA frame may be tailored.

- o Real time response was not a critical requirement.

- o TDMA is easily implemented and allows for network growth.

Once a method for accessing the satellite channel is selected, the remainder of the data link layer functions must be implemented. This may be done through the use of a *sliding window* protocol, explained in Chapter V. This protocol is a point-to-point protocol that is used on top of the TDMA link. The following chapter will present a specification and analysis for a selective repeat, sliding window protocol using TDMA.

V. SPECIFICATION AND ANALYSIS OF A SELECTIVE REPEAT PROTOCOL

In the previous chapter a TDMA protocol was chosen to accomplish medium access on the VSAT link. It allows all stations on the network to share the communication medium without conflict, but it does not provide any other services required of the data link layer such as error control and point-to-point flow control. In order to accomplish this another protocol must be used in conjunction with the TDMA channel.

A *sliding window* protocol allows a transmitter to send multiple packets without waiting for an acknowledgment. The "window" limits the number of frames that may be sent at any time. As a packet is sent the window closes by one. When and acknowledgment (ACK) is received, the window opens back up by one. Packets are assigned sequence numbers to keep track of which ones are sent and acknowledged. The sliding window protocol also must have a means of requesting retransmission of packets that are received in error. There are two methods of accomplishing this: go-back-N and selective repeat. Figure 16 demonstrates their operation.

If a packet is received in error with a go-back-N protocol, the receiver sends a negative acknowledgment (NAK). It discards all incoming packets until the packet in error is received correctly. The sender is thus required to retransmit all outstanding packets once a negative acknowledgment has been received. On a satellite link the one-way propagation delay is approximately 270 ms. In order to get the best utilization from the channel, the window size must be large enough to allow an ACK for the first packet to be received before the last packet in the window is sent and so must be at least .54 seconds. If the system is operating with a full window, then .54 seconds of data must be

53

retransmitted when an error occurs. At a data rate of 56 kbps this would equate to 3780 bytes of data. [Ref. 4:p. 141-143]
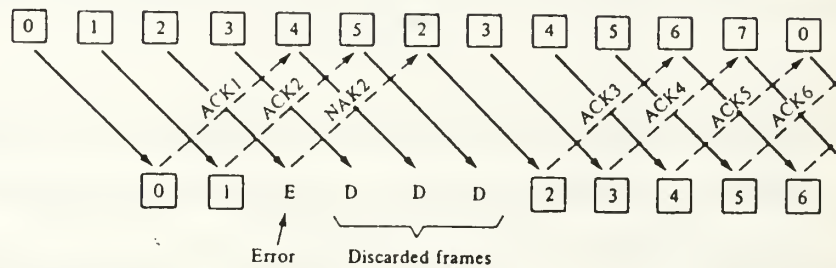
(a) Go-back-N
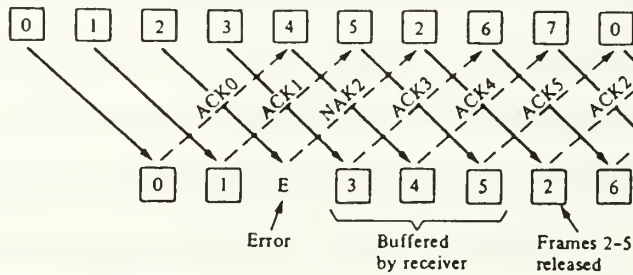
(b) Selective report

Figure 16: Go-back-N and Selective Repeat Acknowledgment
Schemes.
Source: [Ref. 4:p. 144]

A selective repeat protocol requires that only those packets received in error be retransmitted. Once a NAK for a corrupt packet has been sent, the receiver continues to acknowledge subsequent packets. These packets are placed in a buffer until the packet received in error is received correctly. The selective repeat protocol offers more efficient utilization of the channel, but this comes at the cost of more complex logic at both receiver and transmitter and larger buffer requirements at the receiver. These are far outweighed by the benefits gained. The remainder of this chapter will present the formal specification and analysis of a sliding window, selective repeat protocol. A *high level data link control* (HDLC) frame will be used for transmission across he VSAT link. [Ref. 4:p. 143-144]

54

A. SPECIFICATION

The specification for the selective repeat protocol consists of finite state machines for the three entities within the shaded area of Figure 11, their shared and local variables, and their predicate-action tables. Each machine is a graph representing the functioning of an entity within the protocol. The nodes on the graphs are "states" and the arcs connecting them are transitions between the states. The transition taken is determined from the predicate-action table for the corresponding machine. A transition may only be taken if its "predicate," which is determined from the contents of both local and shared variables, is true. Local variables are used by machines to keep track of internal information while shared variables are a means of communication between the processes. If a transition is enabled, then the "action" given by the table is performed and the state of the machines is changed to the next node.

1. Transmitter

Figure 17 and Table 5 are the SCM specification of the selective repeat transmitter with a window size of 3. The finite state machine of the transmitter may be generalized as shown in Figure 16 for a window size of N.

The transmit machine's initial state is 0. As the buffer manager places data in the next available sequence number, the transmitter takes the packet, passes it to the FAD, sets a packet timer, and increments the index for the next packet to be transmitted. As long as the next packet is not empty, the transmitter will continue this process until the bottom state on the finite state machine is reached, indicating transmission of a full window.

Acknowledgment (ACK) and negative acknowledgments (NAK) are passed from the FAD to the transmitter as they are received. If an ACK is received then the transmitter must determine if the window may be opened and if so, how far. If the ACK

55

is not for the first packet in the window then the flag ACK_REC() is set, indicating that the packet was received correctly. The window is not advanced because packets that were transmitted earlier are still outstanding. The sequence number within each ACK and NAK represents the actual sequence number of the packet received and not the sequence number of the next expected packet, as is common in many protocols.

When an ACK for the first packet in the window is received the machine clears its buffer, advances the window, and looks at the next sequence number. If the packet has not been received, ACK_REC() = FALSE, then that becomes the beginning of the window. If it has been received then the next sequence number is examined until the earliest outstanding packet is found or the window is fully opened. If a NAK is received for a packet or the timer expires, indicating that the packet was lost, then the transmitter is allowed to retransmit that packet. ACKs or NAKs that do not correspond to any of the sequence numbers within the current window are ignored.
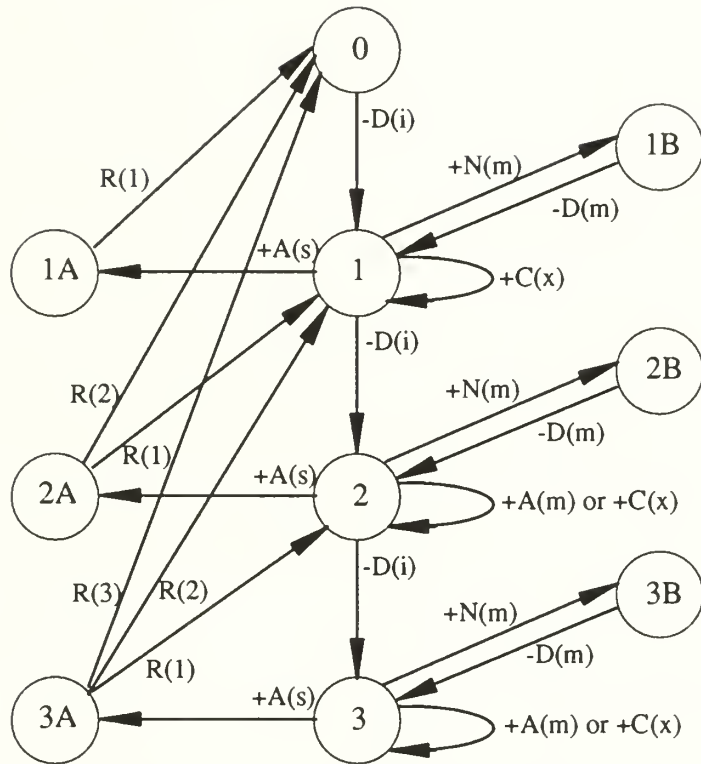
Figure 17: FSM for Selective Repeat Transmitter, Window Size = 3.

TABLE 5: PREDICATE-ACTION TABLE FOR SELECTIVE REPEAT
TRANSMITTER

TRANSITION	PREDICATE	ACTION
-D(i)	OUT_BUFFER(i) $\neq \emptyset$	DATA_OUT<--OUT_BUFFER(i); SET TIMER(i); i := i+1;
+A(m)	CONTROL_IN = ACK(m) $\wedge$ $i_s <$ m < i;	ACK_REC(m) := TRUE; DEL CONTROL_IN;

+A(s)	CONTROL_IN = ACK(s) $\wedge$
	s=i_s;
		W := 0;
		while(i_s<i $\wedge$ ACK_REC(i_s)=TRUE)
		   DEL OUT_BUFFER(i_s);
		   ACK_REC(i_s) := FALSE;
		   i_s:= i_s+1;
		   W := W+1;
		DEL CONTROL_IN;

R(W)	W = 1..WINDOW_SIZE	------
+N(m)	i_s <= m < i; CONTROL_IN = NAK(m) or TIMER(m) expires	DEL CONTROL_IN;
-D(m)	------	DATA_OUT <-- OUT_BUFFER(m);
+C(x)	CONTROL_IN = ACK(x) or CONTROL_IN = NAK(x); x < i_s or x => i;	DEL CONTROL_IN;

TRANSMIT VARIABLES

i - Next packet to be sent. Local variable.

i_s - Start of transmit window. Local variable.

m - Any valid ACK number.

x - Any invalid ACK or NAK number.

CONTROL_IN - Control field from incoming data packets. Shared with FAD.

TIMER() - Array of timers set for packets as they are sent. Local variable.

ACK_REC() - Array of booleans set to TRUE when ACK is received for a packet.
      Local variable.

OUT_BUFFER() - Array of outgoing data packets. Shared with *buffer*.

DATA_OUT - Variable used to pass outgoing data to FAD.

W - Counts the number of frames that i_s has advanced.

WINDOW_SIZE - Max number of outstanding frames allowed. Implicit in FSM.

Figure 18: FSM for Selective Repeat Transmitter, Window Size =

2. Receiver

The specification for the selective repeat receiver is given by Figure 19 and Table 6. The initial state of the receiving machine is 0. Any packets that are received with sequence numbers outside of the window, +D(x) transition, are dropped. If a corrupted packet is received then the +B(i) transition sends a NAK for that sequence number. If a valid data packet is received then either the +D(n) or +D(i) transition is taken, based upon whether the sequence number of the received packet is equal to i_S. If the sequence number is not i_S then the flag PKT_REC is set to TRUE and the packet is

stored. If it is equal to i_S, then the PKT_REC is set, the packet is released to *buffer*, and

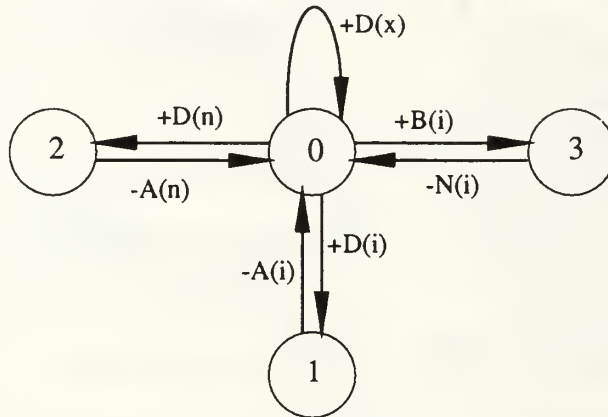i_S is incremented until a sequence number with PKT_REC=FALSE is found.

Figure 19: FSM For Selective Repeat Receiver

TABLE 6: PREDICATE-ACTION TABLE FOR SELECTIVE REPEAT
RECEIVER

TRANSITION	PREDICATE	ACTION
+D(i)	DATA_IN $\neq \emptyset \Lambda$ seq number = i	IN_BUFFER(i) <-- DATA_IN PKT_REC(i) := TRUE;

-A(i)	------	CONTROL_OUT <-- ACK(i);
		while(i<=i_e Λ PKT_REC(i) :=
		TRUE)
		    REL IN_BUFFER(i);
		    PKT_REC(i) := FALSE;
		    i := i+1;

+B(i)	DATA_IN $\neq \emptyset \Lambda$ CRC does not check	------
-N(i)	------	CONTROL_OUT <-- NAK(i);
+D(n)	DATA_IN $\neq \emptyset \Lambda$ seq number n $\neq$ i Λ i < n <= i_e	IN_BUFFER(n) <-- DATA_IN; PKT_REC(n) := TRUE;
-A(n)	------	CONTROL_OUT <-- ACK(n);
+D(x)	DATA_IN $\neq \emptyset \Lambda$ seq number x < i or x > i_e	------

RECEIVE VARIABLES
i - Expected packet. Start of receive window.
n - Any sequence number in window other than i.

60

x - Any sequence number not in window.

i_e - i+WINDOW_SIZE

IN_BUFFER() - Array of frames to hold incoming data packets until they can be released to *buffer*. Equal in number to window size.

PKT_REC() - Array of booleans set to TRUE when a packet is received.

DATA_IN - Variable used to pass incoming data from FAD to receiver.

CONTROL_OUT - Variable used to pass ACKs and NAKs to FAD.

3. Frame Assembler-Disassembler

The FAD is a machine that takes control information from the receiver and data packets from the transmitter, encapsulates them into an data frame such as HDLC, and sends them across the VSAT link. At the receive side the FAD extracts the incoming control information and passes it to the transmitter and passes the entire frame to the receiver. The logical communication within the protocol is between the *transmitter* and *receiver* machines. If the FAD is assumed to be reliable in that it always forwards information to the appropriate entity, its functioning is does not impact on the appropriateness of the protocol. The FAD, therefore, will not specified by this paper.

B. ANALYSIS

A common form of analysis for communications protocols is *reachability analysis*. This is a graphical analysis which examines every possible system state. A system state is a node on the graph defined by the state of the two communicating machines and the contents of the communication channels. Each state consists of the set (T,D,C,R) where T is the state of the transmit FSM, D is the contents of the channel from sender to receiver, C is the contents of the channel from receiver to sender, and R is the state of the receiving FSM. The arcs on the graph are all transitions that may be taken from a given state. If the protocol is functioning properly it should be free from *deadlock*. A deadlocked state is one from which the protocol can not proceed. Once in a deadlocked state the protocol will remain there indefinitely.

A reachability analysis for a window size of 3 was performed and is given in Figure 20. Two assumptions were made for this analysis: all packets are received without errors, packets may not be lost or re-ordered during transmission. Within this graph D represents a data packet from sender to receiver while A represents an acknowledgment. The assumption that packets in the channel cannot be lost or re-ordered eliminates the need to keep track of which specific packet or acknowledgmentit is representing. Figure 20 shows that under these assumptions the protocol is free from deadlock.

For even the simple case of a window size of 3 and error-free transmission there are 25 states within the reachability analysis. By the symmetry of the diagram, it can be shown that for any given window size N the number of states in the error-free analysis is given by:

$$N^2 + (N + 1)^2$$

Obviously, full analysis of protocols using reachability diagrams becomes unwieldy for all but the simplest of cases.

A further analysis of this protocol was performed for a window size of 3 using the assumptions that no packets may be lost, only the first packet in a transmission window is corrupted, ACKs and NAKs are always correct, and all retransmitted packets are received correctly. This analysis, shown in Figures 21a and 21b, contains 65 states. Of these, 8 are duplicated in Figure 20.

By combining Figures 20 and 21, an analysis under the assumptions that only one packet in any window may be corrupted, no packets may be lost, ACKs and NAKs are always correct, and retransmitted packets are always received correctly. The protocol follows the states in Figure 20 until the corrupted packet is the first one in the window. At this point the protocol is one of the states in the far left column. These states map to states in the left column of Figure 21a. When the corrupt packet is received, one of the

+B0 transitions is taken and the protocol moves into Figure 21. Under these assumptions the protocol again is free from deadlock.

Due to the combinatorial explosion of states, another method must be used if a protocol is to be proved free from deadlock under all conditions. The development of an analytical method to prove the correctness of any protocol has been the subject of much work. The validity of many protocols may still only be "proved" by induction or through exhaustive computer simulation.
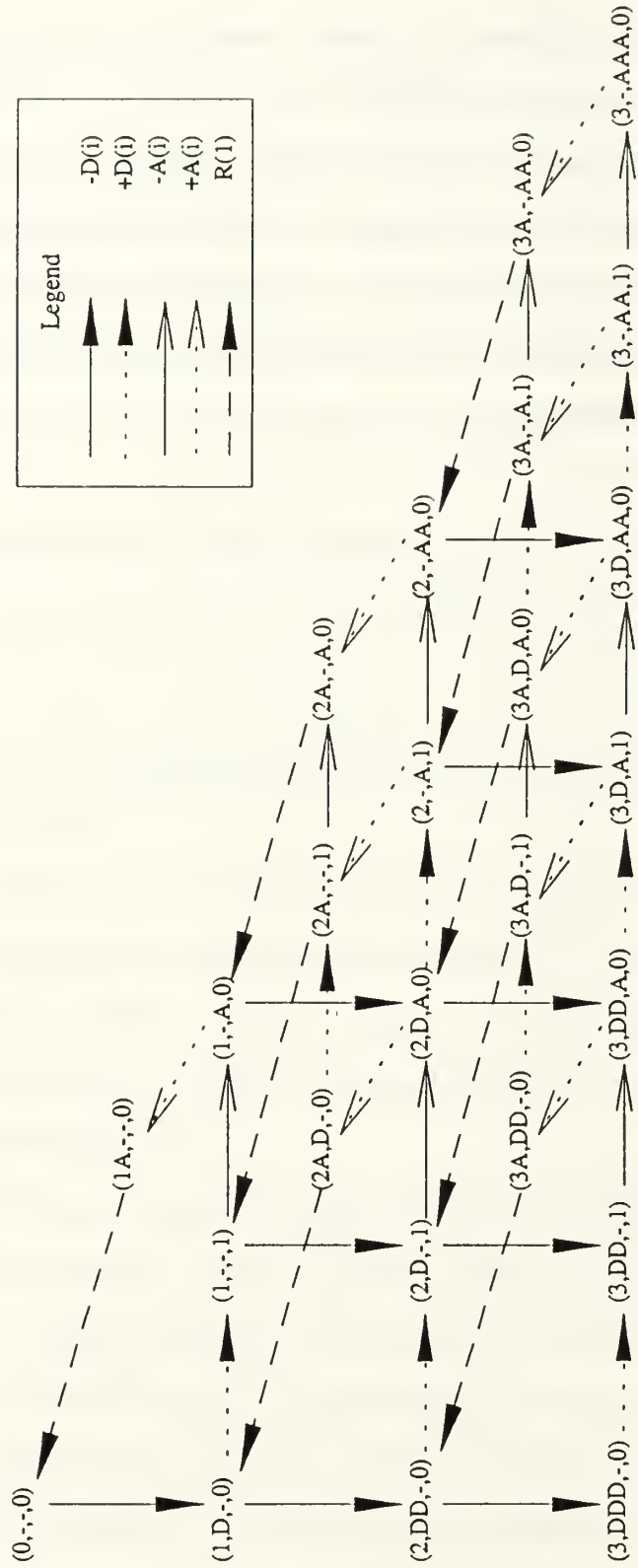
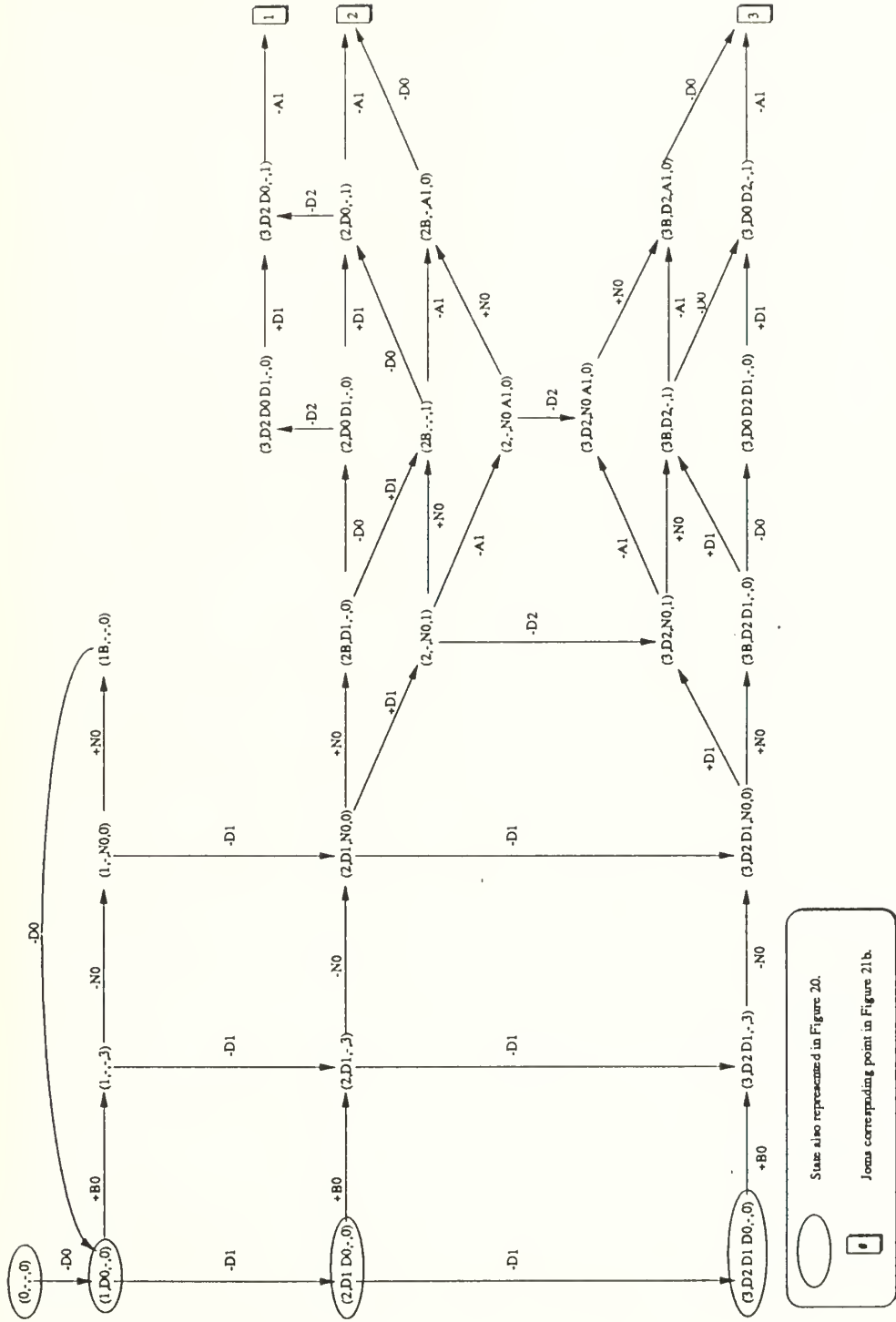Figure 20: Reachability Analysis, Window Size = 3, Error-free Transmission

Figure 21a: Reachability Analysis, Window Size =3. Only 1st Pkt is in error. Joins Figure 21b.
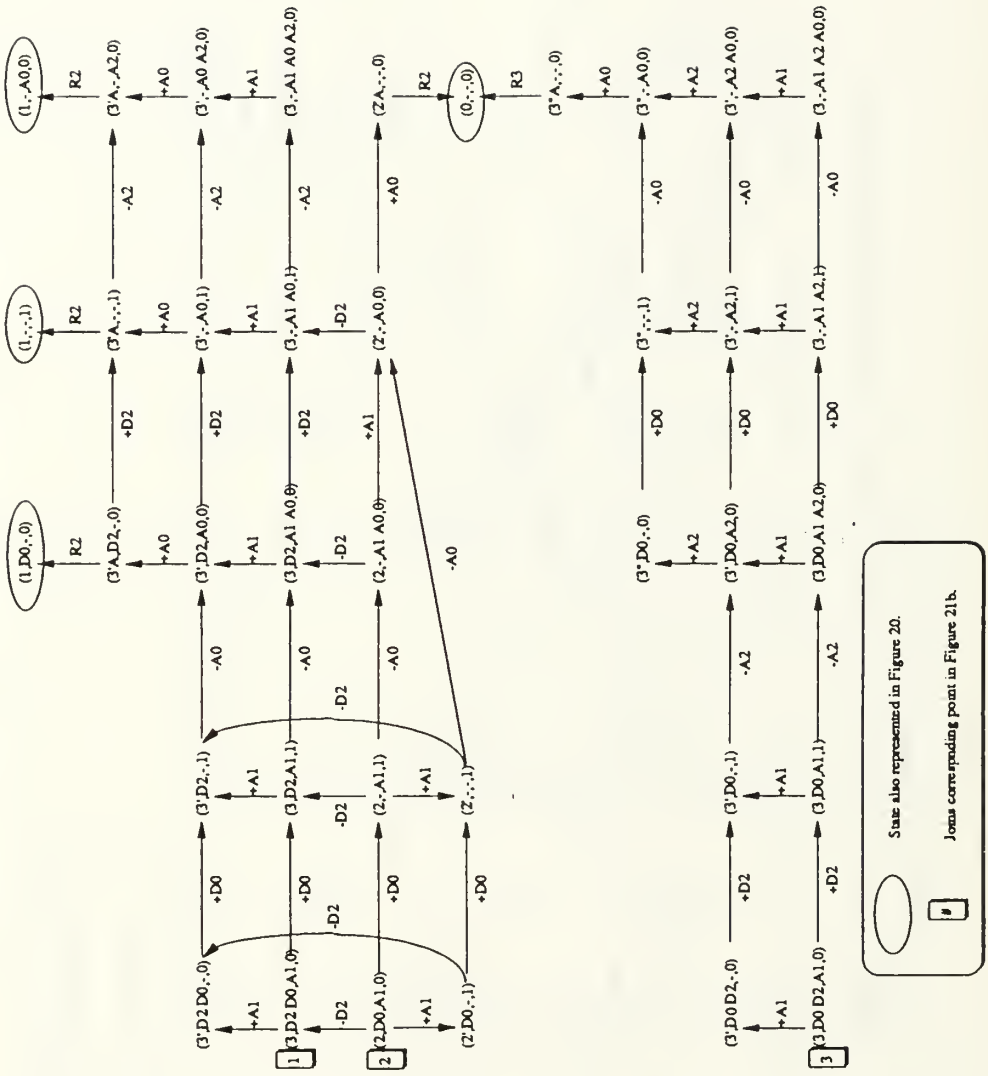
65

Figure 21b: Reachability Analysis, Window Size =3, Only 1st Pkt is in error. Joins Figure 21a.

66

VI.   CONCLUSIONS

In this thesis, an architecture for a VSAT-based LAN bridge was proposed. The bridge was specified using the systems of communicating machines model, and partially analyzed. This architecture specifies that entities within the VSAT network communicate via reads and writes to shared variables. The use of shared variables essentially isolates each entity from the internal functioning of other entities with which it must communicate. CSMA/CD LANs are currently the most widely used LAN protocols, therefore a CSMA/CD LAN was used in the specification of this network architecture. The use of SCM for the specification of the VSAT network architecture should enhance the ability of developers to implement VSAT-based bridges for other LAN standards.

Time division multiple access (TDMA) was chosen as the medium access method for a VSAT-based LAN network. Inter-LAN traffic is estimated to consist mostly of bulk transfers such as data files and E-mail. This type of traffic does not lend itself to the use of random access protocols. Also, it was estimated that each VSAT node would have a traffic to send most of the time and so DAMA protocols would be inappropriate. The use of TDMA allows access to the channel to be tailored to the nature of the inter-LAN traffic during given periods of time, is easily implemented, and may be easily modified to meet the demands of a growing network.

A selective repeat, sliding window protocol for use in conjunction with the TDMA link was formally specified using the SCM model. A selective repeat, as opposed a go-back-N, protocol was chosen due to its more efficient use of channel capacity across an error-prone channel with a long propagation delay. The two primary entities within the

67

selective repeat specification are the *transmitter*, and the *receiver*. Each of these entities are defined by a set of variables, a predicate-action table, and a finite state machine. The specification of the protocol was shown for a window size of 3 and extended to an arbitrary window size of N.

A limited reachability analysis for this protocol specification was shown. The protocol was proved to be free from deadlock if the channel is assumed to be error-free. A further reachability analysis was performed under the assumptions that only the first packet of a window would be received in error and all retransmitted packets were received correctly. For this case the protocol was also free from deadlock. The two analysis were combined and resoning presented to show the correctness of the protocol when any one packet within the window was corrupted. A full reachability analysis of the protocol was infeasible due to the combinatorial explosion of states.

Further work in this area is needed specifying the VSAT bridge for other LAN standards. Complete analysis of this protocol specification should be performed. Also, study of the possibility of connecting high speed networks such as FDDI via VSATs is needed.

REFERENCES

1. School of Information and Computer Science, Georgia Institute of Technology, Technical Report GIT-88/12, *Specification and Analysis of a General Data Transfer Protocol*, by G. M. Lundy and R. E. Miller, 1988.

2. Stanley, W. D., *Electronic Communications Systems*, Prentice-Hall, Inc., 1982.

3. Tanenbaum, A. S., *Computer Networks*, 2d ed., Prentice-Hall, Inc., 1988.

4. Stallings, W., *Data and Computer Communications*, 2d ed., Macmillan Publishing Company, 1988.

5. Freeman, R. L., *Telecommunication Transmission Handbook*, 2d ed., John Wiley & Sons, Inc., 1981.

6. Institute of Electrical and Electronic Engineers, Standard 802.3-1985, *Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification*, 1985.

7. Lundy, G. M., and Miller, R. E., "Analyzing a CSMA/CD Protocol Through a Systems of Communicating Machines Specification," to appear in *IEEE Transactions on Communications*.

8. Morgan, W. L., and Gordon, G. D., *Communications Satellite Handbook*, John Wiley & Sons, Inc., 1989.

9. Briefing book and notes provided to the author by Patrice Louie of Hughes Aircraft, 22 Feb. 1991.

10. Ha, Tri T., *Digital Satellite Communications*, 2d ed., McGraw-Hill, Inc., 1990.

11. Derfler, F. J., and Maxwell, K., "The Media Moves The Message," *PC Magazine*, v. 10 no. 15, pp. 351-374, 10 September 1991.

12. Rom, R., and Sidi, M., *Multiple Access Protocols Performance and Analysis*, Springer-Verlag New York, Inc., 1990.

13. Raychaudhuri, D., and others, "Design and Implementation of the SREJ-ALOHA Access Protocol for VSAT Data Networks," *International Journal of Satellite Communications*, v. 8, pp. 313-321, 1990.

14. Raychaudhuri, D., and Joseph, K., "Channel Access Protocols for Ku-band VSAT Networks: A Comparative Evaluation," *IEEE Communications Magazine*, v. 26 no. 5, pp. 34-44, May 1988.

15. Raychaudhuri, D., "Selective Reject ALOHA/FCFS: An Advanced VSAT Channel Access Protocol," *International Journal of Satellite Communications*, v. 7, pp. 435-447, 1989.

BIBLIOGRAPHY

Agrawal, Brij N., *Design of Geosynchronous Spacecraft*, Prentice-Hall, Inc., 1986.

Chakraborty, D., "VSAT Communications Networks—An Overview," *IEEE Communications Magazine*, v. 26 no. 5, pp. 10-23, May 1988.

Dattakumar, M. C., and McCloskey, J. S., "VSAT Networks: Architectures, Protocols, and Management," *IEEE Communications Magazine*, v. 26 no. 7, pp. 28-38, July 1988.

GTE Laboratories Communication and Network Theory Department Technical Note TN86-499.1, *Modeling and Analysis of Data Link Protocols*, by G. M. Lundy, Jan. 1986.

Holzmann, Gerard. J., *Design and Validation of Computer Protocols*, Prentice-Hall, Inc., 1991.

Lam, Simon S., "Satellite Packet Communication—Multiple Access Protocols and Performance," *IEEE Transactions on Communications*, v. COM-27 no. 10, pp. 1456-1466, Oct. 1979.

Lundy, G. M., and Miller, R. E., "Specification and Analysis of a Data Transfer Protocol Using Systems of Communicating Machines," to appear in *Distributed Computing*.

Raychaudhuri, Dipankar, "Announced Retransmission Random Access Protocols," *IEEE Transactions on Communications*, v. COM-33 no. 11, pp. 1183-1190, Nov. 1985.

Stratigos, J., and Mahindru, R., "Packet Switch Architectures and User Protocol Interfaces for VSAT Networks," *IEEE Communications Magazine*, v. 26 no. 7, pp. 39-47, July 1988.

Vaman, D. R., and Kumar, S., "Performance Analysis of a Multiple Transmission Protocol for VSAT Networks," *International Journal of Satellite Communications*, v. 8, pp. 307-312, 1990.

Wolejsza, C. J., and others, "Multiple Access Protocols for Data Communications via VSAT Networks," *IEEE Communications Magazine*, v. 25 no. 7, pp. 30-37, July 1987.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center   2
    Cameron Station
    Alexandria, Va. 22304-6145

2. Library, Code 0142   2
    Naval Postgraduate School
    Monterey, Ca. 93943-5022

3. Commandant of the Marine Corps   1
    Code TE 06
    Headquarters, U.S. Marine Corps
    Washington, D.C. 20380-0001

4. G.M. Lundy, Code 52   3
    Naval Postgraduate School
    Monterey, Ca. 93943-5022

5. Tri T. Ha, Code 62   2
    Naval Postgraduate School
    Monterey, Ca. 93943-5022

6. Patrice Louie   2
    Hughes Aircraft Company
    Space and Communications Group
    Building S64/B435
    P.O. Box 80002
    Los Angeles, Ca. 90008

7. Capt. Eugene S. Benvenutti   3
    75 Larkwood Ct.
    Stafford, Va. 22554

Thesis
B398225   Benvenutti
c.1   Selection and specifi-
           cation of a data link
           protocol for VSAT based
           inter-LAN communica-
           tions.