MEMORANDUM
RM-3763-PR
AUGUST 1964

ON DISTRIBUTED COMMUNICATIONS:
VII. TENTATIVE ENGINEERING SPECIFICATIONS AND PRELIMINARY DESIGN FOR A HIGH-DATA-RATE DISTRIBUTED NETWORK SWITCHING NODE

Paul Baran

PREPARED FOR:
UNITED STATES AIR FORCE PROJECT RAND

The RAND Corporation
SANTA MONICA • CALIFORNIA

MEMORANDUM
RM-3763-PR
AUGUST 1964

ON DISTRIBUTED COMMUNICATIONS:
VII. TENTATIVE ENGINEERING SPECIFICATIONS AND PRELIMINARY DESIGN FOR A HIGH-DATA-RATE DISTRIBUTED NETWORK SWITCHING NODE

Paul Baran

This research is sponsored by the United States Air Force under Project RAND—Contract No. AF 49(638)-700 monitored by the Directorate of Development Plans, Deputy Chief of Staff, Research and Development, Hq USAF. Views or conclusions contained in this Memorandum should not be interpreted as representing the official opinion or policy of the United States Air Force.

DDC AVAILABILITY NOTICE
Qualified requesters may obtain copies of this report from the Defense Documentation Center (DDC).

The RAND Corporation
1700 MAIN ST • SANTA MONICA • CALIFORNIA • 90406

Copyright © 1964
THE RAND CORPORATION

PREFACE

This Memorandum is one in a series of eleven RAND Memoranda detailing the Distributed Adaptive Message Block Network, a proposed digital data communications system based on a distributed network concept, as presented in Vol. I in the series.* Various other items in the series deal with specific features of the concept, results of experimental modelings, engineering design considerations, and background and future implications.

The series, entitled On Distributed Communications, is a part of The RAND Corporation's continuing program of research under U.S. Air Force Project RAND, and is related to research in the field of command and control and in governmental and military planning and policy making.

The present Memorandum, the seventh in the series, is a consideration of the engineering specifications of the proposed system's Switching Node. It is felt that a small, unmanned Switching Node (yet having higher throughput rates than are found in current large installations occupying thousands of square feet of floor space and requiring many people to maintain operations) can be built. The Distributed Adaptive Message Block Network proposal revolves around the feasibility of utilizing this small, unmanned Switching Node.

---

*A list of all items in the series is found on p. 83.

The Node is described in sufficient detail to estimate the equipment required. Timing calculations, together with a projected implementation scheme, provide a strong foundation for the belief that the construction and use of the Node is practical.

This Memorandum will be of interest primarily to those concerned with the details of design and operation of the distributed network. It may also be of casual interest to communications systems planners and designers having need to transmit digital data. The two other principal components of the distributed network--the microwave link and the Multiplexing Station--are described in Vols. VI and VIII in the series.

SUMMARY

This Memorandum details the description of and the design specifications for the Distributed Adaptive Message Block Network Switching Node. Documentation is presented to verify that the necessary computer operations can be performed within the prescribed timing constraints of limited circuitry, and the equipment components count is determined.

The Switching Node is capable of operating at non-synchronous data rates of up to 1.54-million bits per second per link (with simultaneous input and output, and at a redundancy level of four). It would appear that such a Node can be built within the present state of the art, employing digital computer techniques.

Beyond the design specifications, it is shown that implementation appears feasible, and the details of a particular implementation scheme are provided. Feasibility calculations are given, upon which the designs are based, showing the manner in which the specifications were selected.

The approximate general characteristics of the Switching Node are as follows:

Size of Unit ..... 3x4x6 ft; 72 cu ft

Total Power Consumption
(Including Air Conditioning) ..... 1530 watts

Weight ..... 2400 lb

Size of Core Storage (at 32 bits/word)... 4096 words

Speed of Core Storage ..... 1 μsec/cycle

Number of Equivalent
Flip-Flop Units 3600

Total Number of Transistors
(Including all Link Units) 14,000

Maximum Environment Temperature
for Operation ..... 122°F

Nominal Cooled Equipment Temperature ..... 59°F

The anticipated system reliability appears to be satisfactory and well within the overall requirements for the network as a whole. Approximate initial equipment price--in production quantities, but not including research, development, and installation costs--could be on the order of $150,000 per unit, anticipating extreme care is taken in design production and in system management.

The format of Part One is that of a design specification, and is followed by an equipment implementation alternative (Part Two) which meets both the specification and the requirements established by digital computer simulations* of the overall system.

---

*As reported in Vols. II and III in the series.

FOREWORD

In writing design specifications, one encounters a balance problem. If the specifications are too detailed, the equipment designer has little freedom to depart from these details in order to accomplish the desired end goal of reducing the amount of equipment. On the other hand, if the specifications are left too broad, the designer is unable to discern what might have been in the back of the specification writer's mind. The writer may have had in mind particular implementation methods, effecting equipment economies, which will not be apparent from the broad statements in the specifications. This Memorandum, therefore, combines specifications, feasibility calculations, and a proposed implementation.

As pointed out in the Preface, the general notions representing the distributed network concept are contained elsewhere in the series; the present volume is aimed at the designer and is laid out so as to facilitate a ready understanding of each particular aspect of the design of the network's key component, the Switching Node. The specifications *per se* (Part One) are succinctly enumerated and concisely worded, permitting easy reference to points of immediate interest. Embedded within the specifications themselves are, wherever applicable, discussions of the feasibility calculations.

ACKNOWLEDGMENTS

The writer gratefully acknowledges the continuing aid of T. O. Ellis and K. W. Uncapher of The RAND Corporation in answering an almost endless series of questions about the present and future state of the digital computer art. Many of their suggestions have been incorporated into the text without separate specific credit.

CONTENTS

PREFACE iii

SUMMARY v

FOREWORD vii

ACKNOWLEDGMENTS ix

FIGURES xiii

TABLES xv

PART ONE: GENERAL SPECIFICATIONS 1
A. PURPOSE 2
B. CONSTRUCTION 2
C. NUMBER OF CONNECTING LINKS 4
D. MAJOR ELEMENTS 5
Basic Timing Calculations 9
E. FAILURE PROPAGATION 12
F. CRYPTOGRAPHIC PROVISIONS 13
Cryptographic Clock Drift Calculation .. 16
G. RELIABILITY 18
H. SERVICING PROVISIONS 19
I. ERROR RATE 20
Error Rate Calculation 20
J. LINK AND LINK UNIT SPECIFICATION 25
Cryptographic Pseudo-Random Generator Calculation 27

PART TWO: IMPLEMENTATION PROPOSAL 29
I. DETAILED FLOW CHARTS 30
II. CENTRAL PROCESSOR DESCRIPTION 37
Programming Priority Rules 37
Intra-Switching Node Message Block Housekeeping Bits 44
Common Flag Registers 45
Line State Registers 46
Working Registers 47
Learning and Forgetting Function 48

III. INTERNODE TIMING CONSIDERATIONS 54
Time Required by Node to Process Message Block 54
Effects of Delay Times in Message Propagation and Error Control 55
Use of Satellite Links in the Distributed Network 61
Timing Requirement for Very-High-Data-Rate Time Division Multiplexed Links 71
IV. HARDWARE 73
Logical Complexity 73
Parts Count Calculations 76
Reliability 77
Heat and Power Calculations 80

LIST OF PUBLICATIONS IN THE SERIES 83

FIGURES

Figure		
1.	Equipment at the Switching Node	6
2.	Central Processor	33
3.	Input Link Unit	34
4.	Output Link Unit	35
5.	Buffer Units	36
6.	Subroutine DESTROU	40-41
7.	Subroutine INSTOR	42-43
8.	Subroutine UPDATE	49
9.	Learning and Forgetting Operations from Observations of Handover Numbers	50
10.	Subroutine OUTSTOR	52-53
11.	Transmission Time and its Effects on Verification Timing	59
12.	Low-Altitude Satellite Link	62
13.	Timing Relationship Between Switching Nodes A and B	66
14.	Synchronous Satellite Transmission Link Length	70
15.	Timesharing Two Channels on One Link	72
16.	Two Circuits for Dividing by $1 + X^3 + X^4 + X^5 + X^6$	74
17.	Low Ripple Counters	75

TABLES

Table		
I	Central Processor Major Operations	38
II	Message Block Housekeeping Bits	44
III	Common Flag Registers	45
IV	Line State Registers	46
V	Working Registers	47
VI	Allowable Fractional Values of k_1 and k_2	51
VII	Tradeoff Between Data Rate and Distance if No Additional Storage is Used	60
VIII	Number of Equivalent Flip-Flops Required	76

Part One

GENERAL SPECIFICATIONS

A. PURPOSE

A1. Together with suitable Multiplexing Stations and Communications Links, the Switching Nodes shall form a high-data-rate distributed network (see ODC-I*).

A2. The specified function of the Switching Node shall be to transfer Message Blocks of information from link to link in a highly efficient manner while remaining generally insensitive to heavy link and node destruction.

A3. The distributed network shall be able to simultaneously process signals from a number of separate Terminal Stations† without unfavorable reaction to interference of either internal or external cause.

A4. The complete system shall process military and/or civilian traffic for a large number of subscribers on a common user or common carrier basis.

B. CONSTRUCTION

B1. Lowest-cost construction commensurate with a minimum ten-year overall total system cost shall be a fundamental design criterion.

---

*ODC is an abbreviation of the series title, On Distributed Communications; the number following refers to the particular volume within the series.

†The Terminal Stations are connected to the Switching Nodes via the Multiplexing Stations.

B2. The system shall provide fully stable operation with any number of Switching Nodes inoperative.

B3. Dual-diversity and other premium construction techniques shall not be used except where they can be shown to reduce overall, ten-year costs.

B4. All nodes shall be built of interchangeable units, replaceable without soldering or adjustments.

B5. Full advantage shall be taken of mass-production techniques, since a large number of identical Switching Nodes will be required, and since much of the equipment in each Switching Node is composed of identical units.

B6. Wherever possible, no individual plug-in box shall be heavier or larger than can be carried by one man.

B7. Bench-test jigs, not forming part of the Switching Node, shall be available to repairmen to permit location of defective flip-flop stages. Individual flip-flops need not be plug-removable, but in the interest of economy, may be soldered, welded, or microminiaturized, and fastened to larger circuit boards.

B8. Electrical components used in the Switching Node shall be of present-day state-of-the-art; all design calculations are based upon components available at the time of this writing (December 1962).

C. NUMBER OF CONNECTING LINKS

C1. Each node shall be designed to process a maximum of eight duplex links. (Inasmuch as most of the payoff for redundancy of connectivity is obtained at the modest redundancy levels of three or four, this number is deemed sufficient.)

C2. Each duplex (simultaneous two-way operation) link shall be capable of being connected either to adjacent Switching Nodes or to Multiplexing Stations.

C3. The Switching Node shall be capable of processing traffic at whatever data rate is demanded by the connected link, with a maximum rate of 1.54-million bits per second.

C4. When externally synchronized links are used, each link shall be capable of operating from remote timing and be capable of slaving its operations to that of the remote timing device.

C5. The Switching Node shall be capable of operating with any combination of links, using either local or remote timing, and with different data rates over the various connected links.

D. MAJOR ELEMENTS

The Switching Node shall be composed of the following major assemblies, which are further divided into major subassemblies (see Fig. 1):

D1. Eight Link Units--Each Link Unit shall be comprised of an Input Link Unit and an Output Link Unit. The Input Link Unit shall provide a termination for the Input Line and shall contain means for error detection and cryptographic decoding of the input signal. The Output Link Unit shall contain means for encrypting outgoing Message blocks and for inserting error detection tags. Each Link Unit shall contain cryptographic key base storage and key generation apparatus. Each Link Unit shall contain local timing equipment to synchronize the input and output message streams.

D2. Eight Buffer Units--Each Buffer Unit shall be comprised of an Input Buffer and an Output Buffer. Both the Input and the Output Buffers shall contain two 32-bit registers.* Buffer unit capability shall be to perform serial/parallel and parallel/serial transformations. Each

*32-bit registers are tentatively chosen as a compromise between the amount of equipment required for longer word length, and the limitation of the cost of high-speed random access computer memories if one attempted to use a shorter word length.

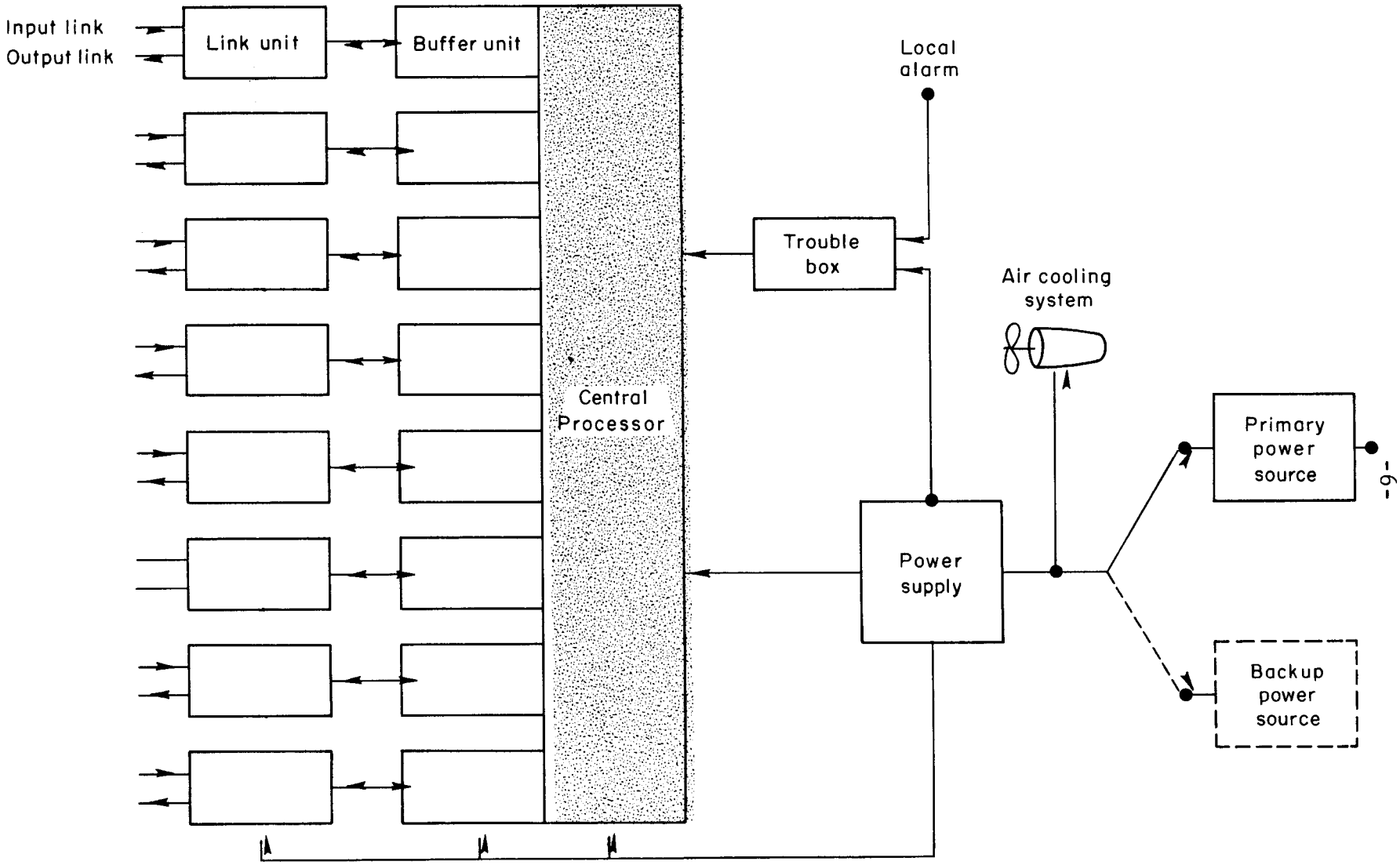


Fig. 1--Equipment at the Switching Node

Input and Output Link Unit shall be capable of operating in a serial-bit manner at a timing rate that may be asynchronous to the Central Processor Unit. It is necessary to block the input serial stream into parallel words for most effective processing by the Central Processor. A similar requirement for parallel-to-serial output conversion exists for outgoing signals. Two Buffer Registers shall be provided, so that while one register is in the process of being filled, sufficient time is allowed to the Central Processor to find a convenient moment to process the already-filled register requiring attention.

D3. Central Processor Unit--The Central Processor Unit is a digital computer type subsystem organized along the lines of a multi-sequence processor.* Several different computer programs are handled simultaneously by hopping to the Buffer Unit that needs immediate attention. The intermediate results at the points of program interruption are stored so that processing can be continued at the interrupted point without the delay of having to back up. The Central Processor is a

*Ackley, J. N., "The Multi-Sequence Computer as a Communications Tool," Proceedings EJCC, No. 16, 1959, pp. 114-119.

time-shared computer simultaneously serving eight input and eight output channels. The Central Processor Unit shall contain a high-speed magnetic core memory, together with necessary read/write amplifiers and word selection equipment. Tentatively, a 1-μsec read/write cycle time memory of about 4000 32-bit words is indicated. Such a choice is well within the present state of the art--indeed is currently available and being marketed. The Central Processor Unit shall contain a Status Buffer connected to the Buffer Units to inform the Central Processor of buffers needing attention. A bank of Index Registers shall record the address location of the most recent word to or from each Input or Output Link that has been processed by the Central Processor Unit. Program memory shall be of the "plug-in, read-only" type, to allow system program modification. Inasmuch as the Central Processor is most often involved in read-in/read-out operations, handover table modification, and handover number sorting* (with arithmetic operations performed only at rare intervals), the Control Unit of the Central Processor shall be designed to operate

*The "handover" concept is fully described in ODC-I.

with a small-order code designed specifically for performing a few commands efficiently. A simple sorter function shall be built into the Control Unit. This will allow the output line with the lowest handover number to be rapidly determined without wasting Central Processor time performing lengthy sequential comparison operations.

BASIC TIMING CALCULATIONS

1. All traffic is processed through the Central Processor.
2. Worst-case assumption: 8 lines at 1,540,000 bits per second throughput: 1,540,000 x 8 = 12.32 megabits/sec.
3. Assume that the memory is composed of 4096 words, each 32 bits in length: 4096 x 32 = 131,072 bits.
4. Assumed storage required for all in-transit messages for all 8 lines: 8 lines x 1024 bits per line = 8192 bits; 3 verification copies are needed (one for each of the last 3 Message Blocks handled) plus a copy of the Block being processed, = 4 x 8192 = 32,768 bits for message storage (the verification copies are called "carbon copies").

5. To store the handover number table for 1000 stations at 8 bits x 8 lines

   = 64,000 bits
   + 32,768 bits for Message Block storage
   = 96,768 bits.

6. Thus, total high-speed memory storage

   = 3024 32-bit words
   + 1072 32-bit words program and spare.

7. Assume that all input/output buffers are 32-bit word length. At a throughput rate of 12,320,000 bits/sec, there will be about

   $$\frac{12{,}320{,}000 \text{ bits/sec}}{32 \text{ bits/word} \times 2} = 1.93 \text{ words/}\mu\text{sec.}$$

   As most of the time will be spent in reading these words into and out of the high-speed core, we shall tentatively choose a 1-μsec cycle time memory. If this proves insufficient, we then face the choice of a faster memory or a longer word length. However, with careful design one can overlap many operations and we shall try to live within this tight constraint.

D4. Power Supply--A Power Supply Unit is needed to convert primary input power to the voltages required by the transistorized equipment. The Power Supply shall contain means to detect a failure of the

primary power source and to provide capability for transient-free switch-over to an emergency secondary power source. In the event of restoration of primary power, the power supply shall provide transient-free switch back to the primary power source and provide signals to shut down the secondary power source.

D5. Trouble Box--A Trouble Box shall contain a register whose bit-states are controlled by local switch closures. The Trouble Box shall monitor the status of local burglar alarms, locks on the cryptographic equipment, local temperature, power source status, and signals from the Central Processor indicating any out-of-normal conditions, such as inoperative links. The output of the Trouble Box shall be formed into Message Blocks by a subroutine within the Central Processor and transmitted into the network, directed toward the nearest Repair Depot. Such trouble messages shall be transmitted only upon receipt of an abnormal condition by the Central Processor.

D6. Air-Cooling System--The electronic equipment comprising the Switching Node shall be exclusively of solid-state construction; refrigeration is not mandatory under all environmental conditions. However, as the mean time between failures of

the germanium transistorized equipment can be markedly extended by air conditioning, such equipment shall be included.* As mechanical air conditioning equipment may be unreliable, its failure shall not constitute sufficient grounds to cause the Switching Node to be shut down, provided that suitable backup capability is provided.

E. FAILURE PROPAGATION

E1. It is imperative that the Switching Node never propagate any possible malfunctions into the remainder of the distributed network. A means of testing incoming signals and disconnecting any link feeding data not conforming to a rigid data format shall be included.

E2. Each of the last four Switching Nodes to process a Message Block shall imprint the Message Block with the Link Number used in transmission; this will allow tracking down any malfunction not detected automatically otherwise.

E3. The logical design of the Switching Node should be premised on expectation of unmanned operation of the nodes and low-quality, accident-prone maintenance personnel.

---

*Since the time this section was first written, it has become apparent that low-cost, silicon transistors are available, eliminating much of the need for life-prolonging cooling.

F. CRYPTOGRAPHIC PROVISIONS*

F1. The system design shall include cryptographic apparatus as an integral part of the Switching Node. While this is not a conventional procedure, it is felt that to do otherwise would require the later addition of equipment duplicating many of the functions already being performed within the Switching Node.

F2. Two levels of cryptography will be used in this system: terminal-to-terminal, and link-to-link. Because of the large number of unmanned nodes in the network, link-to-link encryption cannot be considered to be a high-confidence security measure. If end-to-end encryption were used alone, the addresses of all Message Blocks would necessarily have to be transmitted in the clear in order that the Switching Node could determine routing. This would be undesirable, as rapid changes in network loading status would be conveyed to all listeners. However, a combination of link-to-link and terminal-to-terminal encryption would appear to extract

*The government agency responsible for cryptographic considerations does not normally enter initial system design discussions. However, the high data rates and the large number of nodes used make it advisable that preliminary cryptographic requirements be considered by the designer of the Switching Node (see ODC-IX).

such a high price from an eavesdropper simply to determine Message Block heading data, that it is probable that only very highly classified traffic need be given the terminal-to-terminal double encryption treatment. Thus, it is tentatively suggested that the bulk of the traffic can be safely handled by link-to-link encryption. As a practical matter, all traffic in the network can thus be considered as being encrypted.

F3. All cryptographic operations shall be performed in the Link Units, and none in the remainder of the system. However, it is necessary to protect the entire system since message headings are in the clear within the Central Processor Unit.

F4. Each separate Link Unit shall contain a separate Cryptographic Key Box, sealed by both a key and a combination lock. Any movement of the combination lock or key shall be transmitted to the Trouble Box for retransmission.

F5. Each Cryptographic Key Box shall contain two or more key bases for transmission and two or more key bases for reception, together with means of synchronization.

F6. One of the two key bases shall be changed at least once each month. On the following month, or applicable period, the previously unchanged key

base shall be changed. The period of use of a key base shall be chosen to allow a single person to change the keys sequentially at both ends of a link (instead of requiring two people, as would be the case if only one key base were used).

F7. The key base shall be of a plug-in type and be fundamentally volatile in nature; i.e., the information contained in the key base shall be easily and rapidly destroyed if any attempt is made to tamper with or determine its contents.

F8. The resynchronization used in the cryptographic apparatus shall be such as to permit an automatic pull-in after the communications link has been interrupted for as long as twelve hours.

F9. To permit low-cost cryptographic clocks to be used and to meet the requirement of a long link-interrupt time, each Message Block on each link shall contain a Block Sequence Number. Tentatively, the Block Sequence Number will be eight bits (modulo 256) in length (see below). This number is incremented by one for each successive Message Block.

F10. The Key Base Counter shall be capable of operating without recycling or repetition for a period much in excess of the time between key base changes.

F11. An eavesdropper's knowledge of the construction of the Switching Node, his access to input traffic, and his knowledge of the data format shall be assumed. The generator key shall be undecipherable using any known technique of analysis and using any known computer, working full time on such an analysis for a period of up to five years.

F12. When no valid traffic is being sent, dummy traffic derived from a "noisy" generator shall be sent as filler.

F13. The Switching Node shall be housed in a structure able to delay a forced entry in excess of one hour.

F14. Automatic alarms shall allow automatic destruction of all information in the core of the Central Processor and the key base upon detection of unauthorized tampering.

F15. Switching Nodes shall be situated so that local police protection can be obtained if needed.

CRYPTOGRAPHIC CLOCK DRIFT CALCULATION

1. Assume that the link between two Switching Nodes is operating at 1,540,000 bits/sec.
2. Assume that the Message Block length is 1024 bits.

3. Assume that both the transmitting node and the receiving node are in cryptographic synchronism at time t = 0.
4. Assume that the link between the two Switching Nodes is interrupted at t = 0.
5. Assume that each Link Unit contains an inexpensive piezoelectric time base that does not drift more than 10^{-6} sec/sec.
6. Assume that each Message Block contains a Block Sequence Number.
7. Assume that the interrupted link is restored at t = 12 hr.
8. The number of bits necessary to contain a number equal to the maximum number of drifted Message Blocks is based on the following calculations:
   a) Assume, as a worst-case condition, that the drift of both clocks is in opposite directions.
   b) Total number of blocks in 12 hr

$$= \frac{12 \text{ hr} \times 3600 \frac{\text{sec}}{\text{hr}} \times 1{,}540{,}000 \frac{\text{bits}}{\text{sec}}}{1024 \frac{\text{bits}}{\text{message block}}}$$

$$= \frac{(1.2)\ (3.6)\ (1.54)\ (10^7)}{(1.024)} \text{ message blocks}$$

$$= 6.5 \times 10^7 \text{ message blocks.}$$

c) Drift rate

$= (2 \times 10^{-6})(6.5 \times 10^{7})$

message blocks

= 130 message blocks.

d) $2^{R} \geq 130$

R = 8 bits.

e) Time to drift out of synchronism

$= \frac{256}{130} \times 12$ hr

= 19.2 hr.

G. RELIABILITY

G1. While unit reliability in a distributed network is not needed to the same degree as in the case of conventional communications network elements, conservative design practice shall be used to produce an expected mean time between failures (MTBF) of not less than 30 days for the Central Processor and Power Supply or for any single Link Unit. (See p. 77 for a detailed estimate of the proposed implementation's MTBF reliability values.)

H. SERVICING PROVISIONS

H1. All Switching Nodes shall be capable of unmanned operation.

H2. Link failures shall be repaired during routine test and maintenance periods.

H3. A complete Node failure shall, wherever possible, be indicated by a Trouble Box indication to adjacent Multiplexing Stations. In such cases, a repairman shall be detached to effect repairs.

H4. The field maintenance repairman shall narrow trouble location to within a single major assembly or subassembly, but when in the field shall generally not pin-point the trouble to a specific component. The field maintenance repairman shall carry a full complement of major replacement assemblies in his repair truck. Pin-pointing of faults in specific components and the replacement of defective components shall generally be performed at a Maintenance Center.

H5. All components used shall be commercially available to eliminate the necessity for the maintenance of large stocks of components.

H6. All field maintenance personnel shall have appropriate security clearances.

I. ERROR RATE*

I1. The Switching Node shall be capable of an overall user-to-user system error rate of less than one in 10^8 bits or Message Blocks,† provided that the raw error rates of the links comprising the distributed network have an average value of less than one in 10^5 bits in error.‡

I2. Inasmuch as the statistical error distributions of the low-cost transmission media being considered for use within the distributed network have not yet been fully determined, the calculations for error distribution shall not assume a Gaussian, hyperbolic, or similar distribution that could introduce an optimistic bias into the error rate calculation.

ERROR RATE CALCULATION

1. Assume that automatic error detection and repeat transmission shall be used.
2. Assume that a Message Block length of 1024 bits is used, including error detection symbols.

*Inasmuch as this system shall be used to transmit digital data between computers, a very low overall system error rate is specified.

†It is assumed that if a single bit is in error, the entire Message Block is in error; if a Message Block is in error, all bits of the Block are in error.

‡Expected link error rate is one in 10^{-6} or less (see ODC-VI).

3. Assume the cyclic code method described by W. W. Peterson and D. T. Brown is used.*

4. Using the cyclic code technique, the binary Message Block to be transmitted is divided by a fixed Boolean polynomial. Both the Message Block (less the check digits) and the remainder (which forms the check digits) are transmitted. The receiving station performs a verification operation on the received message using a Boolean polynomial identical to that used in the original transformation. If there are no errors in transmission, the remainder is zero. But, if there is an error in transmission, it can be shown that the probability of creating a nonzero remainder can be made arbitrarily low by proper choice of the Boolean polynomial used in the two operations. This coding scheme is particularly attractive for the proposed system inasmuch as the divide and multiply

*Peterson, W. W., and D. T. Brown, "Cyclic Codes for Error Detection," Proceedings of the IRE, Vol. 49, No. 1, January 1961, pp. 228-235.

operations are easily performed by a short shift register with feedback connections. Further, the technique is highly efficient, requiring only a small number of check digits for very powerful error filtering.

5. Consider, for example, the use of the following coding polynomial, $P(X) = 1 + X^2 + X^{13} + X^{22}$. A cyclic code error detection encoder or decoder using this polynomial can be built using only a 22-stage shift register. Only 2.3 per cent of the transmitted data rate need be expended on error detection.
6. According to Peterson, this resulting code should be able to detect: two bursts of combined length 12 or less; any odd number of errors; a burst of 22 or less; 99.99996 per cent of the bursts of length 23; 99.99998 per cent of longer bursts.
7. If even better performance is required, it can be obtained by the choice of a slightly longer coding polynomial.
8. As a worst-case assumption in the specific system of interest, assume a raw link error rate of 1×10^{-5}. Since the error

detection scheme is perfect for error blocks of less than 12 bits, we could then expect only about one such 12-bit or greater error in about 1200 Message Blocks, each 1024 bits in length. Of these, 99.99996 per cent will be caught. Thus, the actual probability of an undetected error passing through the system will be equal to the probability of an error occurring in a block, times the probability of the error passing through undetected:

8.3×10^{-4}	probability of any Message Block being in error
$\times 4.0 \times 10^{-7}$	probability of error not being detected
$= 3.32 \times 10^{-10}$	probability of an undetected error slipping through on a single link
$= 3.32 \times 10^{-9}$	probability of an undetected error slipping through 10 tandem links.

9. Another, and completely different, source of errors should also be considered. This is the possibility of a catastrophic Switching Node failure occurring just after a Switching Node issues a verification of correct receipt of a message.

If a conservative mean time between failure of one month is assumed for the Central Processor Unit within the Switching Node, then such an occurrence can take place only once during this period. The probability of loss of a message due to this cause is then approximately:

$$\frac{30 \text{ days} \times 24 \text{ hr} \times 3600 \text{ sec}}{6.7 \times 10^{-4} \frac{\text{sec}}{\text{Message Block}}}$$

$$= \frac{3 \times 2.4 \times 3.6}{6.7} \times 10^{-9}$$

$$= 3.87 \times 10^{-9}.$$

10. We can expect three primary sources of errors within the system:

    a) The probability of an undetected error caused by a noisy link passing through the error detection filter, equals 3.32×10^{-9}.

    b) The probability of a Switching Node failure, after having sent a receipted acceptance to an adjacent node, equals 3.87×10^{-9}.

    c) The probability of a circuitous path being taken during a transient network overload, longer than about

twice the minimum shortest network extremity path-length, is less than 10^{-8}, under the worst-case assumption of a heavily loaded network.*

11. Thus, it is felt that the target average overall 10^{-8} system error rate appears to be an attainable goal.

J. LINK AND LINK UNIT SPECIFICATION

J1. Each Switching Node shall have provision for accepting up to eight Link Units.

J2. Each Link Unit shall be capable of simultaneously sending to and receiving from any adjacent Switching Node.

J3. Each Link Unit shall be able to operate at data rates up to 1,540,000 bits per second.

J4. Each Link Unit shall have means to permit adjustment of the transmission and reception rate so as to make most economic use of the transmission facility. It shall be sufficient that the Link Unit be able to operate at up to six different data rates.

J5. Each Link Unit shall have means to operate either on independent timing or to have its timing slaved

*See ODC-III.

to its remotely terminated adjacent Switching Node.

J6. In the event of a line failure or propagation fade, the Link Unit timing shall be capable of pulling into synchronization after circuit restoration within a period of up to 12 hours after the time of failure.

J7. The Link Unit shall be designed to operate with unreliable and noisy communications links. A communication line shall be considered as operating well if it is exhibiting a short-term error rate of 10^{-5} or better.

J8. To avoid the necessity of transmitting DC levels,* every sixteenth bit shall be selected so that not more than 15 consecutive bits are ever transmitted with the same polarity.

J9. It shall be assumed that all communication lines are exposed to public access, but it shall be impossible for traffic inserted into any line by an outside agent to be propagated within the system. (For example, if one were to record traffic on a line and play it back a short time later, such traffic should be automatically rejected and not be allowed to propagate.)

---

*Required in certain types of data links, but not in the mini-cost microwave link described in ODC-VI.

J10. Input timing jitter shall be less than ± 40 per cent of a one-bit period.

J11. Output timing jitter shall be less than ± 10 per cent of a one-bit period.

J12. Each Link Unit shall contain internal cryptographic key generation equipment able to create binary streams in excess of three months operation at 1,540,000 bits per second.

CRYPTOGRAPHIC PSEUDO-RANDOM GENERATOR CALCULATION

1. A cryptographic generator period of three months is assumed.
2. A shift register has a maximum period of $N2^N$ bits, where N equals the number of stages of the register.
3. Assume a 1,540,000-bit rate.
4. $N2^N > 2^N \geq$ 3 months = 3 x 30 days x

$$24 \frac{hr}{day} \times 3600 \frac{sec}{hr} \times 1{,}540{,}000 \frac{bits}{sec}$$

$$2^N \geq (3)\ (3)\ (2.4)\ (3.6)\ (1.54)\ (10^{11})$$

$$\geq 1.2 \times 10^{13} \text{ bits}$$

$$N \geq \frac{1}{\log_{10} 2} \log_{10} (1.2 \times 10^{13})$$

$$\geq (3.3)\ (13 + 0.079)$$

$$N = 43 \text{ stages of flip-flops.}$$

Part Two

IMPLEMENTATION PROPOSAL

I. DETAILED FLOW CHARTS

The following block diagrams and flow charts describe the Central Processor, the Link Units, and the Buffers. The logical design was taken only to the point necessary to determine the major equipment elements needed to perform all the known key functions within the circuitry-timing constraint. No attempt has been made to define a final system configuration.

Intuitively, it is felt that there is enough "fat" in the layout to counterbalance the parts inadvertently omitted.

Separate flow diagrams (Figs. 2-5) are included for the Central Processor, the Input Link Unit, the Output Link Unit, and the Input and Output Buffers (both on a single sheet).

The abbreviation F/F stands for "equivalent flip-flops," which is a unit of circuit complexity corresponding to the number of components required by a single flip-flop stage, together with a modicum of input gating logic.

Most of the Switching Node is to be built of flip-flops connected in a highly iterative register-type structure. Certain of the registers of the Central Processor will require a very heavy logical gating. However, the use of a "standard" flip-flop, for purposes of determining the part-count, appears justified by the heavy counter-balancing number of lightly gated units found in the eight Input, Output, and Buffer Units. The clock speed of the

Input, Output, and Buffer Units must be that of the incoming bit rate: 1,540,000 bits/sec. However, a sizable portion of the Central Processor operates most economically at a much higher speed. A 10-megabit/sec capability is used within the Working Registers. A transfer into storage can be performed by present-day 1-μsec cycle cores in about 0.7 μsec for "write-only," and 0.3 μsec for "read-only."

On the left side of Fig. 2 is a bank of flip-flop registers which monitor the activities of each of the eight separate Link Units. These provide the intercommunication capability between the Central Processor and the Link Units. Other registers indicate the points of program interruption and permit the Central Processor to hop from Link Unit to Link Unit, depending on which requires attention, in the style of a conventional multi-sequence processor.

Three 32-bit registers intercommunicate between a common high-speed core storage unit and the Link Units. A 32-bit portion of a Message Block is transferred to a Working Register. Once in the Working Register, the input word is read into core storage at a location determined by the Line Number (three bits), plus Carbon Copy Number (next two bits), plus Message Block word number (next five bits). Although it does not seem required, an Index Register has been included.

A "read-only, plug-in" type wired logic provides program memory.

The Input Link Unit first restrobes the input pulse train. Next, it strips every sixteenth bit, which the Output Link Unit inserted to avoid the need for DC coupling on the transmission links. Next, error detection is performed by a shift register and the output stream is logically added to a cryptographic stream generator to produce a clean text output. Clocking means are included to permit automatic resynchronization of the input wave train.

The Input Buffer Unit performs a serial-to-parallel conversion of the input binary stream; the Output Buffer performs a parallel-to-serial conversion.

The Output Link Unit is almost a mirror image of the Input Unit and performs the encrypting, error detection, symbol addition, and every-sixteenth-bit blanking operation.

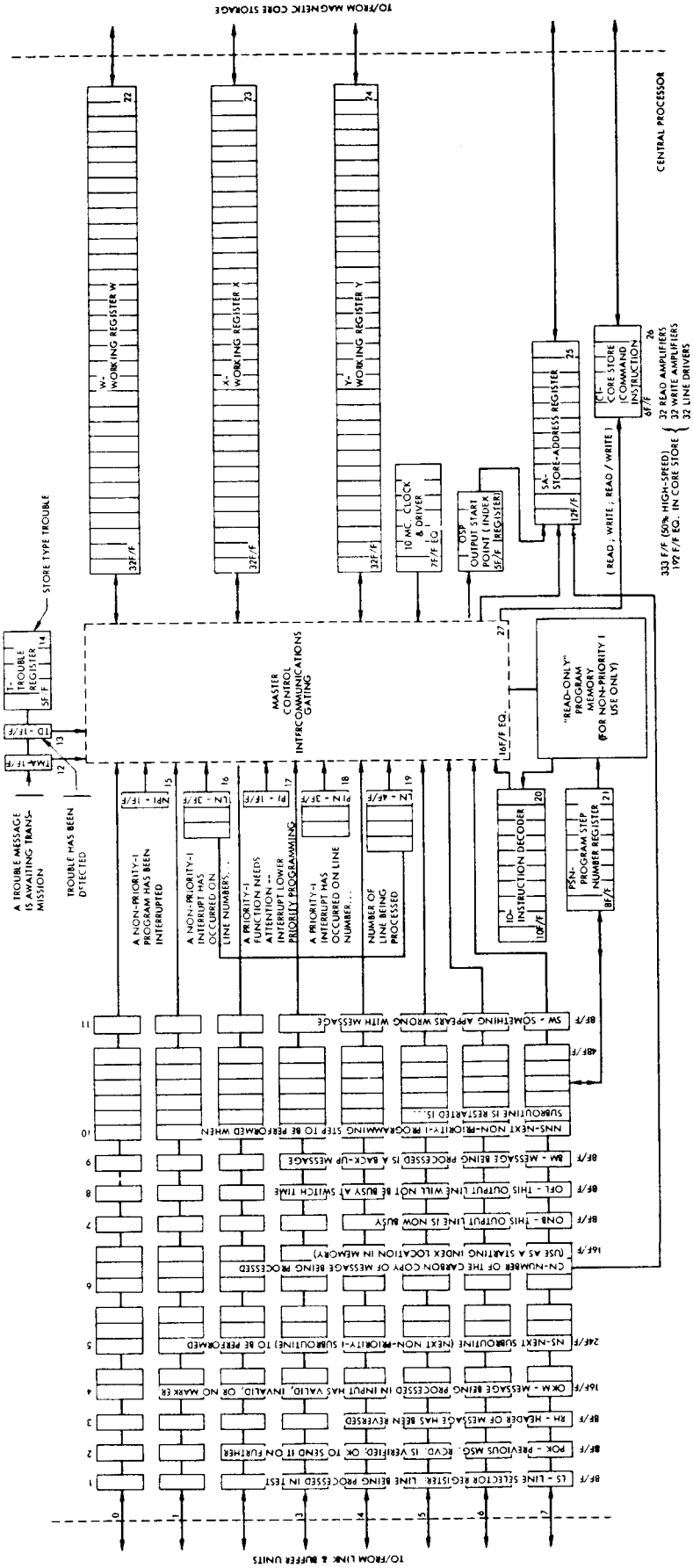


Fig. 2--Central Processor

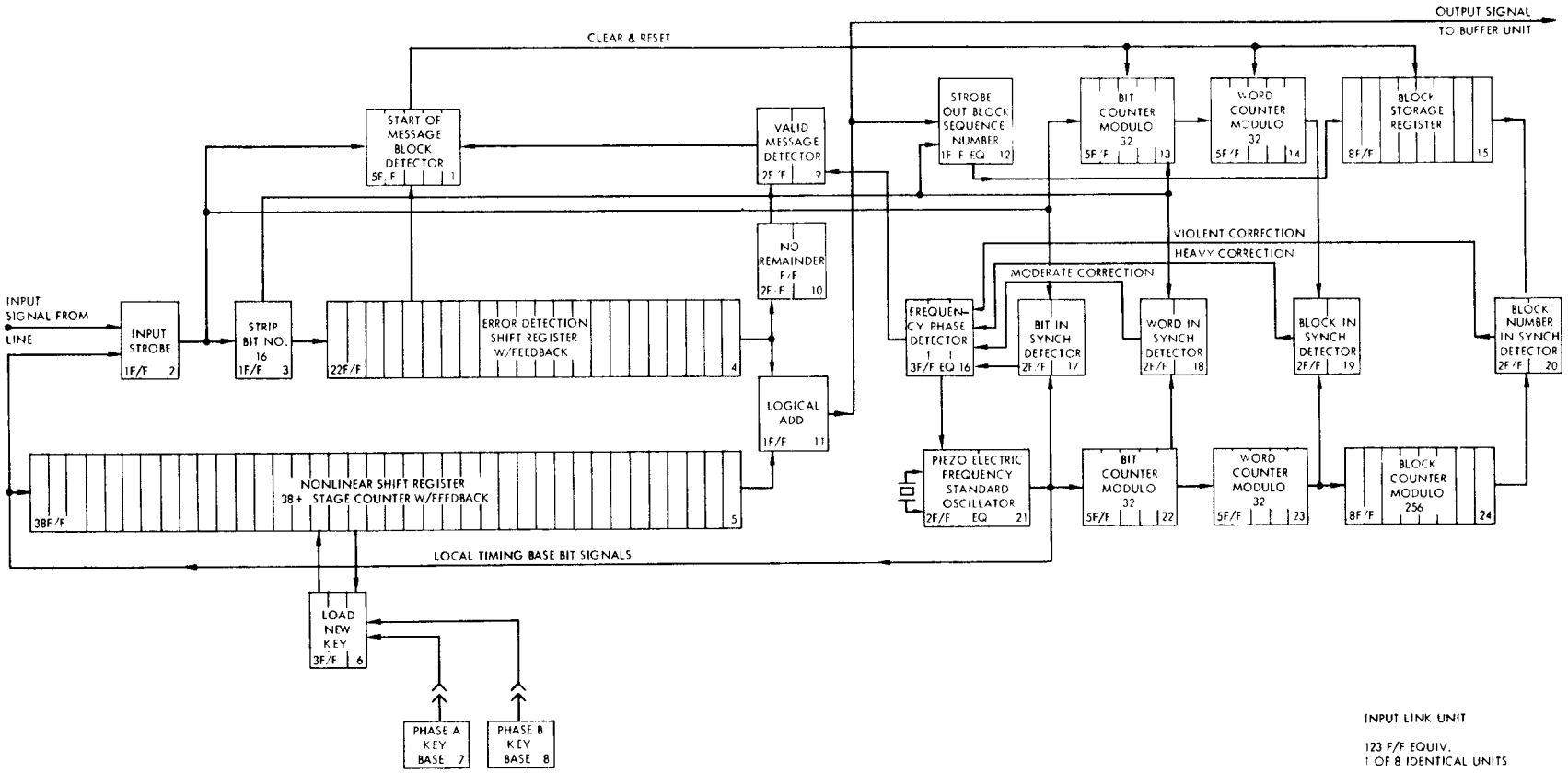


Fig. 3--Input Link Unit

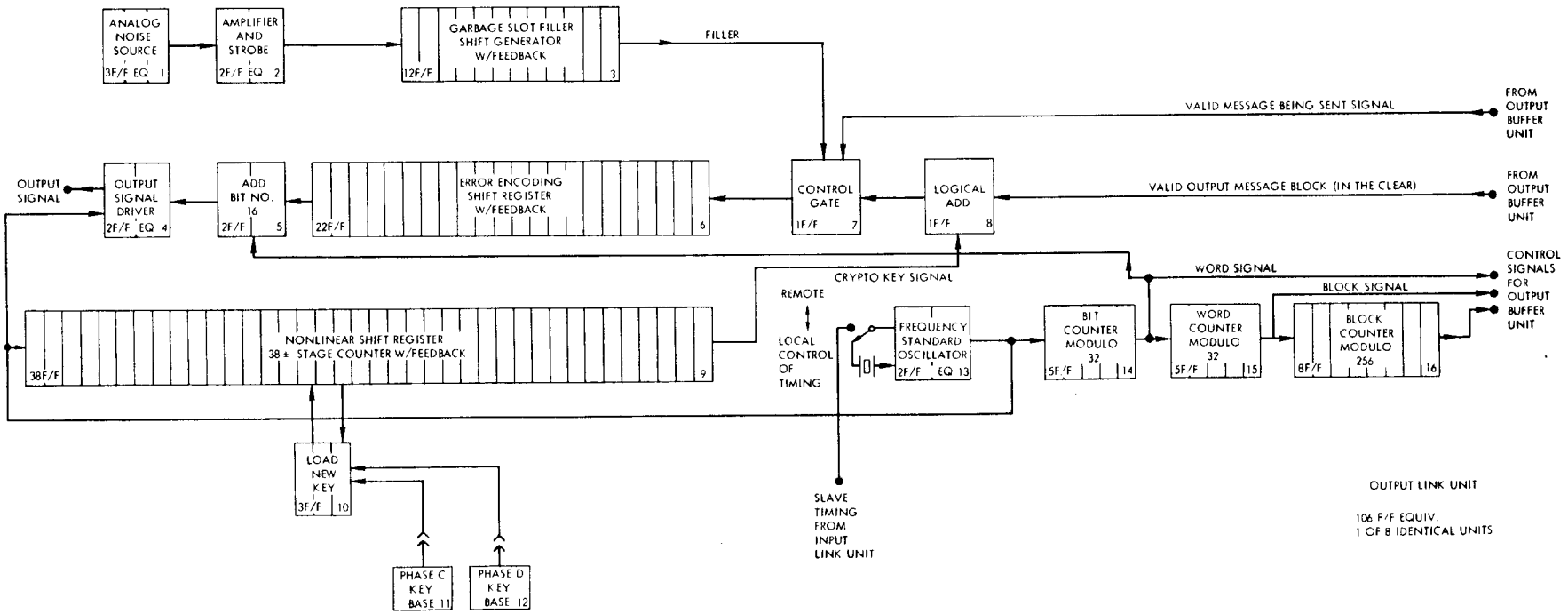


Fig. 4--Output Link Unit

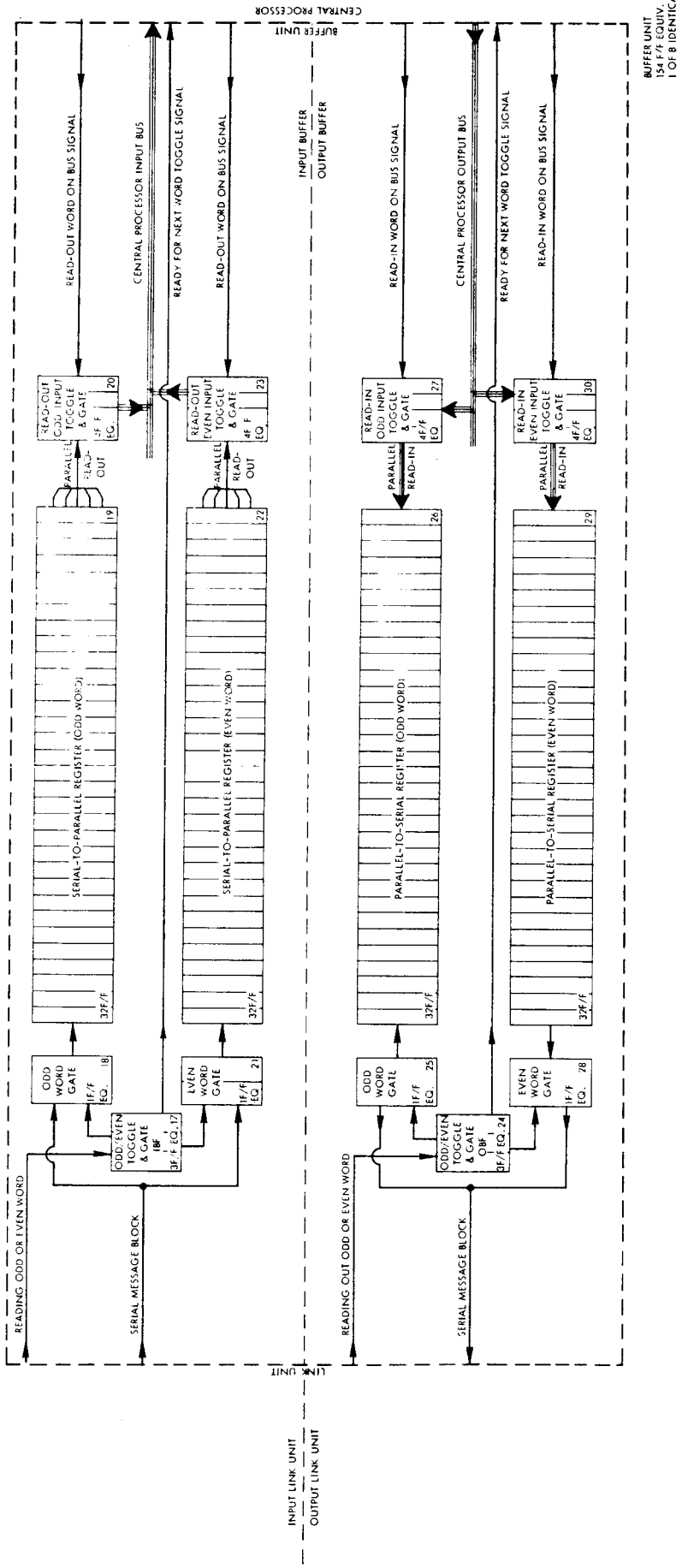


Fig. 5--Buffer Units

II. CENTRAL PROCESSOR DESCRIPTION

The key operations that must be performed by the Switching Node are presented in Table I. No attempt will be made to describe the operation of the Central Processor in any greater detail.

The priority order of the operations, the number of bits allocated for specific purposes, and the purpose of the key registers are presented in tabular form in the following subsections. These, together with the flow charts, delineate the operations that are carried out in the Link Units, Buffer, and Central Processor.

The flow charts (Figs. 6-8, 10) are a combination representation of wired-in, highly parallel, logical state testing, and serial steps of the conventional type general-purpose computer operations. An asterisk denotes where general-purpose computer type commands requiring core storage are implied. The remaining blocks are wired-in tests performed rapidly and continuously.

The subroutines that are most critical in timing requirements have been flow-charted in some detail, while those operations which occur less often and which are not too complex have not been detailed.

PROGRAMMING PRIORITY RULES

This section establishes the order in which the various subroutines within the Central Processor are handled. As

Table I

CENTRAL PROCESSOR MAJOR OPERATIONS

Frequency	Subroutines	Each Time, μsec	Total Time Required Per Message Block, μsec
32	Input to Storage from Buffer	1.2	38.4
1	Decide Route: Read "To" Address of Message Block; Read H.O. Number Table into Sorter; Sort.	6	6
1	Update H.O. Table: Read "From" Address of Message Block; Read H.O. Table; Multiply: Shift Add Shift Add; Store H.O. Table.	6	6
1	Error Verification All Checks OK?; Is Header Reversed?; Is H.O. Number ≥ K?; Reverse Header; Shift Trace Tag; Repeat Carbon Copy; Bad Message Block--Try New Route; Error Noted--Do Not Relay; Choke Input.	Est. < 12	12
32	Output from Storage to Buffer	1.0	32
RARE	Trouble Message		

the unloading of Input Buffers and the loading of Output Buffers cannot be delayed while a multi-step arithmetic subroutine is being processed, without incurring the possibility of a traffic overload, a special-treatment processing-procedure grade is defined:

Priority I:	Input-Buffer-to-Storage Subroutine (IBTS).*
	Output-Buffer-to-Storage Subroutine (OBTS).

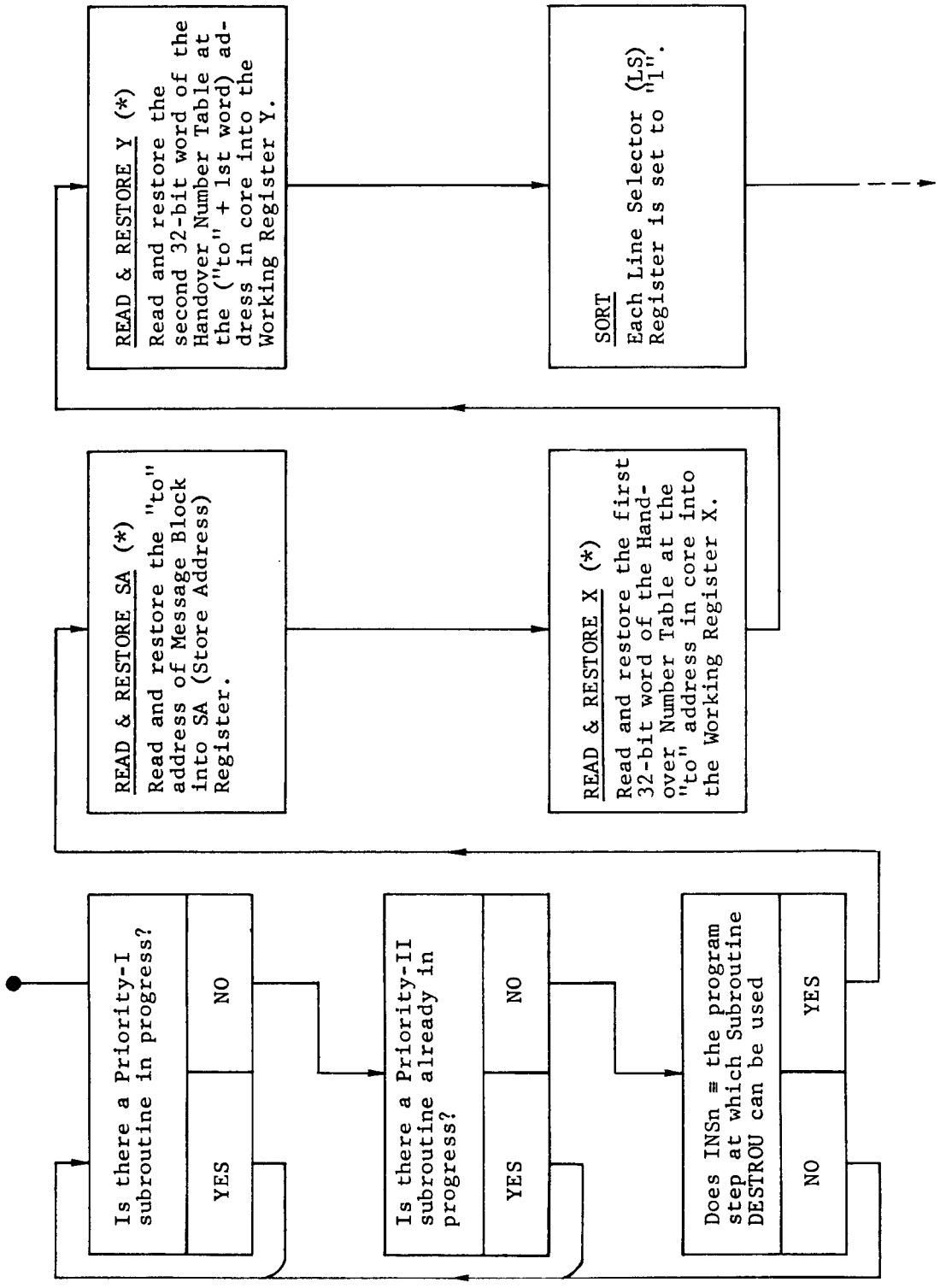
Lower-priority subroutines are processed only when there are no Priority I requirements awaiting action:

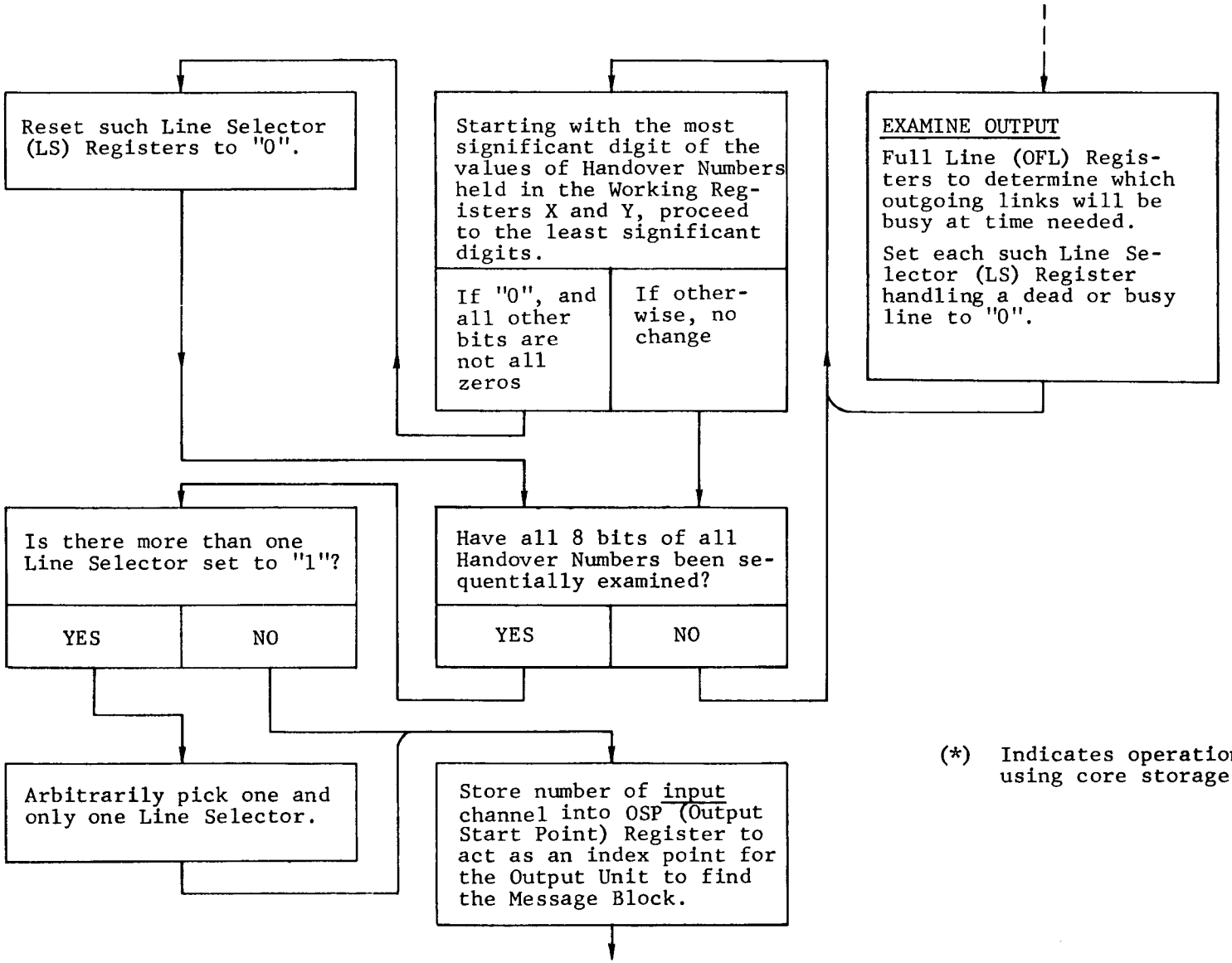
Priority II:	Decide-Best-Route Subroutine (DBR).
	No-Error-Verification Subroutine (NEV).
	Choke-Input Subroutine (CI).

Because of Priority-I interrupts, all Priority-II subroutines should be written so that they can be interrupted at any point and restarted without having to back up.

Priority III:	Update-Handover-Number-Table Subroutine (UHNT).
Priority IV:	Transmit-Trouble-Message Subroutine (TTM).
Priority V:	Wait-and-Twiddle-Thumbs Subroutine (TT).

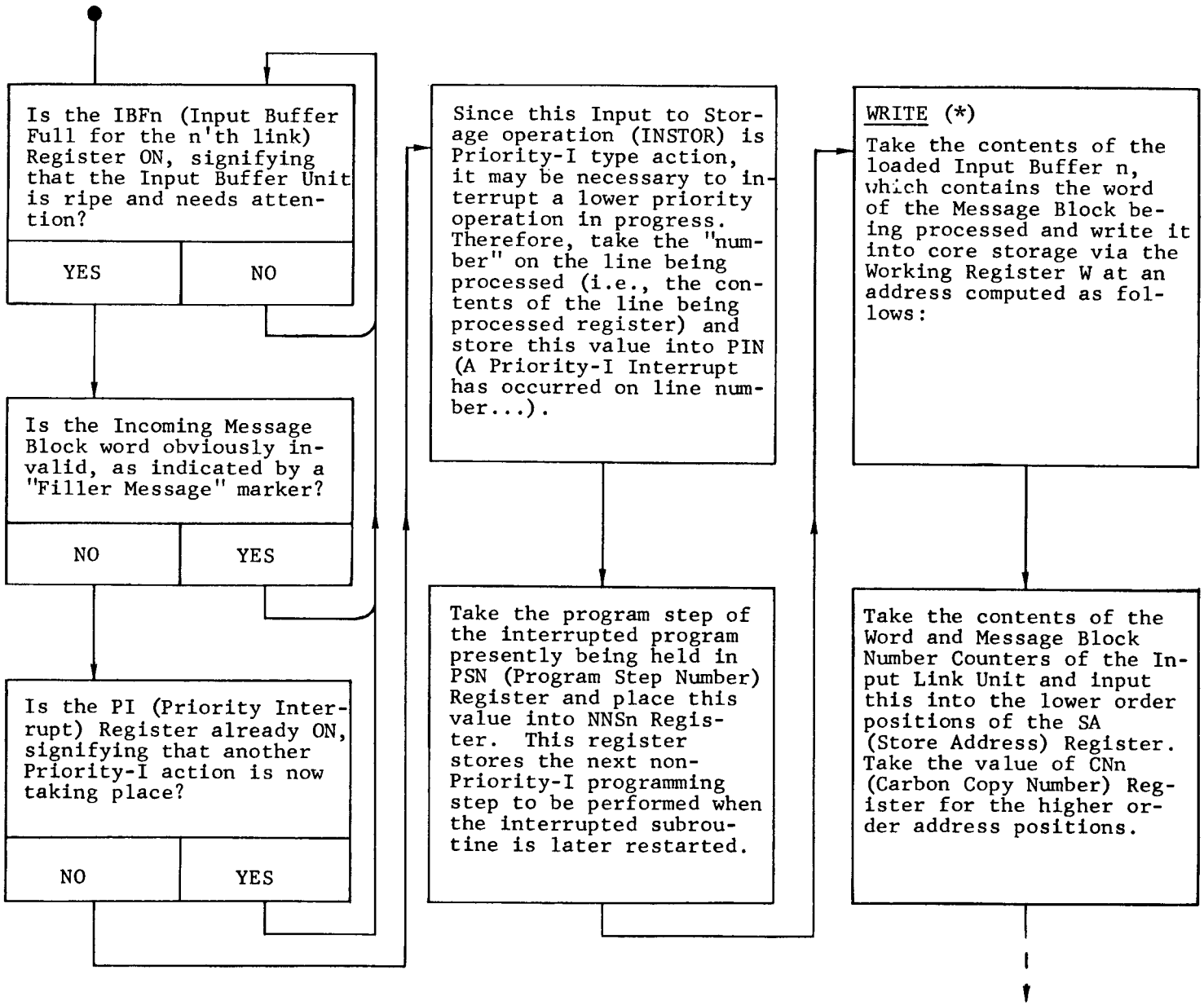
*Initials are used to denote subroutines and operation registers.


Is there a Priority-I subroutine in progress?
YES
NO
Is there a Priority-II subroutine already in progress?
YES
NO
Does INSn ≡ the program step at which Subroutine DESTROU can be used
NO
YES
READ & RESTORE SA (*)
Read and restore the "to" address of Message Block into SA (Store Address) Register.
READ & RESTORE X (*)
Read and restore the first 32-bit word of the Handover Number Table at the "to" address in core into the Working Register X.
READ & RESTORE Y (*)
Read and restore the second 32-bit word of the Handover Number Table at the ("to" + 1st word) address in core into the Working Register Y.
SORT
Each Line Selector (LS) Register is set to "1".



(*) Indicates operation using core storage.

Fig. 6--Subroutine DESTROU: Decide Best Outgoing Route for Incoming Message Block


Is the IBFn (Input Buffer Full for the n'th link) Register ON, signifying that the Input Buffer Unit is ripe and needs attention?
YES
NO
Is the Incoming Message Block word obviously invalid, as indicated by a "Filler Message" marker?
NO
YES
Is the PI (Priority Interrupt) Register already ON, signifying that another Priority-I action is now taking place?
NO
YES
Since this Input to Storage operation (INSTOR) is Priority-I type action, it may be necessary to interrupt a lower priority operation in progress. Therefore, take the "number" on the line being processed (i.e., the contents of the line being processed register) and store this value into PIN (A Priority-I Interrupt has occurred on line number...).
Take the program step of the interrupted program presently being held in PSN (Program Step Number) Register and place this value into NNSn Register. This register stores the next non-Priority-I programming step to be performed when the interrupted subroutine is later restarted.
WRITE (*)
Take the contents of the loaded Input Buffer n, which contains the word of the Message Block being processed and write it into core storage via the Working Register W at an address computed as follows:
Take the contents of the Word and Message Block Number Counters of the Input Link Unit and input this into the lower order positions of the SA (Store Address) Register. Take the value of CNn (Carbon Copy Number) Register for the higher order address positions.

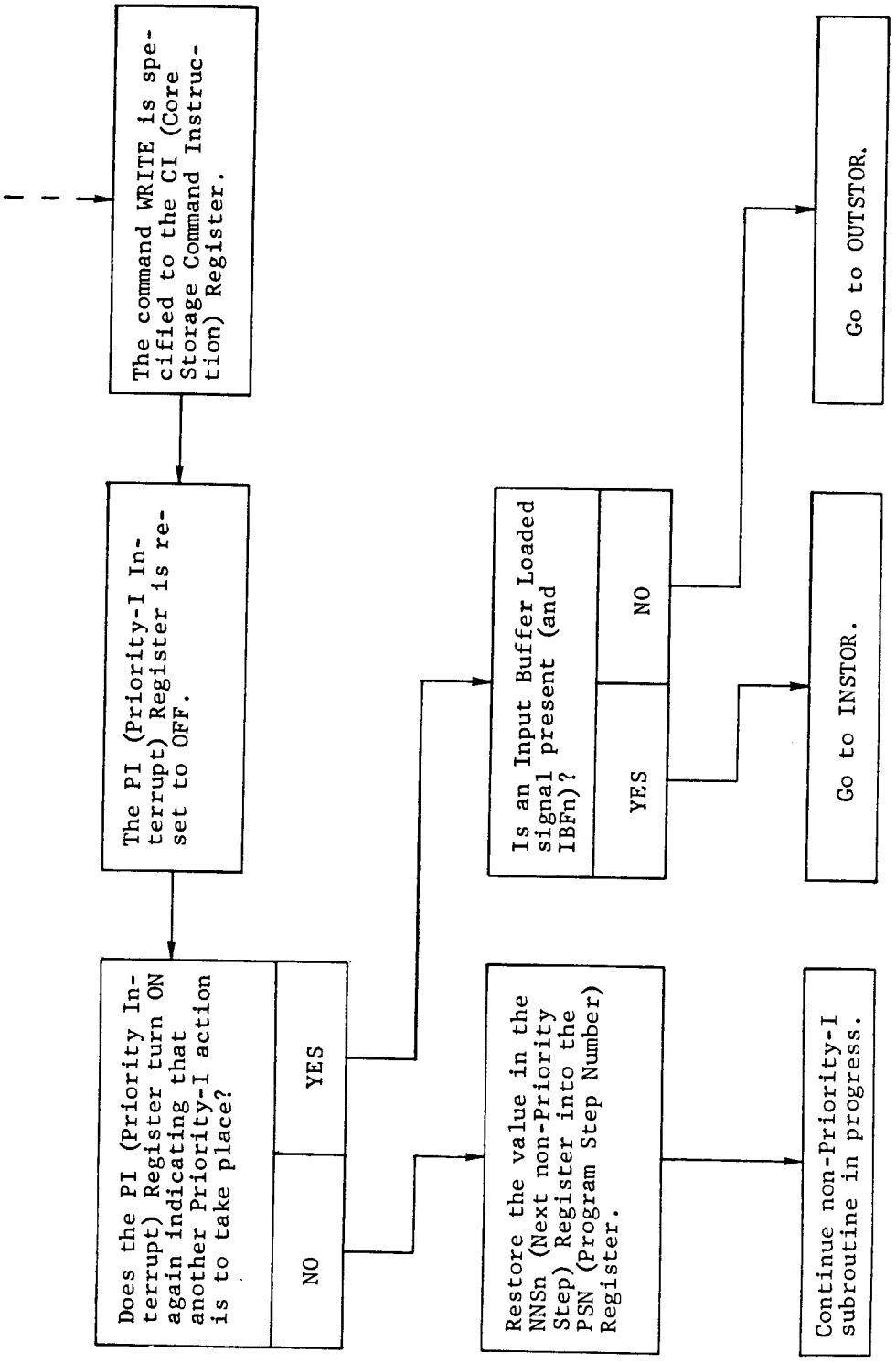


Fig. 7--Subroutine INSTOR: Place Incoming Message Word from n'th Input Link into Storage

INTRA-SWITCHING NODE MESSAGE BLOCK HOUSEKEEPING BITS

Table II denotes the number of bits reserved within each Message Block for each of the specified functions.

Table II

MESSAGE BLOCK HOUSEKEEPING BITS

Symbol	No. Bits
"To" Address	10
"From" Address	10
Handover Number	8
Trace Tags	24
Reversed Header	1
Start of Message Block	8
Block Sequence Number	8
Block Error Check	22
Valid Message	1
Error Spotter	2
Total	94 bits = 3 words

$$\text{Percentage of active information flow} = \frac{(\text{Message Length}) - (\text{Housekeeping Length})}{\text{Message Length}} \times 100$$

$$= \frac{1024 - 94}{1024} = \frac{930}{1024} = 90.9\%.$$

If every sixteenth bit is a dummy bit reserved for inserting polarity change to simplify transmission-link requirements, then the percentage of active information flow drops; i.e.,

$$= \frac{1024 - 94 - \frac{1024}{16}}{1024}$$

$$= \frac{866}{1024} = 84.57\%.$$

COMMON FLAG REGISTERS

The Common Flag Registers form part of the Central Processor and are used in the determination of program interrupts and selection of the next program stop (see Table III).

Table III

COMMON FLAG REGISTERS

Name	Function	Bits	States
TD	A trouble has been detected. (Trouble Detected)	1	2
TMA	A trouble message is awaiting transmission. (Trouble Message Awaiting)	1	2
NPI	A non-Priority-I program has been interrupted. (Non-Priority Interrupt)	1	2
ILN	A non-Priority-I interrupt has occurred on line number.... (Interrupted Line Number)	3	8
PI	A Priority-I function needs attention. Interrupt lower priority programming. (Priority-I Interrupt)	1	2
PIN	A Priority-I interrupt has occurred on line number.... (Priority Interrupt Number)	3	8
WRB	Working registers XYZ are in use. (Working Registers Busy)	1	2

LINE STATE REGISTERS

The Line State Registers (one for each line) form part of the Central Processor and allow the Central Processor to monitor the status of all input and output links to determine which units are in need of attention (see Table IV).

Table IV

LINE STATE REGISTERS

Name	Function	Bits	States
OKM	Message now being processed on input has valid mark. (OK Message)	2	4
POK	Previous message received is verified and it is OK to transmit it on further. (Previous OK)	1	2
RH	Header of message being processed has been reversed. (Reversed Header)	1	2
CN	Number of the carbon copy being output processed; i.e., starting location in memory. (Carbon Number)	2	4
ONB	Output line is now busy. (Output Now Busy)	1	2
OFL	Output line may not be busy later. (Output Free Later)	1	2
BM	Message now being processed is a backup message. (Backup Message)	1	2
NNS	Next non-Priority-I programming step to be performed is number.... (Next Non-Priority Step)	6	64
SW	Something appears wrong with message. (Something Wrong)	1	2
LS	This line is presently being processed. (Line Select)	1	2
NS	Next non-Priority-I subroutine to be performed. (Next Subroutine)	3	8

WORKING REGISTERS

The Working Registers form the heart of the Central Processor. All communications into and out of the core are via these registers. All arithmetic operations are carried out by these registers serving as arithmetic units (see Table V).

Table V

WORKING REGISTERS

Name	Function	Bits	States
W	W-Register	32	-
X	X-Register	32	-
Y	Y-Register	32	-
A	Address Register	12	4096
C	Command Instruction Register	6	64
PSN	Program Step Number	8	256
ID	Information Decoder	10	1024
OSP	Output Start Point (Index Register)	5	32

LEARNING AND FORGETTING FUNCTION

The Central Processor via the Update Handover Number Subroutine (Fig. 8) executes the following equations:

$$\alpha_{t+1} = \alpha_t - (\alpha_t - b_t)k$$

$$\begin{cases} \text{if } (\alpha_t - b_t) \geq 0;\ k = k_1 \\ \text{if } (\alpha_t - b_t) < 0;\ k = k_2 \end{cases}$$

$$k_1 > k_2$$

where:

α_{t+1} = Computed smoothed value to be stored in Handover Number Table;

α_t = Previous computed smoothed value found stored in Handover Number Table;

b_t = Measured value of handover number;

k_1 = Learning constant;*

k_2 = Forgetting constant.

This manipulation permits the Switching Node to modify its Handover Number Table in response to external changes in the network status, as shown in Fig. 9.

In order to reduce the time taken by the multiplication operation in the handover number modification, the values of the multipliers k_1 and k_2 are limited to binary numbers containing but two "ones." This permits the use of a specially designed high-speed multiplier that need not anticipate encountering many iterative additions.

---

*See ODC-II and -III for a detailed description of learning.

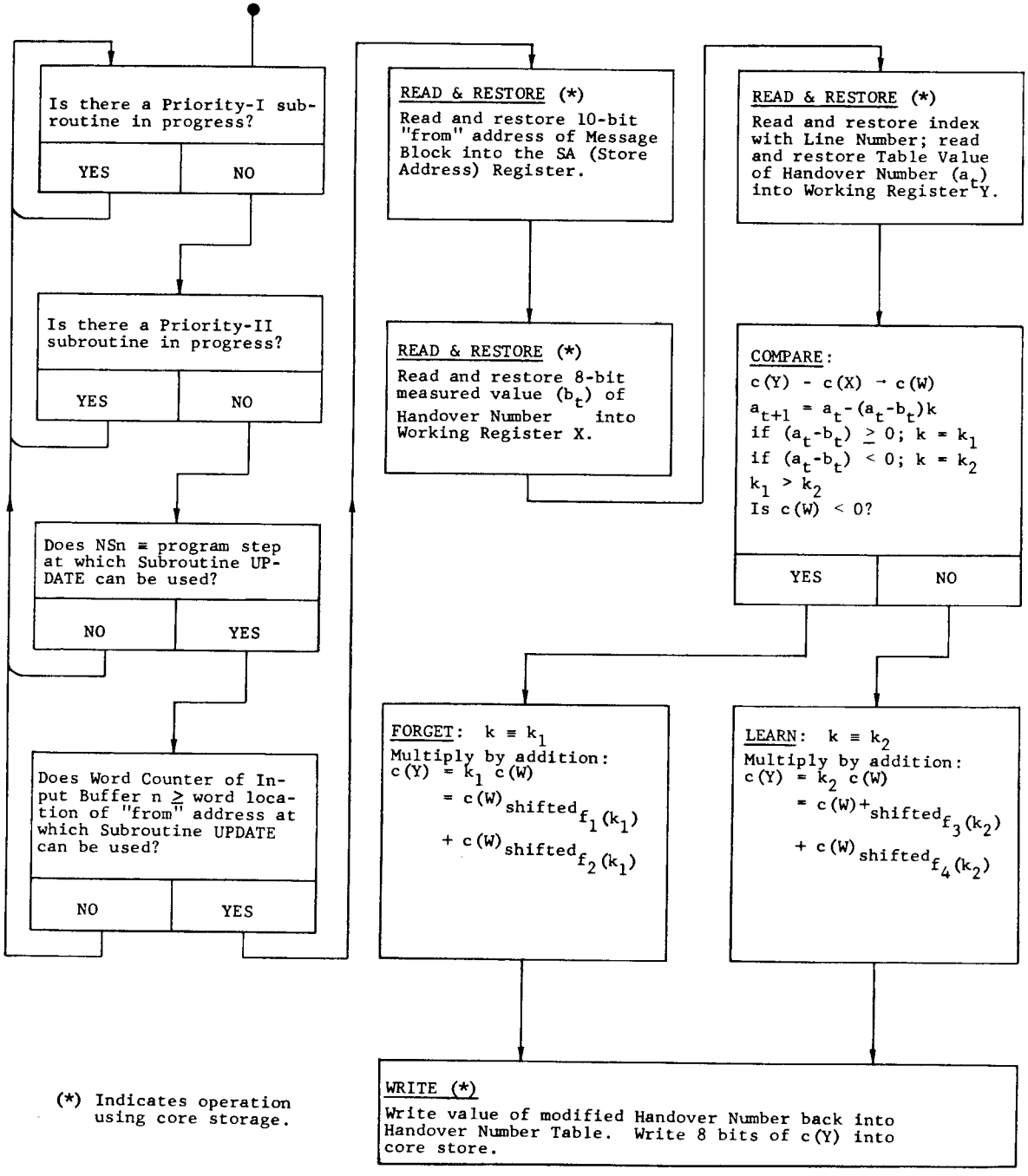


Fig. 8--Subroutine UPDATE: Update Handover Number Table Value

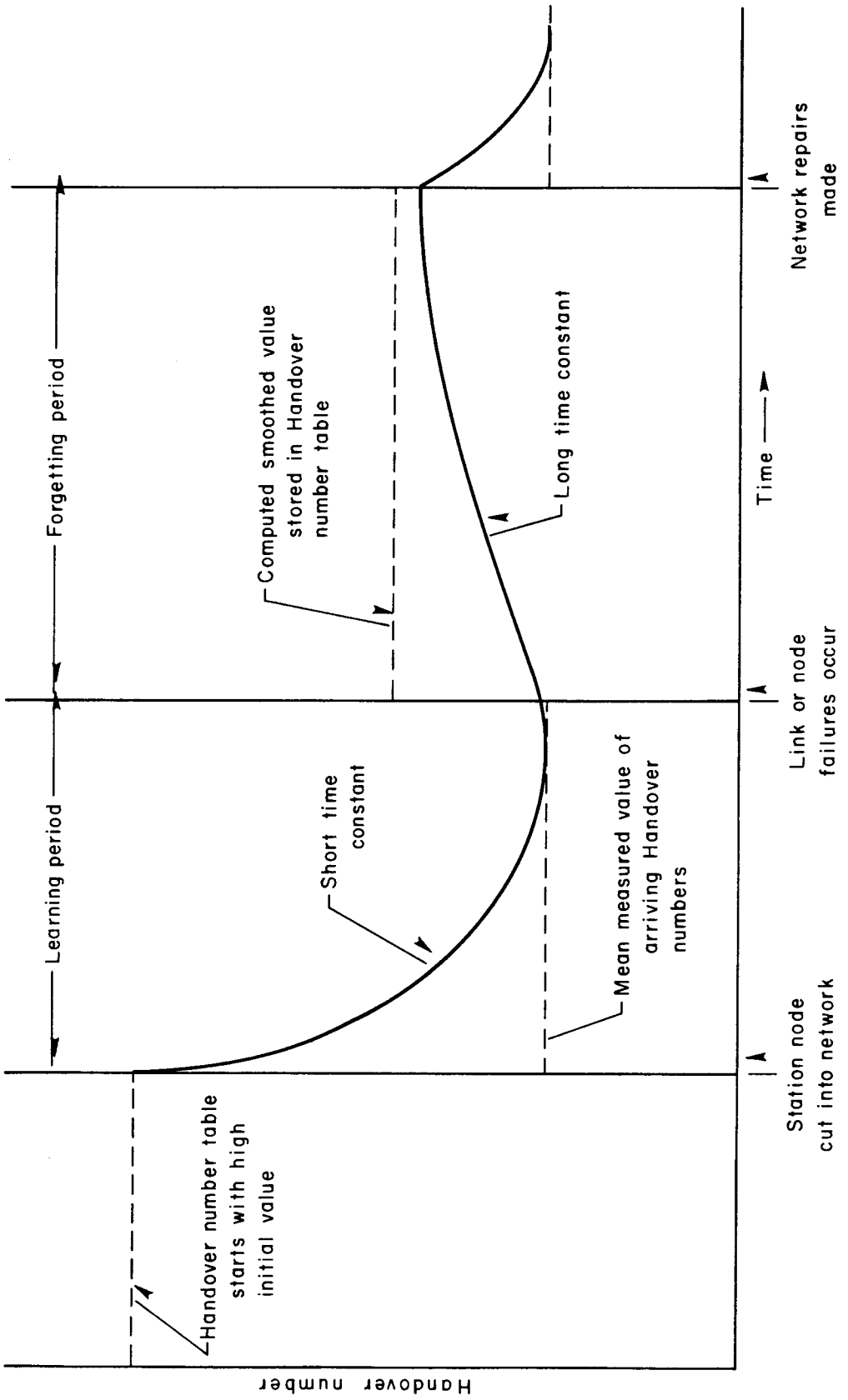


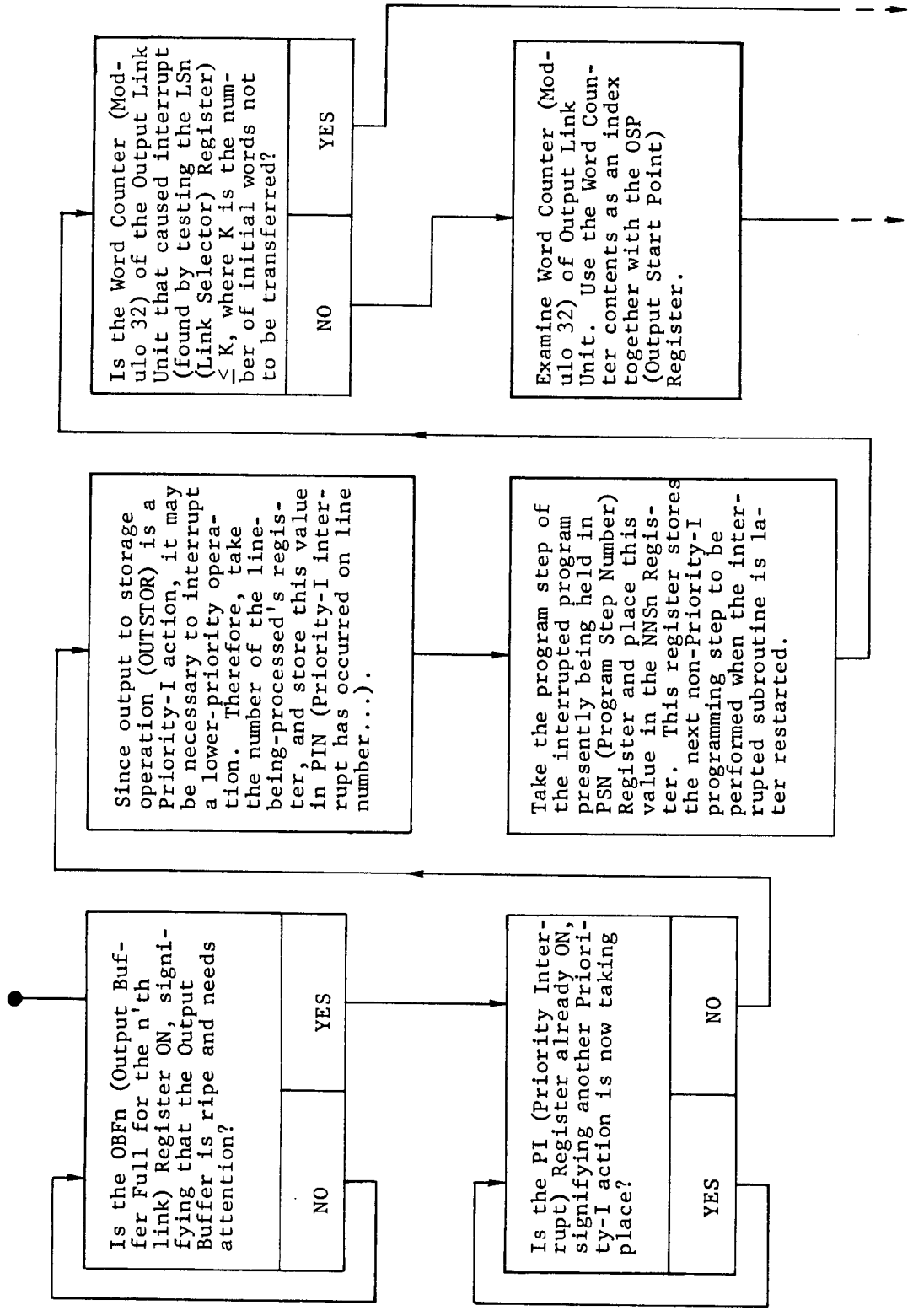
Fig. 9--Learning and Forgetting Operations from Observations of Handover Numbers

Table VI lists the 13 valid values of k_1 and k_2 out of the 16 combinations of four binary digits which meet the criterion of no more than two "ones" in any number.

Table VI

ALLOWABLE FRACTIONAL VALUES OF k_1 AND k_2

Binary	Decimal	NG	OK	Decimal < 1
0 0 0 0	0		X	0.0000
0 0 0 1	1		X	0.0625
0 0 1 0	2		X	0.1250
0 0 1 1	3		X	0.2175
0 1 0 0	4		X	0.2500
0 1 0 1	5		X	0.3125
0 1 1 0	6		X	0.3750
0 1 1 1	7	X		
1 0 0 0	8		X	0.5000
1 0 0 1	9		X	0.5625
1 0 1 0	10		X	0.6250
1 0 1 1	11	X		
1 1 0 0	12		X	0.7500
1 1 0 1	13	X		
1 1 1 0	14	X		
1 1 1 1	15	X		


Is the OBFn (Output Buffer Full for the n'th link) Register ON, signifying that the Output Buffer is ripe and needs attention?
NO
YES
Is the PI (Priority Interrupt) Register already ON, signifying another Priority-I action is now taking place?
YES
NO
Since output to storage operation (OUTSTOR) is a Priority-I action, it may be necessary to interrupt a lower-priority operation. Therefore, take the number of the line-being-processed's register, and store this value in PIN (Priority-I interrupt has occurred on line number...).
Take the program step of the interrupted program presently being held in PSN (Program Step Number) Register and place this value in the NNSn Register. This register stores the next non-Priority-I programming step to be performed when the interrupted subroutine is later restarted.
Is the Word Counter (Modulo 32) of the Output Link Unit that caused interrupt (found by testing the LSn (Link Selector) Register) ≤ K, where K is the number of initial words not to be transferred?
NO
YES
Examine Word Counter (Modulo 32) of Output Link Unit. Use the Word Counter contents as an index together with the OSP (Output Start Point) Register.

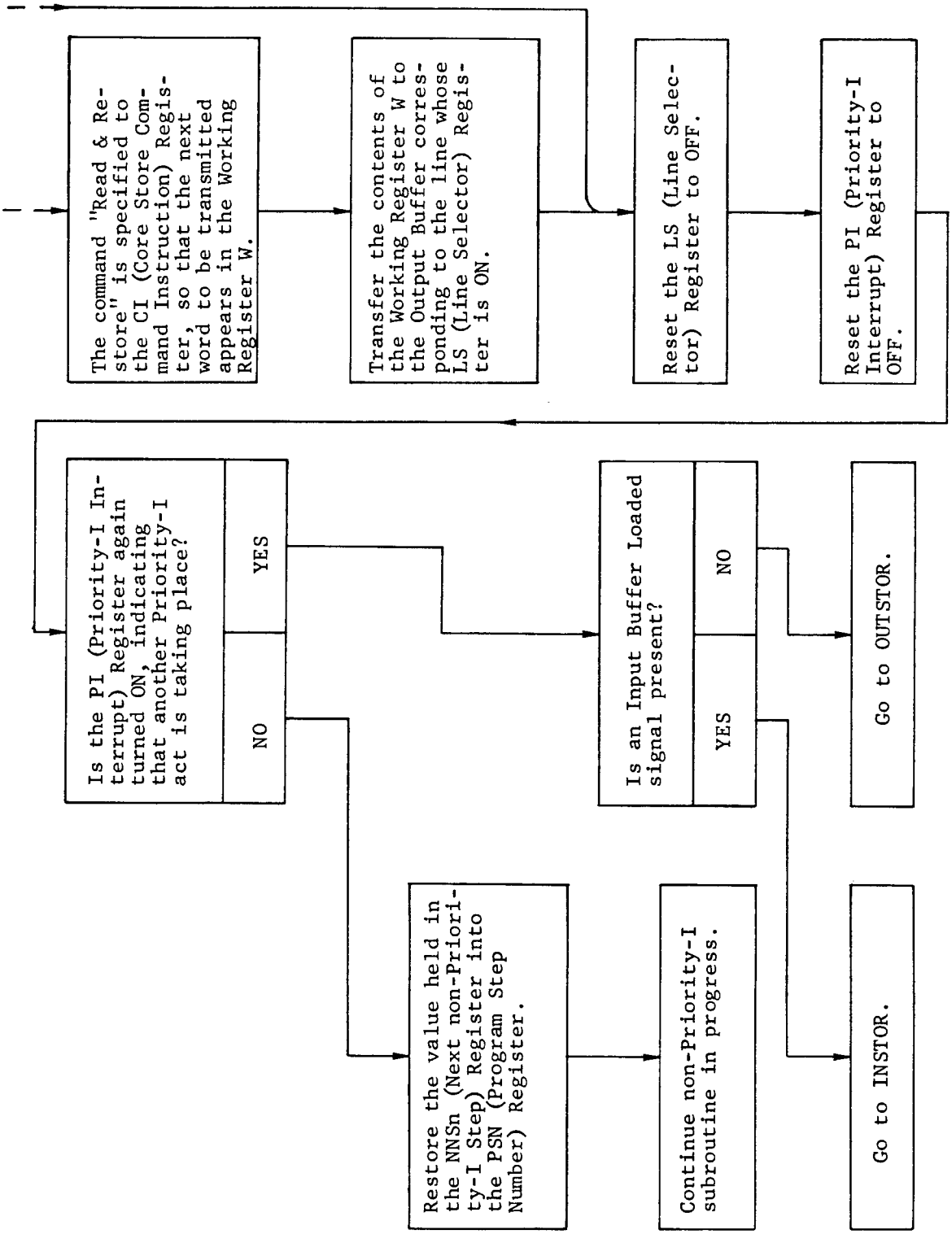


Fig. 10--Subroutine OUTSTOR: Take the Outgoing Message Word from Storage and Place it on the Outgoing Link

III. INTERNODE TIMING CONSIDERATIONS

TIME REQUIRED BY NODE TO PROCESS MESSAGE BLOCK

Following is the estimate of total time required per Message Block:

$$38.4 + 6 + 6 + 12 + 32 \quad \text{(from Table I)}$$

$$= 94.4\ \mu\text{sec.}$$

This value assumes that the rewrite cycle of subroutine OUTSTOR is conducted in overlap with other non-core-memory operations.

At a 1.54-million bit/sec rate, one Message Block is equal to approximately 0.000667 sec, or 667 μsec. Due to the employment of the "chocking" doctrine,* only seven of eight input lines, at most, will ever be busy simultaneously.

$$\frac{667\ \mu\text{sec per Message Block}}{7\ \text{simultaneous Message Blocks}}$$

= 95.3 μsec, the allowable time which can be spent processing any single Message Block. Since this is so near the required value of 94.4 μsec, the designer must be extremely careful; otherwise, an increase in word length or speed of memory will be required.

*See ODC-IV, p. 12.

EFFECTS OF DELAY TIMES IN MESSAGE PROPAGATION AND ERROR CONTROL

In the distributed network, a store-and-forward technique is used which places rigorous demands upon the efficacy of the link error detection and correction method employed. Previous digital communications systems using error detection and repeat transmission dealt with data rates so slow that the transmission time between Switching Nodes was always much less than a fractional Message Block unit time.

As we move toward 1.5-megabit/sec (and faster) links, we encounter a new and generally unappreciated problem, because of the relatively large amount of time that elapses before the return of information that a particular Message Block has been incorrectly received.

Since the probability that a received Message Block has been received in error in even a relatively noisy link is much less than the probability that the Message Block has been correctly received, we can make a tentative assumption that a Message Block has been correctly received and proceed to transmit the next sequential Message Block. At transmitting Station A, it is then necessary that we keep sufficient

"carbon copies" of the most recently transmitted messages for backup purposes, in case we later fail to receive confirmation that the transmitted message has been correctly received at receiving station B. Upon reaching such a finding, we prefer to use an alternate link for retransmission, because we cannot be sure whether we have encountered a random error or a long fade (see ODC-VI).

We shall now consider separately what happens if there is a failure on the transmission link, and/or a failure in the return link conveying the "return receipt."

Failure of the Transmission Link and Not the Return Link

If the transmission link from A to B fails while B to A does not, there is no problem: Both A and B know exactly what Message Block has been corrupted, so B ignores the Message Block. A possesses a clean carbon copy and sends the affected Message Block out over an alternate link.

Failure of the Return Link Only

If the transmission link from B to A fails, then a clear ambiguity exists. A does not know whether B has correctly received the message or not. If B

thinks that he has received the Message Block correctly, as indicated by a successful block parity check, he relays the message on to C. As A does not know whether his message was received by B, he is forced to resend the message out over another link.

If the probability of a failure is assumed to be one Message Block in one hundred, then the additional traffic created by this repeat transmission process is only a small percentage of the total volume. Since the original preparation of this Memorandum, it has become apparent (see ODC-VI) that the raw expected error rate will probably be less than one Message Block per thousand. Thus, the additional traffic created will be negligible--an increase of less than one per cent in the total volume.

The appearance of duplicate Message Blocks calls for the Multiplexing Station to have the capability to detect and reject such occasional duplicates. This is not difficult, because each Message Block already contains a sequence number needed for the end-to-end cryptographic reception equipment. Both copies would bear the same sequence number (see ODC-IX).

Magnitude of the Delay

A convenient unit of time is the "Message Block." In the system being examined, it is the time required to transmit a 1024-bit message of 1.54 megabits/sec.

The abscissa of Fig. 11 shows a series of Message Blocks, A101, A102, A103, A104, ..., sequentially transmitted by Switching Node A. A data rate of 1,500,000 bits/sec, and a Message Block length of 1024 bits is assured. Thus, each Message Block requires about 2/3 ms. The ordinate represents distance in miles between Switching Node A and receiving Switching Node B. Two separate ordinate scales are used: one corresponds to a velocity of propagation of light, 186,000 mi/sec; the second to half that value, 93,000 mi/sec.

In the specific illustration, Switching Node B is shown to be at a distance of 103 mi from A. Velocity of propagation of 186,000 mi/sec from A to B and B to A is assumed. The lines slanting to the right represent the time delay of a bit traveling from left to right, or from A to B relative to A. The lines to the left represent the time delay of a bit traveling from right to left, or from B to A.

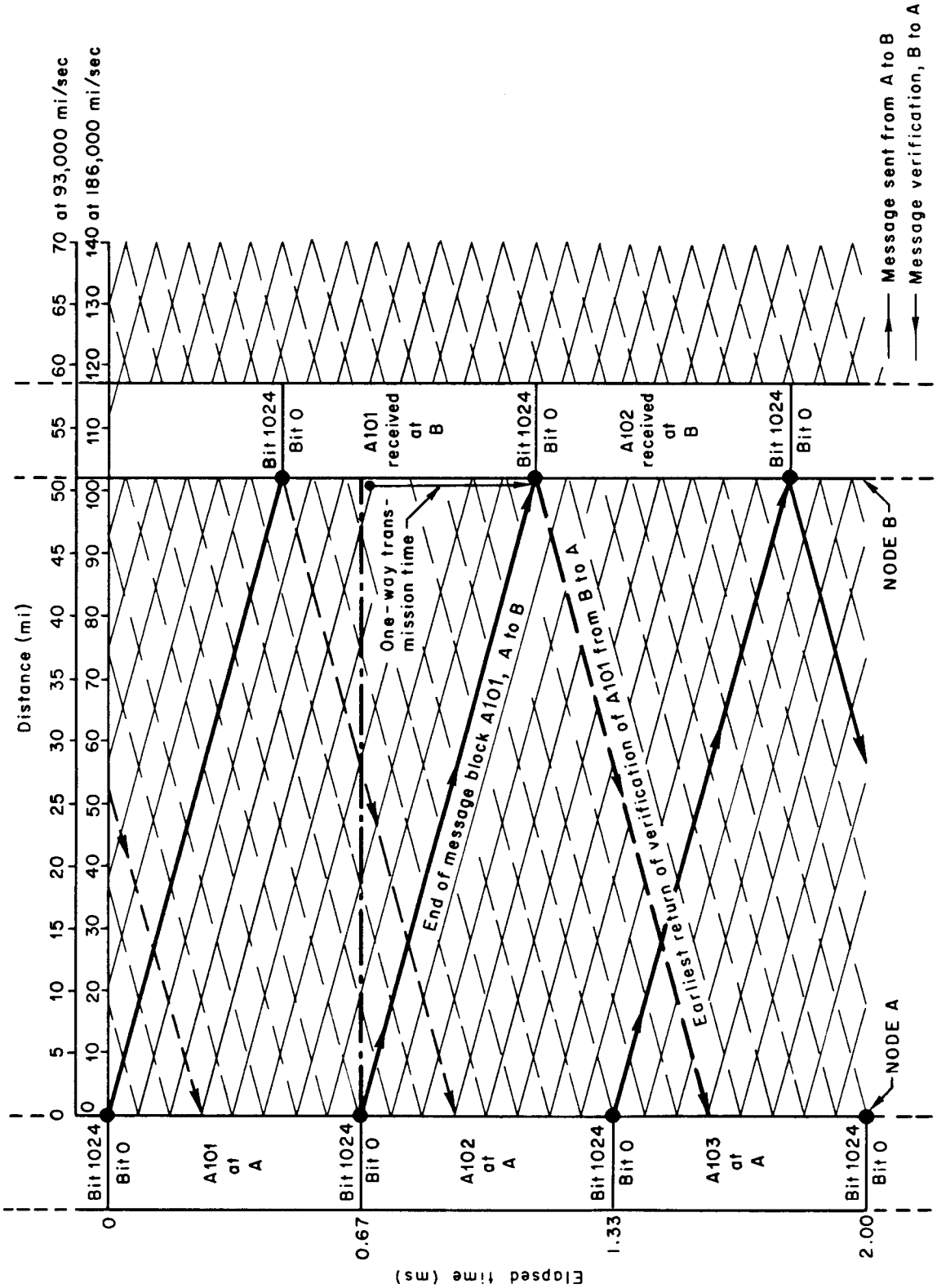


Fig. 11--Transmission Time and its Effects on Verification Timing

It can be seen that bit #1024 of Message Block A101, sent by A, cannot be received by B and returned to arrive at A until about 1 ms after transmission by A. Thus, if A101 was defectively received, Station A would not know about it until the moment it was in the middle of transmitting A103.

No Message Blocks are lost, due to the use of carbon copies, but the need for several Message Blocks of such carbon copy storage can be seen.

Links longer than about 150 mi would either have to operate at data rates less than 1.54-million bits or else more carbon copy storage would be needed. The additional storage required at this data rate is 1024 bits of storage per each additional 150 mi desired. Table VII indicates the data-rate/distance tradeoff if no additional carbon copy memory is used. A mixture of these two separate alternatives can also be used.

Table VII

TRADEOFF BETWEEN DATA RATE AND DISTANCE
IF NO ADDITIONAL STORAGE IS USED

Data Rate (bits/sec)	Link Distance (mi)
1,500,000	150
500,000	450
100,000	2,250
50,000	4,500

USE OF SATELLITE LINKS IN THE DISTRIBUTED NETWORK

We shall now briefly consider the problems that might occur if satellite communications links are used in the system. We shall separately consider low-altitude non-synchronous orbit satellites, and high-altitude synchronous satellites. The reader can interpolate between these two examples.

Non-Synchronous Satellites

Fundamentally, the Link Unit described is designed for a non-time-variant communications link. As a non-synchronous communications satellite link changes its length and spatial position with time, a variable time delay is inserted into the communications link which must be considered in order to allow the Link Unit to operate in conjunction with non-synchronous satellites.

Assuming that there are two stations, A and B, at the ends of a satellite communications link, a shift in the radio carrier frequency will be noted as the satellite comes into range and then passes out of range, due to doppler shift. As the satellite comes into range, its frequency will be higher than its transmitted frequency; as it moves beyond the mid-range point, the frequency will decrease by a similar amount.

We shall assume a satellite with a velocity of about 18,000 mi/sec; the plane of the earth flat; the carrier

frequency at 4000 megacycles; the satellite flying at an altitude that is low in comparison to the distance between A and B; and that it passes directly over A and B (see Fig. 12). The satellite velocity is

$$\frac{18{,}000 \text{ mph}}{3600 \text{ sec/hr}} = 5 \text{ mi/sec.}$$

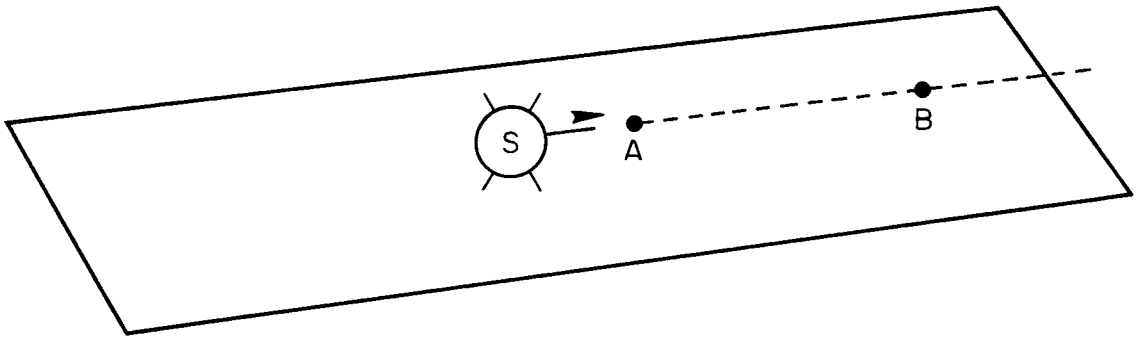


Fig. 12--Low-Altitude Satellite Link

One-way doppler offset frequency, satellite to A

$$\Delta f_A = \frac{\text{velocity of satellite}}{\text{velocity of EM radiation}} \times \text{carrier frequency}$$

$$= \frac{(5 \text{ mi/sec})\ (5 \times 10^9 \text{ cycles/sec})}{186{,}000 \text{ mi/sec}}$$

$$= \frac{2.5 \times 10^{10}}{1.86 \times 10^5}$$

$$= 134{,}000 \text{ cps.}$$

Since this is the same order of magnitude as the bandwidth required to transmit at a 150,000-bit/sec rate, this carrier frequency doppler offset would appear to be manageable with a conventional automatic frequency-control circuit at a slight loss of signal-to-noise ratio.

A 1024-bit Message Block at 150,000 bits/sec will take $\frac{1024 \text{ bits}}{150{,}000 \text{ bits/sec}} \sim 6.83$ ms for transmission. During this time the satellite will have moved,

$$(6.83 \times 10^{-3} \text{ sec})\ (5 \text{ mi/sec})$$

$$\sim 3.415 \times 10^{-2} \text{ mi.}$$

Each bit will arrive with shorter-than-transmitted spacing by a factor of

$$\frac{(5 \text{ mi/sec})}{(186{,}000 \text{ mi/sec})} \sim \frac{5}{1.86} \times 10^{-5} \sim 2.69 \times 10^{-5}.$$

Since there are 1024 bits in a Message Block, the bit timing will be off by $1024 \times 2.69 \times 10^{-5} = 2.76 \times 10^{-2}$ bits per Message Block.

Thus, it will take about $\frac{1}{2.76} \times 10^{-2} \sim 36.3$ Message Blocks to drift one bit out of synchronization. The automatic phase detection bit timing lock used in the Link Unit should be able to compensate for such a change without difficulty--even for a satellite passing over the azimuthal point where the drift rate is about double this value.

If the usable satellite range between A and B is about 3000 mi, the satellite link will be in range for about

$$\frac{3000 \text{ mi}}{5 \text{ mi/sec}} = 600 \text{ sec, or } 10 \text{ min.}$$

If we modify our model by letting the satellite fly higher and extend the range beyond the A-to-B base line by R, then at the extremities of range, the path-length can exceed the path-distance D, between A, by the factor 2R; if R = 1000 mi, D = 3000 mi.

The path-lengths in terms of message length then become:

Minimum: D = 3000 mi, if 1500 mi = 1 Message Block at 150,000 bits/sec = 2 Message Blocks;

Maximum: D + 2R = 5000 mi = 3.3 Message Blocks.

Therefore, it is necessary to be careful that the error detection feedback digits are returned and assigned to the correct "carbon copy" Message Block. This can be

done by examining the handover number of the confirmation signal of the arriving Message Block Sequence Number* and subtracting the presently transmitted Message Block Sequence Number. For example, in Fig. 13, Switching Node A is designated the master timing station and is transmitting Message Block A101; some time later Switching Node B receives this same Message Block (A101) and synchronizes B's local timing of messages to A. However, the messages back to A contain the confirmation of correct receipt of Message A101 at B. The Message Block serial number of the present Message Block being received at A, less the value of the instantaneous Message Block Sequence Number A101 being transmitted, tells us which "carbon copy" contains the correct receipt.

This operation is automatically performed once each Message Block under the subroutine which determines the carbon copy number.

Non-synchronous satellites transmitting broadband signals require that the ground stations take advantage of the signal strength gain afforded by directional antennas. The antenna must follow the path of the satellite across the sky. Generally, the ground station has three options for tracking the satellite:

1) A scanning antenna can be used to seek and lock onto the satellite;

*Note that this is a link sequence number, not the end-to-end number previously described.

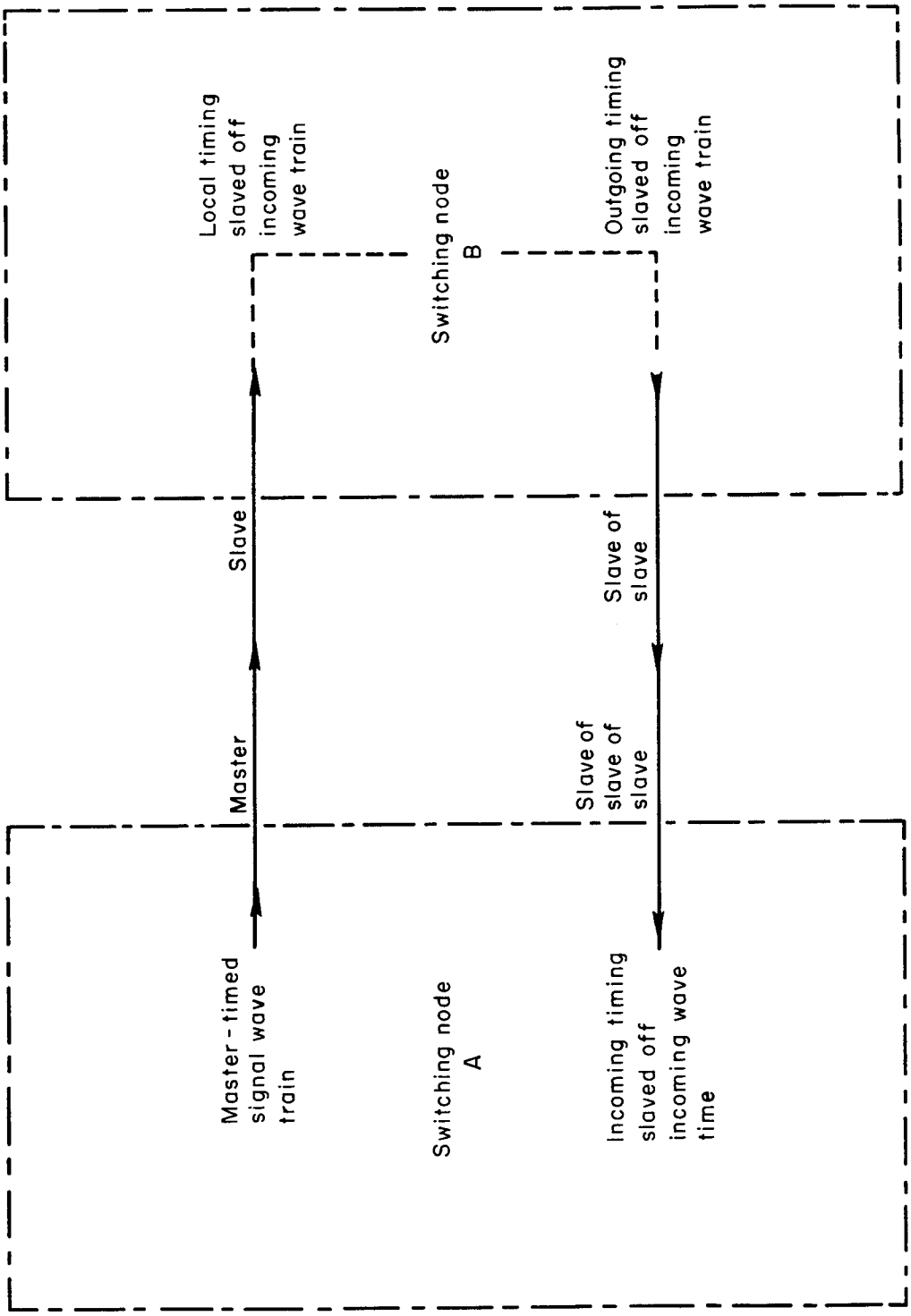


Fig. 13--Timing Relationship Between Switching Nodes A and B

2) A local computer can be used to predict the future orbit of the satellite and point the ground antenna accordingly;

3) Remote control centers can compute the pointing coordinates for a large number of satellites and ground stations and transmit the coordinates for immediate or future use. If immediate use is necessary, a separate non-satellite narrow-band communications link to the ground station is necessary. But, if coordinate storage is allowed at each antenna directional control unit, the upcoming coordinates may be transmitted over the satellite link itself for later use.

Let us consider how this last approach might work. We would like to transmit azimuth angle, elevation angle, doppler offset frequency, and perhaps some crypto information. Using the previous assumptions:

1) The highest expected slew rate is roughly about 360^{o} in 600 sec, equaling 0.6^{o}/sec;

2) Assume a 1^{o} antenna beamwidth;

3) Maintain a steering accuracy on an order of magnitude of 0.1^{o};

4) Steering signals need not be transmitted much more often than about six times per second at accuracies on the order of one part in 3600;

5) Accuracies of one part in 4096 require the transmission of 12 binary bits;
6) Azimuth and elevation data to the remote antenna require the transmission of (12 + 12) bits x 6 samples per sec, or about 144 bits/sec (doppler offset information can be included at the price of a few more bits);
7) Assuming that each Message Block can hold in excess of 800 bits of information, the transmission of merely two Message Blocks would provide for about 11 minutes of tracking time--longer than the time the satellite would probably be within range;
8) Thus, it appears that a little storage at the ground station might provide a possible convenient way of coping with the antenna pointing problem.

Thus, not encountering any new problems that are not being handled by the proposed system, we shall next consider possible problems that might arise when using synchronous satellite links.

Synchronous Satellites

Because of the "fixed" spatial positions of a synchronous satellite, we may omit the variable length link problems and consider the synchronous satellite link as being a long but fixed link.

Suppose that A and B are 8000 mi apart and the satellite is at a 24,000-mi altitude. The round-trip length, therefore, is equal to

$$\left(\left(\frac{8000}{2}\right)^2 + \left(\frac{24,000}{8}\right)^2 \right)^{\frac{1}{2}} \left(2\right) = 48,400 \text{ mi (Fig. 14).}$$

If one additional carbon copy per 150-mi path separation is required at 1,540,000 bits/sec, then the number of carbon copies that must be supplied in a synchronous satellite system will be:

$$\left(\frac{48,800 \text{ mi}}{150\text{-mi carbon copy}} \right) \left(\frac{150,000 \text{ bits/sec data rate}}{1,540,000 \text{ bits/sec}} \right)$$

$$= \frac{4.88 \times 10^4 \times 1.5 \times 10^5}{1.5 \times 10^2 \times 1.54 \times 10^6} = 31.7 \text{ carbon copies.}$$

Total additional storage required = 32 x 1024

= 31,500 bits of storage

$\tilde{-}$ 1000 words of storage

$\therefore$ Maximum possible additional storage that would ever be needed if all eight links were synchronous satellite links $\cong$ 8000 words of storage.

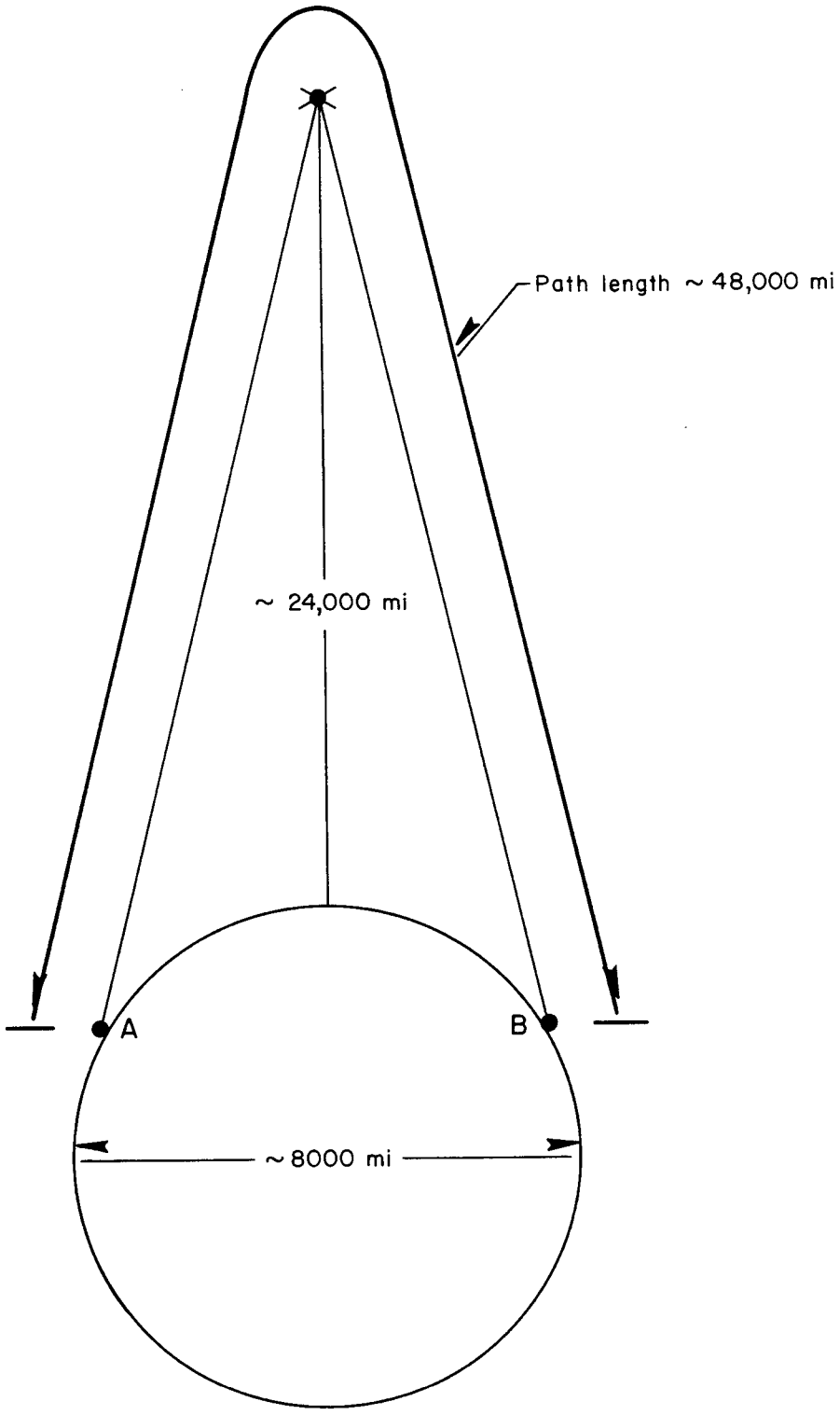


Fig. 14--Synchronous Satellite Transmission Link Length

TIMING REQUIREMENT FOR VERY-HIGH-DATA-RATE TIME DIVISION MULTIPLEXED LINKS

Although the Switching Node is basically designed to operate at link data rates up to 1.54-million bits/sec, the mini-cost microwave transmission links operate at about three times this data rate (see ODC-VI).

One simple scheme that can be used to multiplex three separate bi-directional channels on a link operating at three times the 1.54-megabit rate (4.62 megabits/sec) is by use of simple time division assignment. Three sequential time slots can be used. The first time slot might carry traffic from A to B, and the second from A to C. By making the widths of the three slots slightly different, information is available to allow positive identification of the time-divided channels. In the "grasshoppering" arrangement of Fig. 15 there is no increase in the number of times new timing must be derived, as compared to that which would be required by a separate single link from A to C. The only new requirement is that the system be able to accommodate links whose length is that of A to C, instead of A to B or B to C. Although this illustration is drawn on the basis of three time slots, it is clear that many more channels can be handled in a similar manner.

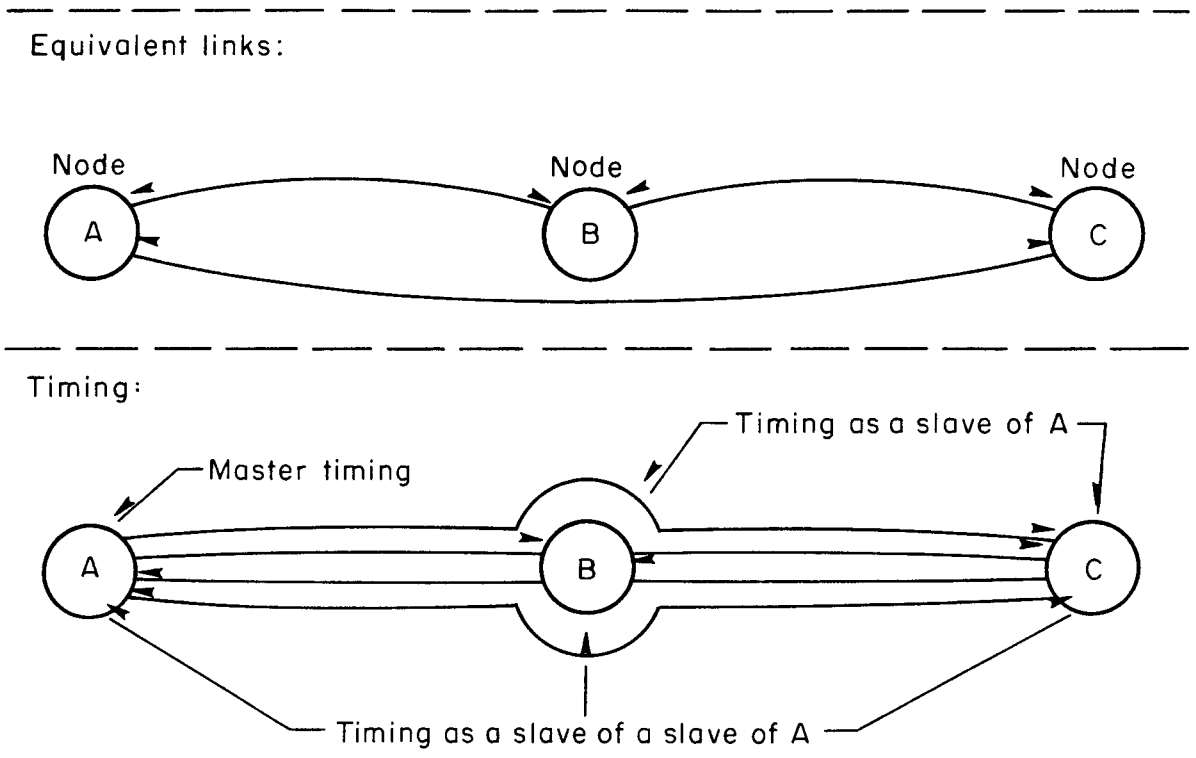


Fig. 15--Timesharing Two Channels on One Link

IV. HARDWARE

LOGICAL COMPLEXITY

Because of the highly iterative structure of the circuitry used in the Switching Node, the designer must avoid buildup of cumulative time delays which would require extremely fast and expensive circuitry. A slight rearrangement of the organization of circuit elements within the system can cut down propagation delays to permit maximum use of the proposed low-cost transistors.

For example, in Fig. 16, two different methods of performing the division operation of a Message Block by a fixed Boolean polynomial as required in the error detection encoder and decoder circuits are shown. The two methods are highly logically similar; the second circuit requires four serial gates, and so should be avoided in preference to the first circuit.

Another example is illustrated in Fig. 17, the Low Ripple Counter. The Link Units contain tandemly connected binary counters that are used to count bits into words, words into Message Blocks, and Message Blocks into Message Block sequences. Although three separate counters are shown--two Mod-32's and a Mod-256 counter, implying two five-stage counters followed by an eight-stage counter--rearrangement of these counters into six tandemly connected three-bit counters will reduce the serial propagation delays so that never more than four tandem delays will occur

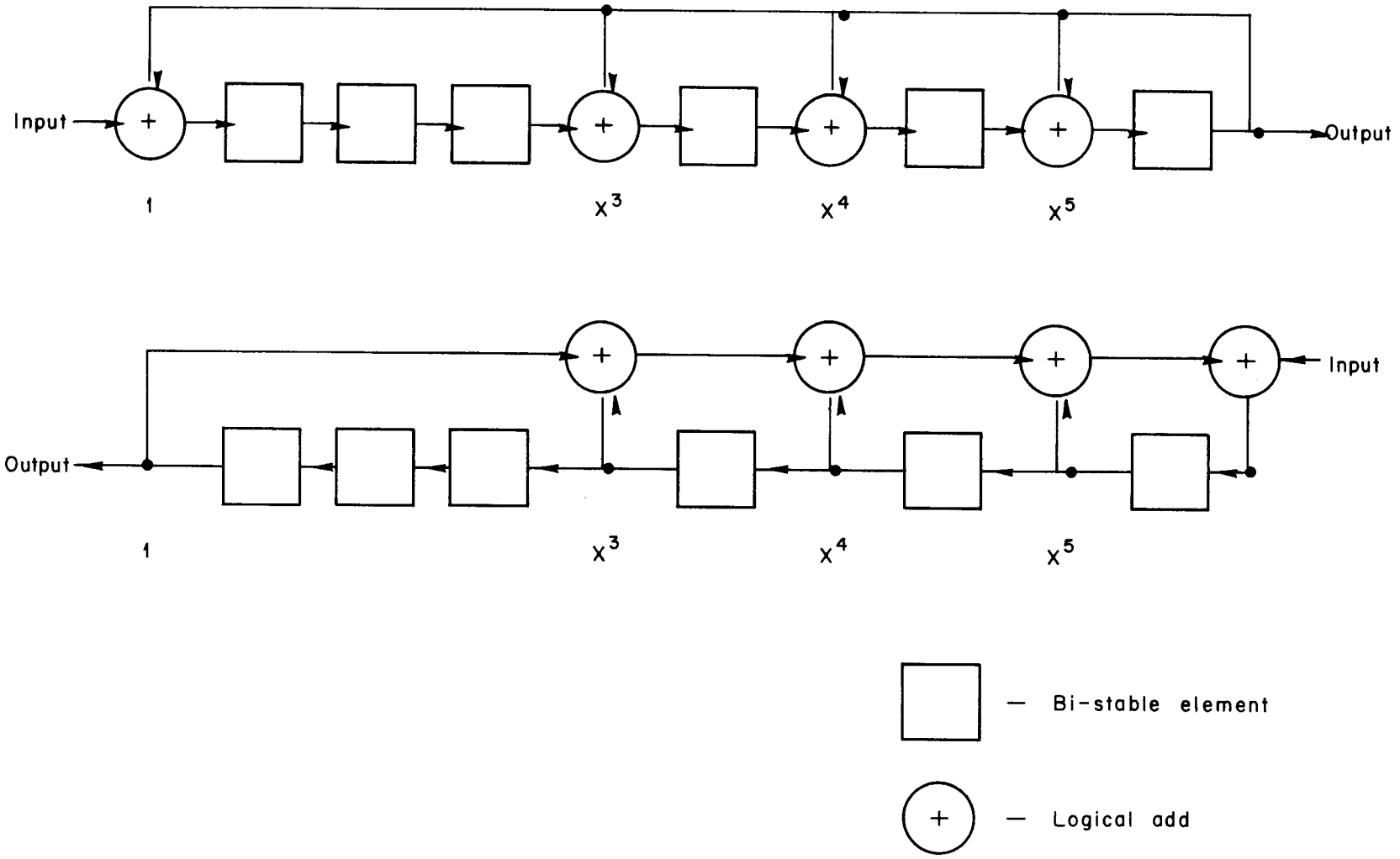


Fig. 16--Two Circuits for Dividing by $1 + X^3 + X^4 + X^5 + X^6$*

*Peterson, W. Wesley, Error Correcting Codes, Wiley, 1961, pp. 111, 130.

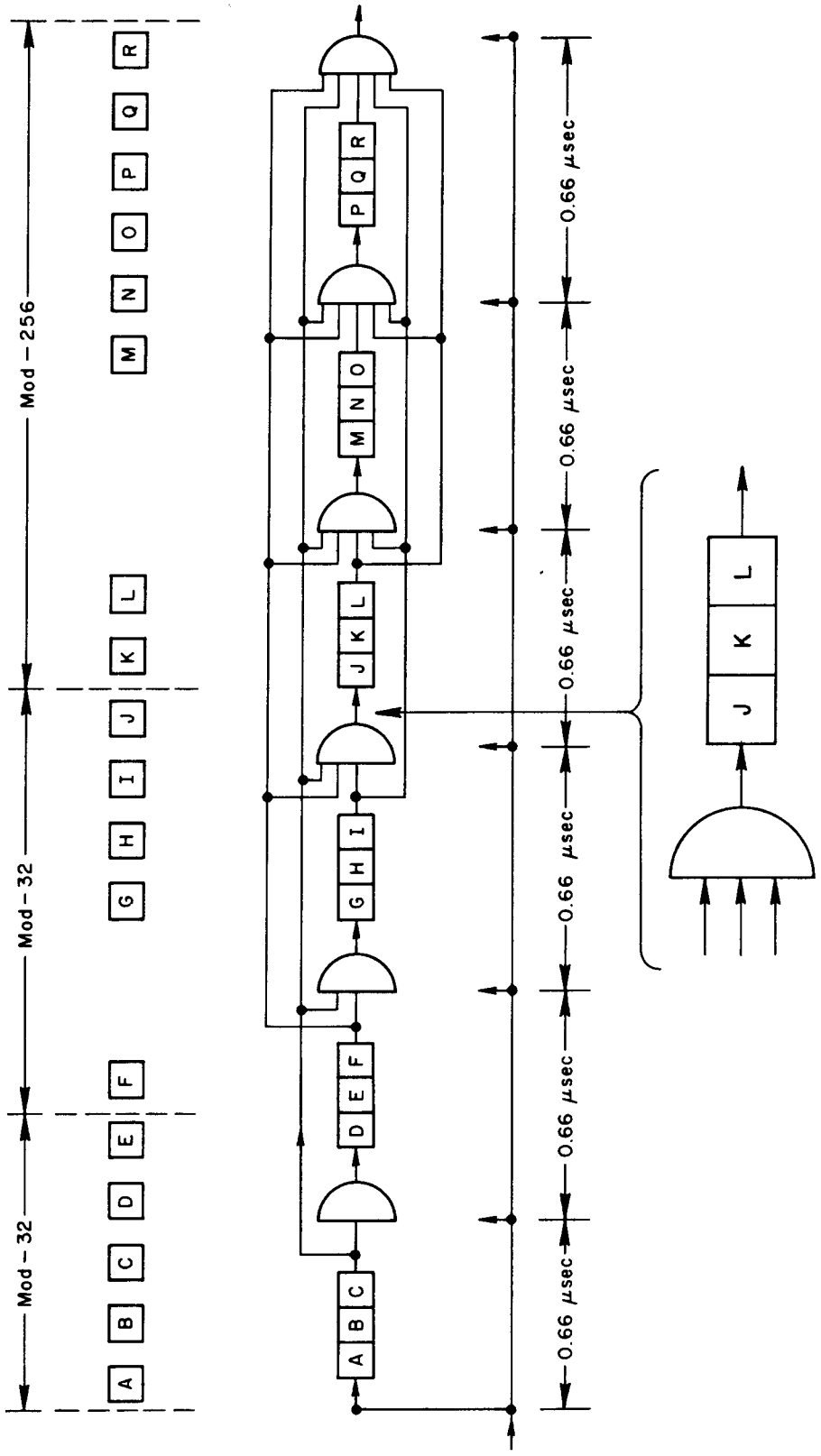


Fig. 17--Low Ripple Counters

within the 0.66-μsec clock period. Unless such precautions are taken, the counter will not read-out "on the fly." While this consideration may appear to be an overdevelopment of a minor hardware design point, it is emphasized because the proposed use of low-cost circuitry makes it mandatory to avoid such logical gating delay buildups. The equipment estimates have been based upon full consideration of this problem.

PARTS COUNT CALCULATIONS

The total number of equivalent flip-flop stages ≃ 3600, as shown in Table VIII. The number of transistors, in all circuits,

≃ 3600 x ~ 4 transistors per equivalent flip-flop

≃ 14,400 transistors.

Table VIII

NUMBER OF EQUIVALENT FLIP-FLOPS REQUIRED

		Equivalent F/F per Unit	No. Units	Sub-Total
Link Unit	Input	123		
	Output	106		
	Total	229	8	1832
Buffer Unit	Input	77		
	Output	77		
	Total	154	8	1232
Central Processor	Logic	328	1	328
	Core	192	1	192
Power Supply and Miscellaneous		16	1	16
Refrigerator		-	-	-
Total				3600

The component failure rate for all non-transistorized elements combined is assumed to have a gross failure rate roughly equal to that of the transistorized pieces.

RELIABILITY

Assumed Failure Rate Calculation

It is assumed that the equipment will operate 24 hr/day, and will be housed in a foam-insulated box, air conditioned by a closed-cycle refrigeration system normally operating at 15°C. The system will also be capable of operating for extended periods at 30°C, and, under battle-short conditions for short periods, at 50°C using blowers only.

Low-cost germanium transistors of well known life characteristics will be used. Experience of the Computer Sciences Department at RAND over a six-month period with a home-built experimental system, using 10,000 one-dollar transistors, indicates that a failure rate lower than 0.02 per cent per 1000 hr is achievable.

Fifty per cent of the failures are assumed to be dealt with during routine maintenance (once per month). The remainder will be unexpected failures. This gives a catastrophic-failure rate of 0.01 per cent for transistors alone.

Mean Time Between Failures: Transistors

Following are the calculations for the mean time between failures (MTBF) for transistors:

229 + 154 = 383 equivalent F/F

≃ 1532 transistors

0.02%/1000 hr

= 0.3064 failures/1000 hr.

MTBF for a single particular link is:

3270 hr

= 136.5 days

= 1635 hours mean time between failures of terminal equipment at either end of the link

= 61.5 days.

MTBF for the Central Processor plus Core is:

328 + 192 = 520 equivalent F/F

= 4080 transistors

= 0.816 failures/1000 hr

≃ 1225 hr MTBF

≃ 98.5 days.

Any failure anywhere within a Node, including those minor failures which permit the Node to continue operating but with one or more of its Link Units down, is summarized as follows:

14,400 transistors

= 1.44/1000 hr

= 695 hr MTBF

= 29 days.

The use of new, low-cost silicon transistors would eliminate the need for refrigeration and, perhaps, increase the MTBF.

Maintenance Procedures

If there is a failure of the Central Processor or the Core Power Supply, either of which will take down the entire Switching Node, a repairman will be dispatched from the nearest Multiplexing Station. An average one-way travel time of five hours is assumed from time of alarm.

If the trouble is in any one of the eight Link Units or Buffers, which would disable only the one Link, the repair may be deferred until it is necessary to change the key during the routine maintenance period. A once-per-month marginal check coincident with a key change will constitute the routine maintenance.

Uptime Calculation

$$\% \text{ Uptime} = \frac{\text{MTBF} - (\text{travel} + \text{repair})}{\text{MTBF}} - \frac{\text{Maintenance time}}{\text{one month}}$$

$$= \frac{1225 \text{ hr} - (5 + 1) \text{ hr}}{1225 \text{ hr}} - \frac{2 \text{ hr}}{24 \times 30 \text{ hr}}$$

$$= \frac{1219}{1225} - \frac{2}{720}$$

= (99.1 - 0.28) per cent uptime (not including prime power failure)

= 98.8 per cent uptime for each Switching Node--much greater than needed (probably an 80+ per cent uptime will be acceptable).

HEAT AND POWER CALCULATIONS

Heat and power requirements are summarized as follows:

$$H = A \times U \times T \text{ (BTU/hr)}$$

where,

A - area of unit

H = heat passing through insulation

U = insulation coefficient

T = temperature differential.

1) Size of unit = 4' x 3' x 6'.
2) A = 2 (4x3) + 2 (3x6) + 2 (4x6)
   = 24 + 36 + 48
   = 108 sq ft.
3) Absolute maximum heat = $50^{\circ}C = 122^{\circ}F$.
4) Nominal lowest temperature = $15^{\circ}C = 59^{\circ}F$.
5) Average room temperature = $25^{\circ}C = 77^{\circ}F$.
6) Average differential temperature between inside and outside $\approx 18^{\circ}F$.
7) U = 0.2 assuming 1" rigid insulation.*
8) H = (108) (0.2) (18) = 388.8 BTU/hr.
9) E = 1000 watts (this assumes a 440-watt safety factor)
   = 3.4 (1000) BTU/hr = 3,400 BTU/hr.

*Trane Air Conditioning Manual, The Trane Company, La Crosse, Wisconsin, p. 306.

10) For equilibrium, refrigerator must pump out

H + E BTU/hr

= 389 + 3400 = 3789 BTU/hr, total heat gain.

11) Tonnage equivalent of cooling load

$= \frac{3789}{12,000} \simeq \frac{1}{3}$ tons air conditioning.

12) Theoretical equivalent of 1 ton of air conditioning

= 0.876 hp.*

13) Electrical power = $(0.876 \text{ hp})\left(746 \frac{\text{watts}}{\text{hp}}\right)$

= 421 watts electrical power input for refrigeration

$$\frac{(\frac{1}{3} \text{ ton})}{(0.50 \text{ efficiency})} .$$

(Therefore, an ordinary household refrigerator motor and compressor appears satisfactory.)

14) Allow 100 watts for blowers.

15) Total input electrical power =

421 watts (refrigeration)

1000 watts (electrical input)

100 watts (blowers)

1521 watts total electrical input.

*Ibid., p. 39.

ON DISTRIBUTED COMMUNICATIONS:

List of Publications in the Series

I. Introduction to Distributed Communications Networks, Paul Baran, RM-3420-PR.

Introduces the system concept and outlines the requirements for and design considerations of the distributed digital data communications network. Considers especially the use of redundancy as a means of withstanding heavy enemy attacks. A general understanding of the proposal may be obtained by reading this volume and Vol. XI.

II. Digital Simulation of Hot-Potato Routing in a Broadband Distributed Communications Network, Sharla P. Boehm and Paul Baran, RM-3103-PR.

Describes a computer simulation of the message routing scheme proposed. The basic routing doctrine permitted a network to suffer a large number of breaks, then reconstitute itself by rapidly relearning to make best use of the surviving links.

III. Determination of Path-Lengths in a Distributed Network, J. W. Smith, RM-3578-PR.

Continues model simulation reported in Vol. II. The program was rewritten in a more powerful computer language allowing examination of larger networks. Modification of the routing doctrine by intermittently reducing the input data rate of local traffic reduced to a low level the number of message blocks taking excessively long paths. The level was so low that a deterministic equation was required in lieu of Monte Carlo to examine the now rare event of a long message block path. The results of both the simulation and the equation agreed in the area of overlapping validity.

IV. Priority, Precedence, and Overload, Paul Baran, RM-3638-PR.

The creation of dynamic or flexible priority and precedence structures within a communication system handling a mixture of traffic with different data rate, urgency, and importance levels is discussed. The goal chosen is optimum utilization of the communications resource within a seriously degraded and overloaded network.

V. History, Alternative Approaches, and Comparisons, Paul Baran, RM-3097-PR.

A background paper acknowledging the efforts of people in many fields working toward the development of large communications systems where system reliability and survivability are mandatory. A consideration of terminology is designed to acquaint the reader with the diverse, sometimes conflicting, definitions used. The evolution of the distributed network is traced, and a number of earlier hardware proposals are outlined.

VI. Mini-Cost Microwave, Paul Baran, RM-3762-PR.

The technical feasibility of constructing an extremely low-cost, all-digital, X- or K_u-band microwave relay system, operating at a multimegabit per second data rate, is examined. The use of newly developed varactor multipliers permits the design of a miniature, all-solid-state microwave repeater powered by a thermoelectric converter burning L-P fuel.

VII. Tentative Engineering Specifications and Preliminary Design for a High-Data-Rate Distributed Network Switching Node, Paul Baran, RM-3763-PR.

High-speed, or "hot-potato," store-and-forward message block relaying forms the heart of the proposed information transmission system. The Switching Nodes are the units in which the complex processing takes place. The node is described in sufficient engineering detail to estimate the components required. Timing calculations, together with a projected implementation

scheme, provide a strong foundation for the belief that the construction and use of the node is practical.

VIII. The Multiplexing Station, Paul Baran, RM-3764-PR.

A description of the Multiplexing Stations which connect subscribers to the Switching Nodes. The presentation is in engineering detail, demonstrating how the network will simultaneously process traffic from up to 1024 separate users sending a mixture of start-stop teletypewriter, digital voice, and other synchronous signals at various rates.

IX. Security, Secrecy, and Tamper-Free Considerations, Paul Baran, RM-3765-PR.

Considers the security aspects of a system of the type proposed, in which secrecy is of paramount importance. Describes the safeguards to be built into the network, and evaluates the premise that the existence of "spies" within the supposedly secure system must be anticipated. Security provisions are based on the belief that protection is best obtained by raising the "price" of espied information to a level which becomes excessive. The treatment of the subject is itself unclassified.

X. Cost Estimate, Paul Baran, RM-3766-PR.

A detailed cost estimate for the entire proposed system, based on an arbitrary network configuration of 400 Switching Nodes, servicing 100,000 simultaneous users via 200 Multiplexing Stations. Assuming a usable life of ten years, all costs, including operating costs, are estimated at about $60,000,000 per year.

XI. Summary Overview, Paul Baran, RM-3767-PR.

Summarizes the system proposal, highlighting the more important features. Considers the particular advantages of the distributed network, and comments on disadvantages. An outline is given of the manner in which future research aimed at an actual implementation of the network might be conducted. Together with the introductory volume, it provides a general description of the entire system concept.