

MEMORANDUM
RM-3764-PR
AUGUST 1964

ON DISTRIBUTED COMMUNICATIONS:
VIII. THE MULTIPLEXING STATION

Paul Baran

PREPARED FOR:
UNITED STATES AIR FORCE PROJECT RAND

The **RAND** *Corporation*
SANTA MONICA • CALIFORNIA

MEMORANDUM

RM-3764-PR

AUGUST 1964

ON DISTRIBUTED COMMUNICATIONS:
VIII. THE MULTIPLEXING STATION

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 eighth in the series, describes the Multiplexing Stations that connect subscribers to Switching Nodes (detailed in Vol. VII) of the proposed broadband distributed network. The description is presented in engineering detail, showing how the Station is able to process simultaneously traffic from up to 1024 separate users sending a mixture of start-stop teletype signals and synchronous signals at various rates.

The Memorandum will be of principal interest to those concerned with the details of design and operation of the proposed network, and also of some interest to communications designers and planners concerned with the transmission of digital data.

*A list of all items in the series is found on p. 101.

SUMMARY

In this Memorandum, the operations of and the equipment in the Multiplexing Station of the Distributed Adaptive Message Block Network are examined and described.

The Multiplexing Station feeds the Switching Nodes (described in Vol. VII in the series), and constitutes the interface between the users and the network; it might be likened to a telephone central office. Each station is able to accept a mixture of start-stop teletype signals; 600-, 2400-, 9600-, 19,200-bit/sec synchronous signals; and a limited number of highly intermittent megabit/sec signal subscribers. It is able to simultaneously process traffic from a maximum of 1024 separate users, connected into any single Switching Node.

The system possesses flexibility for automatic re-routing of calls to the most recent location of a subscriber; it uses push-button dialing, contains automatic self-synchronizing end-to-end cryptographic protection, and is suitable for both digital voice and digital data applications. Additionally, all buffering operations necessary to package and unpack data streams from network users are performed at the Multiplexing Station. Transmission is automatically suppressed when no active data is being transmitted between connected users, allowing highly efficient use of the network in handling secure digital voice data.

The Multiplexing Station is comprised of a magnetic drum, a magnetic core store, and necessary special-purpose transistorized digital processing equipment, occupying about 150 cu ft.

In addition to detailed descriptions of the components and the operations of the Station, some engineering specifications, flow charts, and computational criteria are included. Some conclusions regarding feasibilities, and areas requiring more detailed investigation, are contained in the last two sections.

ACKNOWLEDGMENTS

I would like to thank Tom Ellis and Keith Uncapher of The RAND Corporation and acknowledge their considerable help in providing a stream of useful ideas which have been incorporated into this Memorandum.

CONTENTS

PREFACE	iii
SUMMARY	v
ACKNOWLEDGMENTS	vii
FIGURES	xiii
TABLES	xv
Section	
I. INTRODUCTION	1
Definition and Purpose of the Multi- plexing Station	1
Interconnection Between Multiplexing Stations and Switching Nodes	3
II. OPERATIONS WITHIN THE MULTIPLEXING STATION	10
Address Designation and Numbering Plan ..	10
Remote Addressing	10
Push-Button Dialing	11
Processing Operations	12
Telephone Input	13
Input Operations	14
Blank Space Suppression	14
Choice of an Encryption Scheme	15
Processing an Incoming Message Block ..	16
Other Processing Functions	16
III. INPUT/OUTPUT DEVICES	18
Types of Devices	18
Synchronous Input Devices	18
Retiming Tolerance	19
Timing Calculation	19
Expected Data Rates for Synchronous Devices	20
Non-synchronous Inputs	21
IV. USER-TO-USER CONSIDERATIONS	25
The Quasi-Real-Time Circuit Illusion	25
Signaling Standards	25
V. DETAILED SYSTEM CONFIGURATION	28
Gross Description	31
Unit A, <u>From</u> Subscriber <u>To</u> Drum Unit ..	31
Unit B, <u>From</u> Subscriber <u>Via</u> Drum Unit	31

Unit C, <u>From</u> Subscriber Crypto Unit	31
Unit D, Outgoing Line to Buffer Unit	31
Unit J, Central Processor	32
Unit F, Output Link Unit	32
Unit G, Alternate Link Selector and Failure Mode Multiplexer Unit	32
Unit H, Input Link Unit	32
Unit I, Translator (Address Table Look-Up) Unit	33
Unit K, Trace and Trouble Display Unit	33
Unit L, <u>To</u> Subscriber <u>Via</u> Drum Unit	33
Unit N, <u>To</u> Subscriber <u>From</u> Drum Unit	34
Unit O, Common <u>To/From</u> Subscriber Controls Unit	34
Unit P, Priority Control Console ...	34
Unit Q, Intercept Position and Change Translator Table Input Unit	34
Unit R, High-Speed Drop Point Input/Output Unit	34
Unit S, Common Timing Sampling and Individual Input Phase Selector Control Unit	35
Unit T, Power Supply Unit	35
Unit U, Emergency Power Source Unit	35
Unit V, Emergency Partial Power Supply Unit	36
Unit W, Common Drum Unit	36
Unit X, Zero and Signaling Detector	37
Detailed Description	37
Operation of <u>From</u> Subscriber <u>To</u> Drum Unit, A	37
Composition of Inputs	38
Input Strobing	40
The Crypto Scheme	45
Operation of <u>From</u> Subscriber <u>Via</u> Drum Unit, B	47
Operation of <u>From</u> Subscriber Crypto Unit, C	50
Operation of Buffer Units, D, E; and Input/Output Link Units, F, H	50
Operation of Alternate Link Selector and Failure Mode Multiplexer Unit, G	50
Operation of Input Link Unit, H	59

Operation of Translator (Address Table Look-Up) Unit, I	59
Operations Performed in the Process of Setting up a Call	59
Creating Signaling Tones by the Use of a Repeating Digital Sequence	60
High-Speed-Core Housekeeping Operations Upon Message Blocks Newly Arriving at the Terminal Line Distributor	60
Operation of Trace and Trouble Display Unit, K	66
Operation of <u>To</u> Subscriber <u>From</u> Drum Unit, N	70
Operation of Priority Control Console, Unit P	70
Operation of Intercept Position and Change Translator Table Input Unit, Q	75
Operation of Common Drum Unit, W ...	77
Processing Drum Calculation	78
Operation of High-Speed Drop Point Input/Output Unit, R	79
Calculation of the Number of Drum Bands for Translator Table	82
Read/Write Head Switching Detail ...	82
Operation of Zero and Signaling Detector, Unit X	82
Operation of the Modify Key Box, Unit Y	85
Operation of Remote Devices at Subscriber Stations, Unit Z	87
VI. MAJOR EQUIPMENT COMPLEMENT	95
Caveat	96
Insufficiently Examined Areas	96
VII. CONCLUSIONS	99
LIST OF PUBLICATIONS IN THE SERIES	101

FIGURES

Figure

1. Interconnection Between Multiplexing Stations and Switching Nodes	4
2. Distortion of Network Near Critical Points	6
3. A Set of Nodes Using "Real-World" Geometry	8
4. The Same Set of Nodes Distorted to Fit a Rectangular Grid	9
5. Remote Line Signaling Signals	27
6. Major Block Flow Diagram	29
7. From Subscriber to Drum Unit	41
8. Multiphase Strobe Timing at the Line Input Buffer Unit	42
9. Line Input Unit	43
10. 32-Input/1-Output Switch	44
11. 1-Input/32-Output Switch	46
12. Principle of Crypto Scheme	46
13. Receiving Section, Decryption	48
14. From Subscriber via Drum Unit	49
15. From Subscriber Crypto Unit	51
16. Buffer Unit	53
17. Input Link Unit	54
18. Output Link Unit	55
19. Alternate Link Selector and Failure Mode Multiplexer Unit	57
20. Translator (Address Table Look-Up) Unit ..	61
21. Operations Performed in Setting Up a Call Between Network Users	62
22. Creating Signaling Tones by the Use of a Repeating Digital Sequence	63
23. a--High-Speed-Core Housekeeping Operations Upon Message Blocks Newly Arriving at Terminal Line Distributor	64
b--Subroutine NEW CALL	65
24. Graphical Display for Intercepted Messages Using a 10-Column Output Device	67

25. Footprint Trace	68
26. Span of Coverage for a Trace Unit with a Span of Four--Five Broken Links	69
27. Span of Coverage for a Trace Unit with a Span of Four--Two Defective Nodes	71
28. Overlapping Coverage of Trace	72
29. To Subscriber From Drum Unit	73
30. Priority Control Console	74
31. Subscriber's Card	76
32. High-Speed Drop Point Input/Output Unit ..	80
33. Read/Write Head Switching Detail	83
34. Zero and Signaling Detector	84
35. Tape Playback Unit Used to Insert New Keys	88
36. Typical Telephone Proposed for Use in the System	89
37. Telephone with A/D Converter and Push-Button Signaling	91
38. Counter Unit with Push Buttons	92
39. Modem for Standard Start-Stop Teletype with Signaling Attachment	94

TABLES

I.	Equipment Breakdown for the Multiplexing Station	30
II.	Composition of Inputs	39
III.	Standard Speeds	56

I. INTRODUCTION

A method of interconnecting high-speed all-digital Switching Nodes to form a highly survivable network structure able to transmit large quantities of data has been described in other volumes in this series. But, up to this point, only a portion of the overall communication network--the transmission subsystem for relaying Message Blocks from Switching Nodes to other Switching Nodes--has been detailed.

In the present Memorandum we expand the system description and describe the means by which network users, or "subscribers," enter the network to reach other subscribers.

DEFINITION AND PURPOSE OF THE MULTIPLEXING STATION

The term "Multiplexing Station" is used to describe that equipment which concentrates traffic from a number of simultaneous users into a form suitable for transmission by the Switching Nodes. Multiplexing Stations can be built in a wide range of sizes and for a wide variety of input devices. However, the description here is limited to one having the following specific characteristics:

- 1) The Multiplexing Station shall process information from as many as 1024 separate subscribers.
- 2) The Multiplexing Station shall perform all house-keeping operations necessary to convert low-data-rate input binary streams from any subscriber into Message Blocks for transmission into the network.
- 3) The Multiplexing Station shall provide the data storage buffering means to unpack Message Blocks into a synchronous binary stream necessary for use by the end-addressees.

- 4) The Multiplexing Station shall contain the means to interpret, modify, and transmit signaling information to and from its connected subscribers.
- 5) The Multiplexing Station will probably, but not necessarily, be a manned station and shall contain a means for receiving trouble messages originating from nearby Switching Nodes, and for ascertaining system malfunctions.
- 6) The Multiplexing Station shall contain complete on-line cryptographic apparatus to permit automatic on-line, end-to-end encryption of data from all locally connected subscribers for transmission to any other network user.
- 7) The cryptographic apparatus used and contained within the Multiplexing Station shall be suitable for simultaneous handling of both classified and unclassified traffic. (This is required because many lines feeding the Multiplexing Station could originate from cryptographically non-secure areas.) The cryptographic equipment shall contain safeguards against cipher-breaking attempts based upon the insertion of known traffic into the network.
- 8) The Multiplexing Station shall tie into two or three separate Switching Nodes by separate routes. These may be simple time-division routes multiplexed upon the same routes used between various Switching Nodes. (Alternate routes are necessary because of the limited reliability of a single route, but these alternate routes need not all be simultaneously available.)
- 9) Key network subscribers shall be tied into two or more Multiplexing Stations. The Multiplexing Stations can be designed so that in the event of a major failure, the most important network

subscribers are group-transferred to an adjacent Station for entry into the network--but with a loss of the end-to-end cryptographic and error protection.

- 10) The Multiplexing Station shall be capable of simultaneous assignment of as many as eight separate office codes, for purposes of tactical mobility and reliability.

The large hypothetical Multiplexing Station described herein is designed primarily to handle traffic such as would exist from several hundred major military installations. We will first examine the case in which all the input devices (teletypewriters, telephones, etc.), together with the Multiplexing Station, are within a single, cryptographically secure area. (We will later discuss the case in which the input devices are connected by lines remote from the Multiplexing Station.)

For ease of description, the circuits between the subscriber and his Multiplexing Stations are called lines; lines are generally low-data-rate circuits. Circuits between Switching Nodes and, generally, those circuits operating at 1.5-megabit/sec rates, shall be called links.

INTERCONNECTION BETWEEN MULTIPLEXING STATIONS AND SWITCHING NODES

Figure 1 shows a possible interconnection configuration of Multiplexing Stations and Switching Nodes. One might imagine Fig. 1 as being representative of a portion of a large national network, comprising about 400 Switching Nodes and 200 Multiplexing Stations. The system itself is designed to handle any number of Switching Nodes together with 1024 Multiplexing Stations. Multiplying 1024 stations by 1024 subscribers connected to each, implies a tentative design capacity of about one million simultaneous

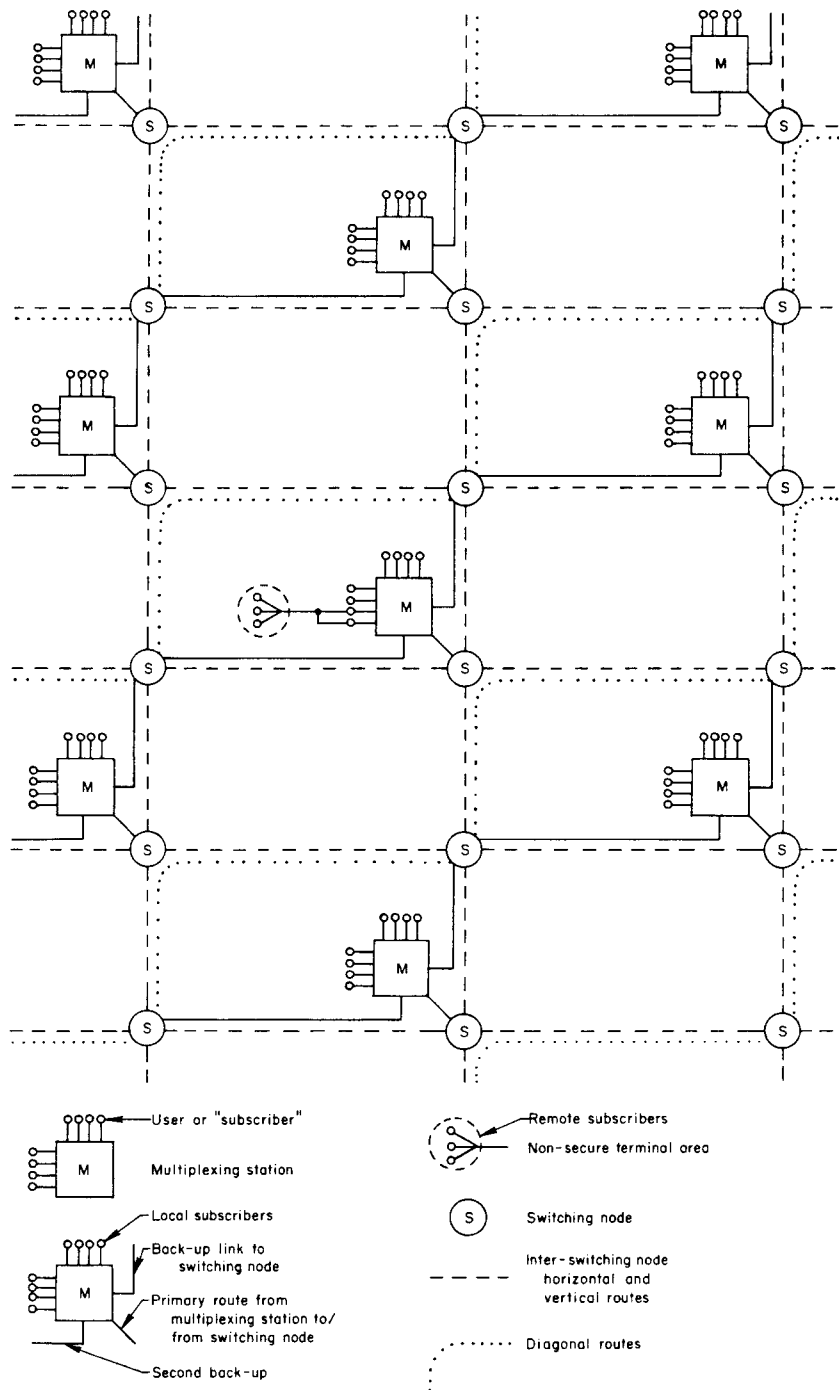


Fig. 1--Interconnection Between Multiplexing Stations and Switching Nodes

network subscribers. But, further expansion does not appear difficult, if it should become necessary. It should be noted that in Fig. 1 there are only about half as many Multiplexing Stations as Switching Nodes. In this illustration, each Multiplexing Station is connected by a primary route to its nearest Switching Node and has two alternate routes leading to adjacent Multiplexing Stations via adjacent Switching Nodes. The routes used to connect the Multiplexing Stations to the alternate Switching Nodes in this example follow the same routes as those between the Switching Nodes. It is not difficult to time-division multiplex an additional channel over the same link as that used to transfer Message Blocks between Switching Nodes. Thus, at slight additional cost, alternate routes from each Multiplexing Station to its (adjacent) emergency alternate Station can be provided by using the same links that interconnect the Switching Nodes.*

Since Fig. 1 is drawn in the form of a highly regular grid pattern, Fig. 2 has been included to remind the reader that the highly regular canonical form of the distributed network will, in reality, be distorted to provide additional close-in access points to certain critical sites. The spacing requirement between the Switching Nodes is that they shall be so separated geographically as to minimize the probability of destroying more than one Switching Node with a single weapon. As unmanned Switching Nodes are physically small, it is economically feasible to physically "harden" them to further reduce the spacing dimension. Thus, Switching Nodes will be closely spaced in those critical areas where it is necessary to allow many communications feeder links to enter the network.

*The mini-cost microwave links described in ODC-VI operate at 4.5-million bits/sec. Each may be split into several lower-data-rate channels, such as three 1.5-million-bit/sec channels. (ODC is an abbreviation of the series title; the number following refers to the particular volume within the series.)

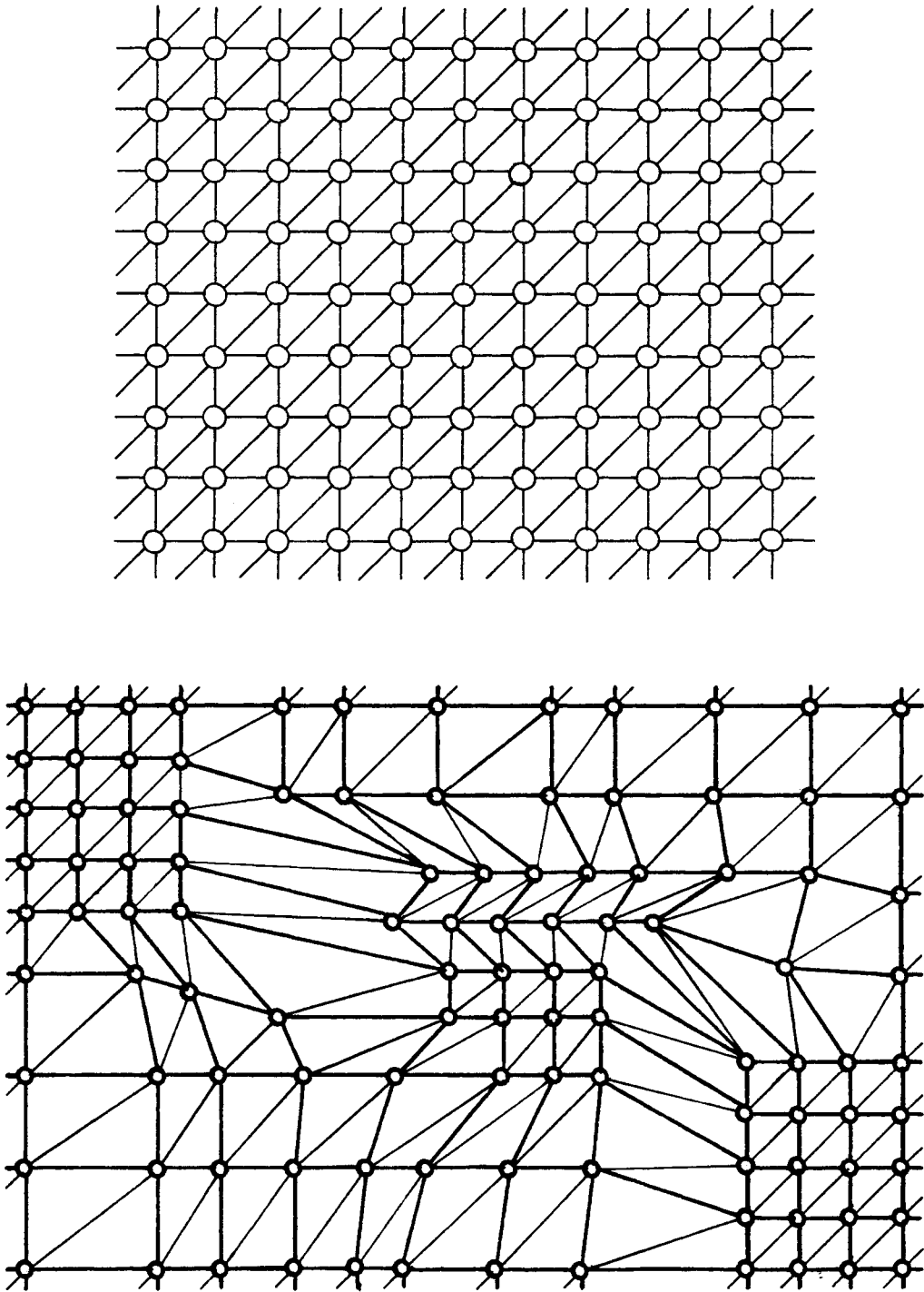


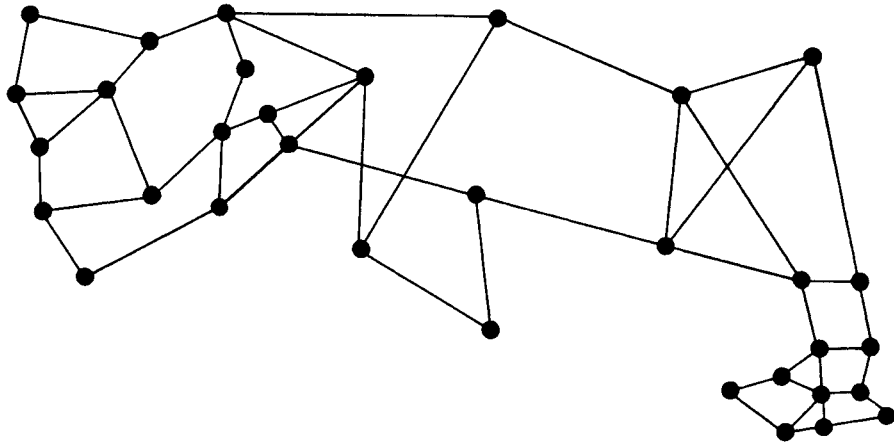
Fig. 2--Distortion of Network Near Critical Points

The precise number of Switching Nodes and multiplexing tie-points and their geometry is not examined in this series. However, we believe it is possible to provide the requisite communication means into the network at a few highly critical points, with a survivability level comparable to that of the remainder of the network.

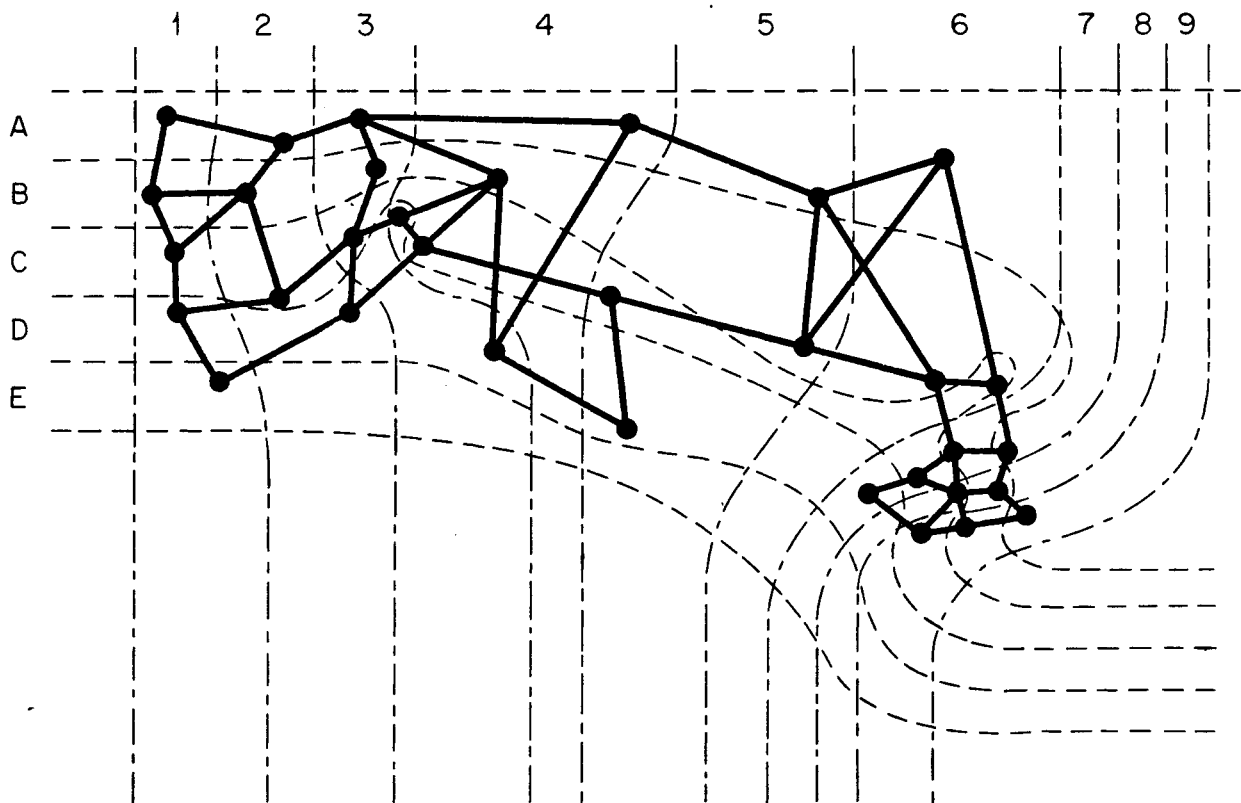
A second form of topographic network distortion occurs when we consider the "real-world" location of the subscribers; this is illustrated in Figs. 3 and 4. Although it is convenient to refer to distributed networks with words that imply an overall uniformity of connectivity, this need not be a restricting condition. The best locations for major communications stations are not at uniformly spaced points, since best routes for communications links are rarely straight lines. Hence, some Switching Nodes may have many links to adjacent Switching Nodes, others few; Fig. 3 is a more realistic view of the topography of a real-world network. Figure 4 shows that the set of Nodes of Fig. 3 can be squeezed to fit a uniform matrix. It might be helpful to visualize the network as being drawn on a sheet of rubber, which is then distorted, for ease of visualization and analysis, to give the appearance of a neat rectangular configuration. Most survivability estimates for perfect-switching distributed networks have been based upon the assumption of a uniform 18x18 array of 324 stations.*

Thus, there are no inherent restrictions to the topography of the network implied in the following discussion, although we will describe a system of uniform connectivity.

*Edge effects, caused by the outside edge of the network being less survivable than the interior of the network due to lesser connectivity, were ignored; it has been found that such effects insert only a slightly pessimistic bias in the survivability estimates for the network. This is briefly described in Reliable Digital Communications Systems Using Unreliable Network Repeater Nodes, by Paul Baran, The RAND Corporation, P-1995, May 27, 1960.



3a



3b

Fig. 3--A Set of Nodes Using "Real-World" Geometry

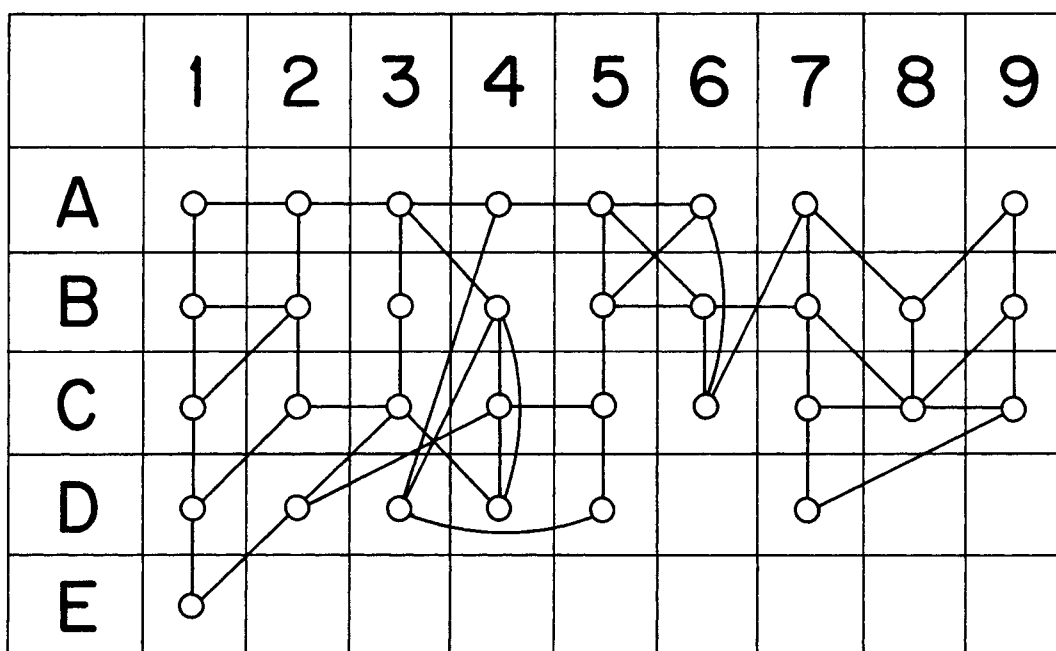


Fig. 4--The Same Set of Nodes
Distorted to Fit a Rectangular Grid

II. OPERATIONS WITHIN THE MULTIPLEXING STATION

Each of the 1024 separate users, or "subscribers," at each Multiplexing Station is assigned one or more permanent "telephone numbers" or "addresses," and each subscriber is allowed to call any other network subscriber.

ADDRESS DESIGNATION AND NUMBERING PLAN

On the basis of 1024 possible Multiplexing Stations and 1024 subscriber lines at each Station, a numbering plan comprising a four-digit octal-number office code (the Multiplexing Station) and a second four-digit octal-number line code is suggested. This permits a possible expansion to 4096 office codes, each having 4056 line codes.*

Each Multiplexing Station may be assigned up to eight separate simultaneous office codes. The office code designations are not permanently assigned to specific Multiplexing Stations. However, each subscriber is assigned a permanent number. Any subscriber can be called by using this permanent number, even if he moves from location to location (provided, of course, that he has informed his nearest Multiplexing Station where he is).

Remote Addressing

When placing a new call, the calling subscriber's first transmitted Message Block, containing the signaling information needed to set up a "quasi-circuit connection," is sent from the calling Multiplexing Station to the called Station. A determination is made at the called Station as

*Having a large excess of possible number combinations imparts a high probability of rapid interception when a network user dials a wrong number.

to whether the particular subscriber being called is currently connected to that Station.

If the called subscriber is at the called Multiplexing Station, and if his line is not busy, revertive signaling information is sent back to the calling Station. This revertive information includes the latest line number of the called party, which shall be used to transmit all subsequent Message Blocks constituting the call.

If the subscriber is not at his "home" Multiplexing Station, but has left a forwarding address to be used, this new forwarding address will be reverted back to the calling Station. The calling Multiplexing Station then automatically replaces the call to the new number. Thus, the calling Multiplexing Station always uses an address for Message Blocks which can be rapidly interpreted by the called Multiplexing Station with a minimum of processing time. This simplifies the high-speed handling of Message Blocks during later transmission. Time-consuming table look-up translation search activities which require access to a slow-speed-access store, such as a magnetic drum, are performed only once during the setting up of the initial call.

Push-Button Dialing

Push-button dialing is used in the system primarily when calls are placed by humans. The following steps describe the placing of this type call.

- 1) To reach subscriber #2345-1241, the digits 2345-1241 are depressed sequentially on the buttons on the calling telephone, or the data transmitter terminal device. The first four digits comprise the office code; the last four, the line code number.

- 2) A Message Block containing the complete called number is formed by the calling Multiplexing Station and sent to the Multiplexing Station currently responsible for office code number 2345.
- 3) A translator table look-up search is performed at (called) Station 2345 for line code 1241.
- 4) This translator table might indicate, for example, that telephone number 2345-1241 corresponds to the subscriber connected to local line number 0532. Next, line number 0532 is tested. Perhaps, it is found to be busy. Again checking the translator table, a search is made to see if there is an alternate number which may be used; if so, this alternate number is tested.
- 5) The alternate table look-up reveals that local line number 0535 is an assigned alternate. This line is tested and found free.
- 6) Local line number 0535 is then sent signaling waveforms which correspond to "ringing signals."
- 7) Upon detecting a signal that line number 0535 has gone "off-hook" (answered), a revertive signal containing a synchronization starting point for an end-to-end cryptographic generator, together with the modified calling number to be used for subsequent Message Blocks for the duration of the call, is sent back to the originating Multiplexing Station. All subsequent Message Blocks making up the call are immediately directed to the desired subscriber's line in cryptographic synchronization without additional table look-up translation.

PROCESSING OPERATIONS

The Multiplexing Station takes the outputs of a large number of low-data-rate devices, forms them into Message

Blocks and semi-asynchronously time-shares them over a single high-data-rate link into the network via the Switching Nodes. To illustrate the data processing that occurs within the Multiplexing Station, let us consider some of the transformations necessary to transmit an audio signal through the system.

Telephone Input

We start from a conventional telephone mouthpiece which transduces speech into an audio voltage. This audio signal is converted by a simple analog-to-digital converter (which may be built into the base of special digital telephones designed for use with this system). The output of the analog-to-digital conversion is a digital stream (whose sampling timing is derived by locking onto the incoming timing signals extracted from the subscriber's line from the Multiplexing Station). The special telephone contains ten push buttons connected into the feedback paths of a simple four-flip-flop, modulo 16, binary counter. To "dial" a number, each of the appropriate push buttons are sequentially depressed. Each button modifies the counter's output to form a repetitive pattern accepted by the local Multiplexing Station. Each button must be depressed for at least one-tenth of a second. This binary signaling stream, because of its highly repetitive pattern, is readily detected and decoded by the Multiplexing Station, permitting rapid separation of signaling from the voice stream of bits.

Signaling operations are generally slow and require complex processing, while the voice stream is handled in a more expeditious "stamping mill" fashion.

Input Operations

The binary stream output data of the digital telephone will depend upon the type of digital modulation chosen. In the following discussions, an output rate of 19,200 bits/sec, using High Information Delta Modulation,* is assumed. This synchronous data stream is temporarily stored in the Multiplexing Station. Separate storage space is used for the signaling information and for voice data. Since the Switching Node will only process the standardized packages of 1024-bit Message Blocks, it is necessary to store and convert the low-speed synchronous stream into these standard-format Message Blocks, suitable for transmission. The signaling information, necessary for addressing each Message Block, is stored in a section of memory called the "rubber stamp buffer." About 1/20 of a second of the digitalized audio is stored into one of three consecutively assigned data buffers. The first of these is called the "Phase-A" data buffer. As soon as this buffer is "full of bits," the incoming synchronous stream to which it is connected starts filling the Phase-B data buffer, etc. The Multiplexing Station interleaves and combines the bits in the various positions of the data buffers with bits from the rubber stamp buffer. These form completed Message Blocks and are burst out of the Multiplexing Station into the connected Switching Node whenever the common output link to the Switching Node is free.

Blank Space Suppression

When two people engage in conversation over a full-duplex channel, much more "silence" is transmitted than

*Winkler, M. R., "High Information Delta Modulation," IEEE International Convention Record, Paper 47.3, March 25, 1963.

voice, as only one person talks at any one time and there are interword spaces. Thus, we have chosen not to transmit Message Blocks unless we have detected some sound during the last 1/20 of a second of the Message Block interval. In return for a modest price increment in terms of additional silence detection and suppression equipment, we believe that we can increase the number of simultaneous voice users by a factor of about four, by utilizing the periods of silence in excess of 1/20 of a second.

This means that a 19,200-bit/sec voice stream really loads the network with an average rate of only about 5,000 bits/sec, producing a highly efficient method of transmitting good-quality digital voice.

Choice of an Encryption Scheme

To protect the secrecy of communications, and to help thwart interference, intentional or otherwise, cryptographic transformations are applied to outgoing Message Blocks to make them intelligible and acceptable only by the specific end-addressee. On the basis of analysis in the design of the Switching Nodes, we expect the system to have an extremely low Multiplexing-Station-to-Multiplexing-Station error rate (on the order of one Message Block lost or incorrect in every 10^8). Thus, we are able to use a form of modified auto-key which requires correct reception of the entire preceding string of Message Blocks before the next block can be properly decrypted. In the event of an error, the "connection" would be "knocked down." To obtain a feeling for the frequency of such an occurrence, consider a 19,200-bit/sec telephone used one hour per day. An interruption of the type being considered would occur only about once a year. When such a transient error did occur, either user could dial the other party and the connection would be automatically reinitiated--and synchronized--using a new modified crypto key. (Re-dialing could also be automatically initiated, if later desired.)

Processing An Incoming Message Block

Message Blocks, each containing 1024 bits, arrive at a receiving Multiplexing Station over the 1.5-megabit/sec links from the connected Switching Node. Each Message Block is temporarily stored in the rapid-access store (magnetic core) while the heading address is examined. Each Message Block also contains an end-to-end sequential transmission number (which is encrypted). If the decrypted sequence number matches the next expected sequence number,* the incoming Message Block is accepted and the crypto count advanced.

The Message Block is stored in three sequentially assigned data buffers (bands on a magnetic drum similar to those used in transmission). This allows flexibility of timing between the local clock timing and Message Blocks arriving by different paths. The differential propagation time between the transmitting and receiving Multiplexing Stations can vary over wide latitudes. The output of the Output Buffer on the drum after decryption is a continuous binary stream stripped of housekeeping; it reaches the receiving subscriber at the same low synchronous speed, locked to be within allowable tolerance limits, as that used by the transmitting party.

Other Processing Functions

The Multiplexing Station not only transforms digital signals from the telephone microphone into Message Blocks suitable for transmission and back into a continuous digital stream, but also provides the means for concentrating a

*This prevents any possible interruptions to the "quasi-circuit" set up between two users by a sophisticated enemy agent who has broken the link-to-link crypto code and has somehow inserted false signals acceptable to the Switching Nodes.

large number of potential network users. Each subscriber's line is continuously, sequentially, and rapidly tested. Only those users that are transmitting active information are, in effect, connected into the network.

The Multiplexing Station further provides facilities to perform priority control for the various users. It also acts as a terminal point for processing trouble information and performs miscellaneous operations, such as inserting a dummy stream of zeros into the line output devices during periods in which no Message Block transmissions are received from the calling party.

III. INPUT/OUTPUT DEVICES

TYPES OF DEVICES

Input data transducers may be categorized into synchronous and non-synchronous devices. Synchronous devices operate at a constant, fixed, and uninterrupted bit rate. Non-synchronous devices, such as start-stop telegraph systems, are fundamentally synchronous, but need maintain synchronization over only a very short time interval; e.g., a single transmitted character spacing. The time interval between characters is allowed to be highly asynchronous.

Although it is possible to build the Multiplexing Station to work with any arbitrary number of data rate input devices, it was found most convenient to restrict consideration to the few most commonly used standardized data rates which appear to be emerging as the most probable speeds for the future.

We shall briefly review the data rates of some of the synchronous input devices we may expect to see in the future, and then discuss the method to be used to handle non-synchronous channels.

SYNCHRONOUS INPUT DEVICES

An examination of those data terminal devices now in use reveals that all the high-speed devices (those in excess of 600 bits/sec) are synchronous in operation. The only non-synchronous devices found were the low-speed asynchronous systems such as start-stop teletypewriters.

The small allowable plus or minus speed tolerance rate of synchronous devices is sometimes called "rubber." It will be assumed that all synchronous devices used with this network can lock onto timing derived from a remote timing signal, provided that this remote timing signal falls within the allowable timing "rubber." Since all lines in the

system within the Multiplexing Station area are essentially "full-duplex," (simultaneously transmitting and receiving), it will be assumed that transmitting synchronization will be derived from the input waveform on the duplexed receiving line. Even when the receiving line is otherwise idle, it will still convey a signal usable for retiming.

RETIMING TOLERANCE

There are several key retiming problems which must be considered, including the problem of the time delay caused by phase shift over conventional telephone lines. A conventional telephone circuit might feed the network at a rate of about 2400 bits/sec. We shall have to live with a difference in timing between the Multiplexing Station and the remote input telephone lines, caused by the phase drift; for example, in the case of transmitting a non-classified data stream from a remote device via the conventional telephone plant into the Multiplexing Station. In this discussion, we assume use of only inexpensive frequency control crystals at the Multiplexing Station (accuracy: $\pm 10^{-7}$).

TIMING CALCULATION

1. A one-bit interval is equal to $1/2400$ sec.
2. Clock accuracy at each Multiplexing Station is 10^{-7} .
3. At the maximum drift rate, it will take 4167 sec to slip one bit.
4. Anticipated drift rate from each input is low and a single time-shared data examination servo-system at the Multiplexing Station could measure and track the timing drift caused by drift on the input line.
5. As the Multiplexing Stations must handle data bursts from the high-speed links from the Switching Nodes, buffering equipment is required to unpack Message Blocks at the desired low synchronous stream output

clock rate. We circumvent the timing drift problem caused by the slightly different data rates of the various Multiplexing Stations and their devices, by storing entire Message Blocks, equivalent to 866 active bits, to form a second level of "rubber." This permits two subscribers to drift apart in timing by as much as one whole Message Block before a timing discontinuity occurs between the two Multiplexing Stations and their subscribers.

6. At the 2400-bit/sec data rate, it would take approximately 40 days to build up to this value of drift.
7. At the 19.2-kilobit rate, it will take one-eighth as long, or about five days. As will be later shown, it will probably be desirable to change the Multiplexing Station end-to-end crypto key every 24 hours. Thus, we do not expect synchronization breaks caused by subscriber-to-subscriber drift.
8. Therefore, only a modest crystal stability accuracy is necessary in the system to allow synchronous transmitting and receiving devices to track with one another.

EXPECTED DATA RATES FOR SYNCHRONOUS DEVICES

While there is an attempt to standardize military digital communications data rates to the $75(2^n)$ -bits/sec series,* only a limited number of these speed values are found in common use. The preferred rates--600, 2400, 9600 and 19,200 bits/sec--are used in the following major applications:

- 1) 600 bits/sec provides a conservative data rate capable of being transmitted over long distances over a conventional switched telephone network, with relatively simple modems.
- 2) 2400 bits/sec may be transmitted over several hundred miles of "private line" telephone company circuits, provided the circuits are carefully selected and equalized for data transmission.
- 3) 9600 bits/sec is a convenient speed for high-speed digital facsimile transmission.

*Where n is an integer.

- 4) 19,200 bits/sec is the lowest standard data rate allowing good voice transmission with relatively simple circuitry.* (Other high-quality pulse code modulation systems used for digital voice require pulse repetition rates of 38.4 kilobits/sec, and higher.) At present, the limitation of high-quality digital voice transmission systems is that they suffer from a slight amount of "quantization noise," noticeable only during periods of silence. This may be a detriment in the proposed system, but a simple background squelch circuit may be used to silence these noise periods.

It is conceivable that one day we would like to have the capability of using on-line computers in the network to intermittently spurt large blocks of data to other computers at a very high data rate (e.g., 1,000,000+ bits/sec), but at a low duty cycle. Because of the low duty cycle, it is felt that many such users at a Multiplexing Station could share a common "party line." In designing such "party lines," the expedient will be described wherein each subscriber transmits only during those times when no other known competing source wishes to transmit. Thus, we shall also allow a party line of very-high-speed devices to feed the Multiplexing Station in a quasi-asynchronous manner.

NON-ASYNCHRONOUS INPUTS

In designing the network to handle non-asynchronous (usually teletype) inputs, the first approach considered was that of storing individual bits into separate low-speed buffers to form complete Message Blocks. However, there were several overriding problems:

- 1) The non-asynchronous characters contain "stop" bits whose duration is longer than the remainder of the character bits.

*Winkler, op. cit.

- 2) Five-, six-, and eight-bit characters are all in common use.
- 3) Most importantly, the slow-speed teletype bit rates require an excessive time to fill the standard-bit-length Message Block. For example, if two teletype stations wanted to converse with one another, the second station would not receive any text from the first station until the first station had typed almost three complete lines:

$$\frac{(866 \text{ bits})}{(5 \text{ bits/character} \times 72 \text{ characters/line})} \cdot$$

The time delay would be on the order of 15 sec:

$$\frac{(866 \text{ bits})}{(60 \text{ bits/sec})} \cdot$$

Therefore, we have chosen to use the expedient of modulating a synchronous 600-bit/sec pulse train by the teletype signal in a conventional amplitude modulation manner. The Message Block loading time for teletype is reduced to only about 1.5 sec,

$$\frac{(866 \text{ bits})}{(600 \text{ bits/sec})} \cdot$$

Therefore, the overall delay in teletype transmission is on the order of two seconds between transmitter and receiver, which allows real-time user-to-user teletype operation.

The 600-bit/sec modulated-carrier approach allows any conventional-speed teletype signal--whether it be 5-level, 6-level, or more--to be transmitted without providing separate apparatus to interpret each character and strip the start and stop pulses. This modulation approach requires that the bit length of the teletype signal be much longer than the modulation carrier period, 1/600 sec (1.667 ms). Even at teletype speeds of 100 wpm, the bit length is 13.5 ms, compared with 1.66-ms pulse length for the modulated carrier. Thus, only a tolerable

12 per cent time-space distortion is introduced to the teletype waveform. No difficulties are anticipated by this time distortion, as it falls within the acceptable operating range of the conventional mechanical teletype printer. (Auxiliary devices are also available which regenerate teletype signals with time-distortion levels up to 50 per cent--if ever needed.)

Transmitting 60-bit/sec teletypewriter signals by using a 600-bit/sec carrier may strike the reader as an inefficient use of the communications resource. However, the marginal capital investment in terminal equipment necessary for more efficient teletype transmission is in excess of the marginal cost of the communication link's capacity to handle this small additional data rate. It appears economically preferable to use "inefficient" transmission within the distributed network in this case, since it is cheaper--less terminal equipment is required. Transmission of 600 bits/sec in lieu of 75 bits/sec is a negligible price to pay when the cost of 1.5- and 4.5-megabit/sec links are considered (see ODC-X).

While a 600-bit wave train is used by the Multiplexing Stations, this does not mean that full-duplex 600-bit/sec teletype circuits are mandatory outside the Multiplexing Station area. It is feasible to modulate or demodulate the 600-bit/sec teletype waveform for the remainder of the distance to the end-subscriber. Thus, we can use conventional narrow-band, full-duplex, half-duplex, or even simplex telephone or teletype circuits to remote points. Conventional high-frequency radio teletype circuits can also be used, and "binary-stream"* transmission maintained to a remote teletypewriter.

* Binary stream teletype transmission is defined as one in which no additional start and stop pulses or characters are added or deleted when passing through relay stations.

The additional equipment required to handle conventional teletype is a cigar-box-size container with the push buttons, generator signaling, and a simple amplitude modulation and detection circuit. The signaling used will be identical in format to that used by the digital telephones, as described.

IV. USER-TO-USER CONSIDERATIONS

THE QUASI-REAL-TIME CIRCUIT ILLUSION

Consider the distributed network as being a large "black box" connected between two subscribers. Thus, if one looks at the transfer function of this box from the viewpoint of either subscriber, it will appear that the black box is a simple delay line; an illusion is created of a quasi-real-time link connecting two terminal points with the following specific properties:

- 1) A fixed time delay exists between input and output. (When setting up a call, a maximum expected time delay is purposely inserted that is longer than the worst-case longest expected differential propagation time between the input and the output caused by Message Blocks arriving by different paths.)
- 2) The output bit rate tracks the input bit rate to within about 10^{-6} or 10^{-7} time drift. Rather than insert extra bits or delete bits, when the output drifts relative to the input, we have chosen the alternative of modifying the overall delay time between input and output.
- 3) A slight, very slow variation of this fixed overall time delay occurs between input and output.
- 4) The overall "quasi-circuit" exhibits a basic very low error rate (on the order of one error in 10^8 bits) between any two subscribers.
- 5) In the rare event of an error, all subsequent transmissions of this single call become "garbage." Both parties and the nearest trouble-monitoring point will be immediately informed of the error and the quasi-circuit will be knocked down. It will be necessary to re-establish the call, unless we choose to re-establish calls automatically, which has not been felt to be necessary.

SIGNALING STANDARDS

One unique property of the network is that the signaling data is of identical pulse shape form and characteristics as the transmitted data, allowing great freedom in

inserting additional signaling information even after the circuit has been set up. This is expected to be most useful when building future computer-to-computer systems, because the signaling information can be intermixed in the data stream by a computer connected into the network.

Signaling digits are expected to conform to the following restrictions:

- 1) Each signaling digit shall be a repetitive binary pattern and shall continue for a time longer than $8/75$ sec (one drum revolution).
- 2) Each signaling digit shall last no longer than 3 sec.
- 3) Signaling digits may follow one another with a delay equal to or greater than $8/75$ sec.
- 4) Any pause greater than 20 sec between punching signaling buttons, shall require the subscriber to redial.
- 5) Addresses shall generally be comprised of eight digits, of which four shall comprise local exchange (Multiplexing Station) number and four digits shall be the line number.

The repetitive digital pattern used for signaling can be created by a set of three flip-flops connected in a feedback counter circuit, or by a simple ring counter. Depressing signaling buttons would modify the feedback connections of the counter. For example, Fig. 5 shows repetitive waveforms which can be created by three flip-flops whose feedback patterns are changed. Ten separate waveforms are shown; these are used to represent the numeric digits 0-9, and are essentially comma-free codes having the property of being easily decoded. (Also shown are five additional states not used since they could be confused with the numbers 1, 3, 4, 6, and 7, in the event of a phase reversal.)

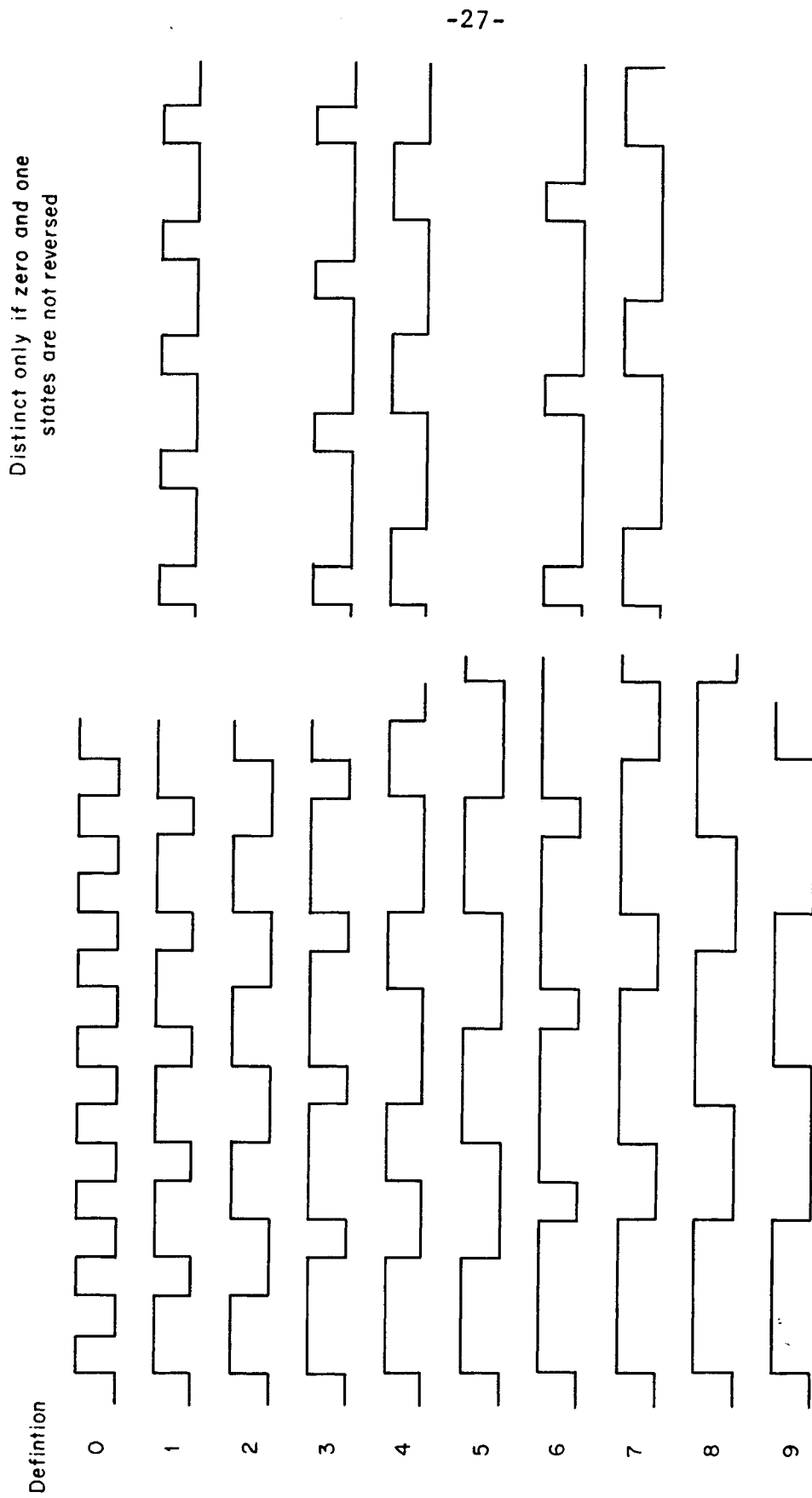


Fig. 5--Remote Line Signaling Signals

V. DETAILED SYSTEM CONFIGURATION

We shall now examine the detail of the proposed Multiplexing Station and explain the mechanisms used to perform the operations described in the previous sections. While the number of subscribers that can be handled by any single Multiplexing Station is not fixed, it is basically a function of cost. In this section the discussion is limited to a single Multiplexing Station having 1024 separate input and output subscriber lines. It is further assumed that this "central office" has been designed to possess a much higher peak-occupancy safety factor than used in conventional telephone systems. In civilian practice--and all too often in the military--the assumption is made that only a very small proportion of the users will ever simultaneously demand service. However, in the military network, we must be more conservative--otherwise we invite overload during critical times. Therefore, from the standpoint of traditional practice, this system will appear to be grossly over-conservative in the value of peak-service capability.

Figure 6 is a block flow diagram of the major units comprising the Multiplexing Station. Each block is designated by letters for ease of identification.

Table 1 lists these major blocks and the approximate number of "equivalent flip-flops" necessary to perform the desired function. We may roughly assume about four transistors being required per equivalent flip-flop. The values shown in parentheses are for those units for which an inordinate amount of design would be required to make an accurate determination: the estimates shown are felt to be adequate approximations, inasmuch as we are interested only in gross orders of magnitude--not in specific details. The column labeled Heads indicates the number of read/write heads utilized on the common drum by each of the examined units.

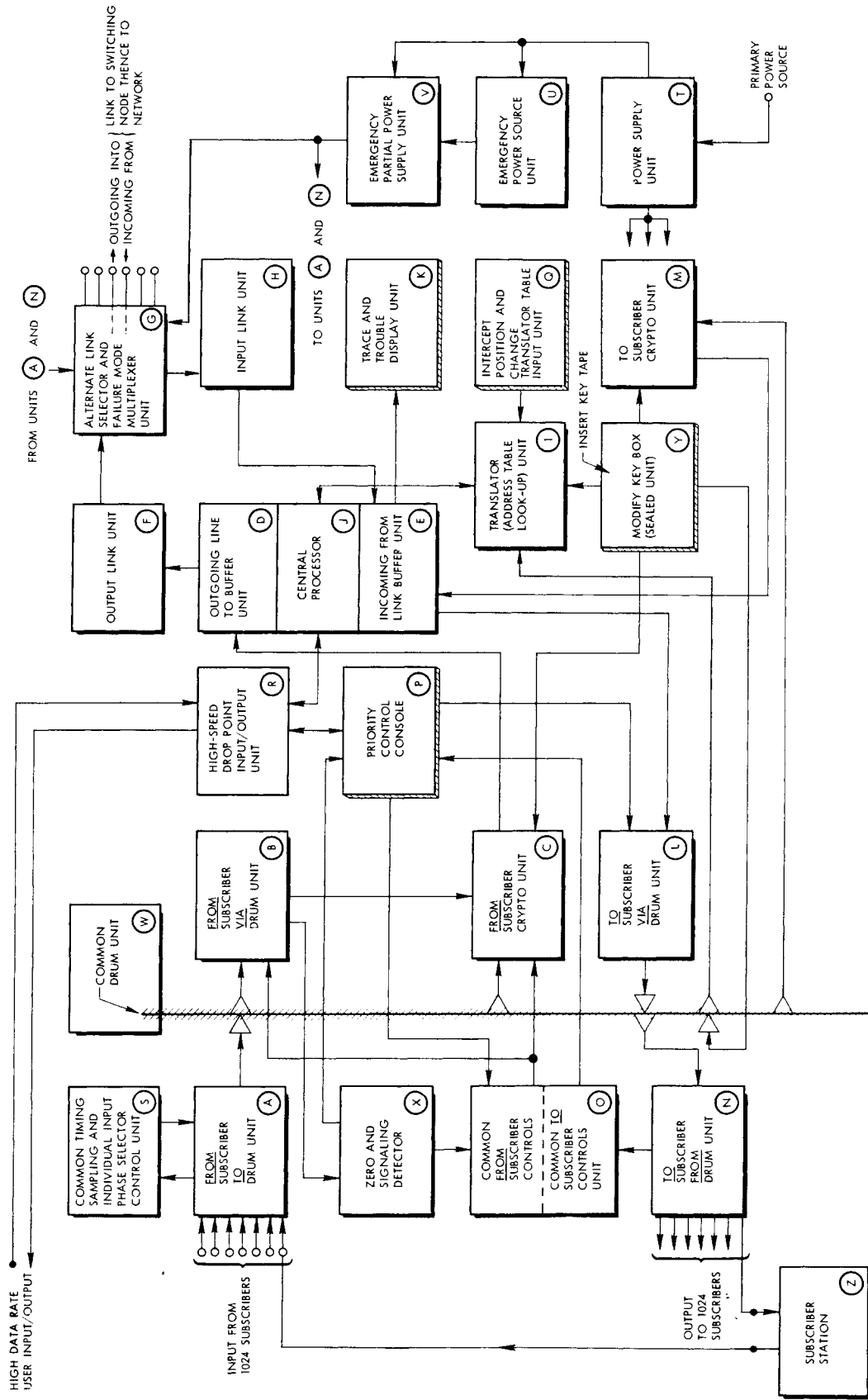


Fig. 6--Major Block Flow Diagram

Table I
EQUIPMENT BREAKDOWN FOR THE MULTIPLEXING STATION

Name		F/F [†]	Heads	Misc.
A	From Subscriber To Drum Unit	3707	96	
B	From Subscriber Via Drum Unit	(60) [*]	96	
C	From Subscriber Crypto Unit	(200)	96	
D	Outgoing Line to Buffer Unit	77	0	
E	Incoming From Link Buffer Unit	77	0	
F	Output Link Unit	106	0	
G	Alternate Link Selector and Failure Mode Multiplexer Unit	400	0	
H	Input Link Unit	123	0	
I	Translator (Address Table Look-Up) Unit	70	2	
J	Central Processor Unit	(600)	32	2000 32-bit words
K	Trace and Trouble Display Unit	(50)	2	
L	To Subscriber Via Drum Unit	(60)	96	
M	To Subscriber Crypto Unit	(200)	96	
N	To Subscriber From Drum Unit	1244	96	

Name		F/F [†]	Heads	Misc.
O	Common To/From Subscriber Controls Unit	(200)	0	
P	Priority Control Console	(50)	0	
Q	Intercept Position and Change Translator Table Input Unit	(70)	4	
R	High-Speed Drop Point Input/Output Unit	(80)	0	
S	Common Timing Sampling and Individual Input Phase Selector Control Unit	(70)	2	
T	Power Supply Unit	(30)	0	~2 kw power
U	Emergency Power Source Unit	(30)	0	~4 kw power
V	Emergency Partial Power Supply Unit	(30)	0	~200 watts
W	Common Drum Unit	(30)	0	1 Drum Unit*
X	Zero and Signaling Detector	(50)	0	256 words
Y	Modify Key Box (Sealed Unit)	(50)	2	1 7½ ips, 3" dia. tape unit*
Z	Subscriber Station	--	0	
Total		7664	400	

*See specifications in text.

[†]Equivalent Flip-Flops.

*Parentheses indicate very approximate estimate only.

GROSS DESCRIPTION

Unit A, FROM Subscriber TO Drum Unit

Unit A includes the input terminating equipment from 1024 separate subscriber lines. Strobed timing signals sample each of the incoming 1024 wave trains at a point near the center of each pulse interval time. The binary state ("0" or "1") for each subscriber's line is stored in a separate flip-flop. Each such flip-flop is unloaded in synchronism via a buffer flip-flop onto a common drum store controlled by a timing track on the drum. The output of Unit A feeds Unit B.

Unit B, FROM Subscriber VIA Drum Unit

Unit B examines the entire Message Block that has been stored on the drum during previous revolutions. Unit B contains filtering means which allow only active Message Blocks to be transmitted. Active Message Blocks are defined as those Message Blocks containing data or signaling--and not all zeros. The output of Unit B feeds Unit C.

Unit C, FROM Subscriber Crypto Unit

Unit C is a cryptographic subassembly unit having access to stored cryptographic keys on the common drum. This unit applies those cryptographic transformations necessary for processing active fully-formed Message Blocks for transmission into the system. Only when complete and valid Message Blocks are ready for transmission is the crypto storage in Unit C incremented to the next portion of key to be used for each line.

Unit D, Outgoing Line to Buffer Unit

Unit D provides the speed transformation means for the Message Blocks from Unit C. Message Blocks are held until

Unit J is ready to accept Message Blocks for further outgoing processing.

Unit J, Central Processor

Unit J is the heart of the Multiplexing Station and contains a high-speed random access memory. This memory is organized in the fashion of a small general-purpose computer for performing complex special operations, as well as for providing the timing flexibility needed between the high-speed synchronous timing of the network block, via the Switching Node links, and the local drum timing. This allows flexibility of the timing necessary for high-speed burst transmission. Units J and D work in conjunction with one another when transmitting the outgoing Message Blocks via Unit F.

Unit F, Output Link Unit

Unit F performs the parallel-to-series buffering into the Input Link Unit, H.

Unit G, Alternate Link Selector and Failure Mode Multiplexer Unit

Unit G is a switch to establish connection to alternate Switching Nodes in the event of a link or Switching Node failure. Unit G also connects the input from the Switching Node or nodes into Unit H.

Unit H, Input Link Unit

Unit H provides the link-by-link encryption devices used by the adjacent Switching Node and provides the link error detection encoding function. Unit H is almost identical in operation to a similar unit contained in the Switching Node and is described in ODC-VII.

Unit I, Translator (Address Table Look-Up) Unit

Unit I is used only when setting up new calls. Unit I converts the incoming called number into the latest correct address to be used for future traffic (Message Blocks). Thus, all Message Blocks are directly addressed to whichever line is presently assigned to the called party. Unit I works in conjunction with, and is controlled by, Unit J which provides control signals to allow the peripheral units of the system to operate in a semi-autonomous fashion. Such semi-autonomous peripheral units include Unit K.

Unit K, Trace and Trouble Display Unit

Unit K contains a 12-digit numeric printout device. This unit prints a tape similar to that used in a conventional electric adding machine, except that the tape material is translucent and preprinted. When an obviously incorrect Message Block or a Message Block "in trouble" (too old) is detected, it is transmitted via Unit J to Unit K. Here the trace portion of the Message Block, together with the to/from addresses, is printed on the adding machine tape. Use of translucent tape allows stacking individual defective trace patterns over one another so that a common fault-pattern can be easily detected, permitting the maintenance man to quickly isolate the source of trouble to within a particular Switching Node.

Unit L, TO Subscriber VIA Drum Unit

If the incoming Message Block is correctly received (passes all tests) it is transmitted via Unit J to Unit E. Units E and L are similar to Units B and D, their output counterparts. The output of Unit L is used by Unit N.

Unit N, TO Subscriber FROM Drum Unit

Unit N provides outputs to the 1024 subscribers at their exact synchronous data rates, with all housekeeping data stripped off.

Unit O, Common TO/FROM Subscriber Controls Unit

Unit O maintains an examination of the status of the subscribers and checks for proper operation of the line units. The use or non-use of each line is noted and is passed along to Unit P.

Unit P, Priority Control Console

Unit P performs the priority control functions useful in preventing overloads.* Unit P contains information as to which lines are actually in use transmitting traffic, and permits insertion of a variable control over the allocation of the communication resource. Unit P normally would be mounted adjacent to Unit Q.

Unit Q, Intercept Position and Change Translator
Table Input Unit

Unit Q is a manual operator intercept position and is the point where manual changes are entered onto the Translator Table, whenever it is necessary to change the address of a subscriber line.

Unit R, High-Speed Drop Point Input/Output Unit

Unit R is a buffer unit designed to process a very-high-speed local subscriber party line directly into the central processor, bypassing the common magnetic drum.

*See ODC-IV.

Unit R provides the buffering equipment to permit several party line users to connect into the Multiplexing Station. While such users would each operate at very-high-speed output data rates, their expected low duty cycles (operating in a highly intermittent fashion) would seem to permit satisfactory party line operation.

Unit S, Common Timing Sampling and Individual
Input Phase Selector Control Unit

Unit S provides the means to test all incoming subscriber lines against a four-phase clock to permit selection of that clock which falls closest to the center of the incoming pulse train, insuring that the incoming lines are strobed at or near the center of their individual input pulse train waveforms regardless of the total amount of phase shift on the lines to remote devices. Unit S measures and compensates for variable phase delay between the transmitted waveform to subscribers and the waveform based upon reconstructed timing from the subscriber back into Unit A of the Multiplexing Station.

Unit T, Power Supply Unit

Unit T provides all proper regulated voltages for operating the individual transistorized units of the Multiplexing Station.

Unit U, Emergency Power Source Unit

Unit U is a standby power source and provides primary power in the event of power failure. The total amount of power required for transistorized equipment is invariably low; probably more power is used by the magnetic drum than all the remaining electronic equipment. Thus, a few kilo-

watts of emergency power will suffice. Batteries or perhaps a fuel cell (if economically feasible) would also provide a suitable backup power source. Even a simple gasoline engine and alternator of the type selling for a few hundred dollars would do as a double backup.

Unit V, Emergency Partial Power Supply Unit

In the event of a failure of the primary power supply, Unit V provides power to the most critical units and lines of the Multiplexing Station. During such a failure, it may be possible to interlace-multiplex important subscribers' signals using neither the drum nor most of the other units comprising the system. Such a simple time-division multiplexed signal could be transmitted via the Link Units to an adjacent Multiplexing Station for necessary processing. Such a fallback procedure would only be used as a last-ditch emergency measure. The chief objection to this procedure is that only a small portion of the subscribers can be handled and even these would temporarily lose normal end-to-end crypto facilities. However, since link-by-link encryption would still be available on the signals for subscribers feeding to the remote Multiplexing Station for processing, this may be sufficient to safely permit highly classified conversations in emergencies.

Unit W, Common Drum Unit

A storage of nearly 13 million bits is required in the system, most of it provided by Unit W, a single large drum having four hundred heads. Timing tracks of the common drum will establish the timing base for all locally connected subscribers. Although a drum is tentatively suggested as the heart of Unit W, the computer state-of-the-art has advanced sufficiently so that the alternative use

of high-capacity acoustical delay lines would eliminate the dependence upon a single, large, rotating component. (A good part of the power required by the entire system is consumed by the drum motor and many circuit elements are necessary to compensate for the pulse jitter caused by the drum.) Splitting the drum into a series of smaller Bernoulli discs would simplify fracturing the system into many identical units, a more desirable alternative for continuity of service in spite of the increase in the probability of individual subunit failures.

Unit X, Zero and Signaling Detector

Unit X, in conjunction with Unit A, performs the high-speed scanning operation to examine all input subscriber lines and ignore those that had nothing to say (all zeros) during the last Message Block frame time (about 1/20 sec in the case of 19.2-kilobit/sec digital voice). Unit X also performs the operation of spotting and separating the signaling information from active data transmitted.

DETAILED DESCRIPTION

We have briefly reviewed the key operations performed within each of the major blocks of the system, and shall now examine the operations and constructions of each unit in further detail. While a full description of each unit is desirable, such a writeup would become voluminous. Therefore, separate block diagrams are provided for only the least conventional of the major units and those most difficult to visualize. The reader is left to his own devices to fill in the unspecified minutiae.

Operation of FROM Subscriber TO Drum Unit, A

At the extreme left of this drum are the 1024 separate lines each feeding its respective line input unit. Each

bank of 32 line units is time-shared by a separate 32-input switch concentrating the sampled waveform onto a single output channel. All 1024 separate line input units have been previously sampled in Unit S by a common time-sampling circuit. Unit S examines each line every few seconds, searching for a slow drift of the arriving waveform from the subscriber. This long interval between samples is felt to be permissible because of the expected slow-drift-rate nature of the phase shift variation in the input lines from the subscribers. By using Unit S, we may choose one out of the four timing strobe phases per pulse. The specific phase chosen is that which falls closest to the center of the incoming pulse train. A temporary storage flip-flop in each line input unit permits an offset of the strobe point necessary for rephasing to match the timing constraint of the drum. Each bank of 32 lines concentrated by the 32-input switches is connected to a single drum amplifier. The output of this amplifier drives write heads on the drum connected in series to a small bank of magnetic cores. These cores are used to indicate whether signaling or data is being transmitted (by means which shall be described later). The output of each drum amplifier is distributed by a three-way switch to permit sequentially writing on three drum heads. This permits inputs to be written on one bank of heads while the second bank is being read out. Unit A thus provides the multiplexing equipment to concentrate 1024 separate units onto 96 different drum bands.

Composition of Inputs

Table II shows an assumed composition of 1024 inputs used in designing the described Multiplexing Station. This particular system can handle, for example, 128 lines, each operating at 19.2 kilobits/sec, which might be digital

Table II
COMPOSITION OF INPUTS

Number of Input/Output Lines	Data Rate, Bits/Sec	No. Drum Revolutions	No. Drum Amplifiers
128	19,200	1	4
128	9,600	2	2
256	2,400	8	1
512	600	32	1
<div>128 x 19,200 + 128 x 9,600 + 256 x 2,400 + 512 x 600</div> <div>Peak Input Data Rate = 4,608,000 bits/sec</div>			

telephones; plus, 128 lines at 9600 bits/sec, which could be high-speed facsimile; plus, 256 lines of 2400-bit/sec circuits, which might be vocoder type digital voice or digital data; and lastly, the system will also simultaneously handle 512 lines, each operating at 600 bits/sec, which could be used for high-speed synchronous data, and/or output of conventional teletype equipments. Table II also indicates that if the drum size is chosen so as to complete a single revolution to store 1024 bits, comprising a Message Block of which 866 bits are active information, at 19,200 bits/sec, then two drum revolutions will be required for the 9600-bit/sec channels and 32 revolutions for the low-speed 600-bit/sec data. The last column of Table II shows that the number of drum amplifiers needed can be reduced by using a single drum amplifier together with an additional layer of switching to further time-share-concentrate the lower-bit-rate channels. Thus, instead of 32 drum amplifiers

being required in the arrangement of Fig. 7, only eight drum amplifiers need be used by this additional time sharing. (The component count of Unit A was based on 32 drum-amplifier channels, while many of the subsequently considered units have been limited to the assumption of only ten separate channels.)

It is to be noted that under the assumptions of Table II, the peak input data rate is in excess of 4.5 million bits, about three times greater than the allowable peak output rate over a single 1.5-megabit/sec link.

The ratio between peak input- and output-limited rates is extremely conservative, as the probability of exceeding this output value, even when the bulk of the lines are in use, is statistically a rare event. Even in the event a peak load is experienced in which the number of input devices have an accumulative output data rate in excess of the allowable output rate, overloads will be handled by automatic priority assignment equipment built into the system (Unit P).

Input Strobing

Figure 8 details what happens to the subscriber's input waveform arriving at the individual line units. P1 through P4 are possible input strobing positions. The incoming time wave, regardless of its relative phase to the local timing system, is sampled near the center of each pulse position and a new wave is created at the input rate in synchronism with the drum timing.

Figure 9 shows the line input unit in more detail; its operations are self-evident.

Figure 10 shows a sketch of a 32-input/1-output switch, in order to provide an approximation of the number of components that will be required to implement gates of this type.

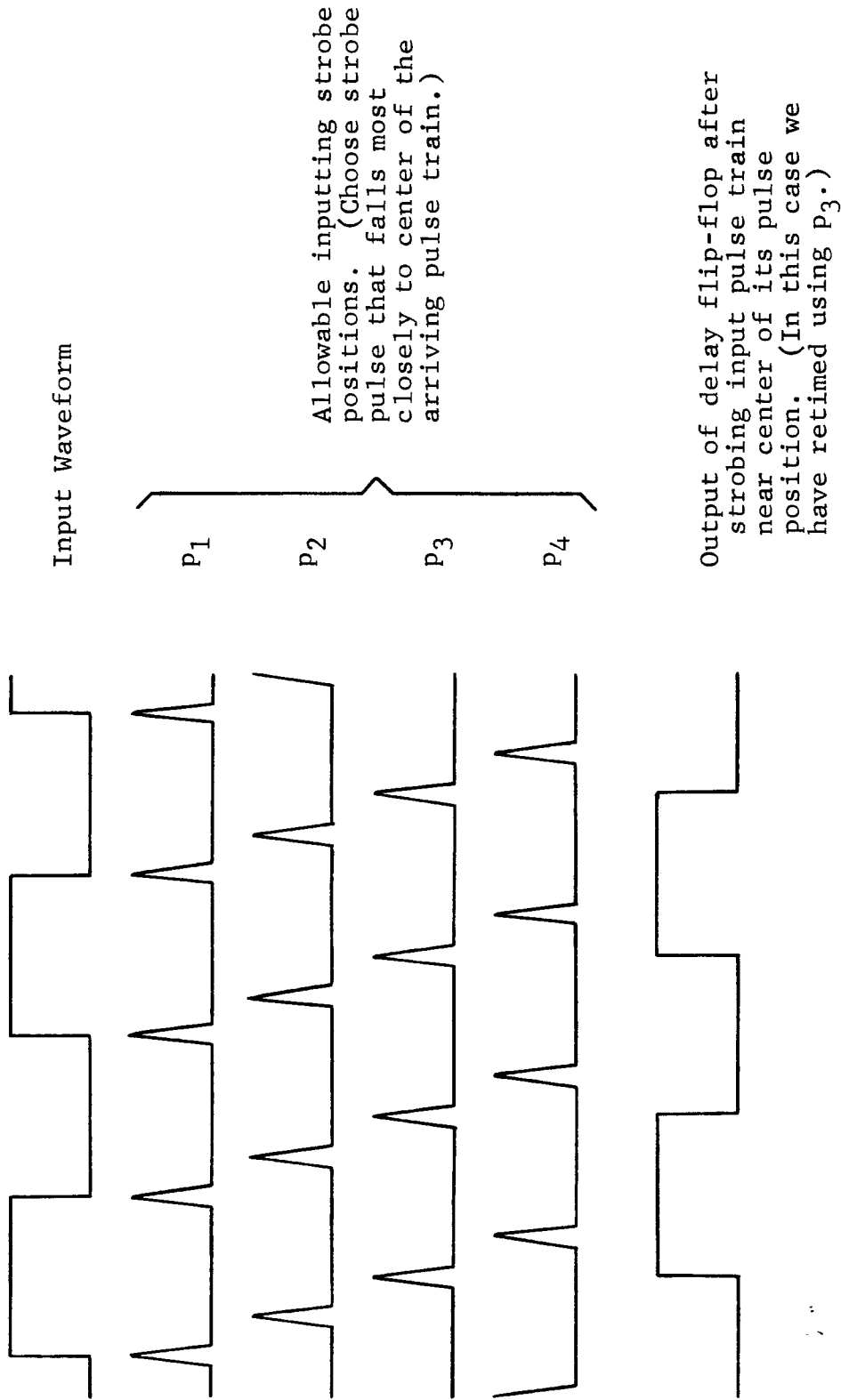


Fig. 8--Multiphase Strobe Timing at the Line Input Buffer Unit

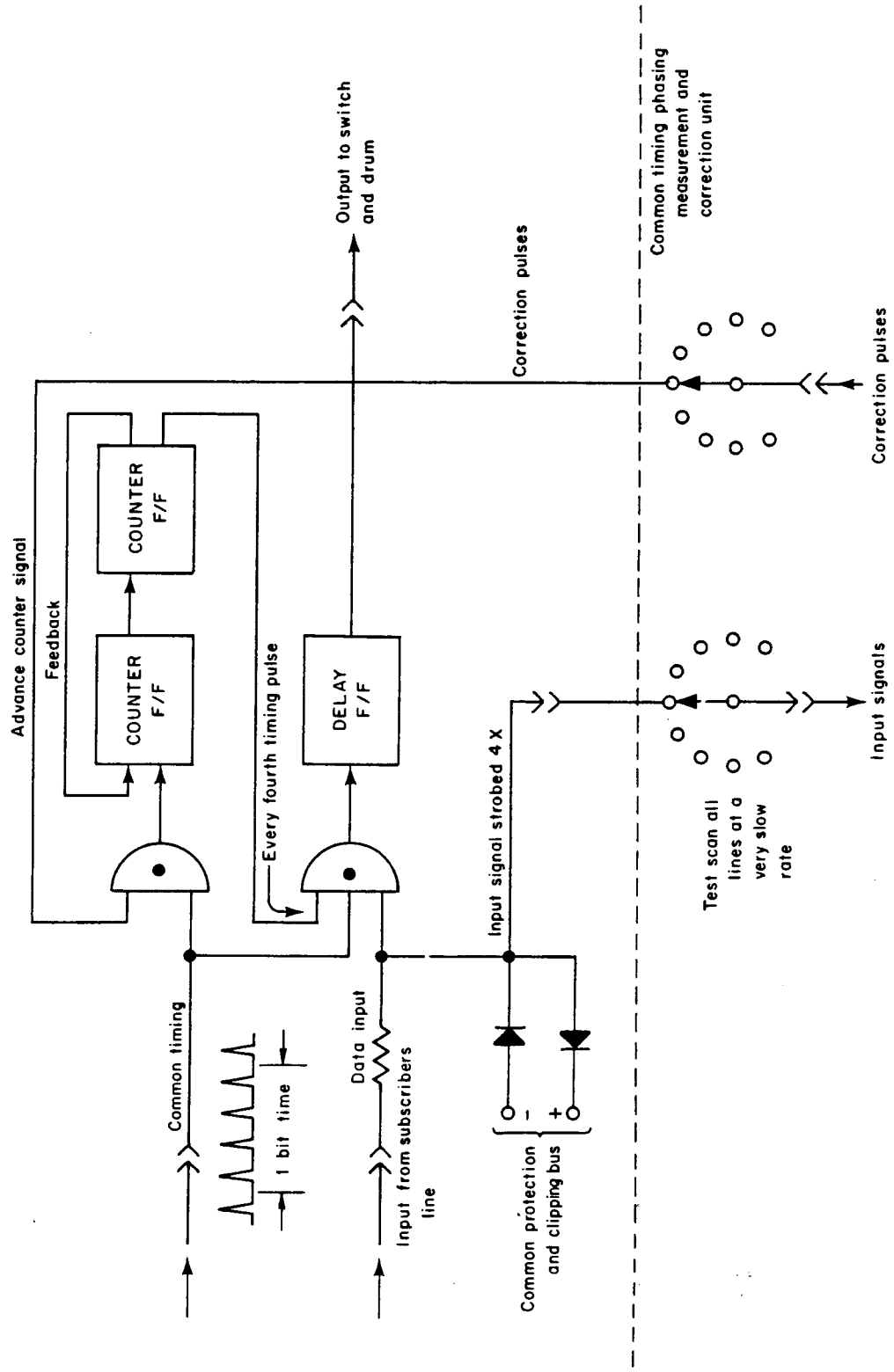


Fig. 9--Line Input Unit

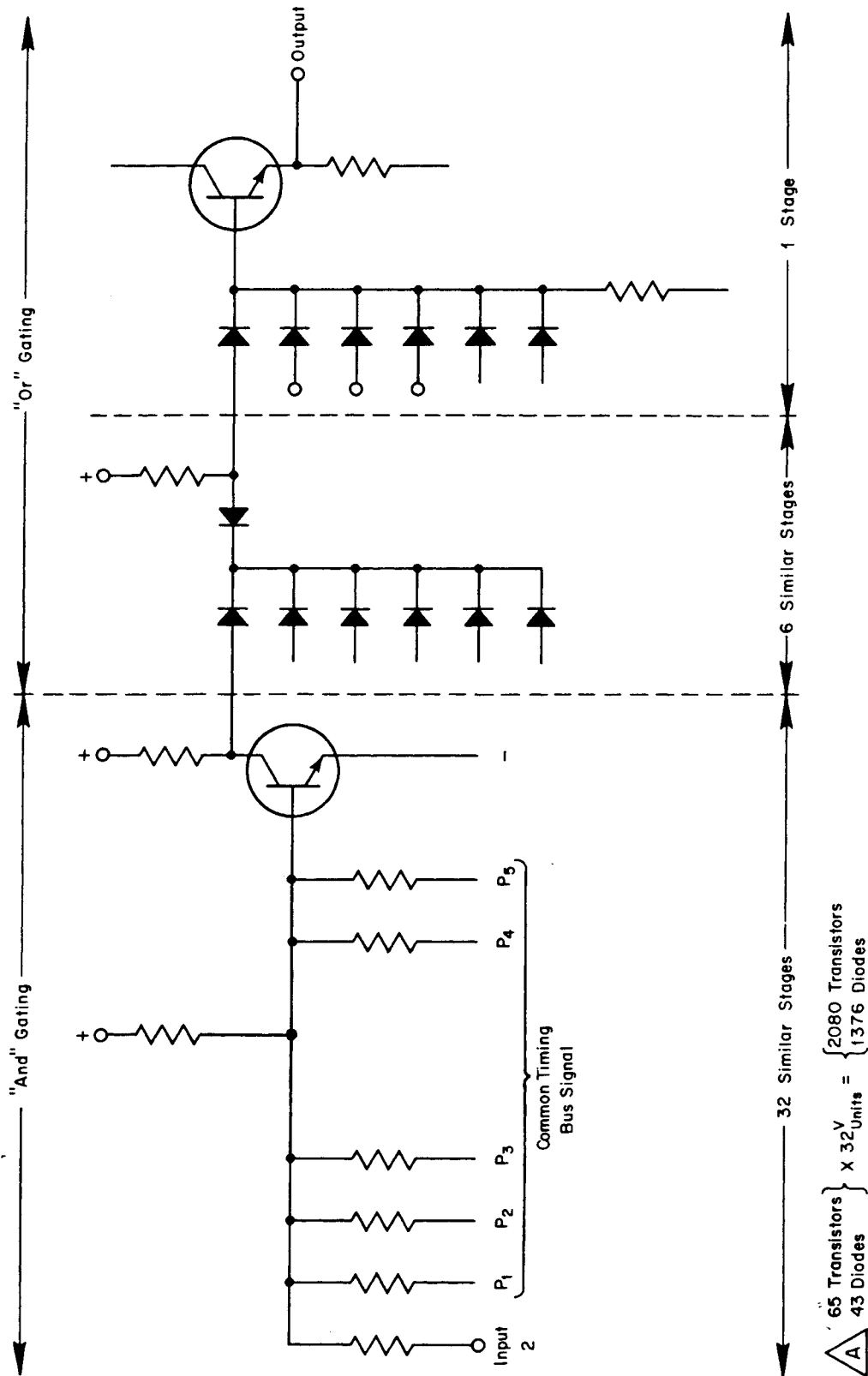


Fig. 10--32-Input/1-Output Switch

Figure 11 is a brief sketch of the 1-input/32-output switch, also providing a rough estimate of the number of parts needed.

The Crypto Scheme

A possible end-to-end cryptographic secrecy system that might be used in the system is shown in Fig. 12,* illustrating the principle of the proposed crypto scheme. Essentially a newly modified key base is created for each new call. (The actual method of developing this key base when setting up each new call is fully described in ODC-IX).

The system is primed each day or so with a set of start keys assigned to pairs of stations. These are modified after each call. The key base sequence used for each call is "logically-added" to the incoming and outgoing text. The output of this "logical-add" circuit is the encrypted transmitted text. The text is also combined with the last section of the key streams and used as part of the generator function for creating the next portion of the key stream. Thus, the modified key is a function both of the initial key base and of the text being transmitted. This, in essence, is a combination of the auto-key principle and the pseudo-random stream approach.†

The receiving decryption equipment is identical with that used in transmission. In order to obtain error-free

*It should be emphasized that the entire discussion on crypto is merely for illustrative purposes, included only to round out the system description. If, and when, it becomes necessary to precisely determine a form of cryptography for use in conjunction with this system, it will be done by the proper agencies. Such decisions reside outside the purview of responsibility, interest, and information available to this writer (see ODC-IX).

†Shannon, C. E., "Communications Theory of Secrecy Systems," Bell System Tech. J., November 1949, pp. 656-715.

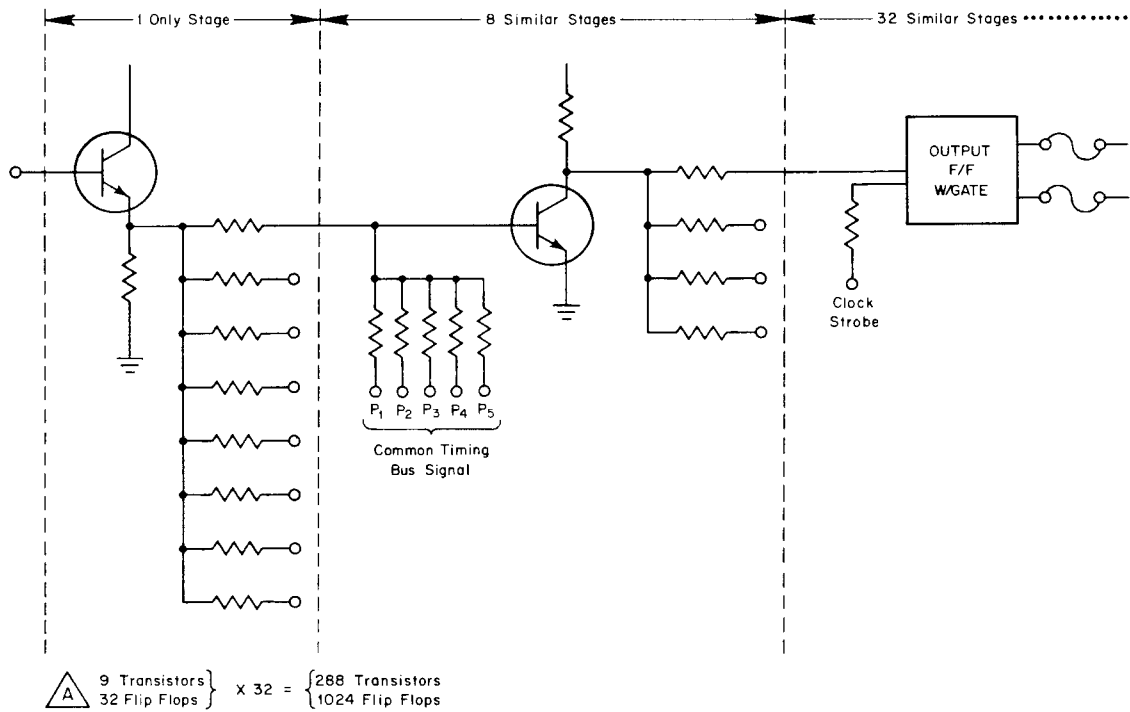


Fig. 11--1-Input/32-Output Switch

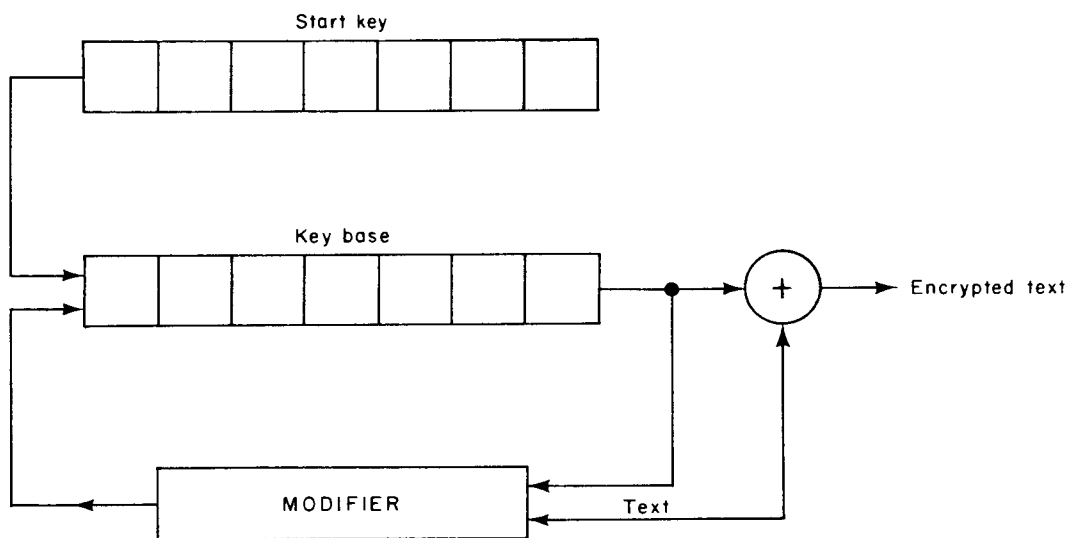


Fig. 12--Principle of Crypto Scheme

decryption, we have purposely made it mandatory that no errors appear in the series of Message Blocks received by the receiving Multiplexing Station. It will be remembered that one of the most important fundamental properties of this proposed network is its extremely low error rate. Thus, this cryptographic procedure appears to be usable in the proposed system while not appropriate to conventional communications systems.

Figure 13 exhibits the receiving decryption apparatus in more detail. The round ring bands at the right of the illustration are intended to represent drum bands on the common magnetic drum of the Multiplexing Station. The third drum band would contain the incoming encrypted text, timed out to pass by in synchronism with the clear text of the last Message Block received. The box within the dotted lines represents the circuit which modifies the next key block. Six separate drum bands are required for these cryptographic operations because of our desire never to read and to write on the same drum band at the same time. (This would have required accurately spaced read and write heads.) Thus, we write on three heads while simultaneously reading three heads. At the end of a drum band revolution, we switch and read the three previously written drum bands, etc.

Operation of FROM Subscriber VIA Drum Unit, B

Figure 14 shows in more detail the operation of the From Subscriber Via Drum Unit. The output from the 96 read-write heads from the subscriber inputs are selected by switches; read is by drum-read amplifiers and logical addition is performed by the crypto key. Here, the signals from various subscribers' lines are read off the common drum in synchronism with the crypto key to form outgoing encrypted text.

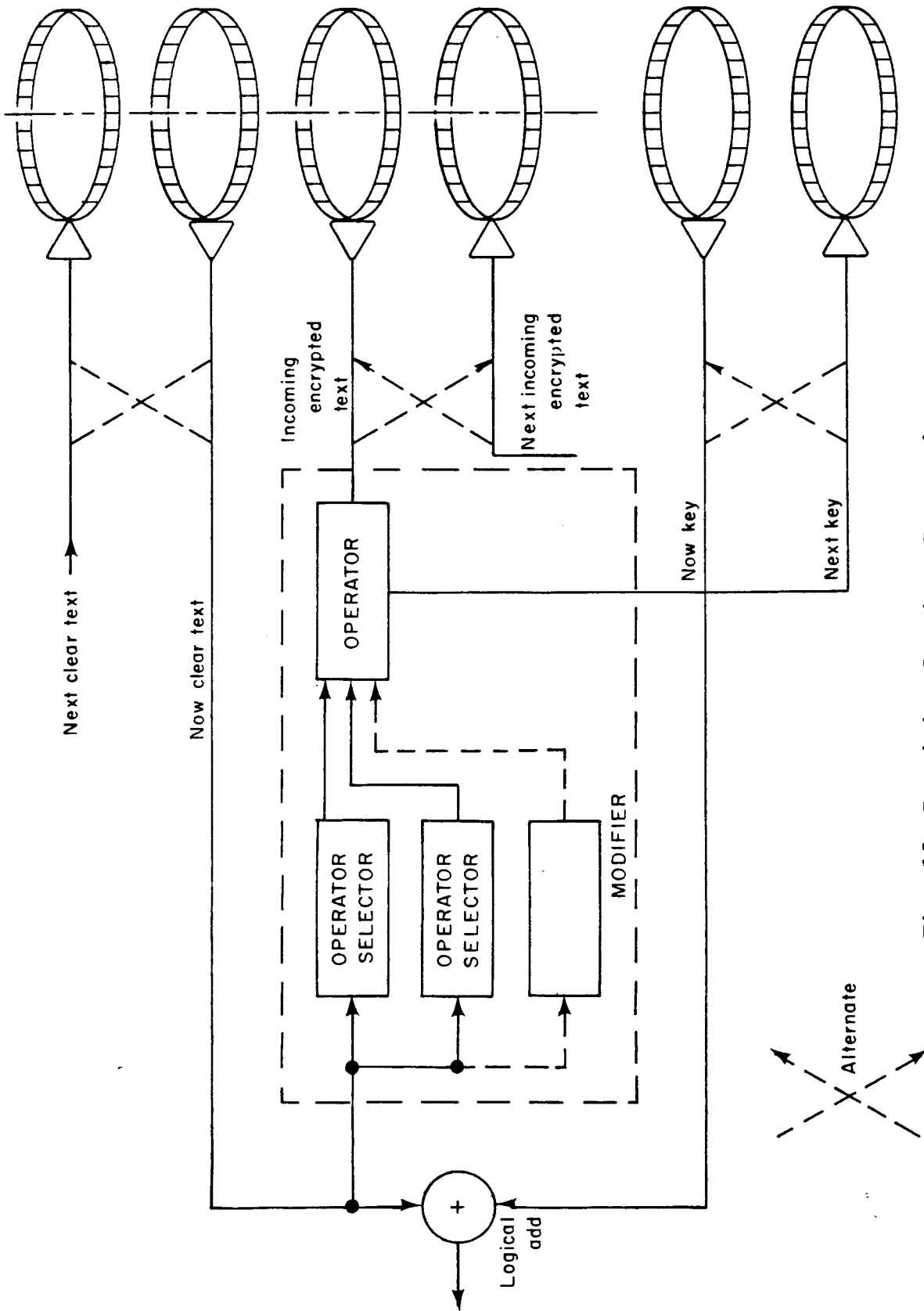


Fig. 13--Receiving Section, Decryption

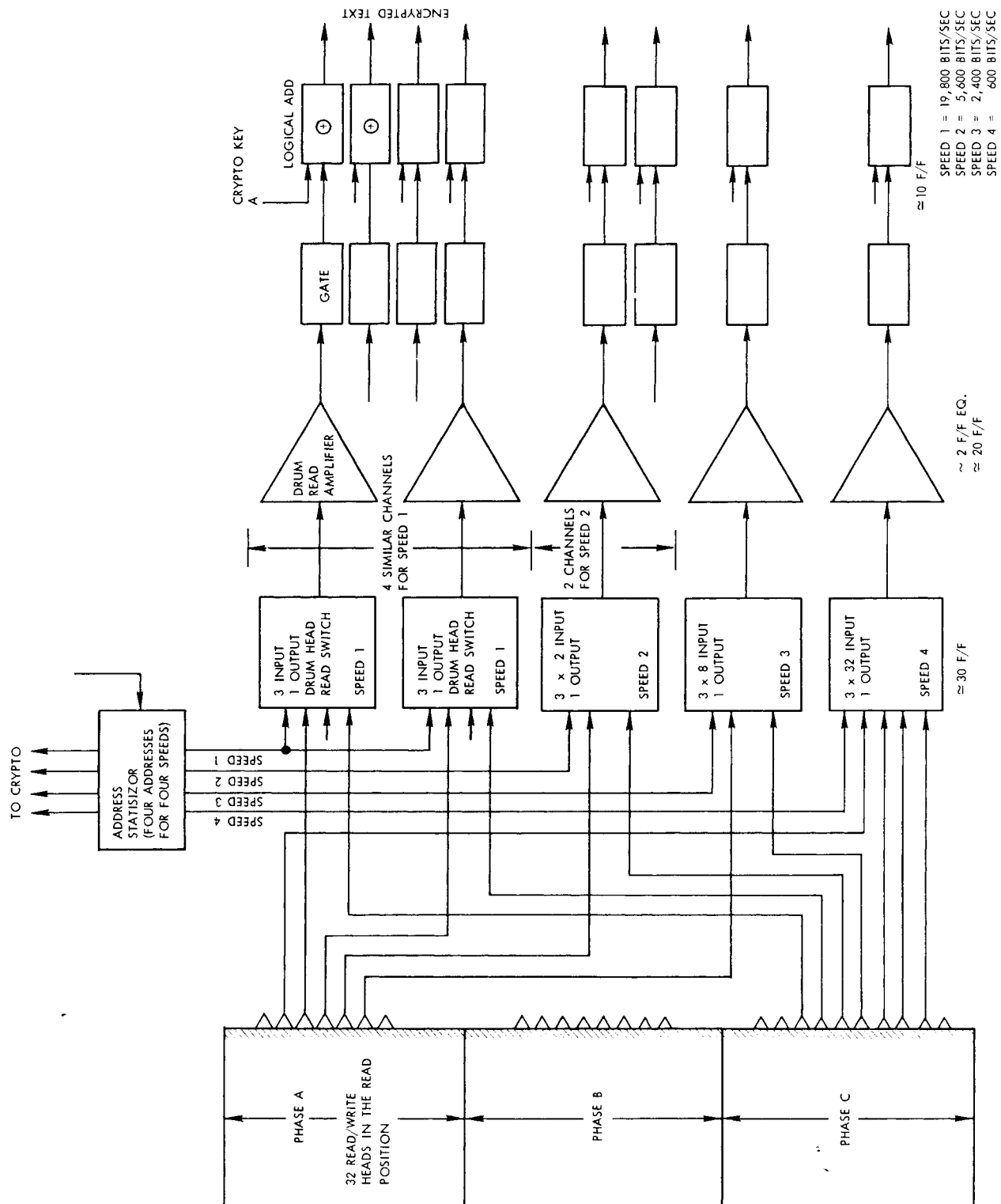


Fig. 14--From Subscriber Via Drum Unit

Operation of FROM Subscriber Crypto Unit, C

Thirty-two read-write heads shown in the read position at the extreme left of Fig. 15 feed ten head switches. The outputs of these switches are connected to drum-read amplifiers. These circuits provide access to previous key information stored in the drum. This allows the incoming text to be combined in a key modifier circuit within Unit C, the output of which is sent to drum-write amplifiers which, in turn, lay down the newly modified key on the drum slot reserved for the next Message Block key. Only ten separate drum-read amplifiers and modification circuits are necessary, as has been mentioned, as the drum revolves many times to process the low-data-rate channels, permitting time-sharing of the read amplifiers to cover many separate drum tracks.

Operation of Buffer Units, D, E; and Input/Output Link Units, F, H

Figures 16, 17, and 18 are essentially the identical circuits of the Buffer Units and the Input and Output Link Units contained within the Switching Nodes. As these units have already been described in detail in ODC-VII, no more will be said about them here.

Operation of Alternate Link Selector and Failure Mode Multiplexer Unit, G

The Alternate Link Selector and Failure Mode Multiplexer is an emergency-use-only unit providing some residual capabilities in the event of failure of the entire Multiplexing Station or of the links to the Switching Node from the Multiplexing Station. Unit G provides an emergency residual capacity, but only at a price of a loss of traffic handling and security capability. In Fig. 19, the output of the Link Unit is connected to a mechanical three-position

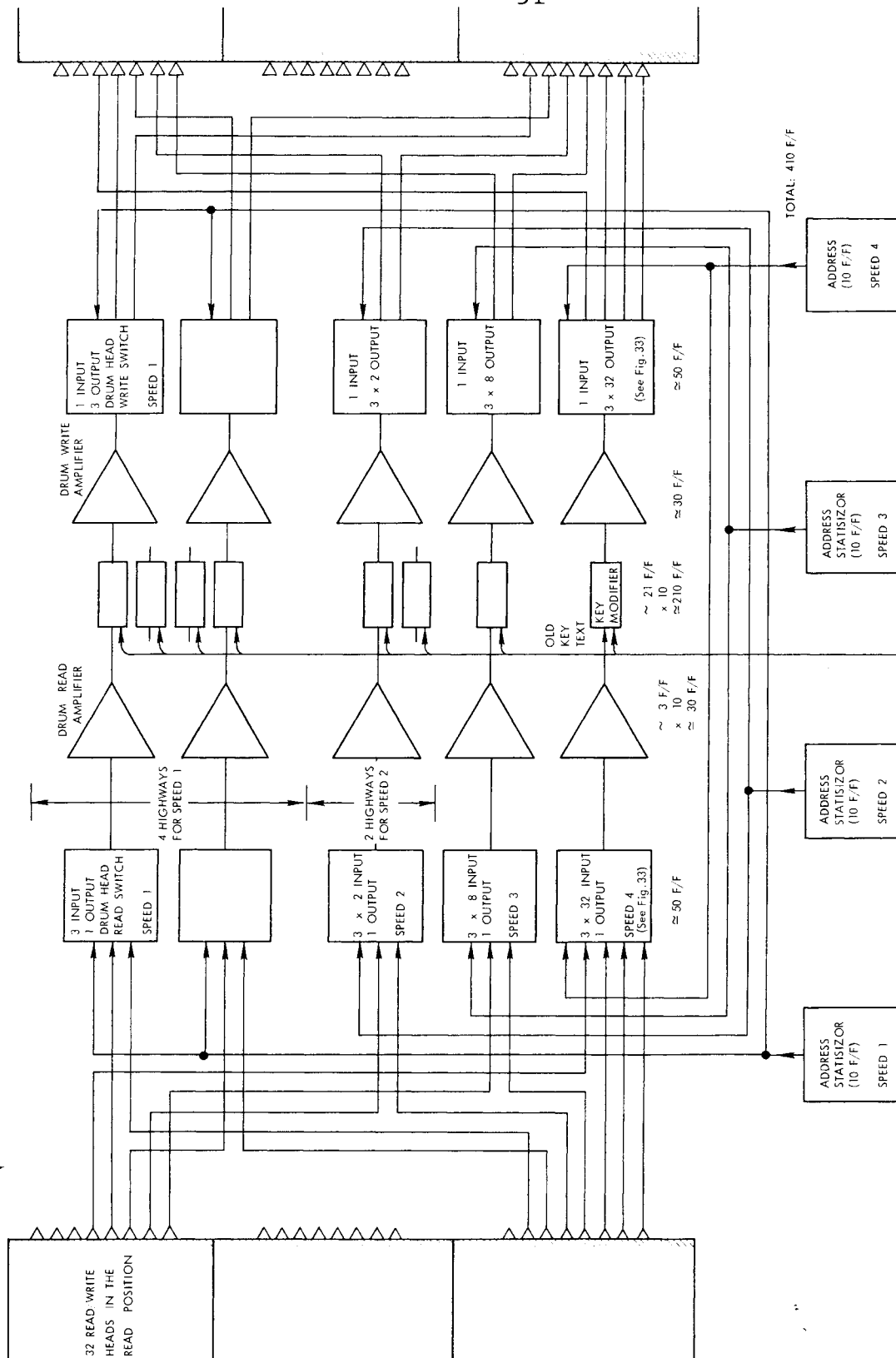


Fig. 15--From Subscriber Crypto Unit

switch connecting to alternate Switching Nodes. In the event of the failure of one of the outgoing links, a new manual connection can be selected. The output stream from the input link unit, which we have assumed to operate at a data rate of 1.5 megabits/sec, is divided by two to produce a 720-kilobit/sec stream. This continuous pulse pattern is used to create new timing in lieu of the timing derived from the drum (in the event of a failure in a drum or similar major component).

Since four samples are required per pulse received from a subscriber at the line unit, the number of channels that may be handled by such a procedure is greatly reduced. For example, instead of handling 1024 channels, capacity is reduced to about 172 channels, of which 128 lines may operate at 600 bits/sec, 32 at 2400 bits/sec, 8 at 9600 bits/sec, and 4 at 19.2 kilobits/sec.

Table III shows the series of standard $75(2^n)$ -bit/sec digital communications speeds.

In retrospect, it appears that we would be better off to standardize data rates for the high-speed Switching Node links at integral speeds, rather than the tentative 1.54-megabit/sec speed mentioned in other volumes in this series. The nearest two such speeds would be 1.2288 megabits/sec and 2.4576 megabits/sec. If we should so standardize, again in retrospect, we could probably simplify the equipment within the Switching Node by limiting the choice of data rates to these mentioned here. Such a standardization would have simplified the design of the emergency Alternate Link Selector and Failure Mode Multiplexer Unit. Better yet, it is appropriate to reconsider the entire system design and the potential savings if the system were to operate only at these fixed speeds, rather than allow for the infinite range of speeds that has been suggested in the previous volumes in this series.

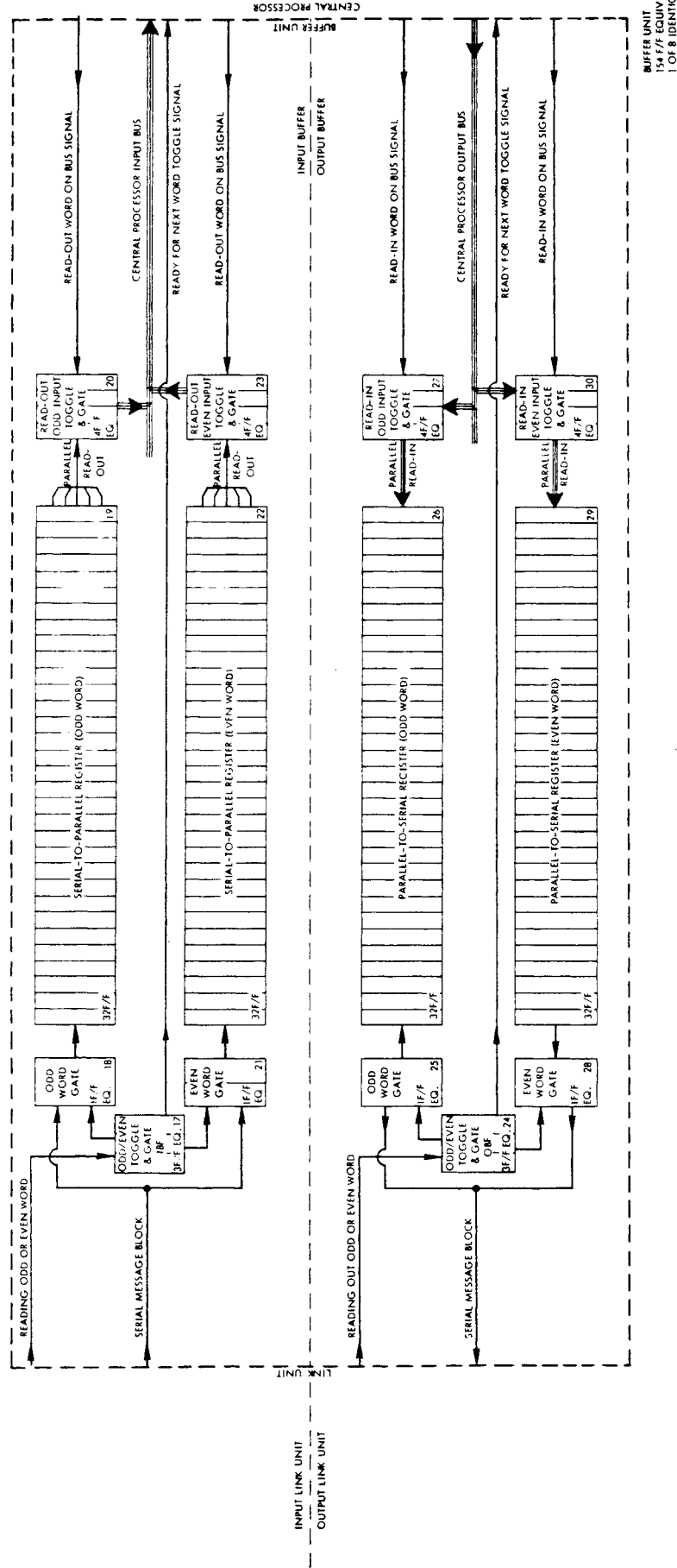


Fig. 16--Buffer Unit

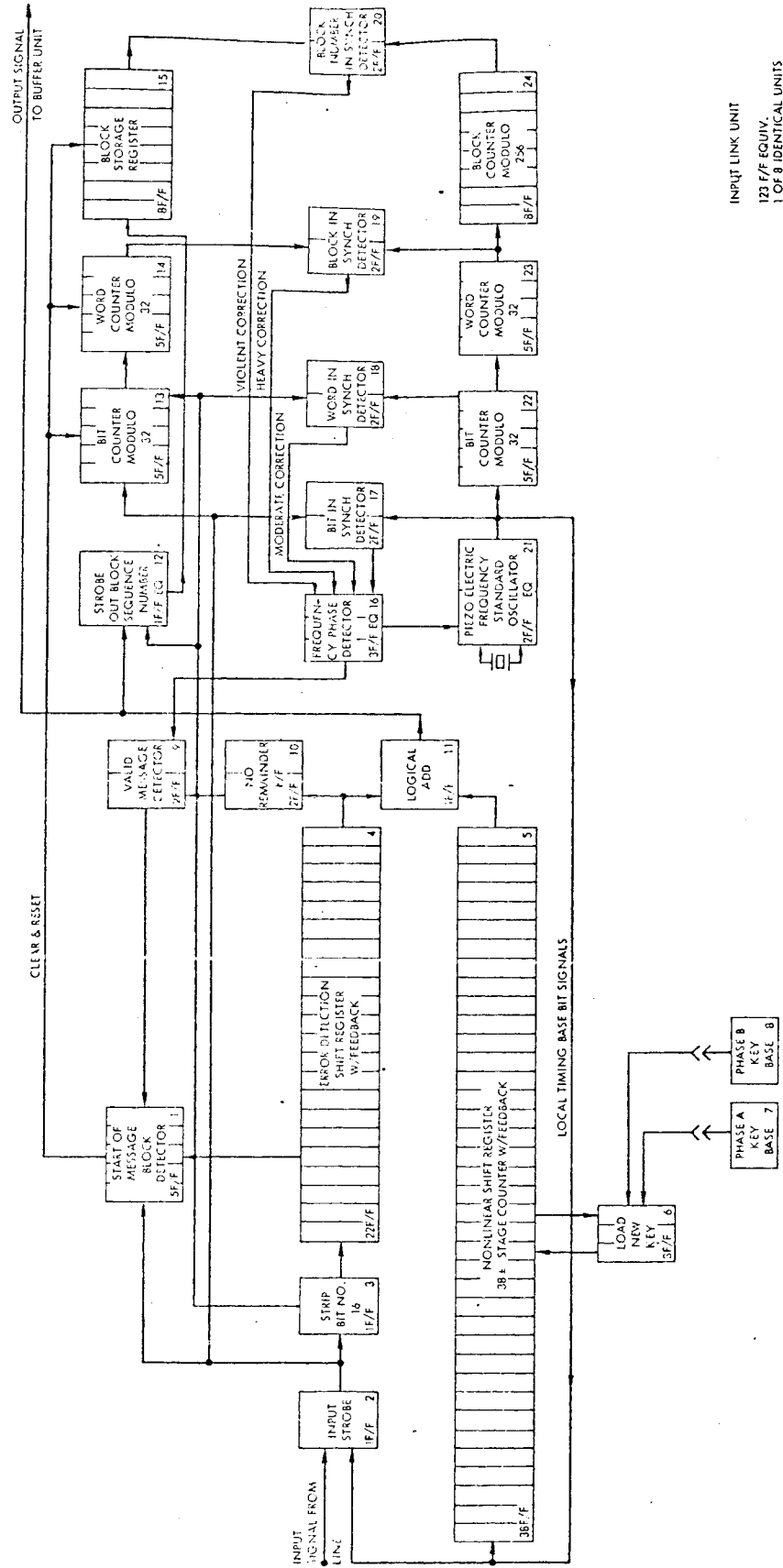


Fig. 17--Input Link Unit

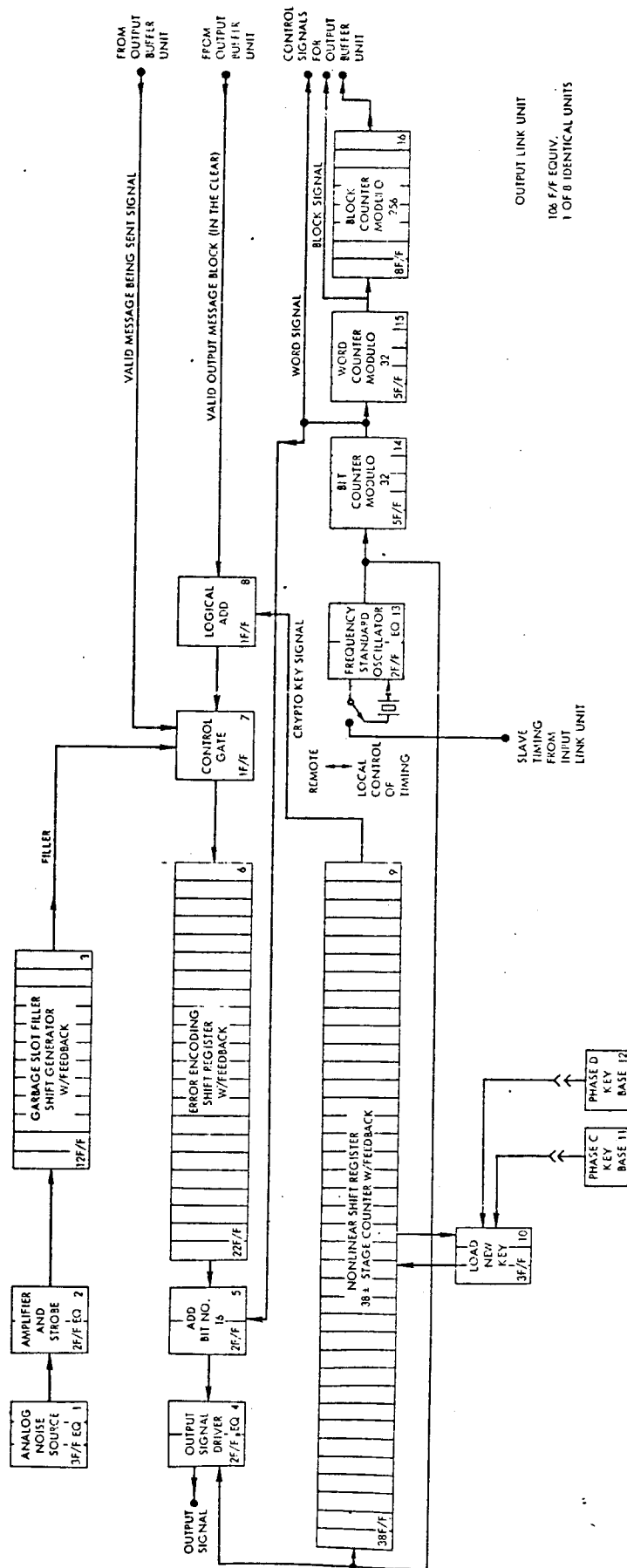


Fig. 18--Output Link Unit

Table III
STANDARD SPEEDS

Bits/sec	N	2^K	K
75	1	1	0
150	2	2	1
300	3	4	2
600	4	8	3
1,200	5	16	4
2,400	6	32	5
4,800	7	64	6
9,600	8	128	7
19,200	9	256	8
38,400	10	512	9
76,800	11	1,024	10
153,600	12	2,048	11
307,200	13	4,096	12
614,400	14	8,152	13
1,228,800	15	16,384	14
2,457,600	16	32,768	15
4,915,200	17	65,536	16
9,820,400	18	121,072	17

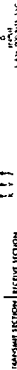


Fig. 19--Alternate Link Selector and Failure Mode Multiplexer Unit

Operation of Input Link Unit, H

As Unit H is identical with that used in the Switching Node, it will not be described in detail here other than to include the circuit of Fig. 17 (p. 54).

Operation of Translator (Address Table Look-Up) Unit, I

Figure 20 is a schematic view of the Translator Table mechanism. Two tracks of the common drum unit are reserved to store alternate "telephone" numbers for all network users. This unit is fundamentally a simple table look-up device. When setting up a new call, this table is examined to convert the called number into the actual office number and line number currently being used by the called number. (The system also has facilities for inserting alternate numbers if the called person is not at his designated extension.)

Housekeeping data is also stored to: indicate when the alternate number may be used; indicate whether the alternate number is a local or a remote station; indicate whether the actual number is classified; and determine the level of urgency of an incoming call before transferring it to an alternate number.

Information updating the Translator Table is stored in a temporary flip-flop register and read out into its proper place on the drum by the equipment shown in Fig. 20.

Operations Performed in the Process of Setting up a Call

Figure 21 shows some major operations performed when setting up a new call between two network users. The sequence of operations starts from the calling subscriber, passes through the calling terminal station to the called

terminal station, and eventually reaches the called subscriber. These operations are self-explanatory.

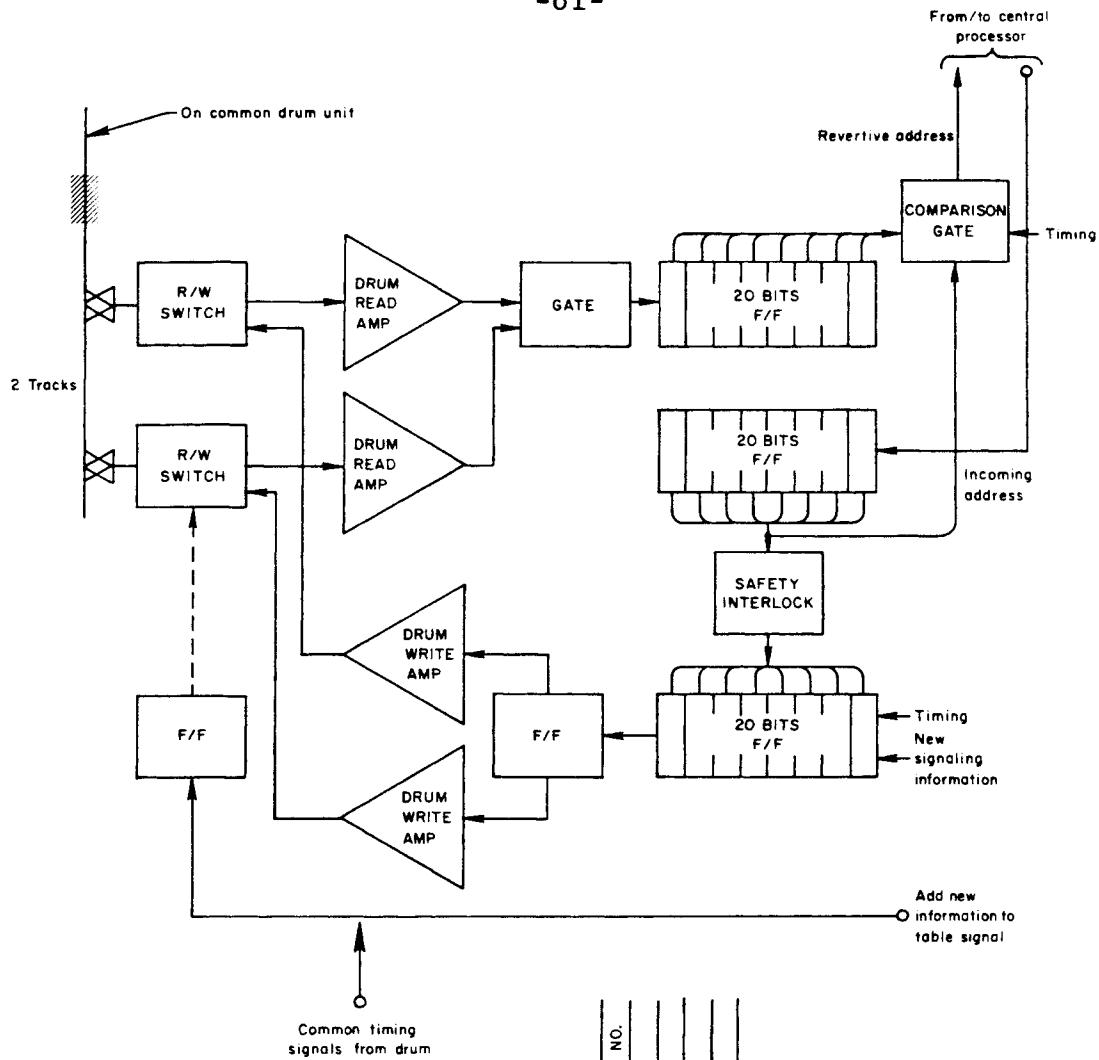
Creating Signaling Tones by the Use of a Repeating Digital Sequence

Inasmuch as the system is all-digital, it is desirable to have simple devices to convert digital streams into signals which can be expeditiously analyzed by inexpensive end-terminal devices (such as telephones). Below is a suggested procedure.

All signals are in the form of a continuous repetitive digital waveform, selected so that a Fourier analysis of the tone will result in a small set of fixed frequencies of known amplitude relationships. For example, a 2400-bit/sec square wave tone passed through a band pass filter will produce a strong fundamental tone at 2400 cycles, with tones one-third as strong at 3×2400 and one-fifth as strong at 5×2400 cycles. A series of five digital patterns are shown in Fig. 22, each of which can be transmitted on an all-digital line and be readily distinguished and interpreted by a simple band pass filter bank. Simple analog detectors, therefore, are capable of analyzing a digital signaling signal into signals suitable for operating switches to insert ringing signals, busy signals, etc., at the end-device.

High-Speed-Core Housekeeping Operations Upon Message Blocks Newly Arriving at the Terminal Line Distributor

Figure 23 is a simplified flow chart of operations performed within the high-speed core, such as unpacking newly arriving Message Blocks. The details of the operation can be easily gleaned from the flow chart.



IF THIS NUMBER IS DIALED		TRANSLATE INTO THIS NUMBER		OK TO USE ALTERNATE NO.	LOCAL/REMOTE	CLASSIFICATION	URGENCY	SPARE(S)	ALTERNATE NUMBER	
PREFIX	BASE	OFFICE NUMBER	LINE NUMBER						PREFIX	BASE
0 0 3 1	0 0 0 1	0 0 3 1	0 0 0 1	1 0					0 0 3 1	0 1 2 1
0 0 3 1	0 1 2 1	0 0 3 1	0 0 0 2	0					0 0 3 1	0 1 2 1
0 0 3 1	0 3 1 0	0 0 3 1	0 0 0 4	0					0 0 3 1	0 0 1 0
0 0 3 1	0 5 2 1	1 1 0 5	0 0 0 2	0						
0 0 3 1	0 0 1 1	0 0 3 1	0 0 3 0							
0 0 7 7	0 0 1 1	0 0 3 1	0 0 0 5							
0 0 7 7	0 1 2 1	0 7 7 0	0 0 0 0							
1 0 7 7	0 1 2 0	0 7 7 0	0 1 2 0							

Fig. 20--Translator (Address Table Look-Up) Unit

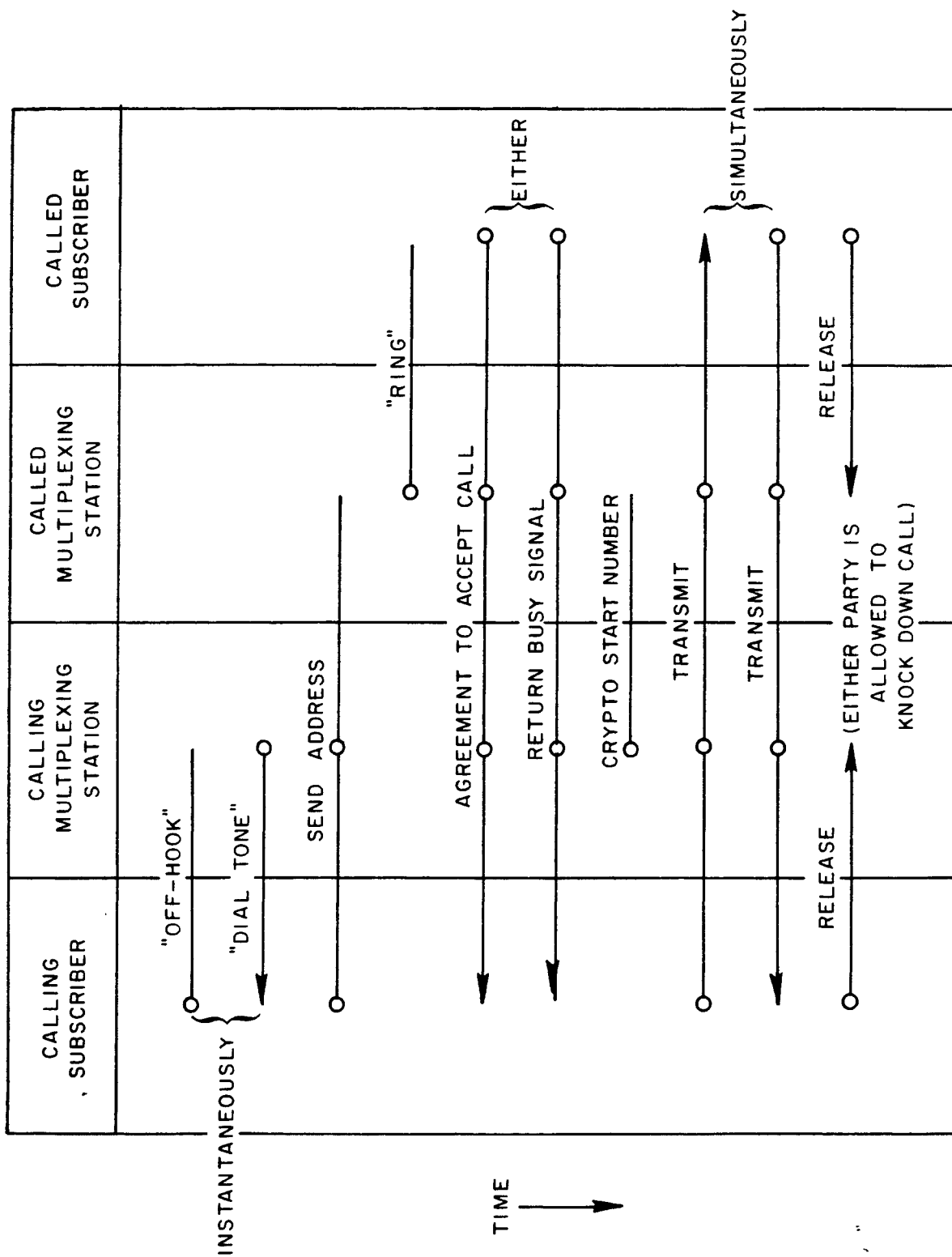


Fig. 21--Operations Performed in Setting Up a Call Between Network Users

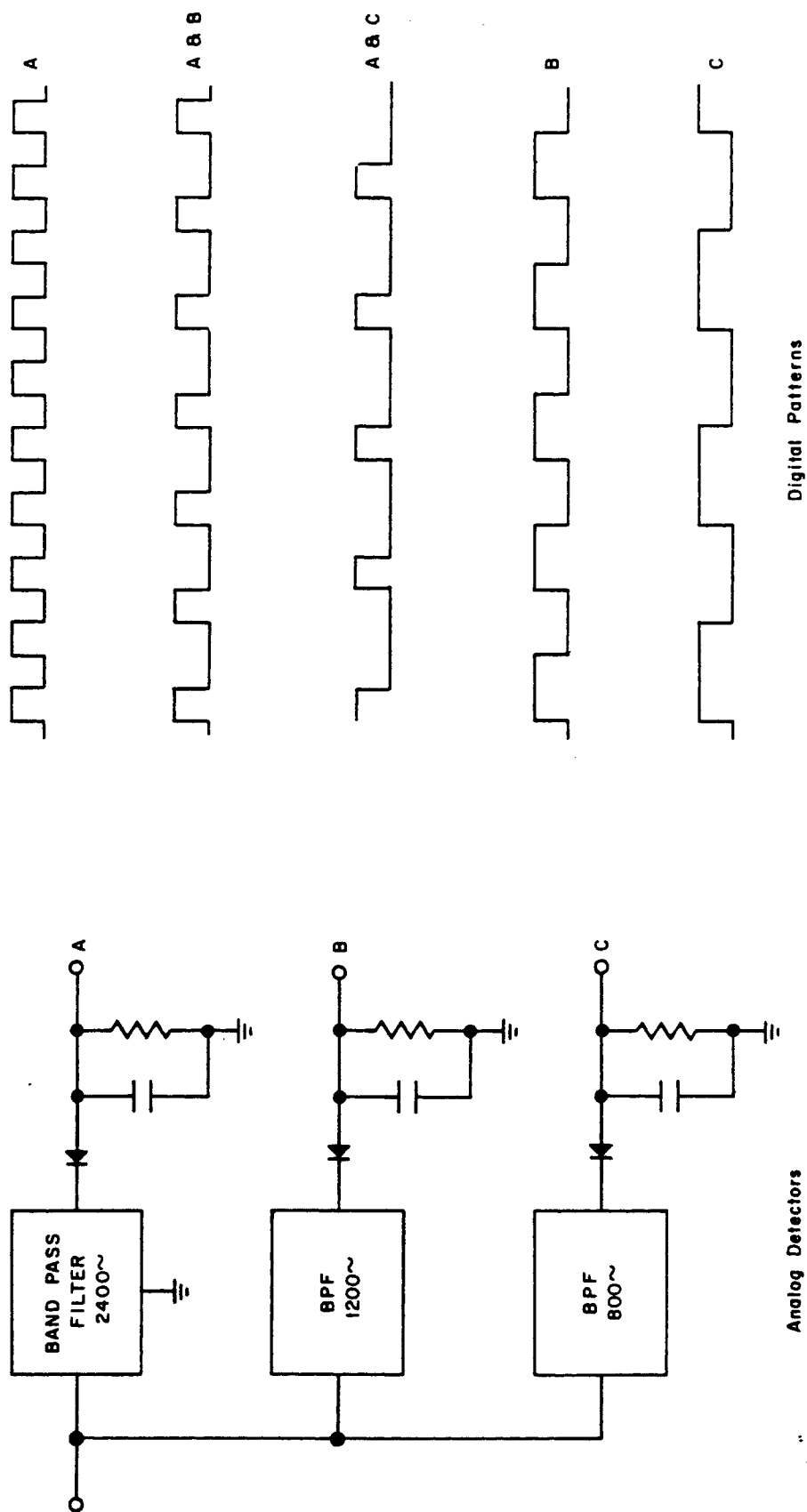


Fig. 22--Creating Signaling Tones by the Use of a Repeating Digital Sequence

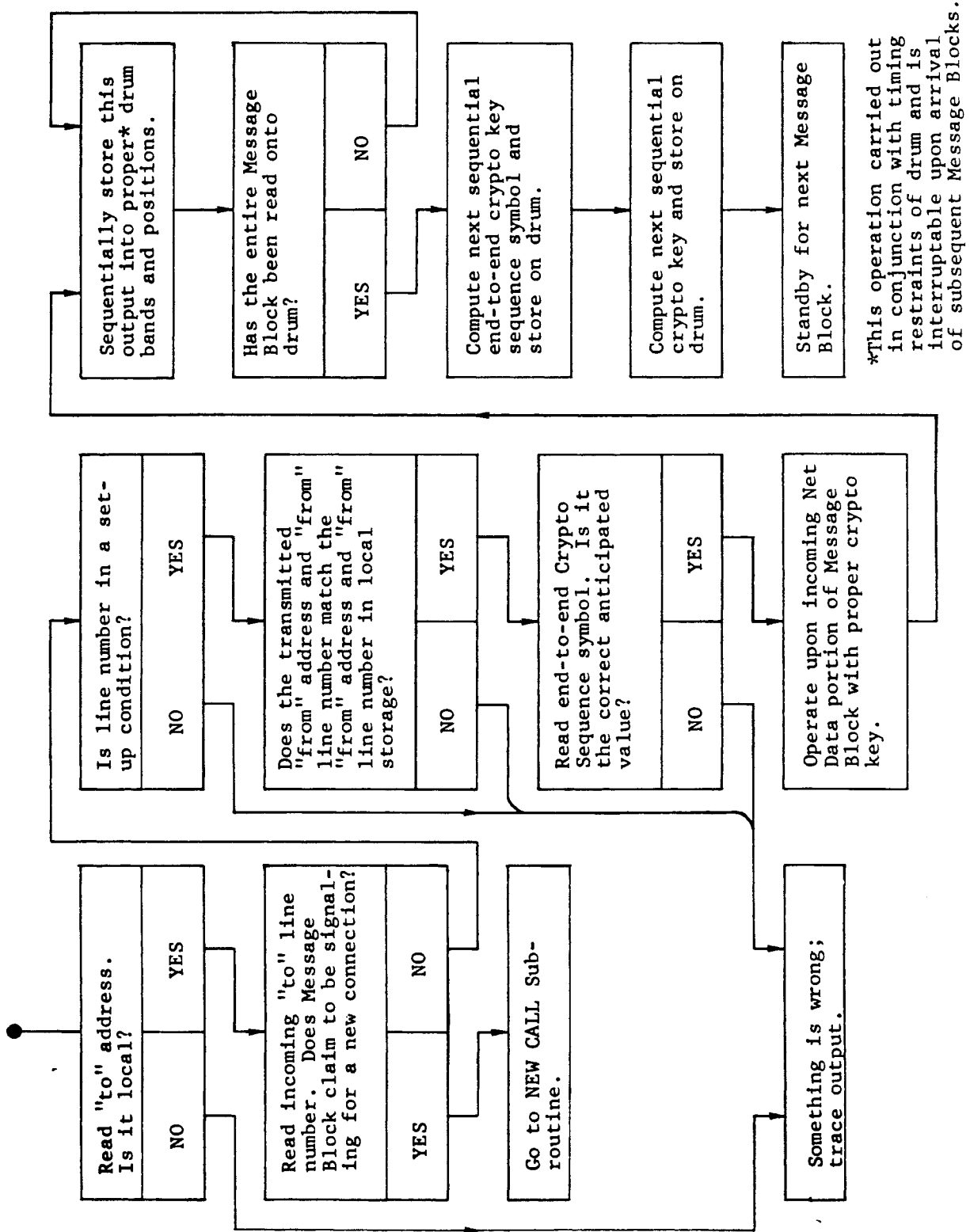


Fig. 23a--High-Speed-Core Housekeeping Operations upon Message Blocks Newly Arriving at Terminal Line Distributor

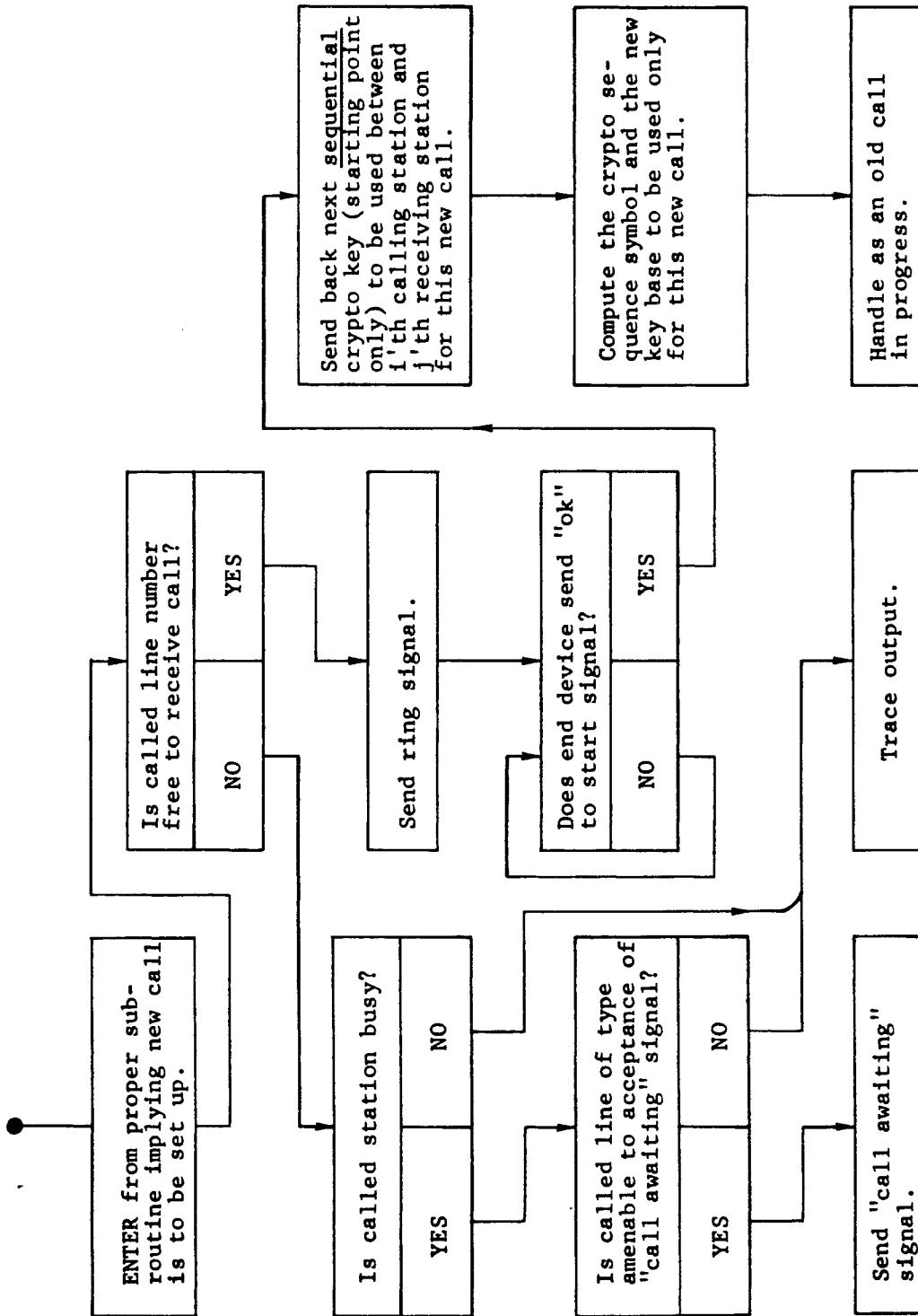


Fig. 23b---Subroutine NEW CALL

Operations of Trace and Trouble Display Unit, K

Each Message Block reserves sufficient housekeeping space to record the last four links it has traversed in its travels. Since there are a maximum of eight links emerging from each Switching Node, only three bits per link, or a total of 12 bits, provide sufficient in-message storage to unambiguously describe the last four links taken by each Message Block arriving at the Multiplexing Station.

The output of the trace signature can be graphically displayed by using a simple 10-column numeral-only printer, such as is found in an inexpensive adding machine; such output is illustrated in Fig. 24. In the event of trouble, an output strip is printed containing the housekeeping information relative to the last Message Block recorded as being in trouble (or in the event of a broken sequence, the last Message Block correctly received). Memory capacity for storing the last Message Block already exists by virtue of the non-destructive nature of the drum memory. Possible causes of trouble might include: maximum handover number exceeded; a reversed leader or broken crypto chain; or no such number existing. As each trouble message will be printed out on a small piece of translucent paper, it is possible to stack them in a small pile against a light source to show the paths used by in-trouble Message Blocks and by correctly received blocks. Interpretation and analysis is left to human intervention. Figure 25 shows a symmetrical network of redundancy level three, illustrating how a path through the network can be described by a simple series of three-bit numbers.

Figure 26 shows the path coverage for a system limited to a four-link trace coverage. The X's indicate the appearance of broken links in an examination of a stack of translucent vellums; the broken links stand out since they are not being used. The area outside the dotted line is that area in which the trace method would not be

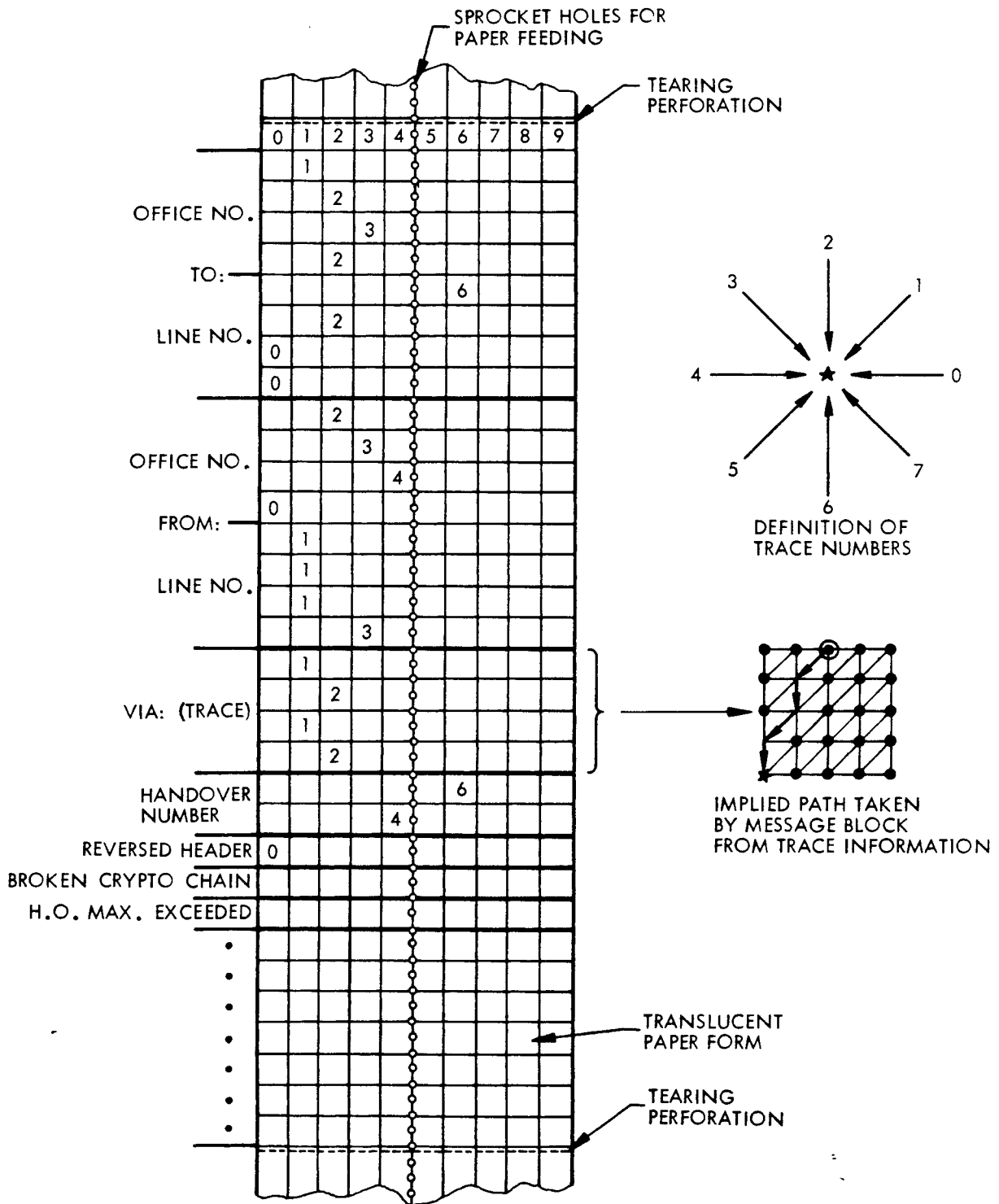


Fig. 24--Graphical Display for Intercepted Messages
Using a 10-Column Output Device

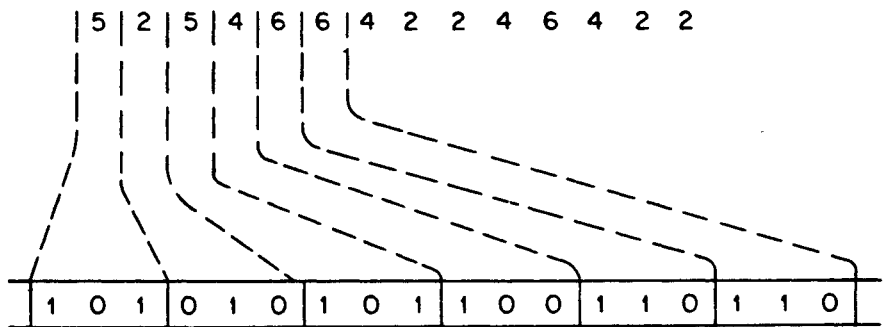
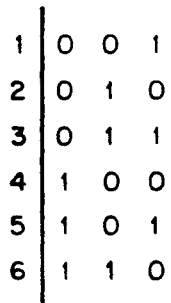
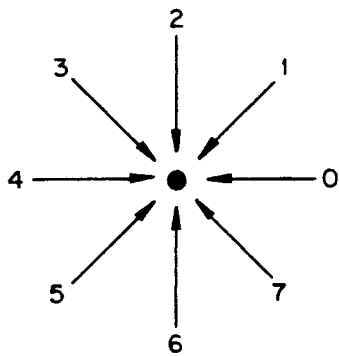


Fig. 25--Footprint Trace

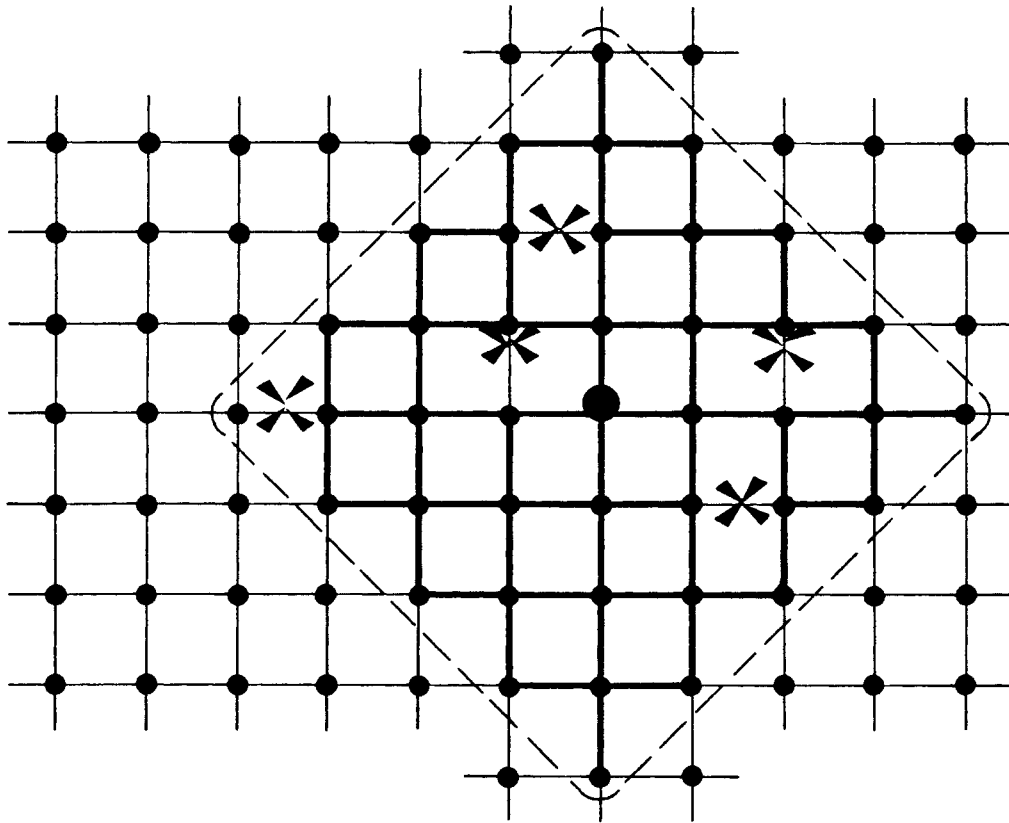


Fig. 26--Span of Coverage for a Trace Unit with a
Span of Four--Five Broken Links

effective for the particular Multiplexing Station shown in the center of the illustration (large dot).

Figure 27 shows the case of two defective Switching Nodes. This conclusion can be readily determined from the pattern since there are no visible links emerging from either of the two known Nodes.

Figure 28 shows the coverage of several overlapping trace zones, each having a span of four.

The trace scheme is intended only as a last-resort measure when all other system trouble safeguards fail. Error messages are expected to be few and far between. However, some method, such as the trace, is required to tie down stations causing intermittent network interference. The innate perversity of inanimate objects requires a safeguard of this sort, in spite of our lack of expectation of the ailment for which the remedy is proposed.

Operation of TO Subscriber FROM Drum Unit, N

Unit N distributes the decrypted Message Blocks from the drum into a bank of 1024 separate output flip-flops connected to each of the 1024 subscribers. Here, as in the input, a multi-input gate can be used to time-share ten separate drum amplifier channels. Switches assign each of the drum bands to its proper output line channel. The output data stream at the output of this unit is a synchronous binary stream to each of the 1024 separate subscribers (see Fig. 29).

Operation of the Priority Control Console, Unit P

Figure 30 shows the manual operator position at the Multiplexing Station, the priority control console, whose operation in analog circuit terms is described in QDC-IV.

We are not suggesting the construction of the priority

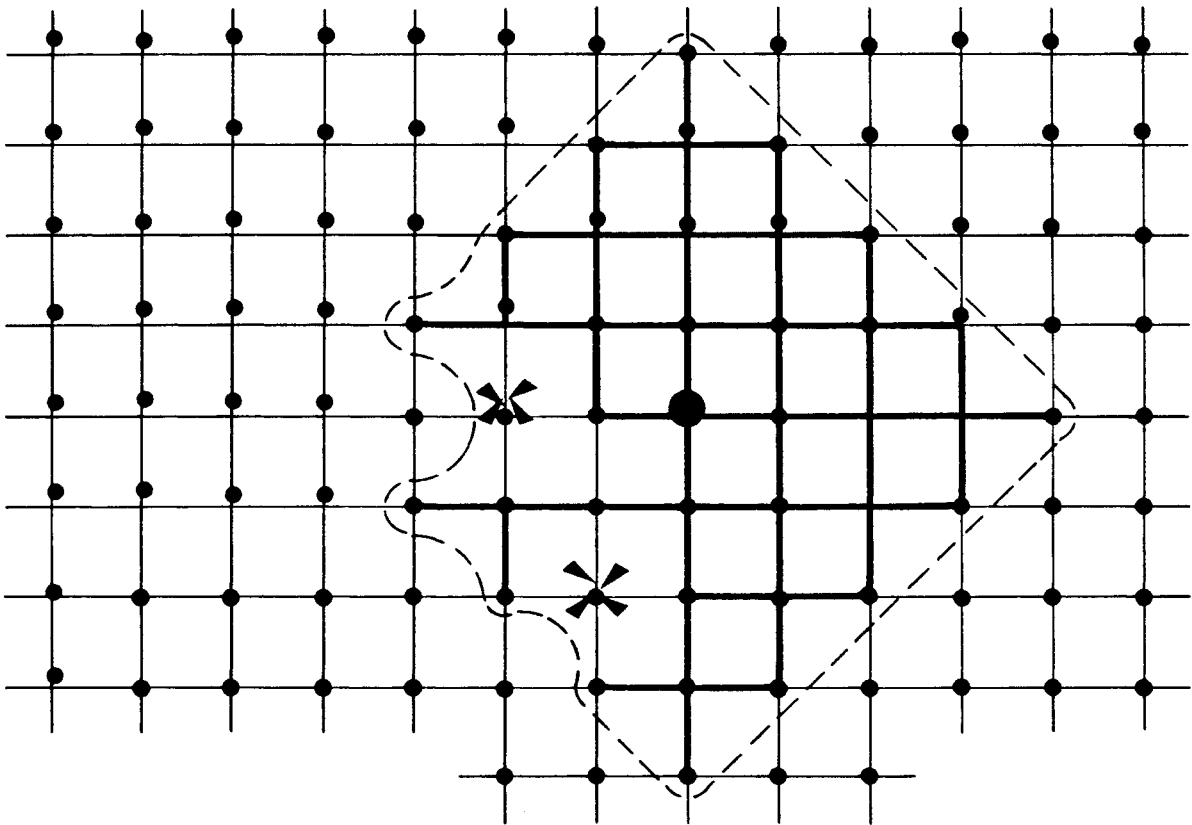


Fig. 27--Span of Coverage for a Trace Unit with a
Span of Four--Two Defective Nodes

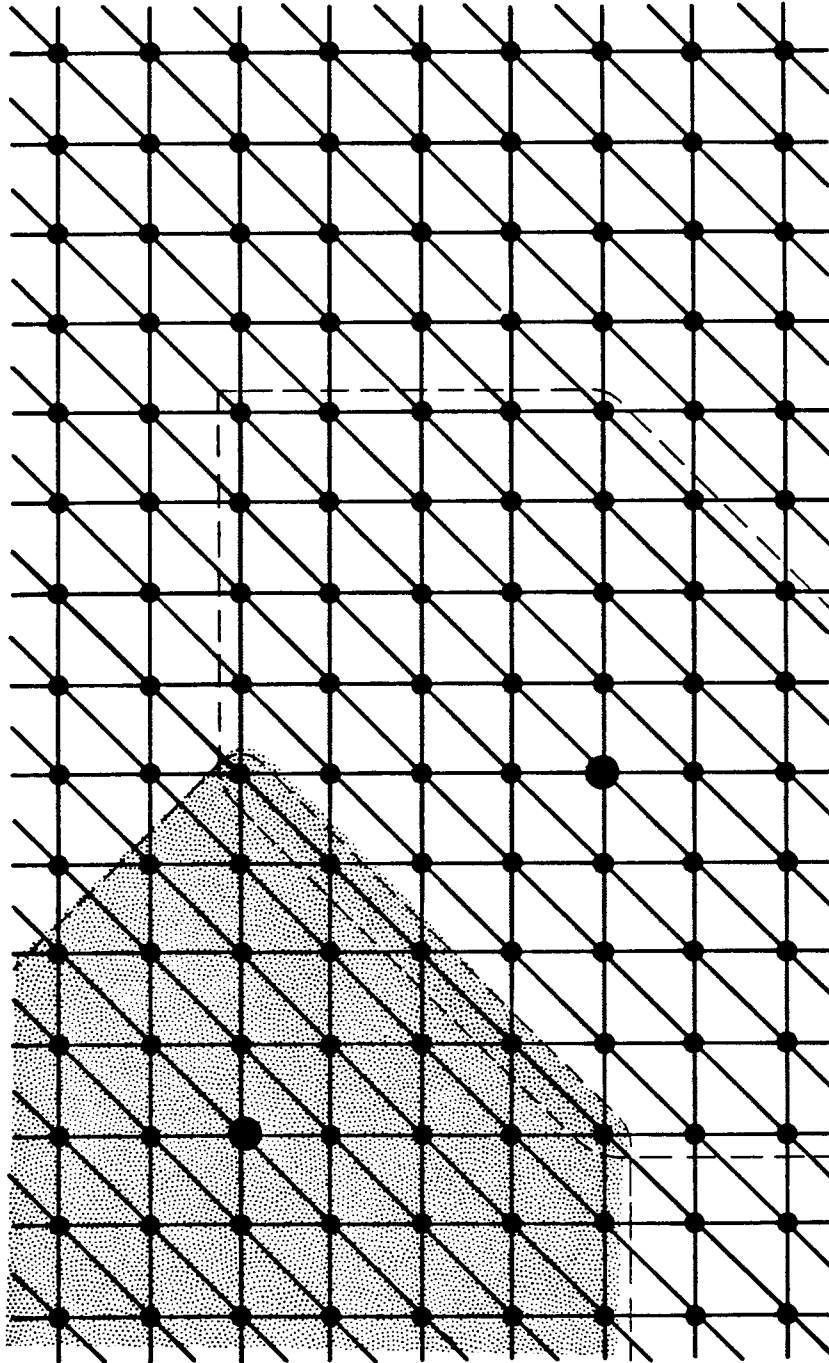


Fig. 28--Overlapping Coverage of Trace

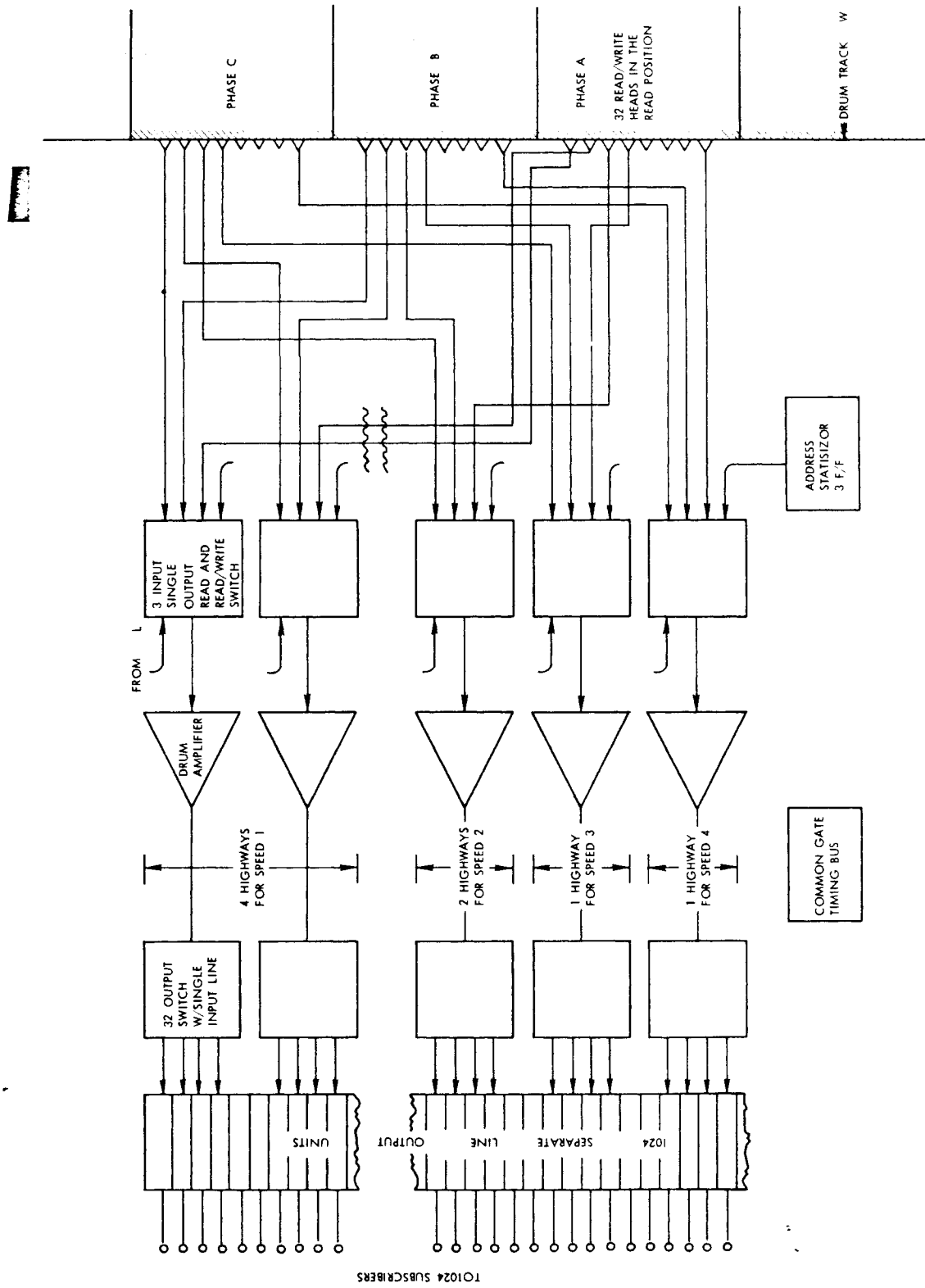


Fig. 29--To Subscriber From Drum Unit

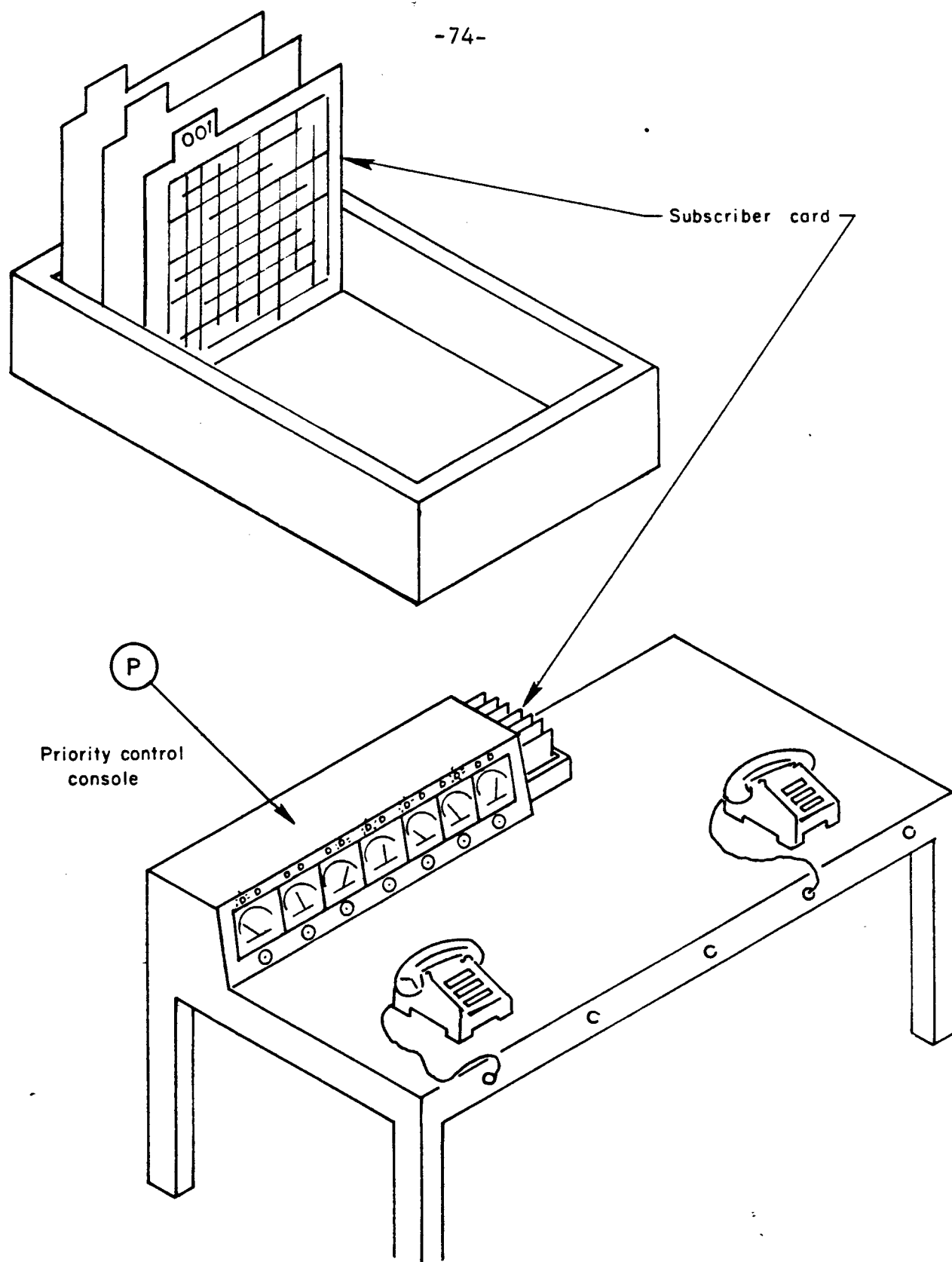


Fig. 30--Priority Control Console

control console in the analog-model manner described. However, all the digital signals needed to indicate the number of devices actively transmitting bits at any one instant which are necessary to the proposed control scheme, are available at the Multiplexing Station with Unit X, the Zero and Signaling Detector Unit.

This priority console controls the allocation of the communications resource among the 1024 users--depending upon their importance and data loading demands. Also seen in Fig. 30, at the operator position, are two telephones used as order wire terminations. The only human operator function that is absolutely necessary in this system is the insertion of information regarding change of address of subscribers and keys; these operations are described in detail in the next section.

Operation of Intercept Position and Change Translator Table Input Unit, Q

Each subscriber has a card upon which his latest line and station number is recorded. This is shown on the top of Fig. 30. Figure 31 shows the subscribers' cards at the operator's position in more detail: the top of each card contains the line code number, below which is the name of the subscriber. The following safeguards are included to prevent imposters from calling in and, posing as a legitimate subscriber, reporting that they are now operating at a different location. To circumvent this potential system weakness is a procedure whereby each subscriber is given a plastic card containing a series of verification numbers. Each verification number is covered with a separate gummed tab. A similar list of verification numbers is on the subscriber's card at the operator's position, and are similarly covered by removable tabs. Thus, if a subscriber moves to a different city, he calls

The diagram illustrates the components of a cryptographic system. On the left, a 'Subscriber's card in operators' position' is shown. It features a grid with 15 rows and 26 columns. The first row is labeled with numbers 1 through 15. The first column is labeled with numbers 1 through 15. The grid is divided into two sections: the top section is labeled 'Line code number' and the bottom section is labeled 'Name of subscriber'. Below the grid, there is a section labeled 'Plastic' and a section labeled 'Write in new number here for record purposes'. To the right of the grid, there is a section labeled 'Gunned tape strip concealing code numbers'. This section contains two rows of numbers: the top row is '2 K 3 1 7 0 1 5 4 7 2 8 2' and the bottom row is '5 9 W A 3 1 0 3 2 1 3 0 1'. An arrow points from the 'Gunned tape strip' section to the 'Plastic' section.

Fig. 31--Subscriber's Card

his original Multiplexing Station and requests that the Station change his alternative number to correspond to that of his new nearest Multiplexing Station. The operator at the original Multiplexing Station will then peel off the tab and ask the subscriber for his verification number. If these two numbers agree, then the operator at the original Multiplexing Station is assured that the change is bona fide. Each subscriber is expected to guard his own card, but, in any case, accidental examination or perusal of the card will not reveal the next authentication number unless the covering tab has been removed. This makes it exceedingly difficult for an enemy agent to determine verification numbers which could be used at a later date.

This method for changing individual subscribers' addresses is to be distinguished from the method used to insert the changes of tie-in points for entire Multiplexing Stations which might, for example, comprise an entire large military unit. Changes of the tie-in point of Multiplexing Stations is entirely automatic using the self adaptive means described in ODC-I.

Thus, it might not be necessary to physically man the Multiplexing Station a full 24 hours per day. Perhaps a few hours per day will suffice to allow changing the cryptographic key and making line assignments and priority allocation adjustments.

Operation of Common Drum Unit, W

The drum is common to many of the units of the system. A conventional drum, about 18" in diameter, 21" in length, rotating at about 2200 rpm, is proposed. As it does not appear necessary to include any short registers on the drum (i.e., writing and reading on the same track simultaneously) only one head per track is required and

interhead gap spacing problems are avoided. The only thing unusual about this drum is that it is necessary to synchronize the speed of the drum to a crystal clock, due to the synchronous nature of the input/output devices used. Complete synchronization down to an actual bit or fraction of a bit is not necessary, provided that long-term drift of the drum speed is prevented by a locked-in servo. If the servo-system can keep the drum angular position to within about ± 10 bits of "perfect" timing, and no long-term buildup of error is allowed (by the use of a clock counting against a timing track on the drum), it appears that system requirements can be met using conventional drum design practices.

Processing Drum Calculation

- 1) Reserve about 158 bits for header and housekeeping functions and allow 32 Message Blocks or channels to be recorded per drum band.
- 2) The drum will be designed to be used with input data rates in the $75(2^n)$ series with minimum intermediate buffering.
- 3) The same drum will be used for all channels, both input and output.
- 4) The raw Message Block length is 1024 bits, the active portion, therefore, being $(1024-158) = 866$ bits.
- 5) The drum will contain a synchronous timing track(s) prerecorded on the drum containing 32 channels, times 1024 bits, plus 1 bit, equaling 32,769 bits.
- 6) Synchronism of drum rotation will be maintained by a servo-system to within ± 10 bits at the drum clock rate against a local time standard, accurate to $\pm 10^{-7}$, or better.
- 7) Bit-packing spacing shall be about 600 bits/linear inch on the drum or disc surface (or whatever values fall within conservative practice for future 18" diameter drums or discs).
- 8) The drum shall contain about 400 read/write heads, fixed position.

- 9) Clock rate shall be 307.2 kc.
- 10) Each track shall be about 0.03 in. wide and each track shall have an approximate 0.05-in. center-to-center track spacing (implying a +20" length drum).
- 11) No short registers are needed; therefore, precise head alignment is not needed.
- 12) The drum need only operate in a room-temperature environment.
- 13) The drum shall reach full speed from a cold start within 10 min.
- 14) Modest vibration requirements only need be considered.
- 15) Life of the drum bearings and motor shall be in excess of five years.
- 16) The read/write heads shall be designed to operate in conjunction with head-switching circuits.
- 17) The drum shall normally be operated 24 hours per day, 7 days per week, and shall only be turned off during power or system failures and perhaps at maintenance periods.
- 18) Multiple discs or acoustic delay lines may be used in lieu of a magnetic drum if all other specifications can be met.

Operation of High-Speed Drop Point

Input/Output Unit, R

Over and above the 1024 separate input/output lines handling synchronous continuous data streams of up to 19.2 kilobits/sec, the Multiplexing Station network can also be designed to handle, on a time-shared basis, those users who make intermittent, but very-high-data-rate demands upon the communications resource (on the order of 1.5 million bits/sec). An example of such an operation might be a computer dumping the contents of its memory into a remote companion unit. In order to reduce the number of high-data-rate feeder lines, a party-line configuration is suggested. Figure 32 shows a "party line," operating at a high data rate, connected between two Multiplexing

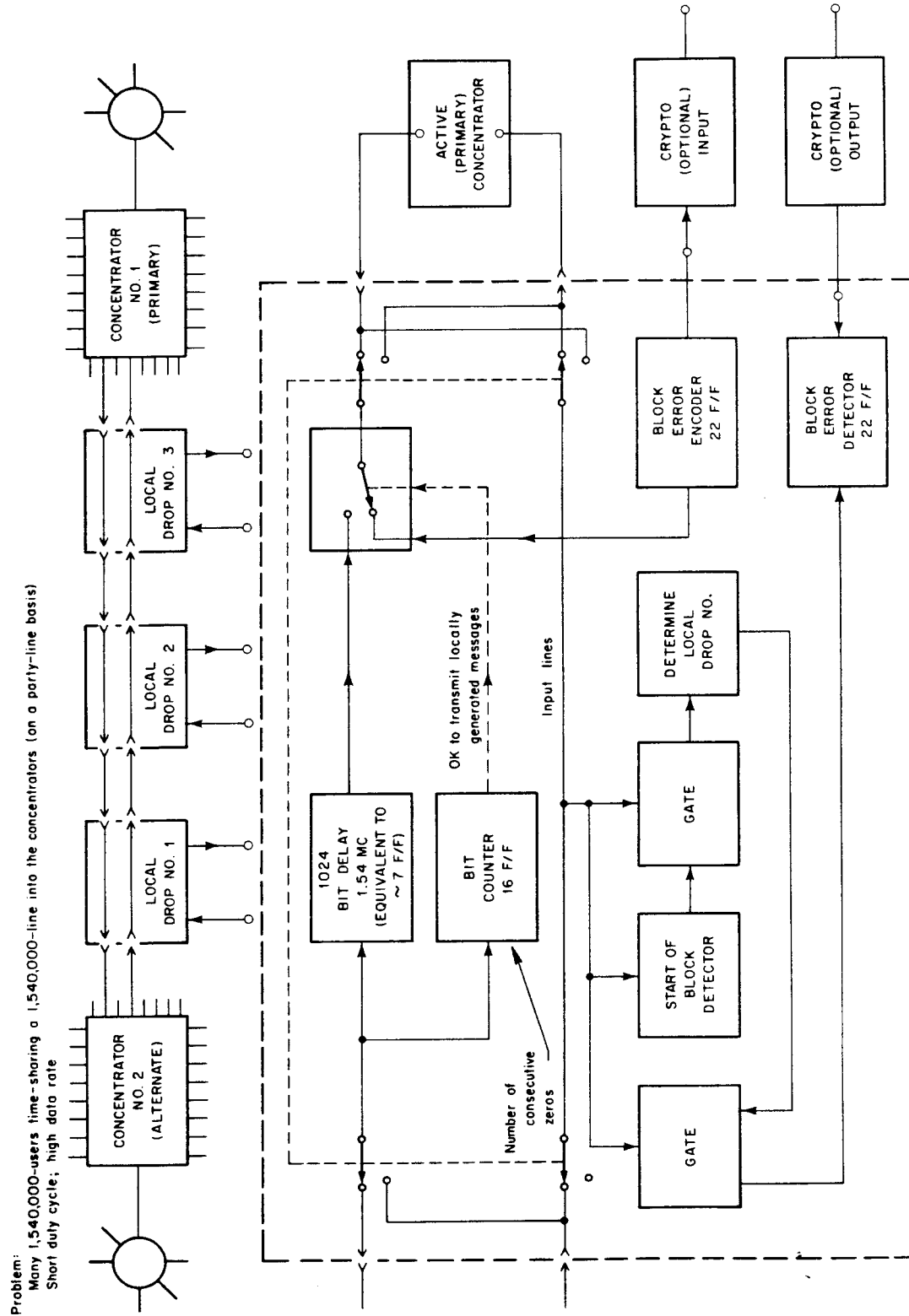


Fig. 32--High-Speed Drop Point Input/Output Unit

Stations which are in turn tied into two separate Switching Nodes. While only one of the Multiplexing Stations need be operative at any one time, two provide some measure of back-up in the event of a line break. These very-high-data-rate channels can be readily multiplexed by a simple time-sharing of the high-data-rate links between Switching Nodes. For example, every third bit would be reserved for this function. Of course, the data rate of such links would have to be raised from about 1.5 to 4.5 million bits/sec, but the marginal cost appears low.

A more awkward problem is that of the propagation velocity of the very-high-data-rate links. The problem is that each tandemly connected station cannot be sure that at the same instant he activates the line, it will not also become occupied by someone at the far end (because of propagation time delay). Whether this will be a major problem or not is unclear at this time. If it is, the difficulty may be circumvented by the expedient of providing one Message Block of storage delay for all traffic passing through each potential local drop point on the way to the end Multiplexing Station. If we examine the input and output streams into and out of the delay, we determine whether we would interrupt an on-going stream if we were to transmit at that instant. Thus, a drop-point station need never worry about "clobbering" traffic in process. Each station on-line would, of course, also utilize error detection and correction equipment in order to permit retransmission of Message Blocks in the event of inevitable link errors. Digital computers designed for on-line operation with an interrupt channel would appear to match the requirement of repeat transmissions with relatively little difficulty.

Calculation of the Number of Drum Bands for
Translator Table

Per Multiplexing Station:

L = number of lines = 1024

D = number of octal digits/address = 6

A = number of alternative addresses/line = 1

B = number of bits/digit = 3

M = number of marker bits/line = 6

N = number of bits/drum band = (1024) (32)

R = number of drum bands.

Thus,

$$R = \frac{L(DB + M + ADB)}{N} = \frac{1024 (6 \times 3 + 6 + 1 \times 6 \times 3)}{1024 (32)} .$$

Read/Write Head Switching Detail

Figure 33 is a schematic sketch of the detail whereby an entire bank of 32 heads are simultaneously switched from the read to the write mode. Figure 33 is included to obtain a feeling for the complexity of the circuitry involved in preparing the parts breakdown.

Operation of Zero and Signaling Detector, Unit X

Figure 34 is a simplified view of the Zero and Signaling Detector Unit. The heart of this unit comprises a bank of eight core planes, each containing 32 x 32 bits. The bi-stable cores used are initially set to their "0" state. If a single bit other than "0" is found in any bit position of any input line, the core corresponding to that particular line is set to "1". At the end of the duration of each Message Block interval, each core is read out. This provides a rapid determination as to whether nothing, valid information, or signaling has occurred during the last interval. If all zeros were noted on a line, no outgoing

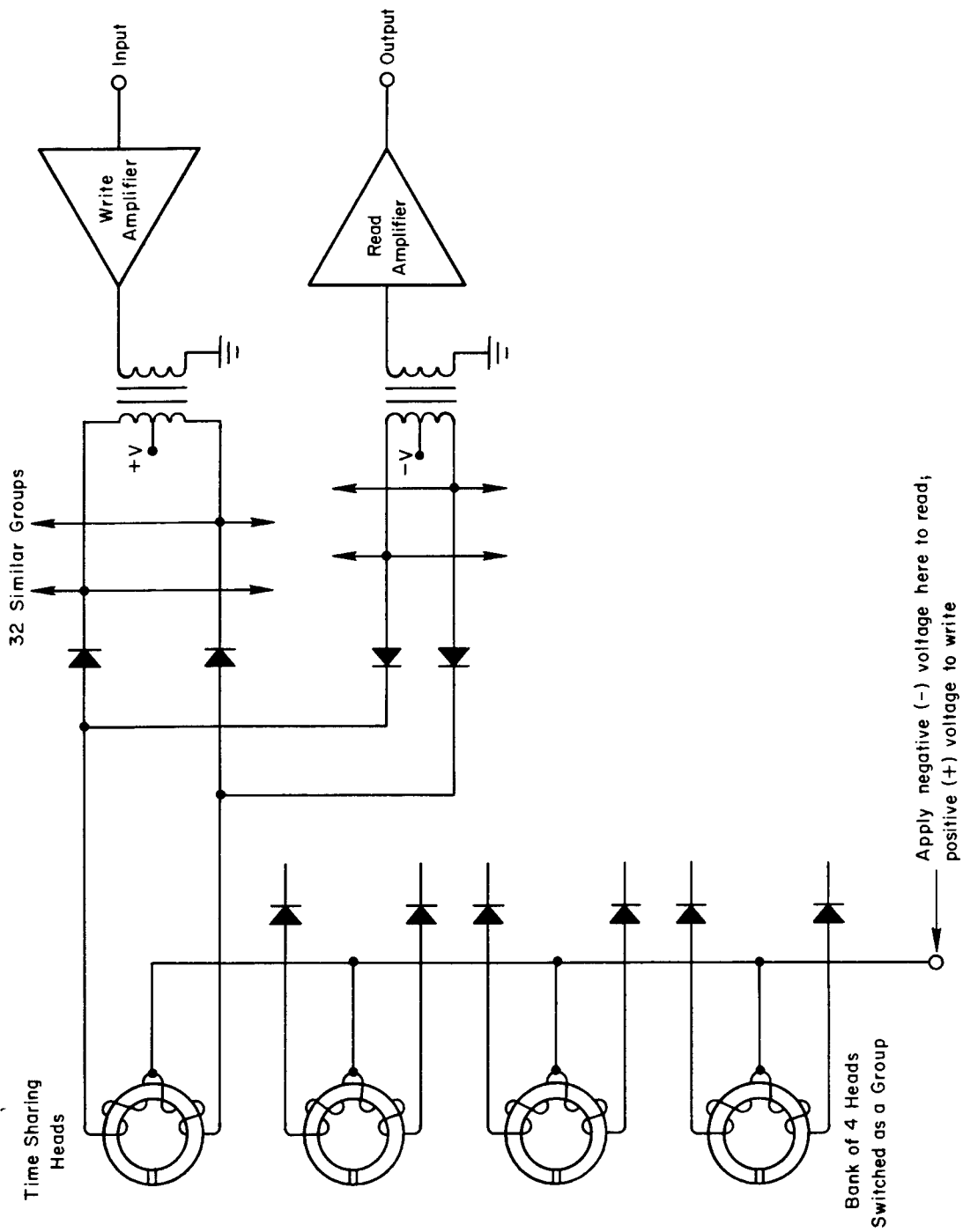


Fig. 33--Read/Write Head Switching Detail

EIGHT CORE PLANES @ 32 X 32 BITS

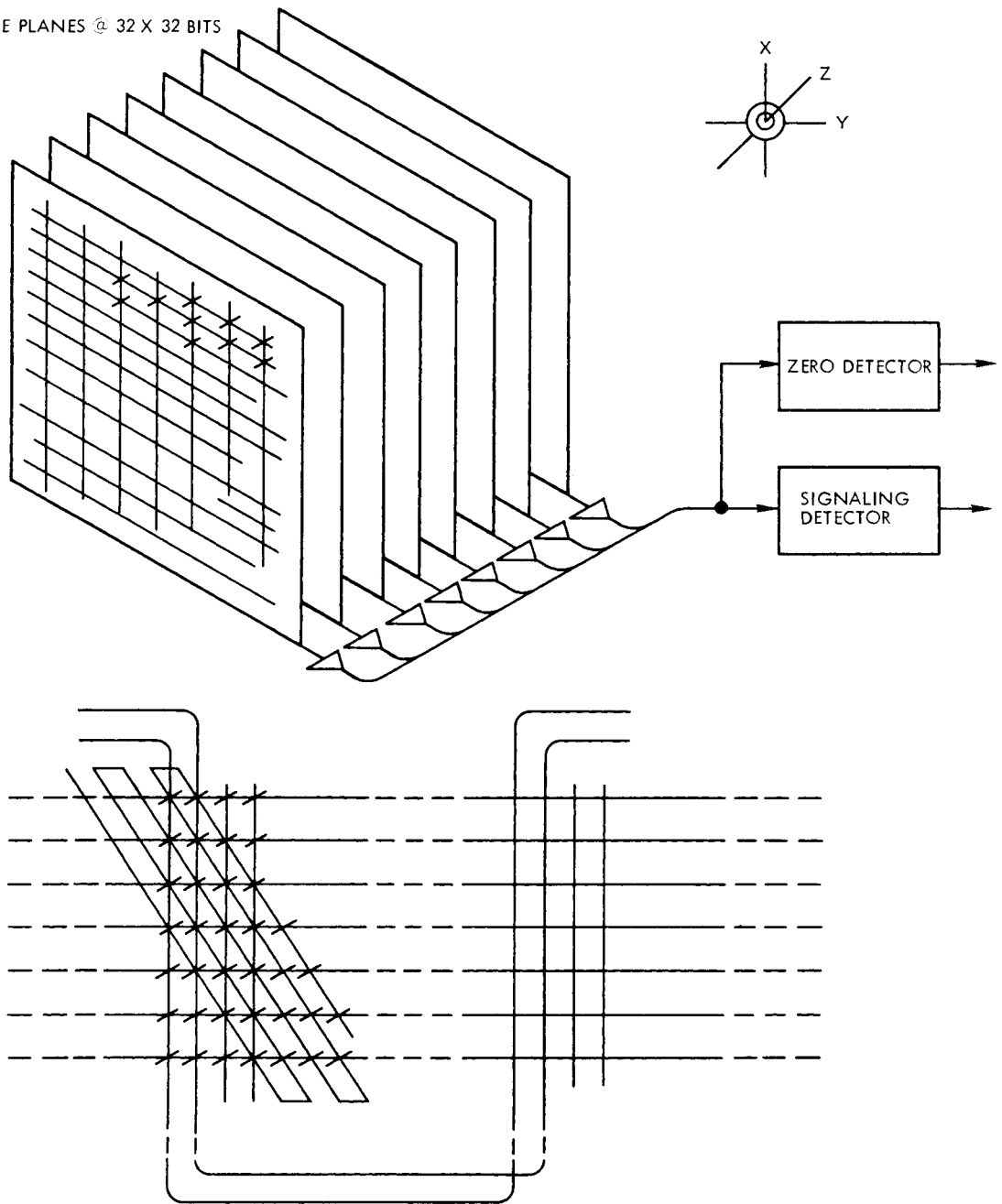


Fig. 34--Zero and Signaling Detector

Message Blocks were created and no further processing is indicated for this line. Thus, the first function performed is that of a fast filter to focus attention upon those channels that may be transmitting signaling or valid information.

The first procedure only filters out those lines transmitting all zeros. Detection of signaling information is somewhat more complicated. In this system, signaling always takes a pattern in which each bit is exactly similar to the polarity of every eighth preceding bit. In order to recognize the entire category of such signals easily, we separately connect each of the eight core planes to its assigned input line. As there are 866 bits of active information per Message Block, 112 input bits would be examined per core per line. If there had been even a single "1" found in the 112 bits, then this core would be set to "1". The entire core is now read out at the end of each Message Block time. If some of the bits are noted to be zeros and others ones, the probability is high that signaling information is actually being transmitted. The chance of an error in which signaling is mistaken for data is less than 2^{-112} , or about one chance in 10^{30} . Of course, there is a high probability that the signaling will start in the middle of the Message Block. But even with 19.2-kilobit/sec channels, the push buttons used for signaling would stay depressed for a longer period than the Message Block time--hence, there appears to be no problem from this cause. The final extraction of valid signaling data--a relatively rare event--requires post-filtering operations performed by the Central Processor, Unit J.

Operation of the Modify Key Box, Unit Y

It is necessary to change the cryptographic key of the Multiplexing Station at periodic intervals. The

equipment necessary to perform this function is provided by Unit Y. In establishing the parameters of the system the following assumptions are made:

- 1) About 2000 bits appears sufficient per send-key base and receive-key base between any two Multiplexing Stations.
- 2) Allow capacity to handle about 1024 different addressable Multiplexing Stations.
- 3) The key shall be contained on a magnetic tape which has been recorded at 2400 bits/sec.
- 4) A reasonable tape speed is about 7.5 in./sec for this bit rate.
- 5) Time to load tape into Multiplexing Station,

$$\approx \frac{2000 \text{ bits/key} \times 1000 \text{ stations}}{2400 \text{ bits/sec} \times 60 \text{ sec/min}}$$

$$\approx \frac{2 \times 10^6}{1.44 \times 10^5}$$

$$\approx 13.9 \text{ min.}$$

- 6) Amount of tape required

$$= 7.5 \frac{\text{in.}}{\text{sec}} \times \frac{1 \text{ ft}}{12 \text{ in.}} \times 13.9 \text{ min} \times \frac{60 \text{ sec}}{1 \text{ min}}$$

$$= \frac{6.25 \times 10^3}{1.2 \times 10^1}$$

$$= 520 \text{ ft of 0.25-in. width tape.}$$

- 7) A small reel containing 600 ft of tape is one possibility. However, it would be preferable to split the key into two pieces, generated at two different sources: two reels, each holding 300 ft, is thus suggested.
- 8) A 300-ft roll of 0.5 mill mylar tape occupies a standard three-inch tape reel.
- 9) After a short synchronization period, the tape drive motor servo-system must lock into within a peak drift of about ± 0.25 bits.
- 10) Assume that the capstan motor of the tape playback unit operates at about 1800 rpm at 60 cps.

- 11) 7.5 inches of tape pass by the heads each second, equivalent to 0.00313 inches of tape passing by in one bit-time (7.5/2400).
- 12) Maximum drift equals 0.00313 in. x 0.25 bit, = 0.00075", implying a tight synchronization loop.
- 13) Assume that a simple synchronization system containing a prerecorded timing track can maintain tape speed to within ± 0.5 cycles. Therefore, a 4800-cycle reference tone is required. This can be created from a 2400-bit/sec track by responding to every zero crossing of the incoming wave train.
- 14) The maximum differential synchronous motor lag angle at 60 cps, before synchronization is broken, is

$$\begin{aligned} & \frac{60 \text{ cps}}{4800 \text{ bits/sec}} \times 180 \text{ deg} \\ &= \frac{1.08 \times 10^4}{4.8 \times 10^3} \end{aligned}$$

= ± 2.25 deg peak 60-cps motor jitter.

- 15) The simple servo-system configuration shown in Fig. 35 should suffice. This servo-system utilizes the heterodyned signal between the system's 4800-bit/sec rate and a separate 4740 cycle time signal recording on a two-track magnetic tape, to produce a 60-cycle motor control signal. Speed differences are amplified by a factor of about 80, times the actual frequency difference.

Operation of Remote Devices at Subscriber Stations, Unit Z

While not truly an integral unit of the system, this unit provides the method whereby voice or other analog signals are converted into a digital stream. Figure 36 shows a typical telephone proposed for use with this system. From the outside, it looks very much like a conventional touch-tone dialing telephone, but there are some major differences; for instance, the output is a four-wire 19,200-bit/sec binary stream. It will be recalled that all input devices

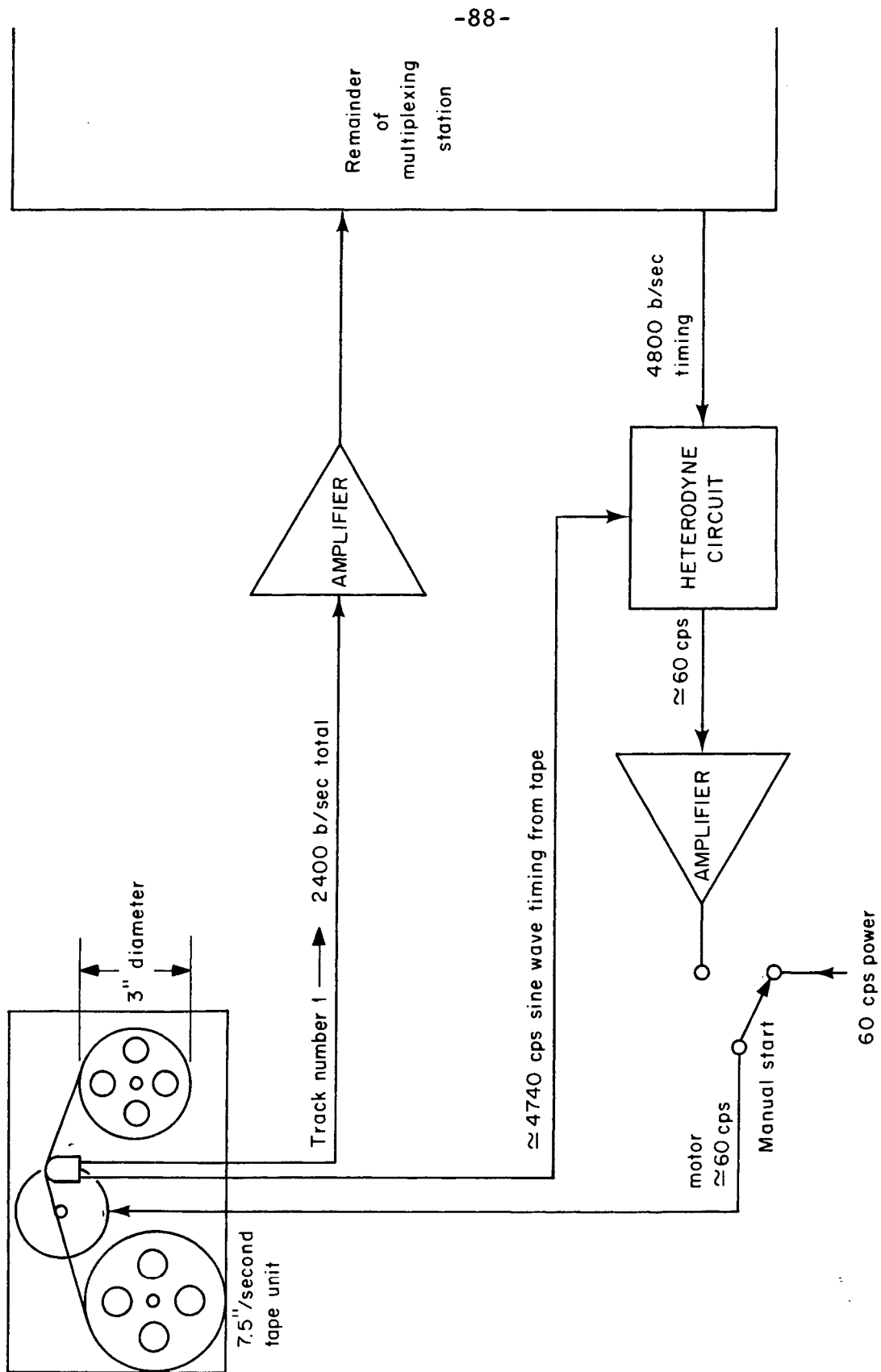


Fig. 35--Tape Playback Unit Used to Insert New Keys

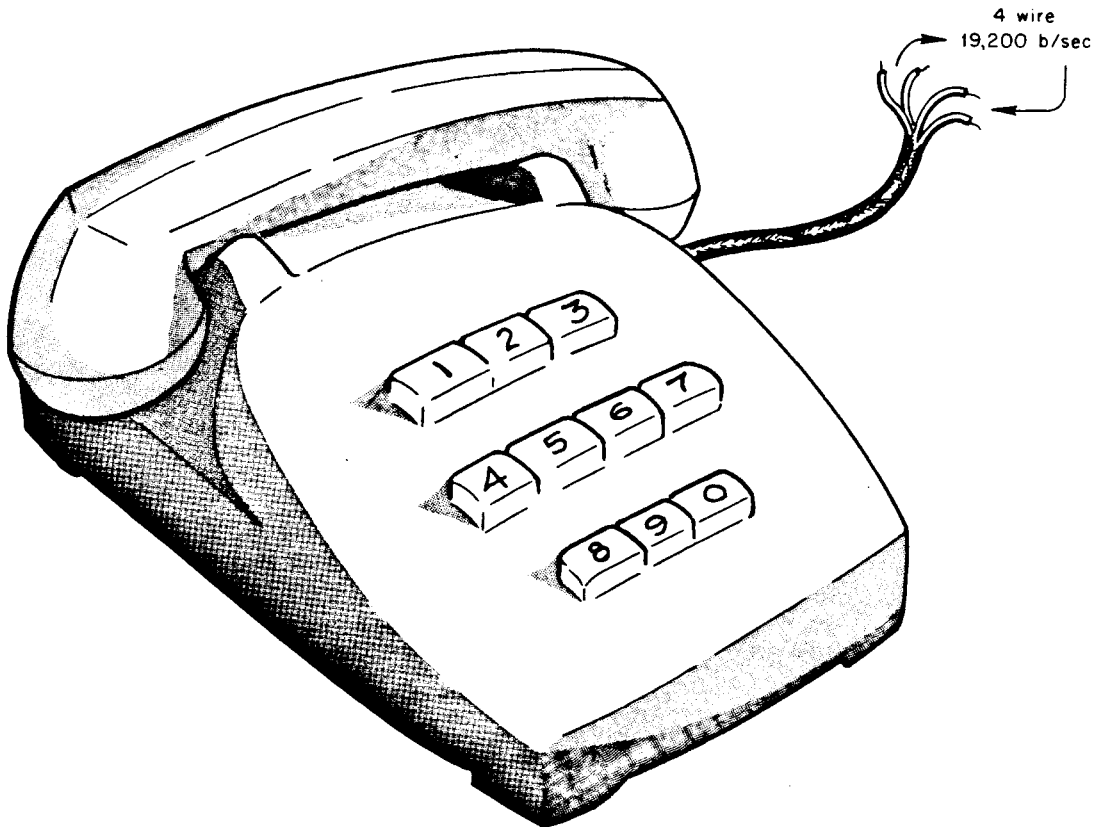


Fig. 36--Typical Telephone Proposed for Use in the System

feeding the system derive their timing from an incoming binary stream originating from the magnetic drum of the Multiplexing Station. Both signaling and data are a binary bit stream synchronized to this timing pattern.

The signaling waveforms are chosen so that they are easily detected by the Multiplexing Station. One of the key ways of possibly generating the binary signaling stream at the telephone includes the use of a small counter with changeable feed-back connections. Only four flip-flop stages are required to generate any of the desired digits.

We have seen how a binary stream used for signaling can be easily generated with a few transistors. Next, let us consider the mechanism that turns an audio signal into

a digital stream, and vice versa. Figure 37 shows the block diagram of the proposed telephone containing a miniaturized analog/digital converter together with the push-button signaling previously described. Starting at the microphone in the extreme right of the illustration, the audio signal from the microphone is amplified and its dynamic range compressed. This audio signal output is applied to a simple analog/digital converter. The output of the analog/digital converter is transmitted only in the absence of a squelch signal which indicates that the user is talking on his telephone. This output digital signal is then applied to the outgoing line amplifier. To the extreme left of Fig. 37 is the input data stream arriving from the Multiplexing Station at 19,200 bits/sec. This signal is amplified, and the timing period extracted. This fixed-frequency signal is used to time the outgoing digital stream.

Incoming binary data is converted by a digital analog converter circuit; the output is amplified and sent to a small earphone/speaker unit.

At the bottom of Fig. 38 is the counter unit with push-button keys used to establish the binary signaling pattern. The equipment required appears to be relatively simple, composed primarily of transistors and similar small electronic components. The present state of the microminiaturization art appears sufficiently well developed so that the entire unit might even be built within the base of the telephone. It appears that a digital telephone need not be large or expensive (if considered on an overall system basis). With such digital telephones, additional signaling information may be transmitted even when the receiver is off-hook, permitting the addition of signaling information at times not now conveniently possible. This simplifies the handling of such new services as being

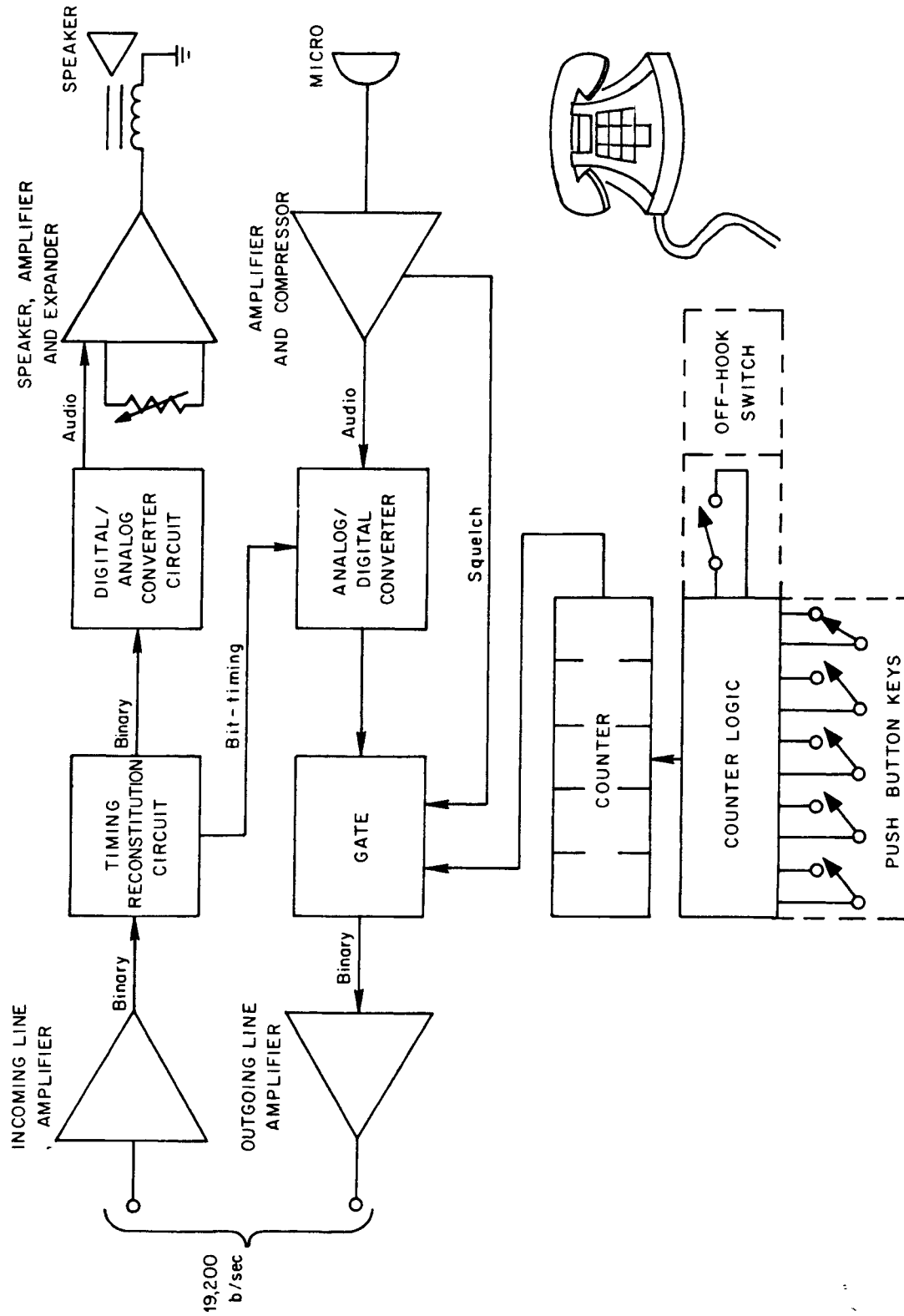


Fig. 37--Telephone with A/D Converter and Push-Button Signaling

able to set up a secure conference call and adding new parties even after the conversation is in progress.

It is necessary to consider methods for signaling information input transducers other than the digital telephone described. Figure 39 shows a modem suitable for start-stop teletype devices containing a signaling attachment. The signaling method is exactly the same as that used in the digital telephones. (It is to be remembered that teletypes operate in this system by modulating a 600-bit/sec square wave pattern.) This tie-in unit is a "black box" connecting the teletype to the line feeding the Multiplexing Station. This box, about the size of a cigar box, contains push buttons to select the called party, a small speaker for signaling and warning, and a high-current teletype line driver. Such a modem provides the interconnection between today's standard input/output devices and the potential network of the future.

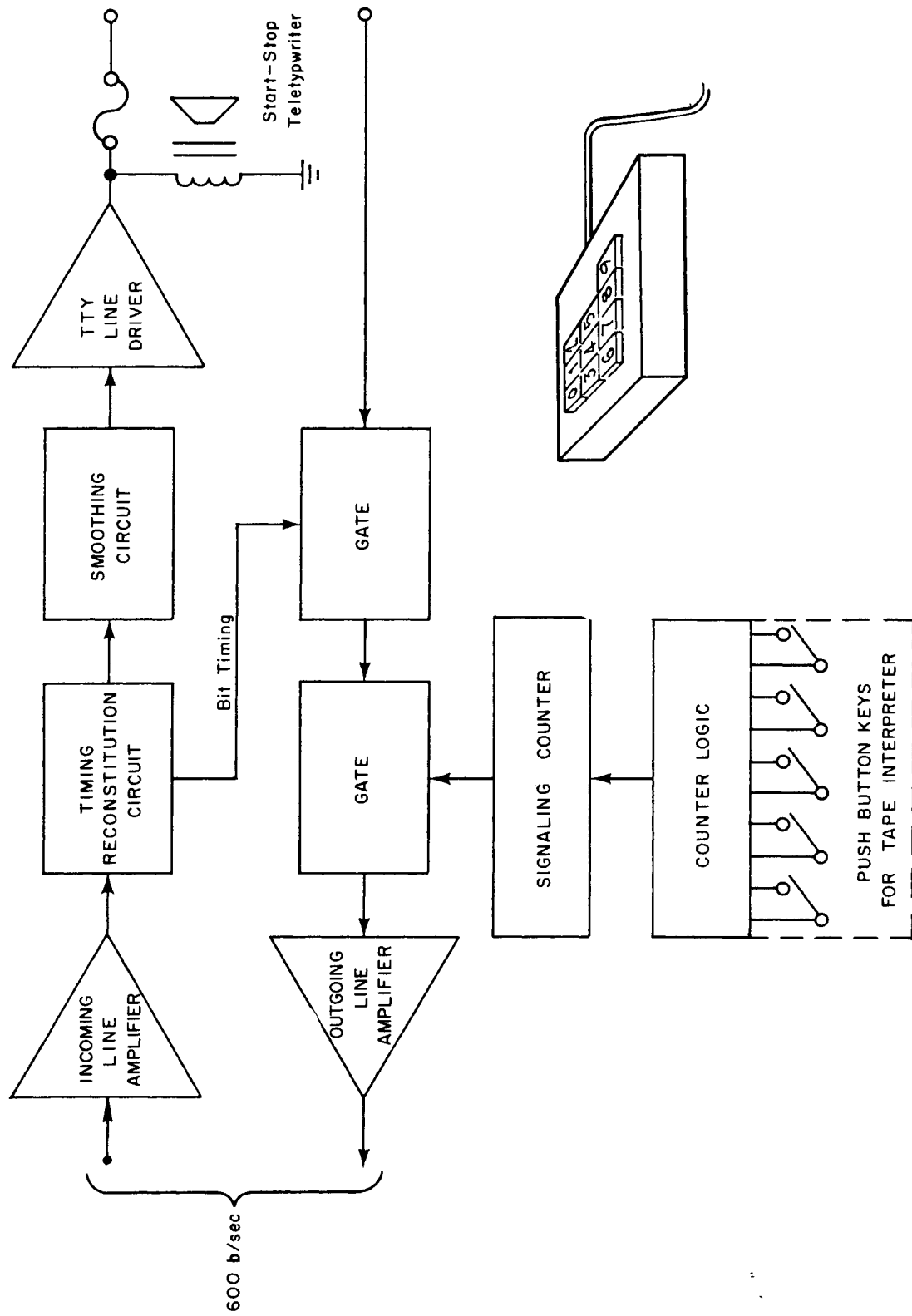


Fig. 39--Modem for Standard Start-Stop Teletype
with Signaling Attachment

VI. MAJOR EQUIPMENT COMPLEMENT

Transistors (= 4 x equiv. F/F)	30,656
Core memory, @32-bit words	~ 2000 words
Power supplies	2 units
Emergency power source	2 units
Audio tape playback	1 unit
Drum, magnetic w/servo and 400 heads	1 unit

This list provides a brief summary of the components implied by the first rough-cut estimate of the proposed system. It is not meant to be complete, as not all the circuits have been examined in equivalent depth. It is a "once-over-lightly" examination of the amount of equipment that each unit performing some function that needs to be performed will probably take. However, in the past this method of analyzing digital equipment has been found surprisingly accurate--usually within a fractional order of magnitude. The number of components required to perform the necessary functions is, upon a second look, usually thought to have been underestimated by a large factor. But, later, when the detailed design of the system is completed by a competent, and ingenious logical designer able to take advantage of minimization of logical functions, a saving roughly equivalent to the underestimate seems to occur.

All that can be said at this point with any confidence is we anticipate that a unit occupying about 150 cu ft, and costing about \$300,000 exclusive of research and development, would be on the approximate order of magnitude of equipment needed to build Multiplexing Stations that permit the interconnection of 1024 simultaneous subscribers into the system.

This low price can only come about after the equipment has been fully developed, tested, and production quantities

manufactured. In order to build such low-cost equipment, it will also be necessary to use industrial-grade components in lieu of standard high-priced military-approved components. It is felt to be much cheaper to maintain a good atmospheric environment for electronic equipment than it is to tighten the specification of the environment and, in turn, the components used.

CAVEAT

Again, it should be emphasized that no detailed complete design has been made; this is only a first-cut estimate. Only those processing operations that are performed continually and quickly, and which require special units, have been examined. All the operations performed in setting up a call appear to be within the constraints of the Central Processor, Unit J, which is almost a general-purpose computer. There appears to be sufficient time available for performing the extremely complex operations. We have attempted to limit our examinations only to those operations that are highly repetitive and which set the boundaries on the amount of equipment required.

INSUFFICIENTLY EXAMINED AREAS

There are certain areas in particular that merit more detailed examination in order to better specify the actual number of components required. These embrace those functions difficult to analyze without more labor than would be appropriate at this time. They include:

- 1) Exactly how much core memory is required in the Central Processor? Some of this memory is needed to perform the signaling functions and special error tracing operations; most will be set aside for handling peak loads of outgoing Message Blocks. While we intuitively feel that about 2000 32-bit words will be sufficient (and will avoid the necessity of dropping messages due to instantaneous overloads), more examination is indicated.

- 2) Message Blocks from 32 separate lines are interlaced on a single drum band, so the bits forming a single Message Block will not appear in sequence on the drum. However, it is anticipated that reciprocal operations at the transmitting and receiving Multiplexing Stations will eliminate any problems originating from this cause. But, if such problems are encountered, there are several possible ways out, but these have only been briefly touched upon. No single best method is being suggested at this time because of a limited amount of time for analysis of the alternatives.
- 3) We are not wholly satisfied with the expected reliability of the Multiplexing Station in its present configuration. For example, in the event of major failure, the number of usable lines drops to a very small number, and part of the secrecy protection is lost until repairs are made. The use of acoustical delay line registers, instead of one big drum, plus the replicating of more of the elements of the Multiplexing Station, would permit more satisfactory operation in the event of failures. A failure mode analysis should be one of the first tasks undertaken.
- 4) We would like to see low-cost, cryptographically secure telephones built specifically to operate with this system, so that complete two-level security can be offered to even subscribers remote from the Multiplexing Station.
- 5) We would like to see work directed toward lowering the cost of conventional hard-copy input devices, such as teletypewriters. All the savings and advantages of an all-digital system cannot be obtained unless the subscriber end-devices are designed with such systems initially in mind.

The individual component failure rates anticipated in the Multiplexing Station are essentially those of the components used in the manufacture of the Switching Node. We do, however, also have a magnetic drum with the servo-unit plus a small magnetic tape recorder that have a limited life--perhaps on the order of five years between major overhauls. Many of the failures we anticipate will occur in elements such as individual line units which will not

take down an entire Multiplexing Station. However, until the equipment has been redesigned on the basis of types of failure, and the reduced capability modes of operation studied in detail, it may be misleading to suggest any mean-time-to-failure estimates for the Multiplexing Station.

The best that can be done is to state that the complexity of this equipment is roughly about two or three times that of the Switching Node and could, at worst, be correspondingly less reliable. But, on the other hand, there are more inherent safeguards and standby provisions in this equipment. To be safe, however, we should plan; therefore, it would seem highly advisable to have the most important users tie into two or more Multiplexing Stations.

VII. CONCLUSIONS

It appears to be feasible to construct the Multiplexing Station within the 1963 state of the computer art.

The use of all-digital transmission and switching of standardized Message Blocks greatly facilitates the addition of new features thought desirable in future communications networks for military and civilian applications. The ease of providing these new services, in comparison to present-day practice, seems to make this new form of communication network desirable--even in those applications where no vulnerability problem exists.

The reader should be cautioned that this preliminary investigation was carried out only to the degree of detail necessary to provide an indication of the degree of complexity to be expected, and to pin-point obviously insurmountable design problems. One weakness did present itself: In the first-cut examination, in retrospect, we feel we have tended to place too much reliance upon a single common-control apparatus. At a price of a moderate increase in the number of components and a more elegant design, a Multiplexing Station might result which is less prone to loss of station performance merely because a few components here and there have chosen to fail.

It is suggested that such a new design, still limited to the use of low-cost, modest-reliability elements, could be organized to better divide the common-control function. This is, it should be noted, not a new problem, but one faced in the design of every common-control telephone central office switching apparatus. It was not felt that such a careful redesign was necessary at this stage of consideration.

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 multi-megabit 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.