
Network Management and Control Systems

U-TNS
1985 C.1

INPUT[®]



Digitized by the Internet Archive
in 2015

<https://archive.org/details/networkmanagemenunse>

NETWORK MANAGEMENT AND
CONTROL SYSTEMS

U-TMS
1985c.

AUTHOR
TITLE
Network Management
and Control Systems

DATE
LOANED

BORROWER'S NAME





NETWORK MANAGEMENT AND CONTROL SYSTEMS

CONTENTS

	<u>Page</u>
I INTRODUCTION.....	1
A. Purpose and Scope	1
B. Report Organization	2
C. Methodology	3
D. Other Related INPUT Reports	3
II EXECUTIVE SUMMARY	5
A. Data Networks Are Growing in Complexity	6
B. Network Management Must Be Multifunctional	8
C. The Role of Network Equipment Suppliers Is Critical	10
D. Which Directions Are Networks Taking?	12
E. What a Network Control System Is--and Isn't	14
F. The Role of Control Is Crucial	16
G. Network Control Wears Many Hats	18
H. Data Networks Must Be Managed	20
III TECHNOLOGY REVIEW AND ANALYSIS.....	23
A. Introduction	23
B. Elements of the Network Control	24
C. Requirements of Control	25
D. Control Configurations	27
E. Network Control Functions	31
F. The Vendor's Role	37
G. Technical Control	39
H. Network Management	42
1. Network Troubleshooting	43
2. Procedural Checkout	44
I. Test and Monitoring Equipment	46
J. Line Considerations	48
K. Line Routing	50
L. Line Conditioning	52
M. The Special Case: Network Control Centers for Packet Networks	57
1. Routing and Flow Control	60
2. NCC Operator Functions	62
N. Network Control Systems Examples by Manufacturer	63
1. IBM	63
2. Paradyne	65

	<u>Page</u>
3. General DataComm	65
4. AT&T	66
5. Tech Control Center Manufacturers	67
O. Major Modem Manufacturers	67
IV CONCLUSIONS AND RECOMMENDATIONS	69
A. Conclusions	69
B. Recommendations	70
APPENDIX: QUESTIONNAIRE	75

NETWORK MANAGEMENT AND CONTROL SYSTEMS

EXHIBITS

		<u>Page</u>
II	-1 Data Networks Are Growing in Complexity	7
	-2 Network Management Must Be Multifunctional	9
	-3 The Role of Network Equipment Suppliers Is Critical	11
	-4 Which Directions Are Networks Taking?	13
	-5 What a Network Control System Is--and Isn't	15
	-6 The Role of Control Is Crucial	17
	-7 Network Control Wears Many Hats	19
	-8 Data Networks Must Be Managed	21
III	-1 Typical Network Management System	30
	-2 Circuit Test Configurations	47
	-3 Line Routing: Example of Multiple-Path Routing	51
	-4 Unconditioned Voice Grade Line Characteristics	54
	-5 Distortion Correction Using Conditioning	55
	-6 Delay Characteristics of Voice Grade Line Conditioning	56
	-7 NCC Configuration Elements	59

I INTRODUCTION

- This report is part of INPUT's Telecommunications Planning Program, designed to help inform senior managers and corporate executives of changes in telecommunications technology. The report:
 - Identifies network control technological requirements.
 - Defines and analyzes current and projected network control technology innovations.
 - Analyzes cost factors affecting network control utilization and implementation.
 - Identifies the direction of network control growth and development.

A. PURPOSE AND SCOPE

- The changing face of telecommunications and its attendant growth patterns and trends are of immense interest to business executives, managers, and users. The recognized necessity for network control to accommodate the expected level of user service mandates that managers and users acquire insights into the technology. Only by understanding network control can both users and information systems providers fully utilize the available capacity in

order to properly exploit the communications capabilities most applicable to the needs of their businesses.

- The scope of the report covers management control planning activities, technical control problem identification and resolution, and network control system design and implementation. It does not, however, provide a series of step-by-step instructions for developing a network control system, since each organization will have its own requirements and philosophy.

B. REPORT ORGANIZATION

- This report is organized as follows:
 - Chapter I is an introduction and sets the stage for what follows.
 - Chapter II is an executive summary, formatted as a presentation for group discussions, and emphasizing the key points within the report.
 - Chapter III outlines some basic principles of network management and control.
 - Chapter IV is a technological assessment and includes a survey of the network control technology to date.
 - Chapter V contains INPUT's conclusions and recommendations for effective network control strategic planning.
 - The Appendix contains the questionnaire used to identify what others are doing about network control requirements and utilization.

C. METHODOLOGY

- The information contained in this report was derived from the following sources:
 - Interviews with senior managers and executives in marketing, telecommunications planning, and information systems.
 - In-depth interviews with senior planning managers and executives.
 - INPUT's own studies in telecommunications.
 - Open literature surveys.
- INPUT has taken the best practices and proposals and subjected them to further analysis to serve as a basis for this report.

D. OTHER RELATED INPUT REPORTS

- Telecommunications Strategic Planning. Defines and describes telecommunications planning techniques and processes (using the case example approach) and further identifies critical telecommunications planning issues.
- Annual Information Systems Planning Report. Evaluates information systems trends and illustrates critical IS management issues.
- Impact of Communications Developments on Information Services Vendors. Analyzes changing communications technology and services as related to information services activities.

- Effective Corporate Planning in the Computer Services Industry. Examines the level and extent of corporate, market, industry, and product planning within the computer services industry. Emphasis is on corporate planning efforts.
- User Communication Networks and Needs. Identifies and evaluates changes in user needs within the communications field, with particular emphasis on network problems and solutions.

II EXECUTIVE SUMMARY

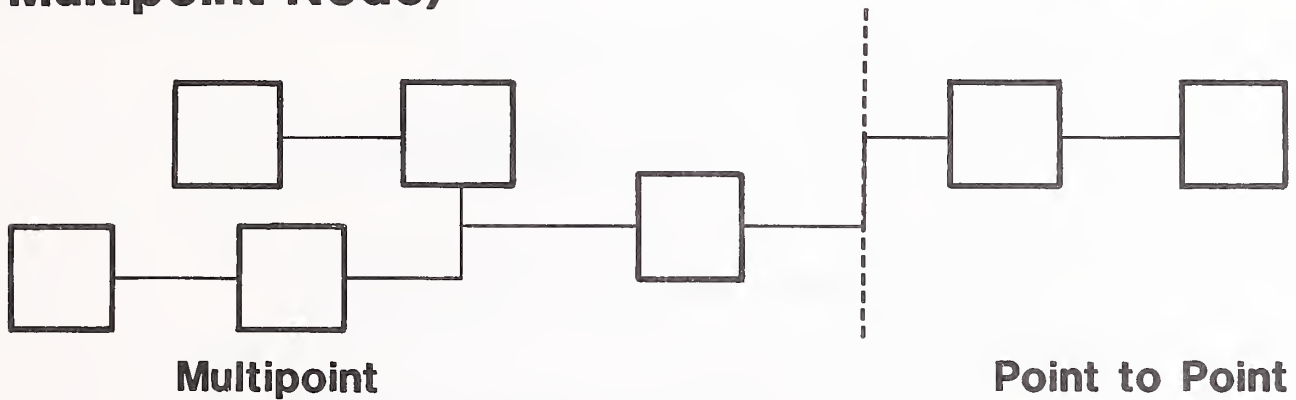
- This executive summary is designed in presentation format in order to:
 - Help the busy reader quickly review key research findings.
 - Provide an executive presentation and script that facilitates group communications.
- The key points of the report are summarized in Exhibits II-1 through II-8. On the left-hand page facing each exhibit is a script explaining the exhibit's contents.

A. DATA NETWORKS ARE GROWING IN COMPLEXITY

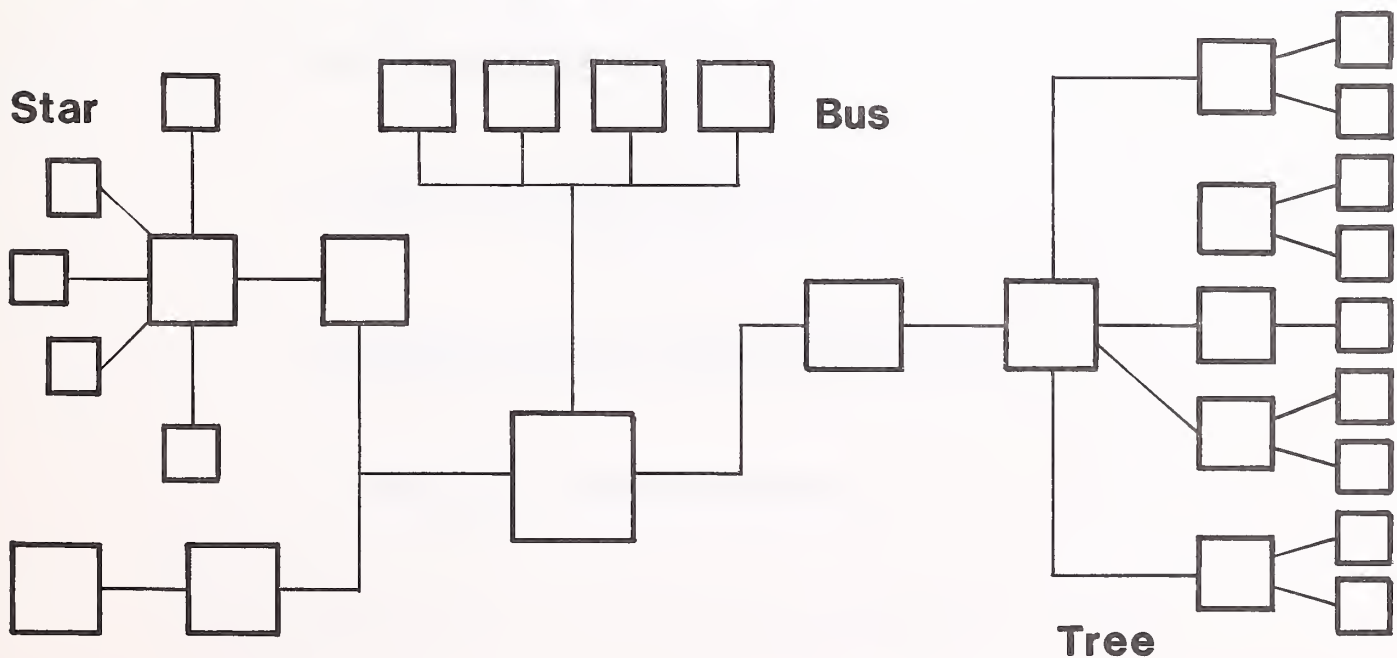
- Data networks are becoming increasingly complex. Digital backbone circuits have become more widespread: 19,200 bps point-to-point circuits now exist; 9,600 bps multipoint circuits are almost commonplace; and network complexity continues to grow.
 - More and more, distributed processing is being incorporated into data networks with a mixture of programmable concentrators, statistical multiplexers, and sophisticated data modems, comprising an extremely heterogeneous network environment. Instead of just the point-to-point and multipoint networks of previous years, we now have such sophisticated topologies as bus, star, and tree networks.
 - Automated testing, diagnostic microprocessors, central network management processors, predictive trending, etc. are all being tied into the new topologies, thus becoming part of modern network management and control systems. In the illustration, individual boxes can represent test equipment, microprocessors, distributed data processing terminals, etc. Combinations of any of these elements might represent equally valid configurations.
- A network management system must be able to handle the complexity of today's data network environment and anticipate those future requirements dictated by increased use of local area networks, satellite communications, cellular radio, dedicated microwave, fiber optics, etc. All these functions can be simultaneously incorporated into existing topologies and configurations.
- In addition, the newer network management systems will be required to address the growing trend toward interconnection of diverse networks (e.g., bus into star, or star into tree), including the combination of voice and data through such common network components as the new integrated voice/data digital PABXs.

DATA NETWORKS ARE GROWING IN COMPLEXITY

Networks 30 Years Ago (Point to Point with a Multipoint Node)



Typical Current Network Configuration (Star, Bus, and Tree Topology Shown)



B. NETWORK MANAGEMENT MUST BE MULTIFUNCTIONAL

- The network management systems suitable for efficient network control and monitoring through the 1980s will include such functions as:
 - Analog and digital link monitoring.
 - Terminal monitoring.
 - Monitoring of gateway and other interfaces.
 - Monitoring of intelligent processors and switches.
 - Multiplexer monitoring.
 - Communication link backup.
 - Communications equipment backup.
 - Automatic circuit restoring and network configuration.
 - Extensive automatic test functions to supplement manual testing.
 - Trend analysis and predictive diagnostics.
 - Remote control of network components.
 - Decentralized control and monitoring of system operation.
 - Redundant control and monitoring functions.
 - Data base management of network links and equipment.
 - Report generation.

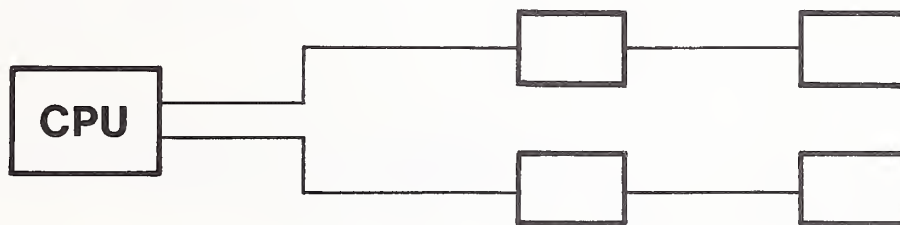
NETWORK MANAGEMENT MUST BE MULTIFUNCTIONAL

- **Monitoring**
- **Link and Equipment Backup**
- **Circuit Restoring**
- **Extensive Test Functions**
- **Trend Analysis**
- **Redundant Control**
- **Data Base Management**
- **Report Generation**

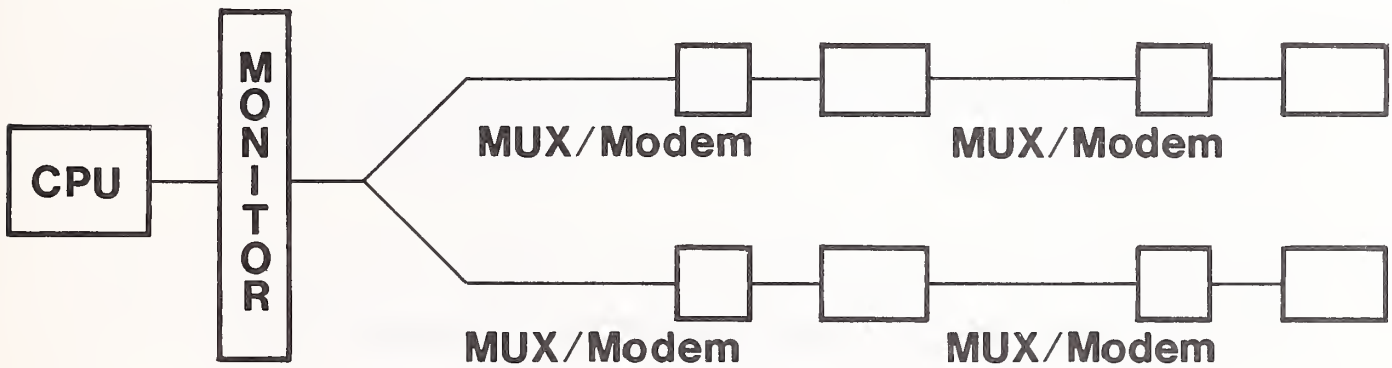
C. THE ROLE OF NETWORK EQUIPMENT SUPPLIERS IS CRITICAL

- The vast majority of business in the network management systems area will be captured by suppliers of major network equipment such as modems and multiplexers.
 - Manufacturers that provide the network management system as a standalone product will be competing in a difficult environment, since most customers seem to prefer obtaining their network management capability from suppliers of other network components, thus ensuring smooth integration into a "total systems" approach to network design.
 - This trend toward obtaining network capability from other system component suppliers is heightened by the fact that many network components are now being developed with self-diagnostics.
 - Thus, any network management system installed must interact with the individual components.
 - This interaction and interrelationship is much easier if the network management system is provided by the same supplier that provides the individual network components.
- For these reasons it pays to work closely with network suppliers that can support your efforts, and in whom you have confidence.

THE ROLE OF NETWORK EQUIPMENT SUPPLIERS IS CRITICAL



Network without Help from Supplier



Network with Supplier's Help and Support

D. WHICH DIRECTIONS ARE NETWORKS TAKING?

- A wide variety of technical control centers is now available, including standard patch panels, switch and monitoring modules, and sophisticated diagnostic equipment.
- In the more complex networks, modem suppliers provide a high degree of automation within their own equipment.
- The new network control systems are able to function within multipoint and distributed processing networks, isolating faults that may occur anywhere in the network. More detailed information concerning network operations is available for integrated network control and management systems, making it easier to manage and modify network performance.
- Typically, a network control system is a computer-based arrangement that supervises and monitors all operations of the network in real time, isolating faults and indicating specific requirements for network service action.
- Network management systems involve software that assimilates network characteristics and performance data and translates them into meaningful management reports.
- This information is used to predict trends, anticipate problems, and accumulate information essential to management in a dynamic network environment.

WHICH DIRECTIONS ARE NETWORKS TAKING?

- **Increased Technical Control**
- **Increased Complexity**
- **Increased Information Reporting and Statistics**
- **Increased Delegation of Responsibility (and Blame!)**
- **Increasingly Effective Software**
- **Better Management Reports**

E. WHAT A NETWORK CONTROL SYSTEM IS—AND ISN'T

- A network control system generally consists of a master controller at the central computer site. This controller communicates with each modem in the network, gathering status and operational data.
 - Diagnostic and control commands can be transmitted through the network without interrupting regular data traffic.
 - CRTs are typically employed at the central site to aid the operator in identifying and resolving network problems.
- The network control system typically operates in automatic monitoring mode, in which each remote modem is polled in sequence and the operators are alerted in cases of exceptional conditions.
 - Once the operator is alerted to an exception in network performance, a variety of diagnostic tests can be run to isolate the fault and to point toward corrective action.
 - Corrective action might include initiating dial backup, patching in a spare modem, or disabling a streaming modem.
- Network control systems are not limited to capacity planning or performance measurement and evaluation statistics, but they have a broader, more useful capability.

WHAT A NETWORK CONTROL SYSTEM IS -- AND ISN'T

IS

- **Line Monitoring**
- **Event Recording**
- **Statistics Gathering**
- **Statistics Storing**
- **A Troubleshooting Tool**
- **A Fault-Isolation Tool**
- **An Error Detection and Recording Tool**

ISN'T

- **A Documentation Generator for Word Processing**
- **A Fault Locator for Blame in Case of Failures**
- **A Club to Beat the Technical Staff With**
- **An Excuse for Managerial Short-Sightedness**

F. THE ROLE OF CONTROL IS CRUCIAL

- The network control center (NCC) monitors the operational status of the entire network and serves as a central point for network diagnosis and repair. In addition, the NCC coordinates new network facilities and collects network traffic and billing data.
- The NCC has the two major functions of collecting network traffic data and monitoring and controlling the status of network operations.
 - The control center collects statistical and traffic data related to the network. This data is used to develop various user reports indicating traffic patterns and changes. It is also used for network engineering.
 - Failures of the network are automatically reported to the network control center.
 - The center has highly trained personnel who are able to pinpoint the network problems and dispatch field maintenance technicians when necessary.
- Each interface processor examines itself periodically under appropriate software controls and forwards examination results to the network control center. The network control center computer reviews these reports and initiates repair activity when failures are indicated.

THE ROLE OF CONTROL IS CRUCIAL

- **The Network Control Center**

 - Monitors the Network**

 - Centralizes Diagnosis and Repair**

 - Coordinates New Facilities**

- **Major Functions Include:**

 - Collecting Traffic Data**

 - Controlling Network Status**

 - Providing Trained Personnel**

 - Reviewing Network Failure Reports**

G. NETWORK CONTROL WEARS MANY HATS

- In addition to detecting and reporting system failures, the network control center performs other functions.
- The NCC collects data on traffic and port usage for subscriber billing.
- It controls the switching of standby network equipment.
- The NCC is also responsible for monitoring:
 - The central office environment including air conditioning, power, physical access, etc.
 - Line error rates and remote loopback testing.
 - Traffic volumes and network blockage conditions to provide advance warning of additional network capacity requirements.

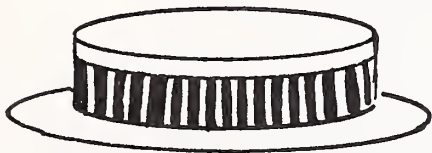
NETWORK CONTROL WEARS MANY HATS



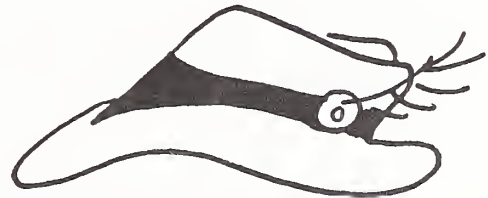
Subscriber Billing



Monitoring Environments



**Telecommunications
Monitoring**



Switch Control



**On-Line
Testing**



**Traffic
Monitoring**

H. DATA NETWORKS MUST BE MANAGED

- In order to properly manage and control these complex data networks, network management systems must be much more sophisticated than in the past.
- To build an effective network management system, determine which of the many functions you will require, and get those that offer the widest control into place first.
- Network supplier support can make your job easier, but only if it de-emphasizes the "sell" and concentrates on the sale. In the future, actual network performance data will be fed back into the network so as to permit optimized network performance.
- Watch out for the increased output reporting capabilities of network management and control systems. You could get buried in statistics, meaningless reports, and blame placing.
- Determine which areas of control are most important, and then develop procedures to track those areas. Consider the following: type of problem, personnel assignments, computer port testing, loopback testing, isolation procedures, diagnostic testing, and transaction logging.

DATA NETWORKS MUST BE MANAGED

- **Be Aware of the Advances in Network Management and Control Systems**
- **Determine Critical Functions**
- **Work With Network Suppliers and Get Feedback**
- **Control Reporting Functions – – Don't Let Them Control You!**
- **Determine Critical Areas**
 - **Develop Procedures**
 - **Isolate Problems**
 - **Log Transactions**

III TECHNOLOGY REVIEW AND ANALYSIS

A. INTRODUCTION

- Network control facilities are normally incorporated into data communications systems to provide a means of monitoring components and the facilities (e.g., lines, modems, multiplexers, terminals, and related equipment); to determine quality of lines, status of components, and cause of failures; and to allow restoration of failed portions of the system.

- Such control facilities were around long before computers came into existence. Historically, network control facilities are responsible for the physical and electrical integrity of the transmission line or circuit.
 - The primary function of a tech control facility is to bring all the lines from computers, modems, and common carriers to a common interconnect panel.

 - This allows the technicians to monitor the physical and electrical characteristics of the equipment or line terminated in the panel to see if the quality of lines and equipment performance meets acceptable levels.

- Modern network control facilities are usually monitored and controlled from a console located within the network control work area. The console contains

manually operated patch panels that terminate equipment and communications lines at the control facility, plus test and monitoring equipment, which can be patched into the line or equipment to isolate problems.

- Network control provides control of the equipment terminated at the central data communications site and of equipment on the other end of lines that are terminated at the central site. Users who want to monitor and control lines and equipment on a remote portion of a large data communications network not connected to the central computer site must configure the network control facility to monitor all remote processor nodes of the data communications network.
- This report treats various aspects of networking, technical control, and network management. The magnitude of the system's network control facility will be dictated by the data communications system's requirements.

B. ELEMENTS OF THE NETWORK CONTROL

- A network control system is defined as:
 - .. A computer-based system.
 - Owned (or leased) and operated by the user.
 - Independent both of host (and front-end processor) applications and of outside transmission facilities.
- This system:
 - Monitors the network's components.

- Records information on those components' status.
- Displays information for the operators' attention and action.
- Maintains one or more data bases of network status, configuration, inventory, and history.
- Generates reports for management based on information in those data bases.

C. REQUIREMENTS OF CONTROL

- The computer that drives a network management system can be a built-in (on-board) microprocessor, a personal computer, or a medium to large, dedicated minicomputer.
 - Minicomputer-based network management systems are centrally controlled by the minicomputer built into the system--not by a machine externally located.
 - Some microprocessor-based systems are completely modular, sometimes to the degree that a single microprocessor controls and monitors each line.
- Some mainframe vendors, notably IBM (with its Network Communications Control Facility (NCCF)), offer network management facilities that run on their mainframes and front-end processors. Such packages are not standalone systems, but components of mainframe systems.
- All network management systems include some mechanism for monitoring the network's components. When the network management system vendor also

manufactures modems, the vendor usually designs the monitoring device as a built-in modem feature, eliminating the need for the user to acquire separate monitoring devices.

- On other systems, standalone monitoring devices must be attached to modems or multiplexers at each remote site. In most network management systems, these devices can monitor only physical information on the status of the modem or multiplexer, its interface with the terminal equipment, its interface with the transmission facility, and the condition of the transmission facility.
 - Information on the modem or multiplexer and its interfaces comes from the presence or absence of signal on various Electronics Industry Association (EIA) interface leads.
 - Information on the transmission facility comes from the measurement of various analog parameters such as signal level, noise, distortion, phase jitter, and line hits.
 - If a given interface signal or analog characteristic falls out of specification, the system's monitors set off an alarm to notify the operator of a failure.
- Advertising sometimes exaggerates the potential of relatively simple monitoring and alarm systems, especially if they have all the features mentioned above. Companies frequently advertise them as network management systems, but a true network management system supports a number of higher-level services in addition to monitoring and alarm functions.
 - A network management system records and processes information from its monitors as well as information on the network's configuration supplied by managers and operators.

- It maintains an active data base of configuration, history, and component status from which users can extract standard or custom reports to identify chronic or recurring problems, project future trends in network use and traffic, and establish general policy based on detailed information.
- Network management systems share this function with a number of other turnkey decision support facilities for specialized applications, such as building and laboratory management.
- Some network management systems also include the ability to switch automatically from a failing component to a "hot" standby unit, either in response to an alarm or on command from the operator.
- Some also include the ability to bypass a failed communications line by placing a call automatically over the switched voice network. Such automatic dial backup procedures require two switched-network calls for full-duplex operation.

D. CONTROL CONFIGURATIONS

- A minimal network management system consists of a central processing unit, a hard disk or diskette storage device, an operator's console, and a set of local and remote monitoring devices.
 - The central processor may be a single minicomputer or may contain a number of function-specific microcomputers.
 - The operator's console is often a color CRT, although some systems use only monochromatic displays. In most systems, the operator station includes a printer; some may also include a color plotter for graphic information.

- The nature of the monitoring devices depends on the native market of the system's vendor.
 - Systems from modem vendors such as Intertel, Racal-Milgo, Paradyne, and AT&T use diagnostic monitoring facilities built into the modems.
 - Systems from some other vendors (e.g., Avant-Garde Computing and Emcom) use independent monitors installed at the interface between the modem and the terminal equipment, between the modem and the network, or both.
 - Devices that monitor both sides of the modem are said to "wrap around" the modem.
 - At least one vendor, Codex, provides both alternatives: integral diagnostics in its own modems and wraparound devices for use with other vendors' modems.

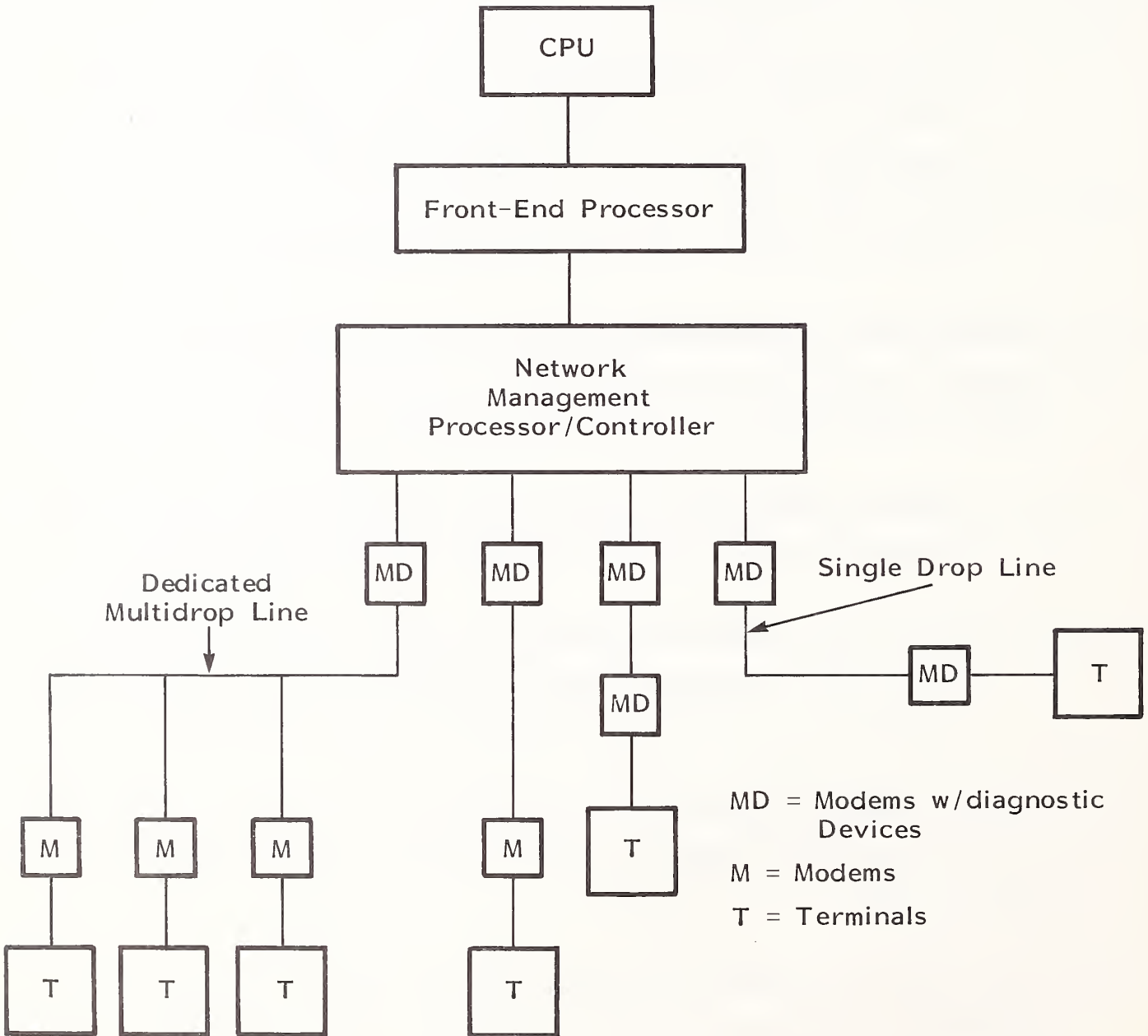
- The network management processor usually resides at a central site along with the network's host computer.
 - Remote monitoring devices communicate with the network management system by one of two techniques:
 - In the mainstream technique, favored by IBM and other vendors of host-based network management packages, the central site unit (either the host processor or an independent network management processor) polls the remote devices (modems or diagnostic units) in a dedicated time slot over the main data channel. (Note that the terminals are connected to modems that may or may not have diagnostic capabilities built in. These, in turn, are connected to the network via single or

multidrop lines. Also note that modems are required on either side or end of the line.)

- . In the sidestream technique, favored by most modem vendors, the remote devices transmit diagnostic information asynchronously over a special low-speed data channel that has been frequency-division multiplexed onto the same facility as the main data channel.
- Some network management systems, usually marketed by test instrumentation vendors or network management system integrators, can support either mainstream or sidestream monitoring.
- Exhibit III-1 depicts a typical network management system.
- The mainstream technique lends itself well to end-to-end monitoring at the application level, since it is often directly in touch with the network's equipment, from host processor to modems and terminals.
 - Host-based mainstream systems have a singular disadvantage: when the host goes down, the network control system goes down with it.
 - Some believe that the network itself is useless without its host. But in many modern distributed processing systems, the network can support a high level of activity even in the absence of a controlling host.
- The sidestream systems are somewhat quicker to report modem, terminal, and communications line failures, since the monitors need not be polled in order to report trouble.
- The sidestream technique also offers a greater chance of survival over degrading communications lines, since a low-speed signal is more likely to reach its destination intact over a noisy or hit-prone channel.

EXHIBIT III-1

TYPICAL NETWORK MANAGEMENT SYSTEM



E. NETWORK CONTROL FUNCTIONS

- The basic functions one should expect from a network control system fall into three general categories:
 - Failure management.
 - Performance management.
 - Configuration management.
 - Functions in any of these categories can serve on two levels: the operations level and the management and planning level.
- Failure management can be reduced to two functions: problem determination and system restoral.
 - The problem-determination facilities of a network management system can alert the operator to a failure, and in more sophisticated systems to a degrading condition, by using a scheme of alarms.
 - When a local or remote monitor detects a problem, it activates an alarm at the operator station.
 - Front-end processors, modems, switches, and multiplexers ordinarily provide a very primitive form of failure alarm: the "carrier detect" light will normally go off on a supposedly active line when the line fails. This is a negative alarm and is rather easy to ignore. Network control systems typically provide a positive alarm signal, usually a message at the operator's console noting the type of device malfunctioning, the location, and the nature of the failure.

- Some systems activate alarms for degrading conditions as well as for absolute failures.
 - Systems with color displays use a special color, usually red, for alarms.
 - Color systems with multilevel alarms use green or blue for normal conditions, yellow for degrading conditions, and red for failures.
- System restoral is a two-stage process.
 - For the short term, the user must find a way around the problem.
 - For the long term, the user must repair the failed component or replace it permanently.
- Some network management systems incorporate a fallback switching mechanism by which an operator can immediately replace a malfunctioning device with a "hot," or ready-to-go-on-line, backup unit.
- For modems, multiplexers, terminals, and front-end processors, the backup units are available from a pool of spares, with one spare ready for a given number of active devices.
- For communications lines, the ready backup is usually the switched telephone network.
- Most network management systems provide some automatic fallback switching, usually as an option.

- Some offer only manual fallback through a patch panel.
- Automatic switching can be either electromechanical or programmed.
- Several switching configurations are possible.
 - The A/B technique switches a single line between two devices, the malfunctioning unit and its one-for-one spare.
 - One-by-N configuration switches a specified group of lines between a multiline controller and its redundant backup, such as a spare front-end processor.
 - In N-by-N and N-by-M techniques, any line within a specified group of lines can be switched among any of a given set of devices; the number of lines may be greater or less than the number of devices.
- Fallback switching is a short-term answer to network problems. For long-term repair or replacement of faulty parts, network control systems provide two kinds of help.
 - The first, available in most systems, is a facility of one sort or another for detailed testing to further isolate problems that have generated alarms. Some systems provide an integral test facility, while others merely provide access ports for the attachment of independent monitor and testing devices.
 - The second is a management device: the trouble ticket data base.
 - Paper trouble tickets have long been a mainstay of network and computer operations.

- . Basically, a trouble ticket is an expanded version of a system log entry. It contains information on the date and time of a problem; the nature of the problem; the specific devices and facilities involved; any short-term actions taken to relieve the problem; the name of the operator who took the action; and any recording follow-up information such as visits from the vendor's maintenance staff, dates on which parts were returned for repair, serial numbers of spares installed, and the date of the problem's final resolution.
- A trouble ticket data base extends the logging and historical function of the trouble ticket to the management and planning level. The manager can call up reports on:
 - All outstanding trouble tickets.
 - All trouble tickets involving a certain subset of the network.
 - All trouble tickets recorded or resolved within a given period.
 - All trouble tickets involving a specific device or a specific vendor.
 - All trouble tickets over a given period not resolved within a specific time.
- Trouble ticket reporting is normally user defined and systems installed (by systems personnel). With such reports, a manager has an objective handle on such factors as the reliability of a given component, the promptness of a given vendor's field service, the reliability of a given operator, and the general proneness of certain segments of the network to failure.
- Performance management deals with the up-and-running network from two viewpoints, response time and availability.

- Most network management systems measure response time at the local end, from the time the monitoring unit receives an "enter" or "end of transmission" signal from a given unit to the time it receives and passes a response back to that unit.
- Some systems can measure end-to-end network response time at the remote unit.
- In either case, the network management system displays and records response time information and generates user-specific response time statistics for a particular end-user device, line, or subset of the network; or for the network as a whole, in real time or over a specified period.
- More sophisticated performance measurement systems can split the overall response time for any of those subdivisions into external network utilization time and computer internal response time.
- Systems with color graphic consoles can display elaborate multicolored network schematics.
 - Specific colors may be assigned to different levels of response time, with blue or green for normal operation, yellow for degrading response time, and red for critically high response time.
 - As with failure alarms, operators can use this information to re-route traffic and to patch in additional resources.
- Availability is a measure of actual network uptime, either as a whole or by segments. Availability statistics can include such measures as total hours available over time, average hours available within a period of time, and mean time between failures.

- With long-term response time and availability statistics massaged and formatted by the network management system, managers can identify current trends in network use, predict future trends, and plan the assignment of resources for specific present and future locations and applications.
 - Managers can also isolate and analyze chronic bottlenecks in specific areas and components.
 - When an application runs over its allotted time (as determined by the user's program or by other externally applied criteria), management should either install more terminals and assign additional personnel, or install faster communications to improve network response time.
 - Response and availability information from a network management system provides an objective tool to solve the problem.

- Configuration management involves both failure management and performance management, along with long-term planning of the network's topology and inventory.
 - Some network control systems provide cost and depreciation information on the network's components in conjunction with the trouble ticket function.
 - Most systems provide an inventory data base with information on both active and spare parts.
 - When properly used, the network control system gives managers objective backup for decisions on purchasing and expansion.

F. THE VENDOR'S ROLE

- Three kinds of vendors--large modem and multiplexer manufacturers, communications test equipment specialists, and network management system integrators--supply network management systems.
 - Each type of vendor supplies a different kind of network management system.
 - The modem vendors consider network management to be a value-added function atop their product lines.
 - The test equipment vendors see network management systems as "top-of-the-line" integrated test systems.
 - For the system integrators, network management systems are often their sole product.
 - Each type of network management system supplied by these three different kinds of vendors has inherent advantages and restrictions.
- The modem and multiplexer vendors, such as Intertel, Paradyne, Codex, Racal-Milgo, and AT&T Information Systems (formerly American Bell), are strongest in end-to-end monitoring and alarming, and weaker in fallback provisions and long-term performance measurement.
 - These vendors concentrate on selling modems and multiplexers and see the network management function chiefly as a way to sell more of those devices.
 - In most cases, these systems will work only with remote devices from the same vendor and can lock a user into a single-vendor network.

- The increasing availability of end-to-end digital communications may soon affect the market for modem-based systems.
 - Users whose plans include large-scale conversion to digital transmission may be reluctant to invest in a potentially obsolescent modem plant.
 - Vendors might answer this objection by providing equivalent diagnostic support in future digital data service units (DSU).

- The instrumentation vendors' systems, such as those from Atlantic Research, Digilog, and Dynatech, are strongest in fallback switching and local-end testing and monitoring.
 - They have evolved from the traditional world of tech control, so they offer little threat of being locked into a particular vendor. However, these systems sometimes require more elaborate arrangements for remote monitoring than the other vendors' products.
 - The remote monitoring unit may be a version of the vendor's standard integrated test set. Such devices are usually more versatile, but are much more expensive, than simple modem diagnostics or wraparound devices.

- The network management system integrators--such as Avante-Garde Computing, Emcom, TITN, and Tesdata--concentrate on software.
 - Their systems provide the best data base management and reporting capabilities and the most elaborate alarms and displays.
 - The systems' strongest asset is performance measurement, with the ability to produce lavishly detailed response and availability statistics.

- These systems usually carry the highest up-front cost for the centralized system, but their incremental costs for service to additional lines falls between the costs for modem vendors' systems and tech control vendors' systems.
- These system integrators' systems are also the most versatile. But full use of their versatility may require that the user program (or custom order) any really fancy, high-level management applications.
- Within these general perspectives and qualifications, most vendors offer ranges of systems to suit individual needs.
 - Prospective users can find systems geared to 16-line networks and systems that can expand to serve up to 1,000,000 lines.
 - Some vendors also offer different functions as increments; entry-level users can start with any one function and add others in any order as their networks grow in size and sophistication. For example, a user can begin with a simple fallback switching system, add remote monitoring, and then add data base management.

G. TECHNICAL CONTROL

- Technical control equipment selection should be part of the overall system design requirements. The various features selected to meet the system requirements will in turn dictate the equipment requirements to meet the need.
- In building a network control facility, a number of areas should be reviewed and analyzed. The following checklist provides some guidance for managers or users. The items and features they need to be concerned with are:

- Modems.
 - . Bust back capabilities.
 - . Error detection.
 - . Detection of signal deterioration (carrier failure).
 - . Bit pattern generation.
 - . Bit rate speed, change capability.
 - . Line conditioning capability.
 - . Bit storage.
 - . Data scrambling.

- Test jack panels.
 - . Monitoring capability.
 - . Patching capability.
 - . RS232 signals to be controlled/monitored.

- Monitoring and testing devices.
 - . Manual.
 - . Automatic.

- . On-line or off-line features.
- . Visual display capability.
- . Printouts.
- Report generation (manual or automatic).
 - . Analytical.
 - . Data flow statistics.
 - . Error statistics.
 - . Maintenance alert--immediate trouble report.
- Line and equipment swapping requirements.
- Line diagnostics.
 - . Character patterns.
 - . Bit patterns.
 - . Fault isolation.
 - . Test data.
 - . AC test capability.
- Data statistics.
 - . Transaction sizes.

- . Transmission types.
- . Transmission times.
- . Line type utilized (variable line type system).
- Error statistics.
 - . Character parity error counts.
 - . Bit error counts.
 - . Block retransmission counts.
 - . Control sequence error counts.
 - . Handshaking failure counts.
 - . Erroneous disconnects (dial-up lines).
- Line loopback capability.

H. NETWORK MANAGEMENT

- A communication data system normally consists of a network of lines and terminals--a network that provides the means for inputting data into a data processing system. This network requires the same operational management consideration as that given to the main data processing system.

I. NETWORK TROUBLESHOOTING

- Troubleshooting guidelines for operational or maintenance purposes should be defined and readily available to those responsible for network management. The guidelines should include individual line terminal layout information. This is necessary to determine causes of failures and to accomplish quick line and/or terminal restoration.
 - Troubleshooting guidelines should answer the following questions:
 - What test procedures can be performed in order to isolate the problem? (Procedures should be included for testing capability of terminals, modems, and computer sites, as well as testing equipment availability.)
 - Can the problem be isolated to a major area (computer site equipment, communication lines, modem, or terminal)?
 - The guidelines should cover different types of problems.
 - Parity errors (intermittent or solid).
 - Carrier failure (modem or line equipment).
 - Multiterminal difficulties.
 - Dial-up problems.
 - Terminal equipment problems.
 - Individual RS232 signal breakdown.
 - Computer site equipment failure.

- Troubleshooting guidelines should also contain past history records for communications lines, modems, terminals, and computer components.

2. PROCEDURAL CHECKOUT

- In addition to the troubleshooting guidelines, procedures may be required to give step-by-step instructions to operations and maintenance personnel.
- Procedures should be given for terminal, input, or output failure.
- Instructions should be provided for isolating the terminal and lines from the computer equipment.
- In addition, the following information should be included in the procedures guide. Read these items as an extract from such a procedures guide.
 - If automatic loopback features are on the line:
 - Place a loopback at the EIA output in the computer equipment, perform data test patterns from the software, and check return pattern for errors (computer equipment confirmation test).
 - Perform a loopback at analog side of computer site modem and transmit test pattern; this tests computer site modem.
 - Perform a loopback at analog side of terminal modem and transmit test pattern; this tests the equipment and lines up to the terminal.
 - Perform a loopback at digital side of terminal modem and transmit test pattern from computer and return pattern; this tests the terminal modem.

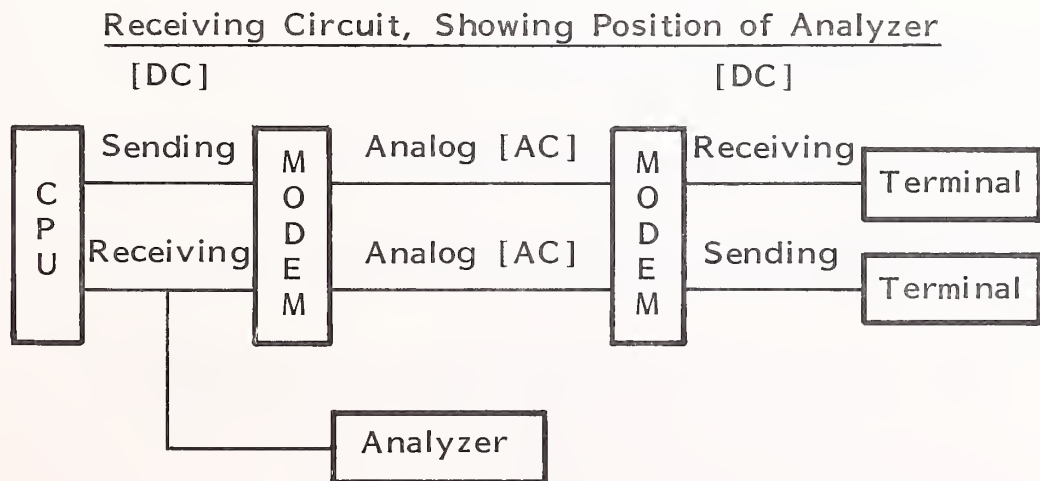
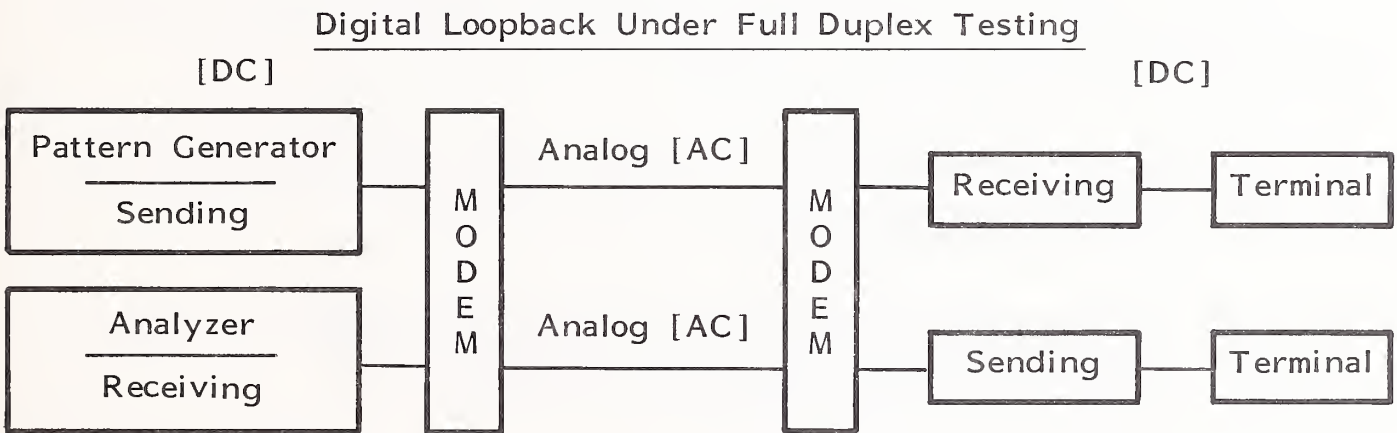
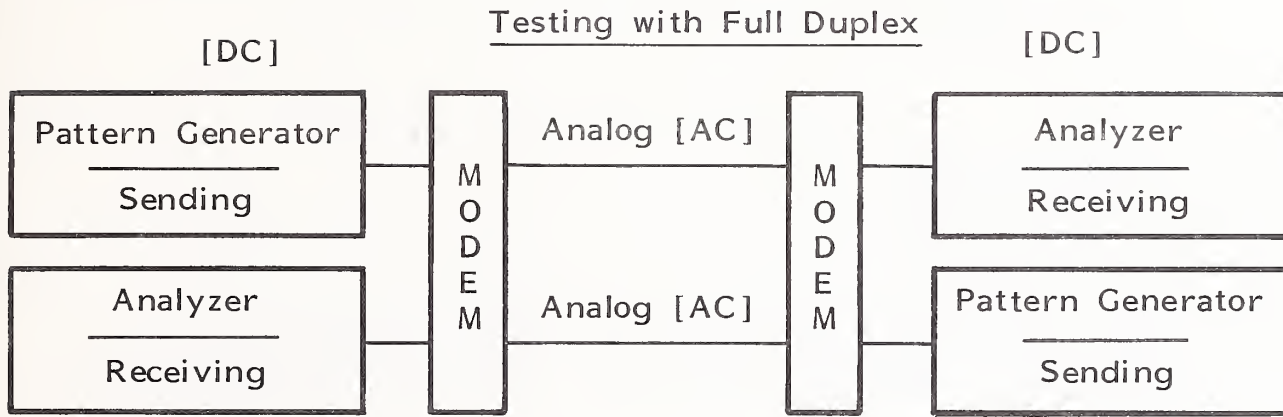
- Perform a loopback at terminal controller, transmit the pattern from computer, and test returned pattern; this tests the terminal connectors, cabling, and jack panels.
 - Send message to terminal for retransmission of original data or test to central site; this test identifies problems in the terminal controller or devices.
- If no automatic loopback features are available or the trouble is not clearly isolated by the loopback testing:
 - Measure analog levels at the central site.
 - Measure circuit delay. Arrange for a loopback at the terminal modem analog side, transmit test data, and measure the propagation time delay of data bits returned to the central site. This test shows if any major reroute of the circuit has occurred in the common carrier facilities and determines if conditioning may be necessary.
- If test equipment is available at the terminal, measure the levels on the analog side of the modem.
- If it appears that a facilities problem does exist, call the common carrier facilities maintenance center (telephone company repair center).
- If the error rate has been increasing and the circuit has been worked on substantially, and if error rate measuring equipment is available at either end of the line, it may be advisable to reestablish the error rate of the circuit by retransmitting a minimum of a million bits of information over the circuit with a parity type code set and either a Bit Error Rate Tester (BERT) or a Character Error Rate Tester (CERT).

I. TEST AND MONITORING EQUIPMENT

- The primary function of test and monitoring equipment is to provide a means of generating various data test patterns and the capability to analyze data patterns.
 - Several types of test and monitoring equipment are available. The equipment may provide displayed, printed, or graphic output information concerning the data under analysis.
 - Some equipment tests signal distortion, counts errors, provides accumulative error counts, gives failure alarms, and provides other individual features as required.
 - The equipment may provide the means to generate the necessary bit, character, or analog signals for testing.
 - Signal distortion may be introduced by the unit in order to check equipment operational margins.
- It is not necessary to provide individual monitoring or test equipment for each line connected to the computer.
 - With network control facilities or a simple patching panel, one or two monitoring or test units could be rotated across the network line connections as required.
 - Several equipment arrangements may be configured to generate test pattern data. Exhibit III-2 illustrates three possible methods.
- The computer hardware and software system can also provide test patterns and data testing features.

EXHIBIT III-2

CIRCUIT TEST CONFIGURATIONS



- Software tables can be established to store error counts, and those tables could be utilized to produce reports or sound alarms.
- A test pattern could be produced by software when maintenance testing is required.

J. LINE CONSIDERATIONS

- Many factors enter into the line selection process. Some significant ones are cost, data bit rate, on-line time, convenience, and types of associated equipment.
- There are basically two types of lines available: dedicated (leased) and dial-up.
 - The dedicated line bit per second (bps) rate is limited only by the type of line and associated equipment.
 - The dial-up lines place a limit on the bps rate because of the common carriers' dial exchange and associated equipment.
- Dedicated lines provide the following features or capabilities:
 - Fixed monthly costs.
 - The availability of bps rates up to or in excess of 9,600 bps.
 - Line conditioning available from the common carrier.
 - Fixed routing, without exchange equipment being involved.

- The absence of common carrier foreign test or control tones.
 - No requirement for echo suppressors.
 - No requirement for dial access arrangements.
 - Full duplex lines (four-wire systems).
- Dial-up lines provide the convenience of dialing connections to many different locations and possible cost efficiencies in situations where low line usage is a system criterion. Dial-up lines provide the following features and capabilities:
 - Dial connection capability.
 - Limited bps rates (up to 4,800 bps and possibly to 9,600 bps--but usually below).
 - Variable monthly costs.
 - Conditioning not available from the common carrier.
 - Variable line routing due to telephone exchange trunk routing during the accomplishment of the dial connection.
 - Possible foreign tones introduced by the common carrier (e.g., a test probe or a telephone tap).
 - The possibility that echo suppressors may be part of the line equipment.
 - Possible signal level losses.

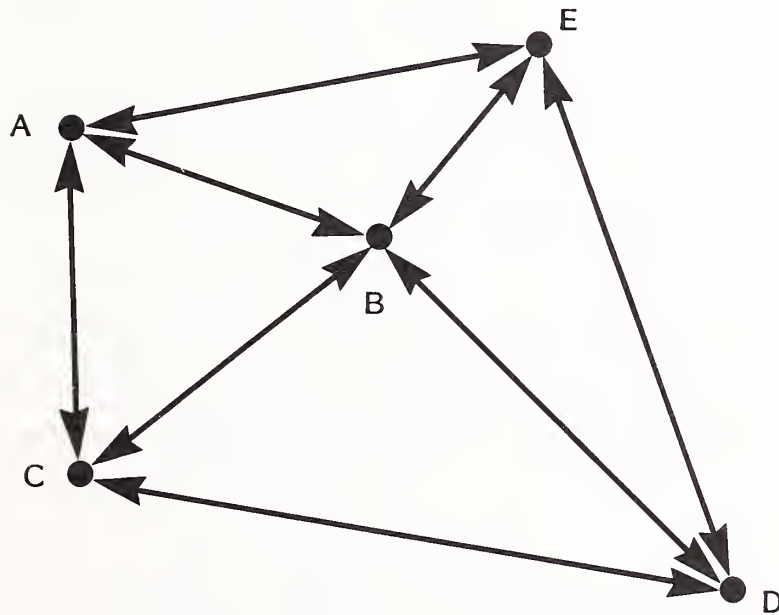
- The possible requirement of dial access arrangement equipment.
- Half duplex lines (two-wire systems).

K. LINE ROUTING

- The proper routing of the connecting lines to a group of terminals or remote computer systems is very important since dedicated (leased) line costs are based partly on line mileage.
- Each system configuration is unique and, therefore, requires that a study be performed to determine the best line routing and associated equipment requirements.
- A line matrix should be drawn to illustrate the required connecting lines and equipment. This illustration should provide a layout of the most efficient line routing and should indicate where to place concentrators or multiplexers to reduce the total line mileage.
 - The end result should be a combination of lines, multiplexers, concentrators, and other necessary equipment that may provide the lowest overall costs while maintaining efficiency of operation.
 - Exhibit III-3 provides a simple illustration of several different routings that may be used to connect five terminals together.
 - When line costs per mile are considered, it becomes clear that line routing can be very important.

EXHIBIT III-3

LINE ROUTING:
EXAMPLE OF MULTIPLE-PATH ROUTING



(Three Route Elements)	A to E	}	1,500 Miles	B to E	}	2,000 Miles	(Four Route Elements)
	A to B			C to B			
C to A	B to D						
	C to D						
(Two Route Elements)	D to C	}	2,500 Miles	A to D	}	3,000 Miles	(Two Route Elements)
	E to D			C to E			

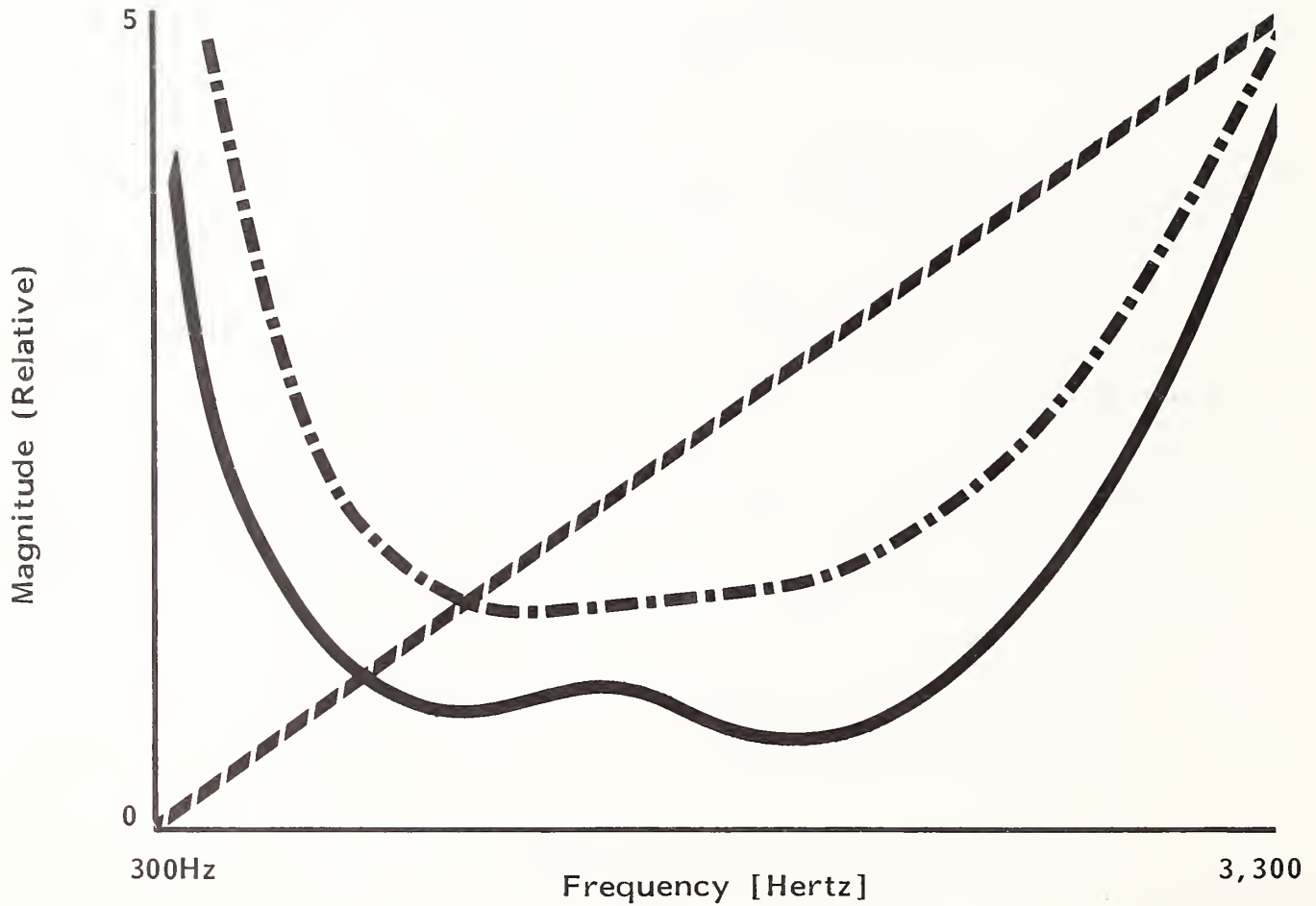
L. LINE CONDITIONING

- Several factors determine the ability, or lack of ability, to transmit data over common carrier or user-provided lines. These detrimental factors usually cause inefficient operation at the higher bps operations.
- Line conditioning or equalizing is used to overcome the line deficiencies (attenuation of carrier, echo suppression, white noise, etc.) that cause problems when operating in the area of 2,400 bps or 9,600 bps or higher.
- Three basic types of line conditions or equalizers are used. These are: compromise, prescription, and adaptive. Normally, these conditioners or equalizers are incorporated into the modem.
 - The compromise conditioner is preset to condition the nominal or average line. The inherent deficiency of this conditioner is that it may contribute to the existing line distortion average from one extreme or the other.
 - The prescription conditioner is manually set to compensate for the distortion on a particular line. This same type of modem conditioner may automatically compensate for one distortion found on dial-up lines.
 - The third type of conditioner has capabilities similar to the prescription type of conditioner plus a monitor feature that automatically provides continuous fine tuning for correction of line distortion.
- Rapid and accurate conditioning of lines can be expensive, but it does provide for increases in frequency bandwidth, which in turn allow higher bps rates. The amount of line conditioning will be dictated by the operational bps rate requirements.

- Line conditioners normally correct for amplitude attenuation, single delay, and phase shifting. Exhibit III-4 represents a typical unconditioned voice grade line. Three curves are used to illustrate the effects of amplitude, delay, and phase shifting on a feasible frequency range of 300 to 3,300 Hz.
- Exhibit III-5 represents the equal and opposite conditions possible by the introduction of a line conditioner. The line conditioner would be adjusted to provide approximately equal and opposite amplitude, delay, and phase shift.
 - In effect, the conditioner would amplify the received signal and correct for bit pattern delay and signal phasing.
 - This would create a constant condition across the total frequency range of 300 to 3,300 Hz and allow the highest possible bps range to be utilized.
- Exhibit III-6 illustrates the effect of several different levels of conditioning on a type-3002 grade line. C1, C2, C4, and D1 are all conditioning levels offered by a common carrier.
 - The C1 level of conditioning provides the narrowest usable bandwidth, and C4 provides the widest usable bandwidth.
 - The widest bandwidth provides the highest bps capability.
- Besides distortion, there are other types of problems that occur on the line and within the equipment connected to the lines.
 - These problems include time jitter, phase jitter, line hits, and frequency shifting.

EXHIBIT III-4

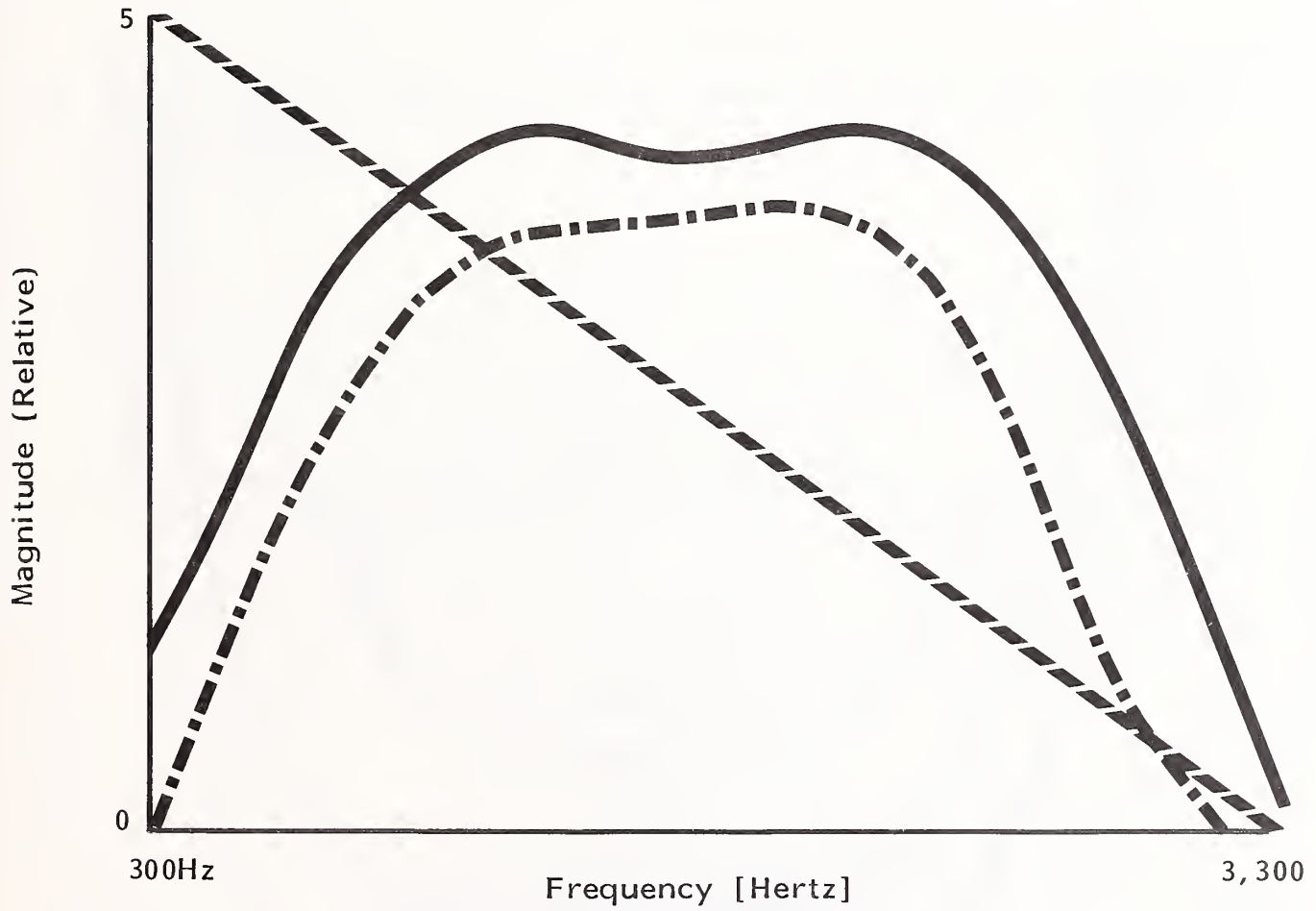
UNCONDITIONED VOICE GRADE LINE CHARACTERISTICS



-  Phase Shift Distortion
-  Delay Distortion
-  Amplitude Distortion

EXHIBIT III-5

DISTORTION CORRECTION USING CONDITIONING






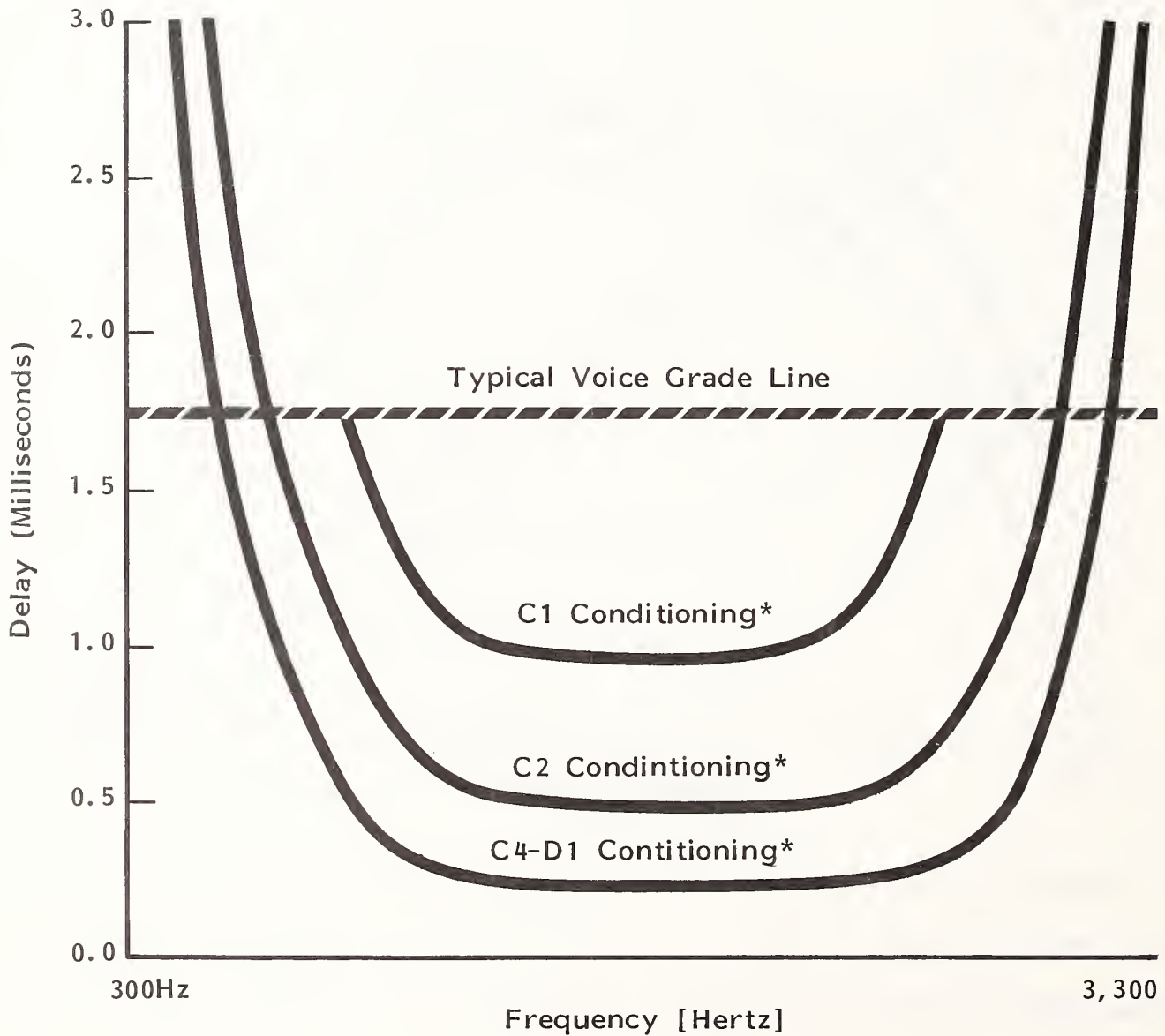
-  Phase Shift Distortion
-  Delay Distortion
-  Amplitude Distortion

EXHIBIT III-6

DELAY CHARACTERISTICS OF
VOICE GRADE LINE CONDITIONING



* Levels of conditioning on a type-3002 grade line.

- Some hardware problems can be corrected by improvements in equipment design.
- It may not be possible, through equipment design improvements, to correct hits on the line or other line interference caused by electrical impulses or human error. Compensation for errors caused by these problems may be handled by error detection and correction schemes.

M. THE SPECIAL CASE: NETWORK CONTROL CENTERS FOR PACKET NETWORKS

- Since control procedures based upon some algorithm generated within the system will not work in a packet-switching environment, it is necessary to consider packet switching separately from other network control activities.
- Over the past decade experience has shown that extremely good control and monitoring network performance can be achieved by a combination of a centralized, essentially passive network control center (NCC) coupled with a set of active controls applied as part of the protocol and software features of each switch.
 - Putting some of the control functions into the switches themselves achieves a large measure of distributed control, at least in making the basic operation of the network immune to the failure of a single control element.
 - Making the hardware of the NCC identical to that used by the switches themselves further increases reliability since, by a relatively simple reconfiguration of network assets, any one of the switches could assume the functions of the NCC.

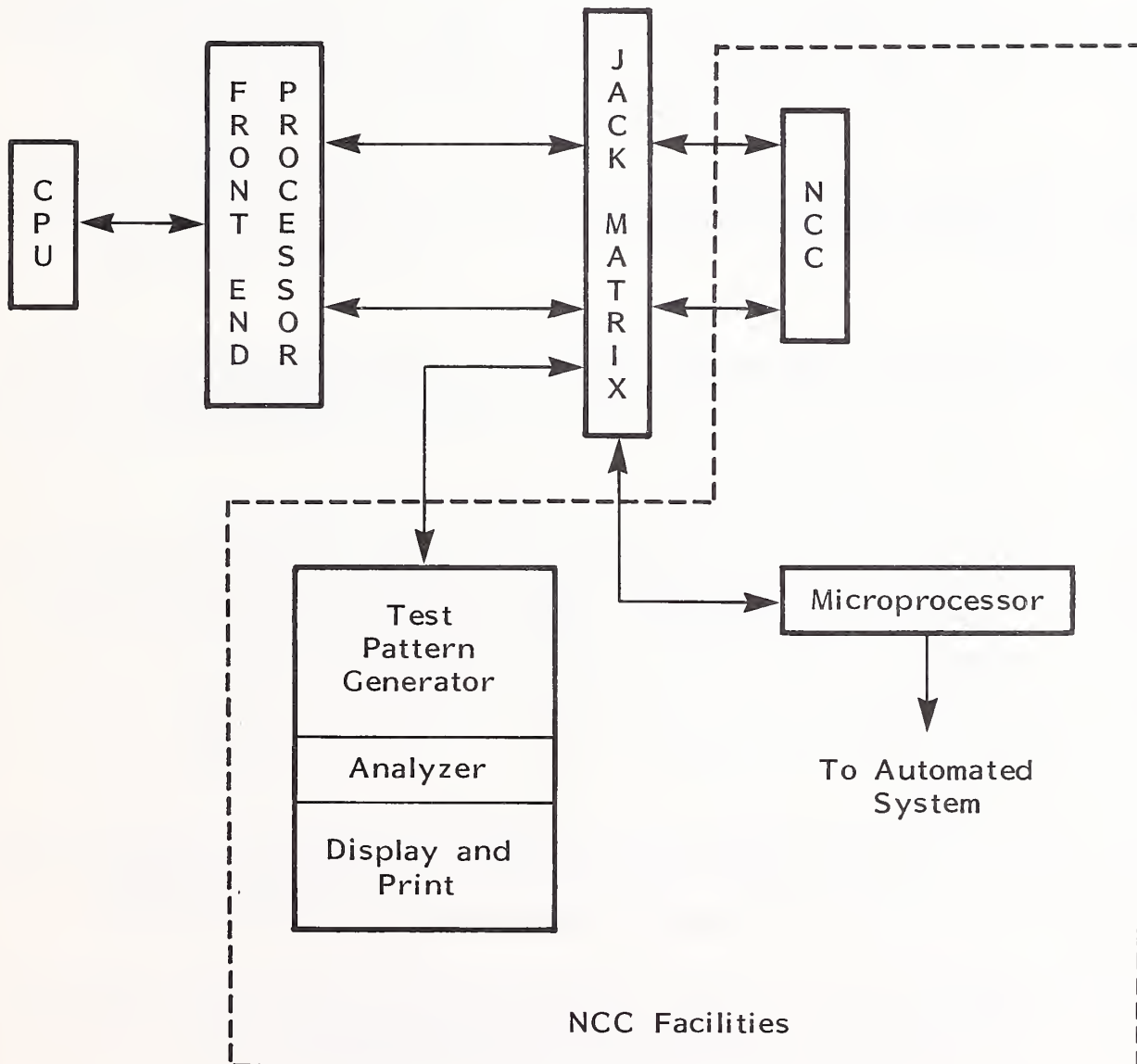
- Exhibit III-7 illustrates a typical configuration of network elements in which the NCC is outside the network boundary.
 - As a passive device with respect to the real-time networkwide flow of information, the NCC is coupled to the network as if it were any other host computer subscriber to the network.
 - For reliability, at least two such connections are provided to two different switches.

- The principal functions carried out by the NCC relate to the information gathering (abuse monitoring, collection of cost and billing information, collection of engineering data) that is part of all control functions.
 - The NCC provides long-term system control and operational direction to the switches and operators in the network.
 - It provides for long-term controls (such as traffic changes) and correlates and analyzes network disturbance data collected from many network locations to determine the cause of networkwide problems.
 - In addition, because the NCC is a single point with good visibility of the entire network, it can provide current status information to aid staff in dealing with totally unpredicted problems.
 - The NCC and its support staff thus comprise a kind of crisis management capability.

- To perform all these functions, the NCC collects disturbance indications, billing and traffic data, and performance data.
 - The disturbance indications include failure of either lines or switches, as detected by other switches, and security/privacy problems, as indi-

EXHIBIT III-7

NCC CONFIGURATION ELEMENTS



cated by excess message rejections, protocol errors, or unusual traffic patterns.

- The billing and traffic data is useful not only for revenue production but also to ensure a high degree of network integrity and traffic throughput.
- Long-term measurements of traffic data indicating that the network is delivering only ten percent of the traffic for which it was designed would suggest that the distributed control operation was faulty.
- The performance data relates to the monitoring of delay, peak load throughput, and call completion rates achieved by the network under varying traffic conditions.
 - This kind of information is part of the engineering data used for sizing network resources and reconfiguring resources when necessary to meet the actual traffic pattern.
 - In addition, since users will judge network service on the basis of the delay their traffic encounters, constant monitoring of this parameter is critical.

I. ROUTING AND FLOW CONTROL

- The real-time operations of control, which are distributed to the network switches, are implemented largely through dynamic routing techniques.
 - The principle employed is that each switch attempts to send its packets over the shortest (in time) path to the destination.
 - The key point is that the shortest path changes as the loading in the network changes.

- In addition, the shortest path, measured in terms of time delay, often is not the shortest in terms of distance.
 - The switches estimate the shortest delay path on the basis of information at each switch, together with delay information given to each switch by its immediate neighbors.
 - Under most loading conditions this distributes the traffic load and achieves the highest possible network throughput as new traffic is routed around congested areas, over lower-delay paths.
- The switches also control the traffic originated at each switch by use of the flow control mechanism.
 - When more traffic is in the network, response times and acknowledgements become longer.
 - The switches are designed to reduce this loading by reducing the flow control window, thus reducing the rate at which new traffic enters the network. Failures of lines or switches in the network are therefore recognized by the distributed control functions because of the large increase in apparent delay over a path utilizing a failed network element.
 - Proper operation of the routing and flow control protects the basic integrity of the network.
 - As long as a path exists between two users, it is possible for traffic to move successfully between those users.
 - If individual lines or switches fail, other network integrity controls, such as failure restoration and directory control, are the responsibility of the network control center.

2. NCC OPERATOR FUNCTIONS

- In most designs the NCC is implemented by hardware that corresponds to the switch hardware. However, it requires specialized control and monitoring software, as well as operators who can deal with unusual conditions.
- Set Parameters and Thresholds: Various network parameters, such as timeout period, frequency of routing table changes, or maximum allowable traffic buildup before flow control is applied, have to be changed from time to time, depending on network operating and local conditions. These changes are initiated and executed from the NCC, generally under direction from NCC operations personnel.
- Analyze Network Problem Indications: Although NCC software is designed to recognize anomalous conditions as reported by the switches, there is always the possibility of totally unpredictable problems or unusually severe combinations of problems. NCC operators will have to deal with these kinds of problems, taking short-term actions (such as initiating parameter changes) to reduce the impact in real time, and performing further analysis to prevent a recurrence.
- Initiate Performance Monitoring: From time to time, particularly in response to user complaints, it will be necessary to monitor the performance of some part of the network. The initiation of such monitoring and the collection and analysis of data will normally be done by NCC equipment and personnel.
- Report Production: The NCC will produce periodic reports on network performance, loading, and other factors as needed for the administration and engineering of the network.
- Respond to User Requests: The NCC will be the focal point for response to user requests for a change of service, addition or deletion of capability, and so on. The NCC will also respond to complaints about services rendered.

- Implement Directory Changes: The networkwide user directory and the directory of network assets and resources will be maintained by the NCC. Any changes in this directory, particularly in response to user requests, will have to be initiated and directed by the NCC.
- Maintain Network Data Base: The master data base, which would include network and user information as well as information about or copies of the software for each switch, will be maintained by the NCC.
- Modify Node (Switch) Software: The NCC can initiate and execute any changes to the software of the switches by performing a downline load via the network.
 - This avoids physically distributing hardcopy versions of the switch software and having personnel available at each switch capable of loading the new software.
 - Thus, the packet network is even more flexible since changes can be implemented easily and rapidly across the entire network.

N. NETWORK CONTROL SYSTEMS EXAMPLES BY MANUFACTURER

- Different companies have different approaches to the problem of network control systems.
 - I. IBM
 - IBM employs a unique approach to network control, interspersing the network monitoring and control signals with the actual data traffic as opposed to utilizing a secondary channel for monitoring and control.

- In IBM's System Network Architecture (SNA), the network management functions are performed by the various network components.
 - The network control program aids the network manager in evaluating activities within the 3705 communications controller.
 - Microprocessor-based modems and the 3867 Link Diagnostic Unit provide information relating to line problems and line quality.
 - SNA controllers collect network management statistics and display them to network control center personnel as requested.
- A variety of other hardware and software network monitoring features and functions are included as part of IBM's SNA environment.
- IBM's network control offering, called Network Communications Control Facility (NCCF) is designed to control, record, and automate a number of operator tasks, besides providing optional logging of operator-involved interactions.
 - Additionally, NCCF can be used with VTAM, TCAM, or both in a single data communications network.
 - The package also provides customizing capabilities, which permit users to write their own command lists, command processors, exit routines, and subtasks.
- In terms of communications network management functions, NCCF provides the user with control over network operations, services for processing VSAM files, and operator authority, including auditing and data security capabilities. Automating many of the operator tasks and processes makes network management significantly easier.

- The functional areas serviced by NCCF include:

- Network operations management.
- Problem determination.
- Configuration management.
- Change management.
- Problem management.

2. PARADYNE

- Paradyne's Analysis 4420 offers monitoring, diagnostic testing, and circuit restoration capabilities.
- In this environment, each modem incorporates a diagnostic microcomputer that collects information on system performance for comparison against standard performance parameters.
- A central site minicomputer polls each modem on a regular basis and displays an alarm for each situation in which a performance limit is exceeded.
- This display occurs on the operator's console where the operator can monitor system performance and take corrective action as appropriate.

3. GENERAL DATACOMM

- General DataComm's Netcon-5 network control system is able to operate within complex networks employing multiplexers, remote processors, and multiport modems.

- A 75 bps secondary channel is used to communicate network stations information to a central site controller.
 - The network controller employs mini floppy disks for system programs and directories and a CRT display printer for establishing system parameters, monitoring system performance, and correcting system problems.
 - All commands and responses are in English and are presented in easy-to-follow sequences.
- The new features for Netcon-5 include the ability to generate an array of statistical reports reflecting network trends, and a user-definable Station Data File and Problem Ticket Report Generation for logging and tracking network events and personnel activity.

4. AT&T

- AT&T's control system employs microprocessor-based modems and a secondary channel for control signals. Multiple controls and tests can be automatically queued or delayed for later execution. Tape cartridges are used to store test routines and information describing the network's configuration.
- AT&T's Dataphone II service offers three levels of network control with the capability to easily upgrade from one level to another.
 - With Level I service, a central-site modem is designated as a control unit and continuously polls remote modems. This central-site modem also has a special address that may contain requests from remote modems for maintenance testing.

- Level II service features a diagnostic console providing test and command capabilities. Level III systems employ network controllers providing command stations able to communicate test data to a central site or remote units.

5. TECH CONTROL CENTER MANUFACTURERS

- In addition to the network control and monitoring systems offered by suppliers of data modems, network management tools are offered by suppliers of tech control centers as well.
 - Dynatech Data Systems offers, with its DMS 200/400 System, a micro-processor-based controller with floppy disk, color CRT, and light pen.
 - The Dynatech system provides for local and remote monitoring and control of up to 1,024 lines.
- Atlantic Research offers a variety of central-site tech control facilities including patching, switching, and testing capabilities. The Atlantic Research NCS-100 offers rapid-testing, fault-isolation, and problem-bypassing capability and provides alarm information for the tech control operator.

O. MAJOR MODEM MANUFACTURERS

- Many other major modem manufacturers--including Intertel, Racal-Milgo, and Codex--offer network control systems. Intertel offers 90/10, Racal-Milgo offers CMS 1000 and 2000 network management systems, and Codex offers Distributed Network Control System (DNCS).

IV CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

- With the continued growth of on-line data networks, network control systems are gaining rapidly in importance.
- Because of the general sophistication of packet-switched networks, some form of network control capability is required to ensure prompt identification of network failures and initiate rapid restoral procedures.
- The need to integrate network management capability into the complex data networks of the 1980s is forcing manufacturers of network components to address the diagnostic and network control requirements that virtually all sophisticated network users are imposing on manufacturers.
 - Without a well-defined and effective diagnostic capability, communication network components will not be easily marketed.
 - Thus, designers of communications products must be willing to incorporate diagnostic and test capabilities in almost all products to be used in communications network environments.
- Several large network providers offer transmission facilities connecting users to their networks on a leased basis from various common carriers, as opposed

to providing these facilities directly to the users. Most of these leased facilities are obtained from AT&T, independent telephone companies, and Bell operating companies.

- When possible, digital transmission facilities, instead of older analog circuits, are utilized because of better error performance, higher reliability, and greater cost-effectiveness.
- Satellite links, which are not utilized to any extent at present, are theoretically adaptable to the packet network environment.
 - For example, the Telenet internode protocol is designed to permit efficient, full duplex operation over satellite links.
 - This full duplex capability permits the use of satellite links on overseas and domestic connections as well as domestically where satellite technology is more appropriate for use than conventional terrestrial circuits.

B. RECOMMENDATIONS

- Some of the items to cover with a network management system include:
 - Analysis and selection of the following control facilities:
 - Modems.
 - Jack panels.
 - Monitor and test procedures.

- . Line diagnostics.
- . Performance criteria and measurement.
- . Report generation.
- Network troubleshooting concerns, including:
 - . Control personnel.
 - . Extent of trouble.
 - . Terminal or controller condition.
 - . Data processing (DP) center.
 - . User terminals.
 - . Line testing.
 - . DP center personnel.
- Test and monitor procedures regarding:
 - . Equipment usage and condition.
 - . Computer port testing.
 - . Analog and digital interfaces.
 - . Software.
 - . Data processing.

- Line consideration, choosing between the following types:
 - . Dedicated lines.
 - . Dial-up lines.
- Line routing concerns, including:
 - . Traffic engineering.
 - . Usage statistics.
 - . Time plots of use.
- Line conditioning factors:
 - . Grades of conditioning.
 - . Line quality.
- The operation and maintenance of the control system is critical to a well-functioning network. Develop procedures and get agreement on them from all the participants, so everyone can follow them. Change them only when required and then only if all the participants agree.
- In determining network control center costs, the two most significant factors are labor costs of the operators and technicians and the cost of maintaining the network.
- It is the network--not the people--that is more error prone, due to system component failure, multiple vendor complexities, interface problems, programming errors, etc. All of these factors can be dealt with easily if you

understand the problem and have a good network management system. So treat the people well; they're hard to replace.

APPENDIX
NETWORK MANAGEMENT AND CONTROL SYSTEMS
SURVEY QUESTIONNAIRE

1. How do you currently handle network control? _____

2. Do you use a Network Control Center? _____

3. Do you have established troubleshooting procedures? _____

4. What sort of systems are covered by your network management system?

5. How long have you been using a control system and what sort of success have you had with it?

6. If you do not have a formalized network control procedure, how do you handle trouble calls?

7. What sort of statistics are being generated by your network management activity and how are they used?

NETWORK MANAGEMENT AND CONTROL SYSTEMS

ABSTRACT

This report is produced as part of INPUT's 1985 Telecommunications Planning Program. The research is based upon interviews with information systems and/or telecommunications users and vendors, and provides the basis for identifying and defining communications network management control requirements, methodologies, and applications.

The report describes various approaches and problems relating to communications network management and control, identifies some of the relevant procedures and techniques for dealing with network problems, defines some of the troubleshooting requirements to quickly resolve problems as they occur, and specifically discusses the unique case of packet-switched network problems. The findings are summarized and future trends are delineated. Topics include planning issues and procedures, troubleshooting procedures, a technology review and assessment, and conclusions and recommendations.

The report contains 75 pages, including 15 exhibits.

INPUT provides planning information, analysis, and recommendations to managers and executives in the information processing industries. Through market research, technology forecasting, and competitive analysis, INPUT supports client management in making informed decisions. Continuing services are provided to users and vendors of computers, communications, and office products and services.

The company carries out continuous and in-depth research. Working closely with clients on important issues, INPUT's staff members analyze and interpret the research data, then develop recommendations and innovative ideas to meet clients' needs.

Clients receive reports, presentations, access to data on which analyses are based, and continuous consulting.

Many of INPUT's professional staff members have nearly 20 years' experience in their areas of specialization. Most have held senior management positions in operations, marketing, or planning. This expertise enables INPUT to supply practical solutions to complex business problems.

Formed in 1974, INPUT has become a leading international planning services firm. Clients include over 100 of the world's largest and most technically advanced companies.

Offices

NORTH AMERICA

Headquarters

1943 Landings Drive
Mountain View, CA
94043
(415) 960-3990
Telex 171407

Detroit

220 East Huron
Suite 209
Ann Arbor, MI 48104
(313) 971-0667

New York

Park 80 Plaza West-1
Saddle Brook, NJ 07662
(201) 368-9471
Telex 134630

Washington, D.C.

11820 Parklawn Drive
Suite 201
Rockville, MD 20852
(301) 231-7350

EUROPE

United Kingdom

INPUT, Ltd.
Airwork House
35 Piccadilly
London, W1V 9PB
England
01-439-8985
Telex 23116

France

La Nacelle
Procédure d'abonnement 1-74
2, rue Campagne Première
75014 Paris
France
322.56.46
Telex 220064 X5533

Italy

PGP Sistema SRL
20127 Milano
Via Soperga 36
Italy
Milan 284-2850
Telex 310352

Sweden

Athena Konsult AB
Box 22232
S-104 22 Stockholm
Sweden
08-542025
Telex 17041

ASIA/AUSTRALIA

Japan

ODS Corporation
Shugetsu Building
No. 12-7 Kita Aoyama
3-Chome Minato-ku
Tokyo, 107
Japan
(03) 400-7090
Telex 26487

K.K. Ashisuto

Daini-Suzumaru Bldg., 6th Floor
8-1, Nishi Shimbashi
3-Chome Minato-ku
Tokyo, 105, Japan
(03) 437-0654
Telex 781 26196

Singapore

Cyberware Consultants (PTE) Ltd.
2902 Pangkor
Ardmore Park
Singapore 1025
734-8142

INPUT
Planning Services For Management

