



**US Army Corps
of Engineers**

Construction Engineering
Research Laboratory

USA-CERL SPECIAL REPORT N-86/23
September 1986

①

800, 501 E. 10th

AD-A206 762

Materiel Readiness Support Activity Automation Plan

by
Calvin C. Corbin
Carol J. Molnar

A comprehensive survey was conducted of the Materiel Readiness Support Activity (MRSA) of the Army Materiel Command (AMC) to determine their uses of automated data processing technology. This survey (unattached Appendix B) was then used to project a long range plan addressing MRSA's data processing needs. The long range automation plan for MRSA is presented in this report.

DTIC
ELECTE
APR 10 1989
S D
H

Approved for public release; distribution is unlimited.

89 4 07 123

The contents of this report are not to be used for advertising, publication, or promotional purposes. Citation of trade names does not constitute an official indorsement or approval of the use of such commercial products. The findings of this report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

**DESTROY THIS REPORT WHEN IT IS NO LONGER NEEDED
DO NOT RETURN IT TO THE ORIGINATOR**

USER EVALUATION OF REPORT

REFERENCE: USA-CERL SR N-86/23, *Materiel Readiness Support Activity Automation Plan*

Please take a few minutes to answer the questions below, tear out this sheet, and return it to USA-CERL. As a user of this report, your customer comments will provide USA-CERL with information essential for improving future reports.

1. Does this report satisfy a need? (Comment on purpose, related project, or other area of interest for which report will be used.) _____

2. How, specifically, is the report being used? (Information source, design data or procedure, management procedure, source of ideas, etc.) _____

3. Has the information in this report led to any quantitative savings as far as man-hours/contract dollars saved, operating costs avoided, efficiencies achieved, etc.? If so, please elaborate. _____

4. What is your evaluation of this report in the following areas?

a. Presentation: _____

b. Completeness: _____

c. Easy to Understand: _____

d. Easy to Implement: _____

e. Adequate Reference Material: _____

f. Relates to Area of Interest: _____

g. Did the report meet your expectations? _____

h. Does the report raise unanswered questions? _____

i. General Comments. (Indicate what you think should be changed to make this report and future reports of this type more responsive to your needs, more usable, improve readability, etc.) _____

5. If you would like to be contacted by the personnel who prepared this report to raise specific questions or discuss the topic, please fill in the following information.

Name: _____

Telephone Number: _____

Organization Address: _____

6. Please mail the completed form to:

Department of the Army
CONSTRUCTION ENGINEERING RESEARCH LABORATORY
ATTN: CECER-IMT
P.O. Box 4005
Champaign, IL 61820-1305

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED			1b. RESTRICTIVE MARKINGS		
2a. SECURITY CLASSIFICATION AUTHORITY			3. DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.		
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE					
4. PERFORMING ORGANIZATION REPORT NUMBER(S) USA-CERL SR N-86/23			5. MONITORING ORGANIZATION REPORT NUMBER(S)		
6a. NAME OF PERFORMING ORGANIZATION U.S. Army Construction Engr Research Laboratory		6b. OFFICE SYMBOL (If applicable) CECER-EN	7a. NAME OF MONITORING ORGANIZATION		
6c. ADDRESS (City, State, and ZIP Code) P.O. Box 4005 Champaign, IL 61820-1305			7b. ADDRESS (City, State, and ZIP Code)		
8a. NAME OF FUNDING / SPONSORING ORGANIZATION Army Materiel Command		8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER Project Order No. MRSA 47-85, dated September 1985.		
8c. ADDRESS (City, State, and ZIP Code) Materiel Readiness Support Activity Lexington, KY 40511-5101			10. SOURCE OF FUNDING NUMBERS		
			PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.
			WORK UNIT ACCESSION NO.		
11. TITLE (Include Security Classification) Materiel Readiness Support Activity Automation Plan (U)					
12. PERSONAL AUTHOR(S) Corbin, Calvin C. and Molnar, Carol J.					
13a. TYPE OF REPORT Final		13b. TIME COVERED FROM _____ TO _____		14. DATE OF REPORT (Year, Month, Day) 1986, September	
15. PAGE COUNT 232					
16. SUPPLEMENTARY NOTATION Copies are available from the National Technical Information Service Springfield, VA 22161					
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUB-GROUP	Army Materiel Command planning		
05	01		Materiel Readiness Support Activity		
			automation		
19. ABSTRACT (Continue on reverse if necessary and identify by block number)					
A comprehensive survey was conducted of the Materiel Readiness Support Activity (MRSA) of the Army Materiel Command (AMC) to determine their uses of automated data processing technology. This survey (unattached Appendix B) was then used to project a long range plan addressing MRSA's data processing needs. The long range automation plan for MRSA is presented in this report. → page 7					
20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☐ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS			21. ABSTRACT SECURITY CLASSIFICATION Unclassified		
22a. NAME OF RESPONSIBLE INDIVIDUAL GLORIA WIENKE			22b. TELEPHONE (Include Area Code) (217)352-6511, ext. 353		22c. OFFICE SYMBOL CECER-INT

FOREWORD

This investigation was performed for the Information Management Division (IMD), Materiel Readiness Support Activity (MRSA) of the Army Materiel Command (AMC) under reimbursable Project Order No. MRSA 47-85, dated September 1985.

The work was performed by the Environmental (EN) Division of the U.S. Army Construction Engineering Research Laboratory (USA-CERL). Dr. R. K. Jain is Chief of USA-CERL-EN. Dr. L. R. Shaffer is Technical Director of USA-CERL.

The following persons at MRSA were major contributors to this study: Mr. Richard Cernek, Chief of the Information Management Division (IMD); Mr. Rufus Prikryl, Chief of the Resource Management Division (RMD); Mr. Gayle Rees, Chief of the Maintenance Division; Mr. Willard F. Statton, Chief of the Readiness Division; and Mr. H. C. Jeffries, Chief of the Supply Division. Special thanks to the following persons within the IMD at MRSA: Mr. Ralph Mitchell, Ms. Carroll Tarvin, Mr. Ronald Ware, and Mr. Larry Moore.

Strategic Innovations, Inc. of Livonia, Michigan was contracted to perform the survey of MRSA.

Special acknowledgement is given to Ms. Carla Peyton, USA-CERL-EN, for her valuable assistance through the various stages of documentation and to the production of the final draft report.

Accession For	
NTIS GRA&I	☒
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

CONTENTS

	Page
DD FORM 1473	1
FOREWORD	3
1 INTRODUCTION.....	7
Background	7
Objective	7
Approach	7
Mode of Technology Transfer	7
2 LONG RANGE AUTOMATION GOALS FOR MRSA.....	8
Take a Network Service Approach	9
Share Resources While Minimizing Competition	10
Provide a Uniform Base Level of Services	10
Use Standard Operating System Interfaces	11
Have a Uniform File Server Interface	11
Access Data Base Services Using RPC Protocols	11
3 RECOMMENDED CHANGES IN AUTOMATION MANAGEMENT AND SUPPORT WITHIN MRSA.....	13
Decentralized Processing and Management	13
The IND Networking Group	15
4 RECOMMENDED AUTOMATED WORKSTATION APPROACH FOR MRSA.....	19
5 VISUAL/GRAPHIC REPRESENTATION OF CURRENT MRSA AUTOMATION.....	21
Office of the Commander	25
Internal Review and Audit Compliance Office	28
Resource Management Division	31
Information Management Division	37
Maintenance Division	41
Readiness Division	45
Supply Division	48
6 RECOMMENDED AUTOMATION CHANGES WITHIN MRSA.....	49
Logical View of the MRSA LAN	52
Office of the Commander	57
Internal Review and Audit Compliance Office	62
Resource Management Division	67
Information Management Division	78
Maintenance Division	86
Readiness Division	93
Supply Division	100
General Comments on Proposed Changes and Network Implementation	101
7 SECURITY CONSIDERATIONS FOR AUTOMATED RESOURCE MANAGEMENT.....	102
System Security	102
Passwords	103
Dealing With Data Destruction	103
Data File Security	104
Network Security	104

CONTENTS (Cont'd)

	Page
8 SUMMARY.....	106
9 ACRONYMS.....	107
APPENDIX A: NETWORKING DEFINITIONS AND PHILOSOPHY	108
APPENDIX B: SURVEY REPORT (unattached)	

MATERIEL READINESS SUPPORT ACTIVITY AUTOMATION PLAN

1 INTRODUCTION

Background

The Army Materiel Command (AMC), Materiel Readiness Support Activity (MRSA), Information Management Division (IMD) saw a need to determine an integrated automation plan that would address their current and future data processing needs. IMD's concern was that their service to their end-user community (in-house Divisions) not be degraded by the acquisition of diverse automation resources which could not communicate with each other and which require specialized training. MRSA asked the U.S. Army Construction Engineering Research Laboratory (USA-CERL) to address this problem which is largely one of networking and porting code between different computers.

Objective

The objective of this research was to develop a comprehensive automation plan for MRSA. *Q13*

Approach

A comprehensive study of MRSA was performed. The study focused on automation equipment and how it was being used. The study also addressed the administrative structure of MRSA as it affected the distribution of both equipment and personnel dealing with automation tasks and problems.

Mode of Technology Transfer

The report is provided to IMD of MRSA to use at its discretion.

2 LONG RANGE AUTOMATION GOALS FOR MRSA

The mission of MRSA is evolving to make it a centralized processor of large data bases. MRSA can expect to be tasked with preparing more reports and analyses of these data bases.

Given the acceptance of the above mission, it becomes necessary for MRSA to provide an environment in which this mission can be accomplished and an architecture that allows new technology to be easily incorporated with minimal impact on the system users.

MRSA needs a responsive interactive system that can analyze data and run large computations. Inexpensive microprocessor-based workstations provide cost-effective interactive response. Local area networks can be used to tie workstations to back-end machines such as large superminicomputers, mainframes, and supercomputers. Peripheral resources such as disks, tapes, communications interfaces, and printers can be shared by providing access to them over the local area network.

No single software or hardware computer vendor can produce the component technologies to make a combined component system cost effective. It is not possible for a single organization to simultaneously track advances in languages, user interfaces, data bases, graphics, specialized high-performance symbolic and numeric architectures, and expert systems, let alone the many applications for these component technologies. Multivendor systems will be required and must depend on standards to interconnect the components. Combining heterogeneous hardware and software elements into an integrated, effective network entails building interfaces at the points at which all systems are homogeneous.

An analogy can be drawn between the emerging networked computing environments and component stereo systems. In the instance of stereos, a task (making music) is distributed over a variety of components, each dedicated to performing some part of the overall job. Because of this modularity, systems are typically built over time through several purchases. As a result, they generally consist of components from several different vendors (given that most consumers try to purchase the best equipment available at the most competitive prices). Thus, the system as a whole can be seen as an evolving compromise between desired performance, the state of technology at various points in time, and the budgetary constraints of the user. Component stereo gear would not even be possible today had vendors not agreed on interconnection standards. Comparable efforts have been made in the computing arena, but the task has been complicated by the existence of differing standards for various networking facets (for example, the Ethernet and Token Ring physical medium standards, and the TCP/IP, DECnet, ISO, and X.25 transport control standards). Compounding the computer interconnection challenge is the enormous variety of network applications. With stereo systems, there is only one application (making music) to worry about. Computer vendors, though, must shape standards that can accommodate and evolve with innumerable applications. Because of the variety of applications, obstacles to creating an integrated, heterogeneous, component computing environment are encountered.

The following architectural principles are the keys to constructing a new multivendor open system environment.

- Take a network service approach
- Share resources while minimizing competition
- Provide a uniform base level of services
- Use standard operating system interfaces
- Have a uniform file server interface
- Access data base services using RPC protocols

All the principles and approaches proposed here have been proven in systems in use today; ideas whose long-term value is unproven were avoided. The explanation of these principles follows.

Take a Network Service Approach

Two major approaches to connecting a network of personal machines (workstations) are the "network of distributed" operating system, typified by the Apollo Domain system (from Apollo Computers), and the Locus system (at UCLA*). These systems, and other PC networks, represent an attempt to extend the monolithic operating systems which were present on mainframes and superminicomputers to the local network environment. They tend to be inflexible and have a very strong bias toward components of the system provided by the primary vendor over other vendors' peripherals. In effect, this approach achieves a high degree of integration by transforming a network of components into what amounts to a loosely-coupled multiprocessor. By using the same software architecture on every hardware system in a network, this type of operating system essentially limits the problems of heterogeneity to hardware. Imposing a single operating system, even one capable of supporting a wide range of hardware, is especially unacceptable in an environment in which previously autonomous operations with existing heterogeneous hardware and software are being integrated into a network because it invalidates the existing software investments. Further, it constrains the organization by locking it into the evolution of a single software base.

The second major approach is a loosely-coupled, open system design that gives network services primacy over the network operating system. The network services approach describes the network facilities available to applications in the form of standardized, system-independent interfaces called services. This approach to resource sharing is the same one employed in the ARPANET. The Berkeley version of the UNIX system known as 4.2BSD, derives much of its flavor from this kind of open-ended set of network services to be defined independent of the system calls to the operating system. (See Appendix A for definitions and explanations of general networking terms and functional usages.) Extensions to the system facilities occur in applications programs, not in extensions to the system. Thus, the system can be developed and enhanced without touching the underlying operating system. This makes code more portable and avoids disturbing the system with continual system interface changes, which is a crucial design goal. The 4.2BSD system contains sufficient facilities in the system interface that an open network system can

* Acronyms are defined in Chapter 9.

be built without changing the system calls. Open systems derived from 4.2BSD and based on the network service approach are being constructed by a number of vendors (including SUN Microsystems). The 4.2BSD system provides a portable and standard open-system base for putting together a network of heterogeneous computer systems to handle large data management and scientific computing problems and activities such as those in the MRSA environment.

Share Resources While Minimizing Competition

The primary measure of system performance in this environment is to attempt to achieve quality in both predictable low-latency response and in high throughput. Needless to say, these are often contradictory goals.

Dedicating peripherals to each user is one end of the spectrum. It gives low-latency response and high throughput, but is not cost effective. At the other end of the spectrum is centralization of services. Here, predictability and responsiveness of the servers (and, therefore the quality of the system) is placed at risk. A central file server or compute server would be practical only if it does not become overloaded, thereby defeating predictable workstation response.

Sharing access to devices on a local network is essential to cost-effective computing. Disk drives, tape drives, printers, and other peripherals become subject to economies of scale. For example, centralized file servers provide a significant cost and maintenance advantage over systems where each user has only a local disk. The larger capacity disk drives are both cheaper per megabyte of storage and also faster than the small, "inexpensive" disk drives that can be provided with each workstation. Even if costs were similar, requirements for shared data access and the difficulty of determining the amount of disk storage required of each user makes it difficult to effectively provide each user with local disk storage.

Current research is being performed in the area of maximizing the throughput in file server nodes. Implementation and use of cache memories at server nodes should eventually result in server-based systems attaining a response performance equal to or surpassing that of systems providing smaller and slower peripherals to each user. An approach to compute serve nodes is to schedule tasks in a batch mode fashion, rather than time-shared, to increase predictability and to minimize competition, but at the expense of some flexibility.

Provide a Uniform Base Level of Services

The simplest form of connection between machines is to allow file transfer, remote login, and remote command execution. Providing these services to all machines in an environment with uniform syntax should be the first priority at MRSA. This level of service is the basis of the success of such networks as ARPANET and DDN. Having this level of service is far more important than any of the services described later and should always be provided for all possible machines.

Small, single-task personal computers such as the IBM PC or the Macintosh will have client telnet (remote login) and FTP (file transfer protocol) implementations so that they can access any file on the network, back themselves up to any other machine, and act as a terminal to larger hosts. Larger hosts can exchange files in a symmetric manner, and a terminal attached to any of the larger hosts can serve to login to any other host.

The DARPA standard TCP/IP/UDP (stream and datagram) transmission protocols, FTP, and telnet protocols provide a widely accepted and implemented standard for this base level connection. Ethernet provides a high bandwidth and inexpensive, vendor-independent hardware interconnect.

Use Standard Operating System Interfaces

There are several important operating systems in the microprocessor market. In the 8-bit world there is Apple/DOS and CP/M; in the 16-bit world, MS/DOS and UNIX; and in the 32-bit world, UNIX and the new Macintosh operating system. Each operating system environment defines an applications program interface for which many applications exist. Providing users access to one or more of these system interfaces can bring along many more applications at low cost.

The UNIX operating system standard is the most important because it runs on a wide range of machines. The system meets two needs: a standard applications interface, and a systems building block for constructing an open-network system. 4.2BSD is currently the only version of the UNIX system that defines a standard and stable, yet extensible interface to networking facilities. It will be several years before an alternative standard interface for a networked UNIX system can be developed. Thus, a number of vendors have adopted the 4.2BSD network interface as an industry standard.

Have a Uniform File Server Interface

Most operating systems now provide a hierarchical file system similar to the one provided in the original UNIX system. Providing a network service that makes all files in the network environment available transparently is an enormous advantage. Operating system independence in the protocol is very desirable because, for example, users would like the ability to access the file system from the IBM PC, the Macintosh, and more powerful workstations. It is necessary that the protocol be able to access files on diverse systems such as IBM mainframes (VM/CMS) and superminicomputers like DEC's VAX-11/780 series (VAX/VMS). SUN Microsystems is currently very close to offering this product based on the 4.2BSD UNIX.

Access Data Base Services Using RPC Protocols

We suggest that MRSA plan to provide data base access through applications-level network services rather than as part of the operating system facilities. This allows a range of implementations of data base services based on applications needs and can yield modular and well-specified systems. An example of a DBMS performing in this manner is the distributed

version of MicroIngres available in a network of SUN Microsystem workstations.

Both high-performance and high-availability systems can be constructed atop an efficient remote-procedure-call mechanism in a distributed environment. This architectural approach also allows construction of reliable data storage systems.

Ensuring predictable response time is the most important goal in creating a production environment in which large data bases are manipulated. In this kind of professional environment, MRSA will often need access to more cycles than one's workstation can supply, and these cycles can be cost-effectively supplied by back-end compute servers. A loosely-coupled system permits a cost-effective mix of workstations and server machines.

3 RECOMMENDED CHANGES IN AUTOMATION MANAGEMENT AND SUPPORT WITHIN MRSA

Decentralized Processing and Management

MRSA is in a position similar to that of many other agencies and organizations which are attempting to solve problems and perform tasks using computers and automation. The situation may be viewed as part of the general pattern of using and managing computer resources over the last few years. Most organizations set up a centralized computing shop in the late 1950's and 1960's. Computers were very expensive pieces of equipment and required exacting maintenance and operations support for effective utilization within the organization. It made excellent corporate sense to task a specific, specially trained group of people with the job of managing and controlling the access to this very expensive resource. Because of the large cost involved in purchasing and operating computer systems, organizations would sacrifice human time (man-hours*) to optimize computer time (cpu hours). The dollar cost weighed heavily on the side of the hardware. People were much cheaper to use than computers and could be used to solve many (nonrepetitive) problems more cost effectively than could be done by using the computer system. Even for the computer programmer, it was often more cost effective to debug a program at a desk than to do it interactively on the computer system.

Today, the situation has changed completely. People are now more expensive than computers. It is far more cost effective to optimize and program human resources than computer resources. The technological advances which caused this huge change in the value of human resources versus that of computer resources has brought about a corresponding change in how computer resources are managed.

The management and use of computer resources has evolved from the centralized, closely controlled data processing shop of the early years to a decentralized, loosely controlled data processing environment which reflects the ever decreasing cost and ease of use of the new computer resources. These resources (like PC's, micros, specialized peripherals, etc.) are now very cheap and easy to use; non-data-processing staff are easily able to perform functions which historically had to be performed by data processing specialists. The future progress of this evolution of centralized processing to the user will soon (in 10 to 15 years) result in the user being able to interact with a piece of software by question and answer to create specialized object code (to solve specific computing tasks) from a general piece of interactive software. Most computer resources are now purchased on an ad hoc basis. The user simply wants a product to meet a specific and immediate need and has little interest in (or understanding of) the problems and advantages of acquiring an ideal system that serves every purpose.

Thus, it is no longer possible for a centralized data processing shop to manage and control all of the processing requirements in an organization.

*Male nouns/pronouns as used in this publication refer to both genders.

MRSA is faced with the fact of decentralized computing but still retains a centralized data processing function (IMD). It is the mission of IMD to provide computer resources and programming support for all of the other divisions. However, this is a function which can no longer be controlled from a centralized support group. Any division request for services which is not perceived to be acted upon properly by IMD will lead to the division simply procuring resources (human or machine) necessary to solve the problem.

The divisions within MRSA are allocated the funding to solve their mission problems. If a division decides that it needs a specific machine to solve a problem, it has the ability and control of funds to bypass IMD and acquire that machine whether or not there might be something better, cheaper, or more easily integrated into the existing set of hardware at MRSA. IMD is currently caught in the role of trying to advise the divisions about procurements, but really has no effective means of controlling the spread of more and more diverse computers and peripherals purchased and addressed toward specific tasks.

A change in the function of IMD, its mission, and how it relates to the rest of MRSA is proposed. It is suggested that IMD be tasked with full control of implementing these recommendations and changes.

- 1) IMD should be tasked with supervising the integration of existing MRSA computers into a workstation network architecture (see Chapter 4).
- 2) IMD should retain the responsibility of maintaining the operation of mainframe machines--those top level processors which are treated as shared resources by other divisions within MRSA (MRSA LAN host machines).
- 3) All programming, programming management, and program development support should be unbundled from IMD to the appropriate divisions so that the divisions (users) directly control the resources necessary to complete their tasks. This may involve creating a division program support function, however, the direction of program support is evolving down to each individual user as high-level languages and applications become more user-friendly. Each project manager should be solely responsible for the resources for that project. The operational support for low-level processors and other division computer resources should be tasked to the divisions which procure and use those resources. It is a fact that each computer user is having to become a system administrator, as the user resource becomes more and more of a full computer system. Again, this is a function that each division may want to allocate/task to specific personnel within the division. However, IMD should be in control of this process. IMD must be given adequate time and resources to shift its emphasis from programming support to network and training support. This shift in emphasis will require a great deal of time in training and reorienting personnel to a different support function. Also, the MRSA divisions must not be immediately tasked with the full responsibility of providing their own system maintenance and programmer support. This must evolve over time and be coordinated by IMD with each division. It would be extremely counterproductive to create a situation within MRSA in which divisions were competing for programmer support and for machine resources. IMD should put together a list of application activities that it currently supports and, in conjunction with the divisions, plan a time line whereby each project (application) can be gracefully transferred to the end user. IMD

should order this project list such that those projects which are *standalone* (projects/activities which affect one division only) come first. It is much more difficult to arrange a smooth transition for those activities which affect more than one division. For example, maintenance of a shared data base should be transitioned so that each division ends up with shared access to the data and so that the support of the data integrity has been clearly allocated to the primary user. The primary user (division) will become responsible for maintaining the data base and will be responsible for it being shared with other users (divisions) that need access to it.

4) The integration and compatibility of further computer acquisitions should be directed toward answering two questions: Will the projected resource satisfactorily address the problem for which it is targeted? How will the resource fit into the existing/planned workstation networked environment?

5) A function of the IMD Networking Group should be to determine if computer resource procurements do or do not fit into the planned workstation network. If a proposed procurement does not fit, IMD (as the MRSA LAN manager) would not be tasked with integrating that resource into the network architecture. However, if the resource does meet the protocol standards of the network environment, it would become IMD's task to make sure that it became integrated into the MRSA network.

6) IMD should also be tasked to perform a technology tracking function (especially as it applies to networking and integration of diverse computer systems) in order to recommend and target new products for the MRSA LAN network.

7) Training (how to effectively use computer resources) is a function that needs to be heavily and continually addressed at MRSA. It is a function that should be handled by a support unit like IMD that is not part of a division, but which has knowledge of the computing resources and usage needs/functions within MRSA. As programming and operational support of local machines is unbundled from IMD, the emphasis on training would be that of local machine operations and specific language or utility applications. IMD should be capable of targeting training programs across MRSA; that is, coordinating interdivisional training of common automation resources. Personnel will need to be trained in how to use a computer network. They will need to adjust dramatically to the reality of shared access and use of automation resources. Resources available on the MRSA LAN are resources for all MRSA users.

The IMD Networking Group

The primary function of the new IMD Networking Group should be to create what the architects of the computer age have been aiming for--a paperless society in which people can communicate with each other instantly. Unfortunately, after 30 years of computer developments and proliferation, this scheme is still visionary. Looking at MRSA's work place, the barriers to such a system seem formidable. A highly competitive environment has produced a multiplicity of computers, software, and peripherals. Since vendors have been pursuing a concept much closer to *proprietary* than *compatibility*, the

inevitable result within MRSA (as elsewhere) has been the acquisition of computer products which have been purposely designed to be incompatible. They offer what no other vendor can. With the advent of cheap PCs and micros, this electronic Tower of Babel has become a deafening roar.

The diversity that has evolved should not be viewed as totally negative. Just as each human language has individual qualities that appeal to the speaker (precision of expression, a certain innate poetry, a variety of nuances to provide rich details and shades of meaning), so each computing language and machine has its own advantages.

While the market has produced this diversity, it is also responsible for spurring industry toward recognized standards. Within MRSA, creating a workstation network which will facilitate access to "corporate" processing at the highest level, "group" processing at the intermediate level, and "local" processing at the individual level will provide an environment from which one can get more productivity from existing computer resources and which will facilitate rapid and simplified communications among dispersed users throughout MRSA.

Although the International Standards Organization (ISO) is just beginning to propose and discuss what will eventually become an international standard for an Open Systems Interconnection (OSI), the technology to set up a complete and useful system of communication between computers that speak different languages can be put in place at MRSA. To address the immediate problem, it is reasonable to work with what is available. Our recommendation is that TCP/IP (Transfer Control Protocol and Internet Protocol, see Appendix A) be used by MRSA as the protocol "language" for communication between computers. TCP/IP was adopted as a de facto standard by the scientific and engineering community since it was designated by DOD as its official protocol standard some years ago. TCP/IP is a known quantity and has evolved steadily over the past 10 years. It is highly reliable and has proven itself in many applications. The choice of TCP/IP by DOD means that a significant portion of all networks installed during the next 5 years will support that protocol, thus guaranteeing its economic viability. TCP/IP has also gained wide acceptance because it is not a proprietary networking protocol. Because TCP/IP does not favor one brand over another, more vendors incorporate this protocol into their products than any other networking protocol in the world. This ability to cross so many proprietary boundaries makes TCP/IP very effective in both local and wide area networks. Networks which implement TCP/IP within the next year or two will not be left high and dry by vendors who abandon the standard and go out of business. Other existing network protocols are limited to proprietary applications and tend to lock data in or out, depending on the brands of processors where they are found (these proprietary standards are often richer in functionality, but are very limited in their ability to communicate with products of most other vendors). It must also be noted that having decided on using the TCP/IP network protocol does not prohibit the use of other protocols. TCP/IP can run side-by-side with other protocols in a single processor, often sharing the same hardware controllers and communication lines. This ability to coexist with other protocols will be of increasing importance as the new OSI standard comes on the scene. Historically, new protocols do not emerge all at once, but grow into a market in progressive stages. Organizations that wish to communicate with processors that the new standard does not support during its early years

will have to rely on dual protocols that can reside together in a single machine.

A decided advantage to the user is that TCP/IP is primarily implemented in software, rather than hardware, eliminating expensive and disruptive board changes whenever parts of the network protocol must be modified. Most implementations of TCP/IP leave the user's existing hardware completely standard, adding enhancements in the form of various communication capabilities. Since it is a software system that conforms to the OSI (seven layer) model, the protocol can easily accommodate future advances in networking technology and standards.

The TCP/IP installation process is fast and simple because no modifications to the host computer's operating system or hardware configuration are necessary.

Although the number and diversity of machines and languages is still proliferating, an organization can still work toward a paperless society (full automation) by implementing a workstation network with a broad range of capabilities that integrates "incompatible" systems and which can flexibly adjust to changing technology.

To prepare for the next generation of computing systems, it is absolutely necessary to take the network service approach. Currently, the most suitable base operating system is 4.2BSD UNIX because its networking facilities can be used to write network applications and protocols without changing the system's programming interface. Back-end computational and server nodes can be placed on the network and can be scheduled to provide predictable response time. 4.2BSD comes with remote login and file transfer services that can be extended to other machines in the network because the standard TCP/IP protocols on which they are based are available on a wide variety of machines.

Using the principles noted previously, and with 4.2BSD UNIX as a base, a cost-effective and flexible system can be constructed without inventing new hardware or software technology. The new DA-approved minicomputer, the Sperry 5000/80, supports TCP/IP and most of the 4.2BSD networking extensions on its implementation of AT&T's UNIX System V. Forthcoming advances in microcomputer technology, cost reductions in memories, and high-performance supercomputers and mainframes can then be easily integrated into the working environments. In the implementation of this schema, it is worth repeating that at any one time, the system configuration will be the direct result of a compromise between desired performance, state-of-the-art technology, and funding constraints.

Ethernet should be used as the media. In the future, users will want a broadband approach which will support activities such as voice and video along with data transfer. However, MRSA's current needs and short range mission forecast indicates that emphasis on the network functionality will be almost totally dedicated to data transfer. Ethernet is a reliable and reasonably cheap (cost effective per node connection) media which is also easier to implement and administer than ring networks. The physical dimensions of MRSA will support an Ethernet topology.

In some cases, thin-wire Ethernet can be used to tie groups of PCs to a second level processor (like a micro or Intel-310). Normal cable Ethernet can be used to tie second level processors to the third level mainframes (see Chapter 4).

4 RECOMMENDED AUTOMATED WORKSTATION APPROACH FOR MRSA

The computer workstation should be the common denominator by which the MRSA user performs automation tasks. The following types and functions of workstations should be implemented where functionally appropriate:

The types of workstations and the attributes of each are as follows:

Manager Workstation

- scheduler, calendar
- auto rolodex
- mail/df with alias lists
- graphic (opt) monitor capable of reviewing analyst's work

Programmer/Analyst Workstation

- scheduler, calendar
- mail with alias lists
- graphic monitor
- access to shared laser printer
- local compiler/DBMS for product development

Data Analyst/Reporter Workstation

- prepare project reports
- scheduler, calendar
- graphic monitor
- access to shared laser printer
- local printer

Clerical Workstation

- local printer
- word processing package
- phone management routines
- auto rolodex
- scheduler/calendar, reminder - coordinate team/group schedule

Individual workstations and terminals can be considered the first level of MRSA processing capabilities. This level should be connected to the second (intermediate) level of processing (e.g., multiuser micros and small minicomputers) by the MRSA LAN. Initially, since the first level of MRSA processing consists of terminals and PCs, the connection from the first level of MRSA processors to the second level of processing will be by hardwire (96K baud). The second level of MRSA processing should be connected to the third and top (mainframe) level of processing (and access to external networks like DDN and DARPA NET) by the MRSA LAN.

Figure A illustrates the different levels of logical processing (from personal workstation to group/intermediate processing to top level processing):

MRSA PROCESSING LEVELS

3rd/Top Level Processing - MRSA LAN / MRSA LAN Processors

2nd/Intermediate Level Processing (Intel 310s, Microcomputers)

1st/Bottom Level Processing (PCs or Terminals) --> Moving Toward Single User Workstations.

Figure A
MRSA Processing Levels

5 VISUAL/GRAPHIC REPRESENTATION OF CURRENT MRSA AUTOMATION

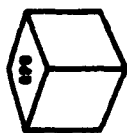
This section illustrates the connectivity and function of the various automation resources currently at MRSA. The information is summarized from the Survey Report (unattached Appendix B).

The information is presented by division (and within division by branch) for all of MRSA. This type of visual/graphic presentation lends itself well to further conceptual design and regrouping (see Chapter 6).

The material is organized as follows:

- > visual diagrams showing data flow and usage,
- > textual description of the functional mission of the division and branch.

Symbol Legend



C P U



VYSE PC



HP PC



INTEL 310



TERMINAL



AND Word Processor



Modem



File Form



Scanner



Tape Drive



Printer



L Laser Printer



Printer

MPSA LAN

INTEL ETHERNET

HARDWARE

NON LINK

ADAPT TO PROTOCOL

? ?

Office of the Commander

Commander



Deputy



Printer Access - All Units

Hardware

[illegible]

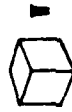
24

Office of the Commander

The Commander directs and is responsible for accomplishing missions assigned to MRSA by the Commander of the U.S. Army Materiel Command. The Commander provides leadership, executive authority, policy guidance, and doctrine necessary to accomplish the assigned missions.

Internal Review and Audit Compliance Office

Auditor

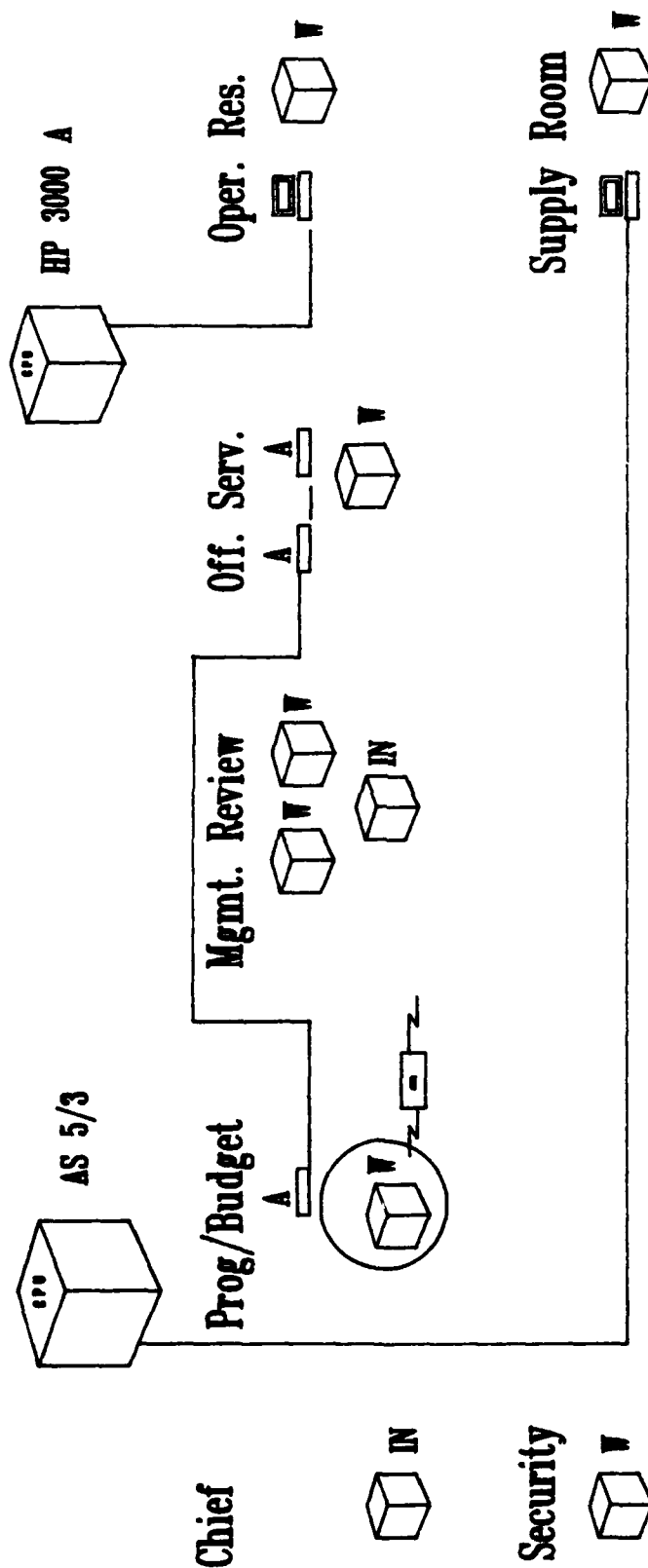


Printer Access - All Units

Internal Review and Audit Compliance Office

The mission of this office is to monitor MRSA expenditures by division and to prepare the MRSA annual audit report.

Resource Management Division



Printer Access - All Units

Resource Management Division

[illegible]

Resource Management Division

Division Chief's Office

This office assures that key functions of RMD as stated in the Organization and Functions Manual 10-1 are carried out.

Program and Budget Branch

Major functions of this branch include reporting 5-year plan information from division chiefs, prioritized task reporting from division chiefs, and summarizing written submissions from divisions into a format for external reporting.

Management Review and Analysis Branch

Major functions of this branch include reporting work measurement to AMC, Command Performance Indicator Review reporting, Commercial Activities Report preparation, and the storage, updating, and output of Manual 10-1.

Offices Services Branch

Major functions of this branch include maintaining the Manning Book (personnel directory), the Principal Action Officer directory, updating and preparing the Activity Property Book for publication, and tracking personnel training in MRSA.

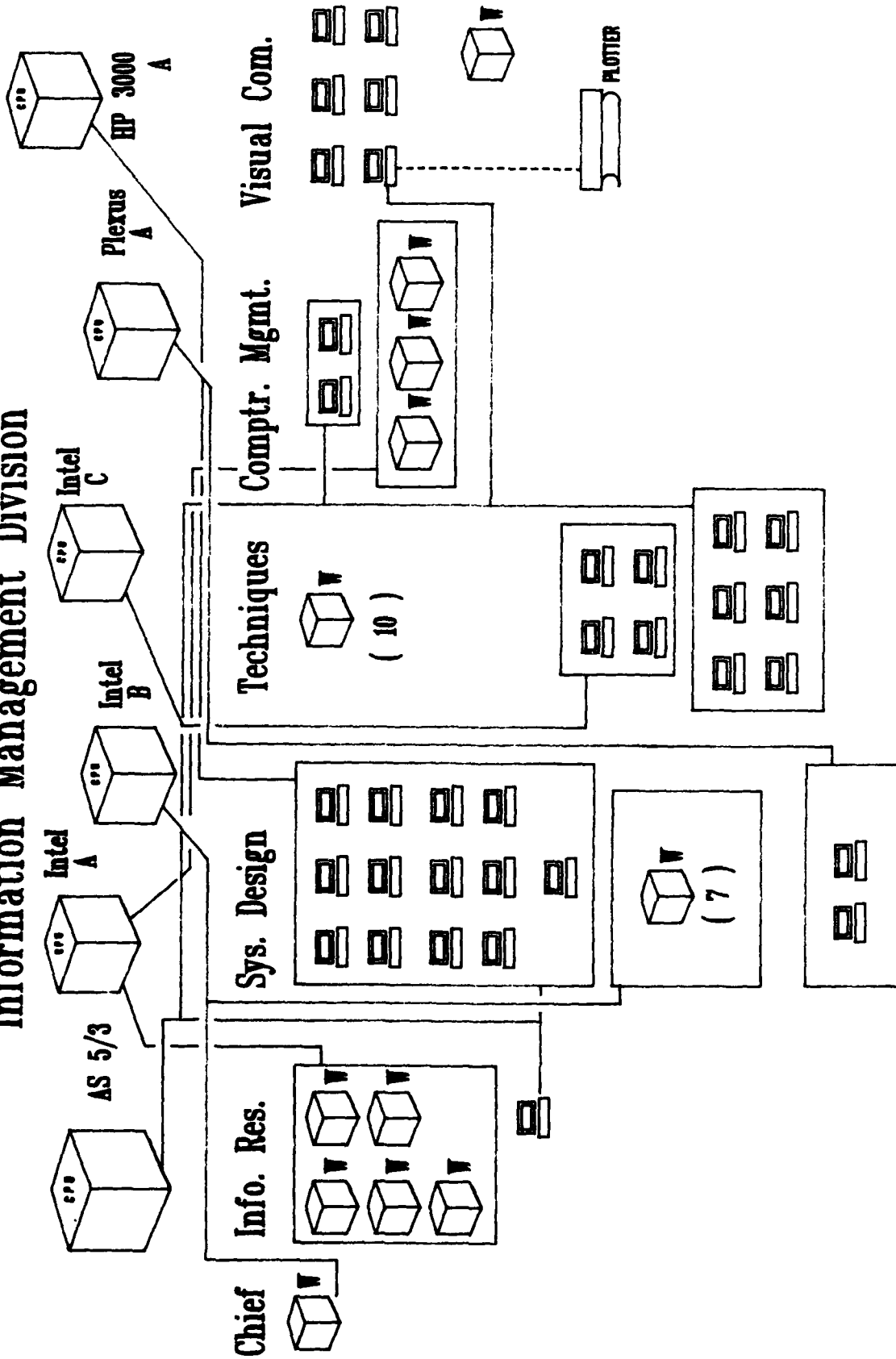
Operations Research Branch

Major functions of this branch include preparing need analyses for potential new IMD computing equipment.

Supply Room

Major functions of the supply room include maintenance of requisition/document expenditures.

Information Management Division



Information Management Division

[illegible]

Hardware

34

Information Management Division (p.3)

Branch- Unit	Hardware										Software										Function									
	BM	Network	Wang	Wang	Wang	Wang	Wang	Wang	Wang	Wang	IBM	AS/400	AS/390	AS/380	AS/370	AS/360	AS/350	AS/340	AS/330	AS/320	AS/310	AS/300	AS/290	AS/280	AS/270	AS/260	AS/250	AS/240	AS/230	AS/220
12																														
13																														
14																														
15																														
16																														
17																														
18																														
19																														
20																														
Comptr. Mgmt.																														
1																														
2																														
3																														
4																														
5																														
Visual Com.																														
1																														
2																														
3																														
4																														
5																														

Information Management Division (p.4)

Branch- Unit	Hardware	Software	Function
	Bull		
	Netrax		
	Hip		
	Wysa		
	Mesa		
	Ad3B		
	Ad3D		
	Ictronix		
	Pexus		
	Elec-Mell		
	AS-3		
	HP		
	Ams-3000		
	Lanix		
	Wase		
	Word		
	Hp Side		
	Lotus		
	Gt-phics		
	Statistics		
	Com'cation		
	Office Auto		
	Prode		
	Reports		
	Program's		
	Graphics		

Information Management Division

Division Chief's Office

The major function of the chief of IMD is to provide guidance and management in developing computer applications pertinent to accomplishing the mission of MRSA.

Information Resources Management Branch

Major functions of this branch include serving as the administrative control point for current and future ADPE equipment, manpower, training, physical facilities, supplies, and services. The branch is also responsible for developing, coordinating, recommending, and implementing division master planning and other functions as outlined in Manual 10-1.

Systems Design and Programming Branch

The primary function of this branch is to develop, support, and maintain computer systems programs and a national level data base throughout MRSA to meet mission requirements.

Techniques Branch

Major functions of this branch include supporting hardware and software on computer systems throughout MRSA. Primary responsibilities for designing communication techniques and providing software maintenance for the mainframe systems also rest with this branch.

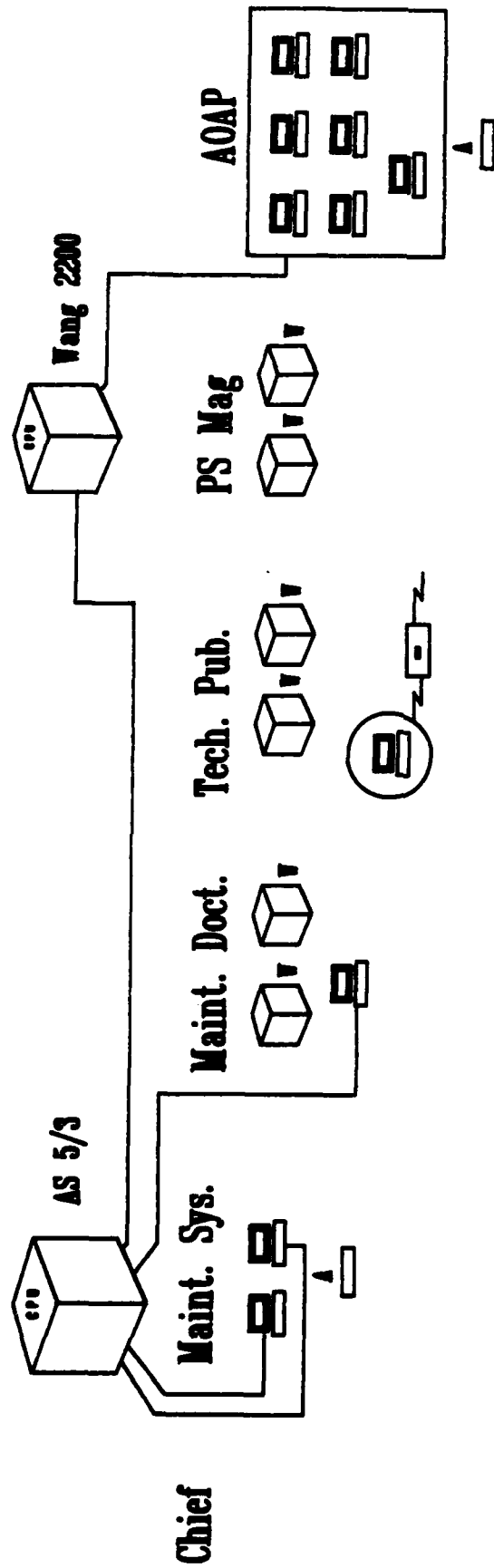
Computer Management Branch

Major functions of this branch include managing, controlling, monitoring, and operating data processing equipment in MRSA.

Visual Communications Branch

The major function of this branch is to provide total visual support for all Depot briefings.

Maintenance Division



Printer Access - All Units

Function

Hardware

**Branch-
Unit
Chief**

Maint. Sys.	1	2	3
-------------	---	---	---

Maint. Doct.	1	2	3
--------------	---	---	---

Tech. Pub.	1	2	3
------------	---	---	---

PS May 1 2

Maintenance Division (p.2)

[illegible]

Maintenance Division

Division Chief's Office

The division chief is charged with ensuring that the key functions of the Maintenance Division as stated in Manual 10-1 are carried out.

Maintenance Systems Branch

Major functions of this branch include monitoring and producing reports and summaries of usage, ownership, maintenance, cost, and downtime of all Army equipment.

Maintenance Doctrine Branch

Major functions of this branch focus on evaluating proposed maintenance doctrine, policies, and procedures. The branch also determines the most feasible method of accumulating storage and determines access to data. These determinations help to define a valid mean usage between equipment replacement and failure factors and are required to manage logistics during equipment life cycle.

Technical Publications Branch

Major functions of this branch include monitoring and evaluating the AMC equipment publications program for adherence to regulations, reporting any deviations to AMC, and initiating corrective action. This branch also maintains the EOPDB (Equipment Oriented Publications Data Base) which is used to track and index all AMC related publications.

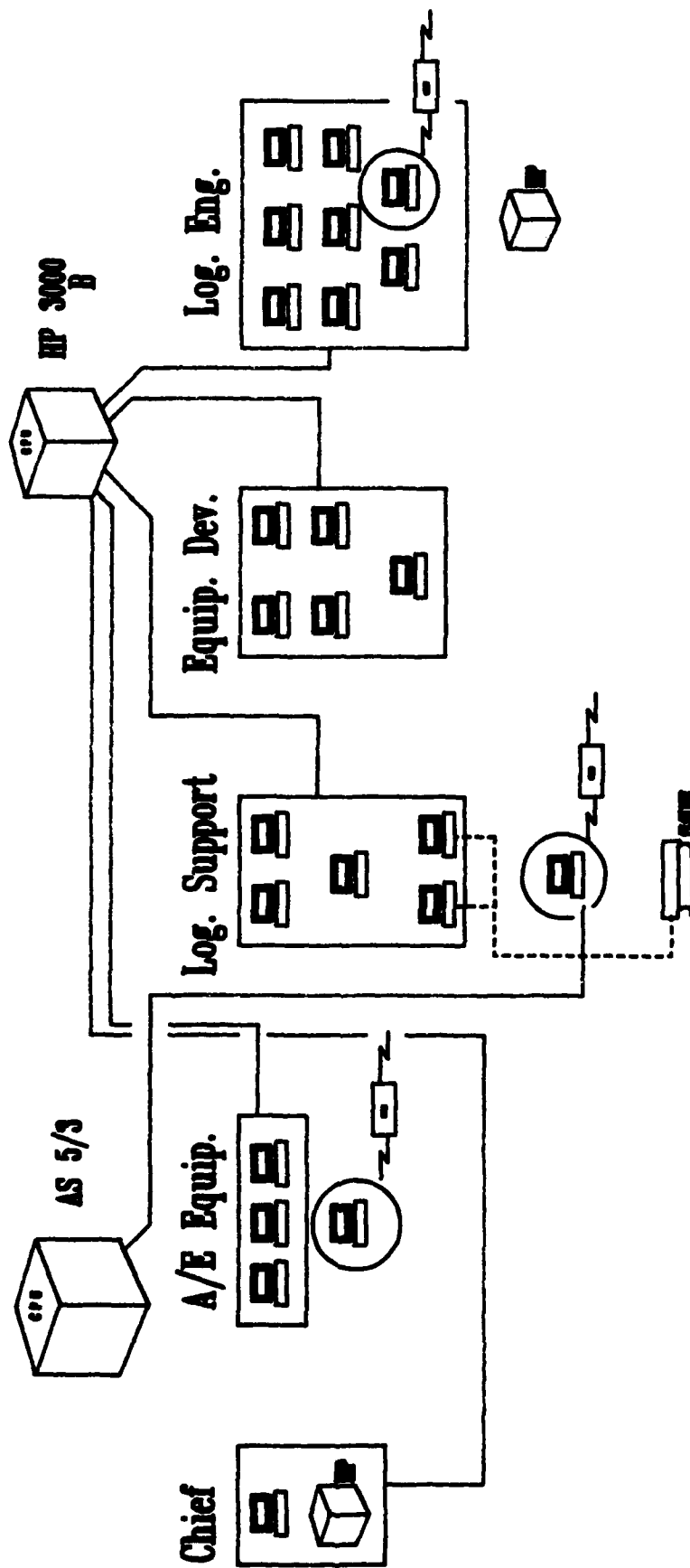
PS Magazine Branch

Major functions of this branch include preparing manuscripts, technical art, and references for publication in PS Magazine.

Army Oil Analysis Program Branch

Major functions of this branch include analyzing and reporting oil usage on every item of Army-owned equipment that uses oil.

Readiness Division



 Printer Access - All Units

Readiness Division

Branch- Unit	Hardware										Software										Function									
	Chief	1	2	1	2	3	4	1	2	3	4	5	6	1	2	3	4	5	6	7	1	2	3	4	5	6	7	8	9	10
Chief	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
A/E Equip																														
Log. Support																														
Equip. Dev.																														

Readiness Division (p.2)

Hardware

Software

Function

Branch-Unit

—

2

→

5

2

2

[illegible]

		+	-
		+	
		+	-
		+	-
		+	-

+	+	+
	+	+
	+	+
+		
+		
+	+	+
+	+	+

-	+	+
-	+	+
-	+	+
-	+	+
-	+	+

[illegible][illegible][illegible][illegible][illegible][illegible][illegible]

Readiness Division

Division Chief's Office

The division chief functions as the high-level manager for all of the systems in Readiness. Depending on conditions, the chief may also function as a system developer. The chief is also responsible for setting and monitoring goals.

Analysis and Equipment Improvement Branch

Major functions of this branch include designing, developing, reporting, and managing Army equipment, reporting historical availability trends, managing unit equipment status, and producing service ability reports.

Integrated Logistic Support Branch

Major functions of this branch include managing the Army Management Milestone System, ILS Review and Analysis reporting, and ILS Milestone tracking.

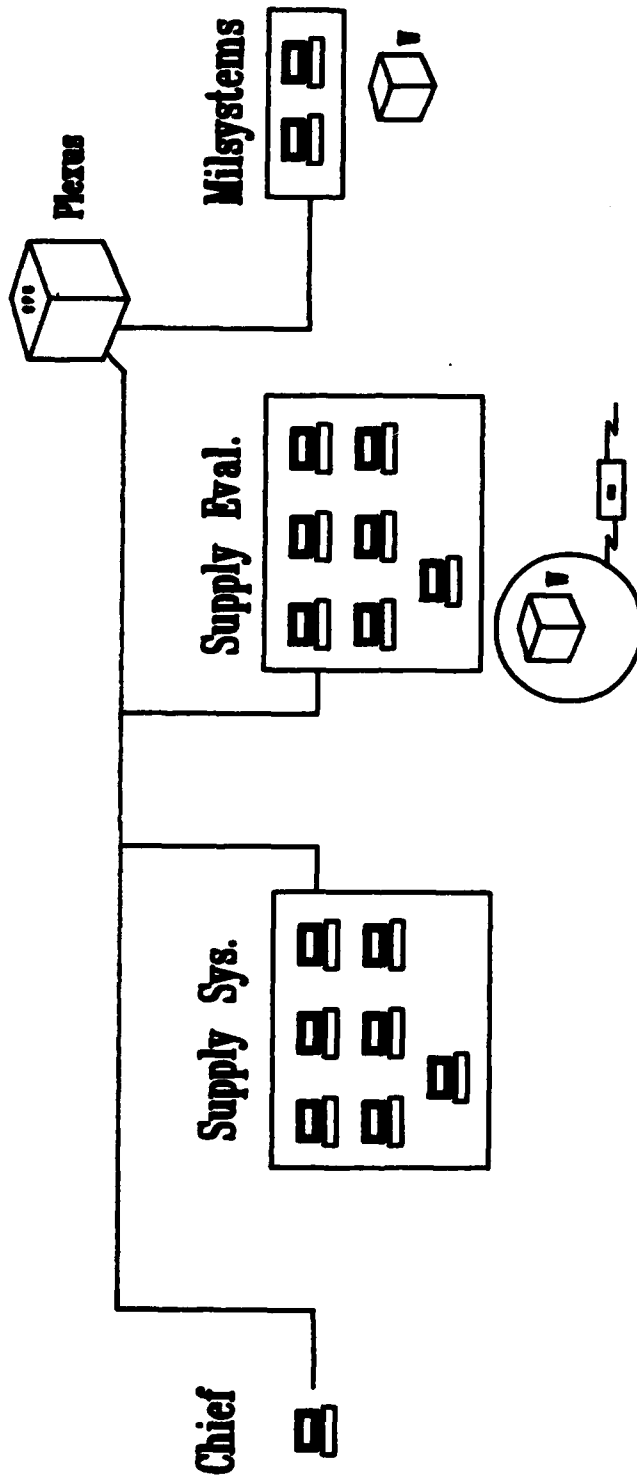
Equipment Deployment and Deployment Evaluation Branch

Major functions of this branch include monitoring and reporting on Army equipment, special studies and reviews pertaining to vehicles, and analyses of weapon systems.

Logistics Engineering Branch

Major functions of this branch include reporting maintenance issues submitted from world-wide units. Reports from this branch provide standardized information, Army-wide, on repair time, parts, training, test equipment, tools, facilities, and failure rates with respect to Army equipment maintenance.

Supply Division



 Printer Access - All Units

Hardware

47

Supply Division

The key function of the Supply Division is to serve as AMC's interface between suppliers and customers to improve communications, ensure understanding, and facilitate exchange of ideas. This division also evaluates new regulations and procedure proposals for impact upon other levels of the Army Supply System.

6 RECOMMENDED AUTOMATION CHANGES WITHIN MRSA

This chapter discusses recommended changes to equipment and connectivity.

The information is presented by division (and within division by branch) for all of MRSA.

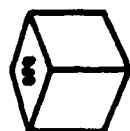
The material is organized as follows:

--> visual diagram of data flow and usage, and

--> textual description of recommended automation changes for the division.

Overlays which diagram the recommended changes are used to allow comparisons with the existing equipment and connectivity.

Symbol Legend



C P U



VME PC



HP PC



INTEL 386



TERMINAL



Aldo Word Processor



Modem



File Form



Scanner



Tape Drive



Printer



Laser Printer



Notes

MPSA LAN

INTEL ETHERNET

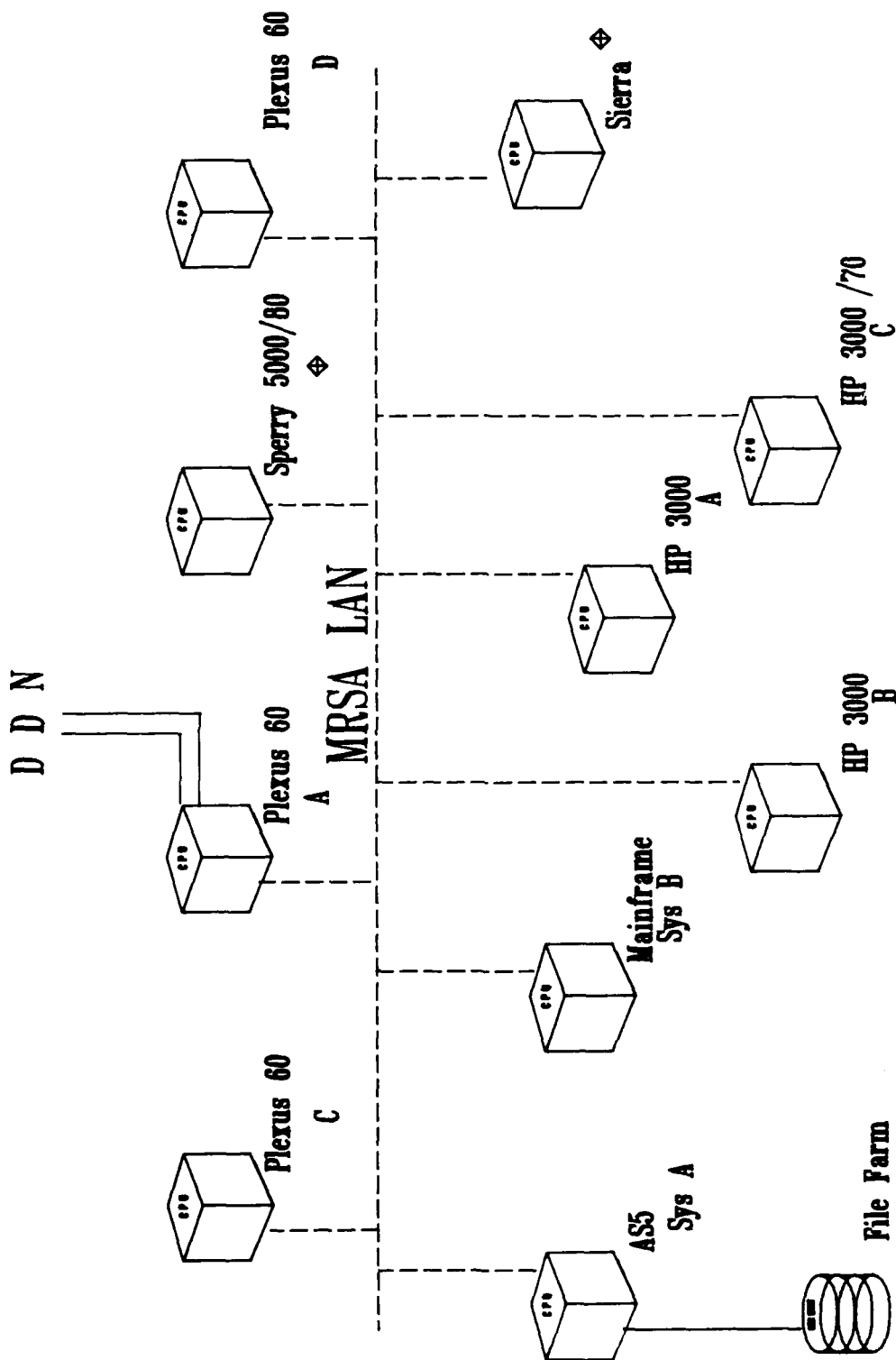
MANOWIZ

IBM LINK

ADAPT TO PROTOCOL

? ?

M R S A L A N



Logical View of the MRSA LAN

The diagram on the previous page illustrates the recommendation for top (third) level processing within MRSA. (See Chapter 4 for a discussion of workstations and three-tiered processing.) It also shows one of the Plexus 60 machines (Plexus-A) as the gateway machine to the DDN (Defense Data Network). The thought is that a Plexus computer will be far more acceptable as a DDN host than the some of the other large processors. Also, the new Sperry 5000/80 machine (which is the recent Army approved minicomputer) has been approved by DCA as a DDN host. The Sperry 5000/80 also supports 4.2BSD networking and TCP/IP protocols which makes it a very good candidate for being a DDN gateway machine. We recommend that the Sperry 5000/80 machine be strongly considered when additional processors are acquired. The machine can be configured from one to four Motorola 68020 cpus. Thus, one can simply add a cpu board to increase processing power.

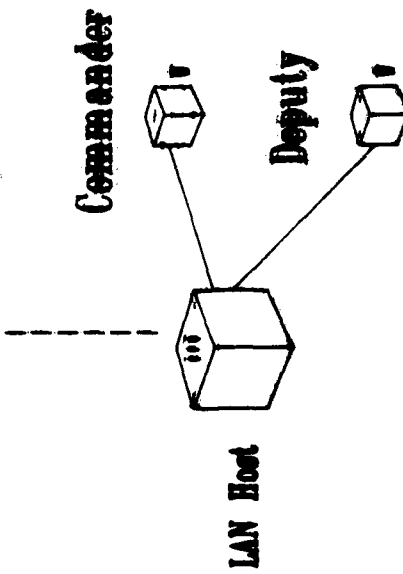
The diagram shows all top level processors at MRSA connected to a MRSA LAN TCP/IP Ethernet and also shows projected and/or recommended processor procurements (a Sperry 5000/80 computer for IMD distributed workload and a Sierra class processor targeted for MRSA-wide applications). One of the more important aspects of the MRSA LAN is that each of the LAN hosts shown on this diagram is considered a *global* MRSA resource; each processor should be thought of as a shared resource. Timely and important processing activities may be targeted for more than one processor (in case one of the machines goes down). This environment will allow applications to migrate from one processor to another as the MRSA work load changes over time. Diagrams in following sections show the division connections to the MRSA LAN through processors labeled as LAN HOSTS. The intent is to promote the concept of resource sharing with this kind of generic presentation. However, one of the AS/5 machines should not be a shared resource. One of the two AS/5 machines should be targeted to process all of MRSA's sensitive data processing requirements. This isolates the sensitive processing to one machine and makes it easier to inhibit access to that one machine from the rest of the MRSA LAN when this kind of processing is being performed.

The intent is that the top level network within MRSA address only processor to processor communications. The MRSA LAN at this level is designed to promote remote logins, distributed data base applications, and the concept of a *file farm* that will eventually move from the AS/5 to hang directly off of the LAN. The file farm will provide common data storage for all processors on the LAN. Users will be able to ask for files regardless of the LAN host originating the request. The file farm can be used as a mass storage and common database source for the LAN hosts.

We initially show the file farm hanging off of one of the AS/5 main processors. In its early implementation, the file farm would simply consist of a large amount of disk storage accessible only through the AS/5 (via the LAN) to relieve the current demand for more storage space.

Office of the Commander

MBEA LAN



Printer Access - All Units

Office of the Commander

Commander



Deputy



Printer Access - All Units

Hardware	Software	Function
1. Processor 2. Memory 3. Storage 4. Input/Output Devices 5. Network Interface	1. Operating System 2. Application Software 3. Device Drivers 4. Network Protocols 5. Security Software	1. Processing Data 2. Storing Data 3. Retrieving Data 4. Communicating Data 5. Protecting Data

French- Unit	Commander	1	1
-----------------	-----------	---	---

A grid of graph paper with a decorative border on the left side. The border features a repeating pattern of stylized leaves and flowers. The grid is composed of small squares, and there are several small black marks or symbols scattered across the grid, including a cross-like shape and some small dots.

Hardware

IBM Network
HP Work
Wye-78
Heng 30
ADS 30
ADS 30
Tadrix
Plexus
Elec. Mfg.
S/S
HP 3000
Amis
Lexix
Ware
HP Word
HP Word
Lotus
Graphics
Statistics
Office Auto
Program's
Reports
Graphics

[illegible]

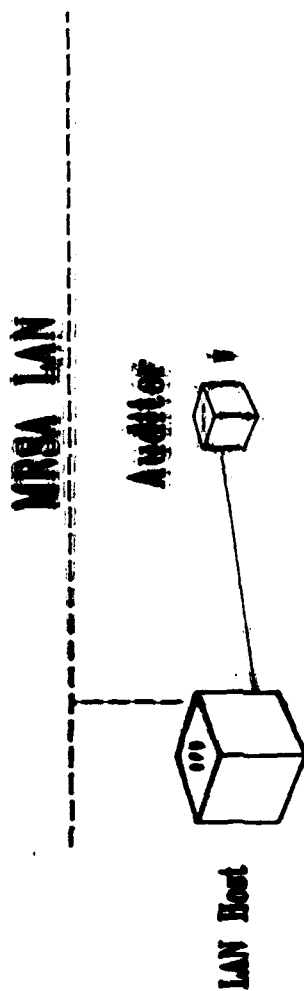
Office of the Commander

As the diagram illustrates, the PCs in the commander's office should be hardwired to a LAN host processor. Access to a LAN host computer gives the commander's office EMail (electronic mail) access to all other MRSA users via the MRSA LAN and also provides DDN access. These PCs should be functionally targeted as devices to be upgraded to *manager* workstations. Uses such as EMail, electronic bulletin boards, and calendar schedulers become immediately available to users of Plexus (UNIX operating system) computers.

To facilitate administrative use of these two workstations, it might be advisable to plan on upgrading the configuration to include touch screen monitors.

This office and its staff should be candidates for manager workstation training courses developed by IMD.

Internal Review and Audit Compliance Office



Internal Review and Audit Compliance Office

Auditor



Printer Access - All Units

Hardware	Software	Function
1. CPU	Operating System	Process Management
2. Memory	Application Software	Data Management
3. Storage	Database Management System	Data Storage and Retrieval
4. Network Interface	Network Protocol Stack	Network Communication
5. Peripheral Devices	Device Drivers	Input/Output Operations

— 1 —

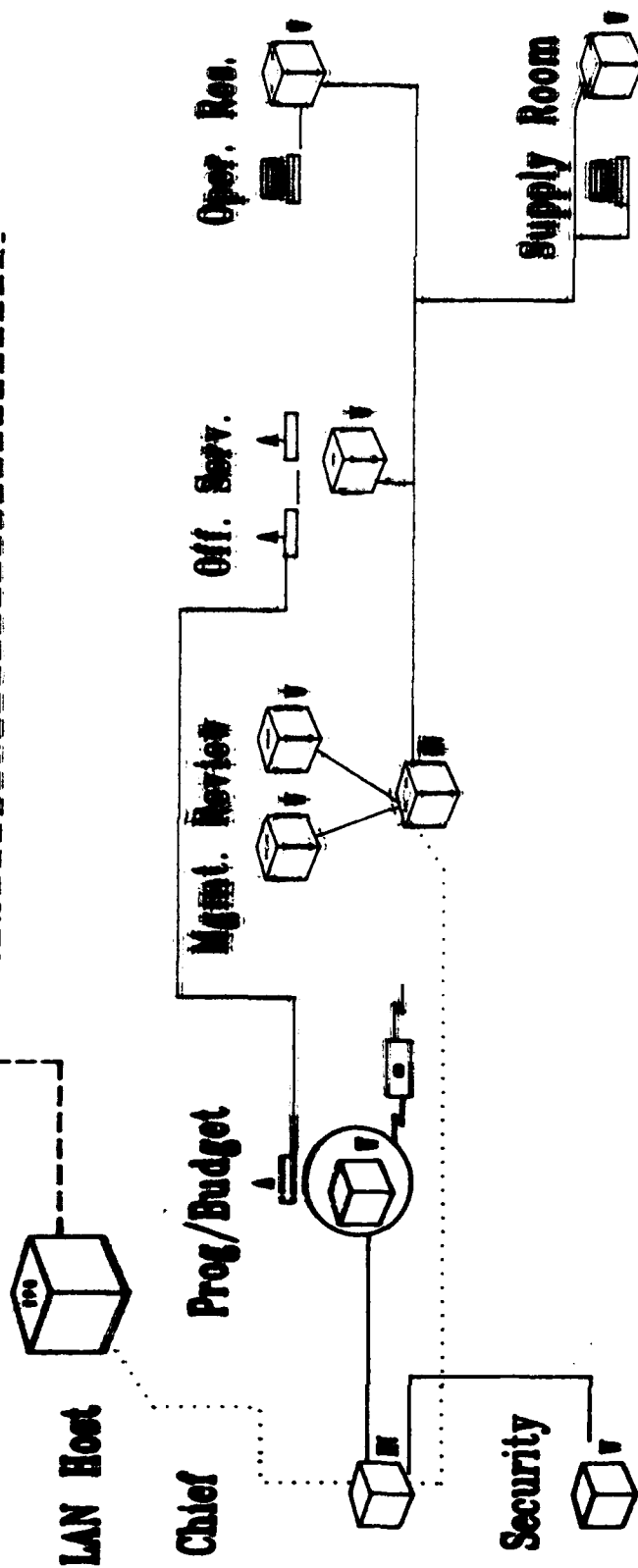
This image shows a full page of graph paper. It features a uniform grid of small squares covering most of the area. On the far left, there is a narrow vertical column that serves as a margin; it contains several plus signs (+) acting as row indicators. The rest of the page is a continuous grid of squares, suitable for drawing or plotting graphs.

Internal Review and Audit Compliance Office

The PC standalone in this branch is shown connected to one of the host machines on the MRSA LAN. This will provide access for this office to the MRSA LAN and all automation resources (hardware and software) accessible from it. This office and its staff should be candidates for manager workstation training courses developed by IMD.

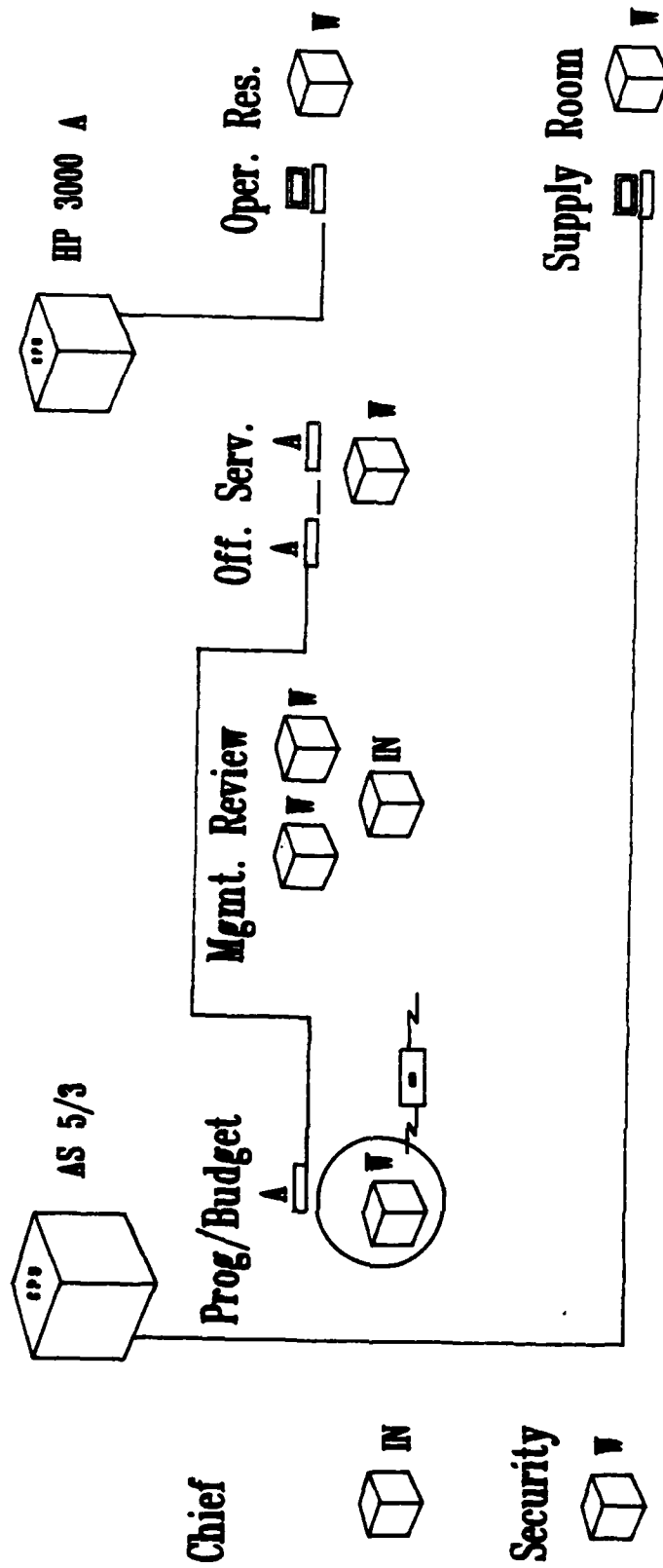
Resource Management Division

MRSA LAN



 **Printer Access - All Units**

Resource Management Division



Printer Access - All Units

Resource Management Division

Branch- Unit	Hardware										Software										Function									
	Netw	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	W. Syst	Com. Auto	Office Auto	Programs	Reports	Graphics	Graphics	Graphics	Graphics	Graphics	Graphics
Chief																														
1																														
Prog/Budget																														
1																														
2																														
Mgmt. Review																														
1																														
2																														
3																														
Off. Serv.																														
1																														
2																														
3																														
Oper. Res.																														
1																														
2																														
Supply Room																														
1																														
2																														
Sec. Vault																														
1																														

Resource Management Division

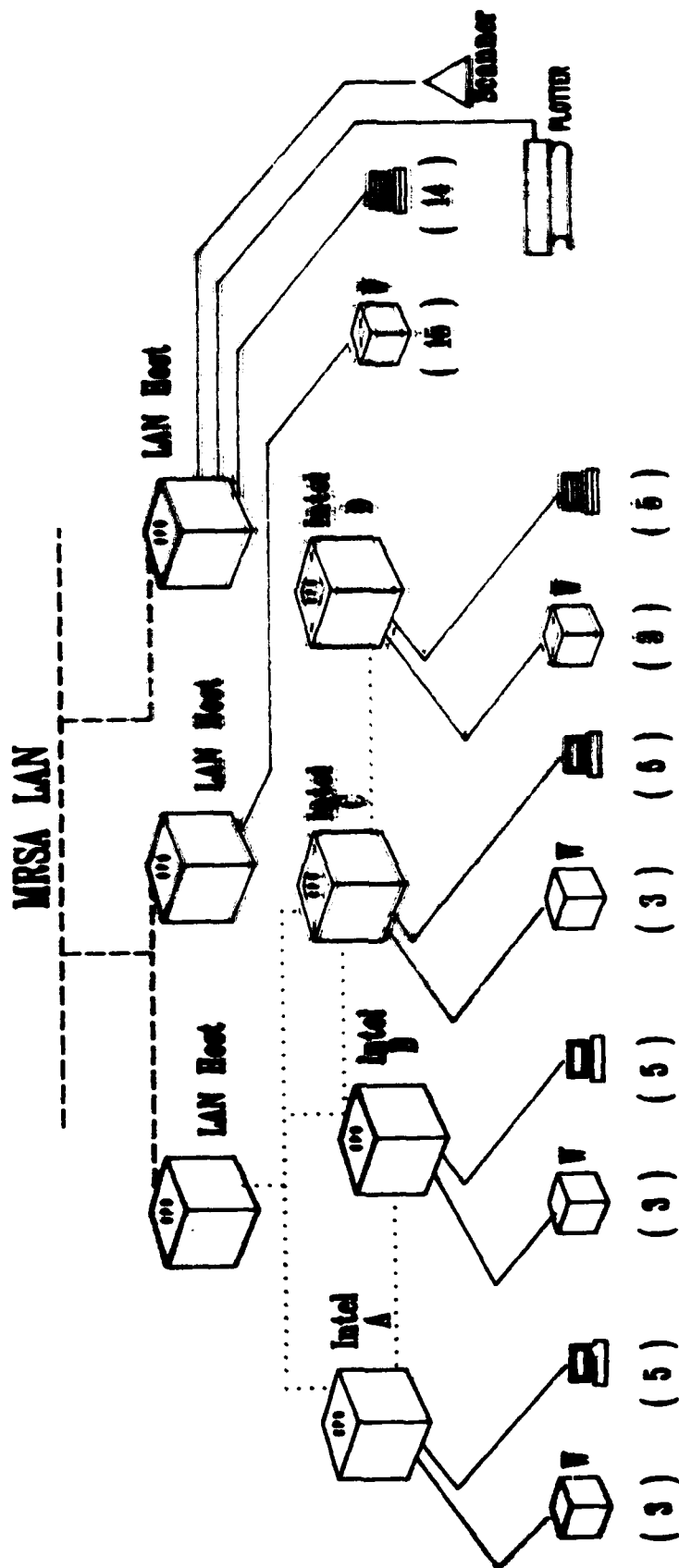
The Intel 310s should be configured together via the available Intel Ethernet. This series of Intel processors networked together provides an intermediate (second) level of processing for the division. Utilities and database applications can be developed and downloaded to this environment for division processing. All access to the MRSA LAN is designed to be provided through one of the host computers on the MRSA LAN via the Intels. It is the task of this computer to act as a gateway machine; in this case, to translate Intel Ethernet protocol (Intel does not provide a TCP/IP protocol on their Ethernet which links the 310s) into TCP/IP protocol.

All PCs and terminals are designed to be hardwired to one of the 310s for intermediate level processing.

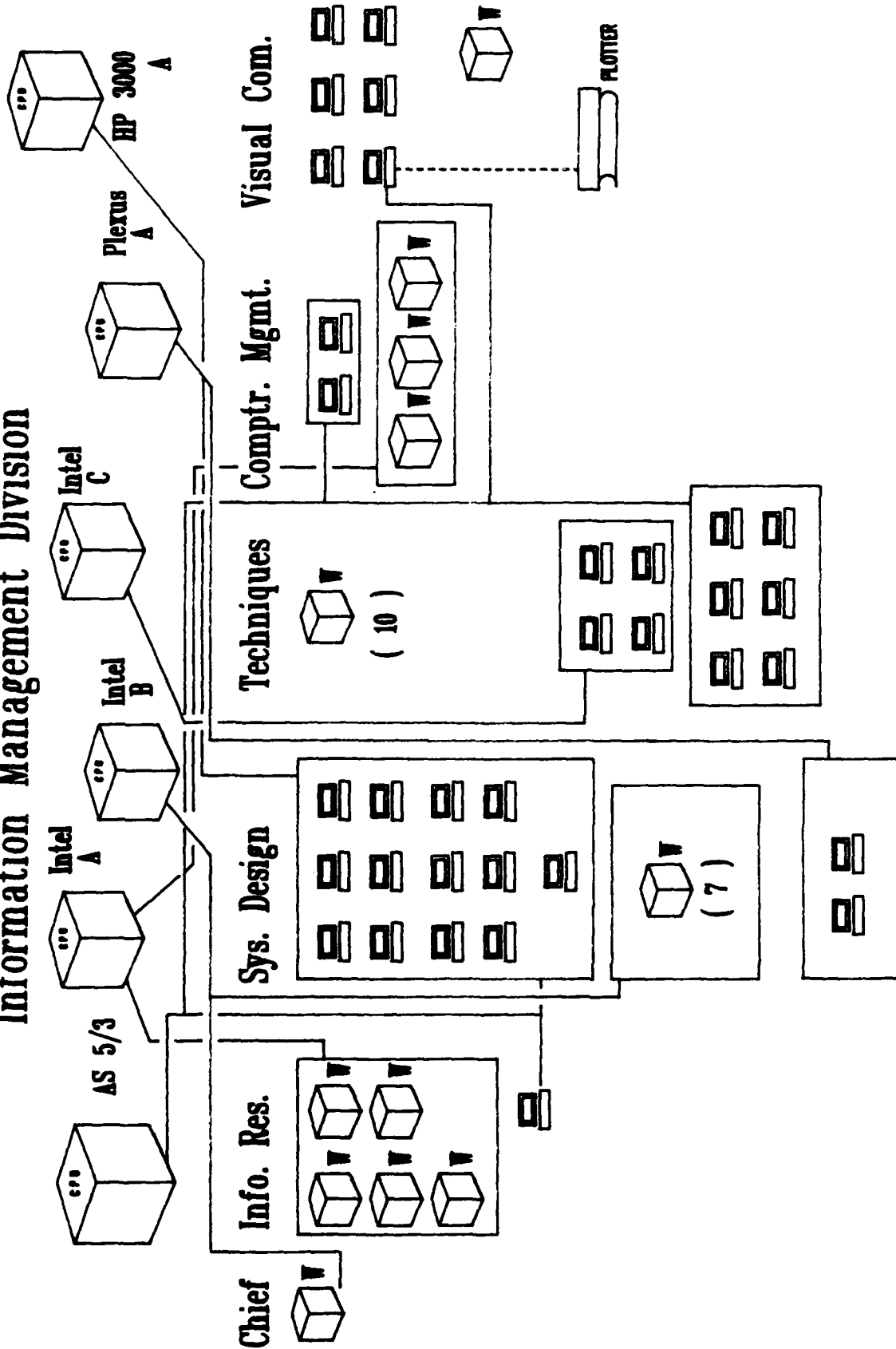
This division also needs interactive access to a full, comprehensive statistical package within the MRSA LAN environment.

The full range of functional workstation design (and its consequent training) should be implemented within this division.

Information Management Division



Information Management Division



Printer Access - All Units

Information Management Division

Hardware

Software

Function

[illegible]

Hardware

[illegible]

Information Management Division (p.2)

Hardware

Software

Function

Branch-
Date

Technique

1 2 3 4 5 6 7 8 9 10 11

Information Management Division (p.2)

[illegible]

Hardware

THE

Information Management Division (p.3)

Branch- Unit	Hardware										Software										Function									
	RA	Netw	Wp	Wp	Field	ADP	ADP	ADP	ADP	ADP	ADP	ADP	ADP	ADP	ADP	ADP	ADP	ADP	ADP	ADP	Com	Office	Office	Office	Office	Office	Office	Office	Office	Office
12																														
13																														
14																														
15																														
16																														
17																														
18																														
19																														
20																														
Comptr. Mgmt.																														
1																														
2																														
3																														
4																														
5																														
Visual Com.																														
1																														
2																														
3																														
4																														
5																														

Information Management Division (p.4)

Information Management Division (p.4)

Branch- Unit	Hardware										Software										Function									
	BA	Network	HP	Wang	Wang	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM	IBM
6																														
7																														

Information Management Division

The logical configuration and connections on the IMD diagram do not reflect the suggested unbundling of all computer programming support to the divisions, although it is necessary that IMD control and manage the process. It is necessary that the changing direction in IMD's mission be effected and the personnel needed to perform that mission be placed at the same time that the divisions are gearing up to acquire their own programming support. It is up to IMD to provide MRSA with a scenario delineating a timed implementation of this process. The process may take from 3 to 5 years to implement a graceful change of function within IMD and within the MRSA divisions. The acquisition and implementation of the MRSA LAN products and processors are expected to make this process much more congenial for all parties. It is desirable that the immediate emphasis within MRSA and within IMD be the implementation of the MRSA LAN; thus, we show the IMD diagram with the same branch configuration as in Chapter 5.

Due to the amount of programming support needed within MRSA, a configuration to support more effective utilization of that programming support is provided. For example, we recommend the acquisition of another Plexus 60 computer (a Sperry 5000/80 may be more easily procurable and serve just as well) and another Intel 310 for this use. The diagram design addresses the problem of competitive access to resources by distributing the communications access and providing a hierarchy for also distributing the applications. All access to the MRSA LAN is provided through two MRSA LAN host computers. It is necessary (as in the Resource Division scenario) that one of the computers act as a gateway machine between an Intel Ethernet and the MRSA LAN.

One of the goals of this design is to provide a framework in which the distribution of MRSA's programming workload can occur. It is expected that database applications and developments for other machines across the LAN could be designed and developed locally (on the intermediate level processing provided by the Intel net or on those MRSA LAN host machines which support an excellent system development environment, such as the Plexus machines and the Sperry machines). In this respect, IMD should be tasked with developing/acquiring and overseeing the implementation of a fourth-generation language DBMS which could be used across the variety of MRSA processors. Initially, emphasis should be given to providing a flat, ASCII file interface between the current products available on these processors (Intel 310s, Plexus 60s, HP 3000s, AS/5s, and the Sperry 5000/80). This would make it possible for applications which access a common data base source (resident on one machine or a file farm) to download the desired data fields for only that application to another processing environment (like the Intels or the Plexus or the Sperry machines). With very fast data transfer at the MRSA LAN level (2 to 10 Mbs) and fast data transfer from the LAN gateway machines to the Intel nets, it is quite reasonable to distribute applications and developments from the database host machine.

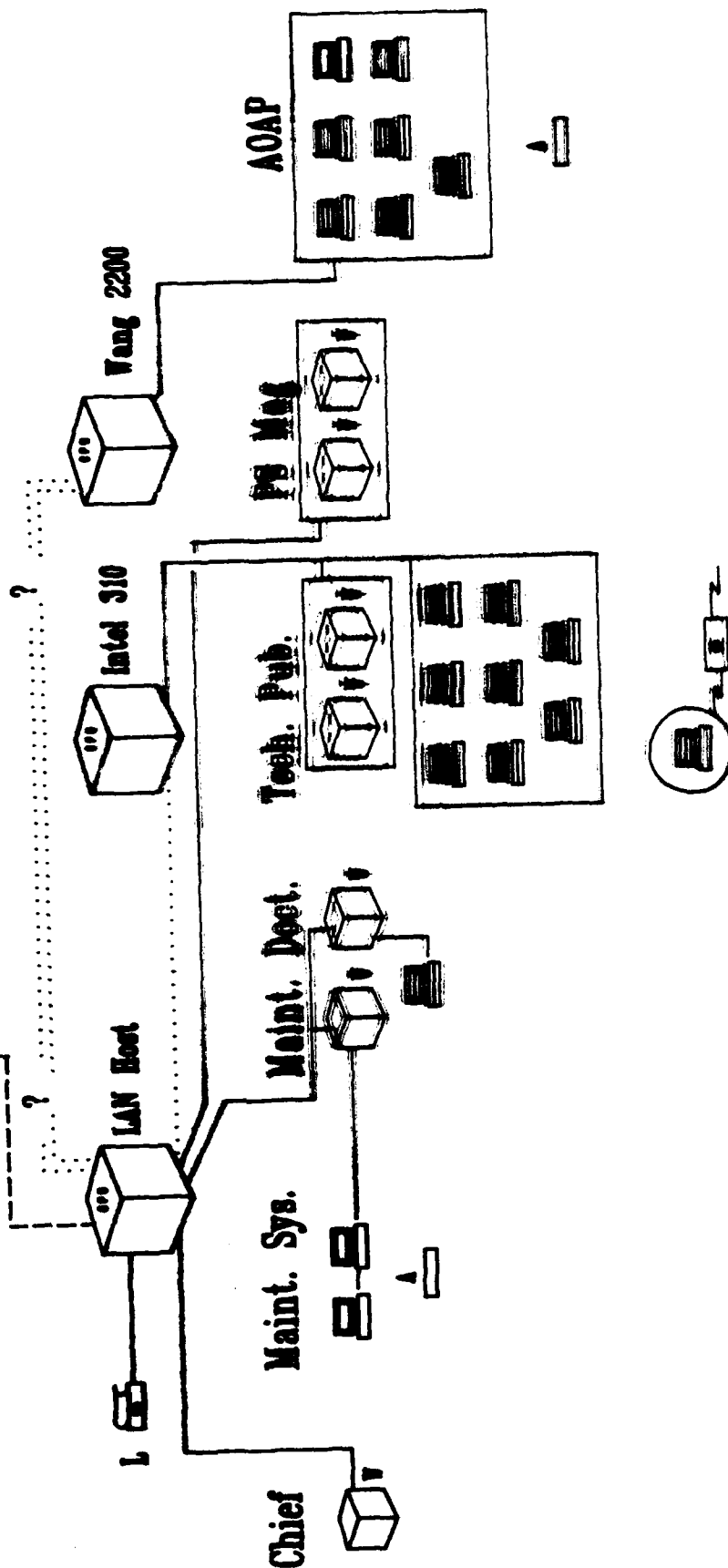
The full range of workstation environments fall into the functions of this division (with a heavy emphasis on the programming/analyst and manager type workstations).

Other automation resources that are shown as being needed by various functions within IMD are:

- an optical scanner (configured on one of the MRSA LAN host machines. Sperry offers an optical scanner on its Sperry 5000/80 machine). The quick transfer of hard copy to machine readable text is a necessity (for areas like the Information Resources branch),
- another Tektronics jet printer for the Visual Arts branch. The need for a system backup and the heavy work load being processed justifies this acquisition.

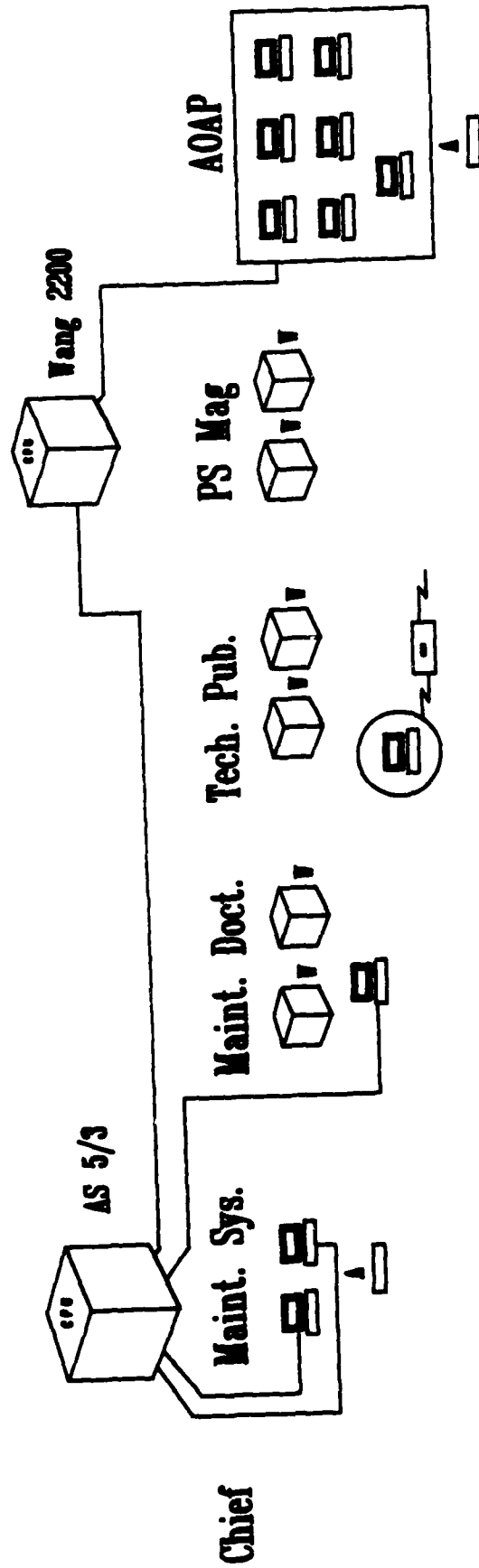
Maintenance Division

MRSA LAN



Printer Access - All Units

Maintenance Division



 Printer Access - All Units

Maintenance Division

[illegible]

Maintenance Division

Branch- Unit	Hardware			Software			Function						
	Chief	1	2	Chief	1	2	Chief	1	2	Chief	1	2	3
Chief													
Maint. Sys.													
1													
2													
3													
Maint. Doct.													
1													
2													
3													
Tech. Pub.													
1													
2													
3													
PS Mag													
1													
2													

Hardware	Software	Function
1. Processor 2. Memory 3. Storage 4. Input/Output Devices	1. Operating System 2. Application Software 3. Database Management System 4. Network Software	1. Processing Data 2. Storing Data 3. Retrieving Data 4. Communicating Data

1

84

Maintenance Division (p.2)

Branch- Unit AOAP	Hardware			Software			Function		
	Relay Control Unit	Electronic Control Unit	Relay Control Unit	Relay Control Unit	Electronic Control Unit	Relay Control Unit	Relay Control Unit	Electronic Control Unit	Relay Control Unit
1	+			+			+		+
2	+			+			+		+
3	+			+			+		+
4	+			+			+		+
5	+			+			+		+
6	+			+			+		+
7	+			+			+		+
8	+			+			+		+

Maintenance Division

Maintenance Division has a Plexus 60 computer (projected MRSA LAN host) in the procurement process. The diagram reflects the proposed recommendation; that this machine be used as this division's gateway machine to the MRSA LAN. All existing processors and terminals within the division are shown linked to the MRSA LAN host.

The AOAP branch is still shown using the Wang 2200 as its intermediate level processing environment (second level). The Wang 2200 is shown as being networked to the MRSA LAN host, thus providing the AOAP users with access to that machine and the MRSA LAN. It should be noted, however, that there is not currently a clear product which will integrate the Wang to other machines. The Sperry 5000/80 has IBM connectivity provided, and thus, may be a resource that could be used as an interface/gateway to the Wang. Until a gateway product can be acquired for this purpose, it is reasonable to provide hardwire (96 Kbaud) lines between ports on the Wang and ports on one of the MRSA LAN host processors and/or a switch facility so that the AOAP users may turn a switch on a black box to provide either 96K access to the Wang or 96K access to the MRSA LAN host. The black box takes one incoming line from the terminal to the box and conducts the communications through one of two lines emanating out of the box (one line to a port on each machine). An approach which would save communication lines would be to configure an 8-port statistical multiplexor over one 96K baud line between the Wang and the MRSA LAN host. Any user of the Wang would then be able to compete for one of the 8 ports to the LAN host at some percentage of 96K baud.

One Intel 310 and eight more terminals are recommended to service the Technical Publications branch within the division. All of the terminals, plus the two PCs within that branch could then be configured to the Intel 310 which would be linked to the MRSA LAN host.

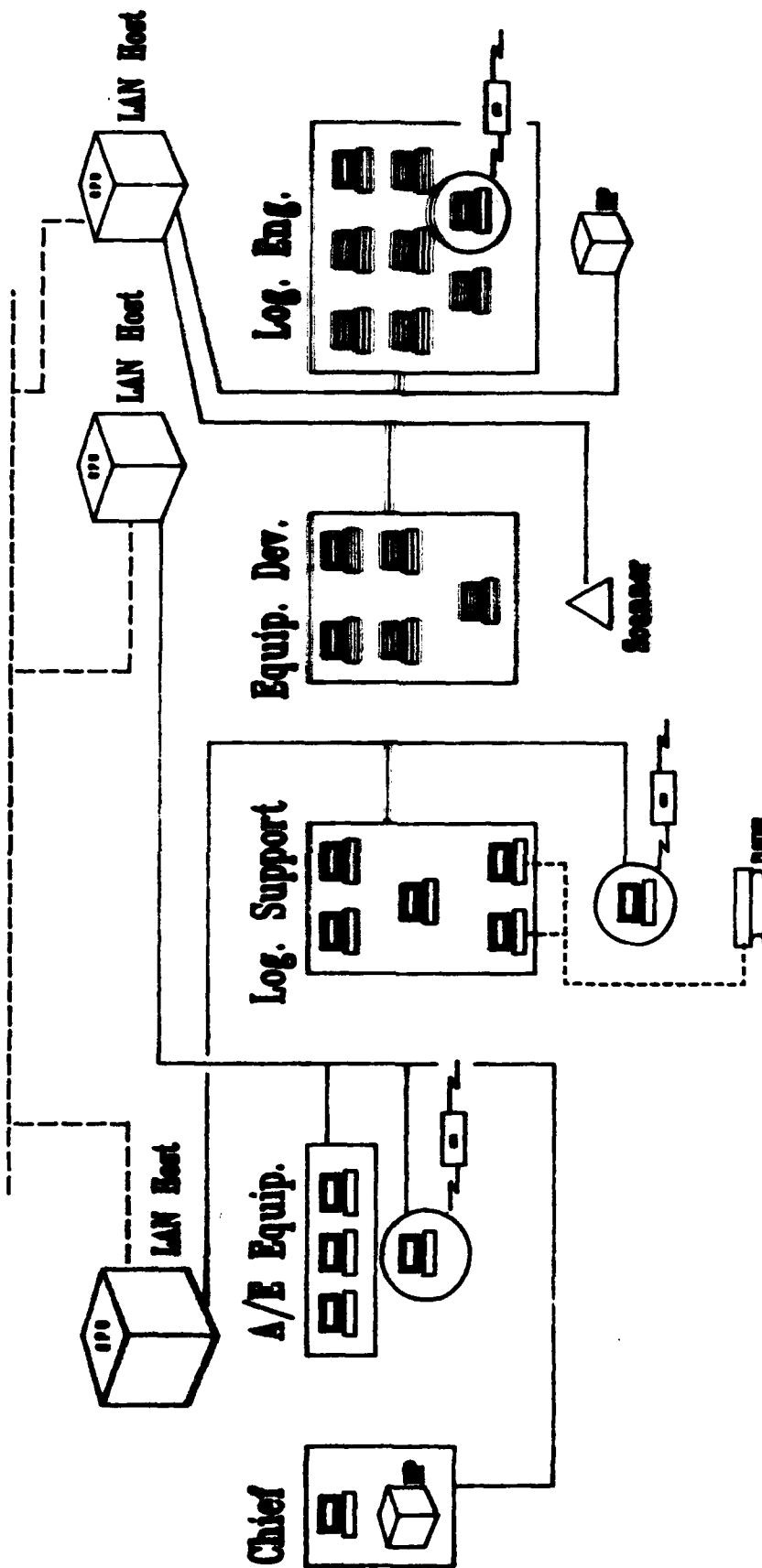
Other automation resources shown as being necessary components within this division are:

- a PC for the division Chief (Wyse PC) to provide the basis for a manager workstation,
- a laser printer (configured on a LAN host such as a Plexus or Sperry machine) to support and enhance the publications and word processing requirements within the division.

This division is a candidate for intensive training in the use of equipment and software utilities which will enable it to more effectively use the shared automation resources within MRSA. The emphasis in this division should be on the development of manager and clerical workstations. The function of the clerical workstation is to support document preparation and publication utilities.

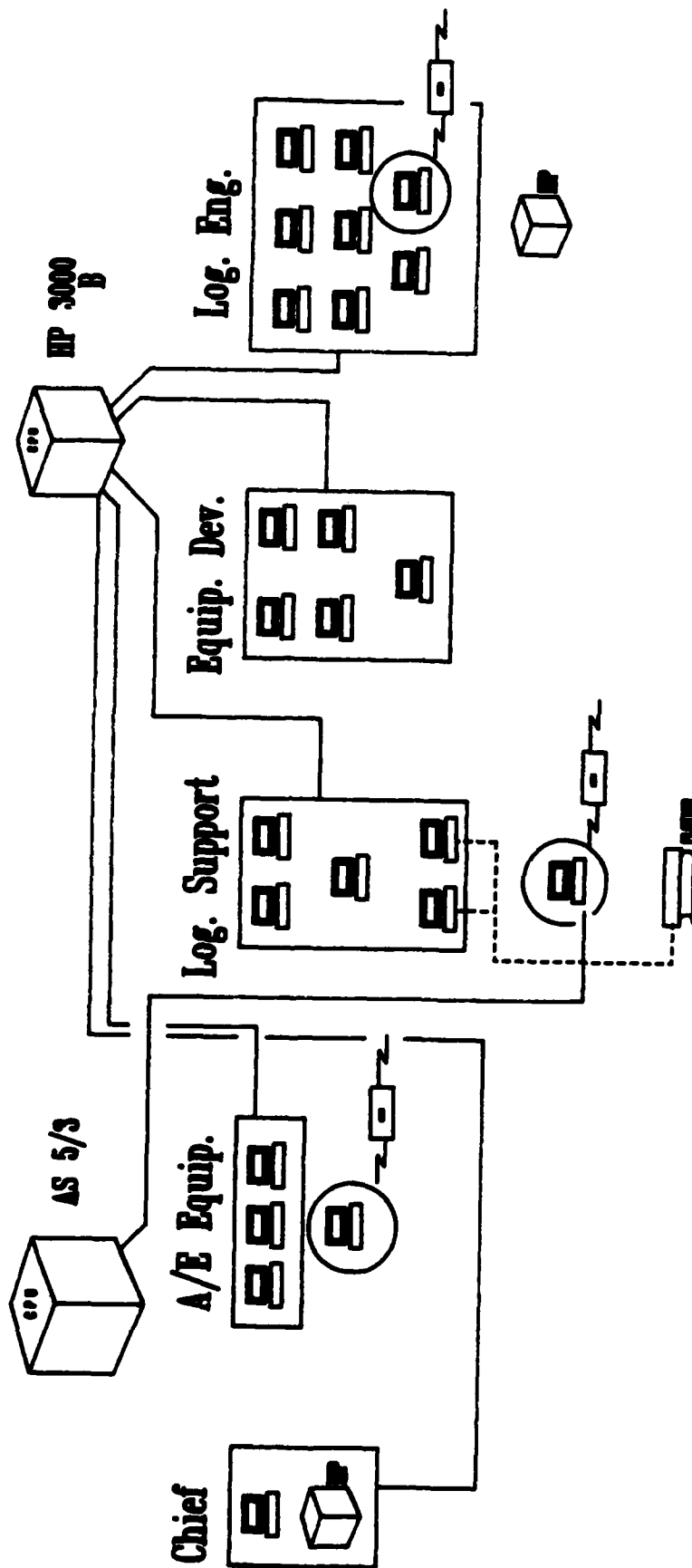
Readiness Division

MRSA LAN



Printer Access - All Units

Readiness Division



 Printer Access - All Units

Hardware

2010

Function

90

Readiness Division (p.2)

[illegible]

Branch- Unit	Log. Eng.	1	2	3	4	5	6	7	8	9
-----------------	-----------	---	---	---	---	---	---	---	---	---

Readiness Division (p.2)

Hardware

Software

Function

Index

Unit

省

1

1 2

20

7

2

—

•

2

●

•

[illegible]

A 20x20 grid with the following plus signs (+) placed in the cells:

- Row 1: Columns 2, 3, 4, 5, 6, 7, 8, 9.
- Row 2: Columns 4, 5, 6, 7, 8, 9.
- Row 3: Columns 4, 5, 6, 7, 8, 9.
- Row 4: Columns 2, 3, 15.
- Row 10: Columns 2, 3, 4, 5, 6, 7, 8, 9.
- Row 15: Column 15.
- Row 19: Columns 2, 3, 4, 5, 6, 7, 8, 9.

Readiness Division

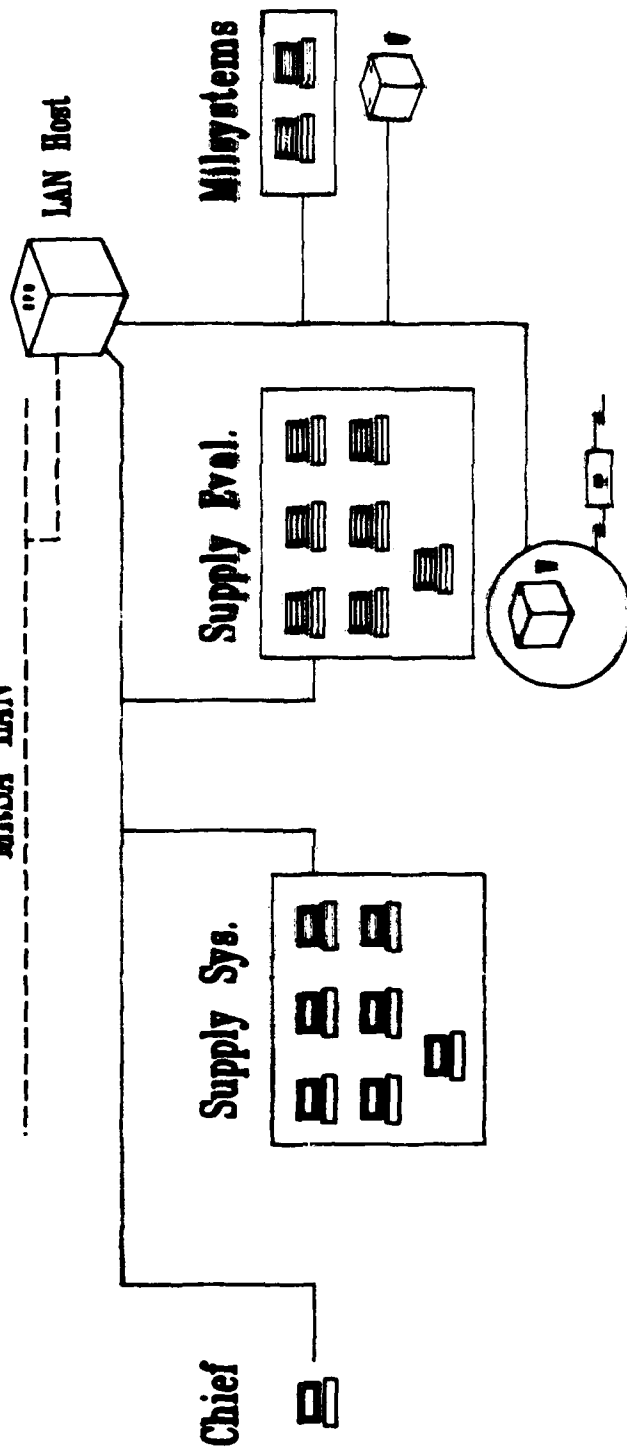
The diagram shows the Readiness Division PCs and terminals being configured into three level 1 processors (MRSA LAN hosts): these processors would probably be the HP 3000, a new HP 3000/70, and access to another of the MRSA LAN host computers to support a number of projected applications (including the Integrated Logistics Support Lessons Learned system).

Other automation resources needed to assist this division in its mission:

- an optical scanner (configured on one of the HP 3000 machines or on a Sperry 5000/80),
- access to an interactive, comprehensive statistical package.

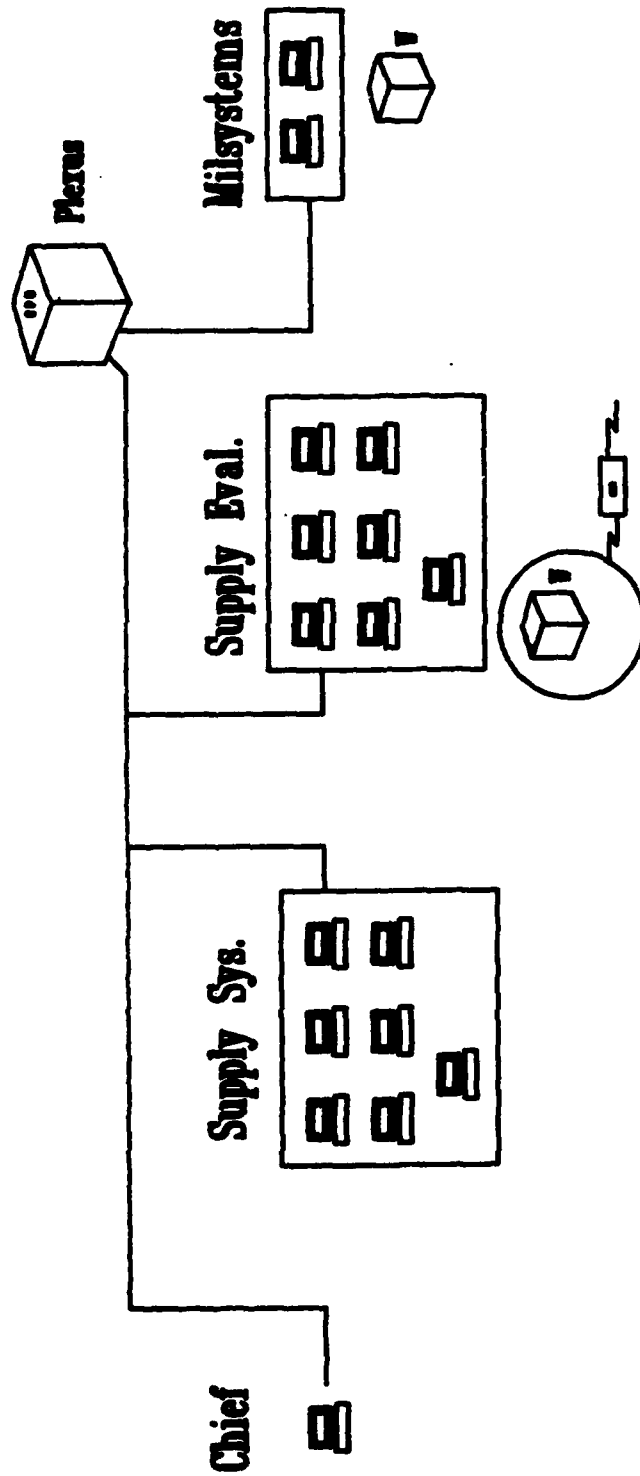
Supply Division

MRSA LAN



 Printer Access - All Units

Supply Division



 Printer Access - All Units

Hardware

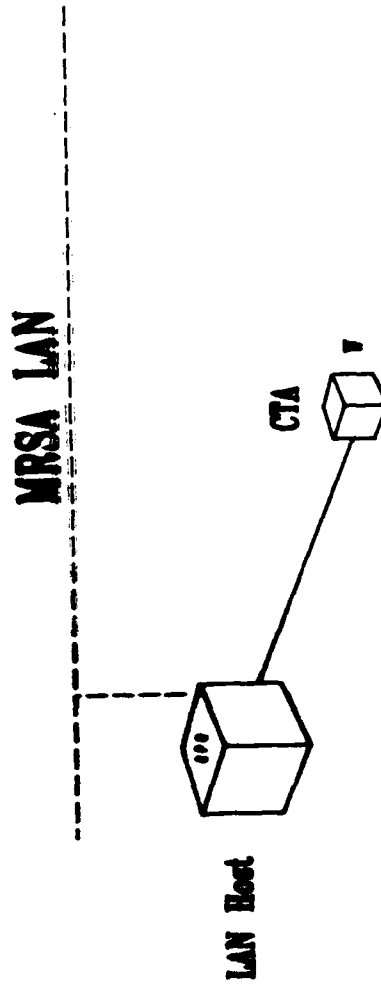
[Illegible handwritten notes]

Function

2.

Central TMD&E Activity

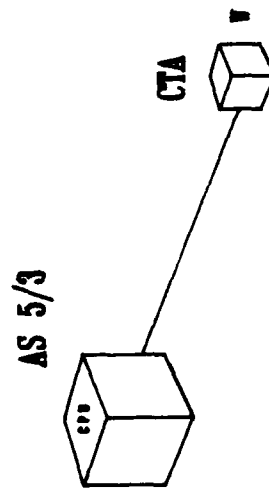
MRSA Client



 Printer Access - All Units

Central TMD&E Activity

MRSA Client



 Printer Access - All Units

General Comments on Proposed Changes and Network Implementation

It is expected that the implementation of this MRSA automation plan will take place over a period of time. The implementation will depend on the speed in which funding (for the LAN materials) and expertise in managing this type of network can be transferred to MRSA. The first priority should be addressed to establishing a MRSA LAN (see the first diagram in this chapter) which will support processor to processor resource sharing.

The proposals in this section, especially regarding the networking strategy and the three-tiered processing environment, will allow a configuration that will be adequate for the next 10 to 20 years. Advances in hardware and software technology will tend to be directed toward the three-tiered environment and should easily be compatible to this kind of processing environment.

It is very important that a MRSA function take the responsibility for maintaining, integrating new resources, and keeping track of new technology applicable to networking and distributed processing. New workstation (end-user) technology, improved high level and intermediate level processing, mass storage devices, and distributed software concepts can be placed into this kind of a network and processing environment. Our suggestion is that IMD should be tasked with tracking technological advances, as this task would fit well with conducting and coordinating in-house training.

7 SECURITY CONSIDERATIONS FOR AUTOMATED RESOURCE MANAGEMENT

Computer security covers both physical security and logical security. The former is enforced by locked doors, guards, and similar precautions; the latter, by passwords, file permissions, and audits. The focus of this chapter is toward logical security, including computers, networks and associated software, users, and administrators.

The goal of MRSA should be to strike a reasonable balance between security and ease of communications. There is a direct correlation between security and ease of communications: the greater the security, the more limited and difficult the communication. Within MRSA, the emphasis should be placed on ease of communication to include communication across boundaries of the organization, technical disciplines, and physical locations.

An obvious, but often overlooked, characteristic of computer security is that it should correspond to the value of the information involved. There should be multilevel security ranging from minimum through medium to maximum, keyed to necessary levels of data protection. Sensitive data should be totally isolated from other kinds of information, and access to sensitive data should be very tightly controlled.

Common security concerns within MRSA are: (1) to protect valuable information from theft, alteration, and destruction when it is stored in computer files or transmitted over data lines, (2) to prevent unauthorized use of computer time and resources, and (3) to assure a high level of security awareness among the computer users and the system administrators. The goal is to maintain a consistent, cohesive set of administrative controls for the entire computing environment including hardware, software, and people.

Again, the most important place to start with computer security is with the people involved: the users and the administrators as well as their supervisors. The biggest threats to security are carelessness--logging in to use a computer and then leaving the terminal unattended, sharing passwords for computer access, and putting sensitive material into inappropriate computer files.

System Security

Each of the processors accessible via the MRSA LAN should be assigned a system administrator. There may be different system administrators for each system; however, all would have the same following functions:

- allocate usercodes and passwords for the users of the computer.
- control access to shared data. Keep an ACL (access control list) for those databases so that only valid usercodes have access to that data. If a 4th generation DBMS is used to access the data, the access can be controlled via the DBMS tools; however, if the access to the shared data is by custom programs, the programs should be modified to identify the user and restrict those usercodes which are not authorized on the ACL.

- set up user profiles so that each user is limited in the number of disk resource units and cpu resource units that can be used.
- use audit routines to monitor system and user usage.

Another aspect of system security involves accountability, defined for all involved with the computer system: user, administrator, and supervisor. All uses of computers require authorization by supervision in order to assign management responsibility to control by whom and for what purpose machines are used. To this end, every machine should have a list of authorized users. Of even broader benefit to MRSA would be a directory of computers with dial-up (or any kind of external access like networks) access, including identification of organizations associated with particular computers, phone numbers, system administrators, and cognizant management.

Passwords

In addition to the precaution of "one person, one password," computer security can be increased by using more complex passwords. Users often use their first names (spouses' names, pet names, birthdays, etc.) as their password. In breaking passwords, a machine can quickly run down a list of first names or the 20,000 most common words in the English language, as well as all possible birthdays. A more complex alternative would be a password of six to eight characters which contains both digits and letters (a mixture of upper and lower case is also very good). This type of password is extremely hard to break.

Passwords must not be "for all time." Passwords must be changed with some frequency, ideally determined and controlled by the system administrator.

Dealing With Data Destruction

Normal file backup in a tape rotation is recommended for each level 1 processor (MRSA LAN cpu). This task would be the responsibility of the computer operations support group of IMD. There are a number of excellent tape backup algorithm schemes. The rotation algorithm should be good enough to allow a user to have a file restored to the state of the previous evening's tape dump (incremental dump). Users should be able to ask for file restoration (when a file is inadvertently corrupted) from tape via electronic mail: specifying the computer on which the file should be placed, and the directory and full path name of the file to be restored.

Besides the normal tape rotation algorithm schema, we suggest that a procedure be established by the IMD operations support group to backup each computer's file system twice a year to an external (off site) storage space. This will mean that a physical data backup will exist to protect against catastrophic destruction at the operations site.

The data manager for each data base should take responsibility for providing adequate backup for the data base in a manner to complement the activity of the normal system support mechanism. Thus, data base managers should be encouraged to make periodic backups of their data base and store the

tapes outside the physical area where the normal system backup tapes are stored.

Data File Security

Special software tools should be used to increase file security by limiting general access to the files of individual users. Information in files should be handled so that the default access granted is to its creator, unless that person explicitly grants access to others. Data base security should be handled (as noted earlier) in the same way; the creator (or data base administrator) should set up an ACL to comprise only those users who need access to the data base. If the OS (operating system) or DBMS does not support this activity, a series of software tools must be created to perform this function.

Network Security

There are two different methods of providing secure network communications. The first is to make the transmission medium physically secure (make it impossible for anyone to tap into or "bug" it). The second is to encrypt the transmitted data. Within MRSA there is no need to encrypt the communications across the "in-house" MRSA LAN (and its subnets), as long as sensitive data is restricted to one computer and it is not disseminated via the MRSA LAN.

This leaves the problem of physical security to be addressed. This can be handled quite adequately with today's technology. One solution is to use pressurized cabling, which has been used for several years by the telephone company (AT&T), consisting of communications cables sealed in plastic and pressurized at both ends of the lines. Monitors with alarms are attached to the line to measure the pressure. If a drop is detected, a break in the cable is assumed and a repair can be initiated. Network activity is suspended until the cause of the drop is determined and resolved. Pressurized cabling is sheathed in overlapping, corrugated aluminum and steel wrapping, so electromagnetic emissions are almost nonexistent. Thus, wiretapping by induction (detecting the transmitted information magnetically, without cutting into the cable) would require very large (and visible) amounts of equipment. The communications lines may be strung throughout the building so that every inch of the cable is exposed and subject to easy visual examination.

Another solution to physical security is to use fiber optics. Fiber optics (once considered untappable, because any break in a fiber optic line is immediately detectable, and splicing is slow and tedious) is not a totally secure medium. There are no electromagnetic radiations from a fiber optic line so inductive tapping doesn't work. The only weakness in fiber optic communications as a secure physical medium is that there is a maximum length to a fiber optic line. Lines longer than this length must resort to converting the signal back into electrical impulses, reconvert (at the repeater) into light impulses, and sending it on down the line. The devices that perform this operation are the weak links in fiber optics communications because the signal may be tapped at that point.

Currently, fiber optics communications may be used for a maximum distance of about 100 kilometers (radius) without having to resort to repeaters. This technology (though currently expensive) would provide an excellent physical security solution to most local area networks (the MRSA LAN falls into this category).

Another method of increasing physical security is to disconnect network, modem, and hardwire access (that is, all external access to the machine) after 5 p.m. (normal business hours).

Encryption of data traffic does not need to be addressed within MRSA as the physical security can be quite easily handled. However, network communication between external hosts (hosts outside MRSA) is another matter. Encryption can be performed on data leaving MRSA via the DDN gateway host and decrypted upon arrival at the destination DDN host; this level of security and type of encryption process will be defined and mandated by DOD.

8 SUMMARY

All programming support functions and all local operations support should be tasked from IMD to MRSA divisions. Individual divisions and project managers will be responsible for managing and funding the computing resources necessary for their mission, to include programmer support and user training.

A Networking Group should be established at MRSA and be given the responsibility of integrating the various MRSA computer resources into a networked architecture. The emphasis of this group should be on the network architecture and design rather than on the specific computing components. This group should be tasked with designing a network architecture which will support the workstation principles and the three levels of processing described in Chapter 4. The Networking Group should also track new network technology and protocols for implementation and upgrade of the MRSA network.

Training on operations management of computer resources and use of specific applications utilities should be managed and coordinated by IMD.

In the transfer of function from IMD programmer support to the divisions, one of the results should be that IMD retain a knowledge base of hardware and software being used within MRSA for purposes of network integration and end-user training. This knowledge base should be a source for MRSA to use in further automation procurements and for reallocating existing resources to solve new problems and new mission requirements.

Within MRSA, logical security (regarding networking) is less important than physical security. Each MRSA multiuser system should have a system administrator.

9 ACRONYMS

ACL	Access Control List
ADPE	Automated Data Processing Environment
AMC	Army Materiel Command
AOAP	Army Oil Analysis Program
ARPANET	Advanced Research Projects Agency Network
ASCII	American Standard Code for Information Interchange
cpu	central processing unit
DA	Department of the Army
DARPA	Defense Advanced Research Projects Agency
DARPANET	Defense Advanced Research Projects Agency Network
DBMS	Data Base Management System
DCA	Defense Communications Agency
DDN	Defense Data Network
DOD	Department of Defense
EOPDB	Equipment Oriented Publications Data Base
ILS	Integrated Logistics Support
IMD	Information Management Division
ISO	International Standards Organization
LAN	Local Area Network
MRSA	Materiel Readiness Support Activity
OSI	Open Systems Interconnection
PS	PS Magazine
RMD	Resource Management Division
TCP/IP	Transfer Control Protocol/Internet Protocol
UCLA	University of California, Los Angeles

APPENDIX A:

NETWORKING DEFINITIONS AND PHILOSOPHY

The seven layer networking model presented in Figure A1 will be referenced a great deal in this discussion. This model was designed by the International Standards Organization (ISO) to break down the transfer of data and tasks between machines into various layers of functional responsibility. This is also often called the Open Systems Interconnect (OSI) model as it is designed to promote functionally independent calls and operations between systems. For descriptions of the functions that occur within each of the OSI layers, see the figure entitled "Functions of the OSI Layers." For a brief summary of some of the networking standards groups and committees, see the figure entitled "Standards Groups."

The language of networking is that of *protocols*. A protocol gives meaning to data exchange; it defines the structure and semantics of communication. Protocols are designed to impose a reliable order on the data. Some well-known protocols are: RS-232, RS-422, IEEE-488, Bisync, HDLC, SDLC, SNA, X.25, X.75, X.3, X.28, X.29, IP, TCP, UDP, NCMP, FTP, SMTP, TELNET, NCP, XNS, Clearinghouse, Courier, and PUP. Given this list, it is easy to understand why it may be said that most of the alphabet soup in networks today is protocols.

The network itself may be defined as an interconnected set of nodes. Logically, a network consists of *media* (physical transmission), *protocols* (data exchange semantics), and *facilities* (application tasks). A network may connect any two or more pieces of equipment as long as information (data) is exchanged via the network. Some common networks are: ARPANET, DDN, TELENET, TYMNET, Phone Network, and Ethernet. Network media is the physical medium over which the information is carried. Typical media are:

- twisted pair wires,
- coaxial cable,
- radio,
- microwave (through guides and air), and
- light (through fiber and air).

Facilities are uses or applications of a network. Some typical network facilities include:

- file transfer,
- electronic mail,
- remote login (virtual terminal),
- remote execution,
- inter-process communication,
- data sharing, and
- name service (database), that is, how do you find someone on the network?

International Standards Organization

Open Systems Interconnect Model

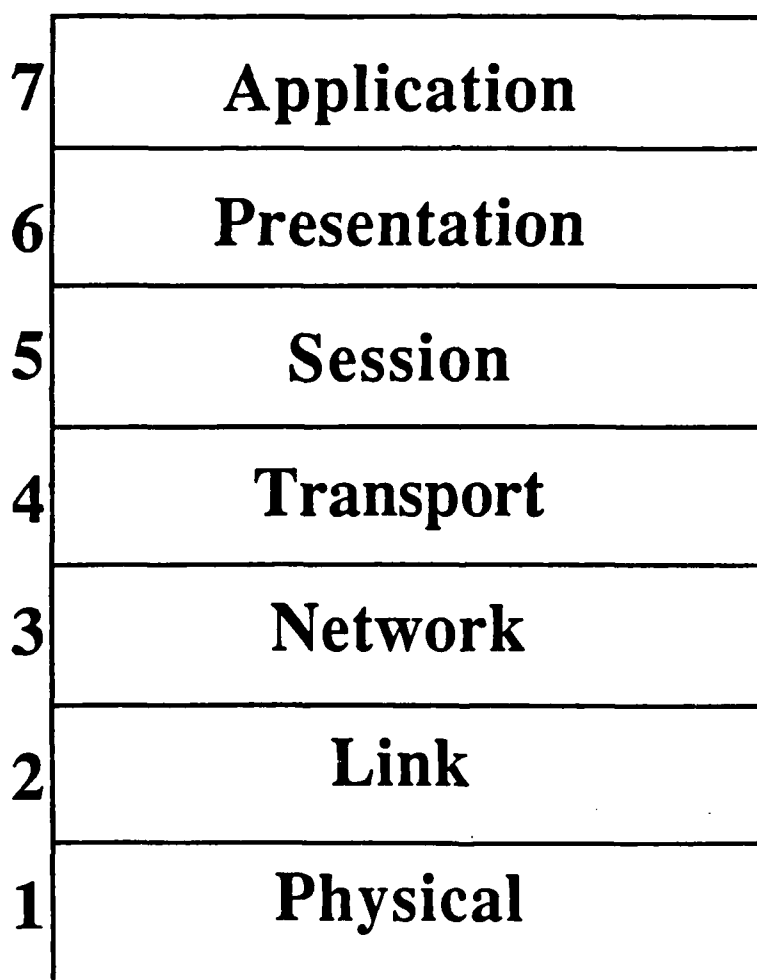


Figure A1. Seven layer networking model.

Functions of the OSI Layers

Application layer

- Common application service elements

 - Login

 - Password checks

 - Set up associations to named peers and agree on the semantics of the information to be exchanged

- Specific application service elements

 - File transfer and file access

 - Basic class virtual terminal

 - Forms class virtual terminal (ECMA)

 - Message handling

 - Document handling

 - Job transfer and manipulation

 - Videotext

 - Graphics (semantics)

 - Commitment, concurrency, and recovery

Presentation layer

- Negotiate transfer syntax for character sets, text strings, data display formats, graphics syntax, file organization, data types, financial information

Session layer

- Connection establishment and termination

- Data transfer

- Synchronization between end-user tasks

- Graceful and abrupt closure

- Map addresses to names (users retain same name if they move)

- Dialog control (who, when, how long, half or full duplex)

- Quarantining of data (buffering of data until instructed to deliver it)

Transport layer

- Address end-user machines without concern for route of message or address of machines en route between end-user machines
- Multiplex end-user address onto network
- End-to-end error detection and recovery
- Monitoring of quality of service
- Possibly disassemble and reassemble session messages

Network Layer

- Set up routes for packets to travel (establish a virtual circuit)
- Address network machines on the route through which the packets travel
- May disassemble transport messages into packets and reassemble them at the destination
- Send control messages to peer layers about own status
- Flow control (regulate the rate at which a machine receives messages)
- Recognize message priorities and send messages in proper priority order
- Internetworking

Data-link control layer

- Add flags to indicate beginning and end of messages
- Add error-checking algorithms
- Make sure data is not mistaken for flags
- Provide access methods for local area networks

Physical layer

- Handle voltages and electrical pulses
- Handle cables, connectors, and components
- Handle collision detection for CSMA/CD access method

Standards Groups

Organization and geography	Affiliation	Membership & Representation	Influence
ISO (International Standards Organization)	Voluntary nontreaty	Standards bodies in participating nations. US representative is ANSI; ECMA is observer	Responsible for Open Systems Interconnection model. Close relationship with CCITT
International			
CCITT (International Consultative Committee on Telegraphy and Telephony)	Part of International Telecommunications Union (a U.N. treaty organization)	Private companies; scientific and trade associations; postal, telephone, and telegraph administrations. U.S. representative is Department of State	"Recommendations" which are law where communications in Europe are nationalized
International			
ECMA (European Computer Manufacturers Association)	Computer suppliers selling in Europe; includes some U.S. companies	Trade organization of suppliers; small, with about 20 members	Contributes to ISO and also issues own standards; known for fast movement
Western Europe			
ANSI (American National Standards Institute)	Voluntary	Manufacturers, organizations, users, and communications carriers	U.S. voice in ISO
United States			
NBS (National Bureau of Standards)	Government Agency	Gov't agencies and network users; much work done by Bolt Berneke & Newman, which is largely responsible for DOD's Arpanet	Issues Federal Information Processing standards for equipment sold to federal gov't; DOD need not comply
United States			
IEEE (Institute of Electrical and Electronic Engineers)	Professional Society	Dues-paying individuals	Contributes to ANSI and issues own standards such as IEEE-802.X
International			
EIA (Electronic Industries Association)	U.S. trade organization	Manufacturers	Contributes to ANSI; known for physical layer's RS-232 C std
United States			
DOD (Department of Defense)	Gov't Agency	Gov't/military	All customers dealing with the military establishment
United States			
Special interest industry groups, such as ANSI X9 banking std group	Voluntary orgs such as ANSI & IEEE	Organizations and firms with a specialized interest	Issues standards that meet a specialized need

There are essentially two types of networks: circuit switched and message switched. X.25 is an example of a circuit switched network. Ethernet is an example of a message switched network. Any network which requires an "end-to-end virtual circuit" is said to be circuit switched; no data may be exchanged between two nodes in the network prior to establishing a conversation. This requires set-up control exchanges, as well as termination control exchanges. In a message switched network, each packet of information is routed from source to destination independently from all other packets. Virtual circuit protocols may be built on top of a message switched network. The difference between circuit switched and message switched networks is becoming very small.

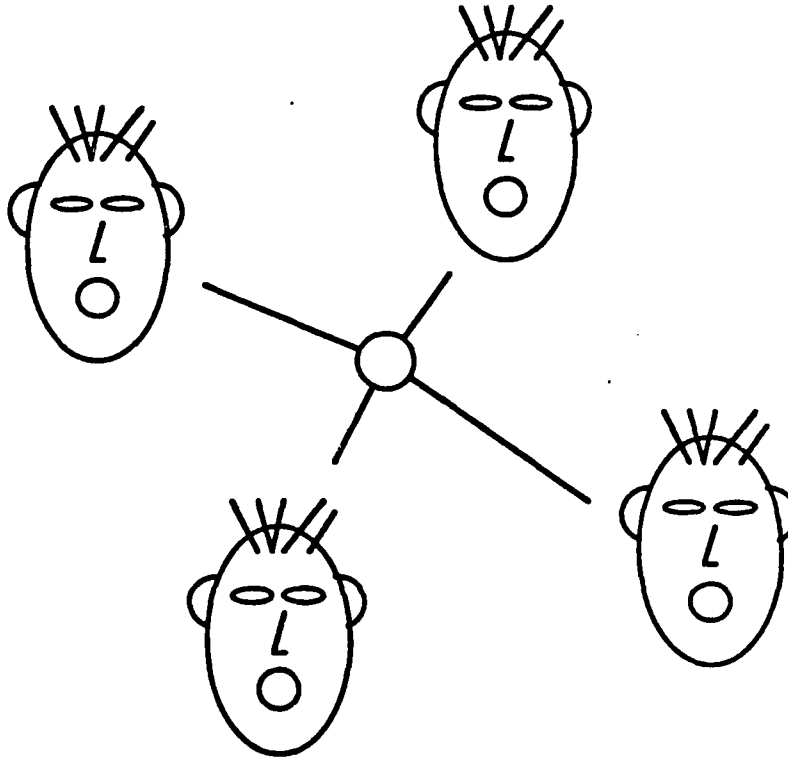
A human example of networking illustrates very simply how many networks function. See the figure entitled "Conversation Network."

For example, a "conversation network" which occurs between 5 or 6 people meeting in a social situation illustrates some important points about networks. The media that we use is air. The protocols used are: English, Robert's Rules of Order, etc. Access to the network is CSMA/CD (Carrier Sense Multiple Access/Collision Detect), which means that everyone listens and only attempts to speak/transmit when there is nothing coming over the media from other nodes/people. This is exactly what goes on with an Ethernet. Thus, in an Ethernet networking environment, to send a packet, wait for the bus to be passive and then toss the packet out on the net. To receive a packet, read the address of every packet that comes across the net and, if it's your address, read it and wake up the host telling him that he's received a packet. Note that this activity occurs at level 3 in the ISO model.

The state of networking regarding the ISO/OSI model is that no vendor has a product that satisfies all seven layers of the model. Most vendors take a physical media (like baseband Ethernet) which addresses only layers 1 and 2 of the model and then impose a suite of protocols to address layer 3 and into layer 4. From layers 4 through 7, all vendors are in a quandary as to how to resolve the complex applications and tasks into a suitable set of protocols that can be agreed upon by everyone. Much of this can be seen to be the fault of the ISO committee for defining such a broad spectrum of tasks for the upper layers of the OSI model. The common approach has been to address particular applications and create protocols for that application. Thus, SMTP (Simple Mail Transfer Protocol), and FTP (File Transfer Protocol), address specific application tasks.

A view of the ISO/OSI model with additional information added to the different layers is shown in the following four figures entitled "Data Communications Model."

Conversation Network



Media: Sound through Air

**Protocols: English, Robert's Rules
of Order**

Access: CSMA/CD

Message Switched

Data Communications Model

Level Number	Function	Examples	Responsibility
7	Application	Database Time Sharing Electronic Funds Transfer Order Entry	ISO
6	Presentation Control	Data Structure Formats Virtual Terminal Protocol File Transfer Protocol	ISO Note 2
5	Session Control	Session Management	ISO
4	Transport End-to-End	Network Independent Interface	ISO
3	Network Control	X25 Level 3	CCITT
2	Link Control	X25 Level 2	CCITT Note 1
1	Physical Control	X25 Level 1	CCITT

Higher Level Protocols

Standard Transport Service

Standard Network Service

- Notes: 1. ISO for private networks
2. CCITT for Network Services (ISO collaboration)

Data Communications Model

Level Number	Function	Examples	Responsibility
7	Application	host software	
6	Presentation Control		
5	Session Control		
4	Transport End-to-End	mixed hardware, software	
3	Network Control		
2	Link Control	hardware	
1	Physical Control		

Notes: 1. ISO for private networks
2. CCITT for Network Services (ISO collaboration)

↑ Higher Level Protocols ↓

Data Communications Model

Level Number	Function	Examples	Responsibility
7	Application	Do things of interest to users	
6	Presentation Control		
5	Session Control		
4	Transport End-to-End	Assure messages get to right place without errors	
3	Network Control		
2	Link Control		
1	Physical Control		



 Higher Level Protocols

- Notes: 1. ISO for private networks
 2. CCITT for Network Services (ISO collaboration)

Data Communications Model

Level Number	Function	Examples	Responsibility
7	Application	mail, file transfer, remote login tcp/ip, SNA, DECnet, XNS Ethernet-logical path-special cards protocols such as X.25, HDLC coax, fiber, copper wire, and electrical/optical definition	
6	Presentation Control		
5	Session Control		
4	Transport End-to-End		
3	Network Control		
2	Link Control		
1	Physical Control		

↑
Higher
Level
Protocols
↓

- Notes: 1. ISO for private networks
2. CCITT for Network Services (ISO collaboration)

Network Summary

A Local Area Network (LAN) may be said to be a series of computers connected by hardware and communications software. The decisions that need to be made when designing a network are:

- > network model (e.g., the ISO model),
- > signaling mechanisms,
- > speed needed,
- > type of cable, and
- > topology of cable.

The following figures illustrate some of the factors which are used in deciding what kind of media to use.

Communications Paths

Low Speed - up to 19.2 k baud

Dial up Analog Phone lines

Hardwire leased lines

Sytek

RF broadband cable modems

Digital phone switched service

Medium Speed - up to 56k baud

RF modems

Digital phone service

High Speed - 2Mbit, 10Mbit or 80Mbit

Ethernet

Fiber Proteon

Fiber ethernet

Broadband ethernet

Private fiber

Communications Paths

Low Speed - up to 19.2 k baud

Dial up Analog Phone lines

- 300, 1200 and 2400 baud typically supported
- installation \$150, \$9 - \$12 per month

Hardwire leased lines

- 9600 baud typically
- installation \$250, \$12 and up per month

Sytek

- up to 9600 baud, speed matching
- Tbox(two ports) \$950
- SMUX(2-32 ports) \$2000 plus \$495 per two ports
- network access fee if not incomming ports

RF broadband cable modems

- up to 19.2k baud
- \$895 per modem, plus installation
- \$25/month maintenance on modem
- \$400 per year bandwidth charge

Digital phone switched service

- up to 19.2k baud switched digital service
- keyboard dialing

Medium Speed - up to 56k baud

RF modems

- up to 56k baud sync modem \$2070 plus installation
- \$25 per month maintenance
- \$1200 per year bandwidth charge

Digital phone service

- Digital point to point 48k to 64k baud sync

High Speed - 2Mbit, 10Mbit or 80Mbit

Ethernet

- cable approx. \$.80 per foot plus installation
- transceivers start at \$285
- interface cards up to several thousand

Fiber Proteon

- 10 Mbit \$3150 for host interface
\$2300 for fiber modems
- 80 Mbit \$8000 for host interface
\$4500 for fiber modems

Fiber ethernet

- \$600 to \$1000 for fiber transceiver
- plus additional interface if bridging local ethernet

Broadband ethernet

- Chipcom transceiver
\$4250 for two ports plus \$4500
distance 2750 meters to head end
- repeater
\$6250 for one repeater plus \$4500
distance 1400 to 1800 meters

Private fiber

- 62.5 micron fiber with .9 db loss per km at 1300 nm
- approx 6 db loss per km at 825 nm
- 4 db connector loss per loop

The seven layer network model (ISO/OSI) may be described as being divided into functional layers. Each layer is responsible for discrete tasks and for handing off information to the next layer. A brief summary of the seven layers follows:

1. Physical Layer

The physical media is generally one of the following:
twisted pair wires,
coaxial cable,
fiber,
microwave, or
satellite.

2. Link Layer

The responsibility of the link layer is to:
make packets, and
identify addresses.

Things like parity, stop bits, number of data bits, and type of character set are also handled in the link layer.

3. Network Layer

The responsibility of the network layer is to handle routing:
point-to-point, or
virtual circuit.

4. Transport Layer

The transport layer provides for reliability of end-to-end services:
error correction,
flow control,
full duplex byte stream, etc.

5. Session Layer

Services such as:
authentication,
authorization, and
synchronization are handled at this layer.
Password verification should be implemented here.

6. Presentation Layer

Data problems such as:
bit order,
byte order,
word length, and
representation are handled here.
Also data compression and encryption are dealt with in this layer.

7. Application Layer

End user services such as:
remote login,
file transfer,
remote job submission, and
mail are dealt with at this level.

As noted before, most protocols only address levels 1 through 4. For example,

Existing Protocols	ISO/OSI Layers
IP	layer 3
TCP	layer 4
TELNET	> layer 4
FTP	> layer 4
STMP	> layer 4
X.25	layers 1-3
DECNET	layers 1-4
SNA	layers 1-7
XNS	layers 3-4

Baseband vs Broadband Signaling

Baseband

- > digital signal
- > coaxial cable or twisted pair wires
- > cannot frequency multiplex
- > bandwidth of 1-10 Mb/sec
- > 1024 nodes, about 1 mile maximum
- > Ethernet and DECNET are examples.

Broadband

- > analog signal
- > coaxial cable
- > frequency multiplexed
- > bandwidth 10-80 Mb/sec
- > 255 nodes, several miles
- > Pronet, Cambridge Ring, Sytek, Protean Pronet are examples.

Speed, Bandwidth Needs

voice	64 Kb/sec.	Satellite links
data	1-2 Mb/sec.	PC networks, Ethernet, DECNET
video	2-90 Mb/sec.	New broadband technology.

Cable Types and Speeds

twisted pair	9.6 Kb-1 Mb/sec
thinwire Ethernet	1-2 Mb/sec
Ethernet coaxial cable	3-10 Mb/sec
token ring coax	10-80 Mb/sec
satellite	56-212 Kb/sec
leased phone lines	9.6-212 Kb/sec.

Ring Networks

A store and forward situation. Each host sees the data as it goes by. A host may "talk" only when it has the token. When a host sees the token go by in a disabled state, the host may "enable" the token and then fire off his data packet. When the "enabled" token comes back around the ring, the host may then "disable" it so that someone else may speak.

- > all data goes one way around the ring
- > all nodes can access it
- > protocol is needed:
 - to determine who uses ring next, and
 - to remove old packets
- > examples
 - token ring (1969)
 - Apollo, Prime, IBM, Pronet
 - slotted ring (1972)
 - Cambridge Ring.

Ethernet Networks (1976)

- > branching bus topology
- > CSMA/CD protocol
 - The algorithm to address the net is analogous to a polite dinner party:
 - everybody listens,
 - if no one is talking, then talk
 - but if someone else starts talking too,
 - both stop
 - wait random period
 - loop back to everybody listens above.

Standards

- Ethernet, version 1 (9/80)
- Ethernet, version 2 (11/82)
- Logical Link Control, IEEE 802.2
- Ethernet, IEEE 802.3 (12/82) - see 802.3 figures
- Token Bus, IEEE 802.4 - see 802.4 figures
- Token Ring, IEEE 802.5 (IBM and Protean) - see 802.5 figures.

Ethernet vs 802.3 Comparison

Addressing

IEEE decided to allow for both 16-bit and 48-bit addressing. In 16-bit mode, the first bit indicates an individual address (0) or a group address (1). In 48-bit mode, the first bit has the same meaning, and the next bit indicates a globally administered address (0) or locally administered address (1).

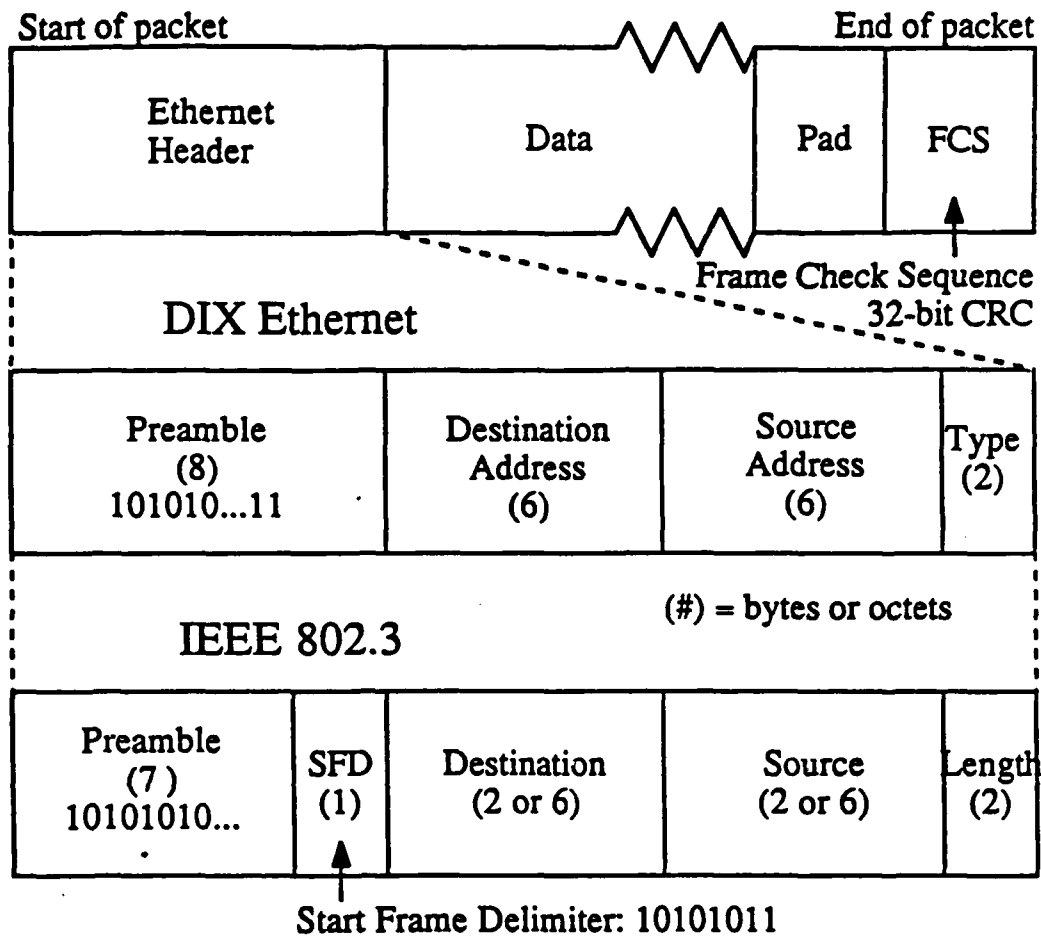
All stations on one network must have the same size addressing!

Ethernet Type field vs 802.3 Length field

Ethernet packet length was determined implicitly by loss of carrier, and a type field was included for selecting the network layer protocol to hand the packet to.

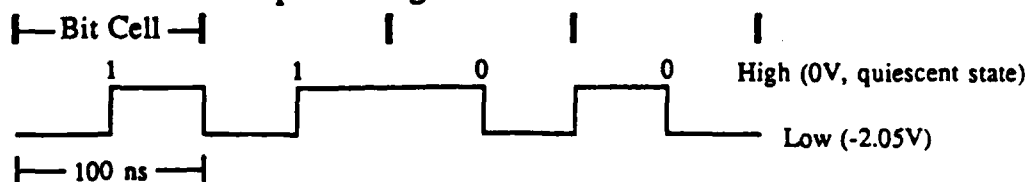
IEEE decided not to count on loss of carrier for packet length detection, so a length field was added. If a packet type is required, it becomes a part of the data in the packet.

Ethernet/802.3 Packet Format



Preambles are identical--nomenclature has changed
Length is implicit in Ethernet, determined by loss of carrier at end of packet; type is pushed into the data in 802.3.

Data is Manchester encoded with a 0-1 transition representing a 1 and a 1-0 transition representing a 0:



802.4

Token-Passing BUS

Phase Continuous FSK (Frequency Shift Keying)

Topology: Omnidirectional bus

Trunk Cable: 75 Ω coax, RG-6, RG-11

Drop Cable: 35 to 50 Ω coax stub less than 350 mm long

Station Connector: 50 Ω male BNC-series

Trunk Connector: 75 Ω tee

Data Rate: 1 Mb/s

Signaling: Manchester

{HL} = 0--high to low transition

{LH} = 1--low to high transition

{LL HH} = non data (control)

High frequency = 6.25 MHz; Low frequency = 3.75 MHz

Phase Coherent FSK (Frequency Shift Keying)

Topology: Omnidirectional bus

Trunk Cable: 75 Ω coax, RG-6 semi-rigid CATV-like

Station Connector: 75 Ω female F-series

Trunk Connector: 75 Ω nondirectional passive tap

Data Rate: 5 Mb/s and 10 Mb/s

Signaling: Direct encoding

0 = two cycles of high frequency

1 = one cycle of low frequency

non data = high, low, high

High frequency = 2*bit-rate (10 or 20 MHz)

Low frequency = bit-rate (5 or 10 Mhz)

Multilevel Duobinary AM/PSK (Amplitude Modulation + Phase Shift Keying) Broadband

Topology: Directional bus with head-end repeater

Trunk Cable: 75 Ω coax, RG-6 semi-rigid CATV-like

Station Connector: 75 Ω female F-series

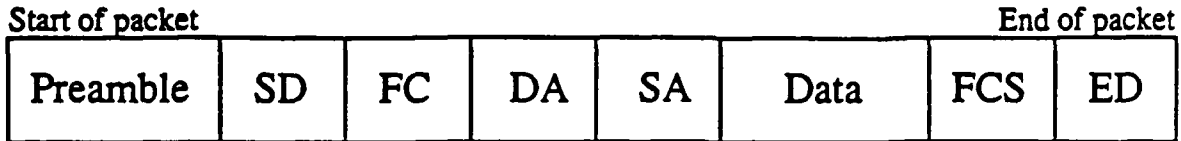
Trunk Connector: 75 Ω directional passive tap

Data Rate: 1 Mb/s, 5 Mb/s and 10 Mb/s

Channel Bandwidths: 1.5 MHz, 6 MHz, and 12 MHz

Signaling: Direct encoding--unspecified

IEEE 802.4 Packet Format



Preamble--1 or more bytes

SD = Start Delimiter--1 byte: N N 0 N N 0 0 0

FC = Frame Control--1 byte: various encodings for control and data

DA = Destination Address--2 or 6 bytes: same encoding as 802.3

SA = Source Address--2 or 6 bytes: same encoding as 802.3

Data = information--0 or more bytes

FCS = Frame Check Sequence--4 bytes

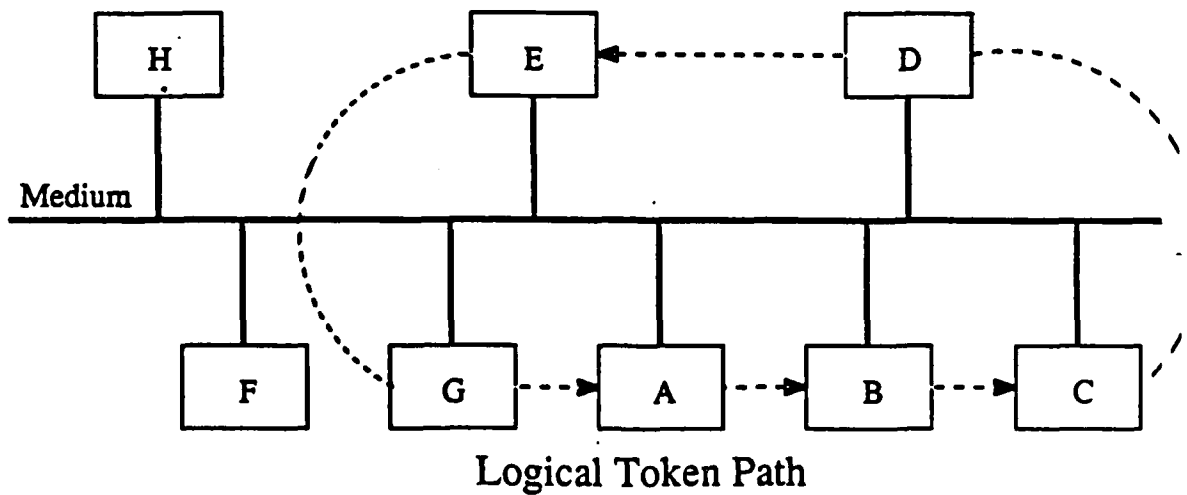
ED = End Delimiter--1 byte: N N 1 N N 1 1 E

N = non_data, 0 = zero symbol, 1 = one symbol

I = Intermediate--1=more to come, 0=end of transmission

E = Error bit--0=no error, 1=error

Abort Sequence: SD ED: N N 0 N N 0 0 0 N N 1 N N 1 1 E



802.5 Token-Passing RING

Topology: Ring

Trunk Cable: 150 Ω shielded twisted pair

Drop Cable: 150 Ω shielded dual twisted pair

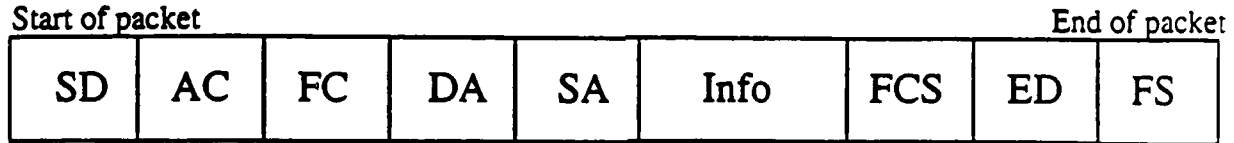
Trunk Connector: specially designed molded connector

Data Rate: 1 or 4 Mb/s

Signaling: Differential Manchester

{OS}	= 0--opposite, same
{SO}	= 1--same, opposite
{SS}	= J non-data symbol (control)--same, same
{OO}	= K non-data symbol (control)--opposite, opposite

IEEE 802.5 Packet Format



SD = Start Delimiter--1 byte: J K 0 J K 0 0 0

AC = Access Control--1 byte: priority/token/monitor bits

FC = Frame Control--1 byte: various encodings for control and data

DA = Destination Address--2 or 6 bytes: same encoding as 802.3

SA = Source Address--2 or 6 bytes: same encoding as 802.3

Info = Data information--0 or more bytes

FCS = Frame Check Sequence--4 bytes

ED = End Delimiter--1 byte: J K 1 J K 1 1 E

FS = Frame Status--1 byte: A C r r A C r r

J = non-data J, K = non-data K, 0 = zero symbol, 1 = one symbol

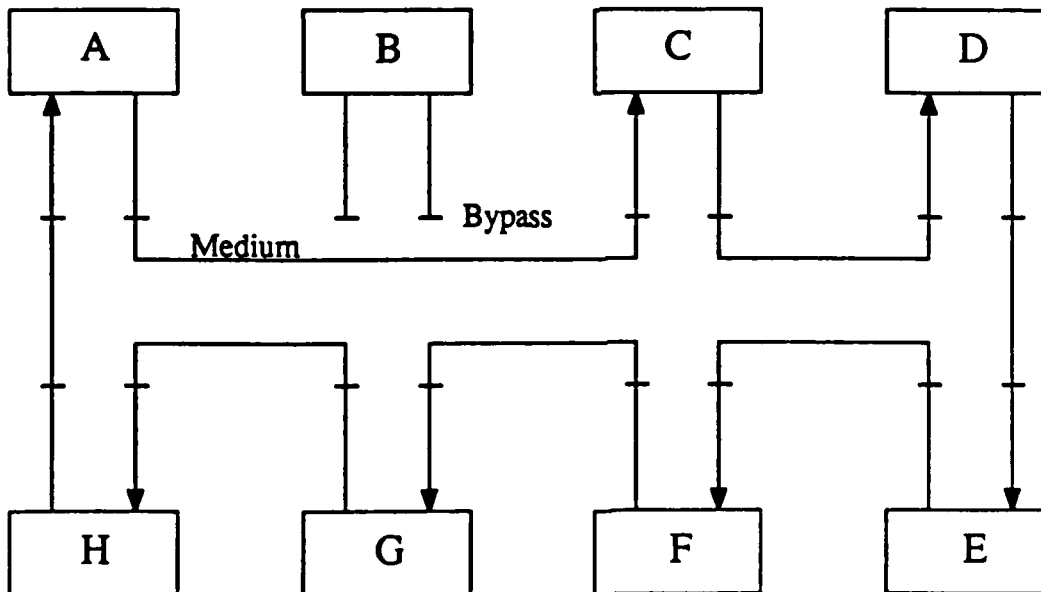
I = Intermediate--1=more to come, 0=end of transmission

E = Error bit--0=no error, 1=error

A = Address recognized; C = frame Copied; r = reserved

Abort Sequence: SD ED: J K 0 J K 0 0 0 J K 1 J K 1 1 E

Token Sequence: SD AC ED



The following figures summarize decisions and their effects pertaining to standard separating levels, network architecture, media choices, and the effect within a network when the decision has been made to network processors only.

Architecture

- Specifying the set of supported interconnects
- Methods of management
- Specifying loss of function at gateway

134

Architectures are likely to:

- Mix media
- Have a hierarchy
- Trade local convenience vs. global functionality

With Standard Separating Levels

Choose media

- Speed, convenience
- Attachment cost

Choose level 2-3 protocol

- Available products
- Performance

Choose level 4-5 protocol

- Functional requirements
- Uniformity to pass functionality
- Uses supported
- Performance requirements

Media Choices

	MAX BITS/SEC	ATTACHMENT COST	LENGTH IN FT.	COST PER FOOT
Short copper wire	2,500,000	25-150	150	\$.02
Long copper wire	56,000	150-1,000	variable	
Broadband coax	1,500,000/ch	100-1,000	miles	\$.20
Baseband coax	50,000,000	5,000-50,000	≤ mile	\$.20
Fiber	100,000,000	5,000-10,000	few miles	\$1.00+

Within a Network (or subnetwork)

The systems all are addressable by name.

Messages are usually broadcast, i.e., everyone hears.
Protocol deals with:

at low levels:

- Traffic management
- Error management
- Signal definition
- Address information (but not content)

at high levels:

- Sessions, calls
- Use of the content

Sender and receiver are processors, not terminals
Difference from current ACC 3270

DISTRIBUTION

Army Materiel Command

ATTN: Materiel Readiness Support Activity (15)

Defense Technical Information Center (2)

ATTN: DDA

17
8/88