NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

P-3 SQUADRON TRANSITION TO THE DEFENSE MESSAGE SYSTEM (DMS)

by

Mark S. Foldy Jr.

March 1992

Principal Advisor: CDR A.W. Tulloch, USN

REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188

1a 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)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b OFFICE SYMBOL (If applicable) AS	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000	7b ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000
8a NAME OF FUNDING / SPONSORING ORGANIZATION 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)
P-3 SQUADRON TRANSITION TO THE DEFENSE MESSAGE SYSTEM (DMS)

12 PERSONAL AUTHOR(S)
FOLDY, Mark S. Jr.

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Master's Thesis	FROM _____ TO _____	1992 March	110

16 SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the US Government.

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Defense Message System; Local Area Network; Naval Telecommunications System

19 ABSTRACT (Continue on reverse if necessary and identify by block number) The Department of the Navy is currently implementing a new Department of Defense messaging system. This new system is the Defense Message System (DMS). DMS is designed to take advantage of the new advances in telecommunications and computer technologies, while phasing out existing inadequacies prevalent in the current DoD messaging system. The purpose of this thesis is to examine the current messaging system in terms of how it is utilized by a typical P-3 squadron. Both external and internal messaging process will be examined. A detailed description of the DMS transition phases and major DMS components will be discussed, along with transition issues that will be of importance to the P-3 community. A basic summary of Local Area Networks (LAN) is provided as well as planning strategy for implementation of a LAN with emphasis on the Navy PC-LAN contract.

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL TULLOCH, Allan W.	22b TELEPHONE (Include Area Code) 408-646-2995 22c OFFICE SYMBOL AS/Tu

Approved for public release; distribution is unlimited.

P-3 Squadron Transition to the Defense Message System (DMS)

by

Mark S. Foldy Jr.
Lieutenant, United States Navy
B.S., State University of New York, Albany, 1984

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1992

Author: Mark S. Foldy Jr.
Mark S. Foldy Jr.

Approved by: Allan W. Tulloch
Allan W. Tulloch, CDR, USN, Principal Advisor

Dan C. Boger
Dan C. Boger, Associate Advisor

David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

The Department of Navy is currently implementing a new Department of Defense messaging system. This new system is the Defense Message System (DMS). DMS is designed to take advantage of the new advances in telecommunications and computer technologies, while phasing out existing inadequacies prevalent in the current DoD messaging system. The purpose of this thesis is to examine the current messaging system in terms of how it is utilized by a typical P-3 squadron. Both external and internal messaging process will be examined. A detailed description of the DMS transition phases and major DMS components will be discussed, along with transition issues that will be of importance to the P-3 community. A basic summary of Local Area Networks (LAN) is provided as well as planning strategy for implementation of a LAN with emphasis on the Navy PC-LAN contract.

TABLE OF CONTENTS

I. INTRODUCTION

A. GENERAL

The Department of Defense (DoD) has initiated a department wide program that will dramatically change the way in which activities communicate using the DoD messaging system. The advent and spread of computer and telecommunications technology in the last decade has led to a review of the existing method of providing communications services for the Department of Navy (DoN) and the other services and activities comprising the DoD. The current traditional Automatic Digital Network (AUTODIN) is inadequate to meet the future DoD communications needs. One of the major inadequacies of the current system is the electronic connectivity gap that exists in the automatic transfer of messages between the Telecommunications Centers (TCC) and the organizational user. A recent initiative that will eventually replace the current DoD messaging system and provide AUTODIN style true writer-to-reader information exchange, as well as Defense Data Network (DDN) capabilities such as electronic mail (E-mail), is the Defense Message System (DMS)..

DoN shore activities currently receive message traffic from Navy Telecommunication Centers (NTCC) that are located geographically in close proximity. The services that are provided by these centers to the shore activities are manpower intensive and utilize outdated computer equipment. Message traffic is typically generated on paper and hand delivered by couriers between the shore activities and the NTCCs. The DMS implementation plan will provide for architectural changes in the current messaging system allowing for the electronic delivery of message traffic directly to the shore activities. The arrival of message traffic electronically to the user organization will allow for the use of Automatic Message Handling Systems (AMHS) in conjunction with Local Area Networks (LAN) to effectively and efficiently distribute message traffic throughout the organization.

B. SCOPE OF THE STUDY

This thesis will examine the implementation of the Defense Message System in the DoN and, in particular, the effects the implementation will have on a typical P-3 squadron, as well as the P-3 community as a whole. The use of Automatic Message Handling Systems in conjunction with Local Area Networks will also be closly examined, with emphasis on how these systems can be implemented and effectively used in the P-3 community.

The major focus of this thesis will be to familiarize the reader with the messaging systems currently utilized by the P-3 community and the impact of the new systems under development. The benefits of these systems to the organization will be examined, as well as the problem areas that will be encountered during the transition.

C. ORGANIZATION OF THE STUDY

This study is organized into chapters that present the following information.

1. Chapter I. Introduction

This chapter provides the general information about the thesis, gives an overview of the major study areas, and provides an outline of the topics to be discussed.

2. Chapter II. Current Messaging Systems

This chapter will describe the current messaging systems utilized by the DoN and, in particular, the P-3 community. The Navy Telecommunications System (NTS) and the Defense Data Network (DDN) will be explored in some detail, as will be the connectivity to the organizational user. The current external and internal message and information flow of a typical P-3 squadron will be examined in this chapter.

3. Chapter III. The Defense Message System

The implementation and components of the DMS will be examined in this chapter, to include the target architecture, implementation strategy, and transition plan. The issues

affecting the P-3 community during the transition to DMS will be discussed in this chapter as well.

4. Chapter IV. Local Area Networks

This chapter will provide an introduction to Local Area Networks (LAN), discuss some existing LANs in operation , and look at issues regarding implementation of LANs in the P-3 community. LAN planning strategies will also be examined in this chapter, with focus on the Navy PC-LAN contract.

5. Chapter V. Summary and Conclusions

The transition and implementation of the DMS are summarized in this chapter, along with the effects of a transition to a paperless electronic message and information environment in the P-3 community.

II. CURRENT MESSAGING SYSTEMS

A. LONG-HAUL MESSAGING SYSTEMS

1. Naval Telecommunications System (NTS)

Since the 1960s, the P-3 community along with the other DoN organizations has used the NTS to provide an electronic link for sending and receiving organizational general service (GENSER) messages (up to TOP SECRET in classification). The NTS is a subsystem of the national communications systems that provide users with worldwide coverage.

The Commander, Naval Computers and Telecommunications Command (COMNAVCOMTELCOM), is in command of the shore elements of the NTS and is the administrative manager of the communications and data processing assets of the NTS. NTS assets are divided into four Naval Communication Areas (NAVCOMMAREAS) corresponding to the geographical areas of responsibility of the Fleet Commanders in Chief (FLTCINCS). The FLTCINCS are delegated authoritative direction of NTS assets in their respective areas. [REF 1: p. 1]

a. *Organization of NAVCOMMAREAS*

(1) Naval Computer and Telecommunications Area Master Stations (NCTAMS). There are four NCTAMS that are delegated operational direction of the NAVCOMTELCOM assets within the NAVCOMMAREA in which they are located, as depicted in Figure 1 [REF 1: p. 4]. NCTAMS are the major communication sites for an area, providing the primary broadcast keying station for that area, and they are the central point for fleet communications support. NCS Stockton holds a unique position, because it is the only NCS that provides NCTAMS functions.

(2) Naval Computer and Telecommunications Station (NCTS). A NCTS provides communication support in a large specified portion of a NCTS (i.e., North Atlantic), controling all communication elements and equipment necessary to provide essential fleet support and fixed communication services. [REF 1: p. 3]

(3) Naval Communication Units and Detachments (NAVCOMMU/NAVCOMMDET). NAVCOMMUs and NAVCOMMDETs normally have more specialized missions than NCTSs, requiring smaller facilities, less number of personnel, and smaller areas of geographical responsibility. [REF 1: p. 5]

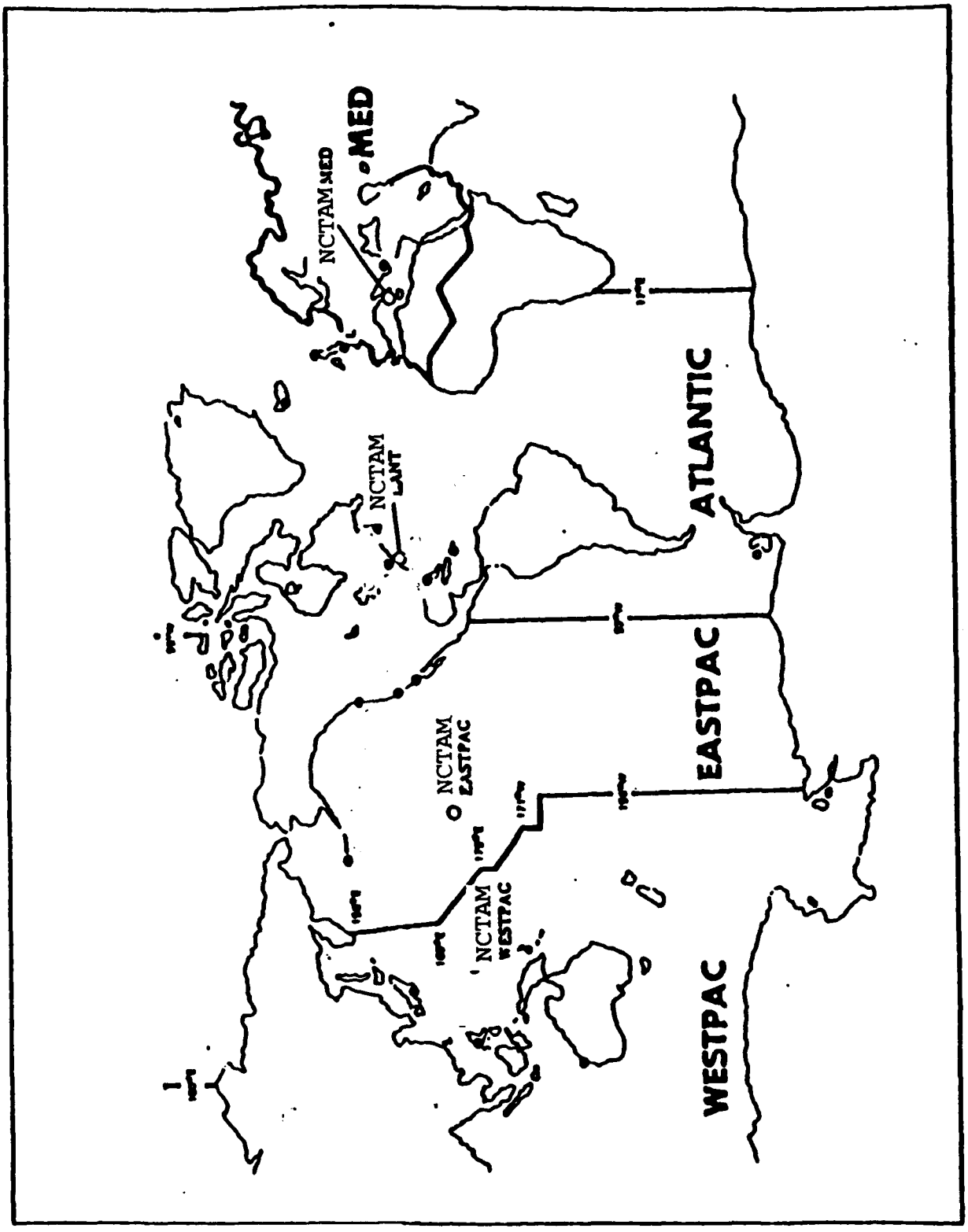


Figure 1. NAVCOMMAREAS.

(4) Navy Telecommunication Center (NTCC). An NTCC is responsible for communication support for DoD subscribers within a discrete geographical location. If it is not colocated with an NTS element and under the command of the nearest NCTAMS, NCTS, or NAVCOMMU, then it will be a component of a local non-NTS activity. [REF 1: p. 5]

(5) Support Stations. There are four types of support stations: primary, secondary, special, and internal. These components provide communication operations in support of a NCTAMS in a NAVCOMMAREA [REF 1: p. 5]. Support stations that are of primary interest to the P-3 community are Anti-Submarine Support Communications (ASCOMM) centers. An ASCOMM is considered an internal component and provides tactical communications support to operating P-3 assets.

b. Components of the NTS

Message routing and delivery throughout the DoN, which are of major concern to the P-3 community, are handled using the NTS communications network consisting of these major components: Automatic Digital Network (AUTODIN), the Naval Communications Processing and Routing System (NAVCOMPARS), the Local Digital Message Exchange (LDMX), the Remote Information Exchange Terminal (RIXT), and the Standard Remote Terminal (SRT).

(1) AUTODIN. AUTODIN is the primary message handling network used by the DoN, providing a secure automated store-and-forward, multi-level precedence system for message traffic. AUTODIN utilizes 15 operational Automated Switching Centers (ASCs). ASCs are remote, interconnected, central processing nodes that the worldwide AUTODIN network is designed around. The ASCs perform store-and-forward message switching functions, some message validation functions, message format conversions, and some specialized routing functions [REF 3: p. 5].

A message that enters the AUTODIN system is handled in the following manner: A message that is input into an ASC node is transmitted through the network one node at a time. As an ASC receives a message from another node it stores the message in a computer and then forwards it to the next node. The communication between ASC nodes could be coaxial cable, commercial satellite relay, microwave relay, fiber optic cable, or some combination of the above. When the message arrives at the destination ASC, it is sent electronically by the ASC to the local NTCC, NAVCOMMU, NCTS or NCTAMS for delivery to the addresses. [REF 2: p. 10]

(2) NAVCOMPARS. The NAVCOMPARS automates most of the message receipt, processing, and transmission functions required by the four NCTAMS and NCS Stockton to support the fleet [REF 4: p. 3-10]. The NAVCOMPARS is interfaced with radio systems that relay communications between the fleet and AUTODIN through an ASC node. Through the use of software programs utilized on mainframe UNISYS computers, NAVCOMPARS provides the following services [REF 2: p. 64]:

- Provides on-line message storage on magnetic disk.
- Provides off-line message storage on magnetic tape.
- Assembles and keys single and multichannel fleet broadcast
- Performs fleet broadcast screening and retransmission.
- Performs format conversion and automatic entry into the Common User Digital Information Exchange System (CUDIXS) (used for long-haul, ship-shore communications).
- Provides an entry point for RIXT into the system.
- Performs format conversion and automatic entry to AUTODIN.
- Performs automatic message format validation.

(3) LDMX. The LDMX provides automated processing services similar to those of NAVCOMPARS. Services such as the controling of and acknowledging of receipt for incoming traffic and the inventoring and logging of traffic are provided only for 13 major ashore telecommunications centers and do not interface with the fleet communication system as does NAVCOMPARS. The LDMX is a large mainframe-based system,

complemented with many disk drives, tape drives and terminals, providing automation of the message processing functions of a communications facility. The LDMX simultaneously transmits and receives messages, converts DD-173 optical character recognition forms into JANAP 128 message format, and provides filing, retrieving and accountability of messages. [REF 2: p. 65]

Messages are received by an LDMX on-line from AUTODIN, RIXT, paper tape readers, card readers, magnetic tapes, optical character readers and dedicated circuits. Messages are delivered by LDMX via AUTODIN, RIXT, magnetic tape, card punch, and dedicated circuits. [REF 4: p. 3-20]

(4) RIXT. The Remote Information Echange Terminal is designed as a modular remote terminal that extends the capabilities of the LDMX or the NAVCOMPARS to the smaller telecommunications centers. The majority of the message processing is performed by a host LDMX or NAVCOMPARS. The RIXT is an entry point for message traffic to the fleet or to the AUTODIN which is remote from the NTCC. The RIXT will provide for determination of message delivery devices, message delivery to output devices, message readdressal, message recall, distribution guide file query, and device-to-device message transfer. [REF 2: p. 3-21]

(5) SRT. The Standard Remote Terminal is similar to a RIXT, providing many of the same functions. However, the SRT ties directly into the AUTODIN and cannot interface with the NAVCOMPARS. [REF 5: p. 14.19]

c. NTS Message Routing and Delivery

The current method of message routing and delivery will be examined in this section from the starting point of when a message physically leaves a typical P-3 squadron in the hands of a designated courier and is delivered to the NTCC holding the squadron's guard, to the termination point when the message arrives at the telecommunication center serving the addressee.

(1) Guard/Protect. A P-3 squadron, whether deployed or at its home station, always has a telecommunication center that is responsible for providing messaging services for the squadron. The telecommunications center providing those services is said to have guard or protect for that squadron. Guard specifies that the center provides the internal office message distribution to the addressee. Protect means that the center provides a set number of copies to the unit, and that unit must provide its own internal distribution. As a squadron deploys or returns from deployment, the guarding or protecting center will change as the squadron transits from one COMMAREA to another. [REF 6: p. 3]

(2) Message Submission into the NTS. When a P-3 squadron generates a message, it is drafted and submitted to the NTCC on a *DD Form* 173. The message is taken over-the-counter at the NTCC and typically entered into the system using an optical character reader. However, some messages may be entered into the system manually, typically using video display terminals. The LDMX or NAVCOMPARS will then assign routing through the AUTODIN network using the Common Source Routing File (CSRF). Each ASC node and telecommunications center is assigned a Routing Indicator (RI) consisting of seven characters for identification. The message is then transmitted electronically and passed by the ASC nodes through the AUTODIN to the receiving terminals identified by the destination RIs on the message. At each ASC, the message is validated and checked for errors. If there are no errors, the message is accepted and passed through to the next node until it reaches the telecommunication center of the addressee(s). The LDMX or NAVCOMPARS at the receiving site, assuming the addressee(s) is Navy, receives the message from AUTODIN and automatically formats it for delivery to the addressee. Multiple copies of the message may be produced based on a number of distribution criteria such as AIG/CAD flagwords, subject matter of the message, or content indicator codes. Over-the-counter paper copies are then generated for pick up by the addressee.

(3) Problems with Current System. One of the major problems with the current long haul message system lies with the telecommunications centers which are the primary entry and exit points for AUTODIN messages. A majority of the equipment in the NTCCs has become obsolete, resulting in costly maintenance efforts and making it difficult to implement modifications and enhancements to the system hardware and software. This has caused limitations in the efforts to extend automation to the users and to reduce the manual, labor intensive operations within the NTCCs. [REF 7: p. 2-3]

Another major problem encountered in the current system is that despite the precedence characteristics provided by AUTODIN, writer-to-reader service has been adversely affected by the labor intensive over-the-counter delivery of message traffic. The manual procedures at both the originating and the receiving NTCCs, and the reliance of user organization couriers for pick up and delivery of message traffic, adds substantially to the lag between the time when the originator writes the message and the time when the addressee reads the message.

2. DEFENSE DATA NETWORK (DDN)

a. Background

The Defense Data Network (DDN) is another system the P-3 community can utilize for long-haul, individual

messaging. The DDN was established in 1982 and is a set of worldwide networks based on technology developed by the Defense Advanced Research Projects Agency (DARPA). The original network developed by DARPA was termed the ARPANET [REF 7: p. 2-9]. The existing ARPANET formed the core of the DDN, which was designed to provide the DoD reliable, survivable, and secure worldwide communications services and the ability to transmit according to precedence requirements during both peace and war [REF 8: p. 59,60]. The research segment of DDN has kept the name ARPANET while the unclassified and classified operational user segment of the network has been designated as the Military Network (MILNET) and Defense Secure Network (DSNET) respectively. As the DDN has matured and expanded, there are now other active DDN segments. Collectively, the long-haul DDN segments and the baselevel transmission facilities are termed the DoD Internet [REF 7: p. 2-9]. Figure 2 [REF 9: p. 7] depicts the DoD Internet working environment utilizing gateway devices that allow seperate networks to talk to each other.

The DoD Internet uses a technology pioneered during the development of ARPANET called packet switching. Packet switching is an efficient method of sending data through a network. A message is divided into smaller segments called packets, and each packet is individually sent through the network. Each packet may take a different route through the network depending on which route is most efficient for

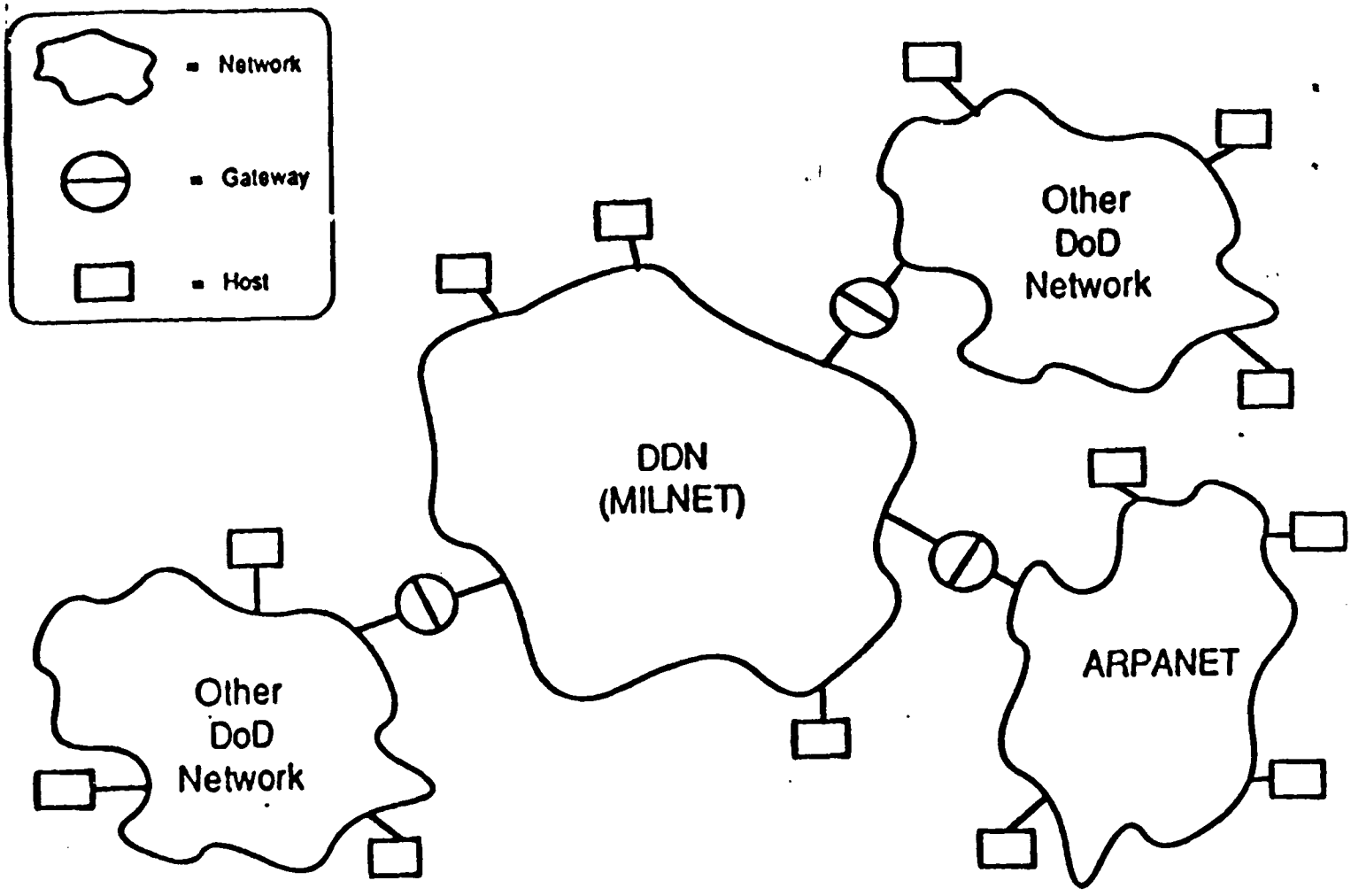


Figure 2. DoD Internet Environment.

that packet. As each packet reaches a packet swiching node, a routing algorithym at the packet switching nodes provide for the ability to adapt to changing network configurations and traffic patterns, contributing to network survivability, reliability, and flexibility. After each packet has reached its destination via its individual route through the network, the message is reconstructed for delivery to the addressee.

DDN switching technology differs from that of AUTODIN. AUTODIN utilizes message switching whereby the message enters and travels through the system in its entirety. Additionally, the AUTODIN has a much smaller number of switching centers than the DDN, resulting in messages stacking up in queues more often over the AUTODIN.

b. Electronic Mail (E-mail)

Individual messaging service is accomplished over the DDN using E-mail. E-mail has become quite popular as an alternative communication medium to the telephone, and it is becoming an integral part of electronic office work stations. The components of the E-mail system are as follows [REF 3: p. 13]:

- E-mail host computers which utilize applications that support E-mail functions such as writing, sending, receiving, editing, and storing E-mail messages.
- User computer terminals or personal computers with proper emulation communication software.

- On-line directories such as the DDN Network Information Center (NIC), which provide listings of DDN user names and mail box addresses.
- DoD Classified packet switching Internet
    1. Defense Secure Network 1 (DSNET1) - classified GENSER messages.
    2. DSNET2 - Worldwide Military Command and Control System (WWMCCS) classified messages.
    3. DSNET3 - Sensitive Compartmented Information (SCI) classified messages.
- DoD Unclassified packet switching Internet
    1. MILNET
    2. ARPANET

c. DDN E-mail Procedures

The DDN is a widely used network. The use of E-mail by DoD personnel has increased steadily, becoming an integral part of the daily communications between individuals throughout the DoD. A typical E-mail scenario starts with a user logging onto an E-mail host computer with a user ID and a password. The connection to the host can be made directly via dedicated circuits or through a DDN Terminal Access Controller (TAC) via a dial-up circuit. If the user is accessing the DDN MILNET from another network (i.e., ARPANET) or by a LAN, the connection is made via a gateway. At log on, the user can utilize a local list of commonly used addresses or request an address of an intended recipient using the DDN

NIC directory. Once the user knows the address of the recipient, a command (i.e., SEND) is given to the host signaling the intent to send a message. The host will then prompt the user for the addresses of the recipient(s), the subject, and the text of the message. The text can be composed on-line, or a file containing the text can be incorporated. After the message is composed and edited as required, the user can send the message by entering a command to the host (i.e., MAIL) or a message termination character. The address of the recipient(s) is then immediately checked by the host for errors or format problems. If there are errors, control is sent back to the user with an error message, otherwise the host adds date and time fields to the message and sends it through the network. The message is sent to the receiving host(s) via the packet switching nodes as described in the previous section. If a receiving host is unavailable, the message is stored at the sending host, and periodic attempts are made to deliver it. If the message has not been successfully delivered after a period of time, the message, along with an undelivered mail notice, is placed in the sender's mailbox. At the receiving host, the intended recipient's name is checked against a list of names that the host serves. If the name is on the list, the message is placed in the appropriate mailbox. If the name does not appear on the list of users or on a list of forwarding addresses, a non-delivery message is sent to the sender. When

the recipient logs on to his/her host, the system will indicate that a message has been received. The recipient can scan through the subject lines of the received messages and choose which message to have displayed or printed to hard copy. [Ref. 7: p. 2-11]

B. INTERNAL MESSAGE PROCESSING

The effectiveness and efficiency of operations of a P-3 squadron are directly related to how well a squadron runs its internal message and information processing. Messages relating to operational tasking, training requirements, administrative/personnel information, and maintenance issues are received and processed daily. The methods that a squadron uses to accept, distribute, and disseminate the daily message traffic are important to the success of the organization.

1. Squadron Organization

This section will briefly describe a typical P-3 squadron's organization. The major departments will be discussed, outlining the basic functions and contributions to the operations of the squadron. Figure 3 depicts an organization chart for a typical P-3 squadron.

a. Commanding Officer (CO)

The CO, or "skipper," has overall responsibility for the operations and integrity of the squadron. All personnel, equipment, squadron spaces, and the success or

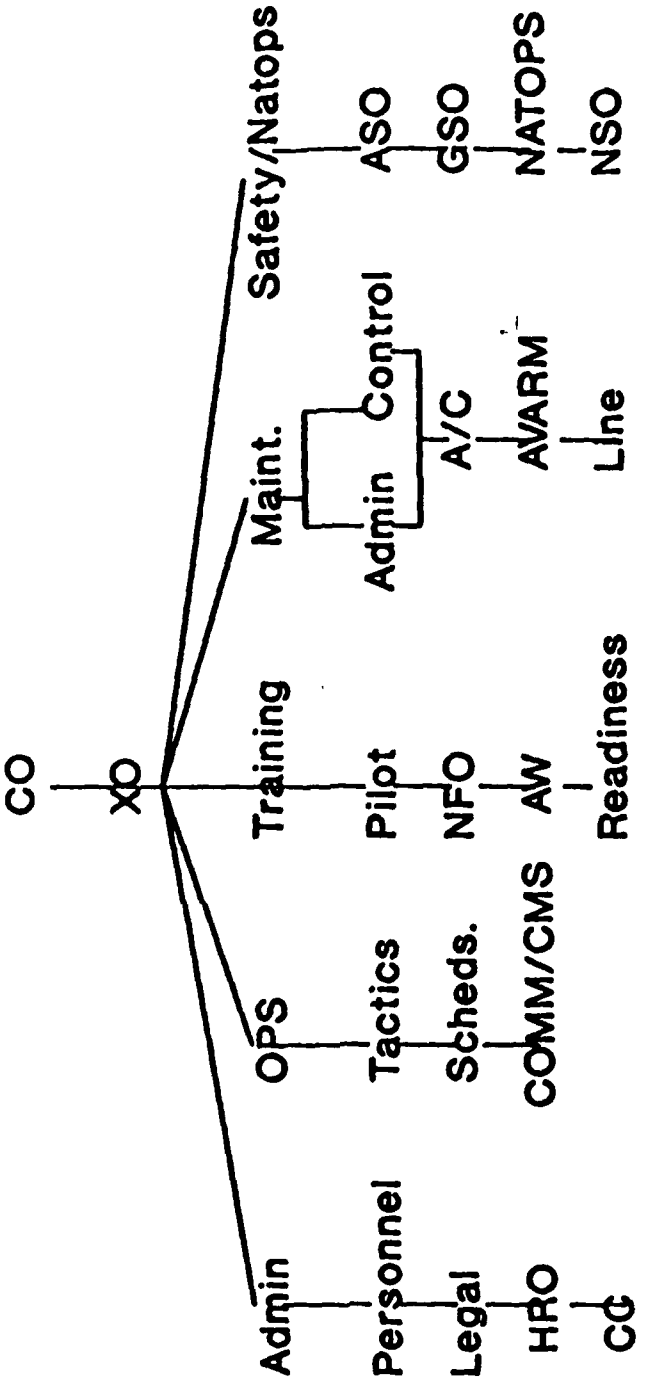


Figure 3. P-3 Squadron Organization.

failure of the mission are the CO's continuos concern and responsibility.

b. Executive Officer

The Executive Officer (XO) handles many of the administrative responsibilities of the front office and assumes the CO's duties and responsibilities when required.

c. Administration (Admin) Department

The admin department works closly with the CO and the XO, screening material, reports, and appointments for the front office, handling many of the responsibilities that affect the squadron's appearance to the senior and outside commands. Officer and enlisted personnel management is conducted by the admin department along with handling protocol issues, submitting recurring reports in a timely manner, tracking instructions, and preparing and publishing the Plan of the Day (POD). The Personnel, Legal, Career Couselor, and Humanitarian Services offices typically fall under the responsibility of the admin department. [Ref. 10: p. 38]

d. Operations (OPS) Department

The primary responsibility of the OPS department is the preparation and publication of the flight schedule. OPS ensures that all operational tasking is accomplished and that the assets needed for training requirements are scheduled. This requires good communications with the maintenance department for scheduling aircraft. Planning the squadron's

fuel budget and flight hours are also the responsibility of the OPS department. The Tactics and Communications /Communications Security Material system (COMMM/CMS) offices typically report to the OPS department head.

e. Training Department

The training department is primarily responsible for the training of the aircrew. Each aircrew member's progress towards positional qualification is tracked by this department along with the continuous training requirements for both qualified and unqualified aircrews. Daily training and readiness requirements are passed to the OPS department for inclusion in the flight schedule.

f. Maintenance Department

The maintenance department is typically divided into two areas, Maintenance Administration and Maintenance Control. Maintenance Admin is responsible for the administration of aircraft, tools, training and maintenance personnel. The tracking of quality assurance, technical publication library, maintenance instructions and monthly maintenance plans are handled by Maintenance Admin. Maintenance Control coordinates the maintenance divisions for the daily maintenance activities on the aircraft, while working with the OPS department to provide the aircraft needed to meet the flight schedule. The processing and tracking of

aircraft log books and maintenance records are also the responsibilities of Maintenance Control. [Ref. 10: p. 39]

g. Safety/Natops Department

The Safety/Natops department is responsible for ensuring the safe operations of squadron activities both on the ground and in the air. This is accomplished by publishing squadron safety Standard Operating Procedures (SOPs), tracking the attendance at safety schools, and running a proper and effective NATOPS program so that all aircrews are trained and qualified up to NATOPS standards for their respective aircrew positions.

2. COMM/CMS OFFICE

SOPs for the squadron COMM/CMS office are required to provide the necessary guidance for communications personnel in their daily routine, and in unique situations that might occur after normal working hours. Some items that should be included in the COMM/CMS SOPs are the COMM/CMS organization, COMM/CMS mission statement, and the Incoming/Outgoing message handling procedures. These are just a few of the items that should be included in the COMM/CMS SOP, and these will be discussed in this section.

a. COMM/CMS Organization

A typical organization chart for a P-3 squadron COMM/CMS office is depicted in Figure 4 [Ref. 11: p. 6].

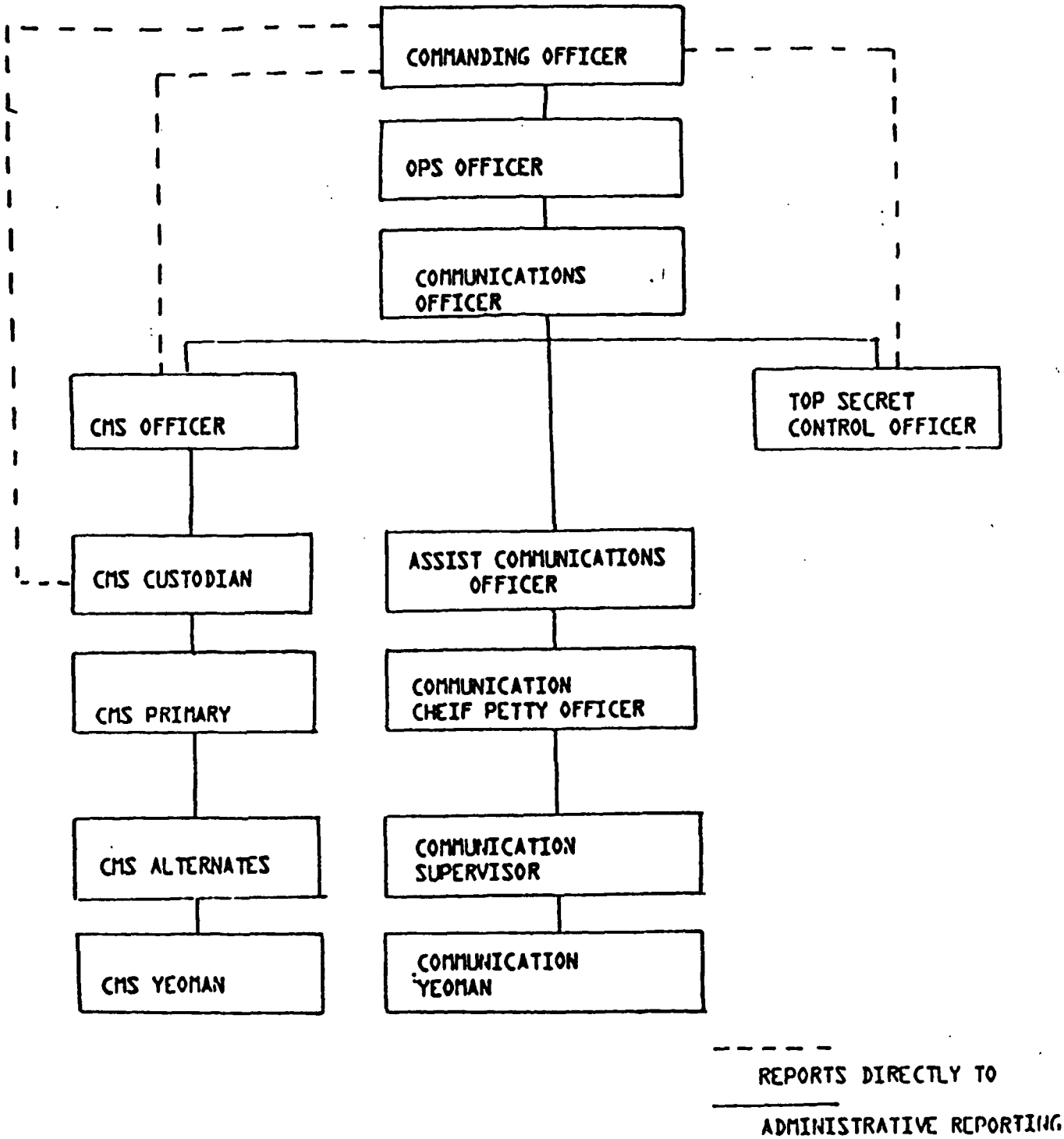


Figure 4. COMM/CMS Organization.

b. COMM/CMS Mission Statement

The following is a standard mission statement for a P-3 squadron's COMM/CMS office [Ref. 11: p. 8]:

- To provide rapid, secure, and reliable communications for the squadron. This includes:
  1. The receipt, transmission, and internal distribution of unit messages.
  2. The proper handling, control, and destruction of material issued through the Communications Security Material System.
  3. The physical security of communications security materials and information.

c. Incoming/Outgoing Message Handling Procedures

The squadron message handling procedures are important in the daily operation of the squadron as alluded to earlier. These procedures should be succiently documented and promulgated to all personnel whose work includes the handling of message traffic. The following is a typical message handling procedures list to be performed by COMM/CMS office personnel and should be included in a squadron's COMM/CMS office SOPs [Ref. 11: p. 9]:

- Outgoing Message Traffic
  1. Receive message through window, check DTGs, header lines, paging and format. Also look for signature on first page only.
  2. Check Plain Language Addressees (PLA).
  3. Make any corrections that need to be made to ensure speedy release.

4. Log out in Outgoing Logbook, place in closable container, and hand carry to NTCC.

- Incoming Message Traffic

1. Pick up message traffic at NTCC.

2. Prepare traffic for routing and message boards.

   * Route traffic to appropriate departments

   * Separate messages classified Secret from traffic and apply a secret control number, log into secret logbook.

   * Apply routing stamp to all messages.

   * Highlight DTG, subject line, squadron number, and info PLAs.

   * Apply action stamp to all action messages.

   * Post messages to correct message board.

d. COMM/CMS Daily Routine and Message Routing

The COMM/CMS daily duties are important in ensuring that the squadron runs efficiently and meets its mission requirements. The day starts early for the COMM/CMS office. A COMM yeoman typically arrives at 0430 to prepare the morning message boards. The yeoman will first stop at the NTCC and pick up the morning message traffic. Currently, at the NTCC the messages are given over-the-counter in hardcopy format. The yeoman will bring the traffic to the secure COMM/CMS spaces, apply routing and action stamps, highlight areas of the messages as appropriate, and log all Secret traffic in the secret log book, applying secret control numbers. The yeoman will then make copies of the messages

that will be distributed to the various departments. Typically, the unclassified messages for distribution will be placed in each department's mail slot or other similar holding device located in the admin department for pick up by department personnel. The classified messages for distribution are placed in each department's mail slot or other similar holding device (security clearance and need-to-know permitting) located in the secure COMM/CMS spaces for pick up on a daily basis by department personnel.

Once the copies of the appropriate messages are made, the Yeoman will prepare the message boards. Normally there are two types of boards: blue and red boards (colors may differ between squadrons). Blue boards contain messages ranging from unclassified to confidential and can be separated by subject matter (i.e., a board for admin messages, a board for maintenance messages, etc.). Red boards are for Secret and Secret LIMDIS messages and are also normally separated by subject matter into separate red boards. After the morning message boards are prepared, they are delivered to the CO's and XO's offices on their arrival.

When the morning message traffic has been read by the "front office", the COMM yeoman will take the boards to the appropriate spaces where they can be read by the department heads, division officers, or other squadron personnel with the proper clearances and need-to-know. The red boards are taken to the secure COMM/CMS spaces where their

access can be rigidly monitored. The blue boards may be taken to the squadron duty office or other space where their access can be constantly monitored.

During the normal workday, a duty COMM yeoman is on call to proofread all outgoing traffic, ensuring that corrections are made prior to delivery to the NTCC, and making corrections to those messages returned from the NTCC for correction. The duty COMM yeomann will make all afternoon message deliveries and pickups, update the boards as necessary, make copies of messages that are requested from squadron personnel, and properly file all messages as they are removed from the message boards. After normal working hours, there is always a duty Comm yeoman on call if their services should be needed. Typically, message pickup and delivery during the night is done by the squadron duty officer, who will pick up traffic both periodicaly or as necessary, depending on message precedence. On weekend days or holidays, a COMM yeoman is assigned to conduct the daily duties as described above, ensuring that the message boards are always up to date and messages are distributed as required.

III. THE DEFENSE MESSAGE SYSTEM (DMS)

A. BACKGROUND

In January 1988, the Assistant Secretary of Defense for C3I (ASD/C3I) formed a Multi-Service agency Defense Message System Working Group (DMSWG). The primary objectives of the DMSWG were to define the baseline DMS, reliably estimate its cost to the DoD, and to formulate a target DMS architecture based on achievable technology that satisfied writer-to-reader requirements while reducing cost and staffing and maintaining services. Improvements in functionality, survivability and security were considered as secondary objectives. The DMSWG formulated a DMS target architecture and the transition phases necessary to evolve from the baseline to the target, utilizing inputs from government and industry, and capitalizing on technological and standards advances. In May of 1988 the C3I Systems Committee of the Defense Acquisition Board (DAB) gave conceptual approval of the DMS target architecture and the transition approach. In August 1988, the Under Secretary of Defense for Acquisition USD(A) issued the DMS Program Guidance that provided approval of the DMS target architecture, phased implementation strategy, test and evaluation strategy, and management structure. The USD(A) also tasked the Defense Informations Systems Agency with responsibility for overall

DMS coordination and provided initial tasking to the services and agencies necessary to begin execution of the DMS implementation strategy. [Ref. 7: p. 1-1]

In October 1988, the management structure, depicted in Figure 5 [Ref. 7: p. 4-5], was fully activated, and the initial Target Architecture and Implementation Strategy (TAIS) document was approved and released for distribution to Government and industry by December 1988. The validated Multi-command Required Operational Capability for the DMS (DMS MROC 3-88) was implemented by the Joint Chiefs of Staff in February 1989. During October and November 1989, ASD/C3I issued interim policy guidance for DMS projects and for transition to the DMS target architecture. In accordance with the transition policy guidance, transition planning is underway by all services and agencies. [Ref. 7: p. 1-1]

B. DMS OVERVIEW

The DMS consists of all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically between organizations and individuals throughout the DoD. Obsolete components, procedures, protocols, formats and media will be phased out as the goal of the target architecture is achieved. The DMS program will be implemented in a series of phases. This phased implementation promises to gradually extend automation from the former line

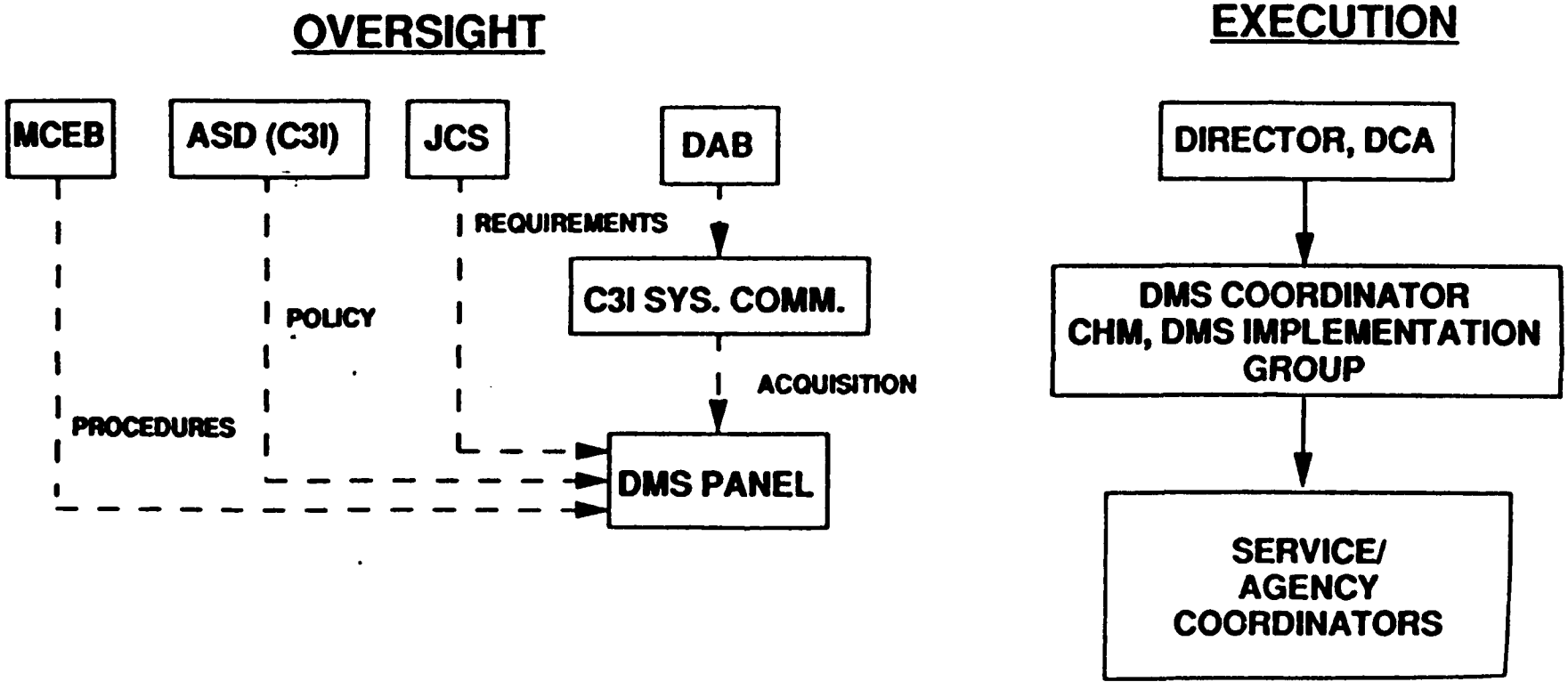


Figure 5. DMS Management Structure.

of demarcation at the NTCC down to an organization's office automation system. The transition has been planned to occur over a 20 year period, from 1988 to 2008. [Ref. 12: p. 2]

1. Baseline DMS

The DMS Baseline, as depicted in Figure 6 [Ref. 7 p. 2-2], consists of the Defense Communications System (DCS) component AUTODIN system and non-DCS components such as the base level NTCCs and the DoD Internet E-Mail system as it existed in September 1989. It will serve as the reference against which the future cost, manpower and performance incurred during the evolution to the Target Architecture will be measured. This baseline, frozen in time, is an evaluation tool which, except for minor technical corrections, will not change over the DMS planning period. [Ref. 7: p. 2-1]

2. DMS Phase I

The DMS Phase I as depicted in Figure 7 [Ref. 7: p. A-2], is targeted for completion by 1994. This phase emphasizes automation of existing NTCC functions and the extension of automated services down to the user level to reduce cost and manning at the base level. The development of an AUTODIN-to-DDN Interface (ADI) will provide an interface capability between AUTODIN and DDN E-Mail systems. E-Mail will evolve from Simple Mail Transfer Protocol to the international standard X.400 protocol, and a DoD Directory Service will be implemented on AUTODIN using the X.500 standard. During this

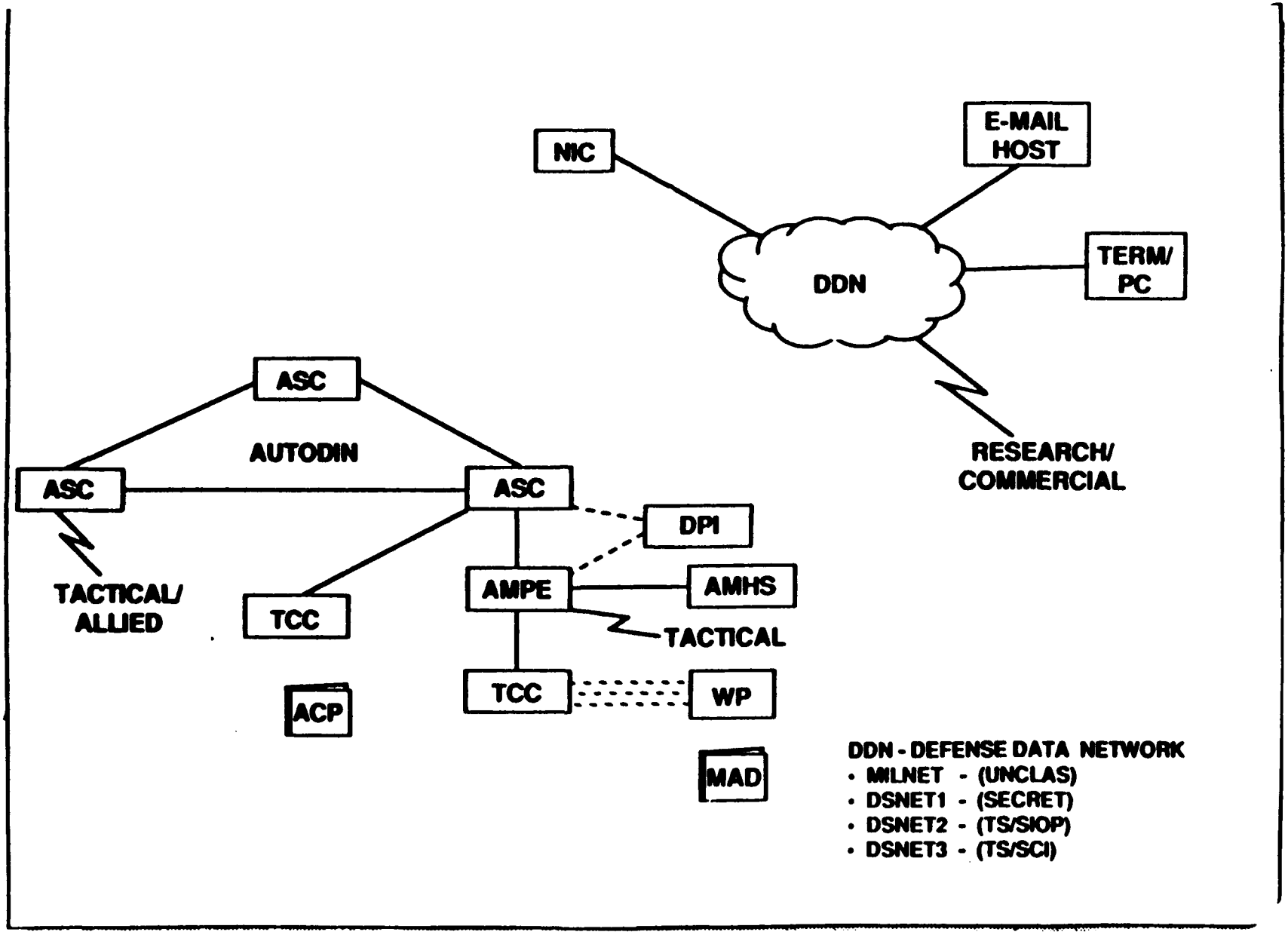
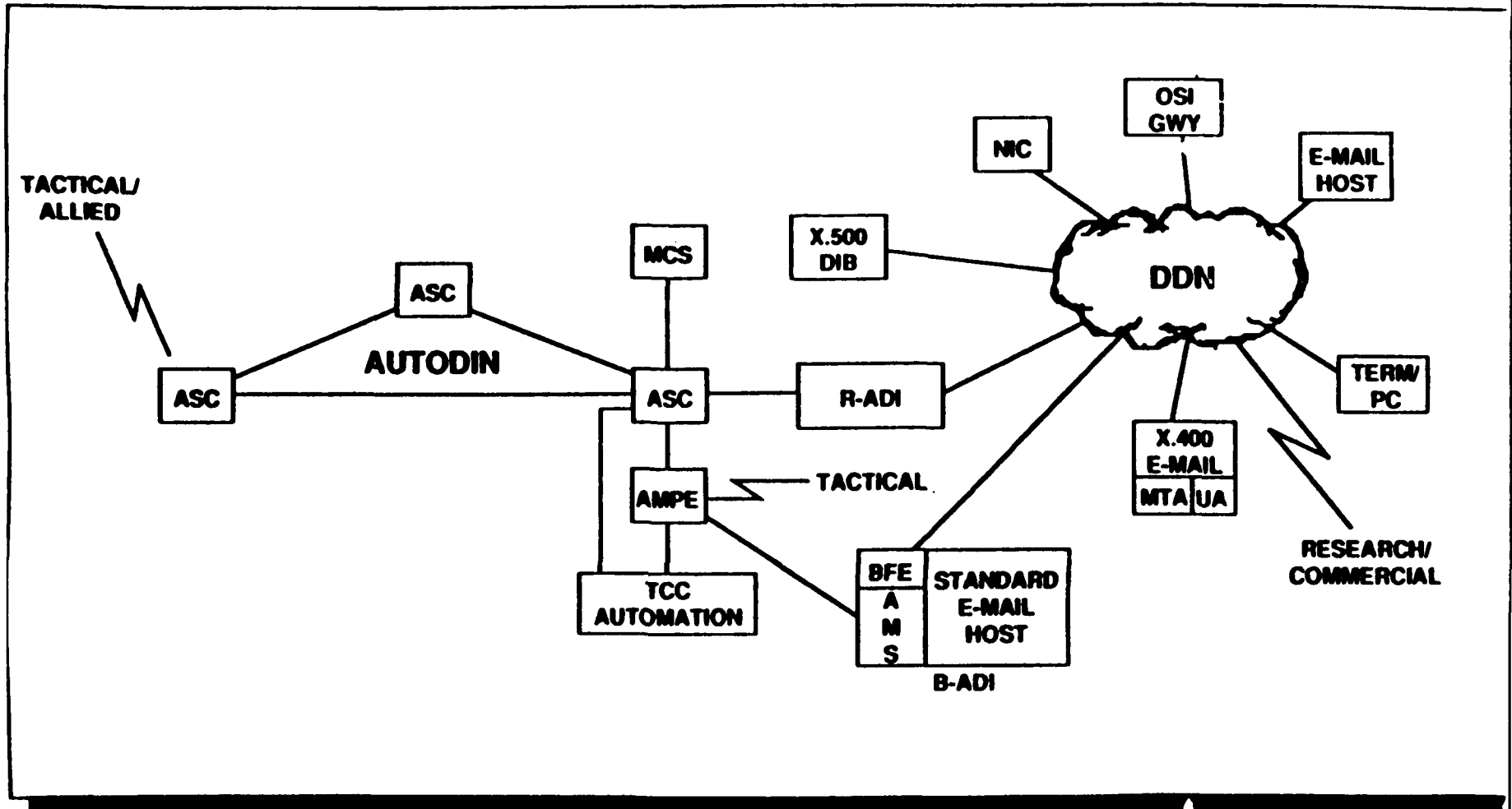


Figure 6. DMS Baseline.



LEGEND		
ASC - AUTODIN Switching Center	X 500 DIB - X 500 Directory Information Base	OSI GWY - Open Systems Interconnection Gateway
MCS - Message Conversion System	R ADI - Regional AUTODIN DDN Interface	UA - User Agent
AMPE - Automated Message Processing Exchange	B ADI - Baselevel AUTODIN DDN Interface	DDN - Defense Data Network
TCC - Telecommunications Center	BFE - BLACKER Front End	AMS - AUTODIN Mail Server
	MTA - X 400 Message Transfer Agent	

Figure 7. DMS Phase I.

phase the Navy will promulgate an E-Mail policy and the DMS will provide AUTODIN equivalent services on DDN using E-Mail technologies. As this service becomes available, the Navy E-Mail policy will evolve to take advantage of this more economical service. These efforts will provide the opportunity to begin phase-out of resource intensive base level NTCCs, and migrate AUTODIN data pattern message traffic to the DDN. [Ref. 12: p. 2]

3. DMS Phase II

The DMS Phase II, as depicted in Figure 8 [Ref. 7: p. B-6], is targeted for completion by 2000, and will produce the most obvious architectural changes and improvements for the users with deployment of an integrated DMS (i.e., incorporation of video, data, and narrative messages). The integrated DMS will be based on X.400/X.500 International Standards with current protocols, procedures, and message formats changing. The DMS X.400 Message Handling System (MHS) will provide User Agents (UAs), Message Transfer Agents (MTAs) and Message Store (MS) components to enable individual users and organizations to send, receive, and store messages. Fully automated X.500 directory services will support the desktop-to-desktop messaging concept. The NTCCs and the AUTODIN Switching Centers (ASCs) will be completely phased out by the end of Phase II. Base-level connectivity with DMS will be additionally implemented during this time frame by the

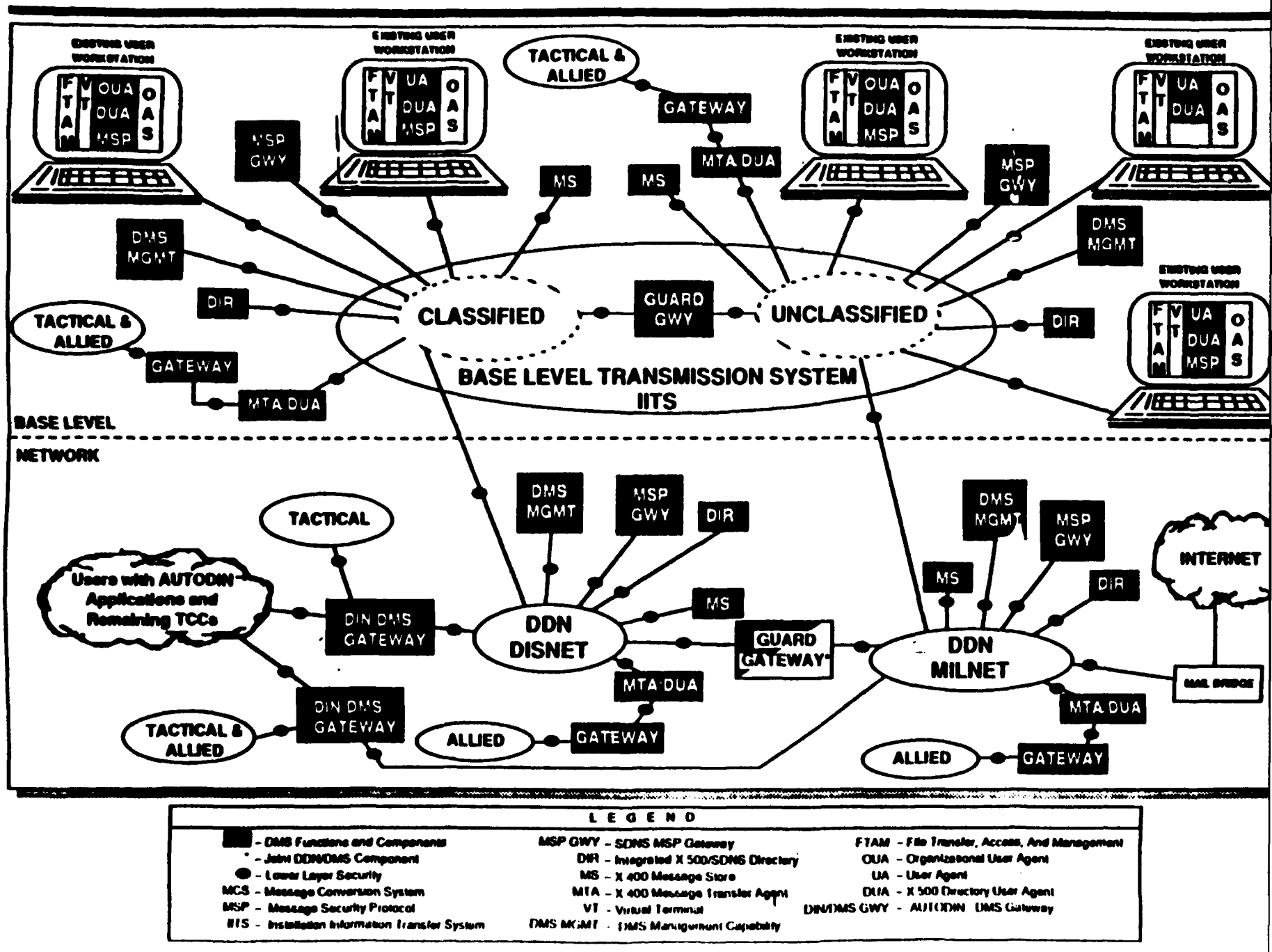


Figure 8. DMS Phase II.

implementation of the Base Information Transfer System (BITS) concept, which will be explored in a later section. [Ref. 12: p. 2]

4. DMS Phase III

DMS Phase III, as depicted in Figure 9 [Ref. 7: p. C-3], is the last phase, scheduled to be completed by 2008. Phase III commences when the last AUTODIN Switching Center is closed. The major effort in this phase is to achieve an Integrated Services Digital Network (ISDN)-based integrated Defense Information System (DIS). The transitional components deployed in earlier phases will be phased out, and the local and long haul portions of the program will mature to achieve the target architecture.

C. DMS TRANSITION

The DMS transition and component changes will be explored in this section. Emphasis will be placed on the transitions to Phases I and II, and the DMS components that will concern the P-3 community during the transition.

1. Phase I Components

a. Personal Computer Message Terminal (PCMT)

The PCMT is a low cost, low volume message terminal located at the NTCC that allows the use of diskette media to send and receive organizational message traffic. Outgoing and incoming message traffic can be delivered or accepted on diskette, eliminating the need for DD173s and the

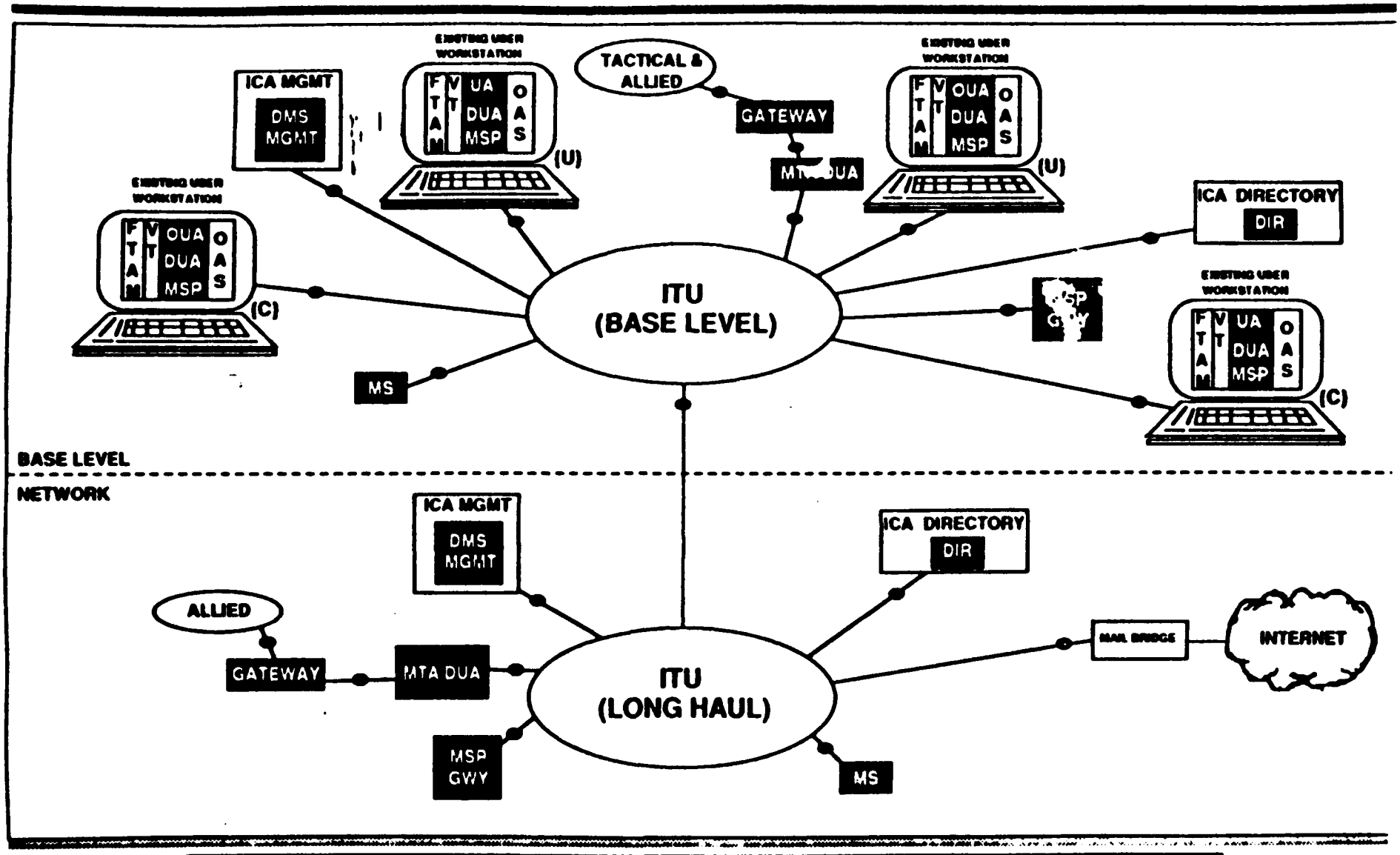
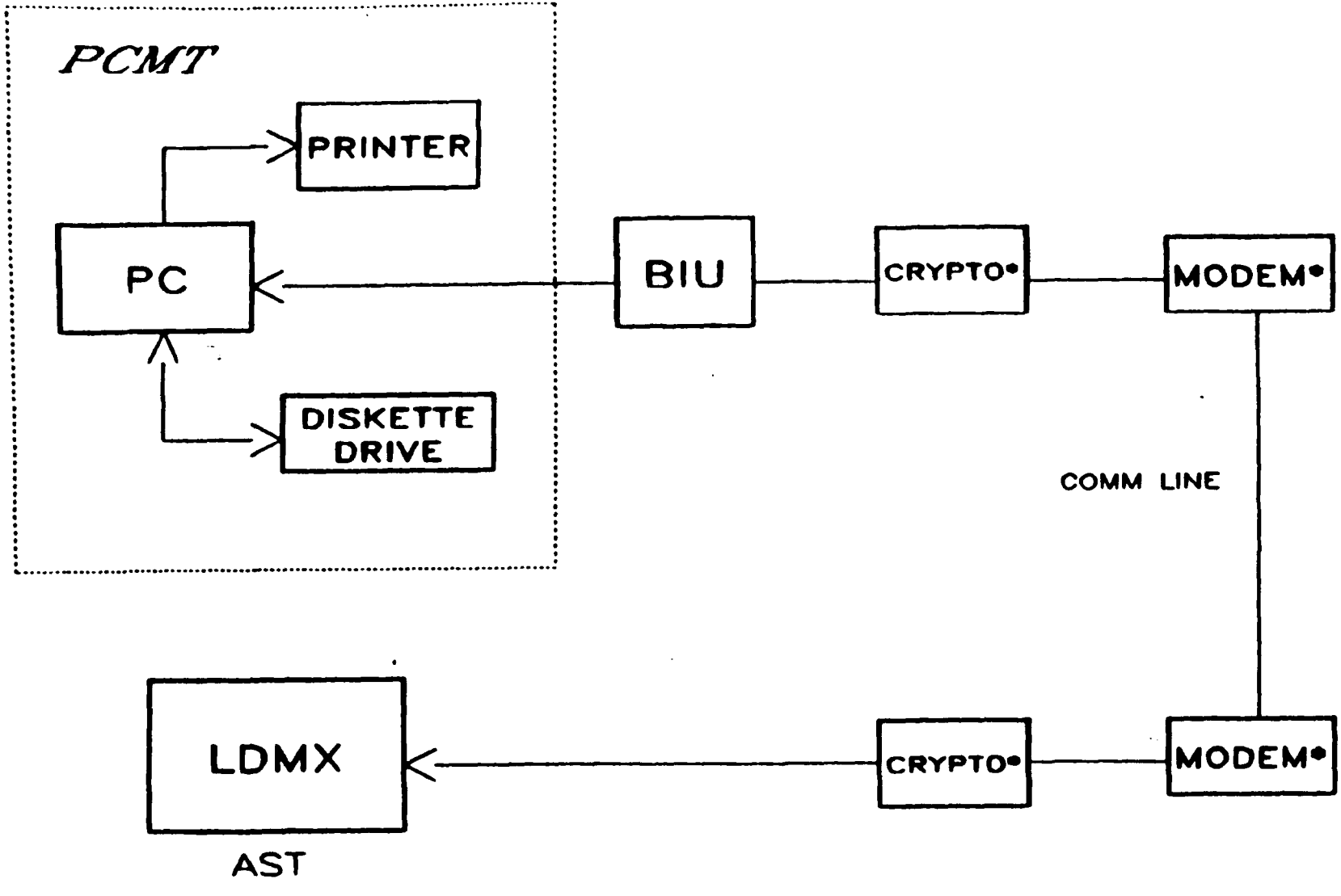


Figure 9. DMS Phase III.

reliance on OCRs. [Ref. 12, p. 3]

The PCMT exchanges organizational message traffic with an AUTODIN Subscriber Terminal (AST) (i.e., LDMX, NAVCOMPARS) over a communication link employing LDMX/RIXT communication protocol, interfaced by using an NTS Bus Interface Unit (BIU). This interface allows the AST to route and process information to and from the PCMT in the same manner as if it had been interfacing with a Remote Terminal System (RTS). The AST will then be able to route the traffic from the PCMT to the AUTODIN. Figure 10 [Ref. 4: p. 3-51] illustrates a typical PCMT configuration. [Ref. 4: p. 3-50]

The hardware utilized by the PCMT is an IBM AT compatible microcomputer equipped with at least 3 MB of RAM, a 10 MB removable disk storage unit, and a diskette media as required by the Diskette Message File Standard for Defense Messaging. Selected DCT 2000s, SRT/RIXT, AUTODIN Mode II and V terminals, as well as some LDMX/NAVCOMPARS backside TTY circuits, can be replaced by the PCMT. The PCMT may be considered for any message terminal requirement where the traffic volume is low and the message media can be satisfied by printed copy or diskette. The PCMT software can be distributed over multiple PCs connected by a bus to handle high traffic volumes. Dial-up capabilities to the PCMT are being pursued to exchange information electronically, eliminating or reducing the requirements for courier services to and from the NTCC. [Ref. 4: p.3-52]



* CRYPTO AND MODEM REQUIRED ONLY FOR LONG DISTANCE LINE BETWEEN PCMT AND LDMX

Figure 10. PCMT Configuration.

b. GateGuard

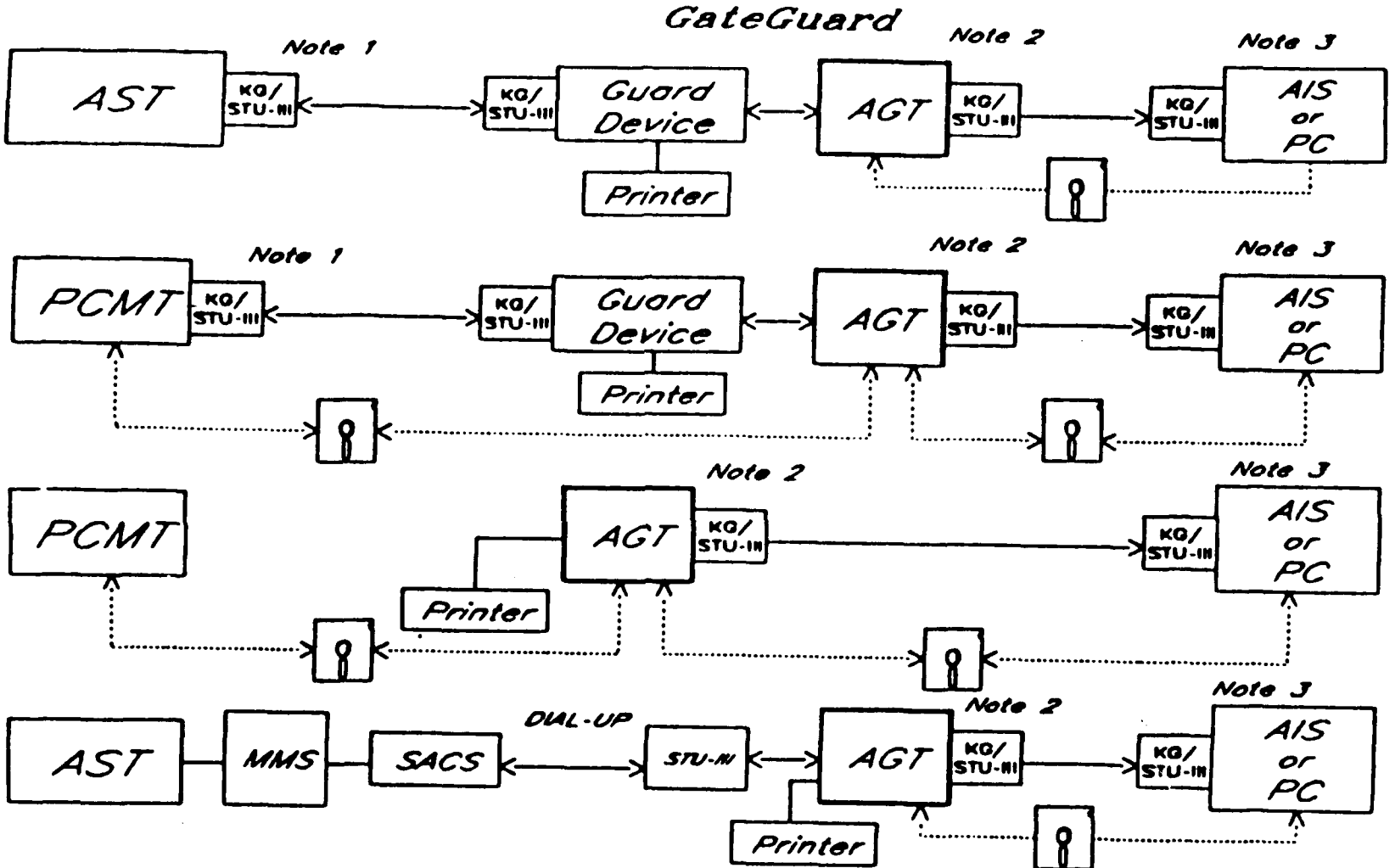
The DMS component that provides dial-up interface to the PCMT and LDMX for the transfer of message traffic electronically is the GateGuard. This message delivery system takes the place of the organizational courier who picks up and delivers messages at the NTCC. It will act as the primary AUTODIN interface point for a single organization. Narrative and card formatted messages can be exchanged using GateGuard, and copies of messages can be generated on diskette and/or paper with the GateGuard. AUTODIN messages can also be exchanged between the NTCC and a user organization's Office Automation System (OAS)/Automated Information System (AIS) over two separate communication links supported by GateGuard. [Ref. 12: p. 3]

The GateGuard system is composed of three elements: a Guard Device (for use on dedicated links), an AUTODIN Gateway Terminal (AGT), and a gateway communication link. The interface to a NTCC's PCMT will be over a Secure Telephone Unit (STU) III or crypto covered dedicated circuit that operates at speeds ranging from 300 to 9600 baud, or a STU-III covered dial up circuit. The GateGuard can also generate diskettes to be exchanged with a PCMT via courier if need be. The GateGuard software will operate on an AGT microcomputer system, available under the Desktop III contract, or on compatible equipment. The AGT can interface electronically with an organization's LAN using Kermit File

Transfer Protocol, or can optionally provide paper or diskette media for message dissemination within the organization. [Ref. 4: p. 3-54]

A Guard Device will be utilized on direct connect circuits from the user organization to the NTCC to prevent messages, which have a classification higher than the organization is authorized to access, from reaching the user organization's LAN or Office Information System. The Guard Device is a TEMPEST hardened Bus Interface Unit and will serve to isolate sensitive data contained in the serving LDMX or PCMT from data processed by the GateGuard. [Ref. 4: p. 3-54]

The GateGuard is designed to interface with the serving LDMX or PCMT in both directions via a communications link or with diskette media. However, if the GateGuard is interfaced with a LAN or office information system at the user organization, messages will cross this interface in one direction only, unless a DMS-approved automated message release capability is available on the LAN. If this release capability is not available, the GateGuard can be physically secured and procedurally controlled to allow for message traffic to be released electrically to the LDMX or PCMT over the communications link, or released via diskette media. If the GateGuard is supporting only unclassified messages, the circuit from the NTCC to the GateGuard at the user organization still must be encrypted by using a STU-III or KG-84 encryption device. A GateGuard configuration, as depicted



Note 1 - AST-GateGuard link must be crypto covered if circuit not entirely contained within controlled spaces regardless of traffic classification

Note 2 - GateGuard-AIS link must be crypto covered if circuit not contained within controlled area and message traffic is classified

Note 3 - GateGuard connectivity to AIS is optional for all configurations

Figure 11. GateGuard Configuration.

in Figure 11 [Ref. 4: p. 3-56], will perform the following functions:

- Audit Trail
- User Identification
- Message Storage and Retrieval
- Format Checking
- Security Checking
- Precedence Notification
- Message Routing.

For those commands that are exchanging messages with the NTCC using diskette media instead of electrically, a GateGuard is still encouraged to provide the central accountability on all AUTODIN received messages as well as a standard entry point for disseminating the message on their LANs [Ref. 4: p. 3-58].

c. Multi-Level Mail Server (MMS)

The GateGuard system as described in the previous section has a shortcoming in that the electronic transfer of messages between the organization's GateGuard and the LDMX/PCMT at the NTCC requires a dedicated, encrypted circuit. Currently, there is inadequate connectivity available on the LDMX/PCMT to support all the organization GateGuards requiring access. Another problem is the arrival of messages during the off-duty hours of some organizations. Thus a method is needed

to store messages for these organizations until normal working hours. This is feasible for those organizations where high precedence messages are not a common occurrence. These problems are addressed by the Multi-Level Mail Server (MMS). [Ref. 4: p. 3-66]

The MMS will provide dedicated and dial-up interfaces between the user's GateGuard to user mailboxes within the MMS, allowing for the electronic exchange of both unclassified and classified (up to Secret) messages. The MMS will be collocated with the LDMX or Remote Terminal System (RTS) (which is replacing the high and low volume RIXTs and SRTs), providing dial-up GateGuard connectivity for organizations that do not have large message volumes and/or do not operate 24 hours a day. Those organizations with large traffic volumes operating on a full time basis will connect their GateGuard directly to the serving LDMX or PCMT. The need for dedicated lines is eliminated by the MMS, and the over-the-counter (OTC) functions at the NTCC for handling up through secret messages are automated. [Ref. 12: p.4]

The basic configuration for the MMS, as depicted in Figure 12 [Ref. 4: p. 3-67], consists of two AT&T 3B2/600g computers, available through the existing Standard Multi-User Small Computer Requirements Contract (SMSCRC). The 3B2/600g supplies enough disk storage to provide dedicated connectivity for up to 256 subscribers. The MMS dial-up capabilities will be provided using the AT&T STU-III Access Control System

(SACS) at the MMS and a STU-III at the user organization. The AT&T System V/MLS multilevel secure UNIX operating system plays a big part in the MMS system. The System V/MLS is a B1 certified (trusted) system and, along with the AT&T SACS, allows the formation of a powerful, flexible, adaptable, fully secure system. [Ref. 13: p. 4]

MMS provides store-and-forward capabilities for organizations that do not operate on a 24 hour basis. The subscriber's incoming messages may be stored in separate, classmarked mailboxes for up to four days, and can be retrieved electronically when the subscriber logs on to the system. Subscriber authentification is accomplished by both user identification and password authentification. The MMS system will automatically record which users are on-line, and provide audit trail capabilities, supplying security data on users logging on to the system. The generation of various usage and audit reports can be provided by MMS on demand, as well as subscriber lists, mailbox assignment reports, and mailbox status reports. [Ref. 13: p. 4]

2. Phase I Software

There are a number of software packages that are being developed and tested for DMS to provide the user with true automated writer-to-reader messaging services. Some of the user software that is being developed for DMS will be discussed in this section.

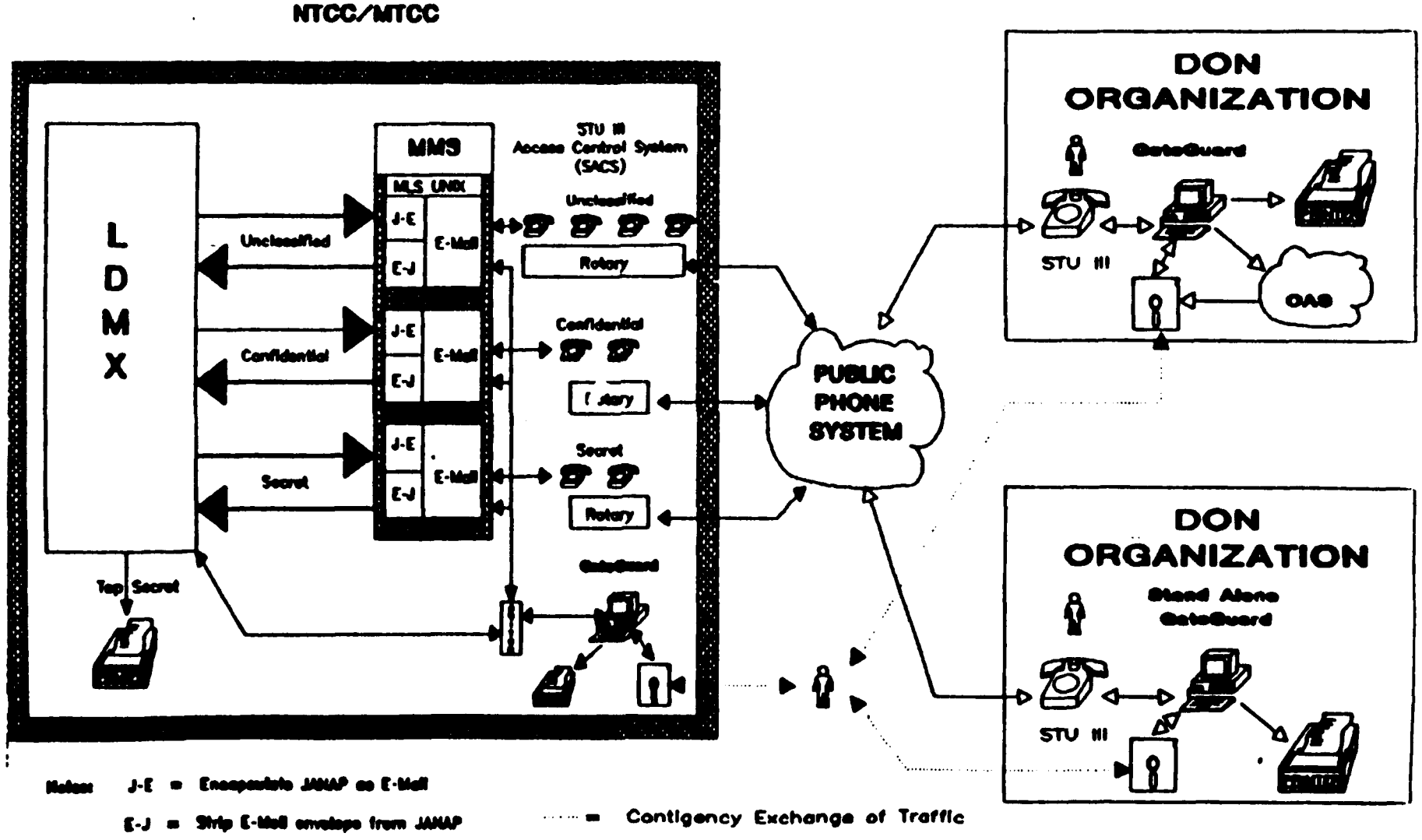


Figure 12. MMS Configuration.

a. Message Dissemination Subsystem (MDS)

Once an AUTODIN message is received electronically via GateGuard or diskette, the manual delivery of the message to action officers within a user organization is automated by MDS through electronic dissemination of organizational messages by office codes, with delivery via a LAN. The MDS is a software package that will reside in the organization's LAN and work with a message preparation software package such as Message Text Format (MTF) Editor. The MDS system provides for two types of users: a Default User and a Regular User. The Default User acts as an MDS system supervisor, setting up system parameters, activating the automatic dissemination of messages and screening any messages that could not be automatically disseminated. Regular users can view any messages that are disseminated to them, delete messages in their personal MDS mailboxes, print messages, or route them on to other MDS users on the LAN. If a DMS approved release authentication mechanism is implemented, outgoing messages can be released electronically from the MDS to the GateGuard. [Ref. 12: p. 5]

b. Message Dissemination Utility (MDU)

For users without access to a LAN, a software package that facilitates the manual delivery of AUTODIN messages is MDU. The MDU system is installed on a stand-alone PC and allows a command to receive traffic electronically from

GateGuard or diskette. The MDU provides the operator with a user-friendly environment for sorting and disseminating AUTODIN messages based on office codes within the command. Messages can be printed for dissemination or segregated into multiple diskettes for dissemination. The MDU runs on an IBM compatible system with a DOS operating system. [Ref. 12: p. 5]

c. Message Dissemination Link (MDL)

MDL is a software package designed to be used in conjunction with MDS in a multiple network environment. The system will receive AUTODIN messages electronically via GateGuard, and route the message to the appropriate network based on office codes. [Ref. 12: p. 5]

3. Phase II Components

This section will briefly describe the major components that are expected to be implemented during Phase II.

a. User Workstations

DMS messaging will be implemented during Phase II using existing user workstations. The X.400 messaging environment will be implemented during this phase, and User Agent (UA) messaging application software will be implemented in user workstations to allow individual messages to be processed by the user in the X.400 environment. Organizational User Agent (OUA) application software will also

be implemented in the user workstation to allow the user to be able to prepare, staff, and release originated messages and distribute received organizational messages from the PC workstation. Thus, the user workstation will contain both OUA and UA functionality to allow the user to send both organizational and individual messages. [Ref. 4: p. 4-10]

Directory User Agent (DUA) software applications will also be implemented in the user workstation to allow the user to access the DMS X.500 Directory Service. The DUA will access the directory through the Directory Systems Agent (DSA), which may use information in its own data base or direct the request to another DSA. The X.500 DUA protocol will allow the user to obtain the appropriate addressing, encryption, and authentication information in support of the X.400 messaging environment. A Secure Data Network System (SDNS) Message Security Protocol (MSP) is currently being designed by the National Security Agency (NSA) to encrypt and decrypt X.400 messages at the user workstation. The goal of DMS is to eventually implement a bundled UA/DUA/MSP package into every workstation that has an organizational or individual messaging requirement. [Ref. 4: p. 4-15]

b. Base Information Transfer System (BITS)

The DoN plans to provide connectivity between user workstations and DMS at the base-level by the Base Information Transfer System (BITS). Figure 13 [Ref. 14: p. 4-7],

illustrates the general configuration for BITS. BITS implementation will be considered on a case by case basis for each base that has DMS connectivity requirements. Some DoN organizations may access a BITS located geographically close by or continue the MMS dedicated or dial-up connectivity provided in Phase I. A Network Management Center (NMC) will reside at each BITS, staffed by retrained personnel previously manning the NTCCs. The following services are expected to be integrated into BITS [Ref. 3: p. 18]:

- File transfer
- Interactive modes
- E-Mail
- Video teleconferencing
- Security
- Voice communications.

4. Phase III Components

There are no major configuration or component changes planned at the base level during Phase III. The design and implementation of X.400 components started in Phase II will be completed in this phase as well as DoN-wide MLS BITS implementation and the evolution of the ISDN-based Defense Message System.

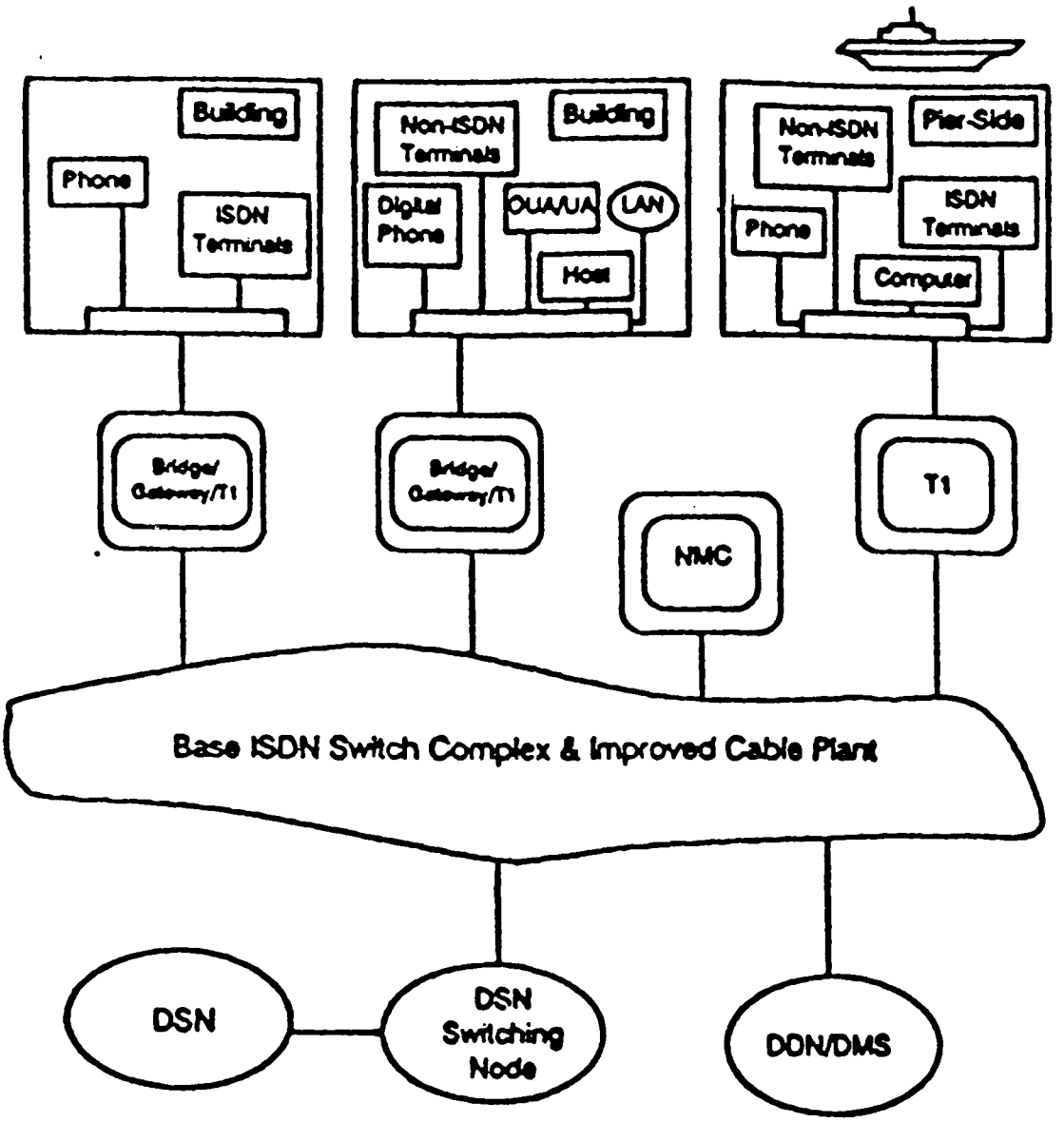


Figure 13. BITS Configuration.

Connectivity between afloat and ashore users will be enhanced in this phase with the implementation of the Communications Support System (CSS). Prior to this phase, the NAVCOMPARS will be providing the necessary messaging interfaces to the fleet, making the DMS transparent to afloat users. The CSS will integrate transmission systems providing connectivity between afloat and ashore users to provide multimedia communications with dynamic load sharing capabilities. The goal is to provide direct DMS connectivity to all fleet units by the end of Phase III.

D. TRANSITION ISSUES

This section will explore the transition issues that are currently affecting or will affect the P-3 community. Current transition efforts that are underway in the community will be discussed, as well as problem areas that are being encountered, or expect to be encountered, as the transition to DMS continues.

1. DD-173 to Diskette Transition

The first major transition issue that the P-3 community is facing is the mandatory elimination of DD-173 message forms. Effective 1 April 1992, the Navy is requiring NTCC subscribers to transition from the use of DD-173s to magnetic media messages submitted on either a 5 1/4 inch or 3 1/2 inch floppy disk. The transition was announced via a

message CNO Washington D.C. OP-094, DTG 062317zDEC91. Some of the highlights of this message are as follows [Ref 15: p. 1]:

> As personal computers move the Navy rapidly into the electronic age of writer-to-reader desktop messaging, we must begin eliminating the use of error prone/high cost DD-173 message forms...Message preparation on a DD-173 requires a unique form/Non-Standard size paper and special OCR printer fonts, all of which are relatively expensive. Additionally, we have all experienced major frustrations due to recurring misreads by antiquated comm center optical scanning equipment...A single 5 1/4 inch diskette costs less than a dollar and can hold up to 80 average length Naval messages. Over the counter diskette service will also allow us to eliminate comm center optical scanning equipment along with its associated high cost maintenance...As terminal equipment becomes available to provide over the counter diskette service at those message centers not currently equipped, over-the-counter customers will be allowed four months to transition and eliminate DD-173s from the date diskette service becomes available.

The transition from the DD-173s to the diskette media raises a number of procedural issues that need to be addressed by the commands within the P-3 community to ensure proper compliance with Navy standards. The procedures for preparing and handling messages on diskette are provided by NTP 3(H) ANNEX D. This section will look at some of these procedures, and address requirements during the early stages of the transition to DMS when mobile commands such as P-3 squadrons will be physically carrying diskettes to the NTCCs.

a. Hardware/Software Requirements

The hardware that currently is being used to generate messages on diskette are the Zeniths Z-200T, Z-248, and Z-386T, IBM PCs, Desktop IIIs, or any other compatible PC hardware that runs Microsoft DOS (MS-DOStm) or Personal

Computer DOS (PC-DOStm) Version 2.0 or higher operating systems. The hardware that will be used to generate classified messages on diskette must comply with the requirements put forth by OPNAVINST C5510.93, and it must be installed in accordance with NACSIM 5100A regarding TEMPEST emanations. [Ref. 16: pp. D-2,D-4]

The application software used to generate the messages on diskette must run on the operating systems described above and be able to perform the following functions [Ref. 16: pp. D-4,D-5]:

- Format, electronically label, and prepare new, blank diskettes.
- Declassify/reformat diskettes.
- Prepare Table of Contents file and Releasing/Receipt Document.
- Generate narrative message prolog format.

A standard message preparation, display, and printing application software package called Message Text Format (MTF) Editor is currently being used by Navy commands and meets the functional requirements specified above [Ref. 4: p. 3-46]. MTF Editor can be requested from the Commanding Officer, Marine Corps Tactical Systems Support Activity, Code (CISD), ATTN: MTF Editor Project Officer, Camp Pendleton, CA 92055-5080 or by calling (commercial) 619-725-2286/2415 or (DSN) 365-2286/2415, with suggestions or problems concerning MTF Editor faxed to (commercial) 619-7252210/2812 [Ref. 12: p.5].

The MTF Editor software can also be obtained from commands that currently utilize it because the software is shareware and thus can be copied for use by another command [Ref. 19].

b. Subscriber Responsibilities

There are a number of responsibilities that organizational NTCC subscribers must adhere to as they transition to diskette media.

(1) Subscriber Incoming Message Procedures

Subscribers may pick up diskettes that contain their incoming messages whenever desired or required, however it is the subscriber's responsibility to process diskettes in a timely manner. The subscriber will provide a properly formatted diskette that the NTCC will transfer the message data to. A single properly marked diskette can be used to handle messages classified up to SECRET. The diskettes shall be safeguarded during the transit to the message center and, at the minimum, kept in a courier pouch and protected from moisture, extreme heat, magnetic fields, and bending while in transit. [Ref. 16: pp. D-1,D-4]

(2) Subscriber Outgoing Message Procedures

Subscribers can submit message traffic classified up to SECRET on diskette to the NTCC. Messages classified as TOP SECRET, SPECAT, or pseudo SPECAT must be delivered to the NTCC on DD-173 forms vice diskette. Subscribers are required to have a write protect tab affixed

to each diskette and the diskette shall have an external label listing as a minimum the unit or activity name, the permanent diskette identification number, and the highest level of classification, most restrictive marking, or associated markings for any message stored on it. Diskettes shall be marked as follows [Ref. 16: pp. D-1,D-3]:

- Unclassified messages - Green, SF 710
- Confidential messages - Blue, SF 708
- Secret messages - Red, SF 707

The subscriber is also responsible for providing a typed or computer-generated releasing/receipt document for each diskette. The document must contain the signature of the releasing officer, who is responsible for ensuring the messages on the diskette are properly formatted, along with a complete listing of all messages on the diskette in precedence order. The manner in which the classification of the message on the diskette was derived must be recorded in accordance with OPNAVINST 5510.1 and local procedures. Diskettes must also be safeguarded in transit as mentioned previously, and classified diskettes shall be stored in proper security containers when not being used and protected with the same security precautions as other classified documents. [Ref. 16: pp. D-1,D-2,D-4]

c. Maintenance/Training

With the transition from the DD-173s to the diskette media and the continued drive towards automation as DMS evolves, computer technology will be utilized at an increasing rate. It is important that personnel are properly trained in the use of the emerging technologies. One of the complaints coming from the telecommunications centers is the "lack of basic computer knowledge among the subscribers" [Ref. 17]. This lack of knowledge of computers hinders the transition process. Many users are not properly or formally trained on the use of the MTF Editor, or even educated in the basic MS-DOS commands needed to access the application software. Ideally the user organizations should provide for training opportunities for their personnel. Commands can arrange to send one or two of their more computer literate personnel to the local telecommunications center to receive either formal or informal training on the MTF Editor and use these personnel to set up training programs within the command on both basic computer skills and MTF Editor. NTCC Moffett has provided formal training at the station theater and has set up trouble shooting teams to go to the individual commands to help with the transition. Videos and documentation on MTF Editor as well as other DMS related software and hardware can be requested by mail, message or NAVGRAM from NAVTELSYSIC in Cheltenham, MD [Ref. 12: p. 9]. RM-A School is also currently

being revamped to include ADP training for Automated Communications Systems [Ref. 18: p. 9].

The maintenance of the computer hardware is another important issue that the organizational users need to be aware of as computer technology is increasingly utilized for communications. Some maintenance items concerning computer hardware are as follows [Ref. 12: p.8]:

- The Z-200T and Z-386T are TEMPEST PCs and must be repaired by Zenith or a designated agent to ensure TEMPEST integrity.
- Z-248 repair is accomplished by training on-board personnel to trouble shoot to the circuit board level. Once the circuit board is identified, the repairman arranges with either NCTS Pearl Harbor, NCTS Washington D.C., or NCTS Jacksonville to repair or exchange the failed board. Until personnel are trained or if onboard repair is not feasible, commands must establish local "time and materials" contracts for repair.
- NCTS Norfolk and NCTS San Diego offer 4 and 5 day courses, respectively, on the repair of Z-248 computers. Organizations wishing to use these courses may contact NCTS Norfolk at (DSN) 565-7976, (commercial) 804-444-7976 or NCTS San Diego at (DSN) 735-8653, (commercial) 619-545-8653.

2. Transition to Electronic Transfer of Messages

The ultimate goal of DMS is to provide true writer-to-reader electronic transfer of message traffic. In the P-3 community the electronic transfer of messages may not occur until well into Phase II of the DMS transition. There are a number of issues that need to be addressed as the P-3

community moves towards electronic transfer of messages. Some of these issues are discussed below:

a. DMS Transition Plan

One of the first items that needs to be addressed is that the DMS transition plan as outlined in a previous section is a living document. This means that the plan is subject to changes as each DMS working group meets and research and tests of components are completed. This should always be kept in mind as the P-3 community moves towards electronic transfer. What may have been the plan previously, may change as time goes on.

b. DMS Components

For a P-3 squadron to transition to electronic transfer of messages there are DMS components that are required to be in place for this to occur. There has to be access to a GateGuard system at the squadron with either a dedicated encrypted circuit directly connected to an LDMX or PCMT or a secure dial-up circuit available that will interface with a Multi-Level Mail Server (MMS) installed at the comm center. The number of commands that will need access to a GateGuard system and comm circuits at the stations the P-3 community works from precludes that the individual squadrons will get a dedicated encrypted circuit. There are a limited number of backside circuit connections available to an LDMX or PCMT, thus it is more feasible that the P-3 community will be

utilizing dial-up circuits to a MMS. Currently there is only a development MMS system installed with 14 more to be implemented in FY 1992 and approximately 24 in 1993 [Ref 18: p. 6]. This means the P-3 community will be utilizing over-the-counter transfer of diskette media for the near future until MMS systems are installed at the comm centers that they are serviced by and the hardware and software that is required by the individual commands to transfer electronically is procured.

c. Procurement

According to the DoN DMS Transition Plan NAVCOMTELCOM is responsible for funding NTCC/MTCC systems such as the MMS and the RTS, while user organizations will be responsible for programming funds to acquire user-operated system such as the GateGuard, STU-IIIs, MDS and LANs [Ref. 4: p. 3-97]. Currently there is a movement within the Navy towards the goal of procurement of the DMS components necessary to transition to electronic transfer of messages. NAVAIR recently surveyed the aviation commands to find out what ADP equipment is already out in the fleet and what the commands have that is compatible for Automated Communications Systems. This information will be put into the DMS data base and NCTC can work with this information to see if the transition can be tailored to utilize existing systems to cut the costs of the transition. [Ref. 19]

One of the methods that may be utilized to provide for money for GateGuards is that initially there would be seed money provided to implement GateGuard at some selected remote sites. These sites will be able to access a larger comm center's MMS via a dial-up circuit, and thus the local comm center can be closed down. With the cost savings provided by closing down the comm center, more GateGuard systems can be acquired and the process can occur again. This will continue until enough of the GateGuard systems are acquired and the manpower intensive NTCCs are closed, which is part of the overall DMS Transition Plan. [Ref. 20]

One of the problems that may be encountered during the transition to electronic transfer is that some commands may be reluctant to part with scarce funds to purchase components that are only transitional through the DMS phases. For instance the end-to-end encryption provided by STU-IIIs in the early phases is transitional since ultimately, connectivity will be provided when BITS with SDNS encryption is implemented at the bases [Ref. 4: p. 3-57].

d. Implementation of Gateguard

When the issue of how the funding will be provided for the acquisition of the DMS components required at the squadron level is decided, the individual commands can start the planning process of implementing the necessary components. When the decision is made by an individual command to

implement GateGuard, a message has to be submitted directly to COMNAVCOMTELCOM, N31, for GateGuard approval, stating that the command wishes to be a MMS subscriber [Ref. 18: p. 5]. The command also needs to contact the message center that will be providing the MMS services for coordination. COMNAVCOMTELCOM will respond with the procedures for obtaining the necessary equipment. The local message center will aid in the installation of the equipment, provide documentation and instructions, and will draw up a memorandum of understanding to be signed by the command and the message center. This memorandum is important in letting the command know what its responsibilities will be concerning the proper handling and distribution of message traffic. [Ref. 21]

Since the GateGuard will be providing the transfer of classified message traffic, it is suggested that the system be installed in the secure spaces of the COMM/CMS office. It is important that the COMM/CMS personnel are properly trained in the use of the system and that local and community wide SOPs are developed and disseminated to provide proper utilization. The connectivity with a LAN with automatic message handling capabilities for message distribution throughout the command will be explored in a later chapter. Without the installation of a LAN the COMM/CMS office will be responsible for the generation of hardcopy messages and distributed throughout the command in the same manner that is currently being done.

e. Other Transition Issues

One problem that still remains in the early phases of the DMS transition is that TOP SECRET messages will still have to be picked up over-the-counter in hard copy form until the Secure Data Network System (SDNS) with Message Security Protocol (MSP) is implemented during Phase II. As the phaseout out of the NTCCs continue, commands may have to send couriers farther distances to handle over-the-counter traffic. The commands that are still utilizing the over-the-counter diskette media face this problem as well. For instance, if NTCC Barbers Point, Hawaii, is phased out before squadrons are on board with electronic transfer then they may be forced to send their couriers to Camp Smith or Pearl Harbor for over-the-counter services.

IV. LOCAL AREA NETWORKS

To provide true writer-to-reader messaging at the squadron level, there has to be connectivity between the squadron GateGuard and the PC at the user's desk. A Multi-level Secure (MLS) Local Area Network (LAN) can provide this connectivity. However, the LAN must have a trusted Message Dissemination Subsystem (MDS) (see Ch. III, section 2) if messages are to be disseminated to members of the command with different classifications. Commodity contracts with a MLS operating system, secure LAN access, and a MLS Data Base Management System that provides proprietary tools for a MLS MDS, are not available today. To ensure availability of a non-proprietary MDS to all DoN organizations, a MLS MDS based on the Naval Research Lab (NRL) Secure Military Message System (SMMS) could be pursued [Ref. 4: pp. 3-87,3-88]. Until these capabilities become available, a squadron or command can still pursue the implementation of a LAN for use within the organization and provide direct connectivity to DMS when the necessary capabilities are available. The purpose of this chapter is to provide a brief overview of LANs and to explore a LAN planning strategy with reference to the new Navy PC-LAN contract.

A. DEFINITION

LANs can be defined as a collection of computers and peripherals connected by shared communications media that covers a limited geographical area, allowing workstations to communicate with other nodes to exchange computer data, word processing and several forms of electronic messaging [Ref. 10: p. 6].

1. Functional Guidelines

A LAN is typically owned and controlled by a single organization, allowing for configurations and decisions to be made based on the organization's requirements, it generally follows these functional guidelines [Ref. 22: pp. 15,16]:

- Ability to transmit data between two nodes without the use of complex routing algorithms and intermediate nodes to store-and-forward data.
- Provide communication between nodes separated by as much as six kilometers at a data rate of at least one Mbps.
- Easy modification after installation considers the addition and deletion of nodes while limiting the impact on the operation of the network.
- The nodes should be connected to the network in such a way that if one fails, the network as a whole is not affected; however, the function provided by the failing node may be lost temporarily.
- The network should be constructed to allow interface to other similar or different networks through the use of appropriate translation equipment.
- Features should be provided to facilitate network maintenance, diagnostics, and services.

2. Components

A LAN is generally composed of the following [Ref. 10: p. 7]:

- File Server: File Servers are dedicated computers, usually more powerful than the user computers, that serve the other nodes by providing a central data base, software applications and a coordination point for managing the network. There may exist one or more file servers depending on the needs of the organization.

- Mass Storage Devices: These devices are typically large capacity hard disks in or attached to the file server for the purpose of storing more data. A tape backup for small organizations is likely to be in order of 60 MB.

- Workstations: Intelligent workstations (PCs with memory) or dumb terminals (no memory) can number from 2 to 200 or more, depending on the size of the LAN or organizational needs.

- Network Interface Card (NIC): A NIC is installed in each computer as well as the file server. These NIC's, sometimes referred to as network boards have built-in functions, such as controlling inter-application communication, thus providing the logic for each type of LAN topology.

- Cables: The cables or transmission media, provide the connection between the NIC in the workstations and the file server. The most common types of cables are: twisted pair, coaxial, and fiber optics.

- Network Operating System (NOS): The network operating system is installed in each file server to control access to common shared areas and devices. The NOS enables the LAN manager to guard security by assigning access rights and is indispensable in organizing multi-user applications such as the database.

B. CHARACTERISTICS OF LAN'S

1. Transmission Media

There are a number of different types of transmission media that are used to provide the physical connectivity for a LAN. The type of transmission media that is chosen for a given LAN depends mainly on the organizational needs and the organizational budget constraints. The three most common types of transmission media are twisted pair, coaxial cable and fiber optics.

a. Twisted Pair

Twisted pair, in the form of twisted pairs of copper wire, has been used as a transmission medium for a long time. The telephone industry initially built its networks using this technology; however, other technologies are being utilized more often today due to the electrical characteristics of copper wire that introduce distortion that increase with speed and distance. Another disadvantage is the low data rate that twisted pair supports. [Ref. 10: p. 17]

The advantages of using twisted pair technology in LANs are [Ref. 10: p. 17,18]:

- Twisted pair is a well understood technology.
- Minimal skill levels are needed to connect devices.
- Twisted pair cabling can be less expensive.
- Many buildings already have twisted pair installed.

b. Coaxial

Coaxial cable is composed of one wire (a conductor) that carries the signal, surrounded by a metal mesh shield that acts as the ground. Both are protected with an insulating jacket. Coaxial comes in a wide variety of types and thicknesses. [Ref. 10: p. 18]

Some of the advantages of coaxial cable include [Ref. 22: p. 68]:

- supports both broadband (analog) and baseband (digital)
- high bandwidth capabilities
- more durable and immune to noise than copper wire
- uses off-the-shelf connectors
- simple installation and trouble shooting
- carries signal further than twisted pair without repeaters.

Some of the disadvantages of coaxial cable are [Ref. 22 p. 68]:

- can be difficult to bend
- not secure from tapping
- modems are required at each user station for broadband LANs.

c. Fiber Optics

Fiber optic cable is used for high speed, high capacity communication applications, and provides a

transmission medium that is free from noise and electrical interference. Fiber optic cable consists of fine strands of glass, silica, or plastic called the transmitting core, surrounded by a layer with lower refractivity called the cladding, that allows the light waves to reflect down the cable. Each fiber is usually covered by an opaque material jacket which keeps light out of the fiber and provides structural integrity. Environmental problems such as electrical noise and corrosion, that are inherent in twisted pair and coaxial, are not present in fiber cables. [Ref. 10: p.19]

Some of the advantages of fiber optics include [Ref. 22: p. 73]:

- small size and lightweight
- no emanations if properly shielded
- high data rate and large bandwidth
- low attenuation loss
- immune to interference (crosstalk and jamming)
- very low bit error rate
- secure, difficult to tap.

Some of the disadvantages of fiber optics are [Ref. 22: p. 73]:

- poor physical flexibility (multi-strand, bundled cable)
- expensive repeaters may be necessary

- difficult to add peripherals or work stations
- skilled installation and maintenance personnel required.

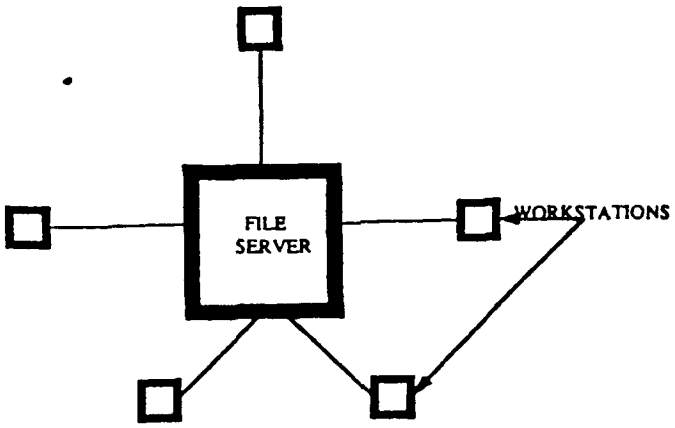
2. Topology

The topology of a LAN is the structure, consisting of paths and switches, providing the communications interconnections between nodes of a network. Network configurations are typically considered to be centralized or distributed. If the network is configured with all nodes connected to a single controlling node, then the network is considered to be centralized. If the nodes of the network are connected to other nodes and not to a single controlling node, then the network is considered to be distributed. Several considerations must be made when choosing the type of LAN topology. Some of these considerations are diagnostics, troubleshooting, bandwidth requirements and expansion capabilities. Some common LAN topologies are: star, ring, bus and hierarchical. Figure 14 [Ref. 10: pp. 10-14] depicts the common LAN topologies that will be discussed in this section. [Ref. 22: pp. 23,24]

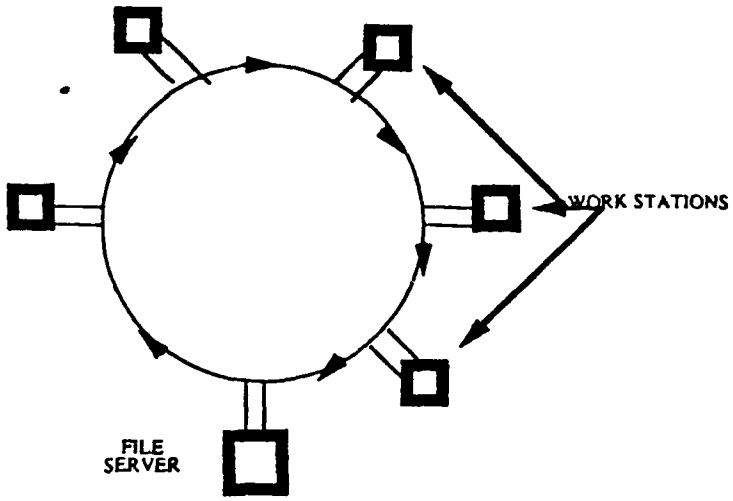
a. Star Topology

Star networks have all terminals connected to a central controlling intelligent computer, typically the file server. The central node acts as a switching device between all the connecting nodes and if the central node fails, the network cannot function. It is important to have reliable

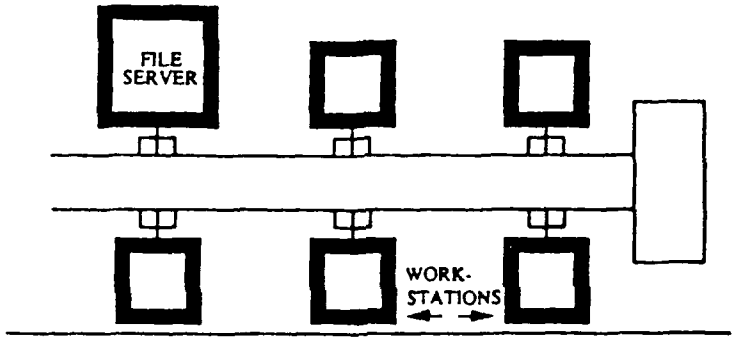
STAR TOPOLOGY



RING TOPOLOGY



BUS TOPOLOGY



TREE/HIERARCHICAL
TOPOLOGY

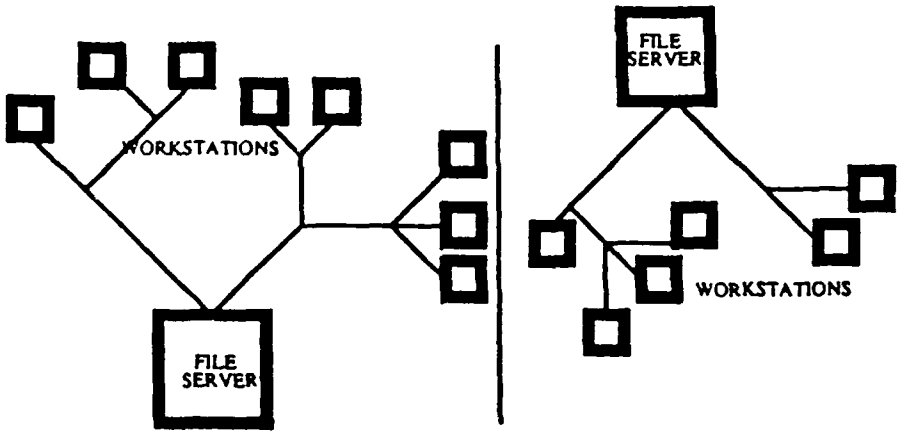


Figure 14. LAN Topologies.

backups to keep the network from shutting down should the central node fail. The star network is best suited for network requirements where the connecting nodes or workstations need access to the central file server more often than they need access to other workstations. This type of network allows for easy troubleshooting and high levels of security. [Ref. 22: pp. 25,26]

b. Ring Topology

In a ring topology, each node on the ring is connected to two other nodes on the ring. There is not a single node that has overall control or authority over the network. The ring consists of a series of repeaters or transceivers located at each node that act as the node's access point and receives the data and forwards it along the network.

Data flow is typically in one direction making the network design less complex, and the cost associated with installing this type of network is usually one of the lowest among the LAN topologies. Some of the problems with this type of network is that the network depends on the repeaters. If one repeater goes down then the flow of the network stops. It is also difficult to lengthen the ring to add new workstations. [Ref. 10: pp. 12,13]

c. Bus Topology

The bus topology is a single communications circuit that is shared by every connecting node and is the most commonly used topology. Each workstation uses the bus to communicate with every other workstation, however the circuit is not joined together to form a loop. In the bus topology, data is typically transmitted in both directions from the originating node. The other nodes on the network will check the message as it passes to determine if the message is intended for them. Bus topologies are best suited for environments with light or sporadic transmission of data. As use of the network increases, contention for the bus needs to be more carefully controlled. Reliability is usually higher for a bus topology due to the lack of having a single point that could fail and shut the network down. Expansion is also easily handled on this type of network. [Ref. 22: pp. 26,27]

d. Hierarchical Topology

The hierarchical or tree topology is basically a series of connections of buses. Typically this topology has a central or backbone bus that has a number of buses connected to it. The hierarchical topology is considered to be fully distributed with several layers evident in the network. The workstations that are used for remote devices have independent processing capabilities, using resources as needed from different levels. [Ref. 10: pp. 14,15]

3. Network Access/Protocols

Network access methods, or protocols, are the rules governing the format and meaning of the frames, packets or messages that nodes on a network must follow to be able to transmit data. Protocols will handle varying data rates, error detection and correction, and message format. Protocols can be grouped into two separate categories: contention and token passing. The contention protocol and token passing protocols that will be discussed in this section are the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) and the token ring/bus protocols.

a. Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

Using the CSMA/CD contention protocol, a node will first listen to the carrier on the channel to check if data is currently being transmitted. If the channel is clear, the node will attempt to transmit. If the circuit is busy, the node will wait a randomly generated amount of time to transmit After the transmission, if a collision occurs, the collision detection feature will pick this up and terminate the transmission. This will allow the channel to be cleared sooner, thus allowing nodes to attempt to access the channel earlier. If a collision occurs, the nodes that are involved wait different randomly generated amounts of time before attempting to retransmit their data. This reduces the

possibility of the same collision occurring again. [Ref. 22: pp. 33-35]

b. Token Ring/Bus Protocols

Token Ring/Bus protocols are considered to be collision free protocols, involving the transmission of a special control frame, or token, over the transmission channel. If a node on the network needs to transmit data, it must capture the token before it can transmit. When the node has possession of the token, it has a maximum amount of time (token hold time) to transmit its data before releasing the token for other nodes on the network. With the token ring protocol the token is passed to the adjacent node on the network which will pass it on to the next node or hold it if it has data to transmit. With the token bus protocol the node holding the token will pass it to its logical neighbor by specifically addressing that node. Logical neighbors may not necessarily be physically located next to each other. This type of protocol is best suited when there is a heavy transmission environment since all stations will be guaranteed the chance to transmit. [Ref. 22: pp. 36,37]

4. Examples of LANs

This section will look at two of the major types of LANs that exist in the market today, which are also supported by the Navy PC-LAN contract with Digital Equipment Corporation (PC-LAN will be discussed in a later section). The two types

of LANs that will be examined are Xerox's ETHERNET and the IBM TOKEN RING network.

a. ETHERNET

ETHERNET was developed at Xerox's Palo Alto Research Center in the early 1970s and is considered to be the first commercial LAN. The primary purpose of ETHERNET was to connect office workstations to other peripheral devices to facilitate the sharing of expensive devices throughout the organization. ETHERNET uses the bus or tree topology and typically uses coaxial cable as its transmission medium. The access method or protocol utilized by ETHERNET is the CSMA/CD contention protocol. The network was designed with the idea of simplicity in concept and operation so as to reduce the costs associated with the network. ETHERNET is suited best to environments where small portions of the total network traffic capacity is used, and where nodes typically transmit data in short bursts. If one workstation has long periods of continuous transmission the pattern of use in the network can be upset by keeping the network busy, thus blocking the access of other workstations to the network.

[Ref. 10: pp. 31,32]

b. IBM Token Ring

The token ring was first proposed in 1969 and the IEEE 802.5 standard that applies to token ring LANs was a result of research conducted by IBM and Texas Instruments. In

IBM's implementation of the Token Ring Network for PCs, the token ring logic and medium access control (MAC) is contained on the interface card that is inserted into the PC. The connection to the interface card is from a wiring concentrator that can be daisy chained to form a ring. The preferred transmission medium is the use of two 150-ohm shielded twisted pair wires, which is also recommended by the IEEE 802.5 standard. The token ring utilizes the collision free token passing protocol that circulates a token, or packet of control codes, around the ring in order for the nodes to capture it for transmission of data. The token ring network is best suited for use in environments where there are long periods of medium to high access rates. The maximum possible delay for a node to transmit can be computed because each node can only hold the token for a given period of time. This allows quick access to the network for higher priority users and critical information to be distributed in a timely manner. [Ref. 10: p. 33] , [Ref. 22: pp. 88,92]

C. LAN PLANNING STRATEGY

By properly developing and employing a LAN planning strategy, an organization can overcome many of the stumbling blocks that are inherent in trying to implement a new system in the DoD environment. LAN planning should not be confused with network design. The procurement process in the DoD can be a lengthy, and the person who fashioned the design for the

LAN may have left the command already when the parts arrive. If there is not sufficient documentation, the person who inherited the implementation of the LAN may not be able to make it work. Also, requirements may have changed, and the original intent for the LAN may have become vague. The following strategy for planning a LAN can help to overcome some of these problems. [Ref. 23: p 17]

1. Project Manager

The assignment of a project manager to determine what needs to be done to support implementation of the LAN is the first step of the plan. The project manager should: organize any support efforts such as network designers, cabling installers, facilities technicians, etc.; establish a plan of action and milestones; maintain documentation; and coordinate between technical personnel and users. [Ref. 23: p. 17]

2. Functional Study

The next step should involve conducting a functional study to determine how the command can and would utilize the network to conduct daily business. The personnel in supervisory roles should be interviewed first to determine project goals, how they currently use their PCs, and their expectations of the network. After determining the supervisor requirements, representatives from work groups who will be users of the LAN should be interviewed. Admin personnel and yeoman are good sources because they are familiar with the

command's correspondence and documentation requirements and will probably be heavy users of the network. The interviews should be documented in detail. They will provide expectations of the LAN, what kind of traffic to expect and where the traffic will be the heaviest. At the same time, the interviews will involve the users in the planning process, which will help break down barriers of resistance to the network. [Ref. 23: p. 17]

Some of the information that should be obtained from the interviews is [Ref. 23: p. 17]:

- what the the user's mission and functions will be
- who uses a PC and how much
- what software/hardware is currently in use
- what and how much paperwork is currently processed
- what processes are automated and what could be automated
- what the security requirements are
- with what other groups they communicate
- what the expectations are of network capabilities.

3. Requirements Analysis Report

Producing a requirements analysis report is the next important step. During this step the network requirements should be documented, project goals and constraints defined and the results of the functional study summarized. A detailed description of physical and data security

requirements should also be provided by this report, along with an itemized listing of project responsibilities. This report can be useful in determining what network application packages, network operating systems, and LAN architecture will be appropriate for the organization. [Ref. 23: p. 17]

4. Site Survey

Conducting a site survey to determine where network equipment will be placed, cabling distances, and availability of power sources is the final step before the actual design of the LAN. It is important that the site survey is properly documented with a detailed floor plan showing placement of equipment and how the cables will be run. [Ref. 23: p. 17]

Some of the other items that should be considered when conducting the site survey are [Ref. 23: p. 17]:

- adequate air conditioning and lighting
- adequate electrical power outlets
- adequate space and furnishings
- excessive dust, dirt and smoke
- sources of possible electromagnetic interference.

5. Network Configuration

After the functional study, requirements analysis report and site survey have been completed, the network design stage can begin. To make the design of the LAN much easier, a Navy PC-LAN contract can be utilized to aid in the

configuration and design of the LAN. The Navy PC-LAN contract was awarded on March 6, 1991, to Digital Equipment Corporation (DEC), and provides for three years of supplies and six years of services to support the integration of LANs within the Navy and other DoD activities. Table 1 provides a listing of supplies and services that are available under this contract. [Ref. 23: p. 20], [Ref. 24: p. iii]

To generate an order on this contract, a command can utilize three ordering tools to assist in developing a configuration and design for its LAN. These ordering tools are the PC-LAN catalog, the configurator, and the 800 number. The PC-LAN catalog provides a technical description of each part and service, pricing tables, guidelines on placing an order and a sample DD Form 1155. The configurator is an interactive software program that allows the user to plan a network for up to 25 users. For larger networks, it is recommended by DEC that the user purchase services to assist in the design of the network. The configurator software will recommend a topology specific to individual sites and cable plant components, and will be made available to procurement officers and users on request. For pre-sales and post-sales assistance regarding the Navy PC-LAN contract, a 800 number (1-800-NAVY-LAN) is available from 8 a.m. to 8 p.m. EST. Figure 15 depicts the order flow for supplies and services. [Ref. 24: pp. iv,v]

TABLE 1. PC-LAN CONTRACT SUPPLIES AND SERVICES

HARDWARE
- LAN Server (486-25)
- Monitors
- Laser Printers
- Tape Storage Device
- Disk Storage Device
- Memory
- Power Products
  - UPS
  - Power Converter
  - Shipboard Power Components
- Vertical Stand

SOFTWARE
- Network Operating Systems
- Application Server Operating System
- Calendar Scheduler
- E-Mail
- DBMS™
- MS-DOS®
- OS/2® Operating System
- C2 Secure NOS (Delayed Deliverable)
- Tape Backup Software

CONNECTIVITY
- Ethernet Cards
- Token Ring Cards
- Bridges
- Modems
- Connectors
- Cables

COMMUNICATIONS
- Gateways
- TCP/IP
- Asynchronous Communications
- GOSIP (Delayed Deliverable)
- Asynchronous Expansion
- Dial-In/Out Software

SERVICES
- Network Consulting
- Database Consulting
- Training
- Site Survey
- Installation
- Maintenance
- Spares

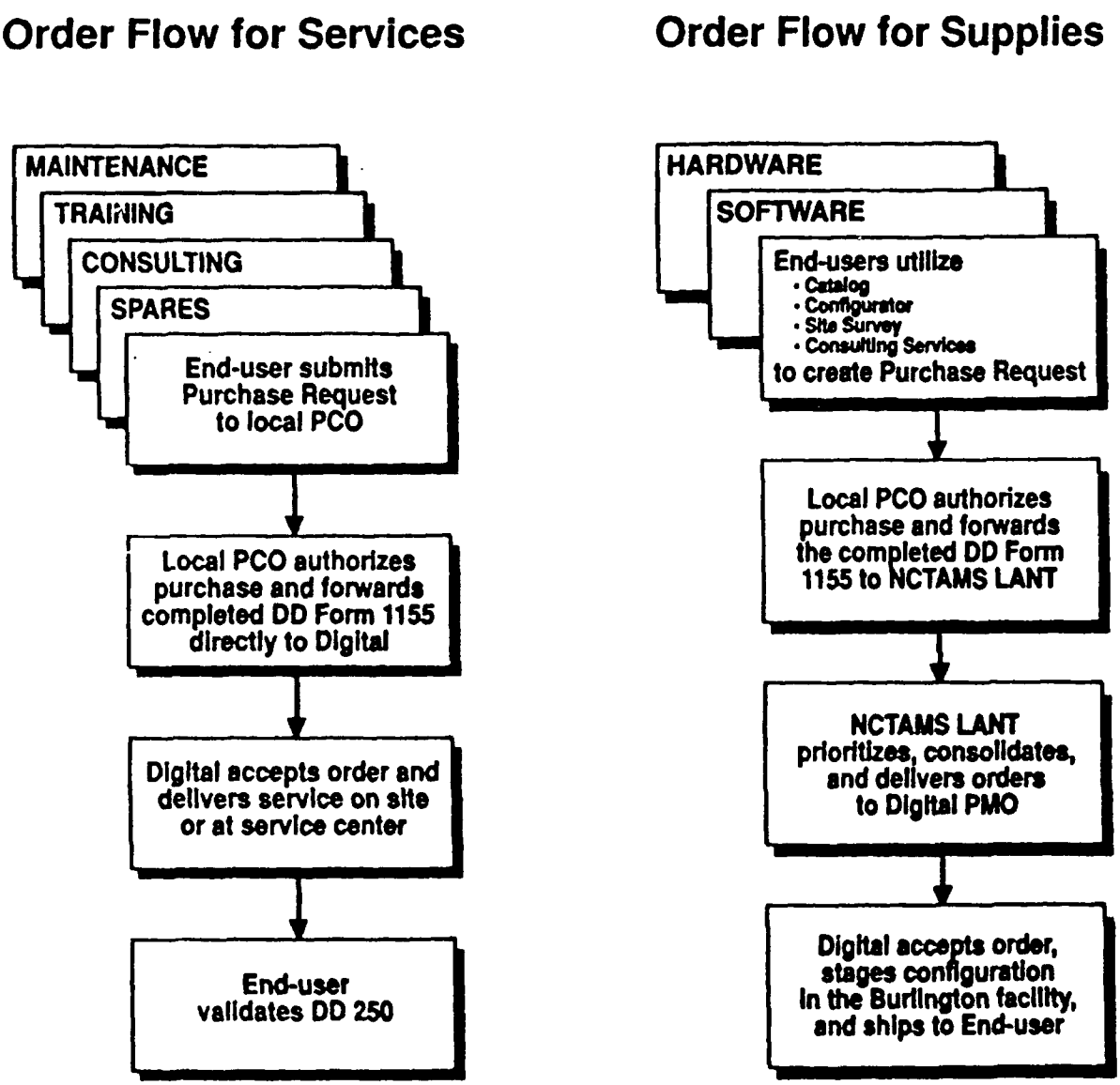


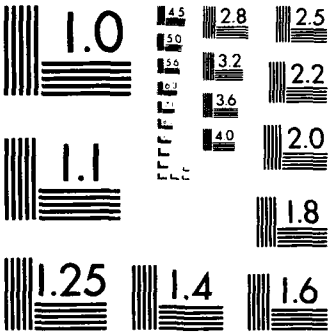
Figure 15. Order Flow for Supplies and Services.

6. LAN Management

One of the areas that is typically neglected in the planning for a LAN is that of LAN management. It should be decided at the beginning of the planning process how the LAN will be managed. The LAN managers should be selected and trained before the network goes into operation. LAN management is traditionally divided into three levels: LAN Administrator, Network Manager, and LAN manager. LAN Administrators establish and maintain network user information, directories and access rights for local users. They schedule and conduct regular backups of all files. Typically there is one LAN Administrator for every file server on the network. The Network Manager will monitor the entire network; installing the operating system, establishing the user environment and setting up the network printing. For small networks, the LAN Administrator and the Network Manager are the same person. For large interconnected networks with diverse LAN applications, there is typically a LAN Manager to provide overall management functions. The key to LAN management, no matter the size of the network, is to identify the management functions that are required prior to implementing the LAN and to put the right people in place to handle these duties. [Ref. 23: p. 18]

AD-A252 934 P-3 SQUADRON TRANSITION TO THE DEFENSE MESSAGE SYSTEM (DMS)(U) NAVAL POSTGRADUATE SCHOOL MONTEREY CA M S FOLDY MAR 92 XN-NPS 2/2

UNCLASSIFIED NL



7. Training

Another important aspect of LAN planning that is sometimes overlooked is user training. It should be determined early who needs to be trained to utilize the system. Key people such as supervisors, administrative personnel and any other personnel identified as prospective heavy users of the system should be involved in a training program at the outset. Acceptance of the system relies on a proper training program. If the users are poorly trained to use the system, they will not feel comfortable with it and will not use it. All the planning efforts will be wasted and the network will sit idle. The Navy PC-LAN contract provides a number of training courses that can be utilized by organization personnel to learn to operate the system effectively. Figure 16 [Ref. 24: p. 44] depicts the various PC-LAN training courses that are available. [Ref. 23: p. 18]

PC LAN Training Curriculum

This map provides recommended training paths for individuals performing these six job functions. Point of entry is determined by experience or previous training.

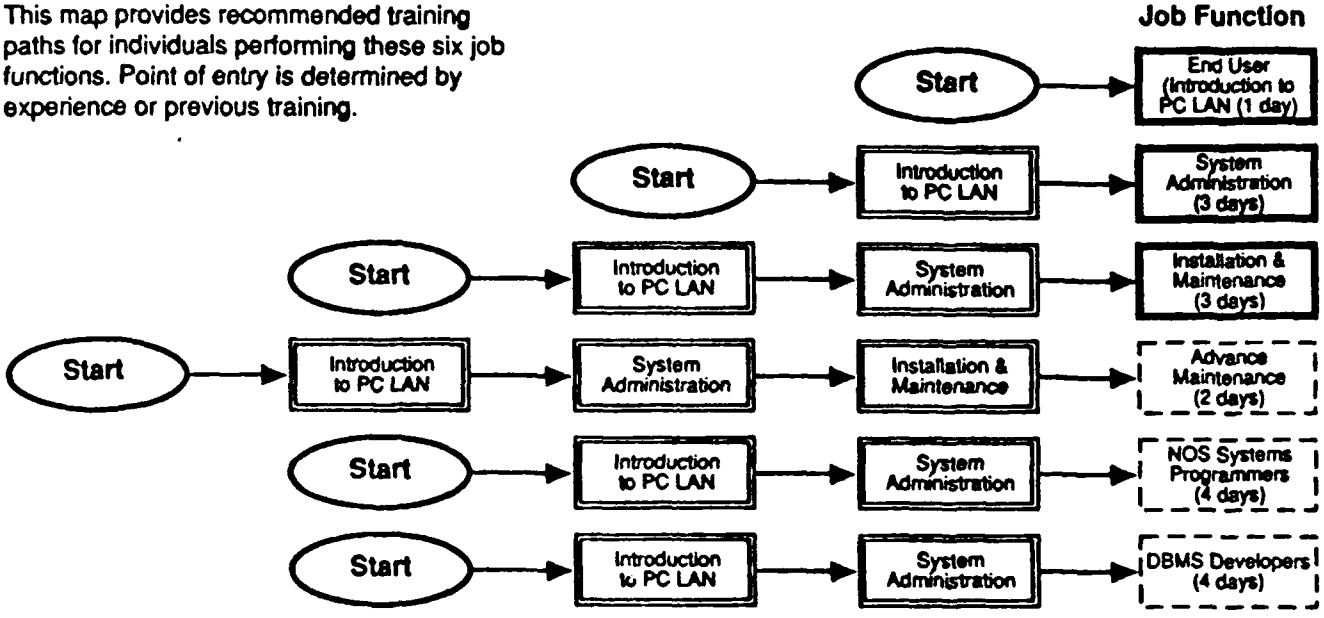


Figure 16. PC-LAN Training Curriculum.

V. SUMMARY AND CONCLUSIONS

A. SUMMARY

The current messaging system that the P-3 community has been using for the last few decades was discussed in detail. Both the internal and external message processing environments were explored to identify how a typical squadron currently processes messages. This was done to establish a base of knowledge for the reader to see where a squadron and the DoD is and has been in terms of message processing. This was established as the baseline architecture for the Defense Message System (DMS). The DMS was then addressed, with descriptions provided of the Phase concept that is evident in the transition plan. Major DMS components such as GateGuard and Multi Level Mailserver (MMS) were described, and the methods of implementation were examined. The DMS transition issues that will affect the P-3 community were then investigated, looking at issues such as the transition to diskette media and the implementation of GateGuard. The need to implement a Local Area Network (LAN) to provide connectivity between the messaging system and the desktops of users was then discussed. A basic overview of LANs was provided, looking at LAN topologies, transmission media, and access methods/protocols. A LAN planning strategy was then

explored that touched on items such as naming a project manager, conducting a functional study, producing an analysis report, designing a network configuration with the aid of the Navy PC-LAN contract, LAN management, and LAN training.

B. CONCLUSIONS

1. Current Messaging System

The messaging system that the DoD has been using for the last few decades is on its way out. The implementation of the Defense Message System (DMS) will eventually alleviate the problems that have been evident in the current system, such as the electronic connectivity gap that exists between the user commands and the telecommunication centers. Obsolete equipment will be phased out, the manpower intensive message centers will eventually be closed, and the longhaul AUTODIN system will be replaced by a fully integrated ISDN network. However, it is important that there is good understanding of the current message processing environment so that as the transition proceeds, the squadrons are sure that the messaging requirements and standards that are currently being adhered to are met, as well meeting the new requirements and standards that will be needed as new systems come onboard.

2. DMS Transition

The implementation of the DMS for the P-3 community at the squadron level is underway. The transition to diskette media vice DD-173 forms is the first tangible step that the

squadrons have experienced in the DMS implementation. This step alone does not drastically change the way in which the squadrons have been processing messages for the last decade. As the transition to DMS continues in Phase I and on into Phase II, there will be more evident changes as the squadrons get closer to true writer-to-reader message processing. This will occur as GateGuard systems are implemented at the squadron level and MMS systems are implemented at the message centers to allow for dial-up connectivity between the squadrons and the messaging system.

At the squadron level, it is recommended that a point of contact for DMS be established. This individual should become the squadron expert on the transition to DMS and how it will affect the way that the squadron handles message processing. He/she should track the progress of the transition both DoD wide and in the P-3 community. Important issues such as procurement for DMS components like GateGuard need to be followed, requiring regular contact with higher levels in the P-3 community and with DMS points of contact at NCTC to ensure that the squadron efficiently and effectively comes onboard with the systems as they become available. This individual should also be aware of the DMS transition status of the possible sites which the squadron may deploy to, so that the squadron will know what messaging services to expect and what equipment needs to be brought on deployment to ensure messaging needs are met.

3. Local Area Networks

As the systems required to provide a multi-level secure LAN become available, the squadron can transition to true writer-to-reader messaging. A plan should be in place to design and implement LANs throughout the community to make this possible. It is suggested that a LAN planning strategy similar to the one presented in the previous chapter be utilized. The assignment of a project manager from the wing level would be preferable. This individual could coordinate the design of LANs for the squadrons assigned to his/her wing. The squadrons are typically located in the same hangers or in hangers in close proximity. The cabling and functional requirements will be similar for the squadrons in the same wing, thus the standardization of LANs will be made easier. This will allow for economies of scale for procurement and will make more feasible the future expansion to a wide area network throughout the wing. Each squadron should assign an individual who will take on LAN management responsibilities and work in conjunction with the wing project manager for planning, design and implementation.

One of the most important roadblocks facing the implementation of LANs is the constant budget constraints that are apparent throughout DoD. The major changes in the world geopolitical situation in recent years have produced great uncertainty in the P-3 community as well as DoD-wide. The P-3 community is bracing for some deep cuts with projections of

the community going from having 24 operational squadrons that were evident during the cold war, down to as low as 12 by 1995. Thus, money being made available for ADP equipment is hard to come by. However, the decommissioning of squadrons will free up existing ADP equipment that is currently in the fleet. This equipment can be used subsequently to outfit the remaining squadrons to ease the cost of implementation of a LAN.

4. Final Remarks

The Defense Message System is in the very early stages of its implementation, and the transition plan is considered to be a living document with changes that have already taken place and changes that will take place. With the DoD going through one of its greatest periods of uncertainty and change in recent decades, it is inevitable that the DMS will evolve to a system that may look different from current expectations in terms of architecture and transition time frame. It is up to the organizations that have stakes in the development of this system to stay abreast of the changes and be flexible enough to manage these changes.

APPENDIX A. ACRONYMS

AIS	Automatic Information System
AMHS	Automatic Message Handling System
ASC	Automated Switching Center
ASCOMM	Anti Submarine Support Communications Center
ASD	Assistant Secretary of Defense
AST	AUTODIN Subscriber Terminal
AUTODIN	Automatic Digital Network
BITS	Base Information Transfer System
BIU	Bus Interface Unit
CD	Collision Detection
CSMD	Carrier Source Routing File
CSRF	Common Source Routing File
CSS	Communications Support System
CUDIXS	Common User Digital Information Exchange System
DCS	Defense Communications System
DDN	Defense Data Network
DMS	Defense Message System
DMSWG	Defense Message System Working Group
DSNET	Defense Secure Network
DUA	Directory User Agent
E-MAIL	Electronic Mail

FLTCINCS	Fleet Commanders in Chiefs
GENSER	General Service
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LDMX	Local Digital Message Exchange
MDL	Message Dissemination Link
MDS	Message Dissemination Subsystem
MDU	Message Dissemination Utility
MLS	Muli-Level Secure
MMS	Multi-Level Mail Server
MS	Message Store
MSP	Message Security Protocol
MTA	Message Transfer Agent
MTF	Message Text Format
NAVCOMMAREA	Naval Communication Area
NAVCOMMDET	Naval Communication Detachment
NAVCOMMPARS	Naval Communication Processing and Routing System
NAVCOMMU	Naval Communication Unit
NCTAMS	Naval Computer and Telecommunications Area Master Station
NCTS	Naval Computer and Telecommunications Station
NIC	Network Information Center
NMC	Network Management Center
NOS	Network Operating System

NRL	Naval Research Lab
NSA	National Security Agency
NTCC	Naval Telecommunication Center
NTS	Naval Telecommunications System
OAS	Office Automation System
OCRE	Optical Character Reader Equipement
OUA	Organizational User Agent
PCMT	Personal Computer Message Terminal
PLA	Plain Language Addressee
RI	Routing Indicator
RIXT	Remote Information Exchange Terminal
RTS	Remote Terminal System
SACS	STU-III Access Control System
SCI	Sensitive Compartmented Information
SDNS	Secure Data Network System
SMSCRC	Small Computer Requirements Contract
SRT	Standard Remote Terminal
STU-III	Secure Telephone Unit Model III
TAC	Terminal Access Controller
TAIS	Target Architecture and Implementation Strategy
TCC	Telecommunications Center
UA	User Agent
WWMCCS	Worldwide Military Command and Control System

LIST OF REFERENCES

1. Sampson, Rita L., *Naval Communications Area Master Stations: An Introductory Text*, Master's Thesis, Naval Postgraduate School, Monterey, CA, March 1989.

2. Babb, Robin M., *The Naval Telecommunications System: A Command and Staff Manual*, Master's Thesis, Naval Postgraduate School, Monterey, CA, March 1987.

3. Weigand, John F., *A Proposed Message System Architecture for a Marine Corps Base Implementation of the Defense Message System (DMS)*, Master's Thesis, Naval Postgraduate School, Monterey, CA, March 1990.

4. Naval Telecommunications Automation Support Center, *Department of the Navy Defense Message System Transition Plan*, Draft, January 1991.

5. Naval Education and Training Command, *Radioman 3 & 2*, August 1986.

6. Naval Telecommunications Automation Support Center, *AUTODIN/NAVCOMPARS Message Routing and Distribution*, NAVTASC Document No. 15X7001 TN-02B, November 1986.

7. Defense Message System Architecture Working Group, *The Defense Message System (DMS) Target Architecture and Implementation Strategy (TAIS)*, Command, Control, Communications and Intelligence (Information Systems), Washington, DC, October 1990.

8. Boutacoff, D. A., "DDN Evolves to Meet Interoperability, Security Needs," *Defense Electronics*, April 1986.

9. Eberhardt, Jean M., *Defense Data Network and the Naval Security Group*, Master's Thesis, Naval Postgraduate School, Monterey, CA, March 1988.

10. Mason, Laura E., *Requirements Specifications for Standardized Local Area Networks and Applications for Naval Aviation Squadrons*, Master's Thesis, Naval Postgraduate School, Monterey, CA, September 1989.

11. Patrol Squadron 40, *Communications Standard Operating Procedures*, Moffett Field, NAS, CA, March 1988.

12. Naval Computer and Telecommunications Command, *DoN Defense Message System*, Newsletter No. 1, April 1991.

13. Ball, E., "LAN Bridges", *Computer Communications*, pp. 115-117, June 1988.

14. Naval Data Automation Command, *Navy Base Information Transfer System (BITS) Sub Architecture*, 7 July 1989.

15. CNO Washington D.C., OP-094, Naval Message, Subject: Mandatory Elimination of DD-173 Message Forms, 062317Z Dec 91.

16. Naval Telecommunications Publication, 3(H), Annex D, *Procedures for Preparing/Handling Messages on Diskette*, January 1991.

17. Telephone conversation between LT Lisa Pardini, NTCC, Barbers Point NAS, HI, and the author, 10 Feburary 1992.

18. Naval Computer and Telecommunications Command, *DoN Defense Message System*, Newsletter No. 2, September 1991.

19. Telephone conversation between LT Rob Toole, NTCC, Moffett Field NAS, CA, and the author, 2 March 1992.

20. Telephone conversation between Mr. George Hill, Naval Computer and Telecommunications Command, Washington, DC, and the author, 2 March 1992.

21. Telephone conversation between LT Barber, NCTS, Jacksonville NAS, FL, and the author, 24 Feburary 1992.

22. Hunninghake, David Patrick, and Ashley, Bradley Keith, *Architecture Selection for Deployable Local Area Networks*, Master's Thesis, Naval Postgraduate School, Monterey, CA, March 1990.

23. Stanley, Barb, "LAN Planning Strategy", *CHIPS*, September 1991.

24. Digital Equipment Corporation, *PC-LAN Contract Catalog*, June 1991.

INITIAL DISTRIBUTION LIST

		No.Copies
1.	Defense Technical Information Center Cameron Station Alexandria, VA, 22304-6154	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, CA, 93943-5002	2
3.	Administrative Science Department Naval Postgraduate School Attn: CDR Allan W. Tulloch, Code AS/Tu Monterey, CA, 93943-5000	1
4.	Administrative Science Department Naval Postgraduate School Attn: Professor Dan C. Boger, Code AS/Bo Monterey, CA, 93943-5000	2
5.	LT Mark S. Foldy 1304 Warner Hall Dr. Virginia Beach, VA, 23454	2