

NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA



THESIS

**IMPLEMENTING A LAN THAT INTERFACES
WITH THE DMS AND USES MISSI**

by

Lawrence J. Brachfeld

March, 1996

Thesis Advisors:

Rex Buddenberg
Gus Lott

Approved for public release; distribution is unlimited.

19960520 024

DTIC QUALITY INSPECTED 1

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE March 1996.		3. REPORT TYPE AND DATES COVERED Master's Thesis
4. TITLE AND SUBTITLE IMPLEMENTING A LAN THAT INTERFACES WITH THE DMS AND USES MISSI			5. FUNDING NUMBERS	
6. AUTHOR(S) Brachfeld, Lawrence, J.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES 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 U.S. Government.				
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) The Defense Message System (DMS) is being implemented throughout the Department of Defense and will replace AUTODIN for individual and organizational messages by the year 2000. The Naval Security Group Detachment, Monterey and any other command that sends or receives organizational or individual messages must be ready to implement DMS on their Local Area Network. This thesis fully describes the Defense Messaging System standards and components and details what needs to be implemented in a Local Area Network in order to be prepared for the initial operating capability of the DMS, scheduled for July, 1996.				
14. SUBJECT TERMS Local Area Network, DMS, MISSI, Firewall, Security .			15. NUMBER OF PAGES 74	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18 298-102

Approved for public release; distribution is unlimited.

**IMPLEMENTING A LAN THAT INTERFACES WITH THE DMS AND
USES MISSI**

Lawrence J. Brachfeld
Lieutenant, United States Navy
B.S., Rensselaer Polytechnic Institute, 1988

Submitted in partial fulfillment
of the requirements for the degree of

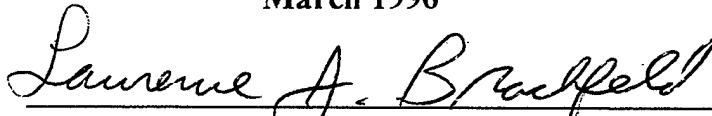
**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
MANAGEMENT**

from the

NAVAL POSTGRADUATE SCHOOL

March 1996

Author:

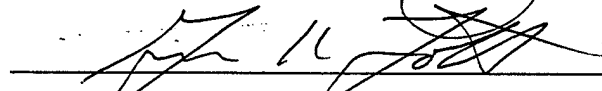


Lawrence J. Brachfeld

Approved by:



Rex Buddenberg, Thesis Advisor



Gus Lott, Thesis Advisor



Reuben T. Harris, Chairman,
Department of Systems Management

ABSTRACT

The Defense Message System (DMS) is being implemented throughout the Department of Defense and will replace AUTODIN for individual and organizational messages by the year 2000. The Naval Security Group Detachment, Monterey and any other command that sends or receives organizational or individual messages must be ready to implement DMS on their Local Area Network. This thesis fully describes the Defense Messaging System standards and components and details what needs to be implemented in a Local Area Network in order to be prepared for the initial operating capability of the DMS, scheduled for July, 1996.

TABLE OF CONTENTS

I. INTRODUCTION	1
A. INTRODUCTION	1
B. WHAT IS A SECURE LOCAL AREA NETWORK	3
1. Data Security	3
2. Securing the Transmission Channels	4
C. CONCERNS FOR ALLOWING TOP SECRET (TS) AND SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION ON THE SAME NETWORK	4
D. DISCUSSION OF OSI REFERENCE MODEL	5
E. DISCUSSION OF MESSAGING SERVICES	6
1. X.400 Messaging Service	6
2. SMTP/MIME/MOSS Messaging Service	7
F. DISCUSSION OF X.500 DIRECTORY SERVICES	7
II. MESSAGE SYSTEMS	9
A. MESSAGE SYSTEMS BACKGROUND	9
1. Description of SMTP/MIME/MOSS	9
2. History of SMTP/MIME/MOSS	9
3. Present Status of SMTP/MIME/MOSS	10
4. Future of SMTP/MIME/MOSS	10

B.	DMS OVERVIEW	11
1.	Description of DMS	11
a.	History of DMS	11
b.	Present Status of DMS	13
c.	Future of DMS	13
2.	Implementation Requirements for DMS	14
a.	DMS User Components	14
	(1) User Agent.	14
	(2) Message Store.	18
	(3) Directory User Agent.	20
	(4) Profiling User Agent.	20
b.	DMS Infrastructure Components	22
	(1) Message Transfer Agent.	22
	(2) Mail List Agent.	22
	(3) Multi-Function Interpreter.	24
	(4) Management Workstation.	24
	(5) Certification Authority Workstation.	25
	(6) Administrative Directory User Agent.	27
	(7) Directory System Agent.	27
c.	Hardware and Software Installation	27
III.	SECURITY SYSTEMS	29

A.	SECURITY SYSTEMS BACKGROUND	29
1.	Description of MISSI	29
a.	History of MISSI	30
b.	Present Status of MISSI	30
c.	Future of MISSI	32
2.	MISSI Building Block Products	33
a.	Cryptographic Cards	33
b.	Cryptographic Card Applications	33
c.	Secure Computing	34
d.	Secure Servers	34
e.	In-Line Network Encryptors	36
f.	Network Security Management	38
3.	Commercial Equivalents of MISSI	38
a.	Firewalls	38
b.	Public Key Cryptography	39
c.	Kerberos	39
B.	Advantage of MISSI Over Commercial Products	39
IV.	PROPOSED IMPLEMENTATION	41
A.	DESCRIPTION OF FALCONLAN	41
B.	INSTALLATION OF THE DMS COMPONENTS WITH FALCONLAN	47

1.	Basic Functionality Implementation	48
2.	Full Functionality Implementation	50
C.	INSTALLATION OF MISSI COMPONENTS WITH FALCONLAN	51
V.	RECOMMENDATIONS AND CONCLUSIONS	53
A.	RECOMMENDATIONS TO PROGRAM MANAGERS FOR SYSTEM MATURATION	53
B.	AREAS FOR FURTHER STUDY	53
C.	CLOSING REMARKS	53
	APPENDIX. ACRONYMS	55
	LIST OF REFERENCES	59
	INITIAL DISTRIBUTION LIST	61

LIST OF FIGURES

Figure 1. Why DMS? "From DMS Expo 95"	2
Figure 2. DMS Functions and Components "From DMS Expo 95"	15
Figure 3. DMS Architecture "From DMS Expo 95"	16
Figure 4. DMS Message Handling Environment "From DMS Expo 95"	19
Figure 5. DMS Message Store "From DMS Expo 95"	21
Figure 6. DMS Mail List Agent "From DMS Expo 95"	23
Figure 7. DMS Multi-Function Interpreter "From DMS Expo 95"	26
Figure 8. MISSI Fortezza Implementation "From DMS Expo 95"	31
Figure 9. Secure Network Server (SNS)	35
Figure 10. In-Line Network Encryptor (INE)	37
Figure 11. Building 629A Layout "From NISE East"	43
Figure 12. Building 616 Layout "From NISE East"	44
Figure 13. FalconLan Layout "From NISE East"	45
Figure 14. Bus Topology	46

I. INTRODUCTION

A. INTRODUCTION

As the Department of Defense (DoD) migrates away from all defense legacy messaging systems (e.g., Automatic Digital Network (AUTODIN) and proprietary e-mail systems) the Defense Message System (DMS) will be the single, seamless, end-to-end global electronic messaging service that meets the future DoD messaging requirements. The DMS supports new advances in technology that allow for the exchange of multimedia messages and attachments. The DMS provides a template for evolving with future technical advances. The full operational capability for DMS is targeted for the year 2000, when AUTODIN is phased out and all organizational and individual messaging in DoD is supported by DMS alone. The DMS is based on international standards consistent with Secretary of Defense guidelines to avoid unique military specifications whenever possible. The DoD intention is that the DMS will be implemented in all environments (e.g., strategic, tactical, fixed, and mobile.) This messaging service is a critical component of the Defense Information Infrastructure (DII) and supports command and control, administrative, and intelligence information exchange to enhance readiness and war fighting capabilities (Paige, 1995). Figure 1 summarizes the need for the DMS. Consider a U.S. Army infantryman in the field with a pair of binoculars waiting for the exact moment to contact the nearest U.S. or Allied aircraft carrier and have them launch their on deck alert strike package. As the DMS is implemented throughout the DoD on various computer networks, it is vital that the meaning of a secure local area network be understood. It is equally important to know what the DMS is and what it is not. This thesis will make it clear how the DMS can be implemented in a local area network using the



Why DMS?

- We must posture for the 21st century
 - Modern msg system is mandatory to provide:
 - Guaranteed timely delivery
 - Authentication of sender & receiver
 - End-to-end security
- AUTODIN can't support today's warfighter needs
 - Antiquated 1960's technology
 - Falling behind the Ops Tempo of the 1990's and beyond
- DMS promises interoperability for Joint & Coalition warfare



The message must get through! We can't stand the consequences if it doesn't!!!

Figure 1. Why DMS? "From DMS Expo 95"

National Security Agency's (NSA) Multilevel Information Systems Security Initiative (MISSI) to provide secure communications over untrusted networks.

B. WHAT IS A SECURE LOCAL AREA NETWORK

"We are at risk."

So begins a report of the National Research Council, a research arm of the National Academy of Sciences, on the subject of computer security chaired by Dr. David D. Clark of MIT (Malamud, 1992). According to the National Computer Security Center (NCSC) network security is defined as follows:

Network security is the protection of networks and their services from unauthorized modification, destruction, or disclosure, and providing an assurance that the network performs its critical functions correctly with no harmful side-effects. It also includes providing for information accuracy (NCSC, 1987).

A network needs a security infrastructure. Within the confines of work groups, the structure may be fairly loose, but will guard against unauthorized intrusions from other work groups. A work group is defined as a group of people brought together and assigned to perform a specific task on their own isolated network as a work group network. Even in the broad confines of the Internet, security is becoming increasingly important. Episodes like the Morris worm, a 1988 worm that was able to paralyze the Internet for several days, not only exhibit the vulnerability of networks, but draw the attention of policy makers to the limitations of networks (Malamud, 1992). The network security problem can be divided into two components.

1. Data Security

The requirements for data security are: confidentiality, authentication, integrity, and

access control. Although encryption is an integral part of data security, it does not solve all the computer security problems by itself. Some of the tools required to ensure data security are either the DMS or Simple Mail Transfer Protocol (SMTP)/Multipurpose Internet Mail Extension(MIME)/Mime Object Security Service (MOSS) products. Confidentiality ensures that information is not made available to unauthorized individuals, entities, or processes. Authentication provides for the verified identity of a communications peer entity. Integrity protects against unauthorized modification, insertion, or deletion. Access control allows only authorized users to send or receive messages or data.

2. Securing the Transmission Channels

The requirements for securing the transmission channels are: denial of service, traffic analysis, and availability. The tools required to ensure transmission channel security are correctly implemented link end to end encryption, network management, and traffic flow confidentiality.

C. CONCERNS FOR ALLOWING TOP SECRET (TS) AND SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION ON THE SAME NETWORK

In a multilevel security network, two or more people with different levels of security clearance wish to have access to the network. This imposes a hierarchy of security levels on the network. A multilevel secure network must preserve the Bell-LaPadula properties of access to data (Pfleeger, 1989):

1. The *simple security property* states that no user may read data at a higher level than that for which a person is authorized.
2. The *star property* states that no person may write data to a level lower than that person has accessed.

We can see that meeting these two properties is a very difficult task, especially for personnel with higher security levels, because once they have accessed data at a higher level, they cannot write to a lower level. A possible solution to this problem is to form a trusted network base, called the trusted network interface that can communicate with all levels of security classifications.

D. DISCUSSION OF OSI REFERENCE MODEL

The Open Systems Interconnection (OSI) seven layer model is the plan by which communications software is designed. The widely implemented OSI model facilitates control, analysis, upgradability, replacement, and management of the resources that constitute the communication network. It also makes it much easier to develop software and hardware that link incompatible networks because protocols can be dealt with one layer at a time (Fitzgerald, 1993). The OSI model serves as a framework around which a series of standard protocols are defined (Fitzgerald, 1993). The OSI model handles the transmission of a message from one terminal or application program to another distant terminal or application program. A description of the OSI reference model layers follows:

- Layer 1: The physical layer is primarily concerned with the transmission of the data bits over the communications circuit. This layer concerns hardware, whereas layers two through seven concern software.
- Layer 2: The data link layer manages the basic transmission circuit established in layer one and transforms it into a circuit that is free of transmission errors.
- Layer 3: The network layer provides for the functions of internal network operations such as addressing and routing. This is sometimes referred to as the packet switching network function (Fitzgerald, 1993).
- Layer 4: The transport layer establishes, maintains, and terminates logical

connections for the transfer of data between end users.

- Layer 5: The session layer is responsible for initiating, maintaining, and terminating each logical session between end users as well as managing and structuring all sessions.
- Layer 6: The presentation layer carries out a set of message transformations and formatting to present data to the end users.
- Layer 7: The application layer is the end user's access to the network.

E. DISCUSSION OF MESSAGING SERVICES

A Message Handling Service (MHS) is used to transmit electronic messages through communication systems from the writer to the reader.

1. X.400 Messaging Service

The X.400 standard defines message handling for electronic mail in the OSI environment, while Unix to Unix Communication Protocol (UUCP) defines message handling in the Unix environment. X.400 operates at layers six and seven of the OSI Reference Model. X.400 defines User Agents (UAs) and Message Transfer Agents (MTAs) along with the names and addresses required for an electronic mail system. Each user has a mail agent which is their UA. This UA allows the person using the system to type a message, include the recipient's address and also receive incoming messages. The interface between two UAs is accomplished by an MTA that takes a message from a sender's UA and delivers it to the UA to which it is addressed (Fitzgerald, 1993).

X.400 also defines a private and a public domain. When an organization's private domain is connected to the common carrier's public domain, E-mail messages can be addressed on a worldwide basis. A prime example of the commercial use of the X.400

standard is in AT&T's EasyLink Service. This service provides global public messaging that allows customers the flexibility of communicating with virtually anyone in the world, anytime, and anywhere (<http://www.nafta.net/attels.html>).

2. SMTP/MIME/MOSS Messaging Service

While X.400 is the standard for use with the OSI model, SMTP is the standard for use with Transmission Control Protocol/Internet Protocol (TCP/IP) networks. Currently, the DMS is designed with a Multi-Function Interpreter (MFI) to act as a gateway for SMTP and non-X.400 compliant domains. Within the DoD there are approximately twenty different e-mail products being used, including X.400, SMTP, and a variety of other proprietary protocols (MITRE Study, 1992). Each system requires a messaging gateway to translate to a common protocol so that messages can be exchanged between various proprietary groups, SMTP is used for this purpose. When Multipurpose Internet Mail Extension (MIME) and MIME Object Security Services (MOSS) are added to SMTP, it makes a very powerful standard that rivals X.400. MOSS is a protocol that uses public key cryptography to apply end-to-end encryption from the writer to the reader.

F. DISCUSSION OF X.500 DIRECTORY SERVICES

X.500 is the directory service standard for OSI networks, it is the interface between the users and the directory. The primary purpose of the X.500 standard is to provide a worldwide directory for obtaining addresses to facilitate sending electronic messages throughout any public or private domain E-mail system (Fitzgerald, 1993). The X.500 standard defines the directory of users so the proper address can be obtained in order to send E-mail messages (Fitzgerald, 1993). All that the writer must do is access the directory and

address the message to the desired reader. The directory will physically fill out the network addresses of the reader that the writer wishes to send the message to.

II. MESSAGE SYSTEMS

A. MESSAGE SYSTEMS BACKGROUND

When the DMS was conceived in 1988, there were two primary e-mail alternatives available:

1. SMTP
2. X.400

SMTP will be described in the following section and X.400 will be discussed as the DMS is described.

1. Description of SMTP/MIME/MOSS

The objective of the Simple Mail Transfer Protocol (SMTP) is to transfer mail reliably and efficiently.

2. History of SMTP/MIME/MOSS

SMTP is independent of the particular transmission subsystem and requires only a reliable, ordered data stream channel. The SMTP model was designed with the SMTP standards of 1982 and it was only capable of handling ASCII text in the message body and therefore did not meet the DoD requirements specified in Multicommand Required Operational Capability (MROC) 3-88 for the DMS. MROC 3-88 is the source document for the system requirements and architectural guidelines of the DMS. As we will see with the addition of MIME and MOSS, this standard rivals the X.400.

3. Present Status of SMTP/MIME/MOSS

In 1992, RFC-1341, which defines Multipurpose Internet Mail Extensions (MIME), was published by a group of people who had become disenchanted with X.400 because it was taking too long to implement it in any products. MIME defines a standard method for extending the capabilities of SMTP to allow items other than ASCII text, such as images, sound, postscript, etc. to be present in the body of the message. Although MIME itself does not provide any security, there is a movement to MOSS, which is a derivative of privacy enhanced mail (PEM) and is a proposed Internet standard for adding security services such as confidentiality, integrity, and authenticity to SMTP/MIME. PEM defines message encryption and authentication procedures for text based electronic mail messages using a certificate based key management mechanism.

4. Future of SMTP/MIME/MOSS

As the WWW continues to pervade all industries worldwide and more browsers are MIME/MOSS aware. Very soon the DoD will be forced to make a decision as to whether or not to adopt both standards or switch from one to the other. As Emmett Paige, Jr. says,

Some people are saying we made a mistake picking X.400/X.500 rather than SMTP for defense messaging. There is no question in my mind that we've made the proper choices. However, I think there is a place for both messaging protocols...I believe that we must stay current with the rest of the world and be flexible to move from one protocol to another when another is better suited to meet our needs (Paige, 1996).

B. DMS OVERVIEW

1. Description of DMS

a. History of DMS

By the late 1980s, it was realized that the messaging systems used within the DoD had reached a point where it was no longer economically or technologically feasible to continue updating existing systems. In 1989 MROC 3-88 stated,

The Department of Defense requires an improved message communication system, responsive to mission requirements, at reduced cost to the Services and Defense agencies. This system, the Defense Message System (DMS), must be based upon a set of validated requirements and organized under basic architectural guidelines (MROC 3-88, 1989).

The DMS consists of all the hardware, software, procedures, personnel, and facilities required for electronic delivery of messages among organizations and personnel in the DoD. It is not a program in itself, but consists of multiple service initiatives concerning electronic messaging. The DMS is centered around the principles of interoperability and standardization. MROC 3-88 defines thirteen DMS requirements:

1. Connectivity/Interoperability. Connectivity must be extended from writer to reader and the DMS must be interoperable with tactical data distribution systems as well as allied systems.
2. Guaranteed delivery. The DMS must deliver a message to the intended recipient.
3. Timely delivery. The DMS must recognize messages that require preferential handling and must dynamically adjust to conditions of changing traffic loads and conditions to provide timely delivery of critical information during both peacetime and crisis.
4. Confidentiality/Security. The DMS must maintain separation of messages within

user communities to satisfy confidentiality and security.

5. Sender authentication. The DMS must verify that the sender did in fact originate the message.
6. Integrity. The DMS must verify that the information sent was the same as the information received.
7. Survivability. The DMS must provide for redundancy so that the system is capable of reconstitution.
8. Availability/Reliability. The DMS must provide users with continual message service.
9. Ease of Use. The DMS must not require extensive training for proper operation.
10. Identification of Recipients. The sender must unambiguously identify the recipient, the necessary directories and their authenticity are part of the DMS.
11. Message preparation support. The DMS must support user-friendly preparation of messages.
12. Storage and Retrieval Support. The DMS must support the storage of messages to allow for readdressal, retransmission, archiving, and analysis.
13. Distribution Determination and Delivery. The DMS must determine the destination of each message and ensure delivery.

The DMS implementation strategy is designed to provide a coordinated transition from the Baseline system of 1989 to the target architecture of 2008. The DMS implementation is divided into three phases, Phase I (1989 - 1994) focuses on the transition of Automatic Digital Network (AUTODIN), the current method of sending organizational messages, and DoD Internet e-mail to the DMS. Phase II (1995 - 2000) provides the bridge between the transitional capabilities and the final operational capabilities. Phase III (2001 -

2008) provides the achievement of final operational capability. Phases I and II will be discussed further under the present status of DMS, and Phase III will be discussed in the future of DMS.

b. Present Status of DMS

The objectives of Phase I were to automate telecommunication centers, extend the messaging interface to writers and readers, to migrate AUTODIN data pattern message traffic to the Defense Data Network (DDN) and the Defense Information System Network (DISN), eliminate the use of paper media, and phase out the telecommunication centers. The DDN provides a means for providing individual message services (e-mail) until the migration to DMS X.400 is complete. The DISN will provide the backbone for all DMS message services as the global telecommunications infrastructure. Phase II relies on the baseline AUTODIN messaging system, DoD Internet e-mail systems, and the X.400 message handling system as it progresses towards DMS compliant X.400 messaging and X.500 directory services. The objectives of Phase II are to expand writer to reader connectivity and support, provide writer to reader message security services, phase out baseline messaging systems, phase out baseline message formats and procedures, maintain interoperability between DMS and non-DMS systems, and implement DMS in a cost-effective manner.

c. Future of DMS

The objectives of phase III are complete implementation of the DMS target messaging components, maintaining interoperability between DMS and non-DMS systems, complete phase out of baseline messaging systems, complete phase out of all transitional

components, and evolution to a DISN value-added service.

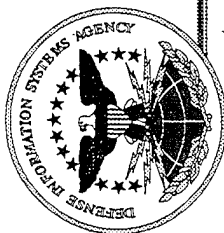
2. Implementation Requirements for DMS

Since the migration of DoD messaging systems to the DMS has been mandated by the Secretary of Defense, it is imperative for all commands to understand the requirements of the DMS. Figure 2 shows the DMS functions and components and Figure 3 shows the DMS architecture. The requirements for implementing DMS have been divided into three general categories:

1. DMS user components
2. DMS infrastructure components
3. Hardware and software installation

a. DMS User Components

(1) User Agent. The User Agent (UA) is a software application that resides on a personal computer or workstation with other office automated applications such as word processors and spreadsheets. The UA application is used for organizational and individual message preparation, transmission, and reception. The UA interacts directly with the user through a Graphical User Interface (GUI), which allows the workstation's operating system to communicate with the user in fast, visual, intuitive ways, such as the use of a mouse to drag and drop icons, to create and edit a message (Hice and Wold, 1995). Depending on the user privileges provided by the Fortezza card, which functions as an



DEFENSE MESSAGE SYSTEM FUNCTIONS AND COMPONENTS

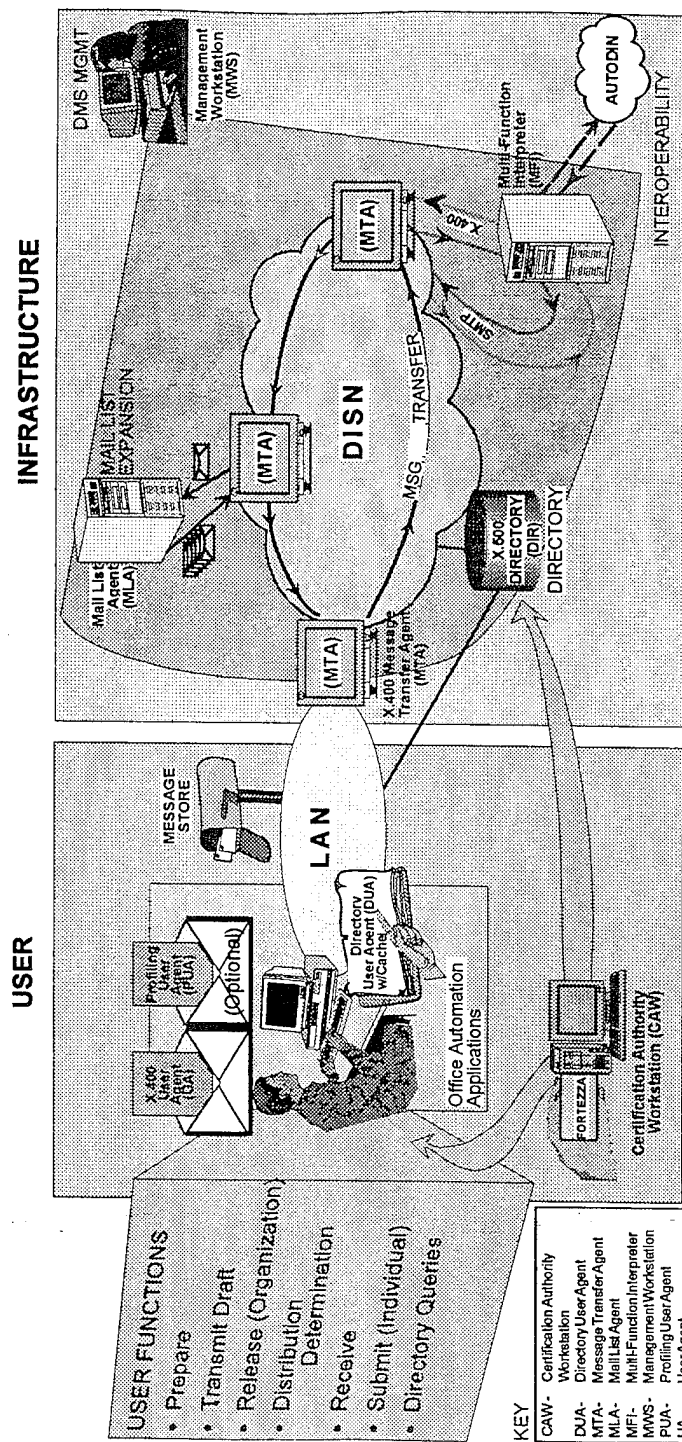
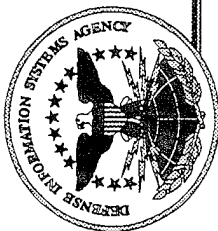


Figure 2. DMS Functions and Components "From DMS Expo 95"



DMS ARCHITECTURE

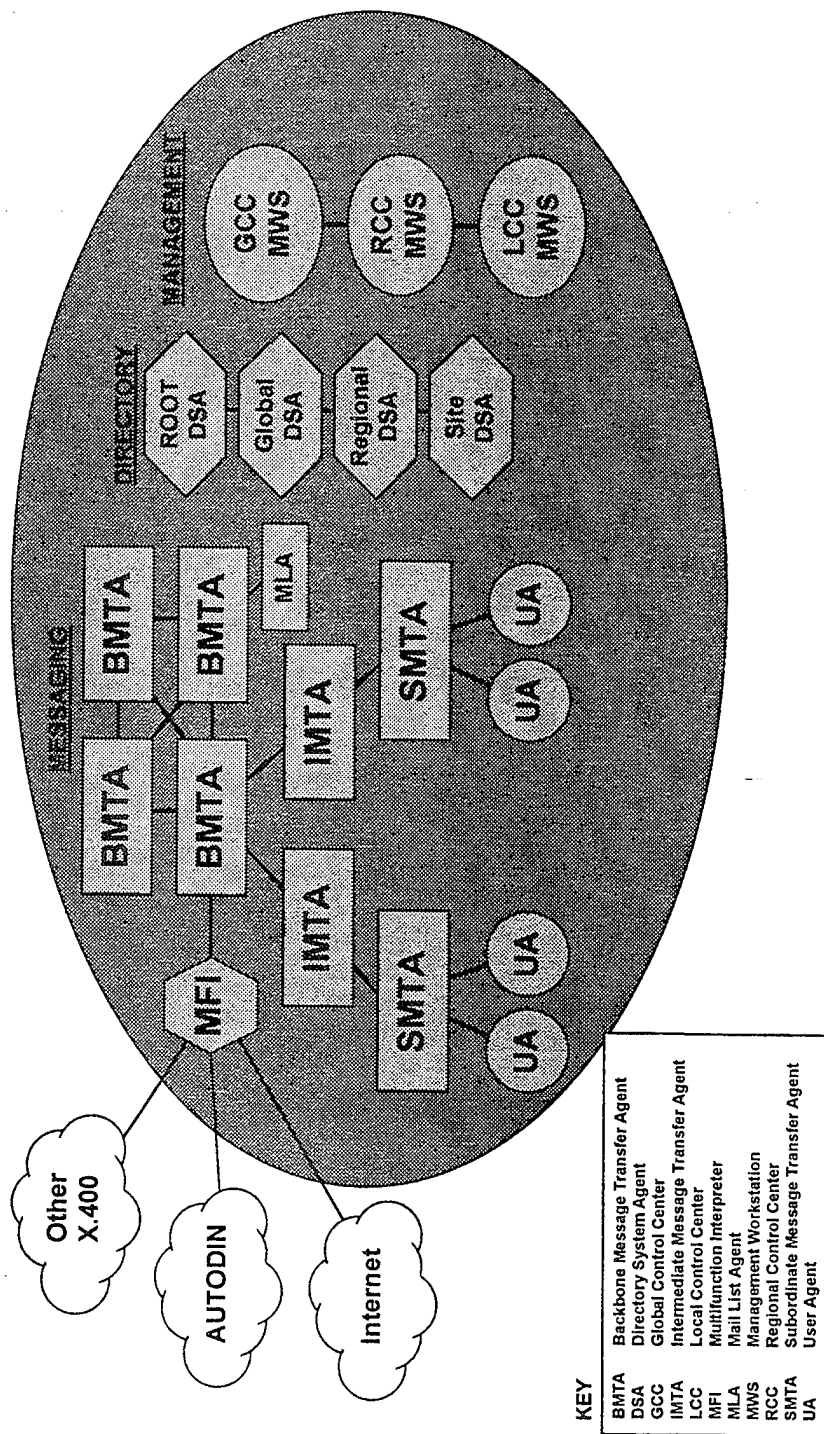
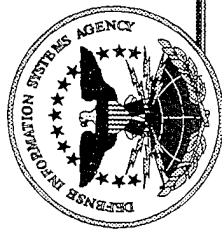


Figure 3. DMS Architecture "From DMS Expo 95"

identification card used to digitally sign, encrypt, decrypt, and verify digital signatures, the user can draft or release organizational and individual messages and receive organizational and individual messages generated elsewhere. The UA provides a directory cache that will store the addresses and security certificates of all addresses normally used by this originator. If the message is destined for an addressee not in the cache, or if the address has changed, queries are automatically initiated to the X.500 directory system agent to obtain the correct address and certificate to update the cache. All directory queries are authenticated by the digital signature function of the Fortezza PC Card (PCMCIA) to allow access to the X.500 directory. This prevents unauthorized UAs from accessing the military message transfer system, the DMS using the Defense Information Systems Network (DISN) infrastructure, and either saturating the system with messages or imitating military organizations (Hice and Wold, 1995). User Agents are divided into two classes, basic (mail only) and advanced (groupware). Within the basic class there is a P3 functionality which does not support the use of a Message Store (MS) and therefore connects directly to a Message Transfer Agent (MTA). As such, the UA must be on-line for messages to be received. A P7 functionality User Agent connects to a Message Store and supports delivery and storage of messages while the user is off-line. This is the recommended functionality for FalconLan. The advanced class of User Agent combine DMS messaging features with groupware features such as scheduling and shared folders. User Agent applications can be implemented either entirely within the user's personal computer or implemented in a client-server environment. Figure 4 shows how the user will interface with the UA in the DMS message handling environment.

(2) Message Store. The Message Store (MS) can be viewed as a mailbox facility. Like the UA it is a software application that can be implemented on each PC or in a network. When a UA is inactive, the MS receives all messages from the message transfer agent and stores them until they are called by the UA. A single MS can serve multiple UAs. When a MS is used, there is a logical, one-to-one relationship between each MS and UA pair. The MS can be configured to provide automatic alert capabilities or automatic forwarding based on message precedence. The MS may only be implemented for



DMS MESSAGE HANDLING ENVIRONMENT

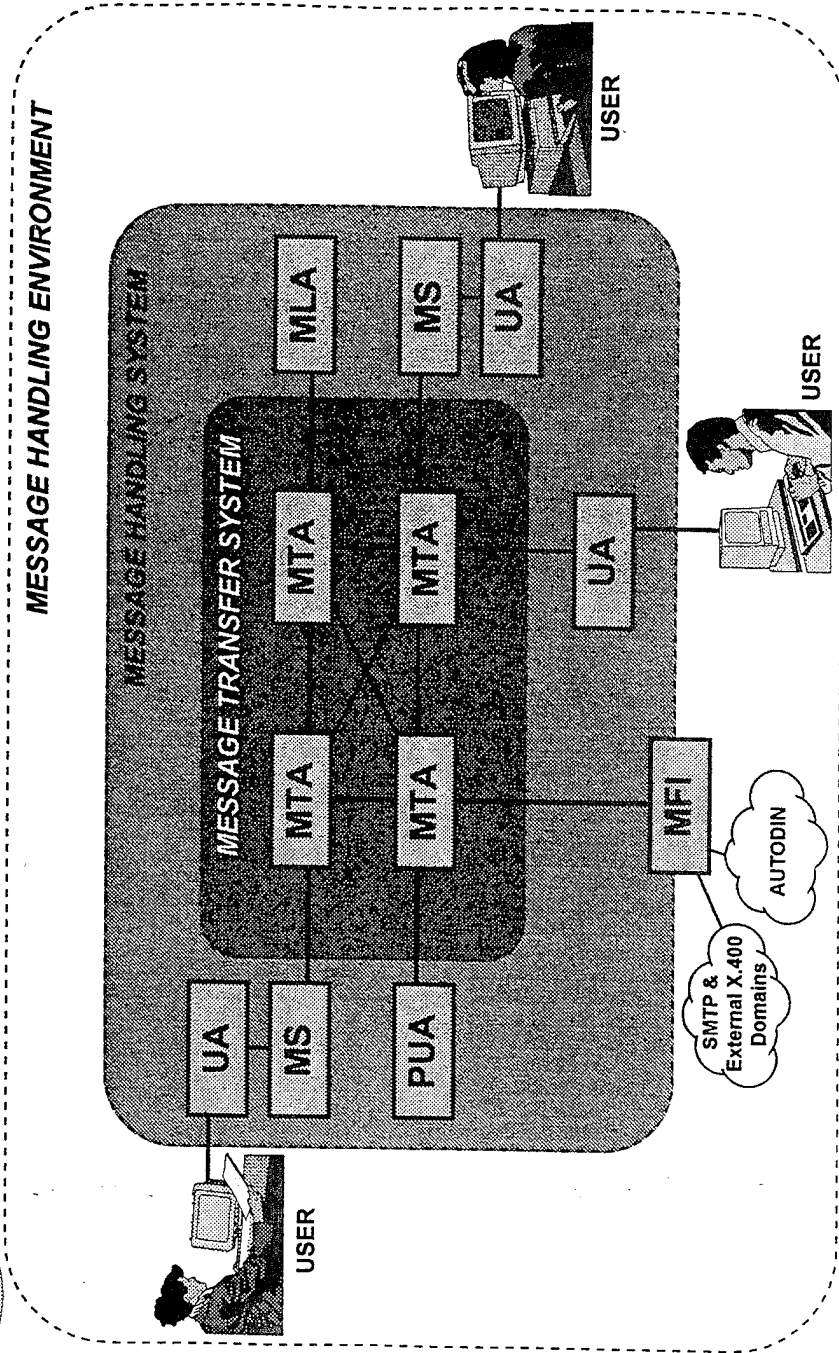


Figure 4. DMS Message Handling Environment "From DMS Expo 95"

individual messaging, not for organizational messaging. Figure 5 describes the DMS Message Store.

(3) Directory User Agent. The Directory User Agent (DUA) is a software application that provides X.500 defined directory services. Additionally, DUAs provide a common user interface, user authentication, and local caching of directory information. All directory services are provided to DMS users and components (e.g., UA, Mail List Agent (MLA), and Multi-Function Interpreter (MFI)) through the DUAs. The DUA may be implemented on the user's LAN, on the campus or base, within a local region, or in an entire theater of operations (Hice and Wold, 1995).

(4) Profiling User Agent. The Profiling User Agent (PUA) provides the same message processing capabilities as the User Agent (UA) and additionally includes functionality to profile messages for automatic distribution determination. The PUA is an application typically implemented along with other organizational messaging applications. After the PUA determines the appropriate recipients to receive the message, it will resubmit the copies of the message to the MTS for subsequent delivery (Hice and Wold, 1995). Each PUA retains the originator's digital signature with the message. Based on information such as the subject, priority, and message content, the PUA can automatically redistribute received messages. This is accomplished by resubmitting the message to the Message Transfer System (MTS) for subsequent delivery to the appropriate addresses.

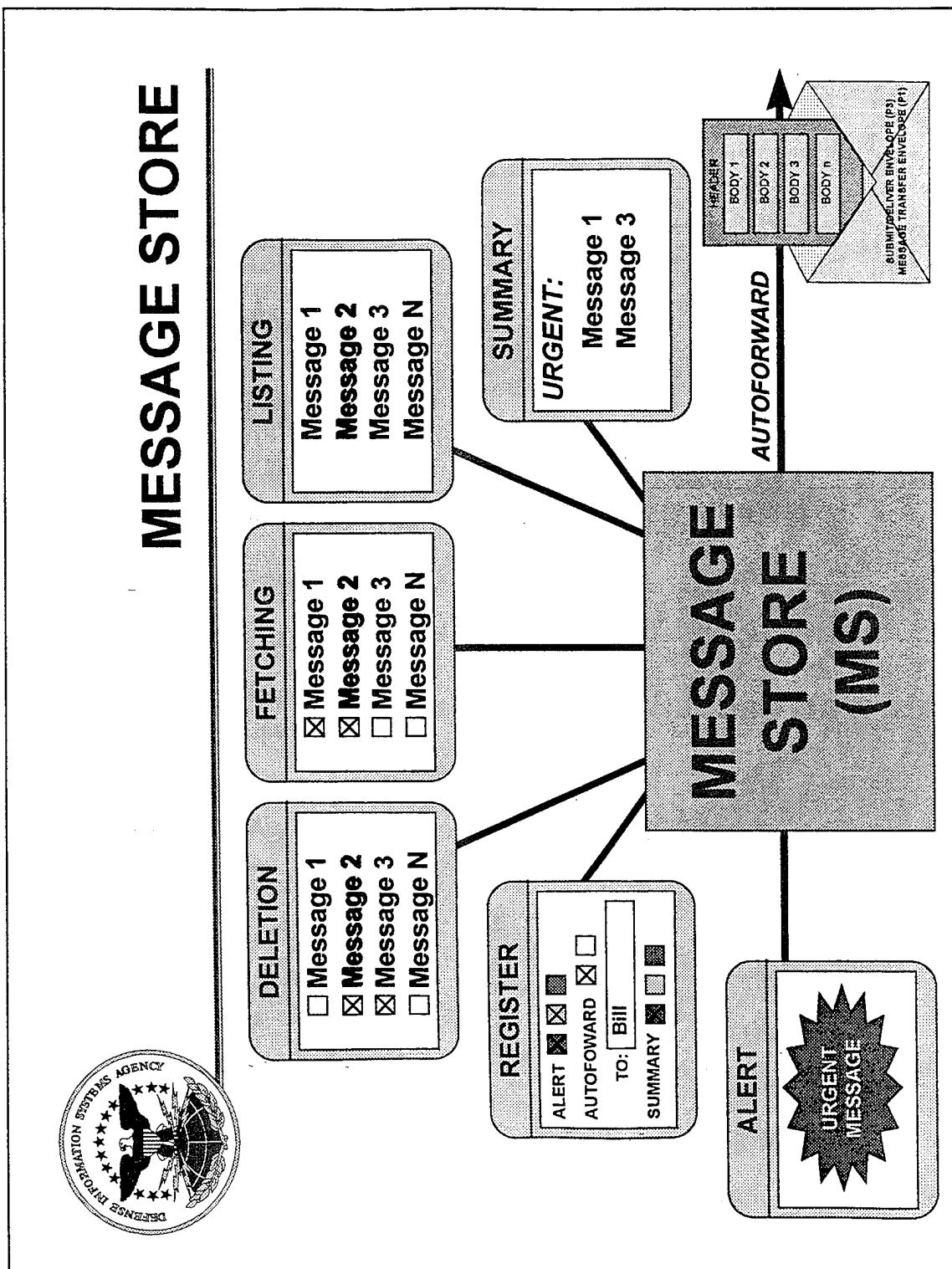
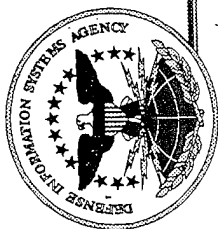


Figure 5. DMS Message Store "From DMS Expo 95"

b. DMS Infrastructure Components

(1) Message Transfer Agent. The Message Transfer Agent (MTA) is a store and forward message switch. An analogy of the MTA is the local post office because it is responsible for routing and transferring the mail, or in this case, the messages. MTAs are implemented at many locations and interconnected using any variety of communications technology, including wireless (Hice and Wold, 1995). The MTA provides mail host services to local users and provides switching services for the infrastructure X.400 messaging network. The MTAs receive messages from a User Agent (UA), Message Store (MS), or another MTA. The MTA is responsible for making routing decisions using the originator or recipient address, it then delivers the message to the next MTA, MS, or a local UA. Additionally, MTAs can deliver messages to Profile User Agents (PUAs), Mail List Agents (MLAs), or Multi-Function Interpreters (MFIs) (Hice and Wold, 1995).

(2) Mail List Agent. The Mail List Agent (MLA) is responsible for managing a number of Mailing Lists (ML). The MLA supports DoD MLs that may consist of several hundred addresses and allows the task of sending a message to a large number of addresses to be off-loaded to a separate application while users proceed with other activities. MLA applications may be executed as an optional DMS UA application on multifunctional workstations with sufficient processing capabilities or on a separate hardware platform. An MLA may be implemented locally or regionally. Figure 6 describes the Mail List Agent.



MAIL LIST AGENT (MLA)

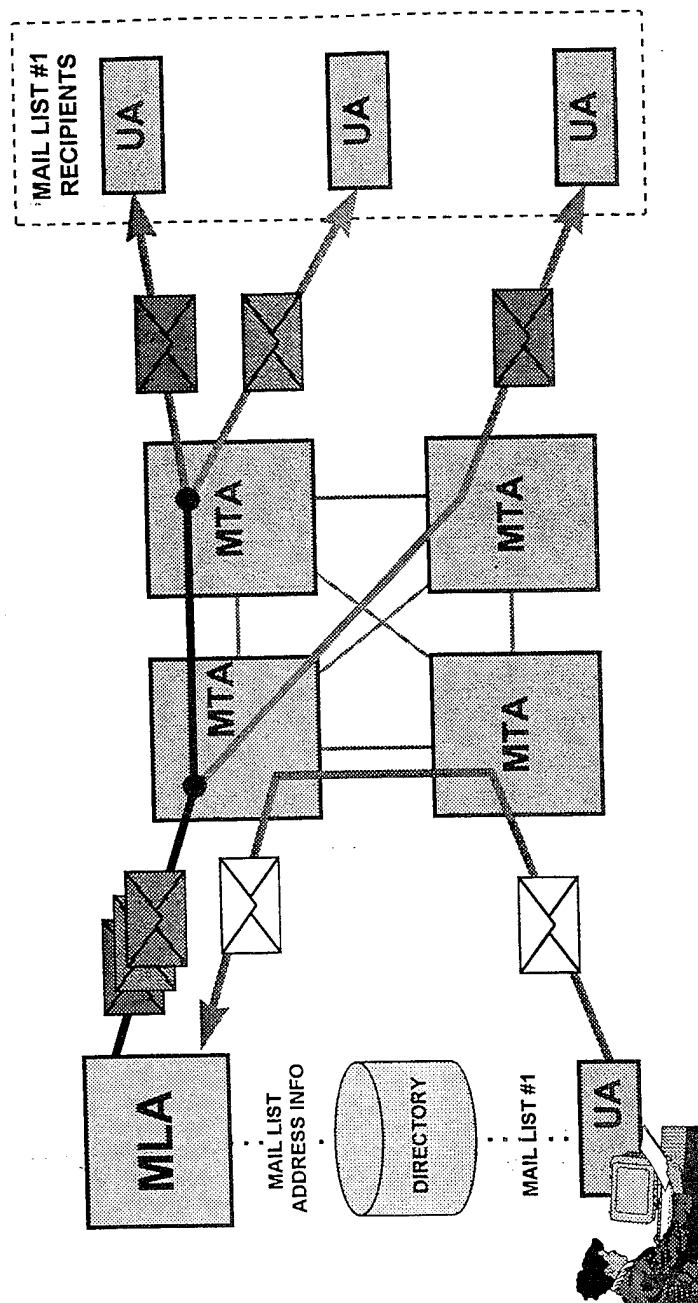


Figure 6. DMS Mail List Agent "From DMS Expo 95"

(3) Multi-Function Interpreter. The Multi-Function Interpreter (MFI) is the DMS infrastructure component that will allow DMS users to exchange messages with users of legacy systems (e.g., AUTODIN or SMTP.) The MFI should be installed in the Message Transfer System (MTS) backbone to make it transparent to the user whether or not this component is used. Once DMS reaches Final Operational Capability (FOC) the MFI will be eliminated. Figure 7 describes the DMS Multi-Function Interpreter.

(4) Management Workstation. The Management Workstation (MWS) is a critical component within the DMS management infrastructure. It provides remote monitoring and control of all DMS products, thereby supporting configuration, fault, performance, security management, accounting for system monitoring and control, system administration, and customer service. It must be able to gather DMS system information globally and present meaningful reports to the DMS managers. A Management Agent (MA) is installed in each DMS component and supports the collection of component information and facilitates the transmission of the data to the MWS (Hice and Wold, 1995). The MWS interfaces to the DMS components using the Simple Network Management Protocol (SNMP). The Loral integrated MWS consists of Computer Associates' ENTERPRISE VIEW for E-mail application management, Oracle Relational Database for reporting and configuration management, and the Remedy Action Request System for trouble ticket generation and tracking. The MWS is a software application usually implemented on a high performance UNIX or NT workstation.

(5) Certification Authority Workstation. The Certification Authority Workstation (CAW) is a PC based application used to program and maintain Fortezza PC Cards (PCMCIA) for users. Each user's Fortezza card includes not only private security keys, but also the user's messaging privileges, individual messaging only or organizational message release, including organizational level, precedence, and classification authorized. This trusted workstation supports functions that include decentralized assignment of directory names and creation of X.509 certificates. As part of this process, the CAW applications initialize the Fortezza card with a PIN, X.509 certificates, and other DMS information.



MULTI-FUNCTION INTERPRETER (MFI)

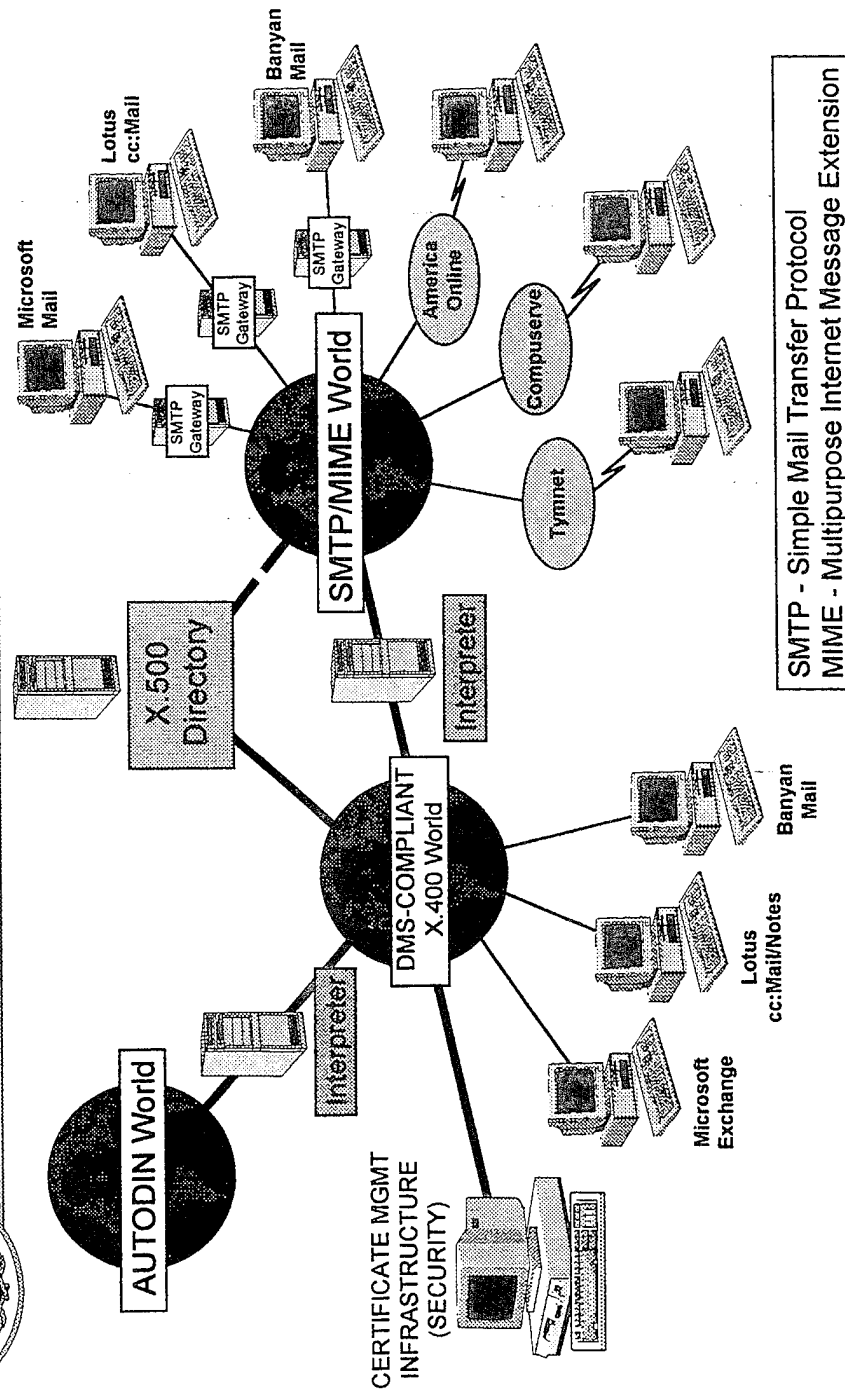


Figure 7. DMS Multi-Function Interpreter "From DMS Expo 95"

(6) Administrative Directory User Agent. The Administrative Directory User Agent (ADUA) is a Directory User Agent (DUA) software application that provides the directory administrator the ability to modify, add, and delete X.500 DMS entries. Certification authorities use the ADUA application resident in the Certification Authority Workstation (CAW) to perform a number of directory related security operations. The Mail List Manager (MLM) will also use an ADUA to update Mail List (ML) information in the directory.

(7) Directory System Agent. The Directory System Agent (DSA) is responsible to respond to queries for DMS X.500 directory information from DUAs and other DSAs. In order to support this function, each DSA stores a fragment of the DMS X.500 Directory Information Table (DIT) and a fragment of the Directory Information Base (DIB). The DIB is the collection of all DITs. The DMS X.500 directory is composed of the sum of all DIB and DIT fragments. The DITs consist of hierarchically related objects which model the geographic and organizational structure of DMS readers and writers. In this distributed directory environment, queries and updates are resolved by groups of cooperating DSAs.

c. Hardware and Software Installation

Defense Information Systems Agency (DISA) will fund and be responsible for the acquisition, installation, and maintenance of all DMS infrastructure components:

1. Backbone Message Transfer Agent (BMTA)
2. Directory System Agent (DSA)

3. Mail List Agent (MLA)
4. Multifunction Interpreter (MFI)
5. Certification Authority Workstation (CAW)
6. Administrative Directory User Agent (ADUA)
7. Management Workstation (MWS)

Each service will fund the purchase of the DMS user components:

1. User Agent (UA)
2. Message Store (MS)
3. Directory User Agent (DUA)
4. Fortezza Cards
5. "PC Cards" (PCMCIA Cards)

In order to be ready for site implementation there are many activities that must be completed, an example of some are listed here:

1. Identify the locations where infrastructure components will be implemented and how many are required.
2. Develop and implement policies and procedures for DMS implementation.
3. Distribute Fortezza cards to all users.

More specific requirements will be discussed in Chapter IV, when we look at the proposed implementation of the DMS and MISSI in FalconLan.

III. SECURITY SYSTEMS

A. SECURITY SYSTEMS BACKGROUND

As computer networks play an increasing role in the DoD, especially with regards to personal and organizational communications, the need for security is unparalleled. Connectivity to a Local Area Network (LAN), Wide Area Network (WAN), or the Internet provides a possible worldwide communications path. In response to this security issue, the National Security Agency (NSA) began a computer security development effort called the Multilevel Information Systems Security Initiative (MISSI).

1. Description of MISSI

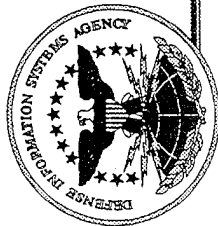
MISSI encompasses communications security and computer security in its goal to provide dependable and affordable security services necessary to protect information from unauthorized disclosure or modification and to provide mechanisms to authenticate users participating in the exchange of information (Cooney and Bilinski, 1995). In order to provide multilevel security (MLS), MISSI is evolving a series of products based on common standards and interoperable with commercially available products. The MISSI initiative is focused on providing security services through a series of increasingly enhanced releases. Each release is designed to increase user capabilities, reduce residual security risks, and keep pace with technology and performance advantages while maintaining compatibility with previous releases.

a. History of MISSI

MISSI is a framework for security of all networks using commercial products and standard service offerings. It is not a security solution for the DMS only. MISSI is to be available to NATO and other U.S. allies as well. MISSI will provide a single, integrated, consistent security infrastructure for all DoD needs: e-mail, electronic data interchange (EDI), electronic commerce (EC), intelligence, command and control, and business systems. The primary MISSI customer is the DMS, but MISSI is planned to be used for applications such as e-mail, remote login, file transfer, and database management.

b. Present Status of MISSI

On Friday, 15 September 1995, the NSA awarded contracts to National Semiconductor, Inc., Santa Clara, California and SPYRUS, Inc., San Jose, California, for the production of more than 310,000 Fortezza PC Cards (PCMCIA). The price of the Fortezza card to be delivered under this contract is \$69.50 with deliveries scheduled to commence in May 1996 at a rate of 15,000 cards per month. The Fortezza cards function as combined individual and organizational identification cards for Sensitive But Unclassified (SBU) data. Figure 8 describes the Fortezza card. The MISSI SBU solution set product is Fortezza/Message Security Protocol (MSP).



MISSI FORTEZZA IMPLEMENTATION

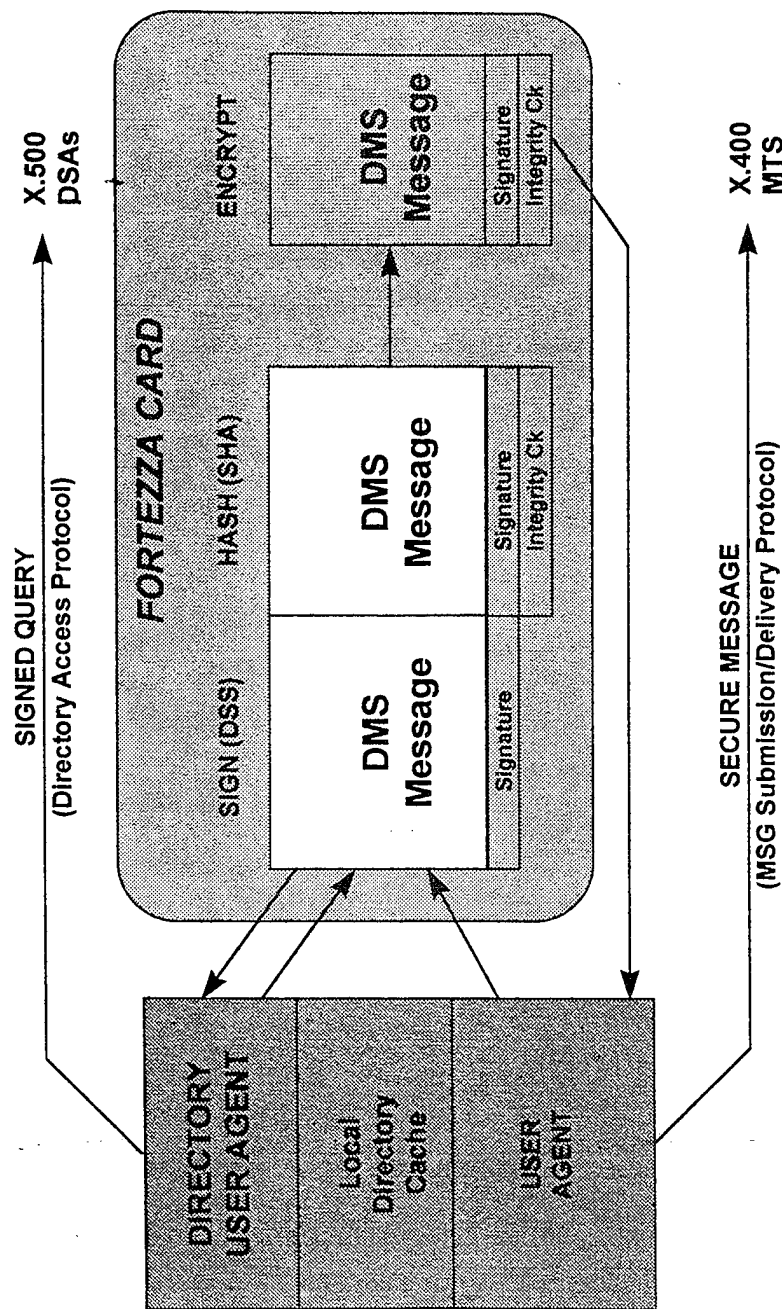


Figure 8. MISSI Fortezza Implementation "From DMS Expo 95"

Fortezza products can be used to protect any type of data including X.400 and SMTP E-mail, in other words there is modularization between the crypto engine and the message security protocol. It uses Type II security algorithms to provide network related security services such as message confidentiality, message integrity, message authentication, access control, and non-repudiation. Type II security provides protection for SBU data, but not classified data. Type I security is used to protect classified and SBU data. The Fortezza card is used to digitally sign, encrypt, decrypt, and verify digital signatures of data. The PC Card (PCMCIA) reader can be connected to a personal computer through a standard bus slot or through an adaptor connected to a parallel port or a Small Computer Systems Interface (SCSI) bus. The Fortezza/MSP software will support applications such as User Agent (UA), Mail List Agent (MLA), Simple Mail Transfer Protocol (SMTP), and file protection software.

c. Future of MISSI

To forge into the future, NSA is developing the Fortezza Plus card which will provide Type I and II cryptographic algorithms. Type I algorithms will be used to protect data classified up to the Secret level for transmission across unprotected networks (Hice and Wold, 1995). The Fortezza Plus card provides Type II algorithms to protect SBU data. The Type II algorithm will be backward compatible with the Fortezza card, so protected data may be communicated between workstations equipped with either the Fortezza or Fortezza Plus card. Additional applications are underway utilizing Fortezza cards for file transfers, web browsers, remote login, database management, and Firewalls.

2. MISSI Building Block Products

a. Cryptographic Cards

A central component of MISSI is a small, low cost, thick credit card sized plug-in card called the Fortezza. The Fortezza card is built to international PCMCIA standards that is inserted in a standard Type 2 PC Card (PCMCIA) reader. Used in conjunction with a personal identification number, the card provides effective authentication of the user's identity and access privileges. There are two basic versions of Fortezza as described above; Fortezza and Fortezza Plus. The Fortezza card contains its own processor and memory, and inputs and outputs through the 50 pin connection points on the end of the card.

Defense Information Systems Agency (DISA) plans to provide every DoD employee who will be issuing DMS messages a Fortezza card. Along with cryptographic data and various MISSI algorithms, the card will contain important security information about the user, such as clearance information and authorizations (Cooney and Bilinski, 1995).

The Fortezza card uses public key cryptography technology where the private key is kept secret and is only used by the owner of the card, but the public key is made available to anyone. For the DMS, the public keys will be available in the X.500 directory.

b. Cryptographic Card Applications

There are currently many applications under development that use MISSI cryptographic cards. Each application is built on a security protocol such as MSP for e-mail. Applications call MISSI libraries, drivers and the standard command sets for the cards by

using the MISSI cryptographic application programming interface (API).

c. Secure Computing

Secure computing adds features and assurances to the computing environment that enhance its overall security. Example features include data labeling, data separation, access control lists, and data integrity. Assurances are specific design and design analysis activities taken to gain confidence that security critical functions are performing properly; and that hidden functions that could be detrimental to security, such as covert channels, are eliminated or minimized. Initially, most user personal computers using MISSI technology will be used in untrusted operating systems. Over time, more users are expected to migrate to the use of trusted operating systems. Trusted operating systems provide data labeling and separation, verified systems access, reliable auditing, and reliable cryptographic card invocation. Integrating secure computing components with Fortezza can provide increased writer to reader security at the desktop.

d. Secure Servers

A Secure Network Server (SNS) typically resides on the LAN boundary acting as an MLS guard for the information handled and transmitted on the local network. An SNS located on the border of a computer network handling Secret information is an example. The SNS would ensure that Secret information handled on the network being protected would not inadvertently be passed to a network that is not equipped to handle Secret data (Cooney and Bilinski, 1995). Figure 9 depicts a Secure Network Server.

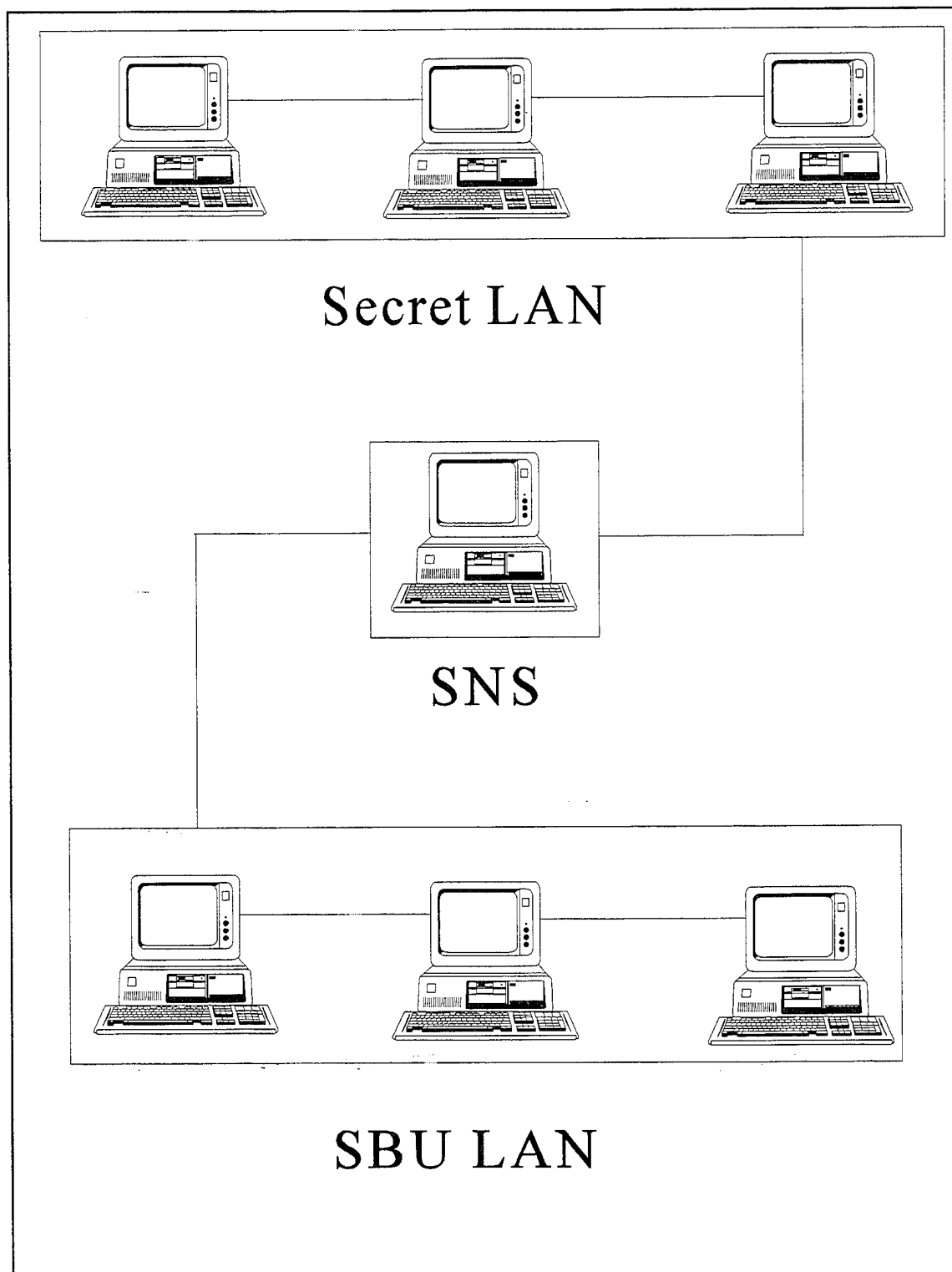


Figure 9. Secure Network Server (SNS)

e. In-Line Network Encryptors

In-Line Network Encryption (INE) products are usually located at user enclave boundaries between local and wide area networks, or on a single network between individual hosts/workstations that are operating at different security levels. The users served by an individual Subordinate Message Transfer Agent (SMTA) are collectively referred to as a user enclave. These products will provide both encryption and access control services. By providing end-to-end encryption of data communications and access control between LANs, INE products will ensure that information being transmitted is not disclosed to unauthorized parties (Cooney and Bilinski, 1995). The INE interface with the Multi-Function Interpreter (MFI) is transparent to the user because the MFI will apply or remove the MSP encryption to the messages as they move in and out of systems that do not support MISSI components (Hice and Wold, 1995). Figure 10 depicts an In-line Network Encryptor (INE).

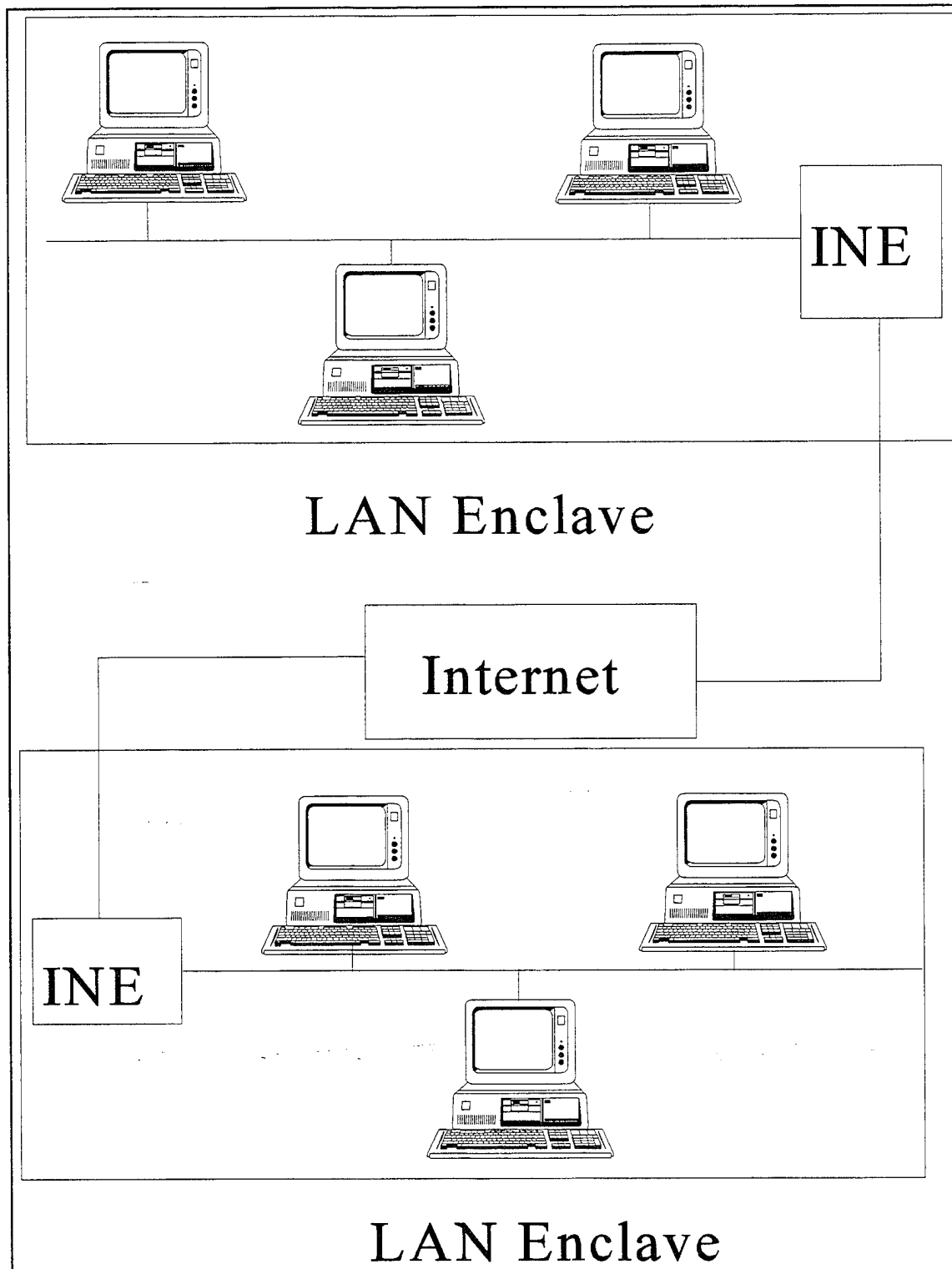


Figure 10. In-Line Network Encryptor (INE)

f. Network Security Management

Network security management products provide the common infrastructure necessary for MISSI. They perform functions such as key, privilege, and certificate management and the collection and analysis of security relevant audit data.

3. Commercial Equivalents of MISSI

a. Firewalls

A firewall is a collection of components placed between two networks that collectively have the following properties (Cheswick and Bellovin, 1994):

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This means that all modems must be located behind the firewall.
2. Only authorized traffic, as defined by the local security policy, will be allowed to pass.
3. The firewall itself is immune to penetration.

Firewalls separate environments operating under differing security policies and control data flow between the different environments. Most commercial Firewalls are low assurance components. MISSI supports usage of low assurance Firewalls, but also provides high assurance Firewalls based on the Secure Network server (SNS). Use of filtering routers and packet screening by both the sender and recipient address blocks provides most of the real work of the firewall.

b. Public Key Cryptography

In a public key encryption system each user has two keys, one key that does not have to be kept secret, the public key, and a key that is kept private. The advantage of this is that anyone can send a secret message to a user by applying the receiver's public key to the message, the receiver then uses their secret key to decrypt the message (Pfleeeger, 1989). Some examples of public key cryptography are: Rivest-Shamir-Adelman (RSA), Privacy Enhanced Mail (PEM), and Pretty Good Privacy (PGP).

c. Kerberos

Kerberos is a system where a client and server share a key used to encrypt data over the network. Because the cryptography is based on shared keys, Kerberos is known as a symmetric key system (Malamud, 1992).

B. Advantage of MISSI Over Commercial Products

By incorporating some of the best to offer commercial features, MISSI will provide the user with a wide range of information systems security capabilities. These capabilities include services which ensure that transmitted data is neither accidentally corrupted nor deliberately tampered with by a third party prior to receipt. Strong identification and authentication measures are included at both the workstation and at various network gateways to deny access and privileges to unauthorized users. Data is encrypted to provide confidentiality. Digital signatures ensure the positive and irrefutable identification of the sender. MISSI services offer protection against the unauthorized disclosure or modification of information while enabling the transmission of data between different security levels.

Additionally, all MISSI products will be X.400 compliant and will be able to be used in the implementation of the DMS. Best of all, as the technology improves, the MISSI product improvements will remain backwards compatible.

IV. PROPOSED IMPLEMENTATION

A. DESCRIPTION OF FALCONLAN

This chapter assumes a basic knowledge of Local Area Network (LAN) technology. For a brief review the author recommends Fitzgerald's *Business Data Communications : Basic Concepts, Security, and Design* or any other LAN text.

The FalconLan is divided between two buildings located at the Presidio of Monterey. Building 616 contains the offices of the Officer in Charge (OIC) and Assistant Officer in Charge (AOIC) and has a total of seven terminals connected to the network. Building 629A contains the general offices of the detachment and has a total of 19 terminals connected to the network. Figure 11 provides the layout of Building 629A and Figure 12 provides the layout of Building 616. Figure 13 provides the Local Area Network diagrams for Building 616 and 629A. Thin Ethernet (10Base2)¹ is used throughout both buildings and the connection between the two buildings will be fiber optic cable. Each building has one Windows NT 3.51 server for all the terminals in its building. Each terminal will have its own copy of WordPerfect, Microsoft Mail, Paradox Data Base, and Intranet/Internet services. All remaining application software will reside with the two servers. The terminals in building 616 are connected to the server in a bus topology, while the terminals in building 629A are divided

¹Thin Ethernet (10Base2) means the transmission speed is ten million bits per second, using the baseband transmission methodology, and it has a maximum distance of 200 meters between terminals or repeaters.

into five bus segments that are interconnected through a hub. The bus topology connects all nodes to a cable running the length of the network. The circuit is not joined together to form a loop, but each terminal uses the bus to communicate with every other terminal. Data is typically transmitted in both directions from the originating node, with other nodes checking the data as it passes to determine if they are the ultimate address of the data. Data may pass directly from one node to another, or it may be routed through a head end control point. The head end controller turns the data transmission around and sends it back down the cable in the opposite direction to the terminator. This topology is easily expandable to accommodate additional nodes and the loss of a single node has no impact on the rest of the network. This is the topology chosen for FalconLan primarily because the network size is anticipated to double to approximately 60 terminals in the near future. Figure 14 depicts a bus topology.

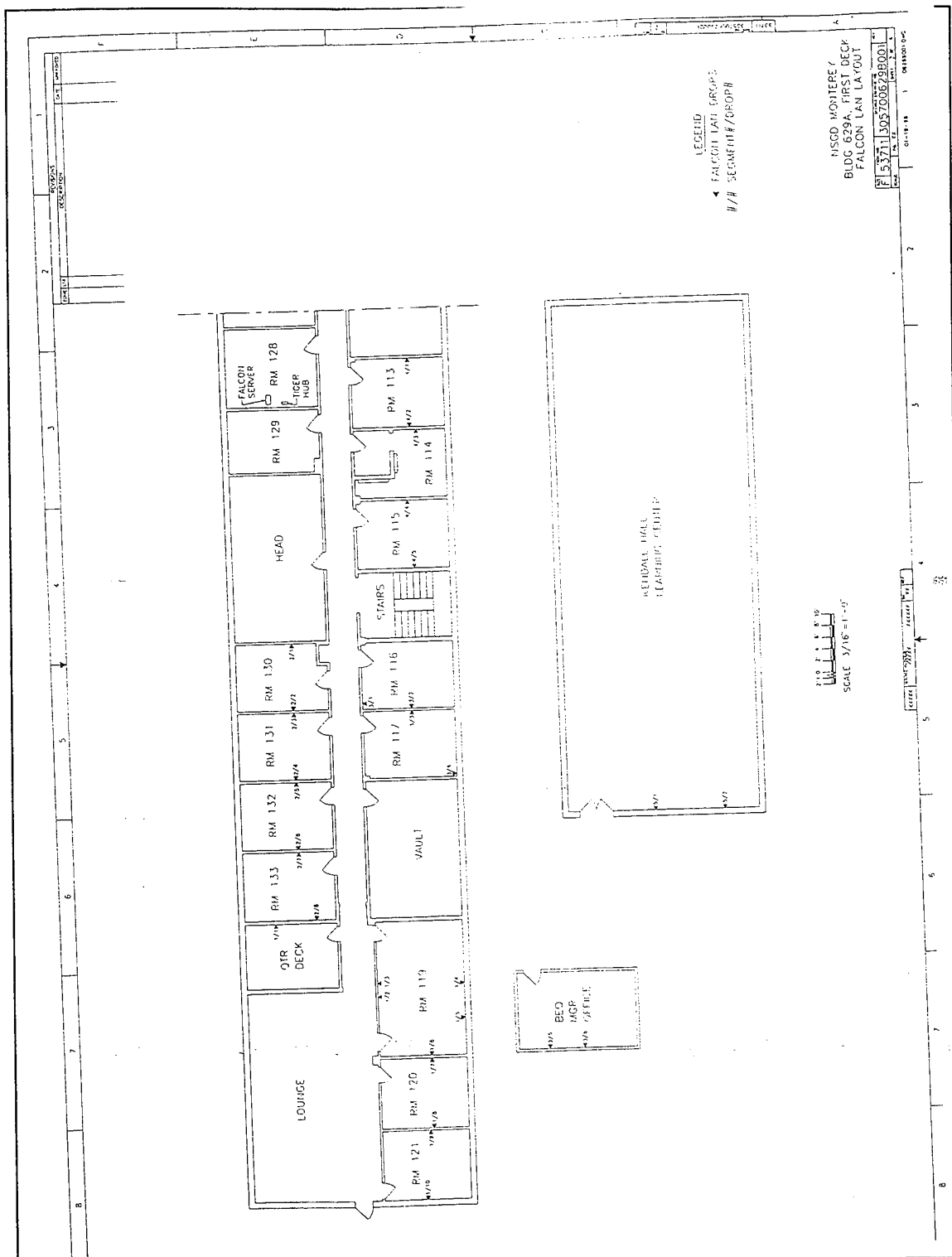


Figure 11. Building 629A Layout "From NISE East"

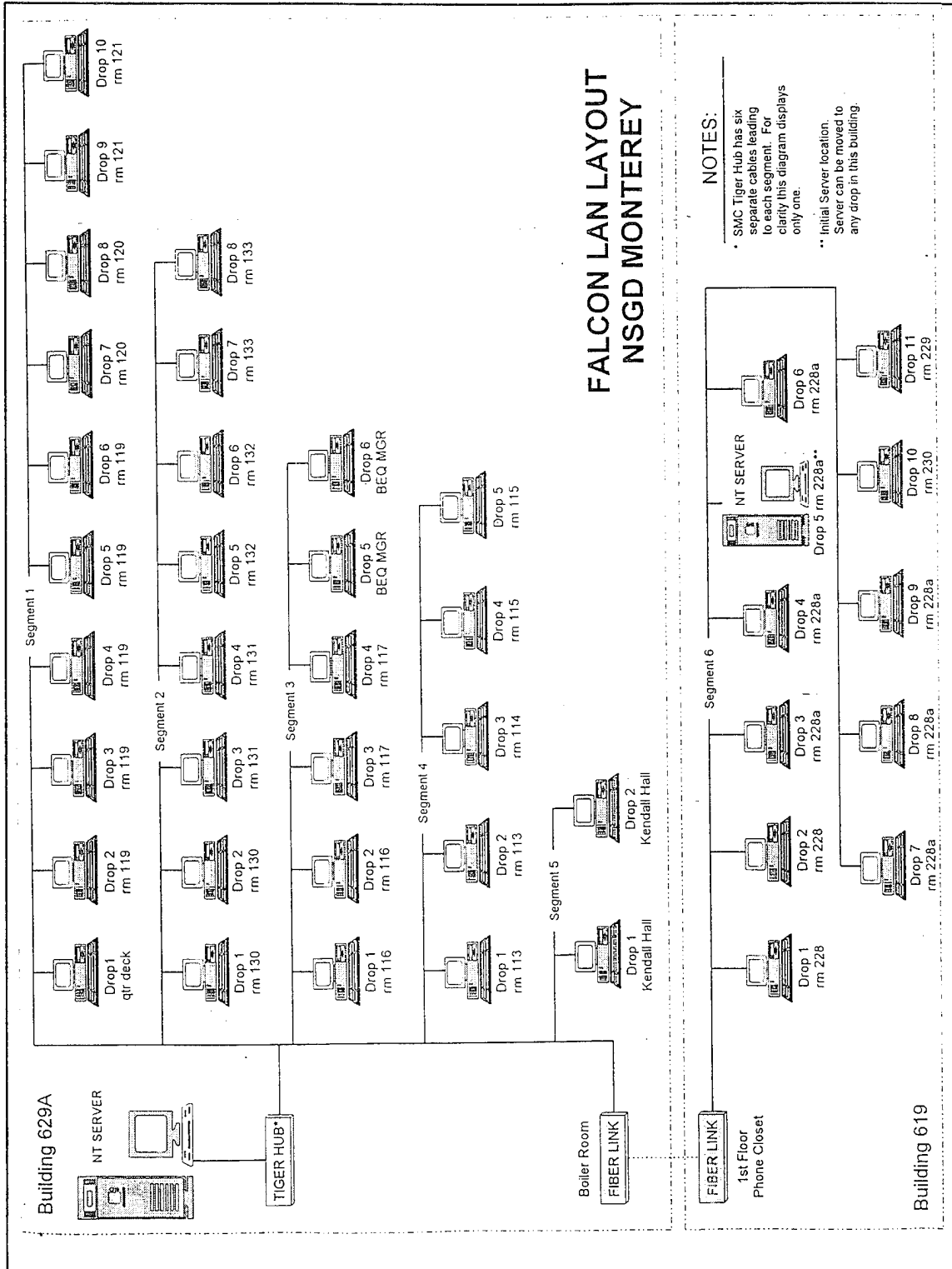


Figure 12. Building 616 Layout "From NISE East"

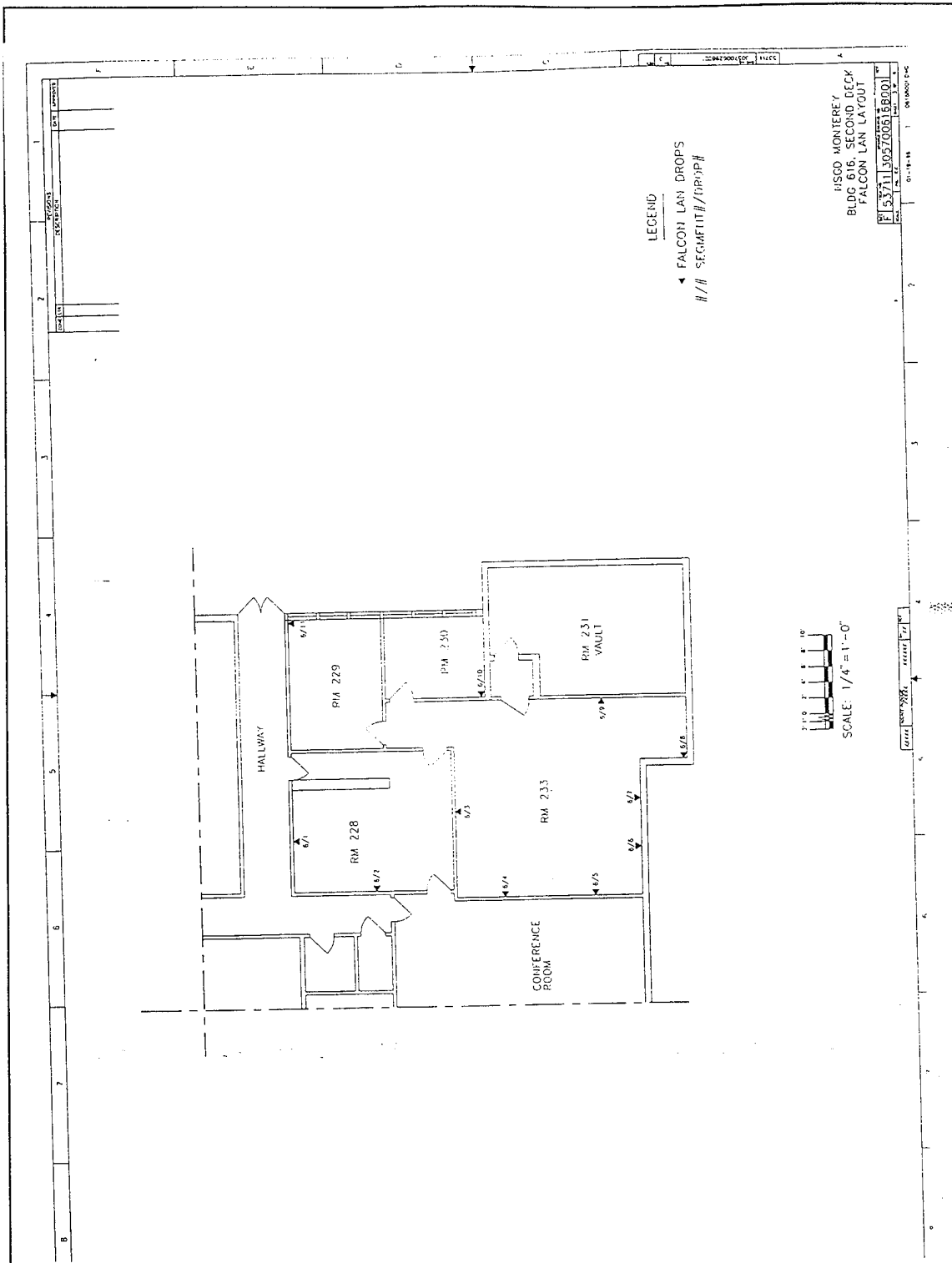


Figure 13. FalconLan Layout "From NISE East"

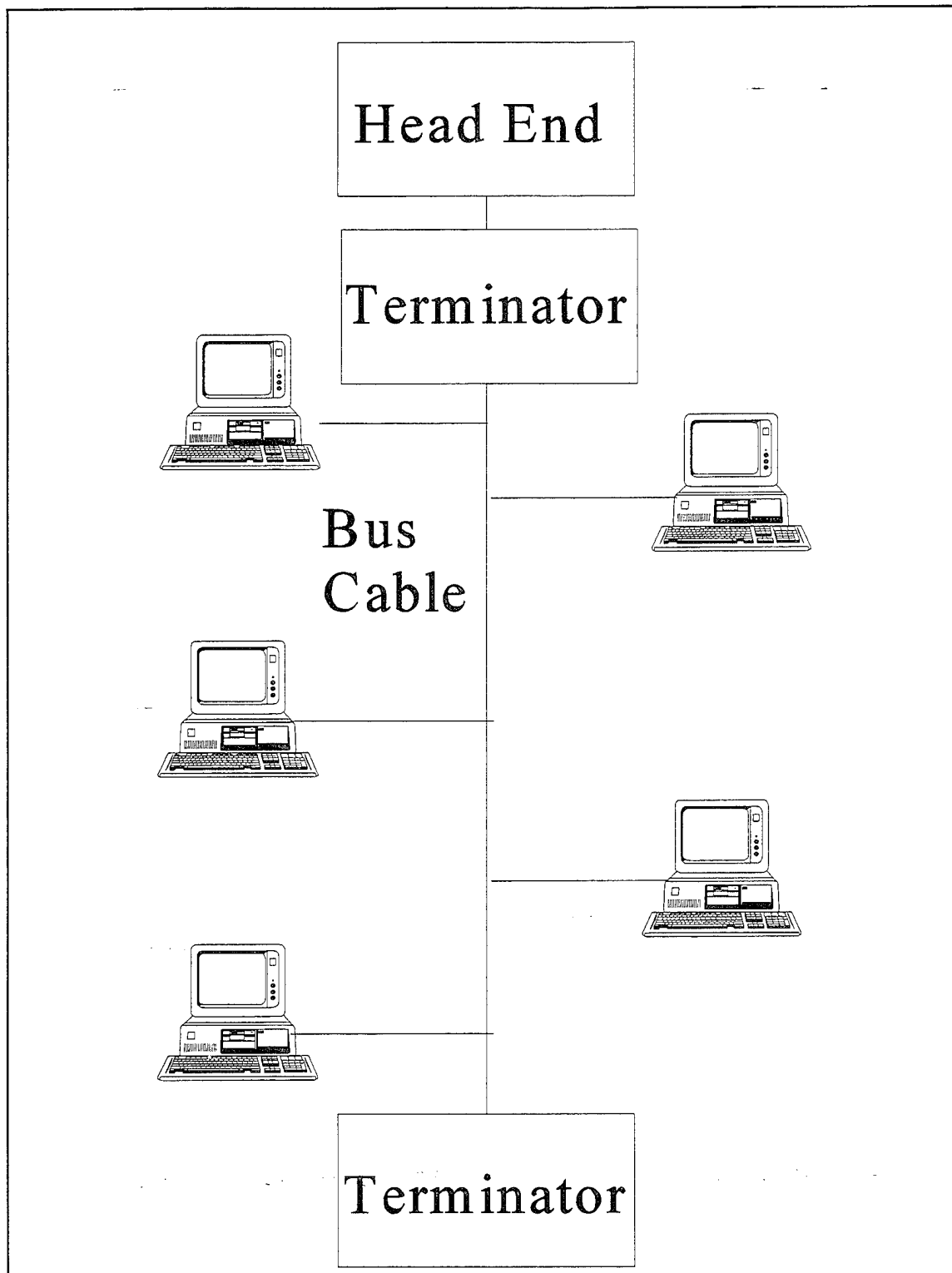


Figure 14. Bus Topology

B. INSTALLATION OF THE DMS COMPONENTS WITH FALCONLAN

The DMS contract, providing software, hardware, and services to create this new messaging system, was awarded in June 1995 to the LORAL Federal Systems team (DMS Product Guide, 1995). The DMS products are currently undergoing mandatory compliance and conformance testing, which is required prior to the products being made available for purchase from the contract (Philbin, 1996). Purchase from the contract will be available after Initial Operational Capability (IOC) is realized. It is anticipated that IOC will occur in July, 1996. The DMS contract provides ten Contract Line Item Numbers (CLINs):

1. CLIN 0001. This CLIN is the program management and infrastructure CLIN. This CLIN will be used by DISA and the Air Force Acquisition Office only.
2. CLIN 0002. This CLIN is for ordering the software products for the DMS infrastructure (eg., Directory System Agents, Multi-Function Interpreters, Mail List Agents, Message Transfer Agents, and Management Workstations) and the DMS user components (eg., User Agents, Directory User Agents, Profiling User Agents, Message Stores, and Management Workstations.)
3. CLIN 0003. This CLIN is for ordering hardware platforms and products (eg., PC Card readers and any terminal upgrades.)
4. CLIN 0004. This CLIN is for support services such as recommendations on site architecture, LAN topology and configuration, etc.
5. CLIN 0005. This CLIN is for an implementation service package to support less than 750 users. Any site survey for more than 750 user should be addressed through CLIN 0004.
6. CLIN 0006. This CLIN is for training. Several training courses are currently planned for implementation in 1996.
7. CLIN 0007. This CLIN is for hardware maintenance. All hardware items come with a one year warranty. The PC Card readers are warrantied on a mail back

basis, with replacement within five days of receipt.

8. CLIN 0008. This CLIN is for manuals, documentation, and reference guides.
9. CLIN 0009. This CLIN is for material and travel expenses for services ordered under CLINs 0004, 0005, or 0006.
10. CLIN 0010. This CLIN provides the contract award fee.

This section will provide recommendations for two implementation options for an SBU enclave: basic functionality and full functionality. An SBU enclave has all PCs protected by having personnel use Fortezza cards and there is a firewall between the LAN and any external network, such as the Internet. These two options are based on the currently available products.

1. Basic Functionality Implementation

Basic functionality implementation will provide the user individual messaging capabilities within the command and will rely on the base infrastructure for organizational messaging. For a basic implementation, the following components are recommended:

1. User Agent
2. Directory User Agent
3. Message Store
4. Message Transfer Agent
5. Administrative Directory User Agent

The available User Agent software package includes an integrated Directory User

Agent (DUA) that provides access to the X.500 Directory Services. The User Agents currently available for Windows NT 3.51 that provide the previously mentioned P7 functionality are listed in Table 1.

Product No.	Product Description	Unit Price
UA0005	Microsoft DMS-GOSIP Mail Only UA for Windows NT	\$62.00
UA0016	Microsoft DMS-GOSIP UA for Windows NT (Group)	\$118.00

Table 1. User Agent Options

The recommended User Agent implementation is the groupware functionality Product No. UA0016. It is recommended that 4 copies be procured, two individual copies for the OIC and AOIC and two copies for the network servers.

The Microsoft Exchange product currently available contains an integrated Message Transfer Agent and Message Store and is shown in Table 2.

Product No.	Product Description	Unit Price
MM0001	Microsoft DMS-GOSIP Information Exchange for Windows NT	\$1,950.00

Table 2. Message Store Options

It is recommended that one copy be procured to service all the User Agents. The enterprise edition with 25 access licences is \$2857.95 (academic price) vice the \$1,950 shown in Table 2.

The Administrative Directory User Agent is shown in Table 3.

Product No.	Product Description	Unit Price
ADUA01	ES/ADUA for Windows	\$38.00

Table 3. Administrative Directory User Agent Options

It is recommended that one copy be procured for the local DMS manager.

2. Full Functionality Implementation

Full functionality implementation will provide the user individual messaging capabilities within the command and organizational messaging external to the command without relying on the base infrastructure. For a full implementation, the following components, in addition to the basic implementation, are recommended:

1. Management Workstation
2. Profiling User Agent
3. Mail List Agent
4. Certification Authority Workstation

The above listed components all require one Hewlett Packard Workstation that will be isolated from the LAN and will run only DMS software. The recommended model for NSGD Monterey is HP Series 700, Model 715/64 (Product No. H00004) with a price of \$5,644. This workstation and all required components should be provided by DISA as part of the DMS infrastructure costs. The cost of the full implementation must be considered to serve all the local commands (Presidio of Monterey, Fleet Numeric Oceanographic Command,

and Naval Postgraduate School) because all three commands can share a common DMS support infrastructure.

C. INSTALLATION OF MISSI COMPONENTS WITH FALCONLAN

The MISSI components required for FalconLan are:

1. PC Card Readers (one per PC)
2. Fortezza Cards (one per person)

The PC Card readers are available as either an external or internal product. The internal PC Card reader is compatible with PCs that support either ISA, EISA, VESA, and/or PCI buses. The external product is either SCSI or Parallel. The available products are listed in Table 4.

Product No.	Product Description	Unit Price
H00013	External SCSI ARGUS/2100-2	\$194.00
H00014	External Parallel ARGUS 2000-2	\$159.00
H00015	ARGUS 2150	\$80.00

Table 4. PC Card Reader Options

The recommended option is the internal PC Card reader, which would take the place of the 5 1/4" floppy drive of each PC and allow for Fortezza card access in the front of the PC.

Every individual at the command will require a Fortezza card. These cards are \$69.50 each.

V. RECOMMENDATIONS AND CONCLUSIONS

A. RECOMMENDATIONS TO PROGRAM MANAGERS FOR SYSTEM MATURATION

The program managers must ensure that new technologies and standards are fully explored to determine what is best for the future of the Defense Messaging System. New technologies are emerging at an increasingly rapid pace and the DoD must review these technologies to see which will best meet the future needs of the DoD.

B. AREAS FOR FURTHER STUDY

There are two main areas that remain for further study of this topic:

1. Providing the best allocation of infrastructure equipment for the Presidio of Monterey, the Naval Postgraduate School, and Fleet Numeric Oceanography Command.
2. Performing software reliability testing of the DMS certified compliant products to determine their reliability.

C. CLOSING REMARKS

This thesis can be extended to any command's Local Area Network to implement the DMS using MISSI. However, DISA must provide further guidelines for Local Area Network Installation teams to ensure that the equipment purchased (e.g., hardware, software, and network operating systems) will interface with the Defense Messaging System and will allow for growth and expansion. Too often, in top-down driven programs, commands are left waiting for equipment and training so long that they go out and do it themselves. This creates

integration and compatibility problems. By allowing commands to purchase the required equipment off of a product list for their network is one solution to the top-down problem. This thesis has provided specific recommendations to the Naval Security Group Detachment in Monterey to ensure that when the DMS reaches final operational capability, they will be prepared to immediately get on board. Additionally, once the DMS has been implemented at NSGD Monterey, it can act as a field site for other commands to see how it was done and then implement their own Local Area Networks that interface with the DMS and use MISSI.

APPENDIX. ACRONYMS

Acronym	Definition
ADUA	Administrative Directory User Agent
AOIC	Assistant Officer In Charge
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
AUTODIN	Automatic Digital Network
BMTA	Backbone Message Transfer Agent
CAW	Certification Authority Workstation
DDN	Defense Data Network
DIB	Directory Information Base
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agent
DISN	Defense Information System Network
DIT	Directory Information Table
DMS	Defense Messaging System
DoD	Department of Defense
DSA	Directory System Agent
DSS	Digital Signature Standard
DUA	Directory User Agent

EC	Electronic Commerce
EDI	Electronic Data Interchange
FOC	Final Operational Capability
FTP	File Transfer Protocol
GUI	Graphical User Interface
IETF	Internet Engineering Task Force
INE	In-Line Network Encryption
IP	Internet Protocol
LAN	Local Area Network
MA	Management Agent
MFI	Multifunction Interpreter
MHS	Message Handling Service
MIME	Multipurpose Internet Mail
MISSI	Multilevel Information Systems Security Initiative
ML	Mail List
MLA	Mail List Agent
MLM	Mail List Manager
MLS	Multilevel Security
MOSS	MIME Object Security Service
MROC	Multicommand Required Operational Capability
MS	Message Store

MSP	Message Security Protocol
MTA	Message Transfer Agent
MTS	Message Transfer System
MW	Management Workstation
MWS	Management Workstation
NATO	North Atlantic Treaty Organization
NCSC	National Computer Security Center
NSA	National Security Agency
NSGD	Naval Security Group Detachment
OIC	Officer In Charge
OSI	Open Systems Interconnection
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PUA	Profiling User Agent
RSA	Rivest-Shamir-Adelman
SBU	Sensitive But Unclassified
SCSI	Small Computer Systems Interface
SHA	Secure Hash Algorithm
SMTA	Subordinate Message Transfer Agent

SMTP	Simple Mail Transfer Protocol
SNS	Secure Network Server
TCP	Transmission Control Protocol
TS	Top Secret
UA	User Agent
UUCP	Unix to Unix Communications Protocol
WAN	Wide Area Network
WWW	World Wide Web

LIST OF REFERENCES

- AT&T WWW Homepage (<http://www.nafta.net/attels.html>), February, 1996.
- Cheswick, W., and Bellovin, S., *Firewalls and Internet Security : Repelling the Wily Hacker*, Reading, MA.: Addison Wesley Publishing Company, 1994.
- Cooney, R. and Bilinski, G., "The Multilevel Information Systems Security Initiative," Chips Online, July 1995. (<http://www.chips.navy.mil>).
- FitzGerald, J., *Business Data Communications : Basic Concepts, Security, and Design*, New York, N.Y.: John Wiley & Sons, 1993.
- Hice, G.F. and Wold, S.H., *DMS : Prologue to the Government E-mail Revolution*, Bethesda, MD.: J.G. Van Dyke & Associates, Inc., 1995
- Joint Chiefs of Staff, MJCS-20-89, "Multicommand Required Operational Capability for the Defense Message System," MROC 3-88, 6 February 1989, Change 1, 4 August 1993. (<http://www.itsi.disa.mil/dmshome.html>).
- Loral Federal Systems, "DMS Product Guide," Manassas, VA, 1995. (1-800-HLP-DMSG)
- Malamud, C., *Stacks : Interoperability in Today's Computer Networks*, Englewood Cliffs, N.J.: Prentice Hall, Inc., 1992.
- Paige, E. Jr., Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), "Electronic Mail (E-mail) Policy," October 13, 1992.
- Paige, E. Jr., Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), "Guest editorial," Chips Online, January, 1996. (<http://www.chips.navy.mil>).
- Philbin, M., "Planning for DMS - POM 98," CHIPS Online, January, 1996. (<http://www.chips.navy.mil>).
- Pfleeger, C.P., *Security in Computing*, Englewood Cliffs, N.J.: Prentice Hall, Inc., 1989.
- Security Study Committee (David D. Clark, Chairman), National Research Council, *Computers at Risk : Safe Computing in the Information Age*, Washington, D.C.: National Academy Press, 1991.

INITIAL DISTRIBUTION LIST

- | | | |
|----|--|---|
| 1. | Defense Technical Information Center
8725 John J. Kingman Rd., STE 0944
Ft. Belvoir, VA 22060-6218 | 2 |
| 2. | Dudley Knox Library
Naval Postgraduate School
411 Dyer Rd.
Monterey, CA 93943-5101 | 2 |
| 3. | Chairman, Department of Systems Management
Naval Postgraduate School
Monterey, CA 93943-5000 | 1 |
| 4. | Prof. Rex Buddenberg, Code SM/Bu
Department of Systems Management
Naval Postgraduate School
Monterey, CA 93943-5000 | 2 |
| 5. | CDR Gus Lott, Code EC/Lt
Department of Electrical and Computer Engineering
Naval Postgraduate School
Monterey, CA 93943-5000 | 2 |
| 6. | Michael J. Mestrovich, Ph.D.
Deputy Director, Joint Requirements Analysis and Integration (D-7)
Defense Information Systems Agency
5201 Leesburg Pike, Suite 1501
Falls Church, VA 22041 | 1 |
| 7. | LT Robert L. Marlett
374 G Bergin Drive
Monterey, CA 93940 | 1 |
| 8. | LT Lawrence J. Brachfeld
1-1 Brooke Club Drive
Ossining, NY 10562 | 2 |