COPY

(2)

AD-A231 180

The Defense Message System (DMS) Target Architecture and Implementation Strategy

DTIC
ELECTE
FEB 21 1991
S B D

Prepared By:

Defense Message System Architecture Working Group

Sponsored By:

Office of the Assistant Secretary of Defense

for
Command, Control, Communications and Intelligence
(Information Systems)
Pentagon, Washington D.C.

October 1990

DISTRIBUTION STATEMENT A
Approved for public release
Distribution Unlimited

91 2 21 023

REPORT DOCUMENTATION PAGE

Form Approved
OPM No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources gathering and maintaining the data needed, 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 Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503

1 AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1990	N/A

4 TITLE AND SUBTITLE
Defense Message System Target Architecture and Implementation Strategy

5 FUNDING NUMBERS

6 AUTHOR(S)
Defense Message System Architecture Working Group

7 PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Communications Agency
ATTN: DISM
Washington, DC 20305-2000

8 PERFORMING ORGANIZATION REPORT NUMBER

9 SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of the Assistant Secretary of Defense for Command Control Communications and Intelligence (Information Systems), The Pentagon
Washington, DC 20301

10 SPONSORING/MONITORING AGENCY REPORT NUMBER

11 SUPPLEMENTARY NOTES
POC: Defense Communications Agency
ATTN: DISM
COM 703-285-5226, DSN 356-5226

12a DISTRIBUTION/AVAILABILITY STATEMENT
Approved for Public Release; Distribution is unlimited.

12b DISTRIBUTION CODE

13 ABSTRACT *(Maximum 200 words)*

Originally published in December 1988, this document reflected the Defense Message System (DMS) Target Architecture and Implementation Strategy (TAIS). In keeping with the intent that the DMS TAIS be a "living document," continually updated as requirements, plans, and technology change, this update reflects programmatic activities and architectural progress since the original publication.

This first update of the DMS TAIS has been validated by the Joint Staff and therefore represents the coordinated positions of the Department of Defense (DOD) Services and agencies regarding the DMS. The document's structure has been modified to accommodate this validation process. The body of this update, containing the introduction, baseline and target architecture descriptions, and articulation of the implementation strategy, has been validated by the Joint Staff and is therefore not subject to change without revalidation. The appendices, containing more detailed descriptions of the phased implementation strategy, are subject to change and have therefore been approved by the Joint Staff for planning purposes only.

14 SUBJECT TERMS	15 NUMBER OF PAGES
Defense Message System (DMS)	198
	16. PRICE CODE

17 SECURITY CLASSIFICATION OF REPORT	18 SECURITY CLASSIFICATION OF THIS PAGE	19 SECURITY CLASSIFICATION OF ABSTRACT	20 LIMITATION OF ABSTRACT
UNCLASS	UNCLASS	UNCLASS	NONE

TABLE OF CONTENTS

		Page
Title Page	. . . . .	i
Table of Contents	. . . . .	ii
List of Appendices	. . . . .	v
List of Figures	. . . . .	vi
Preface	. . . . .	vii
Section 1. Introduction	. . . . .	1-1
1.1	Background	
1.2	Scope	
1.2.1	DMS Elements	
1.2.2	DMS Projects	
1.2.3	Messaging Classes	
1.2.4	Architecture	
1.3	Requirement	
1.3.1	General	
1.3.2	Problem	
1.3.3	DMS Operational Requirements	
1.4	Rationale for Change	
1.5	DMS Objectives and TAIS Purpose	
Section 2.	DMS Baseline	2-1
2.0	Introduction	
2.1	AUTODIN	
2.1.1	Components	
2.1.2	Connections	
2.1.3	Concept of Operations	
2.1.4	Comparison to Requirements	
2.2	Electronic Mail on the DoD Internet (E-Mail)	
2.2.1	Components	
2.2.2	Connections	
2.2.3	Concept of Operations	

TABLE OF CONTENTS
Continued

Page

2.2.4 Comparison to Requirements

Section 3. DMS Target Architecture 3-1

3.0 Introduction

3.1 The DMS Message

3.2 Target Architecture
3.2.1 Overview
3.2.2 Message Handling System (MHS)
3.2.3 Directory (DIR)
3.2.4 Management (MGMT)
3.2.5 Security
3.2.6 MSP Gateway (MSP GWY)
3.2.7 Transmission Components

3.3 Classes of Messaging Service

3.4 Concept of Operations
3.4.1 Message Exchange
3.4.2 Organizational Message Exchange

3.5 Impact on Cost and Staffing

3.6 Comparison to Requirements

Section 4. Implementation Strategy 4-1

4.0 Introduction

4.1 Phased Implementation
4.1.1 Phase 1
4.1.2 Phase 2
4.1.3 Phase 3

4.2 Phase Out of Obsolete Elements
4.2.1 Components
4.2.2 Protocols
4.2.3 Formats
4.2.4 Procedures

DTIC COPY INSPECTED

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

TABLE OF CONTENTS
Continued

Page

4.3 Management Structure
4.3.1 Program Oversight
4.3.2 Program Execution

4.4 Component Development

4.5 DMS Compliance

4.6 Test and Evaluation Strategy
4.6.1 Development Test and Evaluation (DT&E)
4.6.2 Certification Testing
4.6.3 Operational Test and Evaluation (OT&E)
4.6.4 Operational Assessment
4.6.5 Testbeds

4.7 Security Policy
4.7.1 DMS Security Certification and Accreditation
4.7.2 DMS Security Policy Guidance

4.8 Organizational Messaging Transition

4.9 Individual Messaging Transition

List of Appendices

		Page
Appendix A.	Phase 1 Implementation	A-1
Appendix B.	Phase 2 Implementation	B-1
Appendix C.	Phase 3 Implementation	C-1
Appendix D.	Acronyms	D-1
Appendix E.	DMS Glossary	E-1
Appendix F.	DMS References	F-1
Appendix G.	DMS TAIS Distribution	G-1

List of Figures

Figure	Title	Page
2-1	1989 DMS Baseline Architecture	2-2
3-1	DMS Target Architecture	3-4
3-2	DMS Message Handling System	3-5
3-3	DMS Directory Services	3-9
4-1	DMS Implementation Strategy	4-2
4-2	DMS Management Structure	4-6
4-3	DMS Working Groups	4-8

Preface

When originally published in December 1988, this document reflected the Defense Message System (DMS) Target Architecture and Implementation Strategy (TAIS), as coordinated by the Defense Message System Implementation Group (DMSIG) and approved by the DMS Panel. In keeping with the intent that the DMS TAIS be a "living document", continually updated as requirements, plans, and technology change, this update reflects programmatic activities and architectural progress since the original publication.

This first update of the DMS TAIS has been validated by the Joint Staff and therefore represents the coordinated positions of the Department of Defense (DoD) Services and agencies regarding the DMS. The document's structure has been modified to accommodate this validation process. The body of this update, containing the introduction, baseline and target architecture descriptions, and articulation of the implementation strategy, has been validated by the Joint Staff and is therefore not subject to change without revalidation. The appendices, containing more detailed descriptions of the phased implementation strategy, are subject to change and have therefore been approved by the Joint Staff for planning purposes only.

This document is authorized for unlimited distribution throughout Government and Industry. See Appendix H for distribution information. Reproduction of this document in whole or part is authorized. Recommended changes and other comments to this document are welcome and should be forwarded to the address provided below.

For industry recipients: This document is provided for information only and should not be considered a solicitation. Written inputs from industry are welcome but will be used for planning purposes only. The Government does not intend to award a contract based on this document (to include subsequent updates) or otherwise pay for inputs submitted by industry as the result of this document.

Defense Communications Agency
ATTN: Code DISM
Washington, D.C. 20305-2000

Section 1

Introduction

1.1 Background.

A Multi-Service and agency Defense Message System Working Group (DMSWG) was formed by ASD/C3I in January 1988 to assess the future of DoD's messaging systems. Primary objectives were to define the baseline DMS and 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. Secondary objectives were improvements in functionality, survivability and security. Using inputs from Government and industry, and capitalizing on technological and standards advances, the DMSWG formulated a DMS target architecture and the transition phases necessary to evolve from the baseline to the target. Following conceptual approval of the DMS target architecture, and transition approach by the C3I Systems Committee of the Defense Acquisition Board (DAB) in May 1988, the Under Secretary of Defense for Acquisition, USD(A), issued DMS Program Guidance in August 1988. The USD(A) Program Guidance provided approval of the DMS target architecture, phased implementation strategy, test and evaluation strategy, and management structure; tasked the Defense Communications 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.

Following receipt of the DMS Program Guidance, the DMS management structure depicted in Section 4 of this document was fully activated by October 1988. The initial Target Architecture and Implementation Strategy (TAIS) document was approved for release, published, and distributed to Government and industry in December 1988. In February 1989, the validated Multi-command Required Operational Capability for the Defense Message System (DMS MROC 3-88), was implemented by Joint Staff. 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.

1.2 Scope.

by the Defense Message System (DMS).

The DMS consists of all hardware, software, procedures,

standards, facilities, and personnel used to exchange messages electronically between organizations and individuals in the Department of Defense (DoD). The current subsystems of the DMS are the AUTODIN (including baselevel support systems) and electronic mail on the DoD Internet. The DMS also includes interfaces for tactical and allied systems, but does not include those systems. While the DMS is a system in the sense that its components work together to provide messaging services, it is, and will continue to be, the composite result of many coordinated Service and agency development and acquisition projects.

1.2.1 DMS Elements. The elements of the DMS are policies, procedures, standards and components, where a component is the existing and proposed hardware and software implementation of a messaging application(s).

1.2.2 DMS Projects. DMS projects are organized efforts to document, evolve, acquire, and deploy DMS elements. DMS projects fall into the categories of central, joint, or user-unique.

a. Central Project. DMS Central projects support the core architecture and all users of the DMS. In general, they can be characterized as backbone components or major policies and standards which deal with message exchange protocols and formats, security, and directories. Examples of central projects and components in the baseline are Defense communications System (DCS) Mode I protocol, ACP 117 CAN-US SUPP-1, the Message Address Directory (MAD), the AUTODIN backbone and electronic mail service via the DDN. Since central DMS projects and components support all users, the active participation and support of all Services and agencies in their development, testing and deployment is necessary. DMS central projects will receive a high priority from Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD/C3I) in terms of funding support because of their critical importance to the success of the DMS. These projects are appropriate for funding through the Communications Services Industrial Fund (CSIF) and are subject to all CSIF requirements. Only those activities that are totally dedicated to the acquisition, testing, deployment, operation and maintenance of DMS central projects will be funded through the CSIF.

b. Joint Project. These are individual Service agency projects that show maximum likelihood of satisfying operational needs within other Services and agencies and advancing the DMS architecture. Support of these projects will reduce duplication of development efforts and promote standardization of components. Examples of opportunities for joint projects in the baseline are the replacements for the Standard Remote Terminal (SRT), Digital Subscriber Terminal Equipment (DSTE), and Digital Communications

Terminal (DCT) 9000 equipments. Projects designated as joint will enjoy a higher priority in funding support than user-unique projects because they will have the greater potential for cost reduction and/or widespread benefit for multiple Service and agency users. DMS joint and user unique projects do not qualify for CSIF funds.

c. User-Unique Project. DMS user-unique projects are developed or acquired by a single Service or agency to satisfy unique operational requirements. They will conform to the intent of DMS architectural guidelines, except where dictated by unique requirements. Examples of user-unique projects and components in the baseline include use of office codes in message preparation, procedures for message distribution, the Service and agency AMPEs, implementation of local area networks and Automated Message Handling Systems (AMHSs), Remote Information Exchange Terminal (RIXT) and Modular AMME Remote Terminal (MART) software for the SRT, all unique AUTODIN interfaces and terminals in use at TCCs, and electronic mail hosts on the DDN.

1.2.3 Messaging Classes: The mission of the DMS is to handle every message in a manner appropriate to its content. The term "message" is defined in ACP 167, "Glossary of Communications - Electronics Terms", to be "any thought or idea expressed briefly in plain or secret language, prepared in a form suitable for transmission by any means of communications". In the DMS context, the means of communications is restricted to common-user electronic methods. In order to handle every message in a manner appropriate to its content, two message classes are currently identified for inclusion in the DMS; however as the system and its underlying technology evolve, additional messaging service classes may be required.

a. Organizational: This class includes command and control messages and communications exchanged between organizational elements. These messages require approval for transmission by designated officials of the sending organization and determination of internal distribution by the receiving organization. Because of their official and sometimes critical nature, such messages impose operational requirements on the communications systems for capabilities such as non-routine precedence, guaranteed timely delivery, high availability and reliability, and a specified level of survivability and security.

b. Individual: This class includes working communications between individual DoD personnel within administrative channels, both internal and external to the specific organizational element. Such messages do not generally commit or direct an organization. Messages requiring only a basic transport service will be treated as a part of this class. The driving

requirements on the communications system for this class of messages are connectivity down to the user level and ease of use.

1.2.4 Architecture. The DMS architecture is that subset of the DoD Integrated Communications Architecture (ICA) dealing with DoD messaging. It includes all components involved in DoD messaging from writer to reader, with the exception of the transmission systems providing connectivity such as the Defense Data Network (DDN) and the baselevel transmission facilities. The broad scope of the DMS architecture requires some clarification from an organizational and management standpoint. The baseline DMS contains both Defense Communication System (DCS) components such as the AUTODIN Switching Centers (ASCs) and non-DCS components such as the baselevel Telecommunications Centers (TCCs). As the DMS evolves from the baseline to the target, the current DCS/non-DCS distinction is subject to change as the target architecture is implemented. Determination of operational direction and management control responsibilities will be required on a component-by-component basis based upon whether it falls under one of the following categories: central, joint or user unique.

1.3 Requirement.

1.3.1 General. The DoD requires an improved message communications system based upon evolutionary upgrades to the current collection of systems. This system, based upon MROC 3-88, should be organized under a common architectural context and a clear and well defined implementation strategy. It should be centered around the principles of standardization and interoperability, while preserving adaptability for implementing Service and agency unique functionality and customization.

1.3.2 Problem. The major components of the current baseline are the AUTODIN system (to include the baselevel), providing message service between organizational elements, and E-Mail providing message service between individuals (staff personnel). While both components provide messaging service to DoD users, their disjointedness precludes the interoperability required to allow a rationalization of message traffic and the directed migration of interactive data exchanges from AUTODIN to DDN. Further, functional deficiencies with both components cause the services provided to users to be less than optimum. At the AUTODIN baselevel, obsolete equipment results in high maintenance cost and service degradation. The current TCC method of providing service is staffing intensive and results in message service delays to writers and readers. E-mail suffers from a lack of both security features and service standardization. The Inter-Service/Agency Automated Message Processing Exchange (I-S/A AMPE) was aimed at resolving some of these problems and its termination has invalidated the Integrated AUTODIN System (IAS)

architecture. Complicating matters, multiple Service/agency (S/a) architectures have been formulated to resolve baselevel problems. The result is that DoD had no overall future messaging architecture.

1.3.3 DMS Operational Requirements. The specific requirements for the DMS are quoted from the draft Multi-command Required Operational Capability (MROC) 3-88. The requirements are stated from the perspective of writers and readers, independent of specific implementations to allow the flexibility for multiple solutions and satisfaction of Service/agency unique applications.

a. Connectivity/Interoperability.

(1) The DMS should allow a user to communicate with any other user within the DMS community. The community of users includes organizations and personnel of the Department of Defense. In addition, the DMS must support interfaces to systems of other government agencies, allies, tactical and defense contractors. System users may be fixed, mobile or transportable.

(2) Connectivity must extend from writer to reader. Messages should be composed, accepted for delivery, and delivered as close to the user as is practical. Current efforts, such as extension of automation to users and improved base level message distribution systems, are responsive to this requirement.

(3) The DMS must be interoperable with and provide standard interfaces for tactical and allied systems. It should lead DoD's migration to international standards and protocols.

b. Guaranteed Delivery/Accountability.

(1) The DMS must, with a high degree of certainty, deliver a message to the intended recipient(s). If the system cannot deliver a message, a method of promptly notifying the sender of the non-delivery must be available.

(2) For organizational message traffic, the DMS must have the capability to maintain writer-to-reader message accountability.

c. Timely Delivery. The DMS must recognize messages that require preferential handling. The urgency of the most critical information requires handling above and beyond simple priority. The DMS must dynamically adjust to changing traffic loads and conditions to provide timely delivery of critical information during peacetime, crisis, and war. Delivery time for a given message will be a function of message precedence and system stress level.

d. Confidentiality/Security. Confidentiality precludes access to or release of information to unauthorized recipients. The DMS must process and protect all unclassified, classified and other sensitive message traffic at all levels and compartments. The DMS must maintain separation of messages within user communities to satisfy confidentiality. Security is based upon requirements for integrity and authentication as well as confidentiality.

e. Sender Authentication. The DMS must unambiguously verify that information marked as having originated at a given source did in fact originate there. For organizational traffic, a message must be approved by competent authority before transmission.

f. Integrity. Information received must be the same as information sent. If authorized by the writer, the DMS may make minimal format changes to accommodate differences in capabilities between the component systems serving the writer and the reader. However, the DMS must ensure that information content of a message is not changed.

g. Survivability. The DMS must provide a service as survivable as the users it serves. It must not degrade the survivability of systems interfaced to it. Methods such as redundancy, proliferation of system assets, and distributed processing may be employed. Surviving segments of DMS must be capable of reconstitution.

h. Availability/Reliability. The DMS must provide users with message service on an essentially continuous basis. The required availability of the DMS should be achieved by a combination of highly reliable and readily maintainable components, thoroughly tested software, and necessary operational procedures.

i. Ease of Use. The DMS must be flexible and responsive enough to allow user operation without extensive training. Use of the DMS should not require the knowledge of a communications specialist.

j. Identification of Recipients. The sender must be able to unambiguously identify to the DMS the intended recipient organizations or individuals. The necessary directories and their authenticity are part of the DMS.

k. Message Preparation Support. The DMS must support user-friendly preparation of messages for transmission, to include services such as U.S. Message Text Format (USMTF) assistance.

l. Storage and Retrieval Support. The DMS must support storing messages after delivery to allow retrieval for such purposes as readdressal, retransmission, and automated message handling functions such as archiving and analysis, with the capability of incorporating segments into future messages. The minimum storage period for organizational messages will be specified by Allied Communications Procedures.

m. Distribution Determination and Delivery.

(1) For organizational message traffic, the DMS must determine the destination(s) of each message (in addition to the addressee(s) specified by the originator) and effect delivery in accordance with the requirements of the recipient organization.

(2) For individual message traffic, the DMS must effect delivery of each message to the individual(s) specified by the originator.

1.4 Rationale for Change.

Change is mandated by the problems and costs of the current messaging systems, lack of an overall DoD messaging architecture, and the emergence of new international standards and technology. The current AUTODIN and DoD Internet electronic mail messaging systems are expensive and staffing intensive. Even with this high cost, they do not provide the required levels of user writer-to-reader service and satisfaction. Previous efforts to improve DoD's messaging systems have met with limited success. This was due in large part to multiple, uncoordinated implementation strategies that have fostered maintenance of multiple DoD messaging technologies and have assumed that existing formats, procedures (to include manual operations) and interfaces between systems must continue. These old strategies resulted in a paralysis that promoted the continuation of "business as usual" and denied DoD-wide economic and user service benefits that can be realized with newer technology and international standards. Recently imposed DoD budget constraints, rapid advances in both messaging technology and international messaging standards, industry's movement to these standards, and recognized problems with the current systems, provide a strong impetus for change. By coupling improved technology and new standards with needed improvement in DoD's acquisition strategy, the DMS provides the opportunity to improve writer-to-reader service at lower cost and staffing.

1.5 DMS Objectives and TAIS Purpose.

The primary objective of the evolutionary DMS program is to reduce cost and staffing while maintaining the existing levels of

service and security. A secondary objective is to improve both service and security. To achieve these objectives, it is necessary to identify and document a baseline from which proposed DMS costs and benefits can be measured, a target architecture that will satisfy all validated requirements, and an implementation strategy that will be used for evolution from the baseline to the target. The TAIS has been coordinated with the Integrated Communications Architecture (ICA) Planning and Guidance document development to insure mutual consistency. This TAIS, validated by the Joint Staff, describes the coordinated Service and agency DMS position.

Section 2

DMS Baseline

2.0 Introduction.

The DMS baseline consists of the Automatic Digital Network (AUTODIN) and electronic mail on the DoD Internet 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. It is depicted in Figure 2-1.

2.1 AUTODIN.

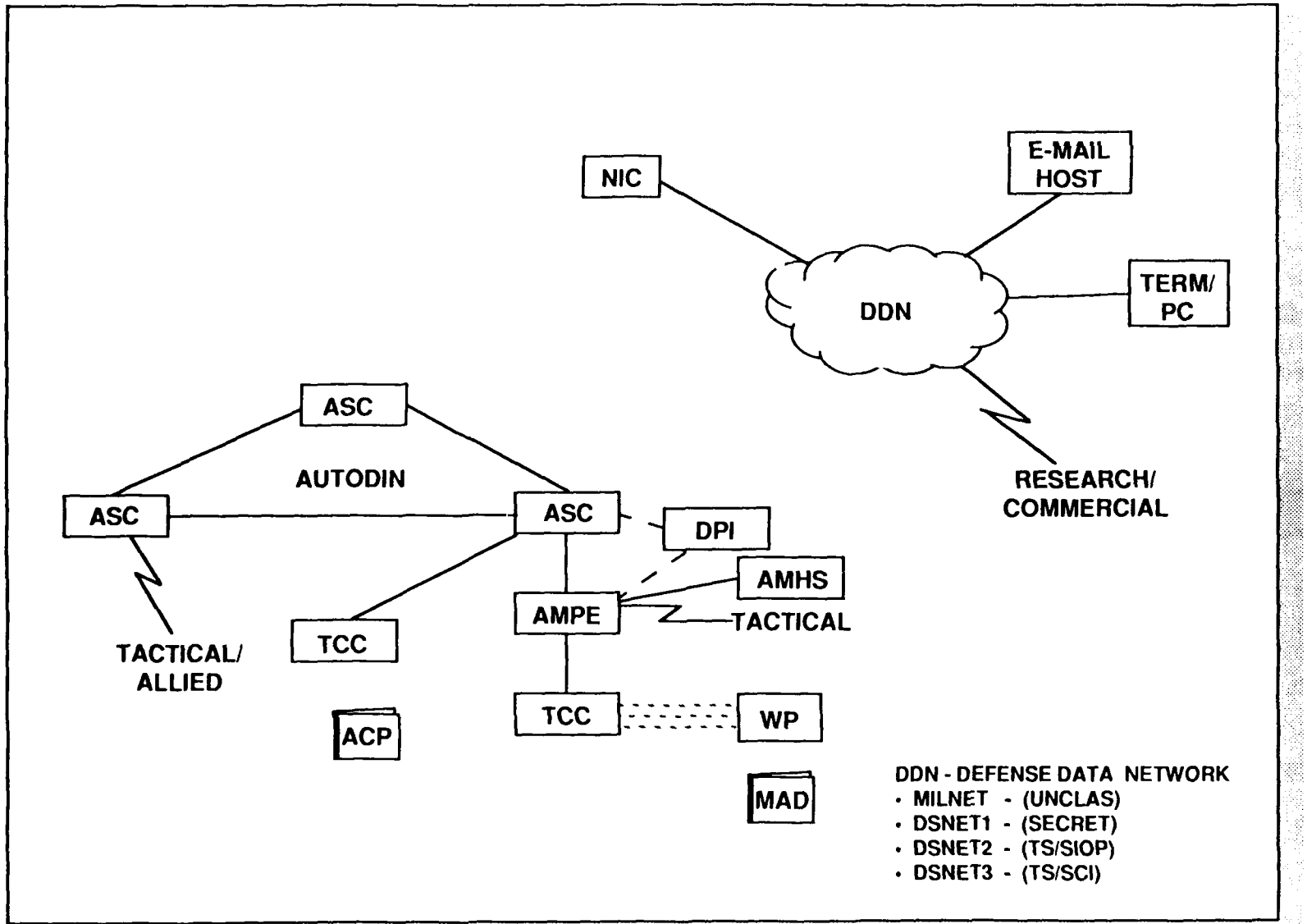
AUTODIN was established in the 1960s to provide secure, automated store-and-forward message service to meet the operational requirements of the Department of Defense.

2.1.1 Components. The principal components of the existing organizational message system are the backbone store-and-forward message switches, Service and agency (S/A) store-and-forward processing facilities, a variety of terminating facilities (message source and destination points), special data pattern processing facilities, special purpose narrative message facilities, and paper-based directory services, and operating procedures which are promulgated in Allied Communications Publications (ACPs), Joint Army Navy Air Force publication (JANAP) 128, and Defense Special Security Communications System (DSSCS) Operating Instructions (DOIs).

a. AUTODIN Switching Centers (ASCs). There are 15 operational ASCs distributed throughout the world and two test ASCs. The ASCs perform store-and-forward message switching functions, some message validation functions, format conversion, and some specialized routing functions.

b. Automated Message Processing Exchanges (AMPEs). There are over 100 AMPEs which include Army's Automated Multi-Media Exchange (AMME), Navy's Local Digital Message Exchange (LDMX), Air Force's Air Force Automated Message Processing Exchange (AFAMPE), NSA's STREAMLINER, and DIA's Communications Support Processor (CSP). The AMPEs provide a concentrator and limited switching functions for attached terminals, plus other functions such as conversion of destination names (Plain-Language Addresses [PLAs]) into internal AUTODIN addresses (Routing Indicators

Figure 2-1. BASELINE ARCHITECTURE



[RIs]), and distribution determination of messages based on a variety of criteria, which may differ for different types of AMPEs. Some of the AMPEs (e.g., AMMEs) are obsolete to the point that the required maintenance effort is costly and incorporation of enhancements is difficult.

c. Telecommunications Centers (TCCs). TCCs are the principal entry and exit points for AUTODIN messages. TCCs contain, or are associated with, administrative message centers which conduct over-the-counter (OTC) operations. A variety of terminal equipment types are used, some specifically designed for AUTODIN while others are standard commercial equipment used with special AUTODIN Interface Devices (AIDs). Narrative messages are generally entered from paper DD Form 173 originals via optical character readers, though some TCCs manually prepare messages on Video Display Terminals (VDTs), punched paper tape or 80 column cards. Additionally, automated message preparation and entry support (including preformatted messages, message masks, etc.) is provided by some systems, by means of VDTs either in the TCC or in the user's work area. Data pattern messages which are transmitted by a TCC (as opposed to those entered directly into AUTODIN from a data processing center) are generally entered from magnetic tape. Some TCCs are beginning to phase in floppy disk as an input/output media for both narrative and data pattern messages. Much of the equipment in the TCCs is obsolete to the point that the required maintenance effort is costly and the age of many of the systems makes it difficult to implement modifications and enhancements to the system hardware or software. As a result, enhancements to extend automation to users and to reduce the manual, staff intensive, operations within the TCCs have been limited.

d. Data Processing Installations (DPIs). Some DPI computers have automated interfaces to AUTODIN (either directly to an ASC or via an AMPE). These interfaces are generally used to send and receive data, rather than narrative messages.

e. Automated Message Handling Systems (AMHSs). Some users have implemented or are implementing components which assist in the automated processing of messages, including message coordination and release, storing, sorting and retrieving messages for various purposes after receipt, and electronic mailbox distribution schemes.

f. Directories (DIR). Directories are distributed as paper documents. The Message Address Directory (MAD) contains organization names and associated Plain Language Addresses (PLAs). The ACP 117 series of publications includes PLAs with assigned routing indicator listings.

g. Specialized User Terminals. Below the level of TCCs, AUTODIN has a number of user terminals which support a single organization (as opposed to a TCC which may support one or more organizations), and which generally are operated by the users (as opposed to being operated by communications personnel). These terminals often support missions which have limited communications requirements, in terms of volume and distribution of traffic. As a result, relatively slow and inexpensive terminal equipment can be utilized to support these requirements.

2.1.2 Connections. Essentially, all equipment connection in AUTODIN is via dedicated transmission lines protected with separate link encryption equipment. ASCs are multi-connected, with a total of 71 trunk lines connecting the 15 ASCs. Trunk line speed is usually 4800 bps with 2400 and 1200 bps also used. There are currently about 1300 terminals (including AMPEs and DPIs) directly connected to the switches. There are about 1000 additional terminals connected to the backside of AMPEs. Terminal line speeds vary from 45 to 4800 bps. ASC connectivity with the tactical community as well as with the Allied and commercial refile communities is via tailored interfaces. Further, tactical units such as Navy afloat commands, communicate with AMPE systems via tailored interfaces.

2.1.3 Concept of Operations. The following is a typical message processing scenario. A message is prepared off-line on a DD Form 173 with a special OCR font. If not already known from previous messages, the preparer determines the PLAs of the intended recipients from the MAD. The message is signed by a designated release authority for the sending organization and carried to the local TCC. The TCC operator checks the DD Form 173 for a signature authorizing release. The message is entered into the terminal via an OCR where it is reformatted in accordance with the ACP 127 or JANAP 128 publication which describes the format for electrical transmission. If the terminal cannot perform PLA to RI conversion or is not connected to an AMPE (which does PLA to RI conversion), the operator looks up the PLAs in ACP 117 and enters the RIs onto the message, together with the Originating Station Routing Indicator (OSRI), the Originating Station Serial Number (OSSN), and the Time of File (TOF). If there is no OCR, then the operator manually reformats and keys in the message. The message is then transmitted electronically using an AUTODIN specific protocol. At either the AMPE or ASC, the first several lines of the message are validated and if there are no errors the message is accepted and processed as required to effect delivery to the addressee(s); messages (known as service messages) are returned to the TCC operator, indicating the nature of any errors encountered. If the receiving device is an AMPE, PLA-to-RI conversion is performed, if required, and the message is sent to an ASC, and any local deliveries are made. The ASC makes

delivery to its directly connected terminals, determines the destination ASCs and makes delivery to the "next hop" ASCs. One copy of the message is sent to each "next hop" ASC, with only those RIs for which each "next hop" ASC has routing responsibility. This process is repeated until the message is delivered to all recipient terminals. At the recipient terminal, multiple copies of the message may be produced based on a number of distribution criteria, such as office codes indicated by the preparer as additions to the receiving organization's PLA, the subject matter of the message, content indicator codes, NATO Subject Indicator Codes, or even the contents of the message text, dependent upon the operational requirements of the users supported by the recipient terminal. This message distribution determination may be done manually or may be automated in the receiving AMPE or terminal. The messages are then distributed to the actual recipients through normal administrative channels. While this is the basic concept of operations, there are a number of special actions which may occur, and many details that support user unique operational requirements have been omitted. The most important of these will be described in comparing the AUTODIN service to the DMS requirements.

2.1.4 Comparison to Requirements.

a. Connectivity/Interoperability. The roots of AUTODIN as a military system cause it to place heavy emphasis on "commander-to-commander" communications, and the MAD, the Joint Staff authorized directory for organizational messaging, extends only to that level of addressing. For example, the Secretary of Defense, together with the Office of the Secretary of Defense (OSD) (about 1900 people), has a single entry: SECDEF WASHINGTON DC. Since the number of messages received daily by the Secretary and OSD is on the order of 1200 to 2000, it is clearly impractical to expect the personal attention of the Secretary or even his immediate staff. A similar situation exists at any large military command. As a result, a number of locally standardized approaches are taken to reach the appropriate recipients. The most common of these is to include staff element identifiers with each PLA. This approach is specified by Service/agency message preparation formats and instructions, and is generally used as one of the methods to distribute messages. The staff element identifiers (office symbols) are not standard across Military Services and Defense Agencies, and their use may be different on messages which cross S/A boundaries. The result is that connectivity between commanders is essentially complete, although generally handled manually at both ends. Connectivity between lower elements of the organization, and even individuals, via "for" instructions in the message text, is accommodated. However, the manual operations and distribution efforts required at most TCCs can introduce substantial delays in communications

between organizational elements.

b. Guaranteed Delivery. From entry into the sending TCC to initial delivery at the receiving TCC, AUTODIN takes many measures to avoid losing messages, and, in the unlikely event a message is lost, to inform the sender so that the message can be retransmitted. Messages are initially logged at the TCC, stored redundantly at the ASC or AMPE at which they are first received, and not acknowledged to the TCC until such storage is complete. Similar positive acknowledgments are required on each store and forward stage until final delivery to a TCC. Finally, if any destination TCCs are unable to deliver the message, the originating TCC is notified. There are problems, however, in the manual stage of the process at the sending and receiving ends. Feedback on errors may not be immediate, dependent upon the priority of the message. As a result, format errors may cause the messages to be sent back to the originator through normal distribution channels, and messages will be delayed or even lost in this process. On the receive end, the limitations in connectivity discussed earlier, and the lack of extension of automation, may cause messages to be distributed to the wrong user(s) within the recipient organization, with the potential for delays or even loss of some messages.

c. Timely Delivery. AUTODIN uses multi-level precedence to assure timely delivery of high priority messages. Many special actions are taken to assure very rapid delivery to the actual user (rather than a distribution box at the TCC) for the highest precedence messages: (1) alternate routing (including to alternate destination TCCs) is used to bypass failed components; (2) preemption of messages in process is employed on input/output lines, and internally if necessary; (3) messages which would otherwise be rejected are marked as potentially flawed and delivered anyway; (4) alarms ring on receipt to get the operator's attention; (5) twenty-four hour a day staffing of the TCCs is provided to assure rapid response; (6) procedures at the receive end assure that the commander or duty officer is immediately notified of receipt. Total TCC-to-TCC time for high precedence traffic is no more than a few minutes. However, manual procedures at both ends may add substantially to the actual writer-to-reader time. Also, lower priority messages are given less extraordinary service, and a large volume of high precedence messages may delay the receipt of the lower priority messages at the TCC. Under extreme circumstances (e.g., high traffic volumes and a large number of high precedence messages) AMPEs or TCCs may remove routine messages from the system and mail them to the recipients. Portions of the AUTODIN also support perishable traffic, e.g., traffic (such as time-sensitive weather data) which the originator has requested to be removed from the system without delivery if it is not delivered within a

certain time frame.

d. Confidentiality/Security. All transmission lines in AUTODIN are required to be protected with military encryption equipment. There are also physical safeguards employed to insure message/community separation. For example, patch panels are segregated from each other and different size Jack Sets are used to segregate GENSER from DSSCS users. Tip/Ring reversal is used within Jack Sets to segregate Non-US subscribers to preclude mispatching a GENSER subscriber into a NATO or other foreign subscriber Jack Set. Terminals are identified by community of interest and classmarked with the security levels they are allowed to process. Messages in ASCs, AMPEs, and some terminals are checked for valid security levels prior to acceptance and before delivery. A variety of measures, including parity and block checksums and header/trailer sequence numbers on messages, are taken to maintain separation of messages. Software in the ASCs is extensively tested before release. Software, hardware, and procedures for AMPEs and TCCs are subject to a standard independent test before they are connected to AUTODIN, in addition to accreditation procedures of the owning organization. The resulting AUTODIN system is accredited for all levels of classified information although some terminal equipment and many TCCs are only authorized to receive certain levels of information. Much of the security is provided by procedures and by personnel security (e.g., TCC operators are typically cleared for the highest level of information authorized the TCC). Equipment is generally dedicated to AUTODIN.

e. Sender Authentication. The signature of the release authority on a message is checked before it is forwarded to the TCC for transmission. In most cases, physical access to a TCC is controlled and appropriate identification is required.

f. Integrity. Within the system, and on most access lines, integrity is maintained by matching header and trailer sequence numbers, and character and block parity checks. Some code conversion will occur, e.g., from 8-level ASCII to 5-level ITA-2, unless prohibited by the sender. Asynchronous lines, especially those using ITA-2 line code (which includes no character parity) may introduce errors which go undetected by the system. Another source of errors are the OCRs which occasionally misread a character on the DD Form 173.

g. Survivability. The AUTODIN backbone (15 ASCs and their interswitch trunks) incorporates redundant interswitch routing, with each ASC multiply connected to other ASCs. ASCs also are provided with the capability of restoring Interswitch Trunks over AUTOVON lines. The routing between ASCs is switchable (under the control of the ASC operators) to deal with the failure of one or

more ASCs. However, the backbone is not considered survivable and almost every stress scenario presumes the loss of some to all of the backbone, isolating surviving AMPEs and terminals. The AMPEs and terminals depend upon the AUTODIN for long-haul communications. Therefore, selected AUTODIN terminals and most AMPEs are connected to multiple ASCs. Additionally, selected AMPE subscribers are also multiply connected.

h. Availability/Reliability. Substantial equipment redundancy, 24-hour staffing, back-up power, uninterruptable power systems (UPS), alternate routing, multiple connectivity of ASCs, multiple connectivity between ASCs and AMPEs/TCCs, and redundant storage of messages are employed to provide very high availability and reliability in peacetime. The AUTODIN availability under stressed conditions is subject to its survivability.

i. Ease of Use. A few hours cf training is required to prepare the usual AUTODIN message on a DD Form 173, and the actual entry of messages into AUTODIN at a TCC is normally done by trained operators. However, increased automation of TCCs, and extension of automation to users (in the form of pre-prepared message masks and other message preparation support) can reduce the amount of training required for users and can reduce the number/training level of TCC operations personnel. The TCC and other AUTODIN communications and cryptographic equipment is maintained by trained maintenance personnel, though the use of more modern equipment is reducing the numbers and training levels of these maintenance personnel.

j. Identification of Recipients. As indicated earlier, the MAD provides the address information required for commander-to-commander messages. While organizational element identifiers (office symbols) are widely used, there is no DoD-wide standard method for identifying recipients below the commander level. Users tend to build up a list of organizational element identifiers for those elements with whom they communicate routinely, and use those identifiers to address the majority of their messages. In other cases, the message is sent to the intended recipient's commander for further distribution determination and delivery. While the intent is to give the receiving commander the flexibility to determine the appropriate organizational elements for action and information, the practical effect is that two types of possible errors may occur; some messages are delivered to recipients who have no interest in the message and some messages are not delivered to interested organizational elements. Additionally, extra copies of messages may be distributed to ensure delivery to interested elements. Procedures are in place to prevent delivery of copies to users not cleared for them.

k. Preparation Support. The amount of message preparation support provided to users varies from virtually no support (other than the use of preprinted DD Forms 173), to office automation equipment/software which supports the proper placement of fields on DD Forms 173, to message editing/preparation terminals (connected to AMPEs) which provide the user with menu-oriented or mask-oriented support of message preparation. While there are no inherent limitations to such user support within the system, at the present time much of the support comes only at the level of office automation equipment/software. AMHS type systems may also be used for message preparation.

l. Storage and Retrieval Support. The ASCs and AMPEs store messages for retrieval. The ASCs may retrieve messages only for redelivery to the original recipients. The AMPEs may retrieve messages for redelivery to the original recipients and for readdressal to other recipients. AMHSs store messages and permit a range of operations, such as sorting, analysis, and editing into new messages. Full integration of AMHSs into AUTODIN is not complete.

m. Distribution Determination and Delivery. At many TCCs, especially lower volume TCCs, message distribution is determined manually. Messages are examined for staff element identifiers, subject matter, key words in a key word field (a NATO requirement), and key words in the text. The next step is to make copies of the messages and put them into distribution bins. At some AMPEs and TCCs, the above procedures are automated. Finally, administrative personnel pick up and deliver the messages to the intended recipients. AMHSs take a somewhat different approach. Users have profiles based on the same elements used by AMPEs, but rather than using these to cause delivery of the messages, only a notification of receipt is placed in a user accessible file. The user can then choose to read the message at a CRT, print it, or delete it based on no interest.

2.2 Electronic Mail on the DoD Internet (E-Mail). The Defense Data Network (DDN) was established in 1982. It is a set of world-wide networks based on technology developed by the Defense Advanced Research Projects Agency (DARPA) as the ARPANET in the early 1970s. A major use of the ARPANET was providing electronic mail to the DoD research community. This capability was extended to other operational users on the DDN. At about the same time the DDN was established, the protocols in use were expanded to facilitate connection of baselevel transmission facilities (including local area networks) to wide-area networks such as the ARPANET and the new DDN networks. Collectively, the long-haul and baselevel transmission facilities are termed the DoD

Internet.

2.2.1 Components. The principal components of the E-Mail system are host computers supporting electronic mail, user terminals, on-line directories, and the DoD Internet. Except for some E-Mail hosts, all of these components may be used for many other purposes besides electronic mail, such as general purpose ADP, access to remote data bases, and general computer-to-computer communications.

a. Electronic Mail (E-Mail) Hosts. An electronic mail host is a computer which has (1) an application program which interfaces with users on terminals to compose, send, and receive messages; and (2) an implementation of the Simple Mail Transfer Protocol (SMTP) and the necessary underlying protocols which allow it to send mail to and receive mail from other E-Mail hosts. Storage to keep received mail until users have read it is also required. Additional support, such as editors for composing messages, and sorting, storing, and retrieving messages after they have been delivered, may also be provided.

b. User Terminals. Almost any computer terminal or PC with terminal emulation software can be used for electronic mail.

c. Directories (DIR). The DDN Network Information Center (NIC) computer contains a directory of over 50,000 users of E-Mail. The directory contains the user's name and mailbox address consisting of an identifier for the user and an identifier for the E-Mail host; e.g., SMITH@DDN1.DCA.MIL. Inquiries are made by users from their terminals. A second directory, which contains host names and corresponding internet addresses, used in the DoD Internet Protocol, is also located at the NIC. This directory is in the process of being distributed throughout the DoD Internet with only the "directory of directories" at the NIC. Processes internal to the mail hosts normally access this directory.

d. DoD Internet. This is not a DMS component per se, but is included for completeness. The baseline DoD Internet has three major divisions:

(1) Classified DDN. A set of physically, procedurally and cryptographically secured packet switching segments providing the backbone for classified E-Mail (i.e., DSNET 1, DSNET 2, DSNET 3).

(2) Unclassified DDN - The packet switching segment providing the backbone for unclassified E-Mail (i.e., MILNET, ARPANET).

(3) Baselevel Transmission Facilities. The baselevel transmission facilities consist primarily of the base cable plant

including the main distribution frame(s) and dial central office(s). These facilities traditionally support switched voice circuits, dedicated point-to-point communications and simple star networks. Many digitization programs upgrading the baselevel transmission facilities are underway to allow more flexibility in the use of newer automation technologies for local area networking.

2.2.2 Connections. Asynchronous terminals may connect to DDN Terminal Access Controllers (TACs) directly or via dial-up circuits (for unclassified terminals). They may also connect to a host computer directly or through a LAN. Synchronous terminals currently connect directly to hosts, which then connect to the DDN. Computers, including those which act as E-Mail hosts, may connect to either a DDN network or a LAN network. The LANs are connected to the DDN by gateways or hosts using the DoD Internet Protocol. In a like manner, interoperability with the research community (ARPANET) and the commercial community is accomplished by the use of gateways.

2.2.3 Concept of Operations. The following is a typical E-Mail scenario. A user logs onto an E-Mail host with a user ID and password. The sending user either uses a local list of commonly used addresses or requests the address of the intended recipients by typing, for example, "Who is Smith, John C.". The E-Mail host makes an inquiry to the NIC directory, and returns the address of the requested name. The user then requests the mail host to send a message by issuing a command, e.g., "send". The mail host then prompts the user for the addresses (usually with "TO" and "CC" prompts), the subject, and the text of the message. If the user is using a PC or workstation, a file on the workstation may be included as all or part of the text, so the message does not have to be composed while on-line to the mail host. Once the message is composed, some systems may permit the user to edit it. After the user is satisfied with the message, the user requests that it be sent by typing a command, e.g., "mail" or a message termination character. The mail host then immediately checks the addresses for proper format and correct host names (which may require inquiries to the NIC host directory, if the names are not already in the mail host's cache of host names and internet addresses), and informs the user of host addressing errors before returning control to the user. The mail host then adds "from", date and time fields to the message and sends the message to all of the recipient mail hosts through the DDN employing DoD standard protocols. Normally, only one copy of the message will be sent to each receiving E-Mail host, even though several addressees may be served by one host. If a receiving host is unavailable, the message is stored at the sending host for a period of time and periodic attempts are made to deliver it. After some time-out period, an undelivered mail notice is placed

in the sender's mailbox, together with the unsent message. The receiving mail host checks the names of the intended recipients against those of the users it serves. If the recipient is registered, the message is placed in the appropriate mailbox. If the recipient is not on that host, it may check for users on a forwarding address list. If the recipient is not on either list, the sending host is notified, and a non-delivery notice is put in the sender's mailbox. When the recipient signs onto the mail system at some later time, the system indicates mail has been received. The recipient can normally scan through the message subjects and senders (and on some systems, search the text and other fields for key words) and read, save or discard the messages based on the results. If the recipient has a printer available, the message may be printed. In some cases, if requested by the sender, the receiving system may deliver a notification message to the sender when the receiving system has sent the message to the user's terminal. If the user wishes to reply to the message, the user issues a command, e.g., "reply". In this case the user need enter only "cc" addressees and the text of the reply because the system enters all other fields. The recipient may also forward the message to other recipients. Finally, the user may keep some number of messages on file at the mail host for whatever purposes needed, for example, to maintain history files on different subjects. Alternately, messages may be stored at the user's PC, although the ability to manipulate messages based on field contents may be lost unless the user has applications software for that purpose.

2.2.4 Comparison to Requirements. User requirements are not uniformly satisfied by E-Mail, because the host software supporting the user is not standard. With the exception of the DDN's Simple Mail Transfer Protocol (SMTP), the remainder of the user service is provided by the host hardware, software and cable distribution. The user's perception of the service is determined primarily by the host's capabilities and limitations.

a. Connectivity/Interoperability. E-Mail service is provided on several disjointed network segments which are physically separated by security classification. For purposes of electronic mail, the unclassified segment of the DDN is a single open system. Any unclassified mail user can communicate with any other unclassified user. The number of users registered in the DoD Internet Directory is over 50,000. These users have mailboxes (which may be shared) and most have individual directory entries. There are many other users with mailboxes who are not entered in the directory, usually because they communicate only with other users or an individual host or a set of hosts with its own directory. Such users may still send and receive mail, but identifying them is more difficult. Mailbox owners also are generally willing to pass messages to other

individuals, but no formal procedure is in place. The classified segments of the DDN are not connected to the unclassified segments nor to each other, and messages cannot be sent between them without a manual extraction from one and reentry into another.

b. Guaranteed Delivery. The source mail host keeps outgoing messages until it has confirmation of receipt from all destination mail hosts. In general, messages are stored on disk only once at the source and destination, so there are windows in which a single disk crash can cause the loss of a message, e.g., between back-ups and before transmission (at the source) or delivery (at the destination). In such cases, users are rarely notified that a message may be lost. If a sender is particularly concerned that a message has been delivered and read, the recipient can be requested to reply (acknowledge) in the body of the message. Since replies are extremely easy (see concept of operations), this approach provides a manual technique to work around the message loss problem, but only if the sender is aware of the potential loss. Again, no standard procedures are available to cover this potentially serious problem.

c. Timely Delivery. Since critical command information is not passed using E-Mail, timely delivery in E-Mail may be expressed in terms of fractions of hours and hours rather than in minutes. As a result, many mail hosts have a process which "wakes up" from time to time to deliver mail. There are no set standards, but, in general, the process is activated at least every fifteen to thirty minutes. On some systems, the user can cause the process to "wake up" immediately (i.e. interrupt) upon receipt of a message. As a result, mail messages are generally sent and received at the destination mail host, and put in the recipient's mailbox, within half an hour. Once mail is delivered to a user mailbox, it remains there until the recipient reads it. Generally, this is dependent upon the recipient's work schedule, and there is no assured time by which it will be read. Some organizations may procedurally require frequent reading of mail; most currently do not.

d. Confidentiality/Security. Limiting recipients to those cleared for the information is accomplished by physically segregating the DDN by different classification levels. The classified segments of the DDN are protected by encryption on all lines and by facility, personnel, and procedural measures appropriate for the level of classification of the segment. Generally, "system high" computer environments are used and computer security measures are those appropriate to the environmental security level. In the unclassified segment, more limited measures are provided such that the users must know who has access to addressee mailboxes before sending sensitive

unclassified information. These security measures are increasing, as described in the DDN Subscriber's Security Guide.

e. Sender Authentication. There are few restrictions on senders of electronic mail, hence sender authentication is a weakness of current E-Mail. While the system normally enters the sender's identifier in the mail message, it is possible to override this mechanism on many E-Mail host systems. Sender authenticity is therefore usually determined by the reasonableness of the message. In case of doubt, the purported sender can be contacted by other means for verification.

f. Integrity. Protocols used internally in the internet provide excellent integrity between the sending and receiving mail hosts. Cyclic redundancy checks are provided on links, and end-to-end checksums are used in the DoD Internet Protocol and Transmission Control Protocol. Similar capabilities are present in the equivalent OSI protocols. There is still the potential for undetected problems between the mail hosts and user terminals at both the source and destination. These access lines tend to employ asynchronous transmission with only character parity checks and limited start/stop flow control. Data overruns are not uncommon. A variety of non-standard approaches are being taken to overcome this problem. They include slowing down transmission rates, using asynchronous line protocols (such as KERMIT and X.MODEM), and employing print spoolers.

g. Survivability. The DDN, the long distance communications for the DoD Internet, contains over 220 packet switches in the unclassified MILNET, and over 150 packet switches in the classified segments. The switches themselves are each multiply connected to other switches, and routes between switches are automatically and dynamically computed. The number of subscribers per switch is relatively small and they are usually near the switch. These features result in high survivability against threats other than nuclear or massive conventional attacks.

h. Availability/Reliability. Extraordinary measures to assure availability, such as uninterruptable power supply (UPS), redundant systems, and on-site maintenance, are generally not provided for E-Mail due to its noncritical, administrative nature. Mail hosts generally have good availability during normal office hours and under normal conditions. The principal cause of downtime appears to be for host system back-ups, which are usually performed at off-peak hours. Host availability and speed of service for the users are also influenced by such items as local power, local weather, and local prioritization of other jobs on a multi-function host. Users with high availability requirements may have several mailboxes on different mail hosts.

This approach helps on outgoing messages, but is of limited use on incoming messages, and of no use for accessing messages already delivered to the unavailable mail host.

i. Ease of Use. Users generally can send and receive typical messages after a half hour of training. System feedback for most errors is immediate, and on-line help facilities are provided. In case of difficulties, either the mail host administrator, or a network help facility can be contacted. Use of capabilities, and extended retrieval capabilities (such as by key word search, subject, or sender) require some additional training, but also tend to be easily mastered. Because the host mail software is not standard, users moving from one host to another may need to learn another system for handling mail.

j. Identification of Recipients. The sending user either uses a local (personal) list of commonly used addresses or requests the address of the intended recipients by accessing the NIC directory ("WHOIS" function). The user makes an inquiry to the NIC directory, and the directory returns the address of the requested name. If there are multiple instances of the name, or if the user only knows part of the name (Smith or Smith, John) then all the matches are returned with the full name and a unique identifier for each name. By entering the unique identifier, more information about the individual is given to the user, such as street address and telephone number. With this information, the user can determine the correct recipient, if the recipient is in the directory. Users are registered in the directory by their E-Mail host administrator who uses E-Mail to register them. The existing directories are adequate for the current user population. However, as the number of users grows, it is expected that a more decentralized directory system will be needed, and work has been initiated to provide for this. A major issue in expanded, decentralized directories, is access control for entering information in the directories themselves. Another problem, which is likely to grow under the current approach, is misidentification of recipients. Since user mailboxes tend to employ user names, a message to SMITH@DOD1.IL is likely to be delivered. Unfortunately, there is no guarantee it will be delivered to the right Smith.

k. Preparation Support. Message preparation may be done on-line with substantial support by the system, including limited editing capabilities. Feedback on errors is provided as soon as the system can identify them. Some host mail systems allow users to build messages by merging notes prepared with word processing software either resident on the host or on the user's workstation.

l. Storage and Retrieval Support. There are neither standard

nor mandated message storage capabilities, but most systems provide some amount of on-line storage under the control of the user. Some host systems provide capabilities to retrieve messages, either on initial delivery or after they have been saved, using a number of criteria. Messages, in some systems, may be filed into categories for future reference. Stored messages may be included in forwarded messages. The sender address, courtesy copy addressee(s), and subject field of saved messages may be used to build "reply" messages, to avoid the look-up of recipient addresses in many cases.

m. Distribution Determination and Delivery. Automated distribution determination and delivery of messages based on subject or other criteria is not supported. The responsibility for distribution (and redistribution) of messages rests with the users. Pre-established mailing lists based on interest groups may be used, however, to assist in both initial distribution by the sender and redistribution by any holder of the message.

Section 3

DMS Target Architecture

3.0 Introduction.

The DMS Target Architecture is characterized by the application of commercially available messaging and directory service standards and protocols to provide a totally automated writer-to-reader messaging system. For the exchange of messages, the Target Architecture employs the International Telegraph and Telephone Consultative Committee (CCITT) X.400 Message Handling System standards and protocols and for directory services, the CCITT X.500 Directory Service standards and protocols. Because of this, much of the Target Architecture may be implemented using commercial off-the-shelf (COTS) products. The DMS achieves end-to-end security and other security related services such as integrity and sender authentication through use of the Secure Data Network System (SDNS) Message Security Protocol (MSP). The architecture effects a decrease in both operating cost and staffing while satisfying the validated DMS requirements defined in MROC 3-88. The centralized AUTODIN messaging system and associated TCCs, the DDN E-Mail components, and the formats and procedures of the Baseline are replaced by a distributed messaging system that places many of the messaging functions at user locations. The Target Architecture emphasizes flexibility to incorporate the products of on-going DoD programs such as SDNS as well as technological advances that may become available between now and the early twenty-first century.

3.1 The DMS Message. In order to properly describe the functional elements of the Target Architecture, it is necessary to have an understanding of the overall structure of the DMS message, including the address. DMS messages are exchanged within X.400 envelopes having the information needed for their transfer and delivery. This concept is similar to the postal system which transfers a physical envelope and a letter within it and requires specific information on the envelope in order to insure proper delivery and the requested level of service.

a. Originator/Recipient (O/R) Name. Every DMS user or distribution list is uniquely identified by an O/R name. It has two parts, a user friendly Directory name that identifies who is sending or receiving the message and the O/R address which distinguishes one user or distribution list from another and identifies the user's point of access to the DMS or the distribution list's expansion point. The DMS naming conventions

insure that each Directory name is unambiguous.

b. Envelope. The envelope contains the originator's O/R address, the O/R addresses of each recipient, a date and time mark, and parameters necessary to control the message transfer through the DMS and effect delivery to all recipients. Each envelope parameter has a standard name and format which is used to distinguish messages within the DMS. They can, for example, specify the type of delivery report desired, priority level, trace information which describes actions taken en route and special handling instructions related to security, proof of submission, non-repudiation of submission, or redirection. The envelope may also contain an identifier to indicate whether the message is organizational or individual. The message envelope is analogous to a postal envelope which contains not only the name and address of the sender and receiver, but also instructions for special handling such as priority mail, air mail or return receipt requested as well as a date and time stamp.

c. Content. The DMS message content is generated by the user agent and consists of three parts: SDNS MSP heading, a message heading and the message body. In the postal analogy, the content is the documents and information within the envelope, for example a letter with an inclosed picture. The format of the content deviates from that of X.400 by the addition of the SDNS MSP heading.

(1) SDNS Heading. The SDNS heading contains the SDNS MSP information needed to perform the SDNS security services, including decryption. Continuing with the postal analogy, SDNS performs a function similar to that of the embossed wax seal placed on envelopes of special significance. If the seal is not broken, message confidentiality and integrity is assured. Authentication is provided by the emblem embossed on the seal.

(2) Message Heading. The message heading contains information to control the internal distribution of the message such as the TO: and FROM: fields, a CC: field indicating who should receive copies, a DATE: field indicating when the message was prepared and the subject of the message. Since each message has a unique identifier (ID), the heading can also contain the IDs of messages which it replaces or amplifies. The X.400 standard provides for optional heading components which can be used to meet specific DMS requirements. The message heading is encrypted using SDNS MSP.

(3) Message Body. The body contains the text of the message. This could be a single page or more generally a sequence of various body parts, each of a different type. These parts are ordered by the user so that various types of encoded

text, graphics, facsimile, teletex, videotex or digitized voice can be transmitted. The message body is encrypted using SDNS MSP.

3.2 Target Architecture.

3.2.1 Overview. The Target Architecture is summarized in Figure 3-1 in terms of the primary functional elements required to provide the DMS messaging services. The message transfer agents (MTAs), message stores (MSs), user agents (UAs), and organizational user agents (OUAs) accomplish the X.400 message handling functions. A hierarchical distributed directory (DIR) together with directory user agents (DUAs) provide the DMS X.500 directory services. Security services are furnished through use of SDNS MSP protection and other various lower layer protection mechanisms. The Target Architecture also includes the necessary DMS management functions. An MSP gateway (MSP GWY) provides the required interfaces with non-MSP DMS users in the NATO, allied, tactical, civil, commercial and research communities. These various functions are performed within physical components which are distributed geographically and organizationally, but act in concert to provide the DMS services.

3.2.2 Message Handling System (MHS). The DMS MHS, following X.400 terminology, consists of message transfer agents (MTAs), message stores (MSs) and user agents (UAs). For the DMS, an extended user agent functionality is defined, the organizational user agent (OUA). The User Agent (UA) and Organizational User Agent (OUA) are functions which act on behalf of individual users and organizations to send and receive messages. The Message Store (MS) functions as a mailbox to provide for message delivery or storage and retrieval; additional message storage for long term recall and user manipulation can be implemented outside the MHS context as required. The Message Transfer Agent (MTA) provides the basic message transport capability for both individual and organizational messages. MTAs acting together form the Message Transfer System (MTS) which delivers message contents to the intended recipients via UAs/OUAs. Except for the OUA which includes the additional functionality at the UA to provide the organizational messaging service, the DMS MHS functional model depicted in Figure 3-2 follows the X.400 MHS reference model.

a. User Agent (UA). The UA function is an application process that interacts with the MTS on behalf of a single user. The UA resides in a terminal such as a PC along with other applications such as word processing, spreadsheet and file transfer to provide the user with multi-functional support. The UA interacts directly with the user to create and edit a message (heading and body) and submit that message to its Message Store

Figure 3-1. DMS TARGET ARCHITECTURE

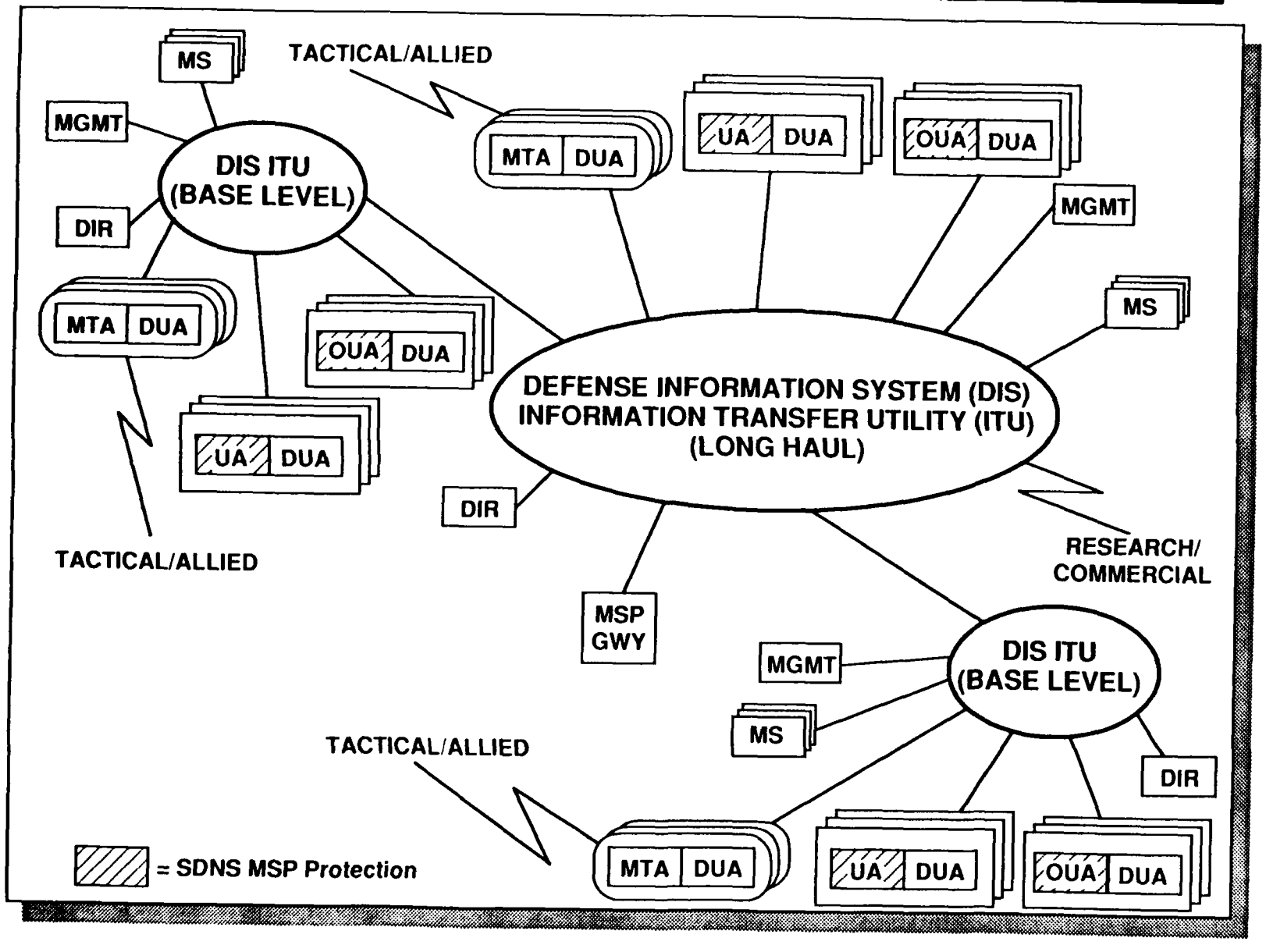
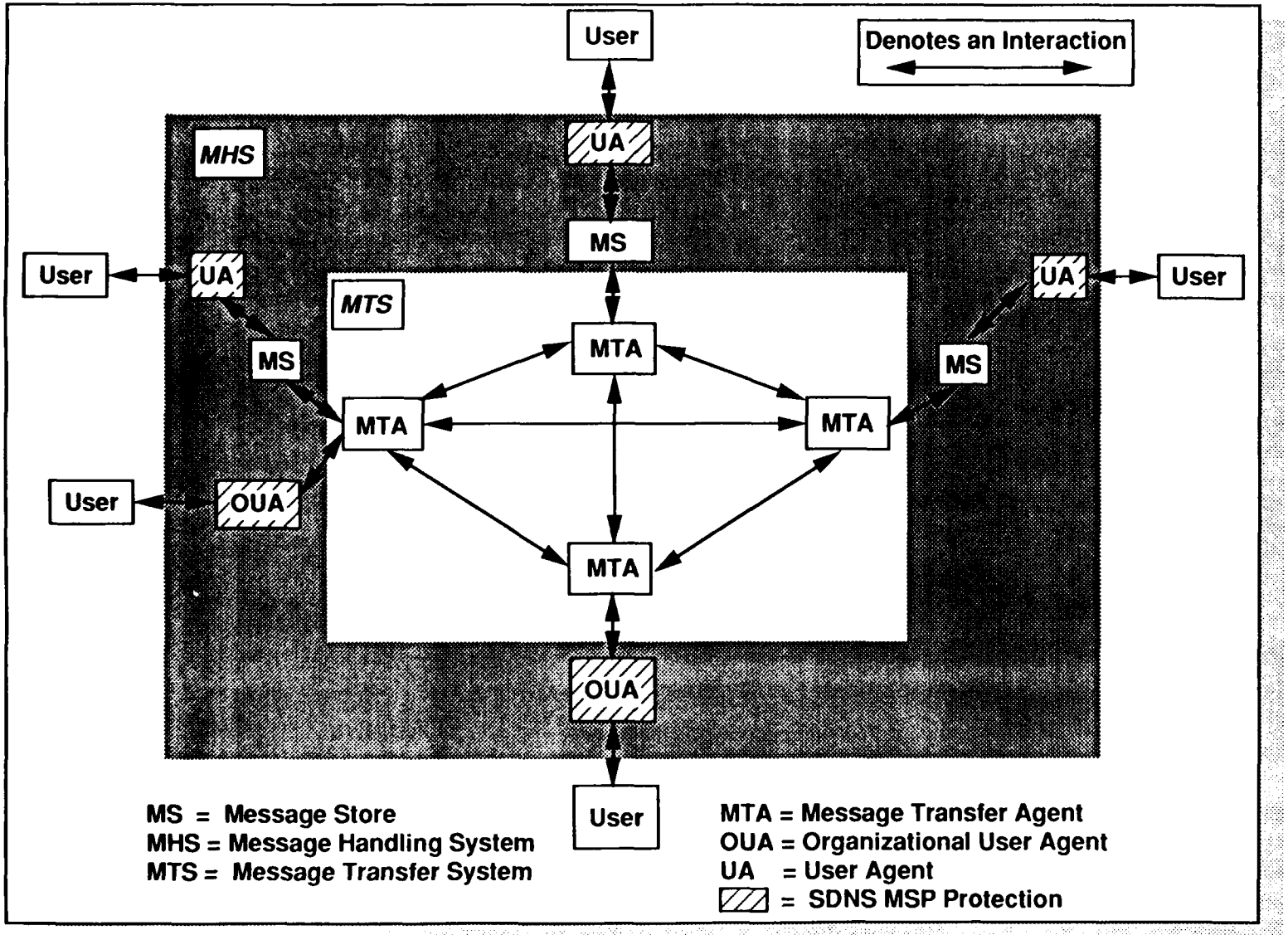


Figure 3-2. DMS MESSAGE HANDLING SYSTEM FUNCTIONAL MODEL



(MS), if implemented, or to its Message Transfer Agent (MTA) for transmission. It also receives and displays incoming message content and, if requested, prepares receipt notification messages. In addition, the UA assists the user in related messaging functions such as replying, forwarding, filing and retrieving. The UA interacts with its corresponding MS, if implemented, or its MTA to receive messages from the MHS.

b. Organizational User Agent (OUA). The OUA is a modified X.400 User Agent created to include features necessary to handle DMS organizational messages. It is an application typically implemented on a PC along with other, non-DMS applications. While the OUA appears to the MHS as an X.400 UA in that it consists of all the normal UA functions to create, edit, transmit, receive and process messages, it also performs the DMS unique functions necessary to handle organizational messages.

(1) Specific OUA Unique Functions. Satisfaction of the unique DoD requirements associated with organizational messages requires the OUA to perform the following functions:

- approval of organizational messages prepared locally or by other subordinate UAs in the organization. This is known as the message release authority function.

- automated distribution determination and submission of delivered organizational messages for subordinate UAs in the organization.

- guaranteed delivery of messages, and capability to receive high precedence or high classification messages any time day or night by any means available.

- returning a message that cannot be released to the originating UA/OUA or forwarding the message to another OUA for release (e.g., for messages that must be released at a higher organizational level).

- storage of organizational messages.

- maintain writer-to-reader message accountability.

(2) Operational Considerations. It is important to note that OUAs may be configured with varying DMS functional capabilities, since all OUA functions may not always be performed. In the local implementation of the DMS, there may be numerous OUAs within a given organizational structure that do not operate on a continuous (24 hours per day, 7 days per week) basis or are only authorized to perform the message release function. Selected OUAs may be dedicated to perform only the distribution

determination and delivery functions or only the release function. Others may be selected to operate only during certain hours. OUAs resident in Command Posts or Duty Officer locations operated on a continuous basis will perform as a minimum, the high precedence and high classification delivery function after normal duty hours but must also be capable of performing all OUA functions if required. The OUA user can return a message that it is unable to release to the originating UA or OUA together with information regarding the rationale for such action.

c. Message Store (MS). The MS is an optional capability of the X.400 MHS that acts as an intermediary between the UA and the MTA. There is one MS per UA. When subscribing to an MS, all messages destined for the UA are delivered to the MS only. The UA, if on line, can receive alerts when certain messages are delivered to the MS. Messages delivered to an MS are considered delivered from the DMS perspective. When a UA submits a message through the MS, the MS is in general transparent and submits it to the message transfer agent before confirming the success of the submission to the UA. For UAs not on-line, the MS, if not co-located with the UA, stores the messages until they go on-line. The MS user can obtain a listing of messages of specified types and a summary of information about the messages stored. The user can specify to the MS messages to be deleted. The MS can alert its UA when messages of specified types are delivered and can automatically forward a delivered message according to recipient MS user instructions. Both UAs and MSs can be implemented on a wide variety of PCs and workstations. For individual messaging, the MS can be implemented with the MTA or with the UA; for organizational messages, functionality equivalent to the message store will be included in the OUA application to meet MROC organizational messaging requirements. Within the DMS, use of all the features of a MS may be limited due to the SDNS MSP encryption of all DMS messages.

d. Message Transfer Agent (MTA). The function of the MTA is to route submitted messages to the next MTA, to a distribution list expansion point, or to one of its associated UAs or OUAs in accordance with the instructions on the envelope. The MTA uses the directory services as necessary to effect the desired messaging service. The MTA may query the Directory System Agent (DSA) to obtain alternate delivery addresses, hours of user operation in instances where messages are to be delivered only during normal duty hours, user capabilities to process specific types of messages (e.g., facsimile or digitized voice), disposition information if delivery cannot be effected or information needed to expand distribution lists. Since within the DMS the UAs and OUAs place the complete O/R name on the envelope, the MTA's use of this aspect of directory services may be limited to updating its routing tables or cache of directory

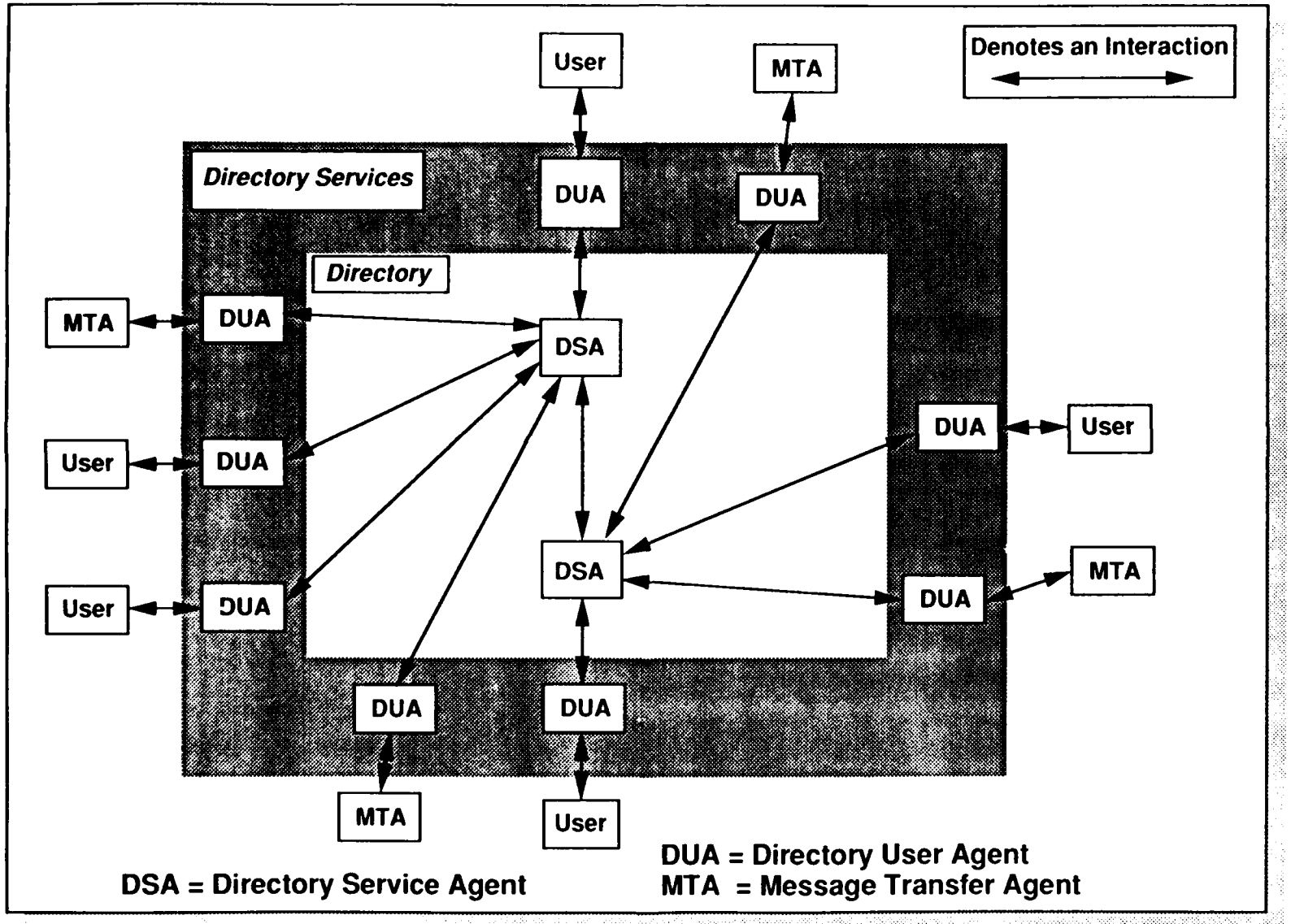
information. To preclude an MTA from having to query the directory each time a message arrives, for frequently used O/R names, the presentation addresses and other Directory information can be cached at the MTA. The MTA will route messages through the Defense Information System in a cost effective, efficient manner. MTAs as a group form a Message Transfer System (MTS) for exchanging messages among users. It is important to note that MTAs neither modify nor examine the envelope's encrypted content. The receiving MTA issues a special message called a delivery report containing audit information which is sent to the originating MTA. The content of this report depends upon the options specified on the envelope by the originator. MTAs can be implemented either stand-alone or co-resident with a UA/OUA in the same PC, workstation or processing system. Since the MTAs and some OUAs are in continuous operation, implementation should consider these functions to be performed at the same location. For efficient service and delivery, the MTA will contain profiles of those user facilities with which it normally communicates. Each MTA, selected MTAs, or some combination can, in conjunction with the directory services, expand distribution lists. The DMS implementation of this X.400 feature may be limited by SDNS MSP.

3.2.3 Directory (DIR). Each DMS message must identify the recipient(s)'s O/R name to effect delivery of a message or notification. The directory services defined by the X.500 series of recommendations is the source of the directory name, the O/R addresses and other information required to provide the messaging services. Within the DMS, the hierarchical DIR will be distributed and will have the capability to translate between user friendly directory names and machine oriented O/R addresses; assist in authenticating the identity of MHS functional agents (i.e.,UAs, OUAs, MSs and MTAs.); store information on user capabilities and messaging service profiles; assist in expanding distribution lists supplied by the MHS into individual O/R addresses; and assist in updating the routing tables at each MTA. The users of the directory include people, organizations and computer programs such as the MTA. They are represented to the Directory by the Directory User Agent (DUA). The Directory System Agent (DSA) is the distributed, hierarchical application process which includes and provides access to the Directory Information Base (DIB). The DMS directory services functional model is depicted in Figure 3-3.

a. Directory Services. The DMS directory provides the following basic categories of service:

(1) User-Friendly Naming. The originator or recipient of a message can be identified by means of his user-friendly Directory name, rather than his machine oriented O/R address.

Figure 3-3. DMS DIRECTORY SERVICES FUNCTIONAL MODEL



The UA/OUA via their DUAs can obtain the unique O/R address of intended recipients by providing the recipients' Directory name. The Directory name and the O/R address are combined to form an O/R name which is needed to construct both the message heading and the envelope.

(2) Distribution Lists (DLs). This is a group name whose membership directory name and O/R address is either stored in the directory itself or at a special expansion point. By simply supplying one name, a DL name, the originator can send copies to each member of the named distribution list. At the DL's expansion point, the list is expanded into the O/R names of its members, the message content is replicated according to the length of the list, and multiple copies are submitted to the MTS for delivery to the intended recipients. Each DL has an owner who is responsible for establishing and maintaining dynamically the group membership list. This owner may also restrict the use of the DL and choose to collect delivery and non-delivery reports. SDNS MSP may restrict the use of the X.400/X.500 distribution list capability. In addition, implementation of this service for classified distribution lists will be unique to DMS.

(3) Recipient MHS Capabilities. The capabilities of a recipient (or originator) is part of his Directory information and may be cached at his MTA. At any t'me, his MTA using either the cached information or the Directory as well as other UAs/OUAs by consulting the Directory, can obtain and then act upon those capabilities. In this way, user terminal requirements such as transmission rate or text code can be satisfied. SDNS MSP may limit the application of this feature.

(4) Messaging Services Control. In certain situations it may be desirable or required to limit user access to certain DMS services or features. For example, not all DMS users may access specific DLs, or certain OUAs may choose not to receive individual messages from all or selected UAs. When an organizational message is released and transmitted, the directory can assist in insuring that it is sent only to another OUA. Information contained in the DIR can be used to implement these access control features.

b. Directory System Agent (DSA). The DSA is the application process which provides access to the Directory's services. Users provide via their DUA the Directory name of the intended recipient to the DSA, and (subject to access control) obtain from the DSA, the recipient's O/R address. If the name is a distribution list, it will have to be broken out at selected locations having DSA access to complete the distribution process. The X.500 DSA function also plays a role in provision of SDNS

protection through storage of cryptographic key information for MHS users.

c. Directory User Agent (DUA). The DUA is the X.500 functional agent which represents the user in interactions with the Directory. The DUA interfaces with the DSA to provide the user with recipient O/R addresses needed by the MTA to effect message delivery. To enhance message addressing via the MHS, each UA/OUA's DUA can implement a limited cache of the DMS Directory containing the names and O/R addresses commonly used. Maintenance of the cache should be accomplished interactively between the DUA and the DSA without user involvement.

3.2.4 Management (MGMT). Management is a hierarchical, distributed function which supports the core architecture and all users of the DMS. It insures the spectrum of DMS services to the users by performing the overall MHS, cryptographic key and directory service management for the DMS. MGMT includes network status and performance monitoring, directory service maintenance and configuration control of the DMS. By automating these operations, they will be performed effectively using a minimum of staffing resources.

3.2.5 Security. Security consists of DMS security policies, procedures and guidance to be developed as part of the phased implementation together with the supporting security components. For the DMS, the primary entities to be protected are the UAs and OUAs and the protection is provided via writer-to-reader SDNS MSP encryption of each message's content, i.e., the heading and the text of the message. Information exchanges between directory elements (e.g., DSAs, DUAs) may also require protection. DMS security is provided at the application layer by the Secure Data Network System (SDNS) Message Security Protocol (MSP) and the use of multi-level secure (MLS) platforms. MSP is a writer-to-reader security protocol used for the staged delivery of a message through a network. Security, traffic flow confidentiality for example, may be required at the lower OSI protocol layers, depending upon the user's environment. To provide writer-to-reader encryption, SDNS MSP protection is required for all OUAs and UAs. The following security services are envisioned:

a. Confidentiality. Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes.

b. Data Integrity. Integrity protects against unauthorized modification, insertion and deletion.

c. Authentication. Authentication services provide for the verified identity of a communications peer entity and the source

of the DMS message.

d. Access Control. This service allows only authorized users to send or receive DMS messages. Control can be based upon the enforcement of specific access rules or upon the identity of the potential user.

e. Non-repudiation. Repudiation is the denial by one of the entities involved in a message exchange of having participated in all or part of the exchange. Non-repudiation is a service that protects an entity from such denial. It has two forms, one that protects the receiver of a communication and the other that protects the sender.

3.2.6 MSP Gateway (MSP GWY). A gateway device is required to interface the DMS community using SDNS MSP with the X.400/X.500 community not using SDNS MSP. The MSP Gateway provides this interface. DMS X.400 messages from the NATO, allied, tactical, civil, commercial and research communities will be directed to the MSP Gateway where they will be decrypted if required, encrypted using SDNS MSP, and transmitted via the appropriate MTA to the intended recipient. Messages coming from the DMS community to the non-SDNS MSP community will follow the reverse process. The commercial and research communities will have supporting MTAs which can transmit X.400 messages from their UAs to the appropriate MSP Gateway. If additional interfacing is required, the NATO, allied and tactical communities will use specifically designated DMS MTAs to connect with the MSP Gateway.

3.2.7 Transmission Components. The DMS will be a user of both the base level and the long haul transmission components of the Defense Information System (DIS). The DIS consists of the information transfer and information processing systems that provide command and control (C2) support to the missions and functions of the Services and agencies. These transmission components are both based upon Integrated Services Digital Network (ISDN) technology. The Target Architecture allows for total connectivity and interoperability from a network standpoint by using the ISDN standards and also by using a standard set of services as offered by the ISDN. These standards and services are to be provided and used at the local level as well as at the regional and global levels. In addition, the DMS may also use the various S/a office automation systems for local connectivity. The total connectivity and interoperability provided by the DMS is, of course, subject to the security and policy requirements of the DoD and the organizations involved.

a. Long Haul Information Transfer Utility (ITU). The Target Architecture will use the Integrated Services Digital Network (ISDN) based ITU portion of the DIS to provide the long

haul interconnection for the DMS Components. This long haul component is managed by the Defense Communications Agency (DCA). It is assumed that the ITU will provide the lower layer protection, below MSP, where required by DMS security policy.

b. Base Level Information Transfer Utility (ITU). The base level ITU is planned and operated by the Services and agencies. It provides the local interconnection of DMS components. As part of the DIS, it is an ISDN based capability, thus ensuring excellent interoperability with the long haul component. It is assumed that the base level ITU will provide the lower layer protection, below MSP, where required by DMS security policy.

3.3 Classes of Messaging Services. The Target Architecture provides two basic classes of messaging service based upon the MROC defined organizational and individual messaging requirements. In order for the DMS to handle every message in a manner appropriate to its content, the architecture is sufficiently flexible to permit other classes of service. Other classes may evolve based upon need, future technology, or both.

a. Organizational Messaging Service. Through the OUA functionality and the use of SDNS MSP, this DMS service provides all the capabilities required for organizational message exchange. These capabilities include release for transmission, distribution determination, non-routine precedence, accountability, guaranteed timely delivery, and high availability and reliability. Either the UA or the OUA can be used to generate and coordinate a draft organizational message. However, due to its extended functionality, only the OUA can be used to send and receive organizational messages, officially release an organizational message and locally distribute the information content of organizational messages to UAs.

b. Individual Messaging Service. The determining requirements of this class of service are messages whose content does not justify them as being organizational in nature. This is a basic individual messaging service designed to provide connectivity to each UA and consenting OUA. It is used to exchange draft organizational messages among UAs and OUAs and by OUAs to internally distribute the content of a received organizational message to UAs.

3.4 Concept of Operations. All messages exchanged via the DMS are categorized as either organizational or individual. This determination rests with the originator of the message and the prevailing policies and guidance. This together with the security classification will determine how the message will be handled within the DMS. Following are potential scenarios envisioned for the exchange of individual and draft

organizational messages and the release and distribution of organizational messages:

3.4.1 Message Exchange. This scenario describes the exchange of individual and organizational messages, noting any differences as they are encountered.

a. Terminal. The user will employ a terminal located in his/her own work area. It will typically be a terminal familiar to the user through other applications. Through this terminal, e.g., a workstation or a PC, the user will access his/her UA or OUA. Each UA or OUA will present standard user-friendly screens and menus to assist in the selection of the most appropriate class of service and options based upon the content of the message, in the creation and preparation of the message, in the release of an organizational message, or in the processing of messages for storage, retrieval, forwarding or replying. Because of its extended functionality, the OUA user will have screens and menus not available to the UA user. However, for common DMS applications, the screens and menus will be identical.

b. Logon. The logon and local procedures will insure that the user is a valid DMS subscriber and for an OUA will authenticate that the user has organizational release authority. A user with this authority may also generate draft organizational messages or other individual messages on the OUA. A user without release authority may, depending upon local procedures, use the OUA for individual messaging.

c. Message Preparation. The UA/OUA will prompt the user for the information required for preparation of the message in the Common Message Format (ACP XXX) and provide help menus as required for completion of the message. Information required from the user for message preparation will include only the basics such as: whether or not an organizational message is being prepared; originating name (FROM:); action names (TO:); information names (INFO: or CC:); message precedence; message classification (to include caveats or codewords as may be appropriate); subject indicator code(s); special handling instructions such as requests for signed receipts; and the message content, which includes both the header and the text of the message. The name may be that of an organization, an individual or a distribution list (DL), in which case the message will go to all members of that list. If a DL is specified, the DMS will insure that the message originator is authorized to use the DL specified.

d. Directory Service. The message must contain the precise Directory names of the intended addressees, either organizations or individuals. The user can obtain Directory name information

and assistance from the DUA cache implemented at the installation level or associated with the OUA/UA, or initiate a Directory query to the X.500 DSA implemented at the regional level.

e. Electronic Coordination. If the message requires staffing or coordination prior to release, additional information to support the coordination process (e.g., a supporting memorandum for record) may be appended to the body of the message. The staffing/coordination process will be accomplished using office automation or IITS capabilities for coordination with local staff members or via the MHS for coordination with distant staff members.

f. Release. When the staffing and/or coordination process is complete, the draft organizational message is transmitted to the appropriate OUA for organizational review and release whereas the individual message is released directly by the preparer.

g. Submission. Once the message is released, the UA/OUA will encrypt it using MSP, create the SDNS and message headings, enclose this information in an envelope, place the necessary O/R names and other information on the envelope and submit the message either to its MS, if applicable, or to its MTA. All messages submitted to the MTS are encrypted. With SDNS MSP protection, the message content is encrypted from UA-to-UA or from UA-to-OUA or from OUA-to-UA or from OUA-to-OUA.

h. Transmission. At the originator's MTA, based upon the O/R name of the recipient(s) and either routing tables, a cache of the Directory, or a DSA query, a determination is made as to where to route the message. If the recipient is associated with the MTA, the message will be routed directly to the recipient's OUA, UA or, if applicable, MS. Otherwise, the presentation address of the next MTA(s) will be determined and the appropriate number of copies will be transmitted. This process is repeated at each destination MTA.

i. Distribution Lists. The DL is a special O/R Name which contains the O/R Address at which the expansion of the DL into its member O/R names is accomplished, or the Directory name of the entry which contains the set of the DL members names. A copy of the message is sent to each member of the list. Since DLs can contain other DLs as members, expansions can be concatenated.

j. Delivery. The destination MTA will recognize the O/R name as belonging to one of its member UAs or OUAs. For an individual message, the MTA delivers it to the individual's MS or on-line UA, as appropriate, at which time the message is considered delivered. The MS in turn alerts the UA that it has a message. The recipient, when logged on, retrieves the message

from his/her MS. If the message is destined for an OUA, it is forwarded directly to it or its co-located MS. If the OUA is operational only during specified periods, the MHS may hold the organizational message until the OUA is open for business. If the recipient OUA is one which is not always on-line or if it fails, the MHS will send a non-delivery notice (including the message) to the originator after a specified time-out period has elapsed and may in addition deliver the message to a designated alternate. If the MTS cannot deliver a message to a UA, a non-delivery notification is sent to the originator in accordance with the instructions on the envelope. Non-delivery notifications include the reason the message was not delivered. Once delivered, appropriate delivery notices will be sent if requested by the originator. Delivery notification carries no implication that any user action, such as examination of the message content, has taken place. For an organizational message, if a signed receipt is requested, a receipt message is generated and sent to the originator.

k. Accountability. Accountability information regarding the complete message transfer is recorded by the MTS. This information can then be recalled for administrative purposes related to accountability.

l. Storage. The originating MTA stores each outgoing message until a confirmation of receipt by the destination MTA(s) has been received. Each message is stored in the MTS until delivery or returned in a non-delivery report. The originator and recipient(s) may as a matter of local implementation choose to store messages locally for as long as required.

3.4.2 Organizational Message Exchange. The scenario for organizational message exchange is similar to the above message exchange scenario. The differences lie in the release authority and in the accountability, receipt and re-distribution of organizational messages. For individual messages the release authority is the individual; for organizational messages release is a formal process and the release authority can be exercised only through an OUA.

a. Preparation. The organizational message in draft form is prepared as an individual message and sent to the appropriate OUA for release and transmission. The message could also be prepared at the OUA itself and coordinated among other UAs and OUAs.

b. Release Authority. Upon receipt of the draft organizational message by the OUA, the release authority reviews the message content on his/her OUA and takes one of the following actions:

- modifies the message prior to release, or

- returns the message to the drafter for rework, or

- returns the message to the drafter with the recommendation that it be released by another OUA, or

- releases the message for submission to the MTS.

c. Release. Once approved for release, the message will be authenticated as being an organizational message. In addition, the originating organization will also be authenticated. Until the message has been released, the message remains a draft and is considered an individual message. The encrypted organizational message is submitted by the OUA to the MTS for delivery.

d. Delivery of an Organizational Message. When delivered to the destination OUA, the message content, header and body, is decrypted using the SDNS header information. The message then is processed by the OUA using the message header for local distribution determination and delivery purposes. Non-delivery reports are mandatory for organizational messages.

e. Distribution. The contents of delivered organizational messages are submitted by the destination OUA via the MHS to the organizational elements specified by the originator and to additional subordinates as determined by the destination organization based upon local policies and procedures. The message content may be re-encrypted and submitted either as an individual or as an organizational message to each subordinate or internal UA or OUA that it and the originating organization selects, depending upon the message's content and prevailing policies and procedures. At each destination, the message text is decrypted, if necessary, for the user who may, through office automation capabilities, read, print, store, or otherwise manipulate the message.

f. Accountability. While accountability requirements for individual messaging are yet to be determined, the accountability requirement for organizational messaging is greater. When the message has been released as an organizational message, strict message accountability information is recorded from the point of release to all points of delivery. Message accountability information is recorded by the originating OUA, the receiving OUA and by the MTS. It reflects the minimum required for organizational messages and refers to the recording of message transactions only (i.e., it does not refer to recording of complete messages). The capability for all MHS components to maintain this audit information for a required period of time (e.g., 30 days) to support problem analysis, statistics

collection and tracer actions is required.

g. Storing of Messages. With regard to requirements for storing complete copies of organizational messages, the following applies: within the MTS, complete messages are stored only until delivery has been effected to the OUA. Long term storage (e.g., 30 days or more) of organizational messages at the OUA to support retrievals, retransmissions, tracers, and other applications, is part of the OUA functionality implemented locally outside the X.400/X.500 MHS context.

3.5 Impact on Cost and Staffing. Reductions in cost and staffing are envisioned as a result of implementing the Target Architecture. The following areas are identified:

a. Acquisition cost savings. DMS component acquisitions that are based on international standards versus unique DoD standards will maximize the use of NDI, commodity contracts, and products endorsed by the CCEP. Such acquisitions will be more cost effective than the traditional DoD acquisitions involving military unique items. User unique components although not entirely eliminated are minimized.

b. Staff and personnel cost reductions. By extending the messaging interface to the user, and phasing out the ASCs and TCCs of the Baseline, major opportunities are presented to significantly reduce dedicated communications personnel and their associated costs. The large numbers of professional AUTODIN and TCC communicators will no longer be required.

c. Equipment maintenance cost reductions. All of the high maintenance components of the Baseline messaging systems will have been replaced by state-of-the-art commercial hardware featuring large scale integration, high levels of availability and reliability, and repair by replacement. This affords significant savings in equipment maintenance cost.

d. Reduction of miscellaneous messaging costs. Through the total automation of the writer-to-reader messaging process, cost reductions can be realized by the elimination of the cumbersome and manual methods currently employed to prepare, coordinate and distribute messages.

e. Software costs. The functionalities of the Target Architecture are implemented using combinations of commercial software, commercial software adapted to meet DMS requirements, and software developed specifically for the DMS. Since the mix cannot be determined at this time, the positive or negative impact of software on acquisition and operations costs cannot be ascertained. This impact, however, could be substantial and must

be managed throughout the DMS implementation cycle.

3.6 Comparison to Requirements.

a. Connectivity/Interoperability. DMS writer-to-reader connectivity is provided at the user work spaces by using the DoD 5200.28, ISO OSI, CCITT, ISDN, and SDNS MSP standards, and communicating over the base level and long haul ITUs. In particular, electronic messages are transferred from UA/OUA to UA/OUA using the CCITT X.400 series of protocols. The use of these standards eliminates incompatible communications protocols and character sets. Interfaces are provided for interconnecting with the civil, tactical, allied, and commercial environments. The DMS requires that the base level and long haul ITUs provide the reliable networking connectivity between DMS components.

b. Guaranteed Delivery/Accountability. The X.400 MTS for DMS delivers messages and provides non-delivery notification as required. A message originator is required to select the type(s) of service parameters appropriate for all messages, the MTS is robust enough to provide the message originator with these selected service(s). All organizational messages require non-delivery notification. Organizational messages also require that the message originator be held accountable for message delivery to all indicated recipients until an indication of message delivery is returned. After message delivery is complete, message accountability is provided as per the appropriate DoD Regulations and Procedures. The guaranteed delivery and accountability capability of the DMS is dependant upon the reliability of the base level and long haul ITUs.

c. Timely Delivery. Timely Delivery of messages in DMS is accomplished using the standard X.400 and X.500 facilities for delivery/non-delivery notices, precedence, and alternate recipients. The MTS holds routine messages until they can be delivered, or until a timeout parameter has expired and a non-delivery notice is returned to the message originator. For high priority messages, non-delivery notices are returned almost immediately (as set by X.400 timing parameters) and the message originator then sends the message to an alternate recipient for action, with a copy also being sent to the original intended recipient for informational purposes. Timely delivery of DMS messages depends on the reliability of the base level and long haul ITUs, and on the availability of the appropriate DMS components (i.e., DSA, DUA, MTA, UA, OUA and MS).

d. Confidentiality/Security. Confidentiality of message text and the association of the appropriate security label during transit through the DMS are provided by the SDNS MSP. Security of messages before transmission, and after receipt, are provided

by a combination of the MSP confidentiality service and the trusted computer systems in which the DMS components exist. These mechanisms afford the appropriate level of security for the data being protected. The confidentiality of directory and message addressing information makes use of the confidentiality services of the lower ISO layer protocols (i.e., SP4). These lower layer confidentiality services depend on the base level and long haul ITUs meeting these requirements.

e. Sender Authentication. Physical security requirements placed on the DMS components and the implementation of the SDNS MSP provides authentication of the DMS message originator. Release authority for organizational messages is also provided by these same means. Authentication of a request for directory information and the authentication of the requested directory information is provided by the transport network's lower layer security. The authentication of MTS components is also provided by lower layer security. These lower layer authentication services depend on the base level and long haul ITUs meeting these requirements.

f. Integrity. The integrity of message text, addressing, and security parameters, during transit through the DMS, is provided by the SDNS MSP. The integrity of messages while in preparation, and after receipt, make use of a combination of the SDNS MSP provided confidentiality service and of the trusted computer systems in which the DMS components exist. These services are provided to a level appropriate for the data being protected. Messages that are transmitted in part, or which exceed a prescribed maximum message length, are reassembled by the recipient UA/OUA. The integrity of directory and message addressing information make use of the integrity features of the lower ISO layer protocols (i.e., SP4). These lower layer integrity services depend on the base level and long haul ITUs meeting these requirements.

g. Survivability. DMS components, and their connectivity, insure that the appropriate survivability levels are met. DMS components do not reduce the survivability of the communications facilities to which they are attached. DMS survivability relies on the base level/long haul ITUs and the Service/agency locations which house DMS components. The connection of DMS components to base level and long haul ITU capabilities will depend on the survivability characteristics of those locations.

h. Availability/Reliability. New or upgraded DMS components are expected to have little downtime and to be supported by inexpensive, highly reliable power and environmental support facilities. Those components requiring 24-hour-per-day availability (e.g.,DSAs, MTAs, MSs, OUAs) will be either

redundant or backed-up. ISDN technology allows for dynamic reconfiguration of the network which greatly enhances the availability/reliability of the DMS.

i. Ease of Use. The emergence of a simplified, X.400 based Common Message Format (ACP-XXX) will allow users to interact directly with the DMS using their own office automation capabilities with which they should be intimately familiar. Specialized communications skills will not be required. User interaction with the MHS, to include the security services and the directory and key management functions, will be for the most part, transparent to the user. Should the user need assistance in preparing or handling a message, automated help will be available for each step or procedure in use.

j. Identification of Recipients. The use of the SDNS MSP and DMS directory services support the users in the identification and location of authorized message recipients together with any restrictions placed on either users or recipients.

k. Preparation Support. The UA/OUA will provide the prompting and message formatting necessary for the user to easily prepare a message with no special training. This function will be fully integrated into the office automation environment which will have appropriate message preparation capabilities. Throughout the DMS, common user-friendly screens and menus will be employed, enabling easy portability of DMS messaging skills from one organization to another.

l. Storage and Retrieval Support. The DMS can use the X.400 Message Store (MS) functionality to provide a highly flexible message storage capability for messages. For organizational messages, this storage capability is part of the OUA functionality. In either case, messages can be stored on-line for a limited time period (e.g., 30 days) to allow for timely retrieval by the users at their PCs or workstations. Additional storage outside the DMS can be implemented locally to meet requirements for extended periods of storage. DMS compliant products can also provide message analysis and editing capabilities at the user's workstation.

m. Distribution Determination and Delivery. This function, which applies primarily to organizational messages, will be an automated capability of the OUA accomplished in accordance with the organization's policy. Distribution profiles reflecting the organization's distribution policy will be implemented at the OUA and maintained by the local organization. Message distribution will normally be accomplished electronically by sending

organizational messages from the OUA to the organization's subordinate OUAs and/or individual messages to individual users' UAs. Abnormal conditions (high precedence, high classification, OUA/UAs inoperable) will be handled by the submitting OUA through alternate delivery, or review and delivery by other means. For example, in the case of an urgent message, if delivery cannot be effected within a specified time period, this will result in a non-delivery notification and cause the message to be hand-delivered to the staff duty officer for action in accordance with local policy. The DMS security services can provide proof of delivery to the originator, provided both the originator and receiver subscribe to this service feature.

Section 4

Implementation Strategy

4.0 Introduction.

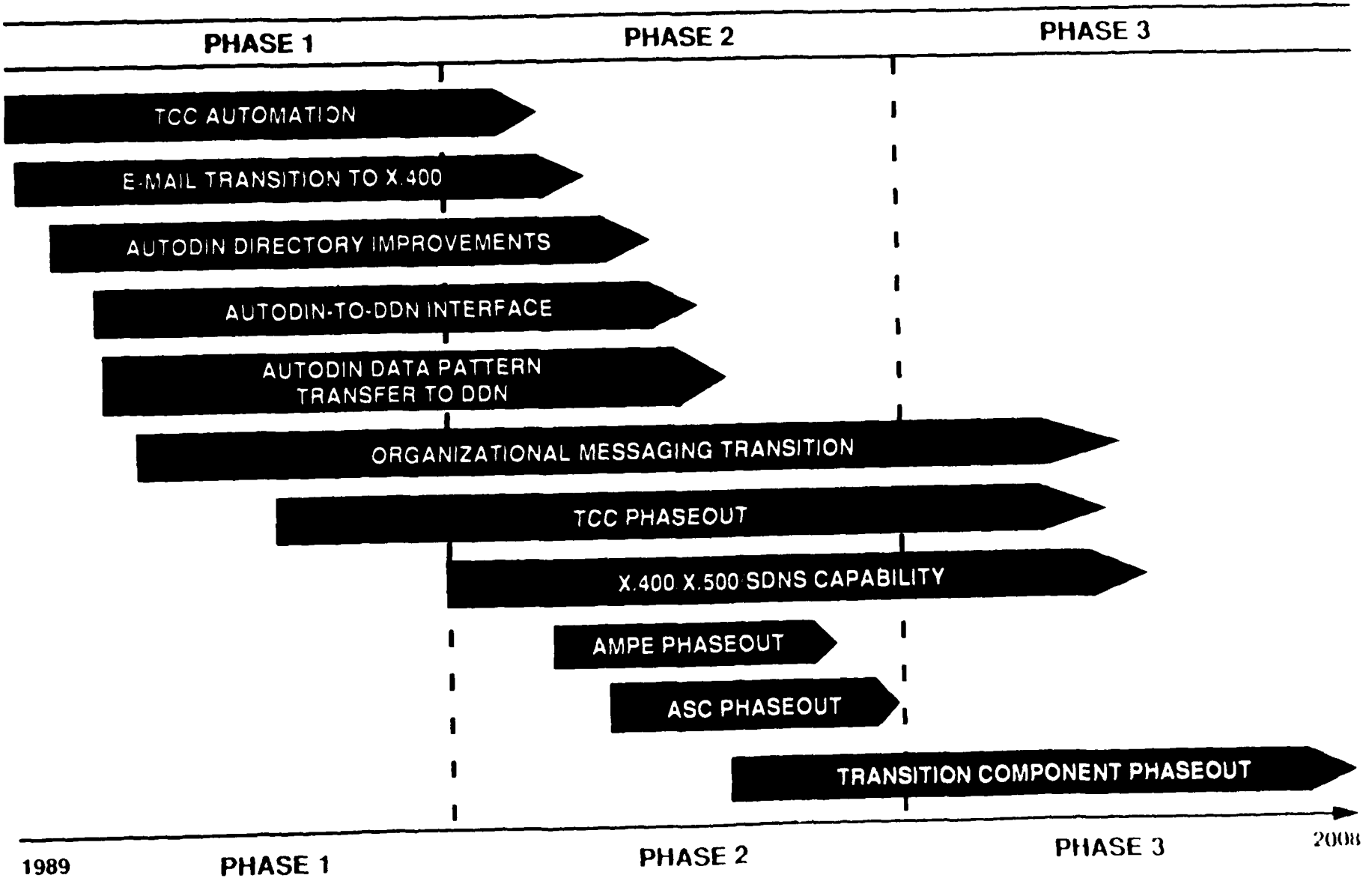
The DMS Implementation Strategy is designed to provide a managed and coordinated Service and agency phased transition from the Baseline system of 1989 to the Target Architecture of 2008. It enables near-term baselevel cost and manpower reductions by the early introduction of DMS transitional components developed in coordination with and shared among the Services and agencies. The phased strategy provides for the evolutionary development and implementation of DMS policies, procedures, protocols, services, and components which rationalize the programmed progression to the Target Architecture. It is a strategy which enables the Services and agencies to integrate the phased transition into their planning process and yet retain control of those DMS components which must differ to accomplish unique local missions. The DMS Implementation Strategy includes operational testing of new components, protocols, and procedures in live user environments to provide proof of purported benefits prior to widespread deployment. Implementation is truly evolutionary with the concept of "releases" being fundamental, not only for software, but for policy, procedures and hardware as well. Although backward compatibility through multiple "releases" is essential to permit phased deployment of new DMS components, aggressive phase out of obsolete components, procedures, protocols, formats and media is also essential. To effect the success of the evolutionary implementation of the Target Architecture, a comprehensive DMS Management Structure is identified which will provide the needed oversight and execution of the DMS Implementation Strategy.

4.1 Phased Implementation.

The evolutionary transition from the Baseline DMS to the Target Architecture is characterized by three implementation phases spanning the period 1989 to 2008. Overall objectives of each phase are outlined below and depicted in Figure 4-1. More detailed descriptions are contained in Appendices A, B, and C.

4.1.1 Phase 1. The first phase emphasizes automation of existing TCC functions and extension of messaging services to users to reduce cost and staffing at the baselevel. Simultaneous deployment of regional transition components during this phase will provide AUTODIN directory improvements, an AUTODIN to DDN

FIGURE 4-1. DMS IMPLEMENTATION STRATEGY



interface capability, and support migration of DDN E mail from Simple Mail Transfer Protocol to X.400. Collectively, these efforts will provide the opportunity for the Services and agencies to begin the phase-out of their resource intensive baselevel TCCs, migrate AUTODIN data pattern message traffic to the DDN, begin the organizational messaging transition, and posture the organizational and individual messaging communities for evolution to the next phase.

4.1.2 Phase 2. The second phase begins with the initial operational capability (IOC) for X.400/X.500 individual and organizational messaging with Secure Data Network System (SDNS) Message Security Protocol (MSP) protection. Phase 2 will produce the most obvious architectural changes and improvements for the users with deployment of an integrated DMS, based on X.400 messaging (vice distinct AUTODIN and E-mail) and X.500 directory services. The Baseline protocols, procedures, formats, policies, and standards will begin the evolution to the Target Architecture. Installation Information Transfer Systems (IITS) will begin to be deployed at the baselevel during this time frame. As TCC functions and responsibilities are shifted to Organizational User Agent (OUA) workstation applications, TCC phase-outs will be accelerated. With the simultaneous deployment of X.400 Message Transfer Agents, X.500 directory services, DMS Management/Control capabilities, and SDNS security protection, an integrated X.400/X.500/SDNS DMS organizational and individual messaging system will be in place and maturing. Transitional components deployed during the first phase will be integrated and upgraded to provide the necessary continued support for remaining TCCs and other unique user interfaces, and thereby allow the phase out of Baseline Automated Message Processing Exchange (AMPE) systems and AUTODIN Switching Centers (ASCs).

4.1.3 Phase 3. The third and final phase commences when the last AUTODIN Switching Center is closed. Primary emphasis during this phase is the maturation of the X.400/X.500/SDNS organizational and individual messaging system, and achievement of the Target Architecture. Remaining TCCs will be closed, and transitional components deployed during earlier phases will be phased out. During this time frame, the local and long haul portions of the DoD Internet will also mature. The DCS Backbone will have evolved to a fully integrated Defense Information System (DIS) and the Installation Information Transfer Systems (IITS) will be mature DoD wide. While evolution of the local and long haul backbones is not part of the DMS Program, achieving the DMS Target Architecture relies upon the availability of these mature capabilities.

4.2 Phase Out of Obsolete Elements.

When fully implemented, the major achievement of the DMS will be the transition from today's obsolete and DoD-unique equipment, protocols, procedures and media to the 2008 state-of-the-art, standard, interoperable elements. Phase out of obsolete Baseline elements will be accomplished through the phase in of elements that are consistent with evolution to the DMS Target Architecture.

4.2.1 Components. The phase out of obsolete Baseline Service and agency components is aimed at reducing maintenance costs and will be based on the phase in of compliant DMS components selected for their ability to implement or evolve to portable operating systems, standard high order languages, and other DoD or international standards.

4.2.2 Protocols. International protocol standards consistent with the Government Open Systems Interconnection Profile (GOSIP), will be phased in as the Baseline AUTODIN and E-Mail messaging systems, standards and policies are phased out. Migration to CCITT X.400 Message Handling System, X.500 Directory Services, and SDNS Message Security Protocols will be completed when the Target Architecture is fully implemented.

4.2.3 Formats. To fully achieve the requirement for a user to communicate with any other user, an X.400 based Common Message Format (CMF) will be developed and implemented as X.400 is phased in. The CMF will facilitate the phase out of existing AUTODIN and E-Mail formats. However, compatibility with the U.S. Message Text Format (USMTF) and with the formats used by the U.S. and the allies (e.g., ACP 127 and JANAP 128) must be maintained during transition in order to maintain interoperability.

4.2.4 Procedures. The procedures of the Baseline are an outgrowth of the manual and semi-automated predecessors of AUTODIN and thus are staff intensive. The procedures originated when the least expensive resource in a communications system was the staff, when the processing equipment was the most expensive and complex resource and when only trained communicators could perform the communication functions. In contrast, today the most expensive resource is the staff and computing power is comparatively inexpensive. Automation of the messaging function and user participation, recognizing that users are becoming more computer literate, will reduce the need for both dedicated communications personnel and staffing intensive procedures. Achieving the DMS Target Architecture will require significant changes to the procedures currently in effect as the DMS moves toward international standard protocols, simplified user formats and the elimination of the current TCC based messaging service. Consistent with the overall DMS Implementation Strategy, procedural actions must be fully integrated into DMS project and

component developments and testing activities.

4.3 Management Structure.

The DMS Management Structure, depicted in Figure 4-2, is designed to ensure the fully coordinated evolution from the Baseline to the Target Architecture while minimizing the resources necessary to manage the evolution. Management of the DMS falls into two major categories; "oversight" and "execution", which are outlined in the following paragraphs.

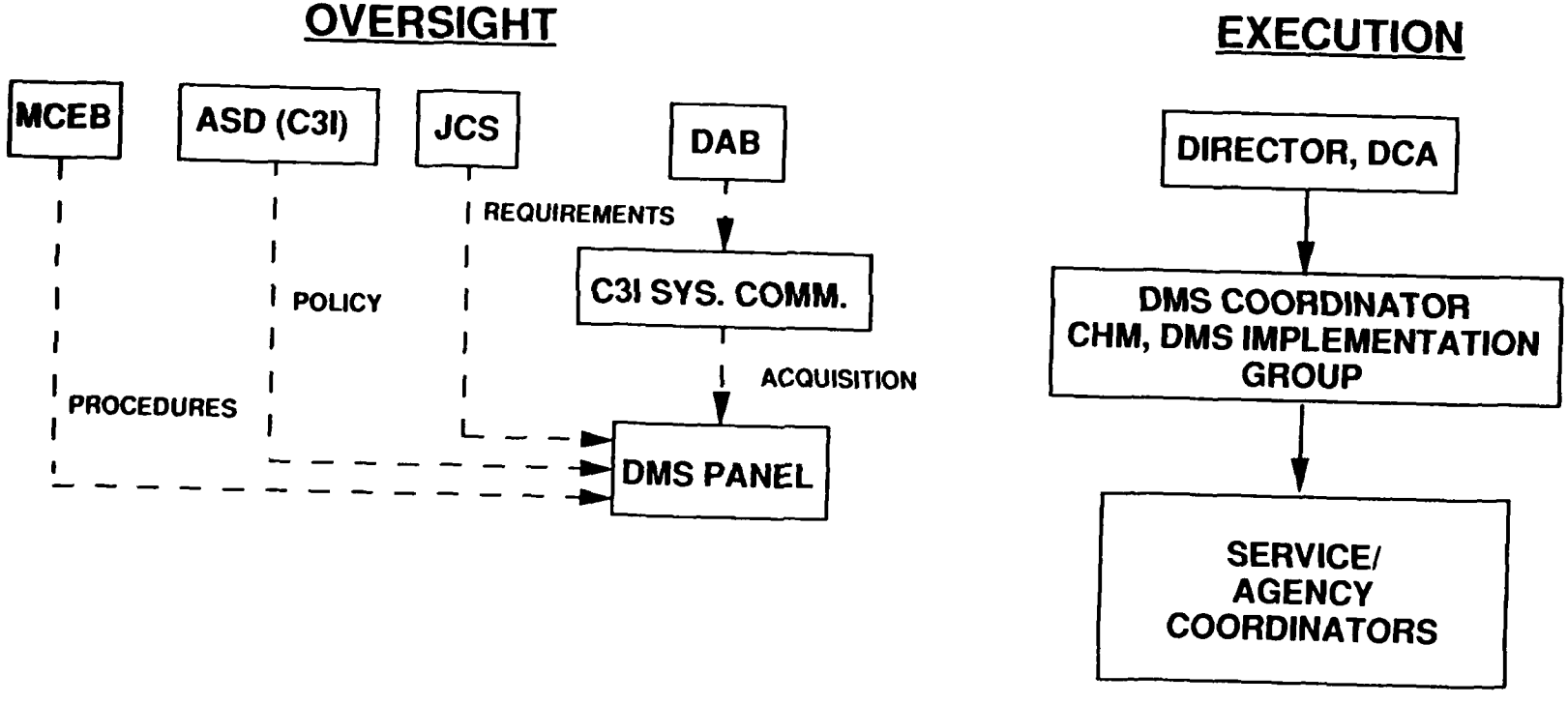
4.3.1 Program Oversight. Oversight of the DMS evolution is accomplished within existing boards and panels to the maximum extent possible. The DMS Panel has been chartered by the C3I Systems Committee of the Defense Acquisition Board (DAB) as the primary oversight body responsible for establishment of DMS policy, approval of DMS projects and resource requirements, and resolution of DMS issues. Normally, issues are resolved at the DMS Panel level. Procedural guidance is provided by the Military Communications Electronics Board (MCEB) through membership on the Panel. Policy guidance is provided by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, ASD(C3I). Requirements guidance is provided by the Joint Staff through membership on the Panel. Acquisition guidance is received from the DAB C3I Systems Committee. The DMS Panel is chaired by the Director, Information Systems, ASD(C3I), and consists of Flag/General Officer and SES members from the Services, agencies, MCEB, Joint Staff, and other elements of the Office of the Secretary of Defense (OSD). Decisions made by the DMS Panel require a unanimous vote of all members. If unanimity cannot be reached on a given issue, minority positions are documented and elevated by the Panel Chair to the C3I Systems Committee (or other appropriate authority) for resolution.

4.3.2 Program Execution. Execution of the DMS program is coordinated by the Director, Defense Communications Agency (DCA) through appointment and supervision of the DMS Coordinator and the Chair of the DMS Implementation Group.

a. DMS Coordinator. The DMS Coordinator serves as the primary interface point with the DMS Panel and is responsible for coordinating DoD wide execution of the DMS Implementation Strategy outlined in this document. The DMS Coordinator provides the Chairman for the DMS Implementation Group, and is supported by a small staff of DCA personnel dedicated to performance of day to day DMS coordination activities.

b. Service/agency DMS Coordinators. Coordination of DoD wide DMS activities is difficult, given the wide geographic and organizational dispersal of DMS program participants. To enhance

Figure 4-2. DMS MANAGEMENT



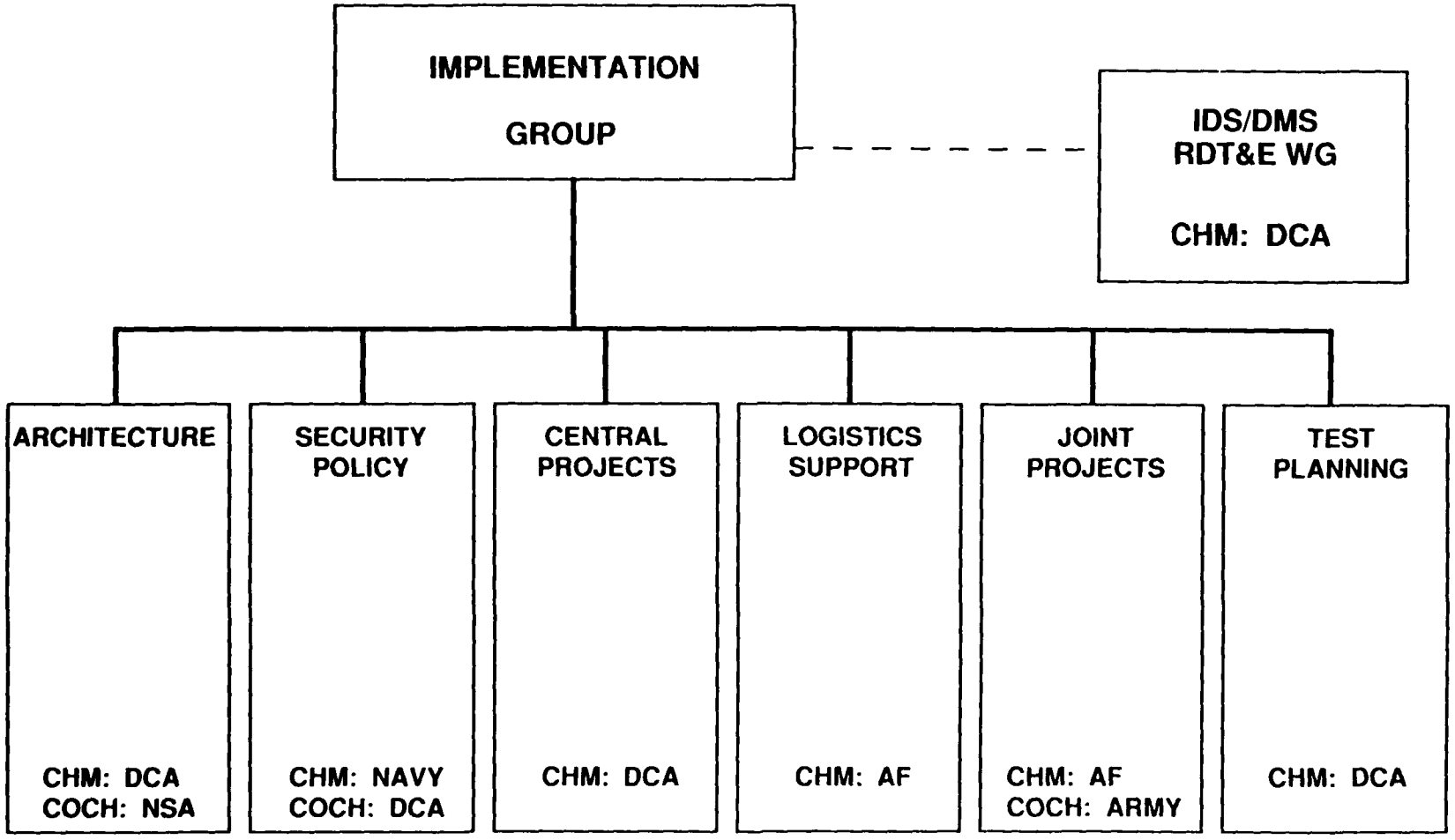
the effectiveness of the DCA DMS Coordinator, ASD(C3I), the Joint Staff, the MCEB, and the Services and agencies (Army, Navy, Marine Corps, Coast Guard, Air Force, DIA, DLA, DMA, and NSA) have each assigned a DMS Coordinator to serve as the DMS focal point for his/her organization regarding DMS technical, programmatic, and coordination matters. Each Coordinator has the ability and authority to solicit participation of technical and programmatic experts from within his/her organization, as required, to actively participate in DMS activities.

c. DMS Implementation Group (DMSIG). This group has been chartered by the DMS Panel to coordinate all DMS implementation activities. It is chaired by DCA and voting members are the Service, agency, ASD(C3I), Joint Staff, and MCEB DMS Coordinators. The primary functions of the DMSIG are to coordinate all DMS implementation activities, achieve Service and agency programmatic and technical consensus on DMS implementation matters, and to provide technical support and programmatic input to the DMS Panel. Achieving DMSIG consensus requires a unanimous vote of all DMS Coordinators. If unanimity cannot be reached on any issue, minority positions are documented and the issue is submitted to the DMS Panel for resolution. The DMSIG is not a decision making body. Decisions regarding DMS policy, project management assignments, funding responsibilities, etc., are made by the DMS Panel. Since this group will also be the forum for distributing overall DMS philosophies and practices, associate members from the Tactical and non-DoD communities are being added to ensure that all DMS users are included in the evolution. The DMSIG is authorized to establish chartered or ad hoc working groups, as required, to address specific DMS program areas or issues. To the maximum extent possible, plans, project recommendations, procedures, and problem resolutions are formulated informally in these working groups prior to submission to the DMSIG for adoption or submission to the DMS Panel, as appropriate.

d. DMS Working Groups. Initial working groups established by the DMSIG are depicted in Figure 4-3 and outlined as follows:

(1) Architecture Working Group (AWG). The DMS AWG is chaired by DCA, provides focus and direction to DMS architectural activities, addresses architectural issues associated with the phased DMS implementation strategy, provides technical guidance to the program participants, identifies research and development initiatives necessary to achieve the target architecture, and serves as the forum for the Services and agencies to pool their architectural resources for a coordinated DoD DMS architectural effort. Through participation in DMS OSI transition planning, and the Service and agency DMS transition planning process, the AWG identifies the architectural need for DMS Central Projects,

Figure 4-3. DMS WORKING GROUPS



recommends Joint Projects, makes DMS compliancy recommendations, surfaces policy and requirements issues, and documents architectural progress through maintenance and refinement of the DMS Target Architecture and Implementation Strategy (TAIS).

(2) Security Policy Working Group (SPWG). The DMS SPWG addresses security aspects of DMS requirements, policies, architectures, components, and implementation strategies, and provides technical guidance regarding security certification and accreditation during the development testing, deployment, and operation of the DMS. The SPWG is rotated annually among the Services and co-chaired by DCA. The membership consists of one accreditor representative from each of the four major Designated Approval Authorities (i.e., NSA, DIA, DCA, and the Joint Staff), and one security representative from each of the Services. Technical support is provided by a technical advisor from the staff of the NSA Deputy Director for Information Security. In coordination with the DMS AWG, the SPWG formulates the DMS Security Architecture and DMS Information Security Policy for publication in the DMS Target Architecture and Implementation Strategy (TAIS).

(3) Central Projects Working Group (CPWG). The DMS CPWG, chaired by DCA, coordinates Central projects and components; to include requirements definition, formulation of operational concepts, project management recommendations, acquisition, testing, and deployment of operational capabilities. Coordination of Central Project execution is performed through Service and agency Project Managers. Initial emphasis is on definition, acquisition, testing and deployment of first phase transitional components. The CPWG is also responsible for coordinating the evolution and eventual phase out of the DCS AUTODIN system. Further, since the target architecture is a significant departure from the baseline, reevaluation and redefinition of operational direction and management control responsibilities for new DMS components will be led by the CPWG. Architectural and security aspects of CPWG projects and components are coordinated closely with the AWG and SPWG.

(4) Joint Projects Working Group (JPWG). The DMS JPWG, chaired on a rotational one year basis by one of the Services, serves as the forum for coordinating the definition, acquisition, testing, and deployment of Joint DMS projects and components. Coordination of Joint Project execution is performed through Service and agency Project Managers. Joint project recommendations are formulated by the JPWG for submission to the DMSIG. Further, Service and agency projects are referred by the DMSIG to the JPWG for review and determination of compliancy with the DMS Target Architecture and Implementation Strategy. Architectural and security aspects of JPWG projects and

components are coordinated closely with the AWG and SPWG.

(5) Test Planning Working Group (TPWG). The DMS TPWG, chaired by DCA, serves as the forum for formulation of test plans and coordination of DMS test and evaluation (T&E) activities. Initial emphasis is on formulation of the DMS Test & Evaluation Master Plan (TEMP) and definition of the DMS Operational Testbed Network (OTN). DMS T&E activities are coordinated through Service and Agency Beta Testbed Managers. The TPWG is also the primary interface point for the independent DMS Operational Test Agency (OTA) and provides primary technical input to the DMSIG and DMS Panel to support OSD (Director, Defense Research and Engineering (DDR&E) and Director, Operational Test and Evaluation (DOT&E)) oversight of the DMS T&E Program.

(6) Logistics Support Working Group (LSWG). The DMSIG is currently pursuing formation of the DMS LSWG through Service Logistics Commands. When formed, an initial task will be definition of a DMS logistics support capability that will stress provision of logistics support to users as the DMS messaging interface moves closer to writers and readers, such as outlining training requirements and end user equipment responsibilities (acquisition, maintenance, upgrade, maintenance of distribution lists and other O&M functions).

(7) Integrated Data Systems/Defense Message System RDT&E Working Group (IDS/DMS RDT&E WG). This working group was in existence prior to the DMS Program and unlike the other working groups depicted, it is not dedicated solely to the DMS program. It is, however, co-chaired by the DMS RDT&E Coordinator who has responsibility for DoD wide coordination of all DMS RDT&E projects. The intent of this group is to efficiently apply scarce R&D resources to those projects that effectively exploit technology and standards advances to further the DMS evolution.

4.4 Component Development.

With the current speed of technology advances, traditional DoD acquisitions frequently result in a new component being obsolete before it can be acquired and fielded. Improved procedures to provide for rapid deployment of both developmental and non developmental items (NDI) after successful Beta/OT&E testing are required to ensure that cost-saving new technology and needed capabilities are provided to users in a timely manner. Components developed for the DMS must maximize the use of non-developmental items (NDI), Portable Operating System Interface (POSIX), Government Open Systems Interconnection Profile (GOSIP), commodity purchases, commercial off the shelf (COTS) products, and products endorsed under the Commercial COMSEC Endorsement

Program (CCEP). Maximum, cost-effective use of SDNS technology and multilevel secure (MLS) components will be made to achieve the DMS security objectives. To meet these objectives, the implementation strategy encourages the use of requirements contracts for hardware acquisitions and requires the use of standards for messaging protocols and operating system interfaces. A major feature of the implementation strategy is the use of the management structure to identify and foster the implementation of compliant DMS components.

4.5 DMS Compliance.

The implementation strategy requires the maintenance of a list of DMS compliant projects derived from the various transition planning efforts of participating Services and agencies. This list of compliant projects will be developed and maintained within the DMS management structure. The purpose of this list is to identify DMS projects that are consistent with the DMS objectives, including the target architecture and the phased implementation strategy. When a Service or agency first proposes an element for use in the DMS either through a central, joint or user unique project, that element will be compared to other similar proposals or to other available solutions in the market place. The solution chosen will be the one that maximizes the benefits and reduces the risks to the overall DMS objectives. An element will be generally compliant if it reduces costs and staffing, improves messaging security and service, and supports evolution to the target architecture. Compliance includes consideration of standards such as Government Open Systems Interconnection Profile (GOSIP), POSIX, Ada, and the Trusted Computer System Evaluation Criteria (DoD 5200.28-STD). Specifically, compliance is based upon the following factors:

a. Reduces cost and/or staffing.

(1) Maximizes reduction of baseline messaging costs and/or staffing.

(2) Maximizes phase out of components with high maintenance costs and/or staffing.

(3) Maximizes phase out and automation of staff intensive procedures.

b. Satisfies DMS requirements.

(1) Satisfies MROC 3-88 requirements.

(2) Satisfies other validated Service/agency messaging requirements.

c. Optimizes the solution for the DoD.

(1) Avoids sub-optimization (e.g., reducing a specific S/a cost while penalizing other DMS users or increasing other DoD costs).

(2) Does not duplicate existing S/a efforts or DMS projects.

(3) Maximizes use of COTS, NDI, and commodity buy solutions.

(4) Minimizes the solution implementation time.

(5) Minimizes funding risks by identifying and programming funds for development and acquisition.

d. Enhances flexibility.

(1) Uses general purpose platforms which support migration to or implement:

- GOSIP
- POSIX OS
- Secure OS
- Secure communications, e.g. SDNS.

(2) Uses software that can be easily ported to other platforms, e.g. software using Ada in a POSIX environment.

(3) Uses software designed in modular fashion and that can readily support modification and introduction of standards.

(4) Minimizes use of proprietary solutions.

e. Supports evolution from older technology.

(1) Eliminates, or at least reduces, the need for components such as TCCs, ASCs, and AMPEs.

(2) Eliminates the need for obsolete manual messaging protocols and procedures.

(3) Replaces obsolete equipment, protocols and procedures.

f. Implements DMS standards.

(1) Maximizes the use of standard message formats (e.g., ACPxxx (CMF)).

(2) Maximizes compliance with DoD policies, regulations, and standards such as: GOSIP, POSIX, Ada, DoD 5200.28-STD and CCEP.

(3) Maximizes adherence to applicable MIL or DoD standards for development and testing.

g. Extends DMS interface closer to the user.

(1) Maximizes extension of message interface closer to the user.

(2) Reduces or eliminates manual message handling (organizational "sneakernet").

(3) Maximizes "user friendliness".

- maximizes transparency of system to the user, i.e., user should not need significantly different procedures to send organizational or individual messages.

- maximizes transparency of transport mechanism.

- maximizes interoperability and connectivity.

h. Supports DMS security policy and architectural objectives.

(1) Maximizes security and confidentiality directly between originator and recipient.

(2) Maximizes transparency of security mechanisms to the user and maximizes their "user friendliness".

(3) Minimizes need for personnel security clearances.

(4) Adheres to applicable accreditation and COMPUSEC certification policies.

4.6 Test and Evaluation Strategy.

An evolutionary developmental approach and early acquisition and deployment strategy is planned for the DMS evolution. To make this possible, a test and evaluation strategy containing both traditional and non-traditional test approaches is being developed by the DMS Test Planning Working Group in coordination with the independent DMS Operational Test Agency (OTA) for documentation in the DMS Test and Evaluation Master Plan (TEMP). Since the DMS baseline is an existing operational system, and its planned evolution contains many projects which, while they

conform to an architecture, are largely autonomous in their development, testing of the DMS will be a continuous but coordinated activity. The scope of test and evaluation, application of T&E strategies and methodologies employed will be formulated by the TPWG for DMS projects and components. The test and evaluation strategy will be designed to support an acquisition strategy that will employ advanced concepts of R&D testing, prototyping, development test and evaluation (DT&E), operational test and evaluation (OT&E) including BETA testing, and operational assessment. Testing will be scaled to fit the scope of the project. For example, a small user-unique project using NDI with limited impact on the overall DMS may be informally tested with limited test planning. However, a major central project would be formally tested with several different test plans published. Following is the DMS approach to the different types of testing.

4.6.1 Development Test and Evaluation (DT&E). DT&E will be conducted on all central, joint and user unique components to determine how well they meet their specifications and whether each component is ready for OT&E. DT&E, in the context of the DMS, includes any independent system level testing normally conducted by the Service or agency having project management responsibility for acceptance of the developed or acquired component prior to network or security certification and component accreditation. The responsibility of conducting DT&E will belong to the Service/agency that has project management responsibility.

4.6.2 Certification Testing. Certification testing is the final phase of DT&E that determines whether a system can be connected to an operational communications network without disrupting the network. It includes independently conducted tests to determine if the system or component has correctly implemented DMS specified protocols and is compliant with established policies related to security, message integrity and accountability. This type of testing is currently being done for all systems before they are authorized to be part of the AUTODIN system. A similar procedure is used for DDN Host Qualification.

4.6.3 Operational Test and Evaluation (OT&E). OT&E will be conducted on each component before it is deployed. For DMS components, most OT&E will be in the form of BETA testing; the project will be part of an operational communications network and will be used to perform an operational mission with data collectors observing and collecting data on the systems performance. These operational evaluations will evaluate the effectiveness and suitability of the DMS components.

4.6.4 Operational Assessment. Four DMS operational assessments will be conducted. The first will provide reference data on the DMS 1989 Baseline. The other three are conducted at the end of each of the three implementation phases to determine progress during the evolution to the Target Architecture. These assessments have four purposes: to assess the current operational effectiveness and suitability of the Baseline, including organizational and individual message exchange; to identify deficiencies and enhancements in the Baseline DMS not previously documented; to identify items to be addressed during subsequent DMS end-of-phase assessments; and to provide a more detailed documentation of the DMS Baseline system configuration.

4.6.5 Testbeds. To support the DMS test strategy, a number of new testbeds are planned.

a. Research and Development (R&D) Testbed. R&D testing is required to gain confidence in the approaches planned for advanced DMS phases (e.g., X.400/X.500 components with SDNS MSP). Specifically, in keeping with the DMS objective of maximizing the use of commercial off-the-shelf (COTS) products, R&D efforts during Phase 1 will be aimed at ensuring that commercial products planned for the Phase 2 time frame such as SDNS, will indeed satisfy DMS requirements. A variety of RDT&E testbed will be used for testing early R&D solutions for feasibility and compatibility with other DMS components, such as SDNS and MLS components.

b. Operational Testbed Network. In addition to development and certification testing, an operational testbed network will be developed for those DMS components, both developmental and non-developmental (NDI), which have satisfied the DT&E, certification testing and OT&E requirements. It will provide resources for coordinated multi-site operational testing of these DMS components in an on-line operational environment to gain confidence in the component's operational effectiveness prior to full scale deployment and to obtain early feedback from the users.

4.7 Security Policy.

4.7.1 DMS Security Certification and Accreditation. The four Designated Approval Authorities (DAAs) are responsible for the ultimate decision regarding authorization of each DMS component to process information. The DMS as a whole and each individual facility gain approval to operate through formal accreditation. Accreditation is a management decision by the DAAs that a DMS facility has been accepted for operational use. Facility accreditation is based upon a certification of the security safeguards. Component certification is function-oriented and

includes a specification of the conditions and limitations under which the component must be installed and operated. Accreditation is a continuing process, and reaccreditation is required at regular intervals. The DAAs collectively approve officials selected to administer and support the DMS security policy during component development and certification, and during facility operation and accreditation.

4.7.2 DMS Security Policy Guidance. The SPWG has set up a DMS security policy framework which outlines policies and plans to support the DMS program; defines standard communication security terminology; identifies existing policies and architectures that apply to the DMS; outlines new policies and architectures that are needed specifically for the DMS; defines the classes of messages handled by the DMS, and also defines the security services that may be appropriate for each class; outlines the process by which the DMS and its elements are technically evaluated with regard to their security features and safeguards, and by which they are approved to operate; and identifies DMS security officials and their responsibilities. Within this framework, the following will be developed:

a. Security Classification Guide. This will specify how to classify, reclassify, declassify, and otherwise handle information about the DMS.

b. Basic Security Policy. This will identify minimum security safeguards that are required for operation of the DMS and its facilities and components, and for subscriber participation in the system.

c. Component Security Standard. This will regulate the life cycle of a DMS physical component from a security viewpoint. This standard will set uniform, general guidance that will apply to all components and their functions, to all organizations that deal with the components, and to all facilities and related activities that house them. The standard will include guidance for computer security evaluation criteria and clearance levels. At a minimum, automated information systems and networks that are DMS elements will be required to satisfy all security requirements that DoD policy mandates for such systems independent of their DMS role.

d. Configuration Security Guide. This will specify security requirements associated with configuration management of DMS components and facilities.

e. A set of security architecture descriptions for the Baseline, Phase 1, Phase 2 and Phase 3.

4.8 Organizational Messaging Transition.

The DMS "organizational" class of message is defined in DMS MROC 3-88, and in paragraph 1.2.3.a of this document. As the DMS evolves from the Baseline to the Target Architecture, methods for providing DMS organizational message service will change as advances in technology and standards are implemented. However, organizational messaging operational requirements contained in the MROC will continue to be satisfied during this evolution.

a. Baseline. Paragraph 2.1.4 of this document outlines how MROC 3-88 organizational messaging requirements are satisfied by the baseline AUTODIN system. To prepare for the evolution, it is important to highlight several factors about organizational messaging in the Baseline.

(1) Messages become organizational upon "release" for transmission by an authorized representative of the organization.

(2) Organizational messages are formal communications between organizations; i.e., from an organization to one or more other organizations. Which individual reader(s) in the organization receive a copy of the message is determined by the recipient organization. Organizational message originators are not authorized to circumvent the authority of the recipient organization by addressing an organizational message to an individual recipient for either action or information.

(3) Following distribution determination by a receiving AMPE, AMHS or TCC, which are Organizational User Agent (OUA) equivalents in the Baseline, actual delivery to readers is an administrative function, not subject to the full range of operational requirements imposed during transmission of the message from OUA to OUA.

(4) Baseline OUA-equivalent systems are certified to perform their organizational messaging function through a DCS AUTODIN certification process administered by the Defense Communications Agency.

(5) Increased use of electronic mail (DMS individual messaging) in the baseline has resulted in a form of message traffic rationalization. In accordance with current JCS policy, electronic mail may be designated as record communications (i.e., formal or directive in nature) within an organization if authorized by the organization commander. Electronic mail outside the chain of command is considered informal information unless prior arrangements are agreed to by participating organizations. From the DMS perspective, use of Baseline electronic mail applications for such purposes within

organizations or between consenting organizations, constitutes a determination by individual organizational heads that specific types of message traffic do not require the guarantees provided by the Baseline DMS organizational messaging system (AUTODIN). These E-mail transactions in the Baseline are considered DMS individual messaging.

b. Phase 1. DMS Phase 1 baselevel and regional transition capabilities posture the DMS organizational messaging community for evolution to the X.400/X.500/SDNS DMS organizational messaging capabilities that will be deployed during Phase 2. As AUTODIN/DDN message traffic rationalization continues, Phase 1 transitional capabilities will accelerate the transfer of AUTODIN data pattern messages to the DDN. Use of Baseline E-mail applications (SMTP or X.400) for record communications within an organization or between consenting organizations, continues to be considered DMS individual messaging. DMS organizational messaging transactions outside of the AUTODIN system (i.e., between AUTODIN and DDN subscribers or between DDN subscribers) during Phase 1 are not considered to be DMS organizational messaging until they satisfy MROC 3-88 organizational messaging requirements. Minimum satisfaction is established as equivalent to AUTODIN system requirements satisfaction, as outlined in paragraph 2.1.4 of this document, and is evidenced by successful completion of the DMS certification process. This process will evolve from the Baseline DCS AUTODIN certification process during Phase 1, and will be administered by the DMS Management Structure as the process through which candidate component systems will be evaluated and certified to perform organizational messaging functions.

c. Phase 2. Beginning with an IOC for X.400 organizational messaging, X.500 directory service, SDNS protection, and DMS Management and Control, Phase 2 provides the capabilities required for full organizational messaging transition. As organizational message writers and readers are transitioned from TCC over-the-counter service to the use of SDNS-protected X.400 Organizational User Agent (OUA) workstation messaging applications using the X.500 directory services, and the X.400 Message Transfer System (MTS), TCC phase outs will accelerate. X.400/X.500/SDNS organizational messaging will become predominant as AMPE systems and ASCs are phased out. All new components used for DMS organizational messaging will be certified through the DMS certification process that was put in place during Phase 1.

d. Phase 3. During Phase 3, X.400/X.500/SDNS organizational messaging will mature. Remaining TCCs and transition components will be phased out and the Target Architecture will be achieved.

4.9 Individual Messaging Transition.

The DMS "individual" class of message is defined in DMS MROC 3-88 and in paragraph 1.2.3.b of this document. Paragraph 2.2.4 of this document outlines how Baseline DMS individual messaging requirements are satisfied (or not satisfied) through Electronic Mail applications on the DoD Internet. As the DMS evolves from the Baseline to the Target Architecture, DMS individual messaging will derive significant benefit from the migration to international standard protocols and standard procedures, deployment of an integrated X.400 message transfer system (MTS), X.500 directory services, SDNS protection, and DMS Management/Control capabilities. While individual messaging requirements will probably never be as stringent as those for organizational messaging, the capabilities will be available to provide several grades of individual messaging service to subscribers based on services provided and cost. Certifying DMS individual messaging grades of service could be another function of the DMS certification process that will evolve from the Baseline DCS AUTODIN Certification of organizational messaging systems.

Appendix A

Phase 1 Implementation

A.0 Introduction.

This appendix amplifies the Phase 1 overview presented in Section 4, Implementation Strategy, of the DMS TAIS. It provides additional detail on the objectives, end-of-phase architecture and the actions planned to be accomplished during Phase 1. These actions have the effect of providing the foundation for the major advances which take place in Phases 2 and 3.

A.1 Phase 1 Objectives.

A.1.1 TCC Automation. The automation of existing TCC functions will reduce the need for dedicated telecommunications staff and associated costs.

A.1.2 Extension of Messaging Interface to Users. Extension of messaging interface to the writers and readers will improve originator to recipient service.

A.1.3 Transfer Data Pattern Traffic to DDN. Special emphasis will be placed on the migration of data pattern traffic away from the messaging system and toward direct data transfers across the DDN.

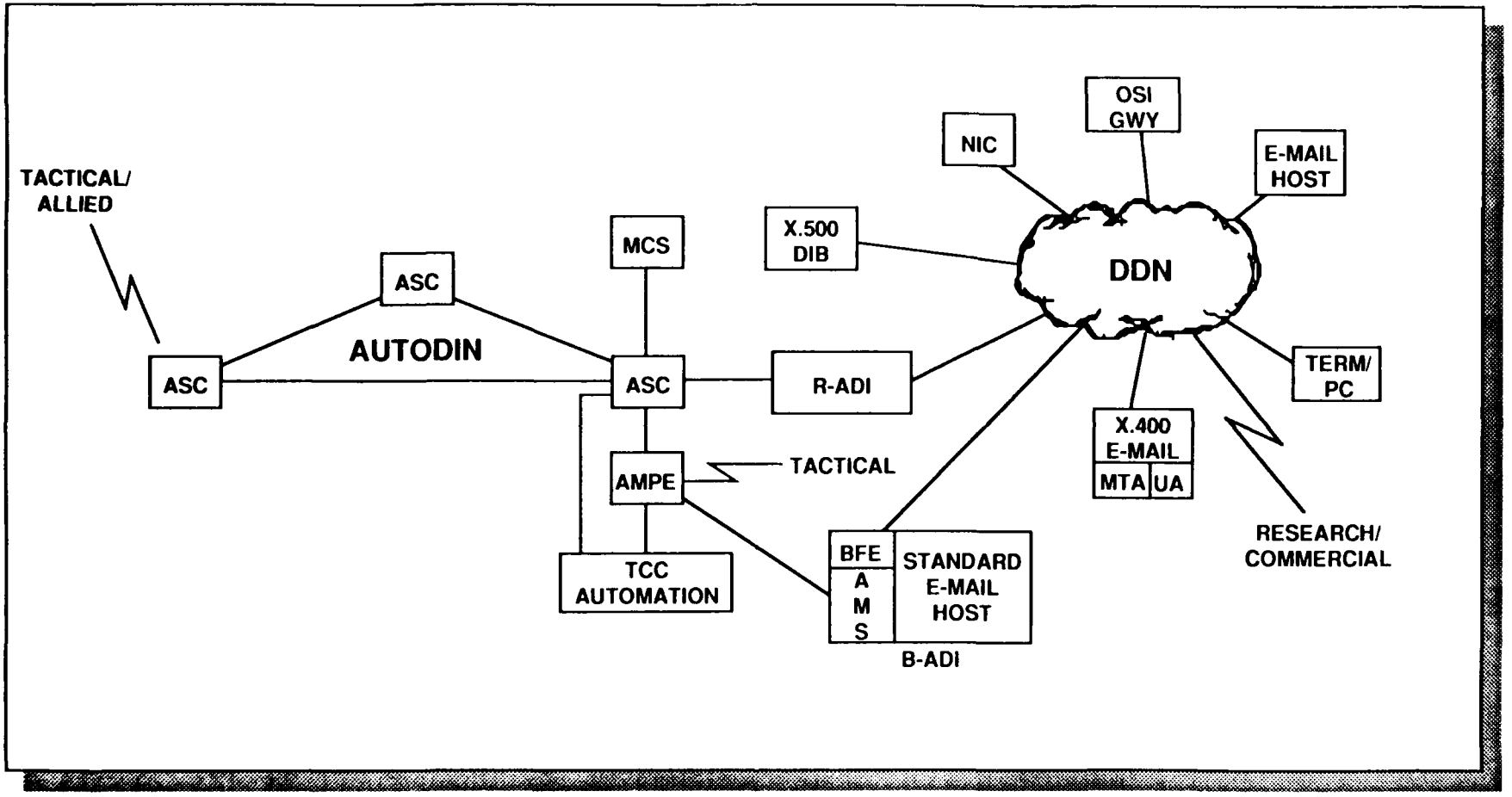
A.1.4 Eliminate the use of paper media. Emphasis will be placed on eliminating the exchange of messages, using media that is costly, bulky, difficult to maintain or staffing intensive (e.g. punched cards and paper tape).

A.1.5 Posture DMS for the phasing out of staff intensive TCCs, AMPEs and ASCs, through deployment of transitional components and initiating the transition to international standard protocols and procedures.

A.2 Phase 1 Architecture.

The major emphasis in Phase 1 is the extension of messaging service directly to the user, while posturing the DMS for evolution to Phase 2. Phase 1, depicted in Figure A-1, is characterized by the addition of AUTODIN-to-DDN Interfaces (ADI), automated Plain Language Address (PLA) to Routing Indicator (RI) conversion capabilities provided by the Message Conversion System (MCS), improved directory services to support the MCS (X.500 DIB)

Figure A-1
PHASE 1 ARCHITECTURE



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	

and to support message preparers/originators, and the migration of DDN E-Mail from Simple Mail Transfer Protocol (SMTP) and RFC822 format to X.400 messaging. In addition to the alleviation of the severe TCC obsolescence problems, this phase will lay the foundation for achieving future changes. The Defense Data Network (DDN) provides the backbone for the Baseline E-Mail and the evolving X.400 Message Handling System. The primary change occurring to the DDN during the DMS Phase 1 time frame will be implementation of BLACKER host-to-host protection elements which will ultimately result in an integrated DISNET. By the end of Phase 1, it is envisioned that the DDN will consist of the MILNET (unclassified) and DISNET (classified) segments connected by BLACKER protected gateways. The users will derive additional benefits from the ADI, MCS, and directories transition capabilities but AUTODIN and DDN E-Mail will still exist as separate but interoperable entities.

A.2.1 Components. The Phase 1 architecture consists of the Baseline components plus the transitional components. As many Phase 1 replacement and transitional components as possible will use platforms (hardware and/or operating system) which are evolvable to components needed for Phases 2 and 3.

a. AUTODIN Switching Centers (ASCs). These are the 15 ASCs of the Baseline. There will be software and hardware changes during this phase for continued viability, operations and maintenance (O&M) cost reduction.

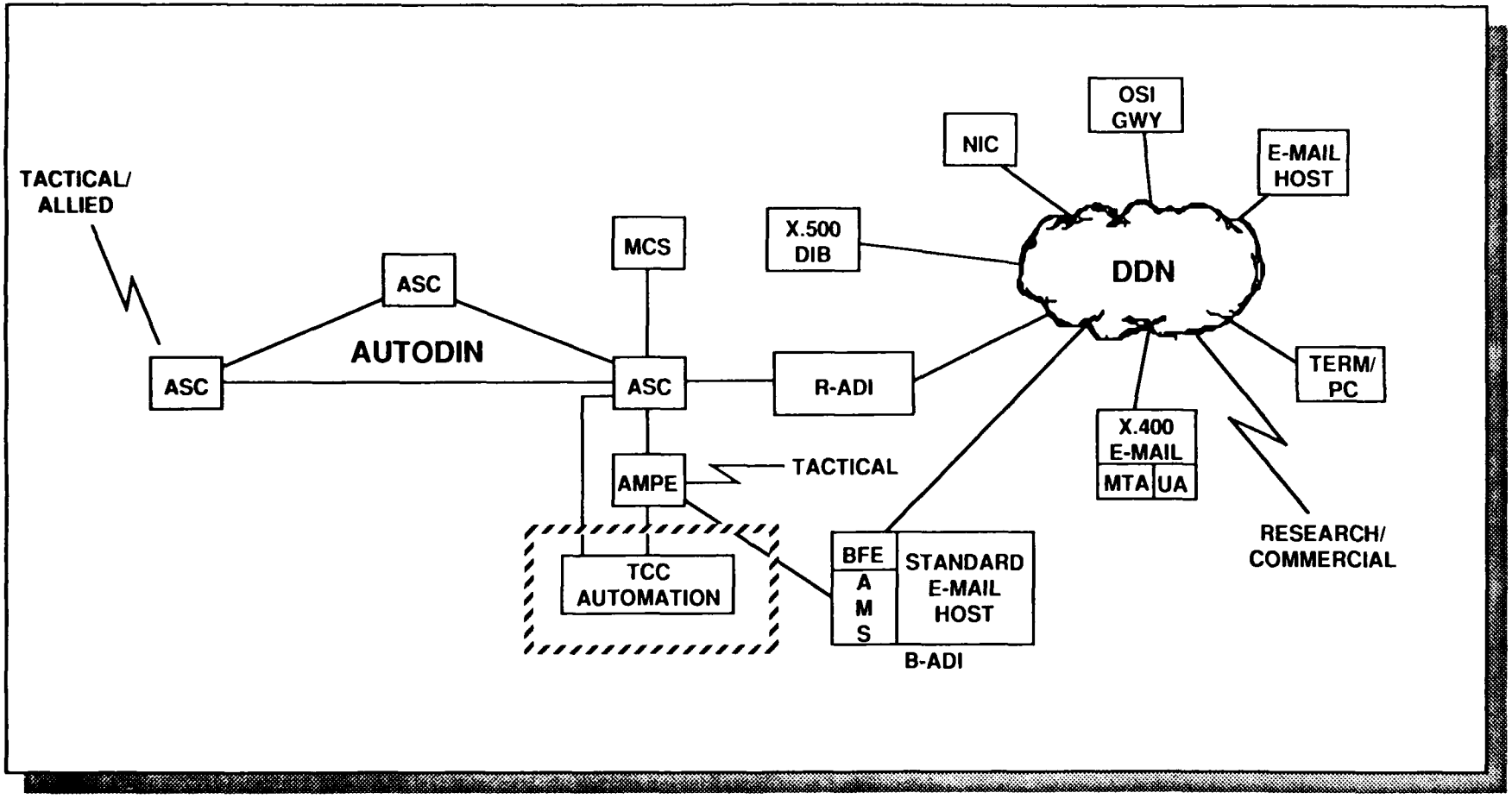
b. Automated Message Processing Exchanges (AMPEs). These are the AMMEs, LDMXs, AFAMPEs, CSPs, and STREAMLINERs of the Baseline. Specific emphasis will be placed on phasing out assembly language based systems during Phase 1 to resolve high O&M cost and obsolescence problems.

c. Telecommunications Center Automation. TCC Automation, illustrated in Figure A-2, is a compilation of the Service/agency efforts toward automating existing TCC functionality, while extending messaging service to the users to the maximum extent possible. The following is a list of these efforts:

(1) AUTODIN Interface Device (AID) with Selective Splitting (AID-SS). This project will develop, test and deploy an AUTODIN Interface Device (AID) with embedded COMSEC and a splitting capability based on security level, routing indicator, precedence and language media format.

(2) Automated Special Security Information System Terminal (ASSIST). The ASSIST is a PC-based AUTODIN terminal that is capable of accommodating DSSCS traffic in a dedicated mode of operation. It is capable of interfacing directly with an

Figure A-2
PHASE 1 ARCHITECTURE
TCC AUTOMATION



LEGEND

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

ASC, and will be used to replace Army operated DSSCS TCCs (Mod40s and the DSSCS side of a DCT9000).

(3) Desktop Interface AUTODIN Host (DINAH). The DINAH is an Army-unique PC-based AUTODIN terminal that will provide a direct interface with an ASC for classified and unclassified GENSER traffic during Phase 1. At present, the DINAH is only capable of interfacing with the AUTODIN via an AMME.

(4) Remote Terminal System (RTS). The RTS will provide automated capabilities to functionally replace all Remote Information Exchange Terminal/Standard Remote Terminal (RIXT/SRT) equipment and DCT 9000 systems with modern low cost, low maintenance hardware. The effort includes the procurement of replacement hardware and the use of a Navy developed high order language software system. The RTS may be configured to operate as a high volume base level communications system, supporting multiple remote backside communication terminals, or as a small low volume office level system. Interface to AUTODIN is provided through direct connection or through an AMPE. The RTS will provide for increased connectivity at TCCs, interfaces to the command and control and information systems which today receive messaging service from the LDMX, and will begin to provide a limited office code distribution service to its backside subscribers. The PCMT and GateGuard systems will be supported by the RTS as backside terminals.

(5) Personal Computer Message Terminal (PCMT). The PCMT is a Navy-unique terminal that allows the use of diskette media to send and receive organizational message traffic. The PCMT exchanges message traffic with the Navy AUTODIN Subscriber Terminal (AST) (i.e. LDMX, NAVCOMPARS, or RTS) over a communication link that employs the LDMX-RIXT communication protocol. ASTs will provide the PCMT with access to AUTODIN. PCMT also provides significant support for High Frequency (HF) message relay operations with the Fleet. The capability to terminate HF full period terminations and primary ship/shore circuits into PCMT eliminates the need for manual torn tape operations at Navy Fleet Centers.

(6) GateGuard. The GateGuard provides a gateway communication link from an AUTODIN Subscriber Terminal (AST) (i.e. LDMX) to an organization's Automated Information System (AIS) or Office Automation System (OAS). The GateGuard can function as either a dedicated delivery device (paper or diskette) or as a gateway. GateGuard allows electrical delivery of organizational messages to a command's AIS without requiring that the AIS be certified as an AUTODIN backside terminal. This does not release the organization's responsibility for message integrity and security which would normally be associated with

delivery of messages to recipients who are behind the GateGuard. The GateGuard software is certified to function as a backside terminal connected to the LDMX. It uses the LDMX-RIXT protocol, operating at 300 or 2400 Baud, to communicate with the LDMX. The Kermit protocol, operating at 9600 Baud, is used to communicate with the AIS. It can process GENSER message traffic through SPECAT A, while supporting JANAP 128, modified ACP 126, and standard diskette (MIL-STD 1832) formats. GateGuard software currently operates on the Zenith model 248 or Unisys PW800/20C hardware.

(7) Multi-level Mail Server (MMS). The Navy's MMS is intended to allow the electrical exchange of both unclassified and classified (up to Secret) messages to user's mailboxes. The MMS will automate the process of message dissemination, extend message delivery and point of origin to user spaces, and reduce/eliminate the exchange of paper media with the TCCs. Collocated with either the LDMX or RTS at the TCCs, it will provide dedicated and dial-up interfaces between the user's GateGuard and user mailboxes within the MMS using a B1 operating system with Secure Mail.

(8) AUTODIN PC-Based Terminal (APCT). As a possible solution to ongoing, independent efforts by the various military departments and agencies to develop/install/maintain AUTODIN terminal systems on PC hardware platforms, (e.g. SARAH, DINAH, MPDT, PCMT and ASSIST), the APCT will provide a DoD standard system, available and supportable under a "commodity" contract. This effort will provide a software system to operate on hardware platforms such as DESKTOP III and TEMPEST II. The system is to be configurable to support General Service (GENSER) only, Defense Special Security Communications System (DSSCS) only, or consolidated DSSCS/GENSER operations. Once this commercial system is available on contract and accredited/certified, Services/agencies can start to down-scale or terminate some of the resource intensive in-house developments.

(9) Standard Automated Remote AUTODIN Host (SARAH). SARAH is an Air Force developed/maintained communications software package written in Ada for the Zenith family of microcomputers. The software allows 286/386 Zenith microcomputers to transmit and receive GENSER messages from AUTODIN by either direct connection to an ASC, through an AUTODIN Interface Device (AID), or connection to the backside of an AFAMPE. SARAH-Lite is a smaller version of SARAH that provides message preparation support in the office environment. It runs on any IBM-compatible PC and allows messages to be prepared on floppy diskette for transmission via the SARAH Communications Terminal or on paper for transmission via an OCR.

(10) Communications Support Processor (CSP) Processor Upgrade Program (PUP). The CSP is an existing Automated Message Processing Exchange (AMPE) which is operated at over 60 locations by all three Services and several Government agencies. Managed by the Air Force since the mid 70s, CSP has continued to evolve and today supports multiple high speed circuits to backside host processors and data base systems. Through these backside connections, CSP provides direct, real-time message support to the backside host terminal users. The CSP PUP effort was initiated in 1987 to migrate the system from assembly language to Ada, to improve system security features, and to move to more modern and cost effective hardware. The rewritten software will be able to operate on a variety of hardware configurations and a POSIX compliant operating system such as used on the AT&T 3B2. Since CSP PUP was begun before award of the current Standard Multiuser Small Computer Requirements Contract (SMSCRC), the choice of hardware for CSP PUP development was the AN/GYQ-21(V) (Digital Equipment Corporation's VAX hardware).

(11) Classified Operational Telecommunications Switching System (COTSS). The existing Government-owned Operational Telecommunications Switching System (OTSS) currently processes only unclassified messages. This project upgrades that system to process all classification levels of GENSER traffic. The COTSS integrated system will satisfy the operational requirements at Vandenberg AFB, California to process classified messages and provide a replacement system for the Standard Remote Terminal (SRT), using the AT&T 3B2 hardware platform.

(12) Host AUTODIN Message Processing System (HAMPS). HAMPS is a software subsystem of the Standard Base Level Computer (SBLC) that connects the SBLC directly to AUTODIN for processing data pattern traffic. HAMPS reduces the SBLC workload, eliminates the "air gap" between the SBLC and the TCC which increases efficiency, reduces hardware requirements in the TCC (magnetic tape drives) and eliminates manual operator intervention at the TCC.

(13) Automated Message Handling Systems (AMHS). Automated Message Handling System (AMHS) capabilities improve the speed, accuracy, and effectiveness of processing, distributing, and viewing incoming messages and the preparation, coordination, and release of outgoing messages. The majority of the baseline AMH systems can be characterized as stand-alone processors using proprietary architectures and dedicated to processing AUTODIN messages. They typically interface to AMPEs and have directly connected operators/users. It is envisioned that a common AMHS will be defined/developed incorporating the DMS specified X.400 MHS and X.500 Directory services standards.

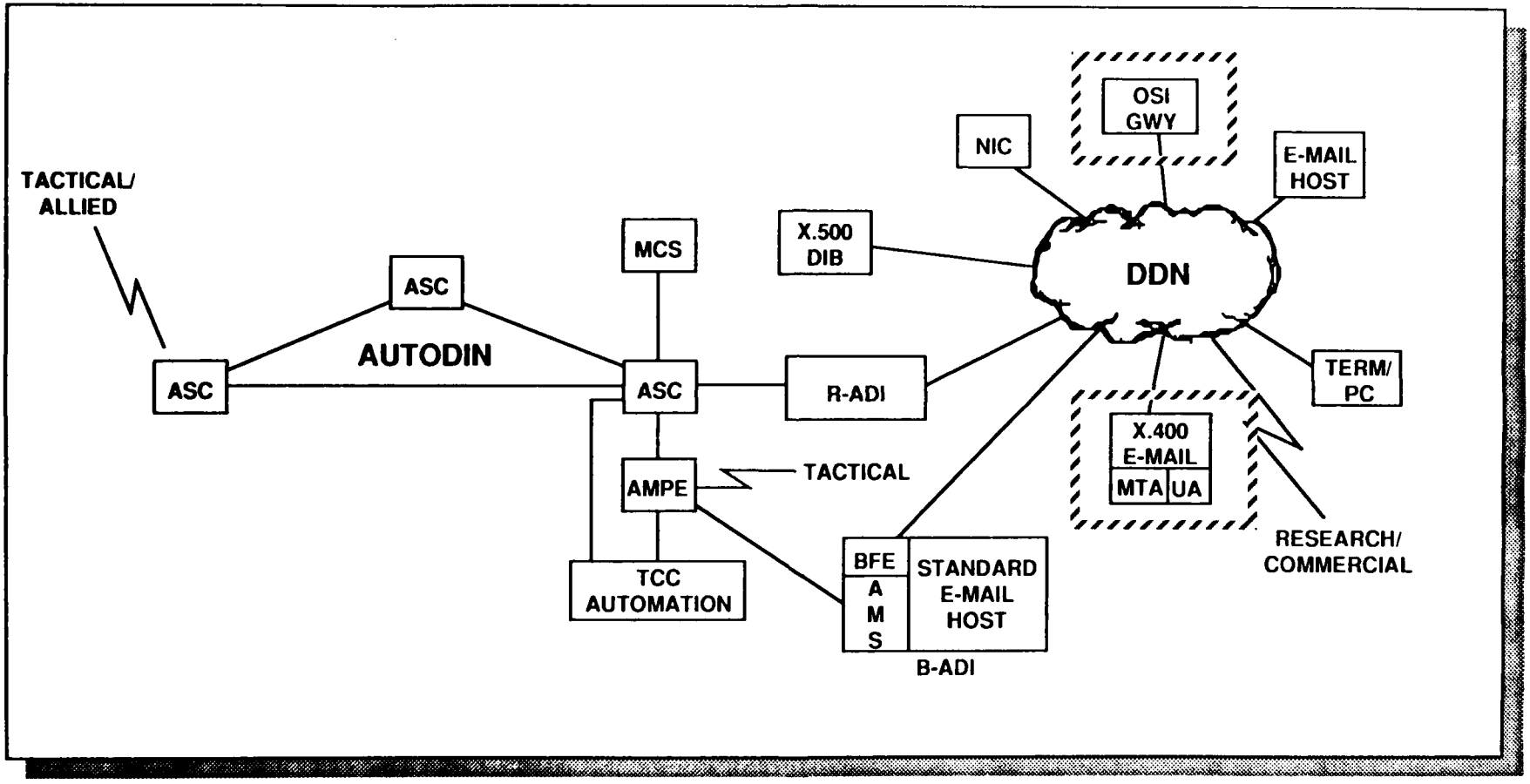
d. OSI Transition Gateway. During Phase 1, an OSI Transition Gateway will be deployed to provide translation capability between Simple Mail Transfer Protocol (SMTP) and CCITT (1984) X.400 protocol, to support early X.400 E-Mail subscribers (illustrated in Figure A-3). This will enable the deployment of X.400 based Message Transfer Agents (MTAs) and User Agents (UAs) for electronic messaging. Since X.400 (1988), with X.500 directory services support, and Secure Data Network System (SDNS) Message Security Protocol (MSP) will not be available in Phase 1, this initial deployment represents a limited implementation of the DMS Individual messaging service of the Target Architecture. Nonetheless, this deployment will begin the migration to X.400 messaging that will be expanded to X.400/X.500 Organizational/Individual messaging, with SDNS MSP protection, during Phase 2.

e. Directory Improvements. These improvements (depicted in Figure A-4), facilitate message preparation/generation, reduce the manual PLA-to-RI operations, reduce manual PLA-to-RI database maintenance efforts at AMPEs and TCCs, and support the AUTODIN-to-DDN Interface (ADI) capabilities, as discussed in later paragraphs. The following directory capabilities are envisioned:

(1) Message Conversion System (MCS). The MCS, supported by the X.500 Data Information Base (DIB), will provide automated Plain Language to Routing Indicator (PLA-to-RI) conversion for organizational messages sent via the AUTODIN network. Message originators will place Plain Language Addresses (PLAs) on their messages and route these messages (in ACP126 format) through the AUTODIN to the MCS. The MCS will accept these messages from the AUTODIN system, look up the Routing Indicators (RIs) for the PLAs, apply these RIs to the message, reformat the message for delivery back into the AUTODIN network, and send the message back into AUTODIN for delivery to the proper addressees based upon the MCS-applied RIs. The MCS will also generate appropriate error messages for conditions such as invalid PLAs. The MCS will provide a network-level/regionalized PLA-to-RI conversion capability, eliminating the requirement for TCCs and AMPEs to perform PLA-to-RI conversion (often performed manually in TCCs) and to maintain databases of ACP117 information. Organizational message originators within the DDN can also route messages through the ADI to the MCS for PLA-to-RI conversion.

(2) X.500 Directory Information Base (DIB). This will provide a centrally maintained directory at the network/regional level, which supports both the MCS and the ADI addressing functions. It will provide both the PLA-to-RI conversion information required by the MCS and the PLA-to-DDN Address

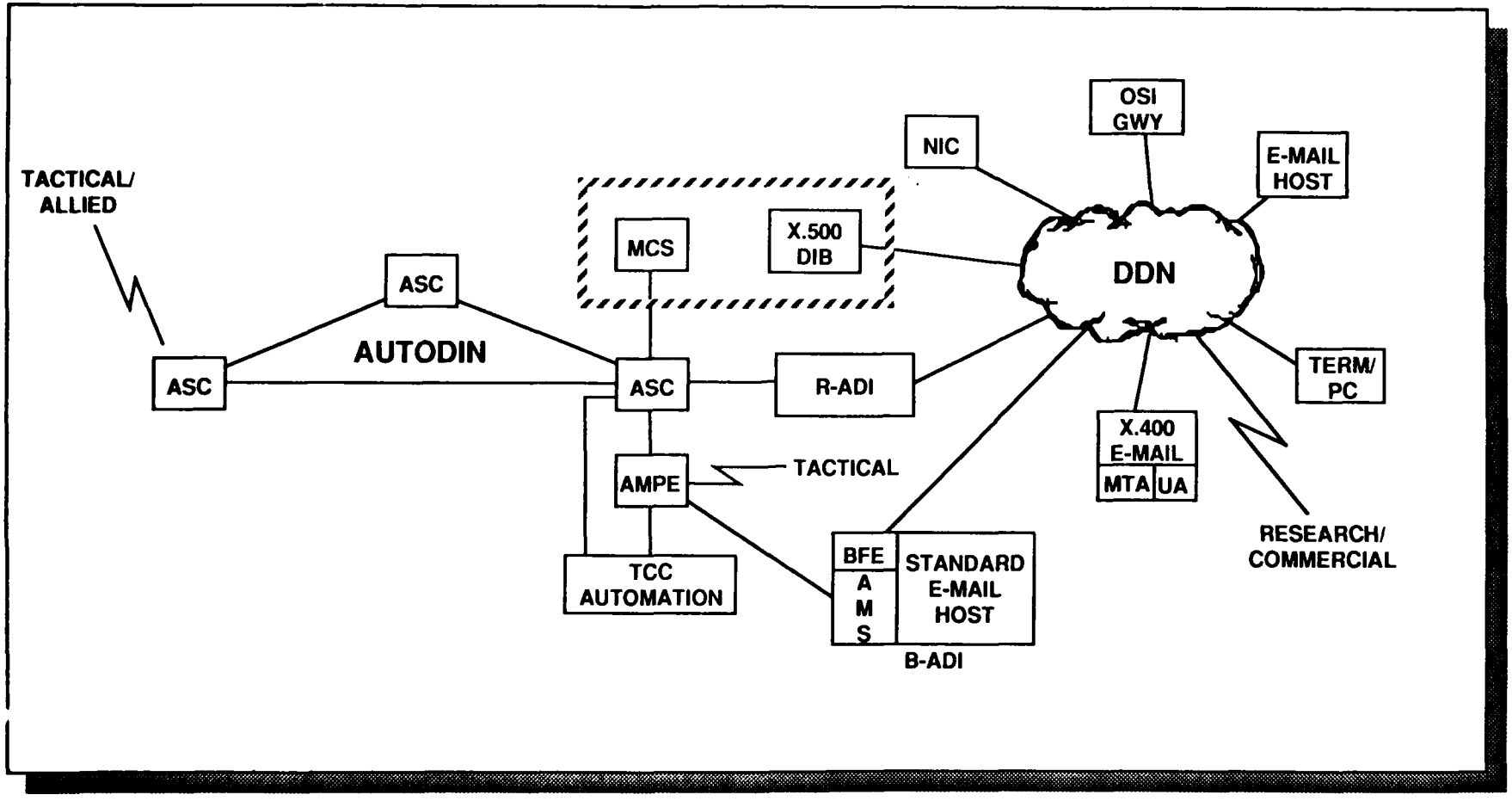
Figure A-3
PHASE 1 ARCHITECTURE
OSI TRANSITION GATEWAY/EARLY X.400 E-MAIL



LEGEND

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

Figure A-4
PHASE 1 ARCHITECTURE
MCS/X.500 DIB



LEGEND

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

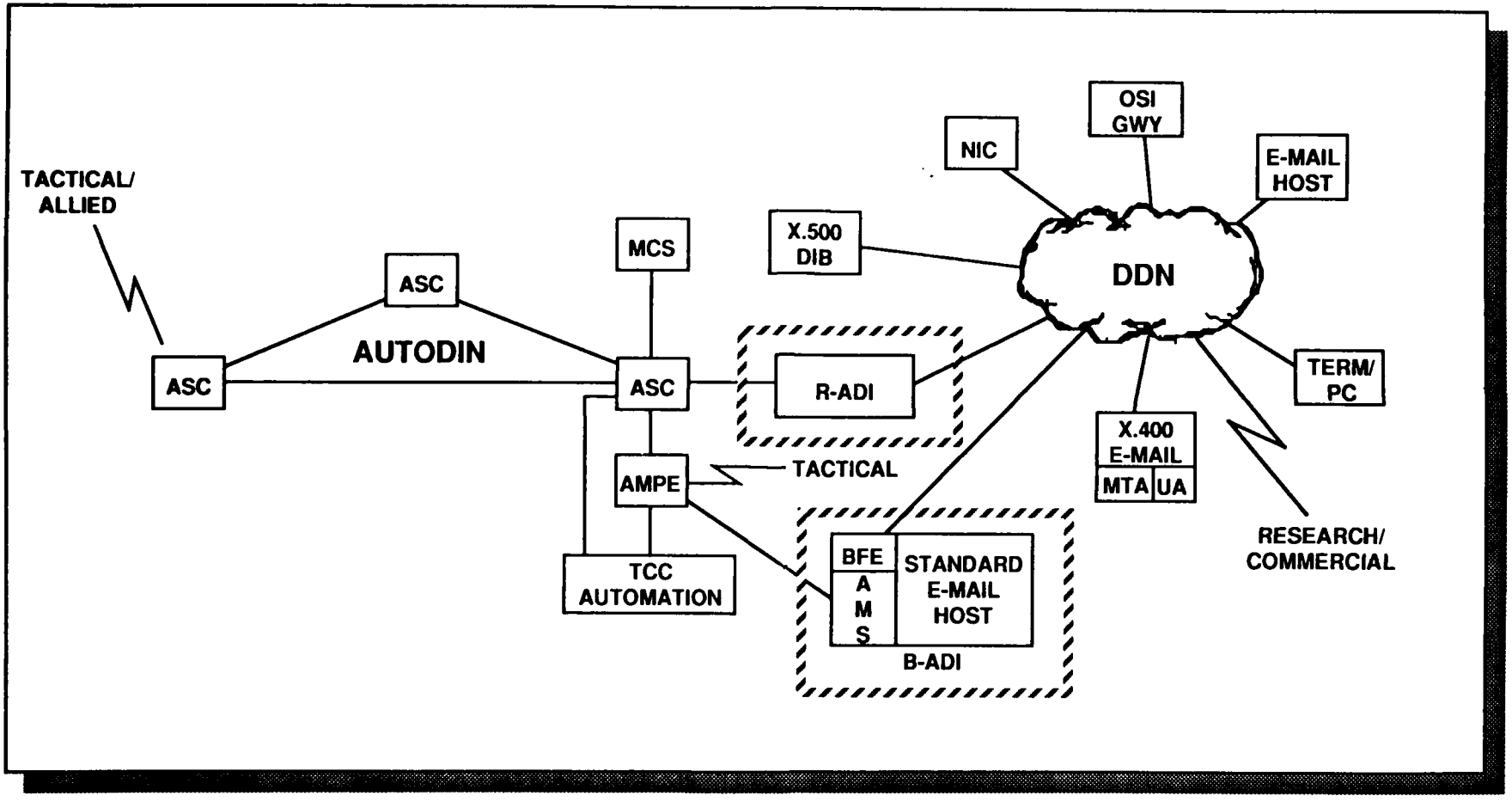
conversion information required by the ADI. The MCS components will cache the subset of directory information required to provide message addressing service to AUTODIN message originators/recipients and the ADI will cache the subset of directory information required to provide message addressing service to DDN message originators/recipients. It is currently planned that the central directory will be maintained by the various S/a update authorities, who will operate X.500 Directory User Agent (DUA) terminals interfacing to the central directory's X.500 Directory Service Agent (DSA). The DIB, which will be centrally updated by this DSA, will be replicated by the DSA to the regionally located ADI and MCS components. In order to allow the S/a update authorities to make one update to the central directories, it is planned that the central X.500 directory "peel off" an unclassified version of daily updates on a regular basis for transfer to the unclassified "MAD" directory, which will reside on MILNET.

(3) Directory to Support Message Preparation/Origination: This directory (not shown in Figure A-4) is currently still in the conceptual stage, but is viewed as fulfilling a requirement to facilitate message preparation and origination functions. Specifically, this would be an unclassified directory, accessible both via the unclassified DDN (MILNET) and also by means of distribution of floppy diskettes. It would allow users to look up the proper PLA to be used on a message, based upon the organization/location being addressed, in the same manner as the hard-copy Message Address Directory (MAD) is used today. It would also allow message preparation and origination points to verify the spelling of PLAs on messages before they are transmitted to the MCS, thereby reducing the number of errors and resultant human intervention/correction.

f. AUTODIN-to-DDN Interface (ADI). To facilitate the initial integration of AUTODIN and E-mail, two Phase 1 components are being pursued, as depicted in Figure A-5.

(1) Regional ADI. This is a transitional project which will provide the capability for AUTODIN and DDN E-mail subscribers to directly exchange organizational messages. The regional ADI (depicted in Figure A-5 as the R-ADI) will provide a direct network-to-network (AUTODIN-to-DDN) interface at the ASCs, to permit narrative and data pattern traffic flow between the two networks. Initially an ADI is planned to be implemented to interconnect AUTODIN with the MILNET, though later a separate device (with the same functionality) will probably be implemented to interconnect AUTODIN with DISNET. In Phase 2, options include the possibility of adding an X.400 capability to the ADI, in addition to the initial SMTP/RFC822 capability, to support organizational X.400 users on the DDN. The initial ADI

Figure A-5
PHASE 1 ARCHITECTURE
AUTODIN-TO-DDN INTERFACE (ADI)



LEGEND

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

implementation, being developed as a proof of concept device, will provide the following capabilities:

(a) AUTODIN-to-DDN. AUTODIN subscribers will address narrative messages to DDN E-mail users by means of AUTODIN PLAs, which will be routed to the ADI and converted in the ADI to DDN E-mail addresses. (In the proof of concept ADI this conversion will be performed using an internal ADI database, though a final ADI would obtain this data from the central DIB.) At the same time, these messages will undergo conversion (or enveloping) of the JANAP 128 message into RFC822 format for delivery using SMTP. The proof-of-concept ADI envelopes the JANAP 128 message into an RFC822 E-mail message, though the final solution may involve a JANAP 128 to RFC822 conversion if that is determined to be the optimum solution operationally. Addressing of data pattern messages to DDN users is based upon the RIs in the message, vice the PLAs as used in narrative messages. Dependent upon user requirements (defined in the ADIs database), data pattern messages received from AUTODIN may be sent to certain DDN hosts using File Transfer Protocol (FTP).

(b) DDN-to-AUTODIN. The ADI can support five methods of message origination within DDN, all of which are being implemented in the proof-of-concept ADI, as follows:

[1] An E-mail user may generate a standard RFC822 formatted message, which is transmitted via SMTP to the ADI, with the AUTODIN PLAs included as part of the SMTP addresses. The ADI then generates a JANAP 128 message using these PLAs, envelopes the original E-mail message into the JANAP 128 message, and delivers the message to AUTODIN. (Initially, the proof of concept ADI will perform PLA-to-RI conversion, though once the MCS is implemented the messages could be sent to the MCS for PLA-to-RI conversion.) Another decision to be made dependent upon the outcome of the proof-of-concept ADI is whether the RFC822 formatted message should be retained and encapsulated into the JANAP 128 message, or whether the conversion should be done in such a manner that the original RFC822 format information is eliminated.

[2] An E-mail user may generate a standard RFC822 formatted message which contains a fully formatted JANAP 128 message. The ADI removes the RFC822 information and routes the JANAP 128 message into AUTODIN. (PLA-to-RI conversion would be accomplished before the message ever reached the ADI.)

[3] An E-mail user may generate a standard RFC822 formatted message which contains a DD 173 formatted message. The ADI removes the RFC822 information, performs DD 173 to JANAP 128 conversion, and routes the JANAP 128 message into

AUTODIN. (Initially, the proof of concept ADI would perform PLA-to-RI conversion, though once the MCS is implemented the messages could be sent to the MCS for PLA-to-RI conversion.)

[4] A DDN FTP user may transfer a fully formatted JANAP 128 message to the ADI using FTP, and the ADI then routes this JANAP 128 message into AUTODIN. This capability is intended to support data pattern users who have transitioned to DDN but still need to communicate with one or more data pattern users remaining on AUTODIN. Certain access control requirements (such as requirements for maintaining user accounts and passwords) may limit the use of this functionality.

[5] A DDN FTP user may transfer a DD 173 to the ADI using FTP, and the ADI then processes this DD 173 in the same manner as discussed in [3] above. This capability is a "fall-out" of other ADI functionality, and it is unclear if it will be used significantly. Additionally, it has the same access control limitations identified in [4] above.

(2) Base-level ADI. At the base-level, the AUTODIN Mail Server (AMS) application, resident on a Multi-channel Memorandum Distribution Facility Version II (MMDF II), will provide the AUTODIN-to-DDN gateway interface (depicted in Figure A-5 as a B-ADI). The MMDF II is a standard mail host that supports a variety of communications protocols and provides a message gateway capability between DDN and other networks. The MMDF II, as a standard mail host, provides a user/action officer with an automated workstation to send/receive unclassified record communications traffic to/from a recipient at the same installation, or at another installation via the DDN, without the intervention of communications center personnel. The AUTODIN Mail Server (AMS) application will provide the conversion of message formats for message transmission/receipt over either the DDN or AUTODIN. In the case of DDN E-mail users, it supports delivery to the intended recipient's desktop workstation. Initially, it will accept either JANAP 128 or RFC822 formatted messages, convert the messages to the opposite format, and forward the messages into the opposite system, (JANAP 128 formatted messages are enveloped with an E-Mail header and trailer). Later, the X.400 channel could provide an X.400 message format conversion capability.

g. User Terminals/E-Mail Hosts. These are the PC terminals/hosts of the Baseline, used for sending and receiving E-Mail messages. With the deployment of X.400 based Message Transfer Agents (MTAs) and User Agents (UAs) for electronic messaging, and the extension of messaging service to the users in Phase 1, changes in the capabilities and level of service provided by current E-mail terminals and hosts must be improved

in order to support organizational messaging service. The reliability/availability and responsiveness of the hosts must be improved, such as 24 hour a day support, back-up power systems, improved technical and operational support, etc. These systems must be improved in their message handling and monitoring capabilities, to ensure outages of these systems are promptly detected and corrected and to ensure that excessive message delays do not result from outages. The level of security protection, authentication, and access control provided by these systems must be improved, to guarantee the integrity and security of organizational messaging. Finally, to support these security requirements the physical protection and access controls for such facilities must be strengthened.

A.3 Phase 1 Transition Strategy.

This section presents the transition strategies that support achieving the objectives for Phase 1. These strategies are structured to provide a coordinated transition from the Baseline to Phase 2. They enable the Services and agencies to integrate applicable transition actions (see Section A.4) into their Phase 1 planning.

A.3.1 TCC Automation. During Phase 1, obsolete TCC equipment will be replaced and TCC functionality will be automated. TCC equipment replacements and automation efforts will emphasize the use of evolvable platforms, standard transportable operating systems, and implementation of international standard protocols to the maximum extent possible. The Services and agencies will deploy AUTODIN replacement systems (e.g. SARAH, DINAH, PCMT and ASSIST) on evolvable platforms (e.g. 3B2 and Desktop III). A number of the baseline TCC systems will be replaced primarily because the existing systems (e.g., DCT 9000, Standard Remote Terminals (SRTs), Automated Multi-Media Exchange (AMME) systems) are costly and staffing intensive. When these objectives have been met, the TCC automation platforms, implemented during Phase 1, can evolve through successive transition steps in support of the DMS architecture and become the base for implementation of base-level Phase 2 components.

A.3.2 Extension of Messaging Interface to Users. Initiatives such as the MMDF II standard E-Mail host (with its AUTODIN Mail Server (AMS) application) will provide vehicles for writers and readers of unclassified messages to transition away from the AUTODIN Over-the-Counter (OTC) method of organizational messaging during Phase 1. The messaging interface will move to the users' work place. Phase 1 Directory improvements will offer changes in writer-to-reader connectivity by improving interoperability and reducing the need for manual handling of messages.

A.3.3 Transfer Data Pattern Traffic to DDN. The Regional ADI will provide the capability for migration of AUTODIN data pattern traffic to the DDN. Additionally, support of the Interim Policy for Transition to the Defense Message System (DMS) Target Architecture, issued by the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)), 2 November 1989, will prevent further data pattern subscribers from subscribing to AUTODIN.

A.3.4 Eliminate the Use of Paper Media. The current office automation equipment of choice is the personal computer, to include a word processing software package. Thus, floppy disks are a medium that is widespread. DoD-wide standards and procedures are being developed for Over-the-Counter (OTC) diskette operations. The advent of PC-based terminals and the handling of messages via diskettes and other electronic media, obviates the need for punched card and paper tape media.

A.3.5 Posture DMS for the Phase Out of Staff Intensive TCCs, AMPEs, and ASCs. The MCS and X.500 DIB will make PLA-to-RI conversion available to customers who are currently provided a plain language address look-up and routing indicator assignment (with associated reformatting) service from a costly and staff intensive regional message processing system. During Phase 2, implementation of international protocols and services such as the CCITT X.400 Message Handling System and X.500 Directory Services will replace obsolete AUTODIN and E-Mail messaging protocols and services (e.g. DCS Mode I, II and V protocols, Simple Mail Transfer Protocol (SMTP), and Autodin Sequential Delivery Service). The advent of X.400 messaging requires new message formats and procedures. Consequently, during Phase 1, a new Common Message Format (CMF) will be developed and documented in an Allied Communications Publication (ACP XXX). ACP XXX will serve as the international implementation agreement for use of X.400 and X.500 protocols during Phase 2, and will facilitate the eventual phase out of baseline AUTODIN (JANAP 128 and ACP 127) and Non-Standard E-Mail (RFC822) formats and procedures. Host improvements (as discussed in section A.2.1.g) will be implemented to improve the reliability and integrity of E-mail hosts so that they can support organizational messaging.

A.4 Phase 1 Transition Actions.

The following sections describe the project and policy actions supporting Phase 1.

A.4.1 Project Actions. Project actions are categorized as Central, Joint, Base-level, and R&D.

A.4.1.1 Central Projects.

a. OSI Transition Gateway. The OSI Transition Gateway provides an application-level gateway which allows intercommunications between hosts using X.400 and hosts using SMTP, and also allows intercommunications between hosts using FTAM and hosts using FTP. As an approved Central Project, a single prototype gateway has been implemented and is currently available for use. Fielding of additional gateways of this type will be driven by user requirements and the pace of X.400 implementations on DDN.

b. Message Conversion System (MCS). The MCS is an approved Central Project being developed in conjunction with the X.500 DIB, by the Navy. It is currently in the preliminary design phase, and is planned to be implemented in CY 1993 (for Beta testing in conjunction with the X.500 DIB), with full fielding to be completed in CY 1994.

c. X.500 Directory Information Base (DIB). The DIB is an approved Central Project currently being developed by the Navy as a transitional component, and is planned to be implemented in CY 1993 (for Beta testing in conjunction with the MCS), with full fielding to be completed in CY 1994.

d. Directory to Support Message Preparation/Origination. This project is still in the conceptual stage, and no firm milestones have been established, though it is required early in Phase 1. This directory would support message preparers and originators, by providing a PLA look-up function and spelling verification, thereby, reducing the frequency of invalid/misspelled PLAs.

e. Regional AUTODIN-to-DDN Interface (ADI). Development of a proof of concept ADI is on-going, and this device is to be available for initial Beta testing in CY 1991. However, there are still significant security/access control issues to be resolved before the Beta testing with operational networks can take place. The results of this Beta testing, along with on-going user actions (such as transition from SMTP/RFC822 to X.400) will better define the requirements for a final regional ADI implementation. Fielding of a final ADI is scheduled for CY 1994 and CY 1995, though earlier implementation may be possible if significant portions of the proof of concept development can be re-used.

f. ACP XXX. This project will prescribe procedures for a Common Message Format (CMF), connectivity, and interoperability with the allies, for both organizational and individual messages in the X.400 messaging environment of the DMS. It can and should serve as an international implementation agreement for X.400 and X.500 implementations, providing the vehicle for the US and its

allies to document protocol and procedural agreements that produce interoperability using X.400 while ensuring Military Message Handling Systems (MMHS) influence on developing standards. It can also serve as the vehicle to evolve to use of the imagery, voice mail, and video capabilities which can be accommodated by the X.400 protocol. The Combined Communications Electronics Board (CCEB) has sponsored an International Subject Matter Experts (ISME) Working Group consisting of the English speaking allies and the Nato Communications and Information Systems Agency (NACISA) to begin the information exchange process necessary for a collaboration on development of the first draft.

g. ASC DMS Transition Project. DCA is responsible for actions required to maintain ASC viability. During Phase 1, these actions include normal maintenance and life cycle support as well as others taken to reduce costs. The ASC Transition Project will (a) replace all components that are obsolete or will soon be difficult to maintain due to unavailability of parts, (b) improve ease of operation and reduce staffing requirements, and (c) provide a common hardware/software base for the CONUS and OVERSEAS ASC systems, allowing current ASC system reliability and maintainability until the AUTODIN network is phased out. As a result of this project, the AUTODIN network will use the same architecture and software worldwide, significantly reducing the system hardware and maintenance costs.

h. Central Testbeds. A major constraint on the DMS is funding. To ensure that the DoD gets the maximum value for its funding, testbeds are being established which will be used to operationally test DMS components prior to full-scale acquisition/deployment.

(1) R&D Testbed. A DCA lead joint R&D testbed capability is required to determine basic feasibility of DMS components planned for advanced DMS phases.

(2) Central Support Beta and OT&E Testbed. A DCA managed Central Support Testbed to perform Beta and OT&E testing will be established at the East Coast Telecommunications Center (ECTC) at Ft. Detrick, Maryland. This effort is an expansion of the current AUTODIN testing function which will use the on-line ASC and DDN capabilities.

(3) Army Beta and OT&E Testbeds. The Army has established a testbed at Ft. Huachuca, Arizona. Army operational and BETA testing will be managed from this location.

(4) Navy Beta and OT&E Testbed. Navy has established a testbed at Naval Communications Unit, Cheltenham, Maryland. Navy operational and BETA testing will be managed from this

location.

(5) Air Force Beta and OT&E Testbed. Air Force plans to establish a testbed at Gunter AFB, Alabama.

(6) DLA Beta and OT&E Testbed. DLA plans to establish a testbed at Gentile AFS, Ohio.

(7) DIA Beta and OT&E Testbed. DIA has no current plan to establish a Beta testbed. OT&E will be performed at contractor sites.

(8) NSA Beta and OT&E Testbed. NSA plans to use test facilities provided by support contract for the Telecommunications Improvement Program (TIP). The location of the NSA test facility has not been determined.

(9) DMS Non-developmental Item (NDI) Demonstration Facility. The Naval Telecommunications System Integration Center (NAVTELSYSIC) Cheltenham, Maryland has been designated to establish and manage the DMS NDI Demonstration Facility. The concept is to develop and implement a project open to voluntary utilization by commercial industry for demonstrating their products' compliance with DMS architectural objectives. It is anticipated that such a capability will encourage vendors to incorporate DMS architectural features into their commercial product lines.

A.4.1.2 Joint Projects.

a. Base-level AUTODIN-to-DDN Interface (ADI). The MMDF II/AMS, under development by Army personnel at Ft Huachuca, has been recently accepted by the Joint Projects Working Group (JPWG) as a Joint Project. It is currently undergoing final approval. The AMS, receive only, has received a complete CAT III certification on the UNISYS 5000-80, and is currently operational at two sites. Several more implementations are scheduled for this year. The transmit portion of the AMS is complete and is currently waiting for the host authentication capability to be added to the hosts. AMS/MMDF II is also being ported to the SMSCRC (Standard Multiuser Small Computer Requirements Contract) hardware platform.

b. AUTODIN PC-Based Terminal (APCT). The APCT is a DMS Joint Projects Working Group initiative, with Air Force as the lead Service, to provide a DoD standard PC-Based AUTODIN system, available and supportable under "commodity" contracts. This product is expected to be available by mid CY91.

c. Diskette Message File Formats for Defense Messaging,

MIL-STD-1832. This standard was developed by Joint Service/agency working groups with Air Force as the lead Service. It is currently in the final coordination phase and is expected to be published by December 90. Although this is not technically a DMS Joint Project, it provides the specific format details required to ensure compatibility and interoperability between all DMS users who utilize computers for message preparation on floppy diskette.

d. GateGuard. The GateGuard project was developed to provide a generic interface with the various commercially available Automated Information Systems for the electrical delivery of AUTODIN messages on the users desktop terminal. The current version of the GateGuard software operates as a backside terminal connected to the Navy's LDMX. A future release will contain the Mode I protocol that will provide the capability to connect directly to AUTODIN or backside to a AMPE. When the Mode I protocol is complete, the Navy plans to offer GateGuard as a DMS Joint Project.

A.4.1.3 Base-level Projects.

a. Army.

(1) AUTODIN Interface Device (AID) with Selective Splitting (AID-SS). The AID-SS specification has been developed by the Army, at Ft Huachuca, for the AMS and DINAH. It is planned that the AID-SS will be available by December 90, allowing the Army (with the AID-SS/DINAH combination) to commence phasing out their DCT 9000s in early 1991.

(2) Automated Special Security Information System Terminal (ASSIST). The Army ASSIST team, at Ft Huachuca, is currently porting the software to the Unisys PW 800 (Desktop III) platform. It is planned that ASSIST will be certified on both the Desktop III and the Zenith 248. This certification is currently scheduled for Oct 90.

(3) Desktop Interface AUTODIN Host (DINAH). Presently, DINAH is DCA Category III certified on the Zenith 248. The Army DINAH team, at Ft Huachuca, is currently working on a Desktop III port for the DINAH software, with certification in early 1991.

b. Navy.

(1) Remote Terminal System (RTS). The RTS effort includes the procurement of replacement hardware and the use of a Navy developed high order language software system. The software system is complete and awaiting integration to the new hardware

suite. The hardware solicitation is scheduled for release in August 1990, with a contract award projected for July 1991. Integration and certification is projected for completion by December 1991. An additional effort is in progress to install and certify the RTS software on the Desktop III platform.

(3) Personal Computer Message Terminal (PCMT). PCMT software version 3.0 is DCA Category III certified to operate as a single workstation connected to the Navy's LDMX or RIXT using the LDMX-RIXT communication protocol operating at 300 or 2400 Baud. A four workstation configuration is currently undergoing certification testing, by the Navy. Estimated completion date for the multi-workstation certification is September 1990. The software will be certified to operate on the Zenith model 248, Zenith model 386T, and Unisys PW 800/20C (Desktop III) hardware configurations.

(4) Multi-level Mail Server (MMS). The MMS will provide a hardware base, trusted software environment, and could evolve to the GOSIP protocols during DMS Phase II. The MMS will also evolve to provide the functional capabilities and connectivity necessary to migrate users from AUTODIN to DDN. Although the Navy has not yet funded the MMS, it is considered a high priority Navy project that could possibly be nominated as a Joint Project. It is currently in the requirements analysis phase, with a proposed IOC target of Summer 1991.

c. Air Force.

(1) Standard Automated Remote AUTODIN Host (SARAH). SARAH is an Ada language PC-Based GENSER only AUTODIN system that runs on the Zenith family of microcomputers. Installation of SARAH continues, and is expected to be completed by January 1991.

(2) Communications Support Processor (CSP) Processor Upgrade Program (PUP). Presently, Air Force Communications Command (AFCC) is expanding the CSP PUP effort to include a POSIX compliant version of CSP to operate on the AT&T 3B2 hardware. By redesigning and rewriting the CSP assembly language software into Ada, the CSP PUP software and hardware can be structured to support future enhancements (i.e. connection to DDN and Compartmented Mode Local Area Network) contributing to improved writer-to-reader services. Current schedule calls for completion of the CSP PUP effort by early FY92.

(3) Classified Operational Telecommunications Switching System (COTSS). This project upgrades an existing unclassified Government-owned system to process all levels of GENSER classified traffic using the AT&T 3B2 hardware platform. Current schedule for completion of the COTSS project is September

1991.

(4) Host AUTODIN Message Processing System (HAMPS). HAMPS connects the Standard Base Level Computer (SBLC) directly to AUTODIN for processing data pattern traffic. The Air Force plans to use HAMPS as a transitional vehicle until DDN connectivity and the ADI are available to all functional users of the SBLC. HAMPS is currently in the implementation phase and is scheduled for completion by mid CY91.

d. DCA and Joint Staff

(1) Automated Message Handling Systems (AMHS) Review. Under an ASD C3I tasking, DoD AMH systems are currently being reviewed to establish which features can be considered common to all DoD AMHSs and which should be unique to communities of interest. It is intended to use these features to specify common DoD messaging requirements and that they form the basis upon which the Services and agencies build their individual AMH systems during DMS Phase 1. In addition, the study will evaluate certain DoD AMH systems to establish how well they satisfy the common set of AMH features. In order to begin specifying the functional requirements of DMS X.400 based messaging components, the study will also map the AMHS features onto the X.400 based DMS components and establish how well COTS X.400 products may satisfy these messaging needs. The completion of the initial evaluation is expected during the first quarter of 1991, with further reviews to be undertaken on an ongoing basis.

A.4.1.4 R&D Projects.

a. DMS MGMT. This is currently a DCA RDT&E project to define the requirements for the management system to be used with DMS, and to develop a recommended system concept. When defined, it is expected to be designated as a Central Project. DMS MGMT will be a hierarchical, distributed function which will support the core architecture and all users of the DMS. It will perform the overall messaging service management, system status/performance monitoring, and configuration control of the MHS, and will support directory and cryptographic key service maintenance. DMS MGMT will rely upon and interact closely with the Directory and other network management entities. A primary objective is to maximize automation of the MGMT functions to make the DMS transparent and trouble free for the users, with minimal expenditure of resources.

b. Secure Data Network System (SDNS) Services.

(1) X.500 SDNS Directory. NSA has initiated a Phase 1 DMS RDT&E project to develop an X.500 SDNS Directory to support

the Phase 2 transition. The X.500 SDNS Directory will maintain and distribute information required by the SDNS MSP (i.e., cryptographic key information), the DMS Message Handling System (i.e., message addresses), as well as standard commercial X.500 information. In addition, this effort will address issues related to the requirement for either classified entries in the DMS Directory (considered classified either by themselves or in aggregate), or classified DMS X.400 message envelopes. Recommended solutions, as a result of this effort, will provide input to the further definition of the Phase 2 and 3 architectures.

(2) Message Security Protocol (MSP). SDNS MSP, used at the application layer, is a writer-to-reader security protocol used to encrypt a message's content (i.e. heading and text). This, in conjunction with security at the lower OSI protocol layers, could provide for delivery of a message through an unclassified network. This is another NSA project in support of the Phase 2 transition.

c. MSP Gateway (MSP GW). An MSP Gateway is needed because: 1) the cryptographic mechanisms used in SDNS are different than that of our Allies, and 2) the interoperability issues between users who have implemented SDNS protection and those who have not. The MSP GW is a Phase 2 project, however, associated security certification and accreditation issues which require identification and resolution, must be worked during Phase 1 to ensure that SDNS protection can be effectively implemented during Phase 2.

d. Guard Gateway. Stringent restrictions, imposed by the current DDN security policy, prevents subscribers from connecting either directly or indirectly to both MILNET and DISNET. However, a requirement exists in Phase 2 to allow DMS users to exchange unclassified messages between these two communities without traversing a circuitous route over the backbone networks. Therefore, R&D is being performed on a DMS Guard Gateway, for both the network and base-level, that will provide this capability. The Guard Gateway will ensure that classified data on DISNET is not passed to users on the MILNET, while at the same time, allowing unclassified messages to be exchanged between the two communities.

d. Mail List Agent (MLA). Submission and delivery of messages addressed to collective addresses (e.g., Address Indicator Groups (AIGs) and Collective Address Designators (CADs)) can no longer be supported by the Distribution List (DL) and DL Expansion features of X.400/X.500, with the implementation of MSP. In cases where such lists are classified, the MTA as envisioned cannot explode such lists because it operates only on

unclassified O/R names and internet addresses. In addition, submission and delivery of such messages assuming SDNS protection when the members of a collective address can number 1,000 or more, raises questions concerning the SDNS keying technique to be used for this application. Further, during the transition to full SDNS implementation, submission and delivery of messages to collective addresses when not all parties (originator and collective members) are SDNS protected, creates a problem for keying and message delivery. In order to insure an orderly transition to SDNS in Phase 2, the MLA is being studied as a possible solution. The MLA provides expansion of secure messages to a large number of recipients (as a result of processing AIGs and CADs), utilizing a 'network or group token' for all recipients rather than a unique token for each recipient.

e. COTS Technology Assessment. This effort calls for an evaluation of the capabilities of currently available or soon-to-be available technologies and/or leased services offerings that will satisfy DMS requirements as described in the TAIS, in a cost-effective manner with a minimum of/or no research and development, and to identify shortfall areas where R&D would be needed. The task specifically requires that a set of not less than eight equipment/acquisition strategies for implementing X.400 Message Handling System and X.500 Directory Service messaging systems in the near term (1990) shall be proposed in the draft analysis report. Upon acceptance by the Government, R&D shortfalls will be identified, a comparative analysis will be performed, and a minimum development approach will be recommended in the final report.

f. Trustworthy Organizational User Agent (TOUA). The purpose of the TOUA is to develop a specification and prototype implementation for an Organizational User Agent (OUA) that send and receive messages with different classifications on behalf of users with different levels of security. The prototype implementation is intended to demonstrate the viability of the specification; it is not intended to be fielded directly. The specifications will include the functions to create, store, retrieve, deliver, and display organizational and interpersonal messages. The methods applied to the specification will be based on the Secure Military Message System developed by the Naval Research Laboratory. The TOUA project has been placed in an inactive status pending identification of the funding support required to develop the specification.

A.4.2 Policy Actions. To achieve the Phase 1 objectives, the following policy actions are required.

a. JCS Policy Revisions. To accommodate the transition from AUTODIN and E-Mail to the DMS target architecture, several

existing JCS documents, (e.g. Memorandums Of Policy (MOP) 107, 165, and 195) must either be amended or replaced. In either case, new wording is required to cover transitional changes. Depending on the degree of specificity, this action may have to be iterated during the period of user transition from AUTODIN and E-Mail to the X.400 organizational and individual messaging.

b. DMS Security Policy. To support Phase 1 procedural and component actions, security policy guidance will be developed as described in Paragraph 4.7 of Section 4. These include the Classification Guide, Baseline and Phase 1 Security Architectures, and initial versions of the Basic Security Policy, Component Security Standard, and Configuration Security Guide. Among other topics, the guidance will address clearance levels of DMS component developers and facilities; interconnection of systems with different ranges of classified information, or different user clearance levels; use of non-developmental items (NDI) in secure environments; use of DMS components in multiple security environments; maintenance of accreditation as major, but evolutionary, changes are made to the DMS; use of DMS equipment developed for one security environment in other environments; and accreditation plans for individual DMS components.

A.5 Phase 1 Operational Concept.

Phase 1 is a transitional phase beginning with AUTODIN and E-Mail as separate and stand-alone capabilities and ending with initial integration. Many of the basic concepts of Baseline messaging operations will change for the better. This section presents Phase 1 organizational and individual messaging, as we know it today. The DMS Architectural Working Group (AWG) has recently initiated a study group, headed by the Army, to develop detailed operational concepts for each of the three DMS phases. It is planned that the information gained from this study will be incorporated in future updates to the TAIS.

A.5.1 Organizational Messaging. An integration of AUTODIN and DDN E-mail messaging services is supported by the regional/network level AUTODIN to DDN Interface (ADI) and is further facilitated by the X.500 DIB which provides directory information to the ADI. Messages can be addressed to organizational users on either network, and several different message formats will be accepted by the ADI from selected DDN users. These include RFC822 transferred to the ADI by means of SMTP, JANAP 128 messages transferred to the ADI by means of SMTP, and DD173 messages transferred to the ADI by means of SMTP. This flexibility facilitates transition of organizational users to DDN, by allowing them to continue message preparation in the format they currently prepare (such as DD173) and to use DDN to pass these messages to AUTODIN via the ADI. Later their message

preparation software can be modified to support other formats accepted by the ADI if operationally beneficial. The ADI supports the extension of messaging to the writers' and readers' desktops, by using E-mail for message origination and delivery, and eliminates delivery of paper/diskette DD173s to the TCCs for Over-the-Counter (OTC) service. This same extension of messaging to the writer and reader is also supported, to an even greater extent, by the AUTODIN Mail Server, Multi-level Mail Server (MMS), and Office Automation Systems (OASs) via GateGuards. Additionally, all of these systems provide significant added features and functionality to support the user over and above the capabilities provided by the ADI. The MCS, and its associated X.500 DIB, allows users to submit messages (either directly into AUTODIN or indirectly via an ADI/AMS) without requiring PLA-to-RI conversion to be performed at a TCC or AMPE. Rather, this function will be performed at the MCS, eliminating the manual PLA-to-RI functions and database maintenance functions required of TCCs and AMPEs. A further directory service would be available to users (message preparers and originators) to look-up and verify the spelling of PLAs during the message preparation process. It is expected that this capability would be made available either through the MILNET or locally at the base level. The typical installation configuration for the end of Phase 1 will use the MILNET for unclassified message exchange, and terminals (many of which will be PC-based) on AUTODIN for classified service. Classified messages will be accommodated via OTC service at TCCs with floppy diskettes, or electronically by those that have the capability (e.g. MMS or DINAH). During Phase 1, a significant volume of unclassified AUTODIN messages will be shifted to DDN, initially in E-mail format and later as X.400 messages, facilitating the reduction and eventual phase-out of TCCs, AMPEs, and ASCs.

A.5.2 Individual Messaging. E-Mail users will initially experience little change as the E-Mail community moves from SMTP to X.400. This change is largely a replacement of one protocol for another and does not provide the messaging capabilities provided by the UA/DUA/SDNS functionality of the Target Architecture. However, the improvements in the level of service provided by the E-mail hosts in order to support organizational messaging, in areas such as system availability, system monitoring, 24 hour a day support, and security/access control, should improve the service provided to individual messaging users.

A.6 Comparison to Requirements.

Each requirement contained in Section 1 is listed below with a brief explanation of changes made to the current baseline by the implementation of Phase 1. Where there has been no change in

the satisfaction of a requirement, this is so stated.

a. Connectivity/Interoperability. The connectivity and interoperability will be significantly improved as a result of the introduction of AUTODIN-DDN Interfaces (ADIs) and the associated DIR improvements. The ability for individual users to have ready access to any/all messaging services will be improved and initial rationalization of AUTODIN/DDN message traffic will be possible.

b. Guaranteed Delivery. The implementation of more sophisticated protocols will provide guaranteed delivery and notification to the sender. This will replace the existing protocols and manual procedures used to guarantee delivery.

c. Timely Delivery. As the messaging interface is extended to the user level, significant improvement in writer-to-reader speed-of-service will be realized based on the reduction of manual handling.

d. Confidentiality/Security. The use of Host-to-Host protection, required on the MILNET to provide security for organizational messaging, will provide confidentiality/security that did not exist in the Baseline.

e. Sender Authentication. Host-to-host protection between the MMDF II/AMSs on MILNET will result in improved authentication and protection of unclassified sensitive messaging.

f. Integrity. As obsolete base-level equipment and protocols such as DCS Modes II and V are replaced by newer equipment and standard protocols, end-to-end message integrity will improve.

g. Survivability. While survivability of the AUTODIN Switching Centers (ASCs) is unchanged, the ability of organizational DDN users to access surviving ASCs via the ADI could mitigate the impact of loss/failure of ASCs.

h. Availability/Reliability. The phase in of evolvable equipment and the phase out of obsolete equipment should result in availability and reliability improvements as well as reduced O&M costs.

i. Ease of Use. The improvements in terminal equipment available to the user and improved directory service should contribute to improved ease of use.

j. Identification of Recipients. The directory service improvements planned for Phase 1 should result in improvements in

service to the users.

k. Preparation Support. For the users affected by the limited introduction of X.400 messaging and improved directory service, there will be improvements.

l. Storage and Retrieval Support. No changes to the current baseline are envisioned for Phase 1. Introduction of the X.400-based Message Store (MS) and the OUA which will provide this support will take place in Phase 2.

m. Distribution Determination and Delivery. Extending service to users will result in some improvement since it begins the phase out of over-the-counter (OTC) service.

Appendix B

Phase 2 Implementation

B.0 Introduction.

This appendix describes Phase 2 of the Defense Message System (DMS). Phase 2 spans the 1995 to 2000 time frame. The early part of Phase 2 is a transitional messaging environment consisting of the baseline AUTODIN messaging system and Defense Data Network (DDN) E-mail systems, and the X.400 Message Handling System (MHS). As shown in Figure B-1, Phase 2 begins with the Initial Operational Capabilities (IOCs) of the DMS X.400 MHS, a distributed X.500 Directory Service, and the Secure Data Network System (SDNS) Message Security Protocol (MSP) and ends when the last ASC is closed. During Phase 2, the extension of the automated TCC services to the user continues, accelerating the phasing out of the baselevel Telecommunication Centers (TCCs). Additionally, DDN E-mail users are transitioned to the X.400 MHS, and the DDN Simple Mail Transport Protocol (SMTP) is phased out. By the 2000 time frame, the DMS is well positioned for Phase 3. The following sections expand upon this evolutionary scenario of Phase 2 of the Defense Message System.

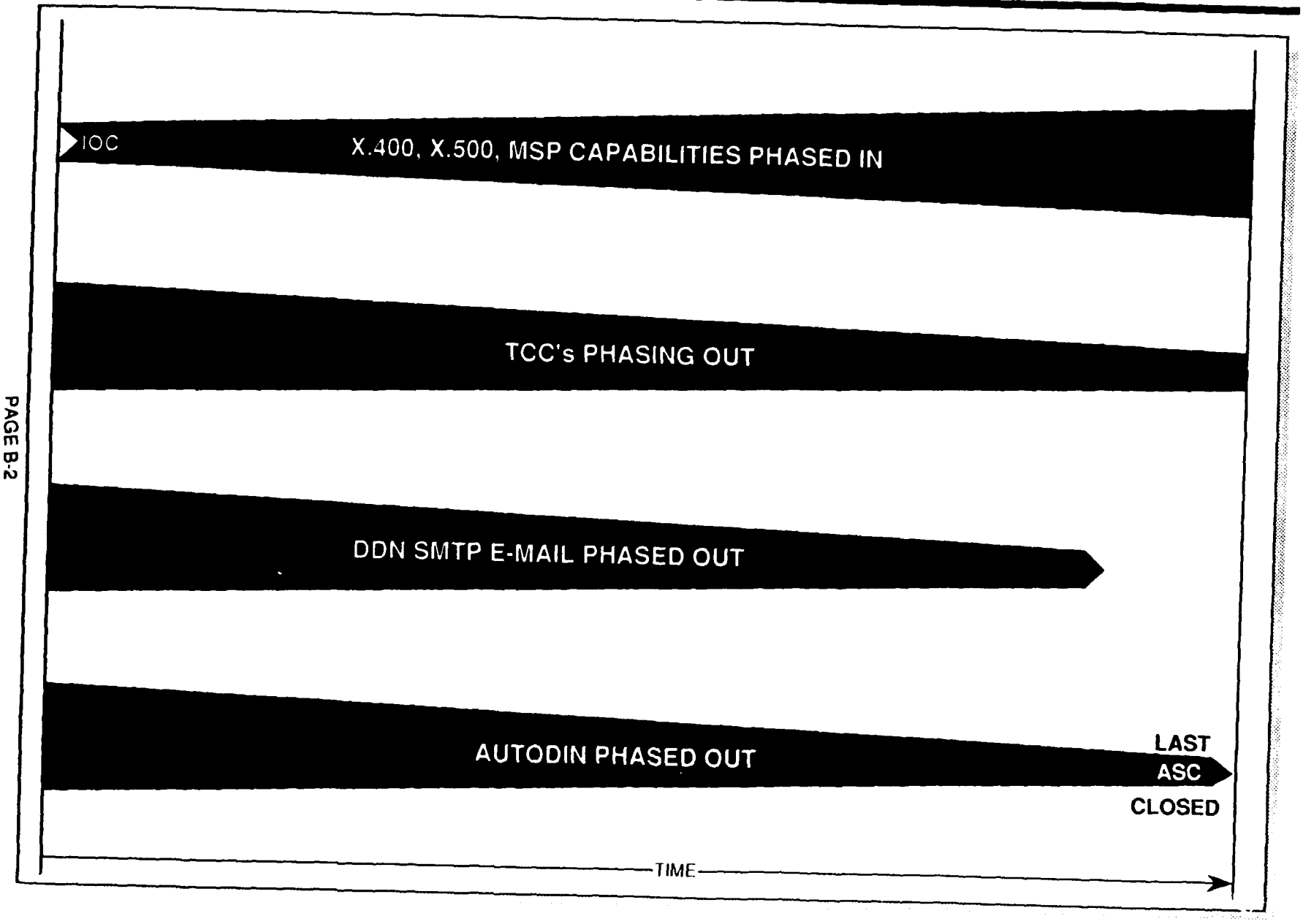
B.1 Phase 2 Objectives.

This section presents the Phase 2 implementation objectives. The achievement of these objectives positions the DMS for transitioning into Phase 3.

B.1.1 Expand writer-to-reader connectivity and support. This objective allows users to transition from the baseline AUTODIN system to DISNET and MILNET using DMS components at the user's workplace. Through the use of transitional gateways, any DMS subscriber will be able to exchange messages with any other DMS subscriber. From their existing workstations, DMS users will have the capability to create, edit, send, receive, read, process, and protect organizational and individual messages. The achievement of this objective also marks the completion of the Phase 1 initiative of extending the automated TCC functions to the end user. Base and network level messaging support functions will be implemented to support these new messaging capabilities. The DMS relies upon the base and network level data transport systems for transmission connectivity and associated security services.

B.1.2 Provide writer-to-reader message security services. The accomplishment of this objective will provide writers and readers

Figure B-1
PHASE 2 OVERVIEW SCENARIO



the security services for end-to-end protection of DMS messages. All DMS messages will be afforded the following security services: data confidentiality, data integrity, authentication, access control, and non-repudiation with proof of origin. Both applications-layer (i.e., GOSIP layer 7) and lower-layer (i.e., GOSIP layers 1-4) security services are needed to achieve this objective. The DMS provides the application layer security services by use of MSP and relies upon the Service/agency (S/a) Installation Information Transfer Systems (IITS) and Information Transfer Utility (ITU) of the Defense Information System (DIS) for lower-layer security services, including traffic flow confidentiality if required.

B.1.3 Phase out baseline messaging systems. As objectives B.1.1 and B.1.2 are achieved the AUTODIN messaging system and DDN SMTP-based E-mail systems are phased out. Both the AUTODIN ASCs and the use of SMTP are to be completely phased out during Phase 2. For a variety of reasons, some baselevel TCCs remain into Phase 3; however, Phase 2 ends with the closing of the last AUTODIN ASC. By the middle of Phase 2, the contents of the integrated MCS database, the X.500 Central DIB, the DDN E-Mail directory, and the X.500/SDNS directory are merged into a single DMS Directory.

B.1.4 Phase out baseline message formats and procedures. ACP-127, JANAP-128, and RFC 822 describe the baseline message formats and procedures used by AUTODIN (ACP-127/JANAP-128) and SMTP E-mail (RFC 822) users. As the baseline messaging systems are phased out, DMS subscribers are transitioned to the Common Message Format (CMF) and procedures specified in ACP-XXX.

B.1.5 Maintain message exchange interoperability between the DMS and non-DMS systems. Non-DMS systems include the Internet (government-sponsored research activities within the commercial and academic communities in the U.S. and Europe), other Federal data networks, and message-exchange networks in U.S. tactical and allied forces. To ensure interoperability between the DMS and the non-DMS message systems until all are fully standardized on X.400 MHS, the DMS will provide transitional interface components.

B.1.6 Implement Phase 2 in a cost effective manner. Component price and security features are the prime cost drivers in Phase 2. The DMSIG will manage the transition and implementation strategies to keep these costs minimal. Resource sharing, staged deployment, use of commodity contracts, and implementing only the minimum required security features are key cost effective implementation strategies.

B.2 Phase 2 Architecture.

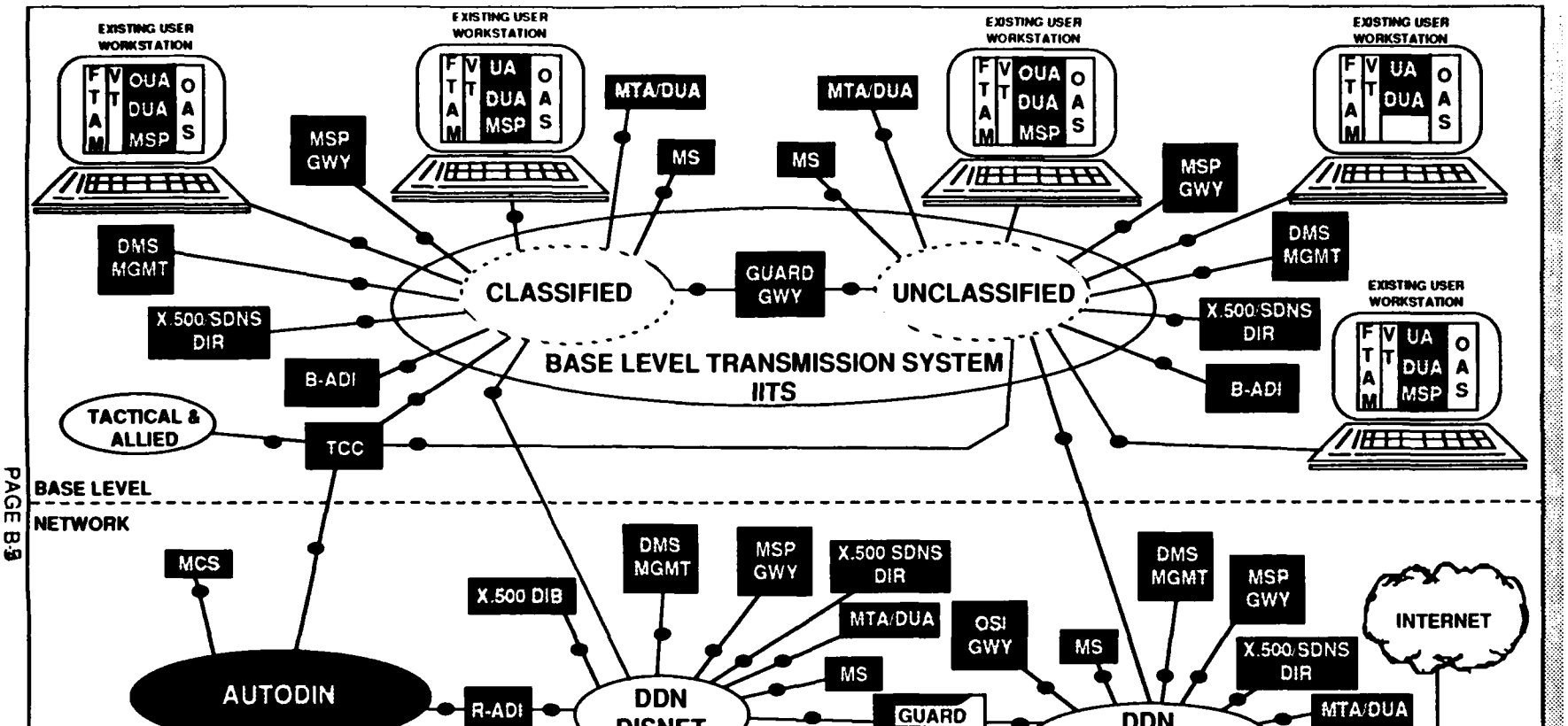
Figure B-2 shows the transitional environment of early Phase 2. Interfaces are in place to maintain interoperability among the transitioning message systems. Figure B-3 reflects the end of Phase 2, when the DMS is a relatively homogeneous X.400/X.500/MSP environment supported by the maturing IITS at the base level. By then, the DMS will have successfully achieved the objectives listed in paragraph B.1 and is well postured for beginning Phase 3. The Phase 2 architectural components are described below.

B.2.1 Messaging Components. Writer-to-reader messaging capability at the user's workplace is provided by the following components in the Phase 2 architecture:

B.2.1.1 X.400 Message Handling System (MHS). The X.400 MHS includes User Agents (UAs), Message Transfer Agents (MTAs), and Message Store (MS) functionalities. A detailed explanation of these components is contained in CCITT, Data Communication Networks Message Handling Systems, Blue Book, Volume VIII - Fascicle VI2.7, 1988. A DMS-unique Organizational User Agent (OUA) is included in the DMS X.400 MHS to satisfy specific DoD requirements for handling organizational messages. The commercial X.400-based software should provide six messaging functions: composition, transfer, reporting, conversion, formatting, and disposition. These functions are provided through elements of service associated with the particular features, functions or capabilities of the UA, OUA, MTA, and MS. Elements of service address specific actions such as access management, delivery notification, and precedence indication. The required X.400 optional service elements for the DMS MTA, UA, and OUA, and MS have not been defined at this time. The X.400-based software can be viewed from two distinct, but related, perspectives: providing human interface into the DMS and delivering the messages to the recipients. The UA, OUA, and MS provide human interface and interoperate with the MTA, whose primary function is message delivery.

a. User Agent (UA). The X.400 UA software is an integral portion of the Commercial Off-the-Shelf (COTS) software which users will acquire along with their workstations/host computers, or will acquire separately and install into existing workstations/host computers. The UA and its associated applications software interact directly with the users allowing them to create and edit an individual message (heading and body) and submit that message to its Message Store (MS), if implemented, or to its Message Transfer Agent (MTA) for transmission. The UA interacts with its MTA or MS to submit and receive individual messages on behalf of the user. Associated

Figure B-2
EARLY DMS PHASE 2 ARCHITECTURE

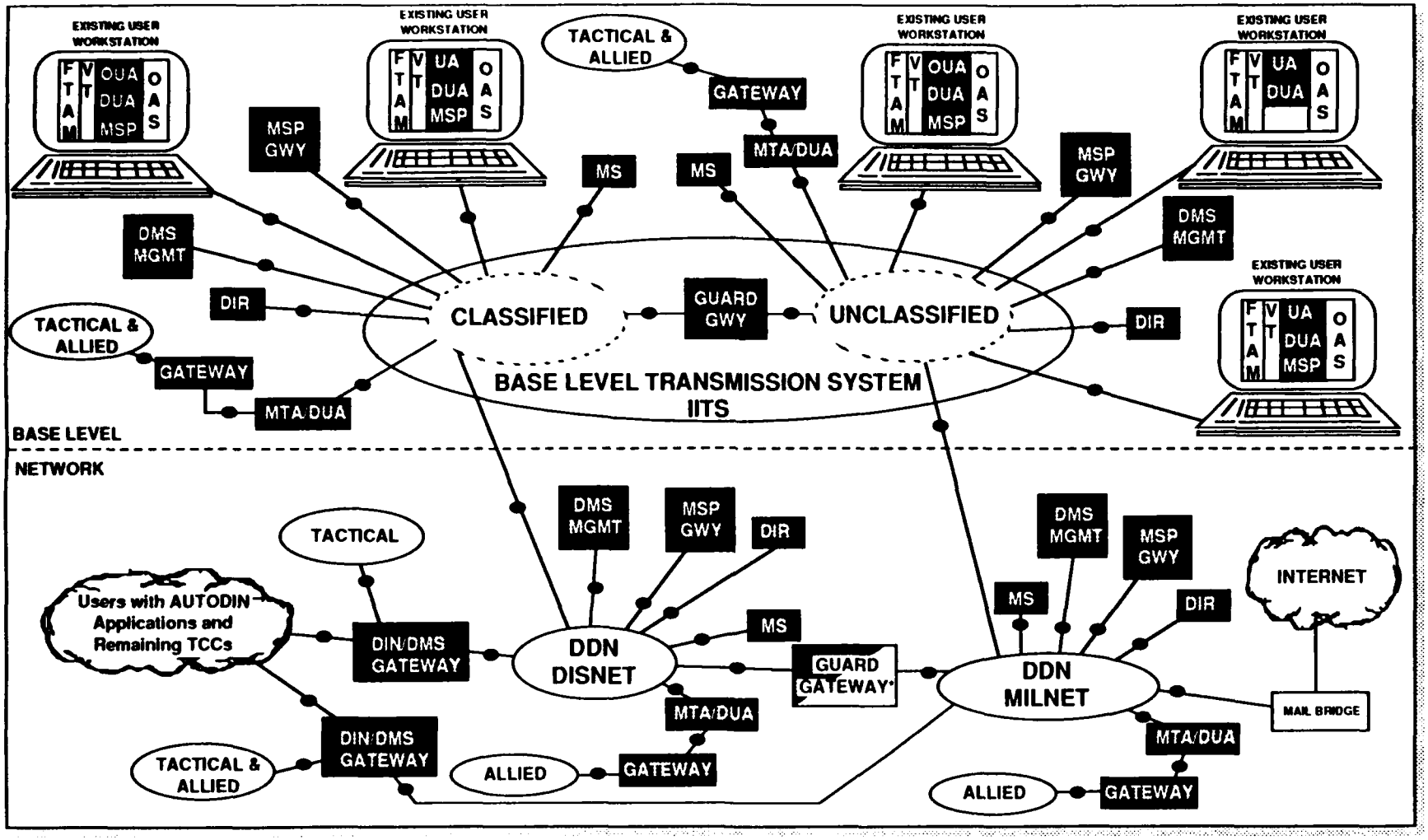


PAGE B-9

LEGEND

- DMS Functions and Components
- * - Joint DDN/DMS component
- Lower Layer Security
- MCS - Message Conversion System
- B-ADI - Baselevel - AUTODIN to DDN Interface
- R-ADI - Regional - AUTODIN to DDN Interface
- Name Server Host - DDN E-Mail Name Server Host
- MSP GWY - SDNS MSP Gateway
- X.500 DIB - X.500 Directory Information Base
- X.500/SDNS DIR - X.500/SDNS Directory
- MS - X.400 Message Store
- IITS - Installation Information Transfer System
- FTAM - File Transfer, Access, And Management
- OSI GWY - Open Systems Interconnection Gateway
- OUA - Organizational User Agent
- UA - User Agent
- DUA - X.500 Directory User Agent
- MSP - SDNS Message Security Protocol
- MTA - X.400 Message Transfer Agent
- VT - Virtual Terminal
- NIC - Network Information Center (DDN E-Mail)
- Login Host - DDN E-Mail User Login Host

Figure B-3
END DMS PHASE 2 ARCHITECTURE



LEGEND

- DMS Functions and Components
- Joint DDN/DMS Component
- Lower Layer Security
- MCS - Message Conversion System
- MSP - Message Security Protocol
- IITS - Installation Information Transfer System
- MSP GWY - SDNS MSP Gateway
- DIR - Integrated X 500/SDNS Directory
- MS - X.400 Message Store
- MTA - X.400 Message Transfer Agent
- VT - Virtual Terminal
- DMS MGMT - DMS Management Capability
- FTAM - File Transfer, Access, And Management
- OUA - Organizational User Agent
- UA - User Agent
- DUA - X 500 Directory User Agent
- DIN/DMS GWY - AUTODIN - DMS Gateway

DMS software using common structured menu formats prompts the user in producing individual messages in the ACP-XXX CMF. It also receives and displays incoming message content and, if requested, prepares receipt notification messages. In addition, the UA assists the user in related messaging functions such as replying, forwarding, filing, and retrieving. Whenever the UA is off-line or inoperable the MS, if implemented and not collocated with the UA, or the MTA stores incoming messages for subsequent retrieval when the UA becomes operational. The UA may reside in a terminal such as a PC along with other applications such as word processing, spreadsheet and file transfer, providing the user with multi-functional support. The user is guided through the messaging session through user-friendly, man-machine interfaces such as formatted screen displays, icons, menus, and help functions. This associated software allows the user to create, edit, send, receive, process, store, and, when equipped with MSP, encrypt/decrypt ACP-XXX CMF formatted messages. Individual messaging scenarios are provided in Section B.5 (Operational Concept).

b. Organizational User Agent (OUA). The OUA is UA software enhanced to include the features necessary to handle DMS organizational messages. It is an application typically implemented on a PC along with other, non-DMS applications software. The OUA appears to the MHS as a UA, in that it consists of all the normal UA functions to create, edit, submit, receive and process messages. The OUA is specifically designed to perform the DMS unique functions necessary to release, determine distribution, provide accountability, store and retrieve organizational messages. Satisfaction of the unique DoD requirements associated with organizational messages requires the OUA to perform the following functions:

- approval of organizational messages prepared locally or by other subordinate UAs in the organization. This is known as the message release authority function.

- automated distribution determination and submission of delivered organizational messages for subordinate UAs in the organization.

- guaranteed delivery of messages with high precedence or high classification received at any time of the day or night, by any means.

- returning a message that cannot be released to the originating UA/OUA or forwarding the message to another OUA for release (e.g., for messages that must be released at a higher organizational level).

- storage of organizational messages.

- maintaining writer-to-reader message accountability.

A PC/workstation containing an OUA and its associated applications software also contains a UA capability thereby allowing an organization to process both organizational and individual messages. To ensure immediate human intervention and action on all organizational messages, the message store functionality is incorporated within the OUA. The OUA software, based on common structured menus, produces organizational and individual messages as specified in ACP-XXX. The user is guided through the messaging session through user-friendly, man-machine interfaces such as formatted screen displays, icons, menus, and help functions. Organizational messaging scenarios are provided in Section B.5 (Operational Concept).

c. Message Store (MS). The MS is an optional capability of the X.400 MHS that acts as an intermediary between the UA and the MTA. There is one MS per UA. When supported by an MS, all messages destined for the UA are delivered to the MS only. The UA, if on line, can receive alerts when certain messages are delivered to its MS. Messages accepted by an MS are considered delivered. When a UA submits a message to the MTS, the MS is in general transparent to the UA; the MS submits it to the MTA before confirming the success of the submission to the UA. For UAs not on-line, the MS, if not collocated with the UA, stores the messages until the UAs become operational. If the MS and UA are both not on-line, and no alternate delivery is indicated, the originator receives a non-delivery notification from the MTS. The user can obtain a listing of messages of specified types and a summary of information about the messages stored in his MS. The user can delete messages from the MS. The MS can alert its UA when messages of specified types are received and can automatically forward a delivered message according to the its user's instructions. Both UAs and MSs can be implemented on a wide variety of PCs and workstations. For individual messaging, the MS can be implemented with the MTA or with the UA; for organizational messages, the MS must be collocated with the OUA in order to meet the MROC organizational messaging requirements.

d. Message Transfer Agent (MTA). MTAs are application-layer software that operate together, in a store-and-forward manner, forwarding messages and delivering them to the intended UA, MS, OUA, or gateway. The function of an MTA is to forward submitted messages to the next MTA, to a distribution list expansion point, or to one of its associated UAs, MSs, OUAs, or gateways in accordance with the instructions on the X.400 envelope. The MTA uses the Directory services, as necessary, to effect the desired messaging service. MTAs neither

modify nor examine the envelope's content. When an UA, MS, or OUA submits a message to its associated MTA, the MTA checks the message envelope syntax for validity, and if an error is found, returns it with the error codes. If valid, the MTA stamps the message with a date/time and thereafter treats the message as it does one coming from another MTA. The MTA next checks to see if the message can be delivered within its local domain. If not, the MTA forwards the message to another MTA according to the addressing information contained on the envelope of the message (see para 3.1.b of the TAIS). MTAs also provide administrative auditing and data collection on the messages that they process. This information is used by the DMS management capability for monitoring and managing the DMS. MTAs can be implemented either co-resident with a UA/OUA or in a separate computer. For efficient service and delivery, the MTA will contain profiles of those user facilities with which it normally communicates. Each MTA, selected MTAs, or some combination can, in conjunction with the Directory services, expand distribution lists. The DMS implementation of this X.400 feature may be limited by MSP. MTAs are implemented at the base and network levels. The MTAs rely upon the IITS and the DDN for transmission, routing, and delivery of the data between MTAs.

e. Directory User Agent (DUA). DMS users acquire and install X.500 DUA software programs in their existing workstations. DUAs are also located in MTAs and gateways. The DIB systems administrators/local custodians will have DUAs so they can maintain the Directory database. Each DUA represents precisely one directory user. The DUA provides the interface between the user and the Directory. Additionally, the DUA maintains a cache database of local addresses. Every user (i.e., UA, OUA, MTA, and gateway) has access to those authorized Directory components required for the support of their DMS functions. The Directory returns the recipient(s) O/R name and MSP certificates. The DUA interacts with the Directory by communicating with one or more Directory System Agents (DSAs) either on a referral or a chaining basis. Thus, a DUA is not bound to one DSA. An underlying protocol, the Directory Access Protocol (DAP), provides user access authentication between a DUA and a DSA. The DUA provides the following basic functions to the user:

(1) Look-up. The user, through his DUA, supplies the DSA a Directory name, together with appropriate attributes. The DSA interacts with the Directory and returns the recipient(s) Originator/Recipient (O/R) name and MSP certificate. This is the most common use of the Directory.

(2) Browsing. The DUA allows the user to browse through the Directory when descriptive names are not clearly

known.

B.2.1.2 Directory (DIR). In relation to DMS, the DIR contains the information necessary for the X.400 messaging system to function. It supports accesses by DMS components which require this information in order to function properly, and accesses by human users who can ascertain information regarding other DMS users based upon specific attributes. An entry in the DIR consists of a set of attribute types and attribute values. Attribute types and values are explained in the CCITT X.500 reference cited below. Each use of the DIR is subject to an access control service provided by the DIR or another application. The Directory components can be categorized into two parts: a Directory System Agent (DSA) that interfaces with the user and the Directory Information Base (DIB). A detailed explanation of these components is contained in CCITT, Data Communication Networks Directory, Blue Book, Volume VIII - Fascicle VIII.8, 1988.

a. Directory System Agent (DSA). The DSA is concerned with carrying out the requests of the DUA and with obtaining the information from the distributed DIB. A portion of this DIB is associated with each DSA. Most information retrieved from the DIB is sensitive-unclassified. The exact technique for handling classified *information is being investigated.* If a DSA cannot obtain the requested information from the directories in its serving domain, it interacts with other DSAs to search the DIB until the information is found or it is determined that the request cannot be fulfilled. DSAs are implemented at base and network levels and are part of the DIR shown in Figures B-2 and B-3.

b. Directory Information Base (DIB). The information held in the Directory is collectively referred to as the DIB. Directory updates are effected through a database administrator or local database custodian. To provide directory access in the most cost effective way for the vast majority of DMS users, the goal of the DMS Directory architecture is to have most of the entries in the database sensitive-unclassified. Information requiring classification, such the association of Directory names with their O/R names will be handled on an exception basis. Should the requirement for classified entries be large, a separate classified segment of the DIB, appropriately secured, may have to be implemented. The Directory and X.400 envelope classification issues are being addressed in the Phase 1 SDNS Directory R&D project and their resolutions will be forwarded through the DMS management structure for incorporation into the DMS Phase 2 and 3 architectures. The central project X.500 DIB referred to in Phase 1 is not the DMS DIB. The DMS DIB is the integrated contents of the MCS database, X.500 Central DIB, DDN

E-Mail directory, and the X.500 SDNS directory. It is distributed at the base and network levels and implemented on a hierarchial basis as part of the DIR shown in Figures B-2 and B-3. By the middle of Phase 2, these four directories are phased out and replaced by the single DMS Directory (DIR). The DMS relies upon lower layer security services for authentication and access control of subscribers accessing the DIB.

B.2.2 Security Components. The DMS provides writer-to-reader security services through MSP. MSP offers five principal security services needed by DMS: Confidentiality, Data Integrity, Authentication, Access Control, and Non-repudiation. These are defined in section 3.2.5 of the TAIS. MSP operates with UAs and OUAs and regards MTAs as untrusted components (MSP provides writer to reader protection). The data in the protected content remains encrypted from UA/OUA to UA/OUA. For unclassified individual messages, MSP protection terminates on the unencrypted side of the MSP gateway. In most cases, these data are considered to be unclassified-sensitive information. The following briefly describes the security services provided by MSP:

a. MSP security services:

(1) Connectionless confidentiality protects data from unauthorized disclosure. This is provided by an encryption process that is applied to the message content.

(2) Connectionless integrity protects data from modification as it is being forwarded through the DMS.

(3) Data origin authentication provides corroboration to the application process that the source of the message is the claimed originator. The key used to encrypt the message content is separately encrypted for each recipient using a token key.

(4) Access control is a service that prohibits an originator from submitting and a recipient from receiving messages that violate security policy.

(5) Non-Repudiation with proof of origin assures that the signed message did not admit tampering. The recipient is assured that the message sent cannot be denied.

(6) Request for signed receipt is a service that asks the recipient to digitally sign a receipt. If the recipient performs this action then the originator is provided non-repudiation with proof-of-delivery service.

b. MSP Key management. User MSP certificates and user

keying material are contained in the DIB. Originating UAs and OUAs use the intended recipient's posted information along with their own private information to construct a token key:

(1) Each MSP supported UA has a unique non-forgeable digital certificate. The certificate contains both a user's/organization's identification and access control privileges.

(2) The message originator creates a unique token for each message using the recipient's MSP certificate obtained from the DIB. This token is included in the SDNS heading for each intended recipient. It is used by the originator to encrypt the message and by each recipient to decrypt the message.

(3) Alternate delivery can be accomplished in a similar manner by including the token of each alternate delivery recipient in the SDNS heading. The Directory in combination with the DMS management functionality could, if required, assist the user in identifying these alternative recipients. Alternate recipients would in general be identified previously as a result of agreements made by the organizational elements involved.

(4) Since computing and inserting tokens into a message for each and every intended recipient or alternate recipient could be a very lengthy and resource consuming process, the Phase 1 Mail List Agent project has been identified to develop a more efficient mechanism.

c. MSP message protection structure. The following security service elements are contained in the secure message:

(1) Protected Content. Each message is protected with MSP confidentiality, integrity and access control services. The non-repudiation and request for signed receipt services are optional.

(2) Originator Security Data. The originator's credentials, access control information, and algorithm identifiers are provided.

(3) Signature Block. The originator's signature exchange data and message signature value are provided. MSP includes an electronic signature check which will be used on all organizational messages and optionally on individual messages. These capabilities provide the recipients with proof of organizational release of the message and the capability to prove the identity of the message releaser to a third party.

(4) Per Recipient Token. The recipient's credentials,

security labels, and message encryption key are provided.

d. Distribution Lists. The DMS requires the capability to deliver single messages to large distribution lists. The method of dealing with these types of lists and MSP protection, is being determined. The Phase 1 MLA project is to address and resolve these concerns. Depending upon the outcome of this effort, MLAs may be included in Phase 2 and 3 architectures.

B.2.3 Transitional Interface Capabilities. To ensure message exchange interoperability until the baseline messaging services are phased out, interface capabilities are provided in the Phase 2 architecture:

B.2.3.1 ADI, MCS, and AMS. By the middle of Phase 2, these AUTODIN messaging and DDN E-mail interface capabilities, described in Appendix A, are integrated into the DIN/DMS gateway. The ADI and/or AMS will be enhanced with an X.400 capability during the early part of Phase 2. This enhancement is required to eliminate dual conversions (DIN-DDN-X.400) when exchanging messages between AUTODIN and X.400.

B.2.3.2 DIN/DMS Gateway. During the early part of Phase 2, the DIN/DMS gateway will be fielded. This component provides AUTODIN to X.400 interface for those tactical, allied, and other organizations that may not be able to transition to X.400 MHS capability at the same time their supporting ASCs/AMPEs are phased out. This component also provides the ASC functionalities needed to support TCCs in the absence of ASCs. By the end of Phase 2, the ADIs, MCS, and AMS functionalities will have migrated into the DIN/DMS gateway and thus can be phased out. Thus, the DIN/DMS Gateway provides interface among all three message systems (AUTODIN, DDN SMTP E-mail, and X.400). As an ASC is closed, any remaining subscribers who still use AUTODIN-type applications (i.e., JANAP-128/ACP-127) will normally be transitioned to a DIN/DMS gateway, which will provide the required AUTODIN functionality as well as an interface with the X.400 users on DDN. This interface gateway will be phased out in Phase 3, when the last TCC is phased out.

B.2.3.3 MSP Gateway. The MSP gateway provides interoperability between message subscribers who have MSP and those that do not. This component does not provide an automated upgrade/downgrade capability; the DMS does not require such a capability. The MSP gateway simply provides encryption/decryption interface between appropriately cleared organizations/individuals. Protected distribution systems or other security means are assumed between the gateway and the end-user. The DMS provides MSP gateways at the baselevel and network levels.

B.2.3.4 Guard Gateway. MILNET and DISNET remain separate DDN networks during Phase 2. Current DDN security policy prohibits a subscriber from connecting either directly or indirectly to both MILNET and DISNET. Therefore, the DMS subscribers on each of these networks are logically and physically separated. However, a requirement exists to allow DMS users to exchange unclassified messages between MILNET and DISNET communities. This requirement applies between separate users on the same base as well as across the network. Therefore, a DMS component is required at both the network and IITS levels to provide a certain amount of interoperability between these classified and unclassified segments of the DDN. The Draft DDN Program Plan dated 30 Jan 90, defines a DDN Guard Gateway to satisfy this need at the network level. The DMSIG and DDN PMO are working jointly to implement this network level gateway. The DDN Guard Gateway planned between MILNET and DISNET will ensure that classified data on DISNET is not passed intentionally or inadvertently to users on the MILNET while allowing unclassified traffic to pass between the networks. Traffic flow control is also provided by the DDN Guard Gateway. The DMS also requires the capability to pass unclassified messages between DISNET and MILNET subscribers located on the same base without having to pay network service charges just to utilize the DDN Guard Gateway. A DMS guard gateway is developed and implemented at the base level to provide this capability. The DMS guard gateway must be capable of examining the classification of the message as well as contain MHS functionalities to exchange appropriately screened unclassified messages between the two communities.

B.2.3.5 OSI Gateway. This Phase 1 component is required in the early part of Phase 2, at the network level, to provide interface between SMTP users and X.400 users. The OSI gateway is phased out in conjunction with SMTP phase out.

B.2.4 DMS Management Components. The DMS management capability, initiated in Phase 1, becomes an operational entity in the Phase 2 time frame. DMS management, not to be confused with the DMS management structure described in Section 4 of the TAIS, encompasses a comprehensive set of tools, procedures and staff required to make the DMS transparent and trouble free for the user. Potentially, the DMS management function could be a subset of DCA's overall Integrated Communications Architecture (ICA) management function, at both the base and network levels. The separately managed DMS functionalities include:

a. Fault/Problem Management. The detection, isolation, and correction of abnormal messaging operations. Restoration of messaging service to users during failure and degrading conditions is a primary management function.

b. Configuration/Change Management. The control of DMS components from a central management capability.

c. Performance/Growth Management. Gathering statistical data, analyzing this data, and projecting growth and performance requirements for the DMS. This function monitors the behavior of the DMS and measures its effectiveness.

d. Security/Access Management. Monitoring and maintaining DMS security assets, policies, and procedures to ensure required authentication of users, access control, security auditing, and support to key management.

e. Directory Service Management. Assisting in managing the DIB to ensure it is well-formed and maintained over time. This DCA undertaking is expected to soon be designated as a Central Project.

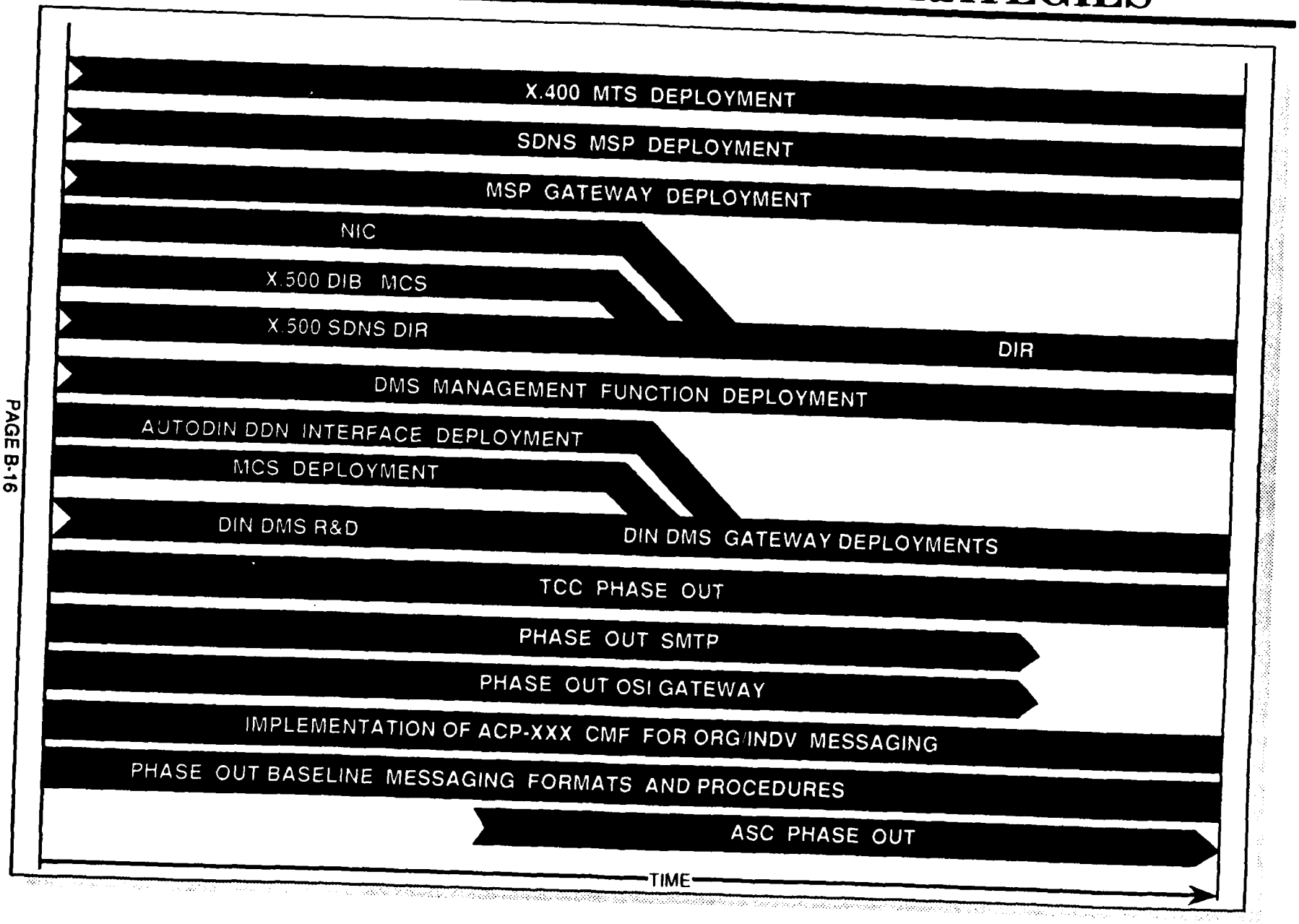
B.2.5 Baselevel Transmission Facilities. Although these are not DMS components, the DMS relies upon these transport facilities for connectivity and security features. In the early part of Phase 2, the baselevel transmission facilities are expected to transition to an ISDN-based Installation Information Transfer Systems (IITS). This transition is considered in the development and implementation of the Phase 2 architecture.

B.3 Phase 2 Transition Strategies.

This section presents the transition strategies that support achieving the objectives for Phase 2. As shown in Figure B-4, these strategies are structured to provide a managed and coordinated transition from Phase 1 to Phase 3. These strategies enable the Services and agencies to integrate applicable transition actions into their Phase 2 planning.

B.3.1 Expand Writer-to-Reader Connectivity and Support. X.400, X.500, and MSP capabilities (software) are made available to the users, through commodity contracts, for use in their existing PCs/workstations and/or from host servers. The new ACP-XXX, initially fielded in Phase 1, provides message format, protocol, and policy information to the users. Supporting baselevel and network level DMS components, such as MTAs, DSAs, MSP gateways, MSs, Guard gateways, Management, and DIN/DMS gateways are deployed. By mid Phase 2, the DDN E-mail directory (NIC and hosts shown on Figure B-3), the MCS database, the Phase 1 X.500 DIB and the SDNS X.500 directory are merged into the single, integrated DMS Directory (DIR). Initially in Phase 2, installations will not require local X.500/SDNS directories to support the implementation of X.400 MHS; they will utilize the regional X.500/SDNS Directory off the DDN. The DMS will enhance

Figure B-4
PHASE 2 IMPLEMENTATION STRATEGIES



user connectivity by capitalizing on the advancements offered by the evolving baselevel IITS.

B.3.2 Provide Writer-to-Reader Message Security Services. This strategy focuses on providing users all the security services needed for end-to-end protection of the information contained in their messages. Both applications layer and lower layer security services are employed. As stated in B.1.2, the DMS provides application-layer security services and relies upon the IITS and DIS ITU for lower-layer protection services.

B.3.2.1 Application Layer Security Strategies. The goal is to implement MSP in all user workstations. Depending upon the level of protection required, alternative security services may be considered as users transition to MSP:

a. MSP. MSP is the target applications layer security service for DMS. At the beginning of Phase 2, MSP applications are made available to DoD through commodity contracts. MSP will be fielded with all OUAs and those UAs that process classified material. Terminals equipped with MSP must employ the appropriate security assurance mechanisms to meet the level of trust required for the Automated Information System (AIS). Most UAs will be used for unclassified-only individual messaging and therefore will not initially have MSP.

b. Transition to MSP. Until MSP is available to unclassified UAs, alternative security services may be considered by the SPWG and the DMSIG.

(1) MSP Gateway. For interoperability between users with and without MSP, MSP gateways are provided. The gateway does not provide protection from the user to the gateway; this is assumed to be provided locally.

(2) Alternative Security Services. An example of an alternative transitional security service is Privacy Enhanced Mail (PEM), a pending commercial product that will provide low-grade security features such as confidentiality, integrity, and authentication.

B.3.2.2 Lower-layer Security Services. The DMS relies upon the IITS to satisfy lower-layer (layers 1-4) security requirements for transporting data on the base. Likewise, the DMS relies upon the ITU of the DIS to satisfy lower-layer security requirements for transporting data across the long-haul networks. The DMS planners participate in the ICA security architecture development process.

B.3.3 DMS Management. The DMS provides management capabilities

at the base and network levels. A S/a coordinated management plan is being generated which will specify management domains, functional areas, and S/a responsibilities. Some of the personnel positions previously required to operate and maintain the ASCs and TCCs may become personnel allocations for operating and maintaining the DMS management capability. DMS coordination with the IITS and ICA planners is ongoing to ensure an integrated management capability. It is likely that the DMS management capabilities will be incorporated into the IITS and ICA management components. The structure and functions of the DMS management are being developed in the Phase 1 DMS Management R&D project and will be incorporated into the Phase 2 and Phase 3 architectures upon the review and approval of the Architecture Working Group (AWG) and the DMSIG.

B.3.4 Maintain message exchange interoperability between DMS and non-DMS communities. Transitional interface capabilities are deployed to ensure interoperability between disparate messaging systems. This evolutionary strategy, begun in Phase 1, consists of managing the phasing of these transitory capabilities.

B.3.4.1 Phasing out of transitional components.

a. In the early part of Phase 2, an X.400 enhancement is added to the B-ADIs and R-ADIs. This enhancement allows the Phase 1 OSI gateway to be phased out. The ADIs therefore provide interface among all message formats: AUTODIN's ACP-127 and JANAP-128; DDN's RFC 822; and, ACP-XXX CMF. Toward the middle of Phase 2, the ADI and MCS capabilities are merged into the DIN/DMS gateway.

b. OSI Gateway. With the deployment of X.400 in Phase 1, a transitional interface is required between those subscribers using the X.400 and those using DDN E-mail (i.e., SMTP). This interface capability is fielded with the IOC of the X.400 capability. Since the OSI gateway is only a message protocol converter and not a message format converter, it will be phased out when the B-ADIs and R-ADIs are fielded.

B.3.4.2 Phasing in of gateways. The following gateways are deployed in Phase 2.

a. DIN/DMS Gateway. This interface capability translates between message formats and protocols. The DIN/DMS gateway is fielded around mid Phase 2 and is expected to remain into Phase 3, until the last TCC is phased out.

b. MSP Gateway. To provide applications layer security interoperability between those users having MSP and those without, an MSP gateway is fielded in concert with the SDNS MSP

IOC. This gateway will required into Phase 3.

c. Allied and Tactical Gateways. For those users in the Allied and tactical communities who have evolved from AUTODIN messaging to OSI and/or X.400, a gateway may be required to account for any differences with the DMS implementation. This gateway will be required into Phase 3.

B.3.5 Phase out baseline messaging systems. This subsection also includes the strategy for phasing out the baselevel TCCs.

B.3.5.1 TCC Phase Out. The close out of the baselevel TCCs begun in Phase 1 continues. It is not expected that all TCCs will be phased out in Phase 2; this is a Phase 3 objective. Reductions in manpower and the cost of messaging at the baselevel are realized as this strategy progresses. The following Phase 2 actions reduce the need for over-the-counter service from a TCC:

a. In the early part of Phase 2 most organizations are transitioned to DDN for sending and receiving unclassified organizational messages.

b. Transitional devices, such as the MCS and the baselevel and regional AUTODIN-to-DDN transitional interface capabilities are deployed.

c. The IOC of X.400/X.500/MSP organizational messaging capabilities in the user's workstation facilitates the phasing out of the TCCs. As the new organizational messaging capabilities are made available to the users at their workplace, the base TCCs can be scaled down and finally closed.

d. As TCCs and AMPEs are phased out, baseline AMHSs must transition to DMS specified X.400 based messaging or risk being obsolescent and non-interoperable with the rest of the DMS community.

e. The DIN/DMS gateway is deployed to connect remaining TCCs, allowing the ASCs to be phased out in Phase 2.

f. DMS users are transitioned to the CMF specified in ACP-XXX.

g. DMS users acquire the capability for complete, MSP protected, organizational message exchange at their workplace.

B.3.5.2 SMTP Phase Out. As DMS subscribers attain X.400 MHS capabilities, the baseline DDN E-mail protocol, SMTP, is phased out toward the latter part of Phase 2.

B.3.5.3 ASC Phase Out. By implementing DIN/DMS gateways, AUTODIN switching centers (ASCs) are phased out in Phase 2. ASC services are continued via DIN/DMS gateways to those remaining users still requiring them. The closing of the ASCs continues throughout Phase 2, but is targeted to be completed by the end of Phase 2 - the closing of the last ASC is the milestone that ends Phase 2. The following events comprise the strategy to achieve this:

a. AUTODIN narrative messages are transitioned to DDN in the early part of Phase 2. This removes most of the AUTODIN message traffic from the ASC backbone. The MCS and the R-ADI, implemented in Phase 1, facilitate this migration.

b. Baselevel and network MTAs are deployed to provide X.400 MTS support. This capability further negates the need for AUTODIN backbone transport.

c. TCCs are phasing out.

d. Full-scale DMS base and network level management capabilities are deployed that include Directory services and MSP key distribution and management.

e. DMS users are transitioned to the CMF specified in ACP-XXX.

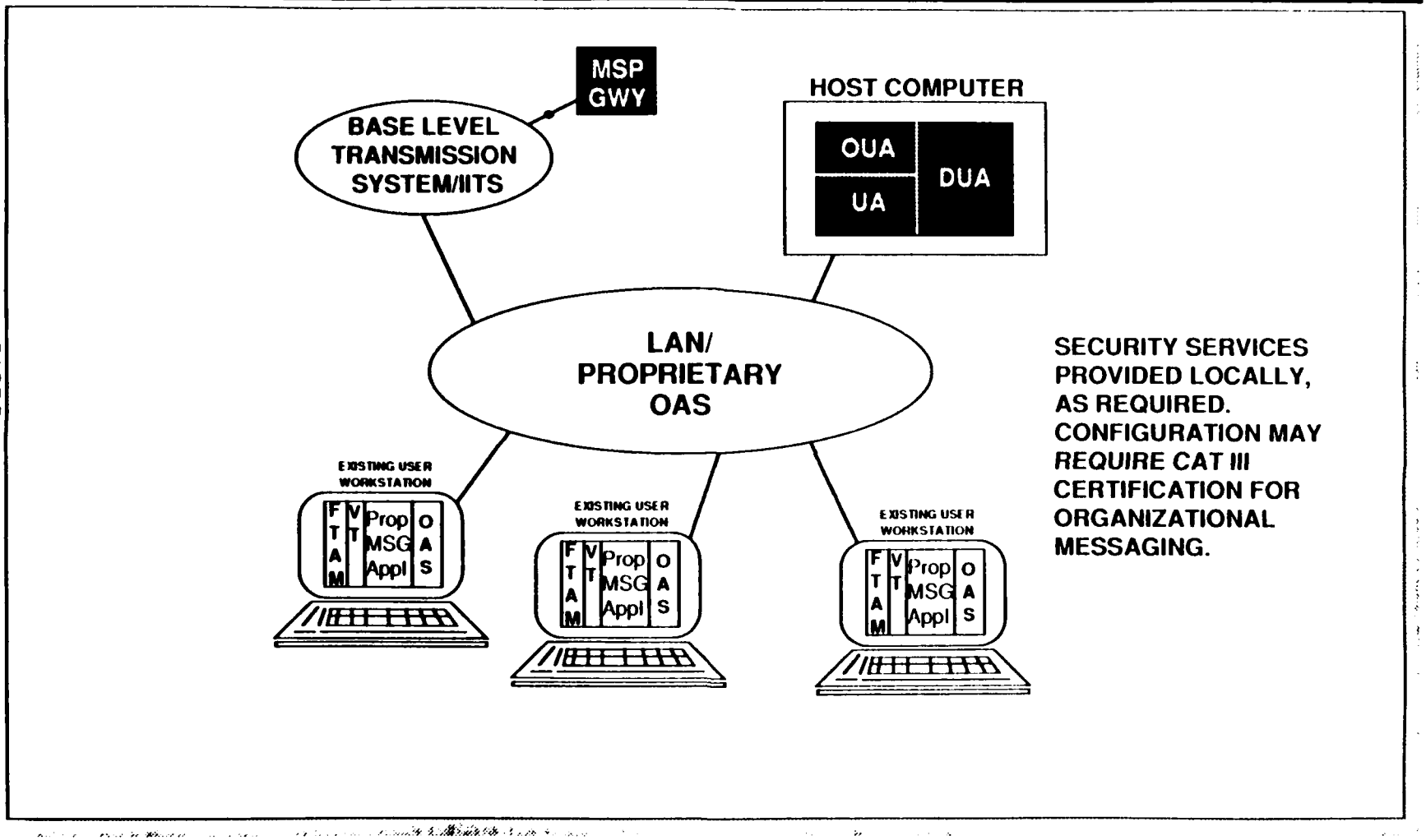
f. DMS users acquire the capability for complete, MSP protected, organizational message exchange at their workplace.

B.3.6 DMS Logistics Support Guidance: This implementation strategy addresses the need to orient the user to the new way of exchanging messages. DMS logistics support guidance is currently being developed.

B.3.7 Cost effective Phase 2 implementation strategies. The following are current strategies being developed to manage the cost of implementing Phase 2.

a. Sharing DMS applications among users. Users may access and use an OUA, UA, and DUA that may be resident in a host computer. These shared messaging and directory service programs may simultaneously support multiple users or one individual user at a time, with the use of MSP encryption as appropriate. See Figure B-5.

Figure B-5
TRANSITIONAL RESOURCE SHARING



LEGEND

	DMS Functions and Components	MS	X.400 Message Store	FTAM	File Transfer, Access, And Management
MSP	Message Security Protocol	VT	Virtual Terminal	OUA	Organizational User Agent
MSP GWY	MSP Gateway	LAN	Local Area Network	UA	User Agent
Prop MSG Appl	Proprietary Message Application	OAS	Office Automation System	DUA	X.500 Directory User Agent
	Lower Layer Security				

b. Implementing X.400 messaging on baseline AMHSs. In some cases, users may want to upgrade their baseline AMH systems to provide DMS specified X.400 individual and/or organizational messaging services.

c. Sharing existing user workstations. The DMS software will coexist with other applications running on or accessed from an existing workstation. The DMS does not require dedicated workstations.

d. Using commodity contracts. The requirement for MSP will be included in the acquisition package for Desktop IV (and beyond) workstations. MSP will be an affordable option that can be ordered by users who plan to implement DMS messaging applications. MSP will not be centrally procured by the National Security Agency (NSA) as a stand alone device nor as a special DMS MSP workstation. If required, the appropriate security assurance mechanisms to meet the level of trust required for the AIS will also be included as options in the commodity contracts.

e. Minimize security costs. Employ only the appropriate security assurance mechanisms to meet the level of trust required for the DMS component (AIS). Reduce the personnel security clearance levels required to operate and maintain the DMS components. These may be achieved through the use of MSP on all classified messages, structuring the DIB data entries so that at most they are sensitive-unclassified, and by implementing only the minimum number of security features that provide the required levels of security.

f. Maximizing benefits from previous capital investments. Those TCC and AUTODIN messaging transitional devices installed in Phase 1, such as the Navy's RTS, MMS, and the MDS will be utilized/upgraded to X.400/X.500 capabilities to the maximum extent possible.

B.3.8 ICA-related Transition Issues. Several areas within Phase 2 implementation require DMS/ICA mutual consideration. These include:

B.3.8.1 Directory Services. It can be envisioned that the DMS DIR is a subset of the larger comprehensive ICA directory. This issue is being jointly considered; the DMS Directory service initiative is being used as the guide and pattern for the ICA directory.

B.3.8.2 Security Services. The ICA is being provided DMS security requirement for incorporation into the comprehensive ICA security architecture. Of particular interest to the DMS are the

lower-layer security services reflected in the ICA Security Architecture. Another subarchitecture, under the ICA umbrella, of great interest to the DMS is the DDN Security Architecture.

B.3.8.3 Network/Systems Management. It can be envisioned that the DMS management and database are subsets of the larger ICA network management capability. Integrated and coordinated management capabilities are being discussed between the ICA and the DMS.

B.4 Phase 2 Transition Actions.

The following sections describe the Phase 2 project and policy actions.

B.4.1 Project Actions. Project actions are categorized as Central, Joint, baselevel, and R&D.

B.4.1.1 Central Projects.

a. DMS Directory (DIR). The DMS X.500 SDNS Directory, developed by NSA in Phase 1, will be expanded into an integrated DMS Directory that includes the information contained in the DDN E-mail directory, MCS database, and the X.500 Central DIB.

b. ACP-XXX. As described in Appendix A. Implementation and deployment continue throughout Phase 2.

c. DIN/DMS Gateway. The incorporation of the ADI and MCS functionalities into the DIN/DMS Gateway occurs in the early part of Phase 2. Implementation of the DIN/DMS gateway at the base level begins during early-to-mid part of Phase 2.

d. MSP Gateway. Deployment of MSP Gateway continues throughout Phase 2. This component is required into Phase 3.

e. Guard Gateway. The Guard Gateway developed under the DDN program may provide the same services required at the baselevel. This feasibility is being considered by the DMSIG.

f. Allied and Tactical Gateways. These gateways are required to maintain DMS interoperability with the Allied and tactical communities at the end of Phase 2 and into Phase 3.

g. MTA. The MTA is a candidate as a Central Project.

h. DMS Management. This is a candidate Central Project.

B.4.1.2 Joint Projects. Candidates for Joint Projects include:

a. OUA

b. UA

c. MS

B.4.1.3 Baselevel Projects.

a. Acquire and implement X.400/X.500/MSP capabilities in users' workstations.

b. Implement components such as MTAs, Guard Gateways, DSAs and their associated portions of the DIB, and DIN/DMS Gateways.

c. Implement baselevel DMS management capabilities.

d. Implement baselevel Directory service.

e. Phase out TCCs.

f. Orient/assist new users to the capabilities and use of X.400/X.500/SDNS MSP. Establish local training courses, as required.

B.4.1.4 R&D Projects. The DMS requires continued R&D initiatives to ensure DoD is afforded the best, economical implementation of messaging technologies. R&D is required to influence industry development of messaging technologies so that military unique features are integrated into the COTS products. When this is not feasible, DMS R&D efforts produce the specifications for the special applications required by DoD. Before large scale DoD implementation is allowed, analysis and testing of COTS products is required. During Phase 2, R&D is required to maintain a forward looking objective to evaluate and improve upon Phase 3 and beyond DMS architecture requirements. The following highlights expected R&D initiatives for the Phase 2 era.

a. COTS technology and capabilities assessments. Directory enhancements. Next generation management capabilities assessments.

b. Software engineering. Software reusability/payoff analyses. Bundled X.400/X.500/MSP software development and assessments. Another area is the use of X.400 MHS for other than text messages.

c. Integrated Services Digital Network (ISDN) impact analysis. Narrowband ISDN (NISDN) implementation is expected to be supported within DoD through 1996, beyond will be Broadband

(BISDN).

d. Expanded user services. As experience is gained, technology improved, and the DMS MHS subscriber base expanded, additional services or messaging features may be identified and included. This may include additional categories of messages as well as the ability to include voice, video, and advanced graphics into the body of a message.

B.4.2 Policy Actions. ASD/C3I and the Joint Staff are responsible for overall DMS policy. With the changes in the DoD message exchange environment during Phase 2, it is expected that updates to DMS policies will be required.

B.4.2.1 DDN security policy. The current DDN security architecture prohibits a subscriber from connecting either directly or indirectly to both MILNET and DISNET. In Phase 2 of the DMS, the requirement exists for subscribers off MILNET and DISNET to exchange unclassified messages. This requirement is in conflict with the current policy. Technical solutions (i.e., the baselevel and network level Guard Gateways) are available to satisfy the requirement and appear to be acceptable to both the certifiers and accreditors. Current DDN security policy may need to be revised.

B.4.2.2 Joint Staff (JS) Memorandums of Policy (MOP). The consolidation of the individual and organization message systems in Phase 1 requires the modification of multiple JS MOPs. It is expected that this modification process, begun in Phase 1, will continue well into Phase 2. In fact, the process is assumed to be continuous to ensure updated policy tracks with the current technologies being used by the DMS. It is envisioned that a DMS MOP is required to define operation and maintenance responsibilities, management control, and other changes to existing "joint" responsibilities.

B.4.2.3 Security Policy. Policy is needed to define certification requirements and criteria to be used to accredit DMS components. The following security policies are needed to support the Phase 2 transition.

a. DMS security requirements. Security policy is being written that defines the DMS security requirements. From this policy, MSP or other security mechanisms can be identified as appropriate means for satisfying DMS requirements. This policy is being coordinated with the ICA Security Architecture developers.

b. DMS DIR Security Policy. Policy is being developed that defines the composition, utilization and maintenance of the DMS

Directory. This policy is being coordinated with the ICA Working Group.

c. Security certification criteria for DMS components. The policy contained within the DMS Component Security Guide will set uniform, general guidance that will apply to all DMS physical components and their logical functions; to all organizations that develop acquire, test, install, operate, use and maintain DMS components; and to all facilities that house and support these activities. DoD 5200.28-STD permits replacing Enclosure 4, Procedure for Determining Minimum AIS Computer-based Security Requirements, with different methods, if approved by ASD(C3I). The DMS characteristics suggest that adjustments should be made to the trusted computer security evaluation criteria values assigned to DMS components by Enclosure 4. The basis for this would be to take into account more risk factors, as suggested by the Rationale for the Trusted Computer Security Evaluation Criteria Environmental Guidelines. This overall guidance will define the requirements and criteria to be used to certify DMS components and accredit facilities.

B.5 Phase 2 Operational Concept.

B.5.1 Introduction. This section presents the various messaging scenarios that can occur during Phase 2. Scenarios that continue from Phase 1 into Phase 2 are not discussed; these are presented in Appendix A. Each scenario is based upon a specific configuration derived from the different possible operational situations The following lists the variables used to construct the Phase 2 messaging scenarios:

a. Three different message systems - AUTODIN, DDN E-mail, and X.400 MHS.

b. The sender and receiver may be using the same or different message system.

c. The messaging may be intrabase or interbase.

d. The users may or may not have MSP.

e. The message may be individual or organizational.

f. The message may be classified or unclassified.

g. The sender and recipient may be subscribers to the unclassified or classified segments of DDN, or both.

h. Some originators and recipients may be part of the Internet or Tactical/Allied messaging systems.

B.5.2 Scope and Diagram Definition. Due to the numerous combinations of the operational variables, many scenarios can be designed. The following discusses the most likely scenarios. The basic X.400 scenario is presented and detailed first, then the following sections describe the significant changes from this basic construct. In this section and the accompanying diagrams, "or" is an important discriminator. All the diagrams within Figure B-6 use the same construct in presenting a scenario. The top line(s) connecting the two subscribers indicate which transport segment(s) (i.e., Class and/or Unclass IITS; MILNET and/or DISNET) are involved in the message exchange. The center arrow indicates the path the message travels from originator to recipient, and the messaging components used along the path. The bottom line(s) indicate the format and protocols used along the path and where conversions occur. The stick figures represent users who manually interface with a baselevel TCC. In the following discussions, the message flow is described from the subscriber on the left of the diagram (the originator) to the one on the right (the recipient). To maintain some brevity, the reverse flow is not discussed, but assumed to follow the same path and component interaction in the reverse perspective.

B.5.3 Scenarios 1, 2, and 3. The first three scenarios shown on Figure B-6 depict straightforward message exchange within a base by users all having X.400, X.500 and MSP capabilities. These scenarios also reflect message exchange among users connected to either the unclassified or classified baselevel transport networks, not between the two communities. Scenario 1 is one organization exchanging messages with another organization; scenario 2 is an individual to individual; and, scenario 3 is an organization to individual. The following describes a notional concept of operations for these basic scenarios, highlighting the DMS components involved. The actions and formats discussed below reflect a typical process for most DoD applications.

a. Access and logon. To begin a messaging session the user must have access to DMS messaging software and appropriate security services. DMS messaging software and supporting security mechanisms (MSP) are acquired by the user, from commodity contracts, and installed in the user's existing workstations/PCs/host computers. These are shown in the diagrams as the shaded OUA, UA, and MSP blocks in the existing users' workstations. Users requiring the capability to process organizational messages will acquire OUA and DUA software and MSP mechanisms. Users requiring the capability to process individual messages will acquire UA, MS, DUA software, and, depending upon user requirements, MSP mechanisms. Once installed, the user now accesses the applications software resident in the terminal or a supporting host computer (see resource sharing concept in Section B.3.7). In addition to the access control features provided by

Figure B-6
PHASE 2 CONCEPTS OF OPERATION

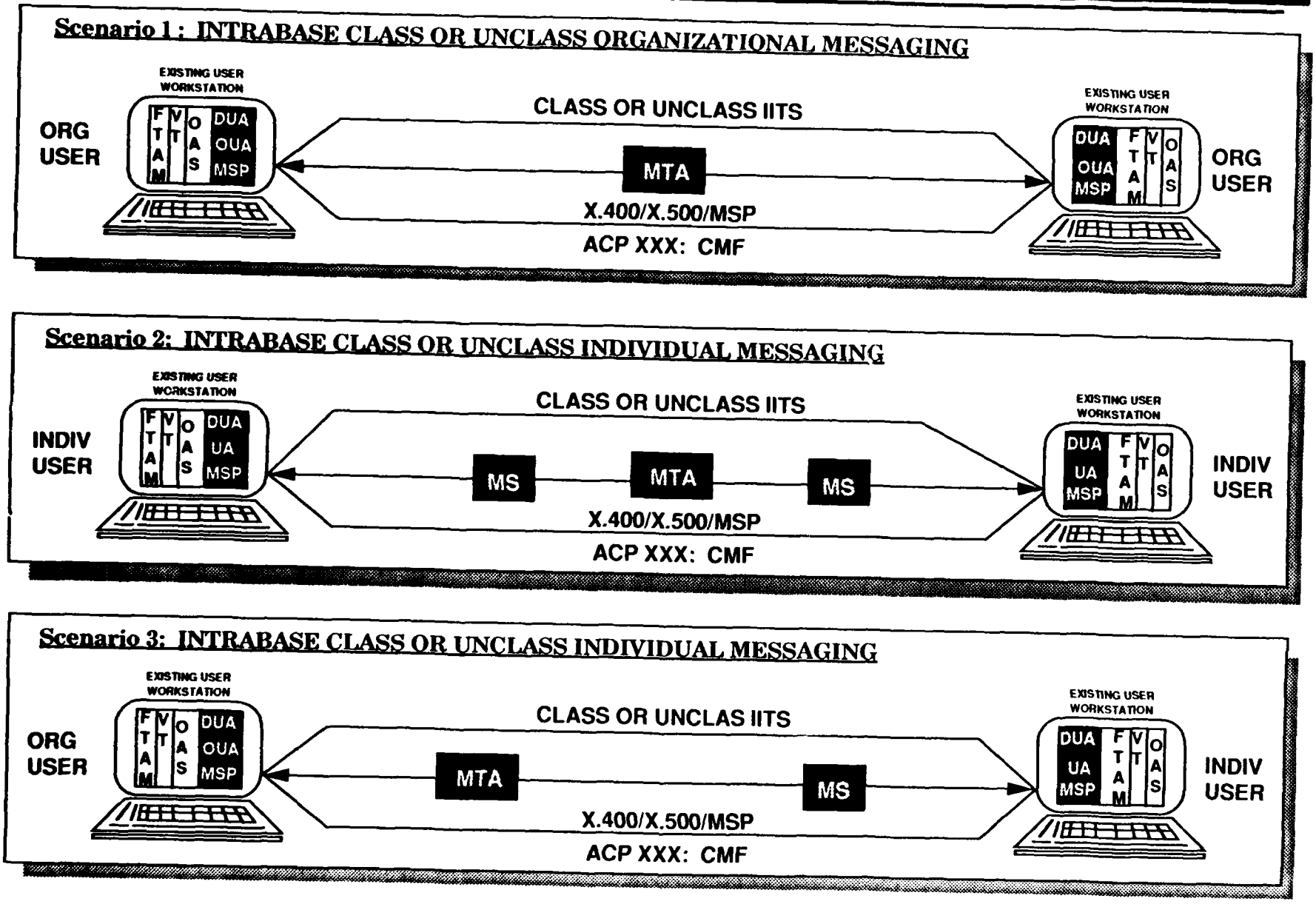


Figure B-6
PHASE 2 CONCEPTS OF OPERATION

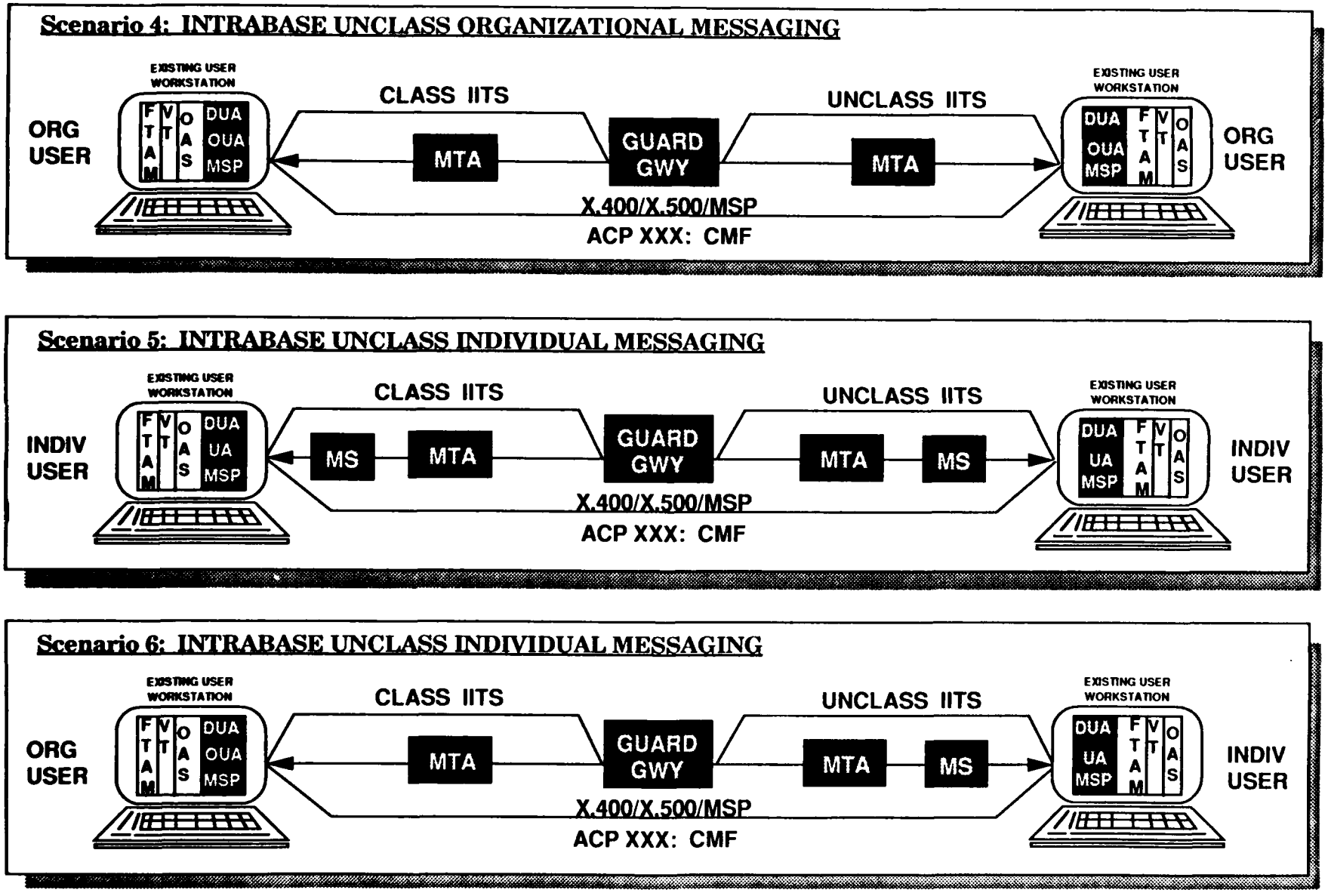


Figure B-6
PHASE 2 CONCEPTS OF OPERATION

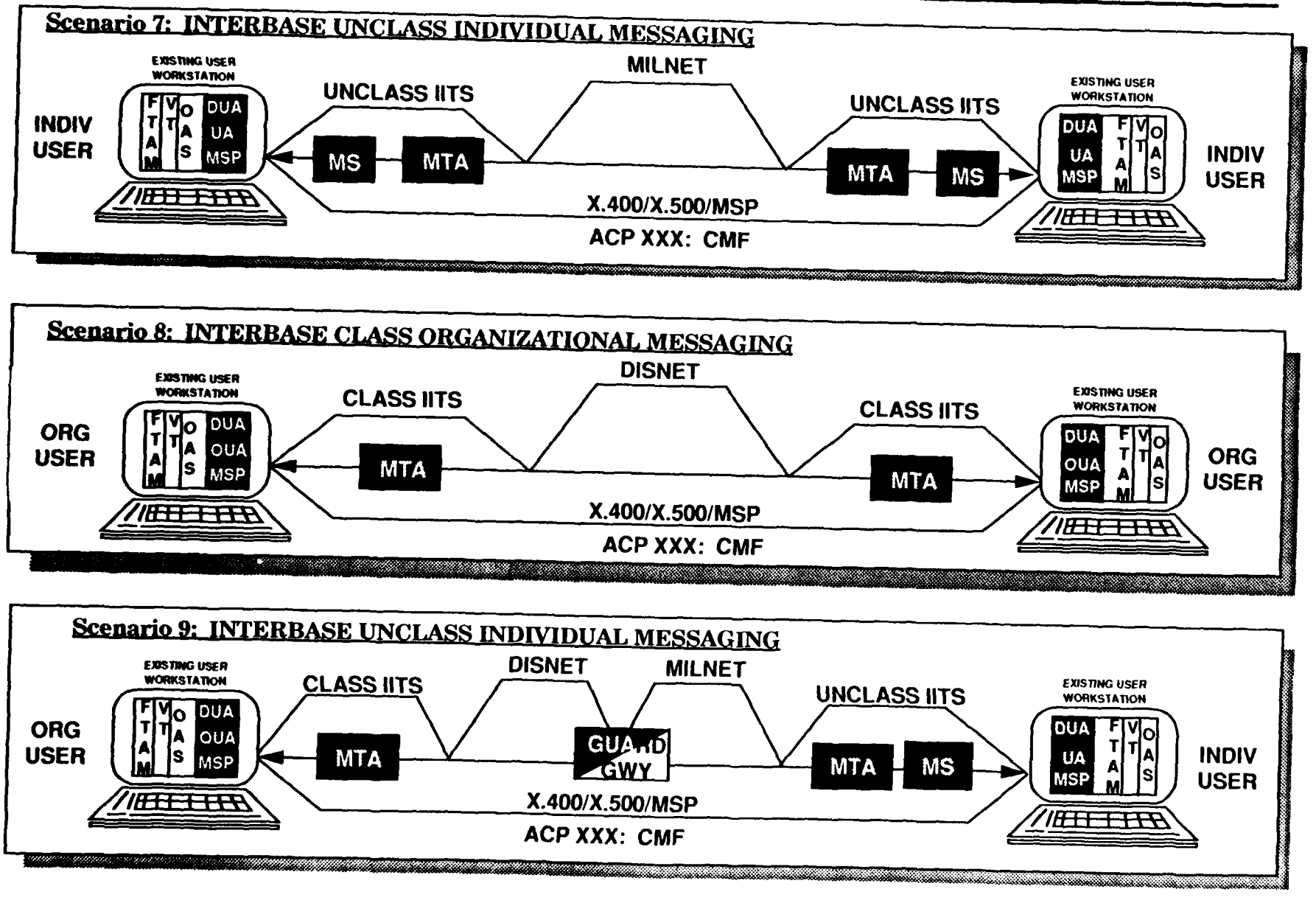
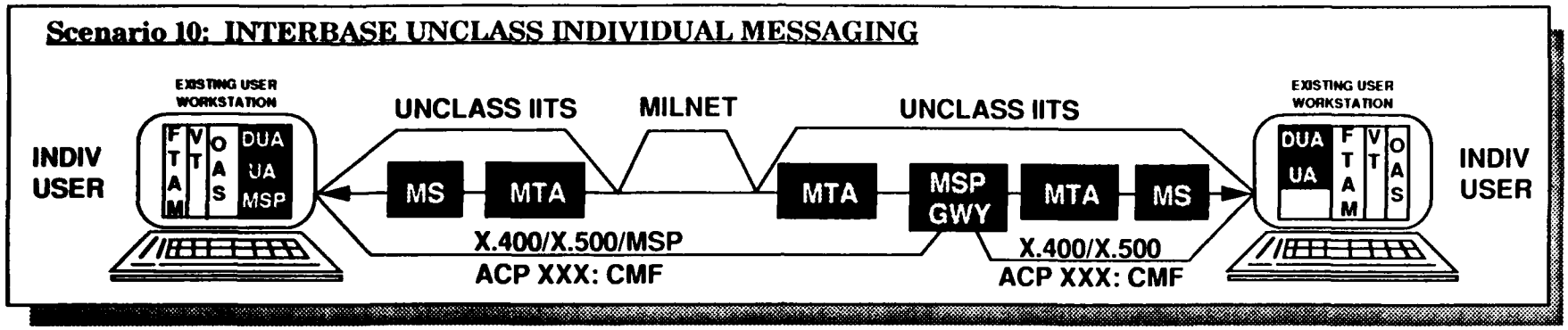
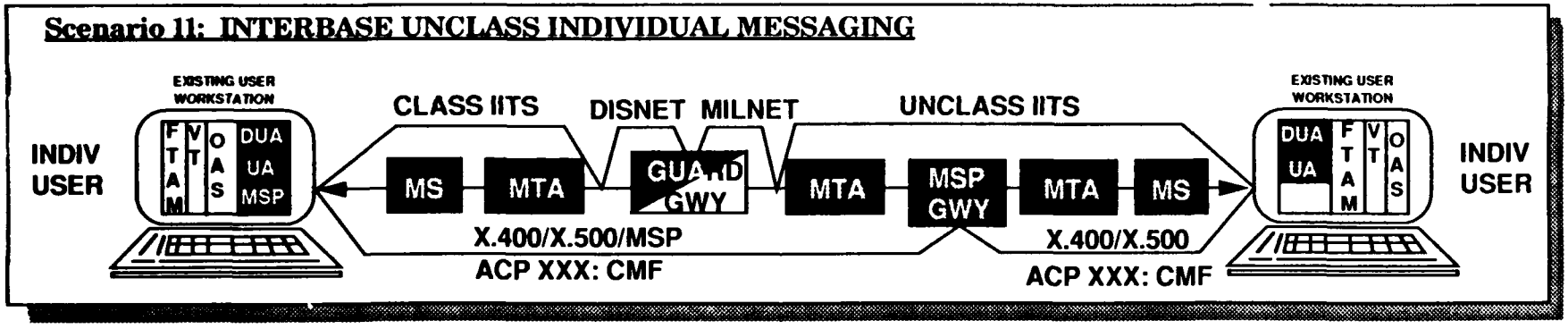


Figure B-6
PHASE 2 CONCEPTS OF OPERATION





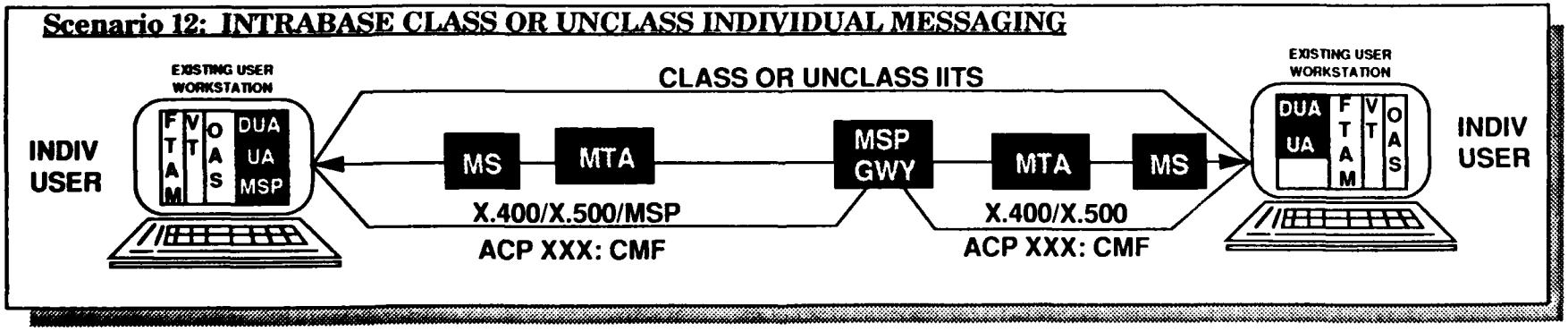


Figure B-6
PHASE 2 CONCEPTS OF OPERATION

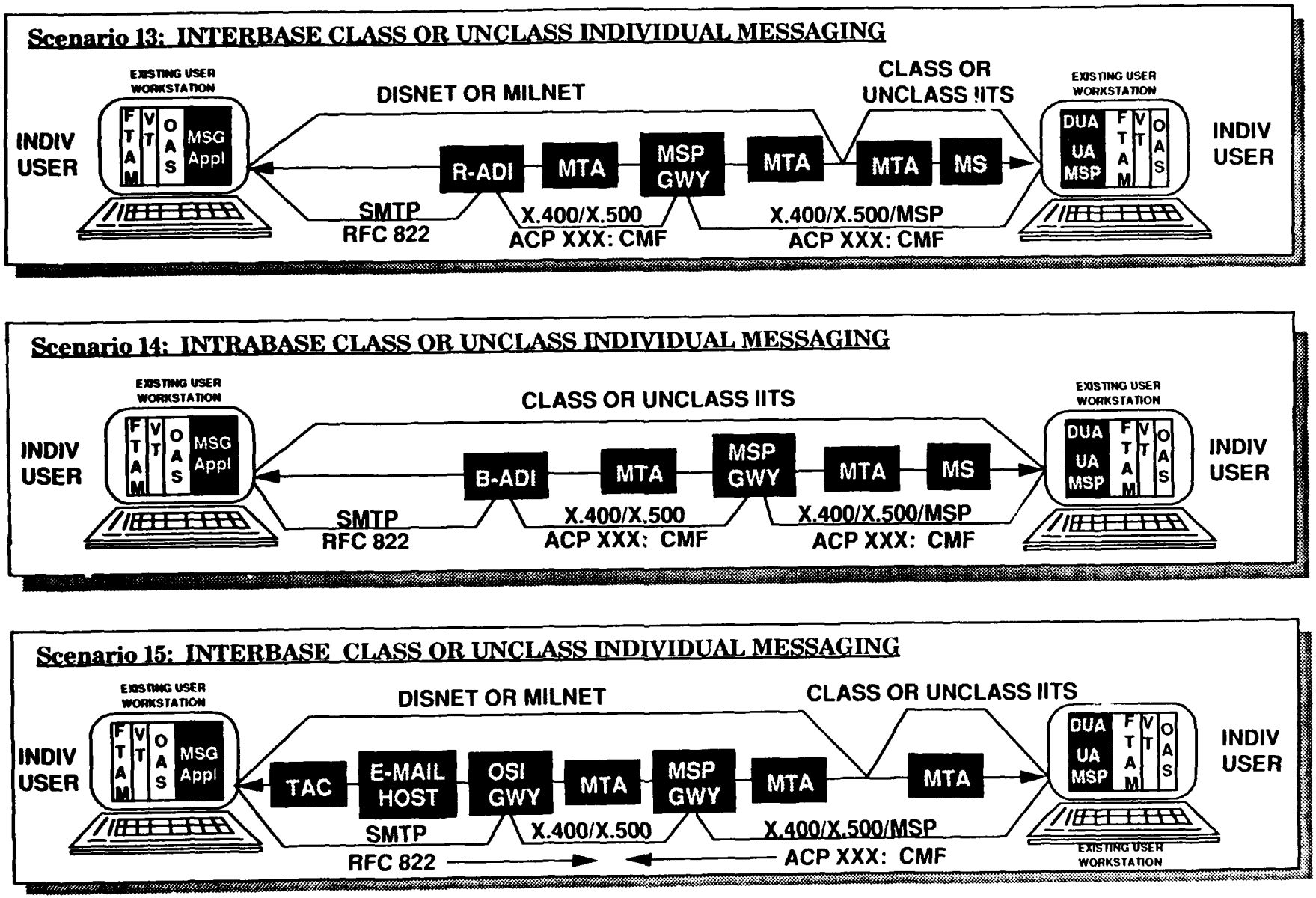
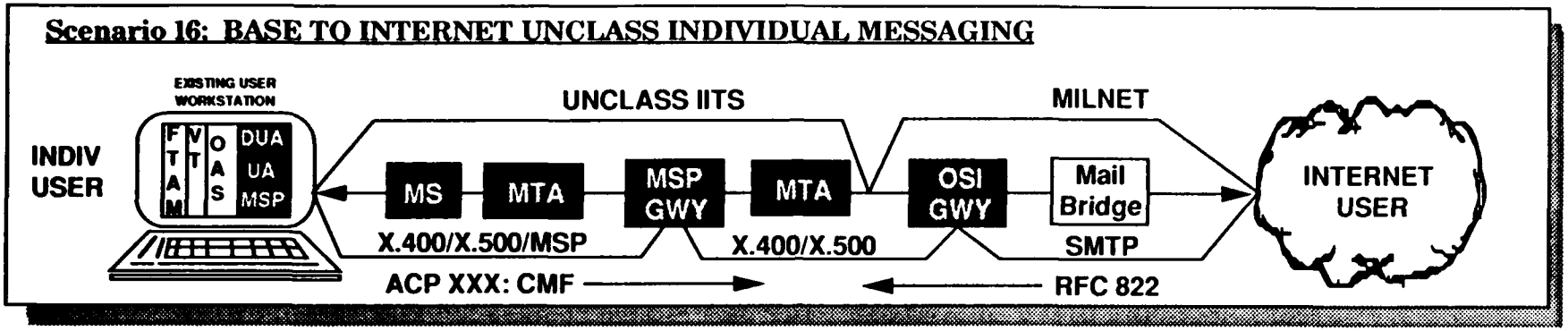
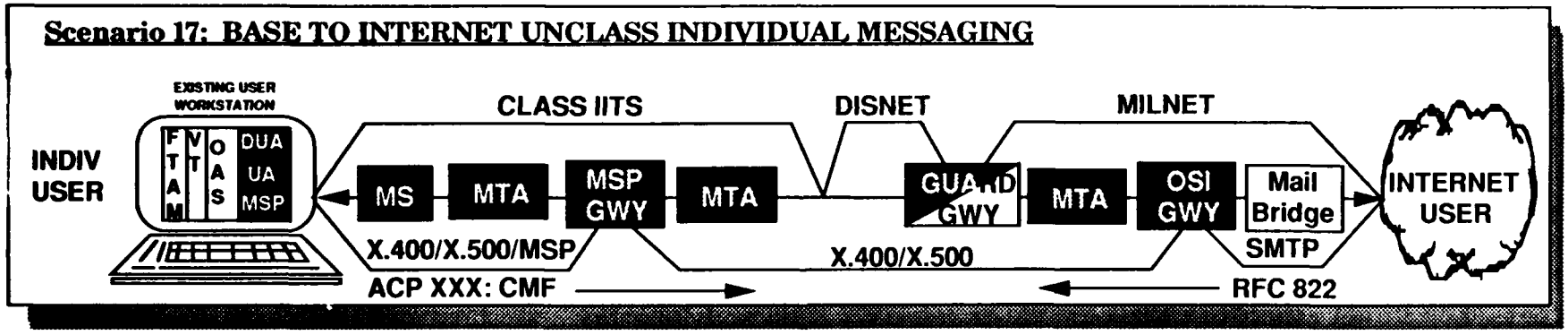


Figure B-6
PHASE 2 CONCEPTS OF OPERATION





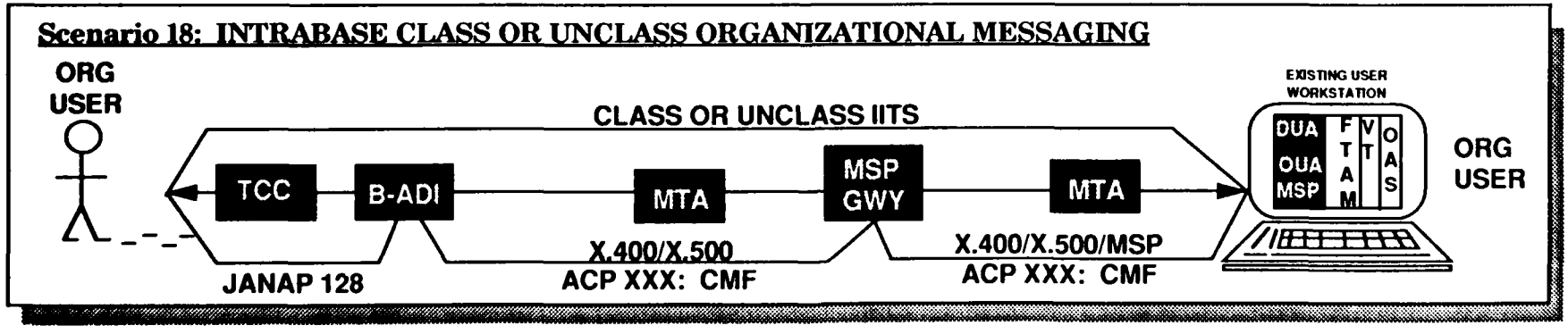


Figure B-6
PHASE 2 CONCEPTS OF OPERATION

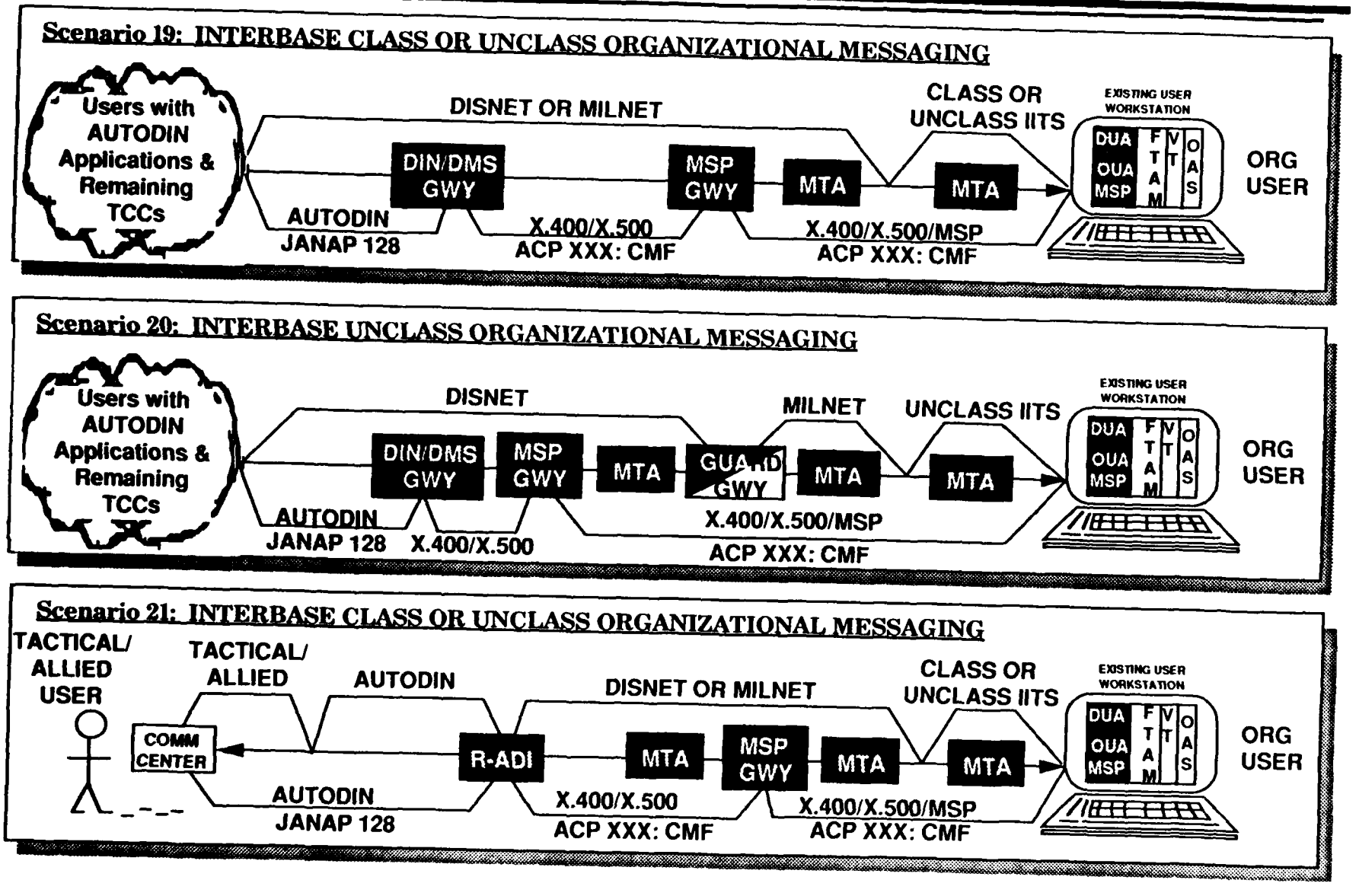
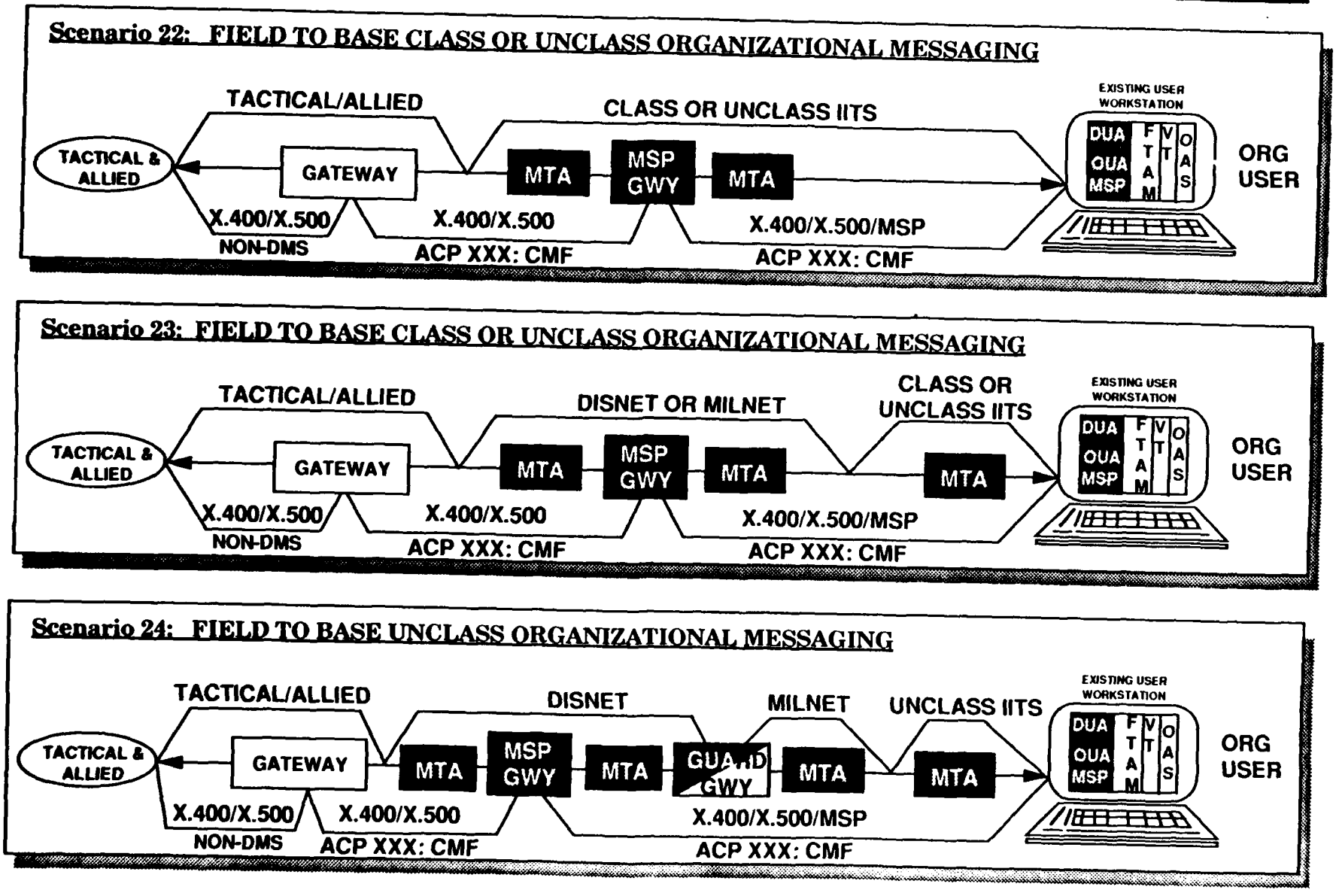


Figure B-6
PHASE 2 CONCEPTS OF OPERATION



the DMS programs, it is assumed that there will be local procedures to ensure only authorized users have access to the DMS. In situations where multiple users share DMS application programs, at logon each user will be individually authenticated, and the user's individual identity may be made available to the message recipient(s). MTA, MS and DIR DMS functional components will be acquired and installed in common-user computers at the base and networks levels. MTA and DSA software will provide message transfer and Directory service support to the subscribers in the respective classified or unclassified baselevel community. Note in Figures B-2 and B-3 that separate MTAs, MSs and DIRs will be installed on both the classified and unclassified segments of the baselevel networks.

b. Message Preparation. After accessing the DMS messaging software, the users will be prompted by a user-friendly messaging software interface. The organizational and individual message formats will be as specified in ACP-XXX. The OUA/UA application programs will employ common, user friendly menu screens to prompt the writer for the following information to prepare organizational and individual messages:

(1) Type of message. The user selects whether this session will be individual or organizational.

(2) Classification label. The user selects the appropriate security classification option based upon the content of the message.

(3) Class of service. The user enters the priority and precedence for the message.

(4) Originating name. The name of the originator is automatically appended to the "FROM" field of the message. Depending upon the type of message being created, either the organization's name or the individual's name is entered. The identity of the releaser is established automatically and indisputably at logon into the DMS.

(5) Action names. The recipient's name(s) is entered in the "TO:" field and may be an organization, individual, distribution list, or MLA name. Should the user not know the recipient's DMS name, the user invokes a "search and find" mode and sends a "best guess, alias, or common name," by the DUA, to the DSA. The DSA asks the local DIB for the "name match" information and returns the recipient's Directory name, O/R address and MSP certificate to the user. Mixed-mode addressing is not permitted in DMS; that is, a single DMS message cannot addressed to both an individual and an organization.

(6) Alternate Recipients. For many organizational messages, depending upon the exact nature of the contents, the user may specify alternate recipients to be used by the MTA in the event of a non-delivery. The O/R name of these alternates would appear on the envelope and their MSP tokens included in the SDNS heading. Normally, alternates would be designated previously based upon agreements made among the organizations involved. However, in the event of unforeseen service disruptions, the DMS management function in conjunction with Directory services may assist the user in identifying appropriate alternates.

(7) Information names (INFO: or CC:). The organization, individual, distribution list, or MLA names of intended recipients of information copies are appended as described for the "To:" names.

(8) Subject indicator code(s). The user enters the subject of the message in this field. This may also be accomplished by other user software applications.

(9) Handling code(s). Special handling instructions, such as requests for signed receipts or alternate delivery actions, are also prompted by the OUA/UA software. The user selects the features desired for the specific message being created.

(10) Message text. The message content is keyed in or appended from a separate file. In the context of DMS, the text is normally narrative; however, X.400 supports data and imagery (including facsimile) as well as text body parts.

(11) Electronic Signature. For organizational messaging, the OUA software automatically enters the MSP digital signature that the recipient can use to indisputably recognize and verify the releaser of the message. For individual messaging, the UA offers the originator the option of invoking the electronic signature.

(12) Probing. This service element contained in the OUA/UA software, enables the user to command the OUA/UA to determine, before the message is submitted to the MTS, whether a particular message can be delivered. The MTS provides the surrogate transfer information and generates delivery and/or non-delivery notifications indicating whether a message with the same information could be delivered to the specified recipient OUA/UA.

c. Directory Service. Directory service is provided by the DMS Directory; there is no need for directory service support to

be provided from AUTODIN messaging or DDN E-mail directories for X.400 - X.400 scenarios. The DUA accesses the DIB through the DSA. A DUA will use information stored locally or interact with DSAs to obtain the requested directory information.

d. Electronic Coordination. If the message requires internal staffing or coordination before being released, a supporting memorandum for record may be appended to the body of the message. The staffing/coordination process may be accomplished using the X.400 MHS or local office automation systems.

e. Release. Once the staffing and/or coordination process is competed, draft organizational messages are transmitted to the appropriate OUA for organizational review and release; whereas, individual messages are release directly by the preparer.

f. Submission. Once the message is released, the MSP application will encrypt it, create the SDNS heading, enclose the headings and encrypted contents into the envelope, place the necessary O/R names, alternate delivery points and other information on the envelope and submit the message to the MTS. Certificates and tokens are generated and exchanged as described in Section B.2.2. After encryption, the content of the DMS message will normally be considered to be unclassified-sensitive information. With MSP protection, the message content is encrypted from UA-to-UA or from UA-to-OUA or from OUA-to-UA or from OAU-to-OUA. If the message is being forwarded through an MSP gateway, then MSP encryption ends at this point. In the scenarios being discussed, one or more MTAs may be resident on the classified or unclassified IITS.

g. Notification. If the MTS cannot deliver a message, a non-delivery notification is sent to the originator in accordance with the instructions on the envelope. Non-delivery notifications include the reason the message was not delivered. Delivery notification carries no implication that any user action has taken place. If a signed receipt is requested, a receipt message is generated and sent to the originator.

h. Accountability. During the message transfer, accountability/audit statistics are recorded by the OUAs, UAs, and gateways involved in the message transfer. The accountability requirement for organizational messages is greater than that for individual messages. When the message has been released as an organizational message, strict message accountability information is recorded from the point of release to all points of delivery. Message accountability information is recorded by the originating OUA, the receiving OUA, and intervening gateways. This information reflects the minimum data

needed to account for organizational messages and refers to the message transactions only (i.e., the data does not refer to recording of complete messages). All MHS components shall be capable of maintaining this audit information for a required period of time (e.g., 30 days) to support problem analysis, statistics collection and tracer actions. The DMS management function can collect this information for administrative and management purposes.

i. Distribution. The recipient's OUA submits the received organizational message, via the MTS, to the ultimate organizational elements specified by the originator. Additionally, the recipient OUA distributes the message to subordinates in accordance with local message distribution policies and procedures. The message content may be re-encryted and re-submitted as either an individual or as an organizational message to each subordinate or internal UA or OUA. This is determined by the message content, prevailing policies and procedures, and the policies and procedures established between the originating and recipient organizations. At each destination, the message text may be decrypted so the user can use an appropriately protected office automation system to read, print, store, or otherwise manipulate the message.

j. Storage. During message transmission each MTA will store the message until a confirmation of message receipt is received from a intermediate MTA or destination MTA. When the originating MTA receives the delivery notice, the message is deleted from the MTA's temporary storage. The originator and recipient(s), as a matter of local procedure, may choose to store messages in off-line storage capabilities (tapes, disks, paper copy) for as long as required. The OUAs will have the capability to store messages in a co-resident message storage system.

B.5.4 Scenarios 4, 5 and 6. These scenarios portray intrabase X.400 to X.400, unclassified individual and organizational messaging, between the unclassified and classified subscriber communities. The general procedural discussions and events described in B.5.1 apply to these scenarios. However, the difference is in how the DMS allows subscribers on the classified and unclassified IITS to exchange messages between the two communities. This need exists in DoD. To accommodate this requirement, a baselevel guard gateway is provided. As described in Section B.2.3.4, the guard gateway discerns the classification of the message and allows only unclassified messages to be exchanged between the two communities. The routing of messages to the guard gateway is a function of the address and profile data of the intended recipients contained in the DIR. The guard gateway uses the Directory to re-submit messages to the MTS. The baselevel guard gateway will send a non-delivery notice to the

originator if the user attempts to send classified information. The routing through and functions performed by the Guard Gateway are transparent to both the originator and the recipient.

B.5.5 Scenarios 7, 8, and 9. These scenarios show the exchange of X.400 messages between different bases interconnected by MILNET and/or DISNET. The message processing/handling steps described in B.5.1 remain valid for these scenarios. The significant difference in these scenarios is that the X.400-X.400 message exchange is interbase. As can be seen in scenarios 7 and 8, network level DMS components are not required to exchange messages between bases as long as the connectivity remains solely MILNET or DISNET. To exchange messages between MILNET and DISNET subscribers, across the network, a network level Guard Gateway is required. As in the similar baselevel scenarios (4, 5, and 6), the employment of the Guard Gateway is transparent to the users. Likewise, only unclassified messages may be exchanged between the two communities through the network level Guard Gateway.

B.5.6 Scenarios 10, 11, and 12. The next three scenarios highlight the events and components involved in exchanging X.400 messages between users that are not end-to-end security compatible. As shown in these scenarios, the users on the left have MSP while those on the right do not. Scenarios 10 and 11 limit the exchange to any messages that are unclassified after MSP decryption since the subscribers are connected to only MILNET or are exchanging messages between MILNET and DISNET. Additionally, the sender-to-recipient pair is mismatched with respect to MSP. Therefore, the MSP Gateway is employed to add or delete the MSP encryption, making the exchange compatible end-to-end. The MSP gateway is transparent to the sender or recipient. The employment of and routing to the MSP gateway is facilitated by the information contained in the DIB. For example, the MTA on the left of the MSP gateways in each of these scenarios uses its DUA or local Directory cache to determine if the intended recipient has MSP. If not, the MTA forwards the message to the MSP gateway. If the intended recipient has MSP capability, the MTA forwards the message to the recipient's MTA, not to the MSP gateway. Scenario 12 shows the exchange of both classified or unclassified messages between subscribers on only DISNET or MILNET Additionally, the sender and receiver do not both have MSP. Since users with MSP do not have the option of by-passing or turning off MSP, a mismatch occurs. Again, the MSP gateway is utilized to allow compatible end-to-end message exchange. For the DISNET option, it is assumed that the connectivity between the user without MSP and the MSP gateway is protected by other means.

B.5.7 Scenarios 13, 14, and 15. These scenarios portray messaging between X.400 users and those using the baseline

SMTP-based E-Mail. The SMTP-based DMS users in Phase 2 access the DMS through the baselevel and regional ADIs, which they may access through a network level TAC, through a dial-up port, through a local area network, or through a direct connection. As mentioned before, an early Phase 2 transition strategy is to incorporate into the B-ADIs and R-ADIs the capability to translate between the SMTP protocols and RFC 822 format and the X.400 protocols and the ACP-XXX formats. The SMTP-based E-Mail host that cannot connect to an ADI must interface with an OSI Gateway at the network level to obtain conversion between SMTP and X.400. The ADI and/or OSI gateways use the Directory to submit the message to the MTS and on to the intended recipient(s). In the process, the MTA passes the message through an MSP gateway to be encrypted so that it will be compatible with the recipient's OUA/UA employing MSP. If the Directory indicates that the X.400 recipient is not employing MSP (an individual user), the MTS will not deliver the message to an MSP gateway (note: this variation is not depicted in these scenarios). The MSP gateway submits the message to the MTS for delivery to the designated recipient(s). If the message is traversing from the network level to the base level, as shown in Scenario 15, the interface between the SMTP and X.400 systems is at the network level. Since the OSI gateway performs no RFC 822/CMF conversion, the RFC 822 message format is retained but packaged in X.400 envelopes as the message progresses from left to right in Scenario 15. In the reverse process, the CMF format is retained as the message progresses to the SMTP user on the left. It is assumed that each user in this exchange has application software which enables each user to read the other's message text. It is noted that the MSP gateway is shown at the network level, since it is logical to provide MSP protection as close to the non-MSP subscriber as possible. As in the previously defined scenarios, the message will be delivered by the MTA to the destination OUA, UA, or MS as appropriate.

B.5.8 Scenarios 16 and 17. The following two scenarios reflect the message exchange between X.400 DMS users and the Internet community. It is planned that classified and unclassified base level X.400 users shall require an UNCLASSIFIED ONLY interface to users in the Internet. The X.400 users will invoke their messaging capability as described in the previous scenarios. Once the message is prepared and submitted to the MTA, it will be delivered to an MSP gateway for decryption. If the unclassified message is being submitted from a classified IITS, it will be passed through a baselevel or network level Guard Gateway (only the network level scenario is shown). This places the message on MILNET, which has the only direct network interface with the Internet. The MTAs on MILNET will then forward the message to a network level OSI gateway for X.400 to SMTP. The DDN supported Mail Bridge provides the final interface to the Internet

community. From left to right, the messages remain in CMF. In the reverse direction, since the OSI gateway performs no format conversion, the messages remain in RFC 822 format. Again, it is assumed that the users have application software so that they can read each other's message text. At the end of Phase 2, the OSI gateway is phased out and its functionality is assumed to be provided by the Mail Bridge. Messages originated from the Internet follow the reverse path to the X.400 subscriber.

B.5.9 Scenario 18. This scenario reflects the exchange of messages between an AUTODIN-based subscriber, serviced through a TCC, and an X.400 subscriber. This scenario supports the exchange of only organizational messages. The AUTODIN user interfaces with the TCC, as described in Appendix A. Once the TCC injects the message into AUTODIN, it will be routed to either a B-ADI or R-ADI. These components provide conversion between the AUTODIN JANAP-128 and CMF formats and the X.400 protocols of the DMS target architecture. The ADI submits the message to the MTS. Along the path, an MSP Gateway will be used to provide encryption/decryption compatibility.

B.5.10 Scenarios 19 and 20. These scenarios reflect the exchange of messages in the transition period during which remaining AUTODIN subscribers begin to receive service for DIN/DMS gateways (rather than form ASCs), as the ASCs are phased out. Specifically, as an ASC is closed, any remaining subscribers who still use AUTODIN-type applications (i.e., JANAP-128/ACP-127) will normally be transitioned to a DIN/DMS gateway, which will provide the required AUTODIN functionality as well as an interface with the X.400 users on DDN. An MSP gateway is employed at the network level to encrypt or decrypt the message, as needed. Scenario 20 reflects the situation where a user with AUTODIN applications may only have access to the DIN/DMS gateway connected to the DISNET but has the requirement to send an unclassified message to a MILNET subscriber. In this case, the Guard Gateway is used to pass unclassified messages between the classified and unclassified communities. The network level MTAs forwards the message to the appropriate base level MTA, which ensures the delivery to the appropriate recipient.

B.5.11 Scenario 21. This scenario shows the message exchange between a Tactical/Allied subscriber, connected directly to an ASC, and an X.400 organizational user. The tactical/allied subscriber referred to is the one on the bottom left of Figure B-2. The AUTODIN message is routed to a regional ADI. The ADI converts to X.400 and submits the X.400 message to a network level MTA. Also at the network level, an MSP gateway is involved to apply or remove MSP encryption. The MTS then delivers the message to the X.400 organizational user.

B.5.12 Scenarios 22, 23, and 24. The final three scenarios depict message exchange between tactical/allied subscribers having non-DMS X.400 messaging capabilities and the DMS X.400 subscribers. The DMS assumes the development and deployment of an interface that translates between X.400 systems that are incompatible with the X.400 software used within the DMS. This gateway is a DMS component designed to provide continuing interoperability with the tactical/allied communities. The tactical/allied gateway submits the message to the DMS MTS. At that point, the messaging scenarios within the DMS are as described before.

B.6 Comparison to requirements.

This section compares the objectives and transition strategies defined in this appendix to the basic DMS requirements stated in the body of the TAIS. This comparison ensures the Phase 2 events and plans comply with and support the attainment of the basic DMS requirements.

B.6.1 Connectivity/Interoperability. Components and logical functions based on the X.400 MHS model, implemented during Phase 2, provide significant improvements in flexibility and interoperability among users. For the majority of DoD users, writer-to-reader connectivity from their workstations is achieved by the end of Phase 2. Continued emphasis is placed on achieving writer-to-reader connectivity between the DMS and non-DMS communities. This requires specific coordinated security policy negotiations and interoperability engineering by the planners in each community.

B.6.2 Guaranteed Delivery. The elements of service provided by X.400, X.500, SDNS, and the DMS management functions ensure satisfaction of this requirement. The combined use of such elements as delivery or non-delivery notification, alternate recipient assignments and routing, probing, message/packet accountability, non-repudiation of delivery, proof of delivery, etc., provide a high guarantee that a message will be delivered to an authorized recipient. The dynamics, such as routing, bandwidth utilization, and high reliability of packet delivery, offered by a packet-switched network enhances the satisfaction of this requirement.

B.6.3 Timely Delivery. The extension of the message system interface point to the user's workstation is the major contributor to the satisfaction of this requirement. The three grades of delivery selection are available to the originators of X.400 messages. The originator can request that the transfer through the MTS be urgent or non-urgent, rather than normal. The time periods defined for non-urgent and urgent transfer are

longer and shorter, respectively, than defined for normal transfer. The time delivery selection made by the originator is also sent to the recipient with the message. The implementation of the X.400 optional priority-level-qualifiers may enhance the COTS X.400 priority scheme. These are being currently defined in a Draft NATO STANAG XXXX: Military Message Handling System, dated 16/02/90. These are currently viewed as potential optional service elements to a COTS X.400 package. The Draft NATO STANAG defines these priority-level-qualifiers as an optional extension field of P1, P3 (both submission and delivery) and P7 protocols. The qualifiers are "low" and "high" for each of the grades of delivery mentioned above. The DMSIG is investigating these suggested options. Figure B-7 depicts the grades of delivery and suggested optional qualifier relationships.

B.6.4 Confidentiality/Security. MSP, in combination with lower layer security, affords all DMS messages the protection appropriate to the sensitivity or classification of the information contained in the body of the message. The baselevel and network Guard Gateways and the Directory maintain appropriate separation and protection between MILNET and DISNET communities. The IITS and DIS afford the appropriate protection of the data being processed through their transport utilities. Special gateways are implemented to maintain security integrity and compatibility between writers and readers not having the same encryption mechanisms. The DMS relies upon effective local policies and procedures to ensure appropriately cleared personnel have access to sensitive material.

B.6.5 Sender Authentication. X.400 offers elements of service such as non-repudiation of origin and originator indication to satisfy this requirement. In addition, SDNS MSP offers security services such as non-repudiation of origin, access control, and authentication. These capabilities provide unambiguous verification that the information marked as having originated from a given source did in fact originate there.

B.6.6 Integrity. Implementation of newer transport utility protocols that use cyclic redundancy checks instead of the simple parity checks offered by some of the DoD protocols (such as DCS Mode I) provide improved error detection and correction capabilities. Within X.400, the content integrity service element enables an originator to provide the recipient a means to verify that the content of the message was not modified. X.400 also offers the message sequence integrity service element that allows the originator to provide the recipient a means to verify that the sequence of messages from originator to recipient has been preserved. SDNS also offers a data integrity service that corroborates the source of all data units transferred on a message exchange connection. These SDNS integrity services

Figure B-7
PHASE 2 DMS PROPOSED DELIVERY PRIORITIES

MILITARY PRIORITY	X.400 SCHEME	X.400 OPTIONAL QUALIFIERS
	NON-URGENT	LOW
ROUTINE	NON-URGENT	HIGH
PRIORITY	NORMAL	LOW
IMMEDIATE	NORMAL	HIGH
FLASH	URGENT	LOW
CRITIC	URGENT	HIGH

include connection integrity with recovery, connection integrity without recovery, selective field connection integrity, connectionless integrity, and selective field connectionless integrity. The use of the various integrity services mentioned above satisfy this requirement.

B.6.7 Survivability. DMS components are as survivable as the environment in which they are placed. The DMS has enhanced survivability characteristics based upon highly distributed, resource sharing implementation concept and the high degree of connectivity among these distributed components via the IITS and DIS.

B.6.8 Availability/Reliability. The DMS uses COTS components requiring little downtime (high Mean Time Between Failure (MTBF) and low Mean Time To Repair (MTTR). Since most DMS components are COTS items, component replacement and repair are relatively fast. Redundant DMS components can be placed to support critical availability and reliability requirements. DMS components, such as OUAs, can provide back-up for other DMS components. The multiple connectivity between MTAs, the alternate delivery schemes provided by the DMS, and the routing inherent in a packet-switched network provide very high availability and reliability to the DMS. The DMS relies upon effective local procedures to maintain required levels of operational readiness.

B.6.9 Ease of Use. The publication and use of ACP-XXX facilitates the ease of interfacing with and using the DMS. The X.400 MHS applications will reside in the user's workstation and include a user-friendly, man-machine interface. The use of menu-driven, screen prompts, object-oriented interfaces, and help functions are some of the user-friendly tools contained in COTS X.400 packages. Likewise, user-friendly naming and other directory service characteristics afford a friendly human-oriented interface between the user and the DMS Directory Services.

B.6.10 Identification of Recipients. The DMS Directory Services provide unambiguous identification to the MTS of the intended recipient organization or individuals. The DMS naming conventions include aliases and distinguished names. Through the DUA, the sender can look-up and browse the Directory based upon employing one of the naming conventions mentioned above. Further definition of the recipient is provided through the Directory's use of attributes associated with each database entry. Additionally, X.500 and SDNS offer strong authentication services to guarantee identification of recipients to the releaser of a message.

B.6.11 Preparation Support. At each user workstation, the DMS

provides user-friendly prompting and help functions to permit a user to process a DMS message with no special training. Through the use of common, user-friendly menu screens, the writer is guided in the preparation of DMS messages in the ACP-XXX Common Message Format.

B.6.12 Storage and Retrieval Support. The X.400 message store provides a highly flexible storage and retrieval capability to DMS users. For organizational users, additional internal or collocated storage and retrieval mechanisms are provided. ACP-XXX specifies the minimum storage period for organizational and individual messages.

B.6.13 Distribution Determination and Delivery. This function, which applies primarily to organizational messages, will be an automated capability of the OUA accomplished in accordance with the organization's policy. Distribution profiles reflecting the organization's distribution policy will be implemented at the OUA and maintained by the local organization. Message distribution will normally be accomplished electronically by sending organizational messages from the OUA to the organization's subordinate OUAs and/or individual messages to individual users' UAs. Abnormal conditions (high precedence, high classification, OUA/UAs inoperable) will be handled by the submitting OUA through alternate delivery, or review and delivery by other means. For example, in the case of an urgent message, if delivery cannot be effected within a specified time period, this will result in a non-delivery notification and cause the message to be hand-delivered to the staff duty officer for action in accordance with local policy. The DMS security services can provide proof of delivery to the originator, provided both the originator and recipient subscribe to this service feature.

Appendix C

Phase 3 Implementation

C.0 Introduction.

The evolution to the DMS Target Architecture is nominally completed during this phase. However, given the anticipated pace of change in telecommunications technology, by the beginning of Phase 3 the DMS Target Architecture itself will undoubtedly evolve from that presented in Section 3 of the DMS TAIS. The vision of Phase 3 is to complete the evolution to X.400/X.500/MSP messaging started in Phase 2, and incorporate those intervening technological improvements which will enhance DMS services or reduce user cost. Thus, this phase will take full advantage of the experiences gained during Phases 1 and 2, the advances in user terminal and messaging technology and the migration of local and long haul communications to the Integrated Services Digital Network (ISDN) as envisioned by the Integrated Communications Architecture (ICA).

C.1 Phase 3 Objectives.

During this phase, actions previously initiated will be completed. Policy and procedural actions previously completed may need to be reviewed as the result of the lessons learned during Phases 1 and 2 and the advances in technology. The major Phase 3 objectives are:

(a) Continue the implementation of DMS writer-to-reader services started in Phase 2.

(b) Maintain the message exchange interoperability between DMS and the tactical, Allied, non-DoD Government, commercial and research messaging communities.

(c) Upgrade messaging applications in user facilities which do not have the complete X.400/X.500/MSP suite.

(d) Complete the phase out of TCCs and the related protocols, procedures and policies.

(e) Phase out the DIN/DMS gateways.

(f) Evolve to become the store-and-forward messaging portion of the Integrated Communications Architecture (ICA).

C.2 Phase 3 Architecture.

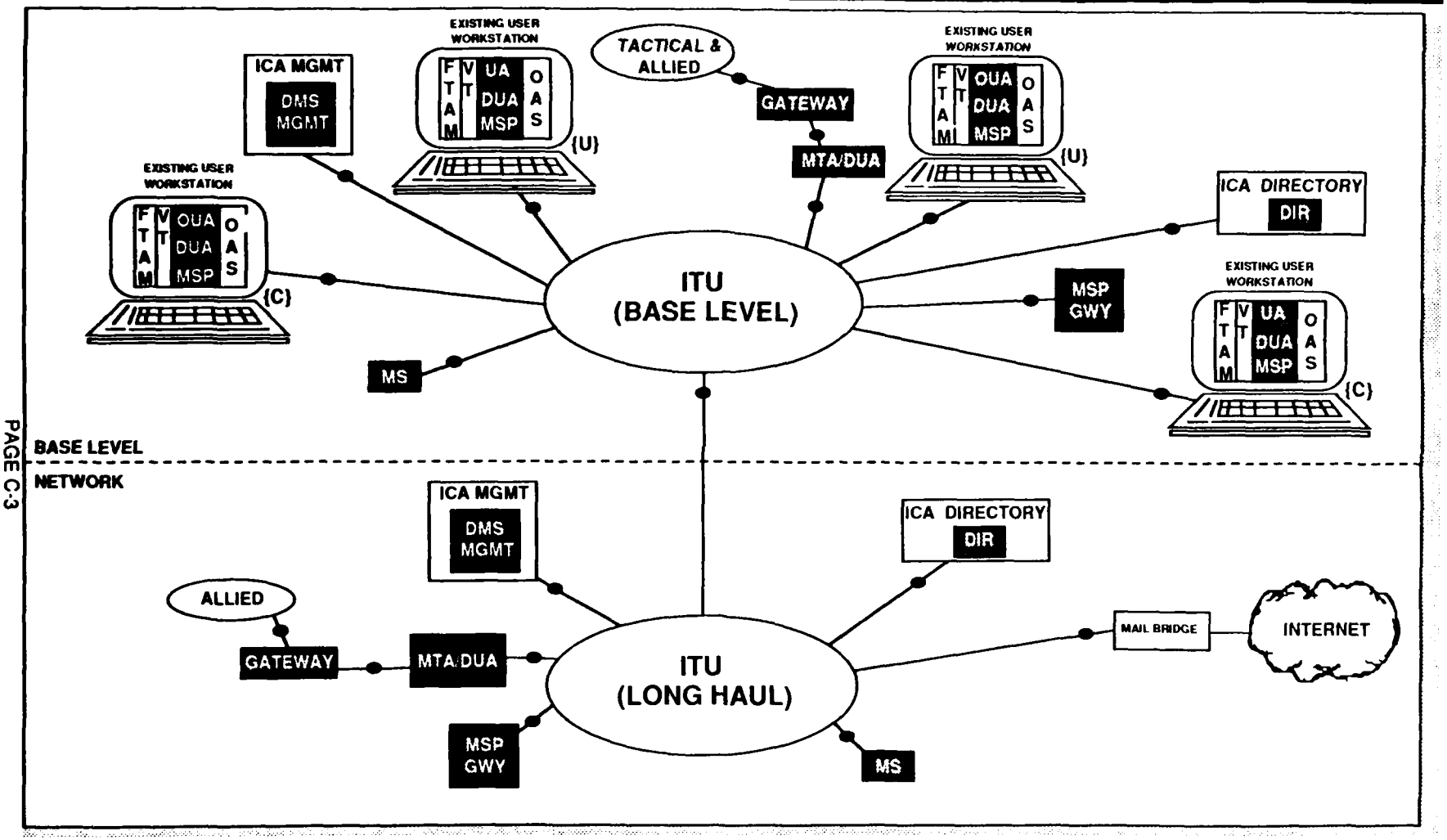
The initial fielding of X.400 messaging and X.500 directory functions along with MSP end-to-end encryption was accomplished during Phase 2. These DMS components have been detailed in Appendix B and their implementation will continue into Phase 3. No new DMS components are currently planned. However, advances in technology may result in new components for either new service(s) or further cost and manpower savings. The DMS Phase 3 architecture is depicted in Figure C-1 and represents a further level of detail to that shown in Figure 3-1 of the TAIS. However, as a result of the evolution of the Defense Information System and the emergence of the Integrated Communications Architecture, some components will be Multi-Level Secure (MLS) rather than being dedicated to either classified or unclassified service.

C.2.1 DMS Message Handling System (MHS). DMS employs the X.400 based message handling system which includes the User Agent (UA), Message Transfer Agent (MTA), and Message Store (MS) functionalities. In addition, a DMS-unique Organizational User Agent (OUA) is identified to satisfy the specific DoD requirements for handling organizational messages. The description of these MHS components provided in Section 3 of the TAIS and amplified in Appendix B continues to remain valid for Phase 3.

C.2.2 Directory (DIR). The Directory consists of the integrated Directory Information Base (DIB) implemented in Phase 2 and the Directory Service Agents. Users which access the DIB include UAs, OUAs, MTAs, and gateways and obtain this access via the interaction of their DUA with the DSA. These components, described in Section 3 and detailed in Appendix B, remain valid and within Phase 3 are expected to be part of the larger ICA directory.

C.2.3 Management (MGMT). The DMS management capability, operational during the Phase 2 time frame, continues through Phase 3 as an integral DMS component. These capabilities, as detailed in Appendix B, include fault and problem management, configuration management, performance monitoring, security and access management, accounting, and directory service management. The network and base level MGMT components reflect cooperating functionalities which will be interoperable with the Defense Information System (DIS) management. MGMT will take full advantage of the operational experience of Phases 1 and 2 to incorporate within it enhanced capabilities and improved services. In Phase 3, it is anticipated that DMS management will continue to evolve as a part of the ICA management functionality.

Figure C-1
DMS PHASE 3 ARCHITECTURE



PAGE C-3

LEGEND		
■ – DMS Functions and Components	DIR – Integrated X 500/SDNS Directory	FTAM – File Transfer, Access, And Management
● – Lower Layer Security	MS – X 400 Message Store	OUA Organizational User Agent
MSP – Message Security Protocol	MTA – X 400 Message Transfer Agent	UA User Agent
MSP GWY – SDNS MSP Gateway	VT – Virtual Terminal	DUA – X 500 Directory User Agent
ICA – Integrated Communications Architecture	DMS MGMT – DMS Management Capability	ITU – Information Transfer Utility
C – Classified	U Unclassified	

C.2.4 Security. As detailed in Appendix B, the DMS provides writer-to-reader security services through SDNS MSP and lower layer security as may be appropriate. In Phase 3, all users, individual and organizational, will employ MSP protection as improved workstations are expected to be common place. It is expected that the DMS security requirements will continue to be satisfied through MSP and lower layer devices as a subset of the ICA Security Architecture.

C.2.5 MSP Gateway. The MSP gateway provides the continued interoperability required between DMS subscribers, all of whom have MSP in Phase 3, and the non-MSP community (i.e., the Internet, consisting of commercial, industrial, other government, and university users, some tactical components and, in particular, the Allied community).

C.2.6 Guard Gateway. In Phase 2, the Guard gateway was fielded to allow controlled exchange of unclassified messages between the classified and unclassified communities. In Phase 3, this functionality is expected to be performed within the base and network level Information Transfer Utilities (ITU). Continuation of the Guard Gateway as a DMS component depends upon the evolution of the Phase 2 base and network level transmission components into the Defense Information System.

C.2.7 Allied and Tactical Gateways. It is anticipated that in addition to an MSP gateway, the Allied and tactical community may require an additional gateway to interface with DMS. This requirement is being studied in Phase 2 and the results will be incorporated into the Phase 3 architecture.

C.2.8 Defense Information System (DIS) Information Transfer Utility (ITU). As envisioned by ICA, in Phase 3 the base and network level connectivity will be provided by an Integrated Services Digital Network (ISDN) based ITU. The Installation Information Transfer System (IITS) and the long haul DCS (MILNET and DISNET) evolve into the ITU. The DMS is not predicated upon this outcome since the Phase 2 transport systems together with the Guard Gateway met the DMS requirements in this area. As with these components, the DMS will rely on the ITU to furnish connectivity, the lower layer security protection needed to provide peer entity authentication (e.g.,SDNS SP4), and connection integrity (e.g., Blacker or SDNS SP3/SP4) as may be required by DMS security policy. The interoperability of the base and network level transport mechanisms, provided by the ITU, permits DMS to achieve complete writer-to-reader connectivity.

C.2.9 Connections. The target architecture allows for total connectivity and interoperability from a network standpoint by using the available ISDN standards and a standard set of

available ISDN service offerings. These standards and services are to be provided and used at the base/local level as well as at the network level. This connectivity and interoperation is, of course, subject to the security and policy requirements of the DoD and the individual organizations.

C.3 Phase 3 Transition Strategies.

C.3.1. Continued implementation of DMS writer-to-reader services. This phase will continue the deployment of the X.400/X.500/MSP organizational and individual messaging services using the integrated DMS Directory, MSP gateway, Allied and tactical gateways, and management capabilities implemented in Phase 2.

C.3.2 Maintain message exchange interoperability. Interoperability with the Allied, tactical, non-DoD Government, commercial and research communities will be maintained through the use of appropriate standards or gateways. In Phase 3, these may include the Allied, tactical and MSP gateways, and the mail bridge interfacing DMS with the Internet community.

C.3.3 Upgrade or Replace Phase 2 Messaging Applications. Those Phase 2 workstations which have not implemented the complete X.400/X.500/MSP suite, or those workstations/terminals which shared the OUA/UA/DUA/MSP functionalities, will be upgraded to the full suite of the DMS capabilities.

C.3.4. Phasing Out of Telecommunication Centers. The evolutionary phase out of TCCs begun in Phase 1 and continued during Phase 2 will be completed within Phase 3. Consequently, SMTP, JANAP 128 and ACP 127 will no longer be supported by DMS.

C.3.5. Phasing out of DIN/DMS gateway. As a result of completing the phase out the TCCs, the transitional DIN/DMS gateway is no longer required and will be phased out.

C.3.6 Transition to the Integrated Communications Architecture (ICA). During Phase 3, it is envisioned that the DMS security architecture, Directory and Management components will be phased into the ICA. The details of this transition will be developed as a result of the ICA/DMS issues addressed in Phase 2. While DMS messaging is not predicated upon ICA, the DMS Target Architecture can, however, serve as the basis for the ICA in these three areas. Depending upon the ICA security architecture, the guard gateways at the base level may be phased out if their functionality is subsumed by the DIS ITU.

C.4 Phase 3 Transition Actions.

C.4.1. Central and Joint Project Actions. The Phase 3 objectives include the continued expansion of DMS services and the phase out of TCCs and the DIN/DMS gateway. It is envisioned that as the DMS evolves, new service features will be requested and the subscriber base will increase. While no specific Phase 3 Central and/or Joint project is identified, the Implementation Strategy will include new project actions to the extent that service improvements and cost or manpower savings warrant their inclusion. Also, projects may be required in Phase 3 to insure DMS compatibility with the ICA implementation of ISDN in the backbone and the IITS at each installation and base in the DoD. In addition, the expected merging of the security architecture, DMS Directory and Management services into the ICA may also require some project actions to insure that DMS user messaging services are maintained. Specific project actions for Phase 3 will be identified in subsequent updates of this appendix.

C.4.2 R&D Projects. Evolving messaging and communications technology demand that R&D be an integral part of the DMS evolution. During Phase 3, R&D is required to maintain a forward looking objective to evaluate and improve upon what then will be the current DMS architecture. It is anticipated that there will be a continuing need for R&D in the areas of technology and capabilities assessments to include directory and management services, security, user interfaces, MTS components, transmission and a broader set of messaging applications and services.

C.4.3 Policy Actions.

Policy issues will continue to be worked during this phase. Perhaps the most pressing policy issues will deal with the amount of freedom users at the local level will be given in message origination and how to control the capabilities that are inherent in the evolving messaging and communication technologies.

C.5 Phase 3 Operational Concept.

C.5.1 Introduction. Those Phase 2 users enjoying the X.400/X.500/MSP DMS services will perceive no change in transitioning from Phase 2 to Phase 3 for messaging within that community. As this service is expanded, improvements will be apparent both for the newly serviced users and the existing X.400/X.500/MSP user community exchanging messages with them. The concept of operations during Phase 3 remains as described in Section 3, Target Architecture. The message originator logs onto a workstation to prepare a message and the UA or OUA prompts the user for the required information using common, interactive screens. If the user needs help in understanding the prompts, informative help menus will be available for each step of the messaging process. The user can obtain message recipient(s)

addressing information and MSP certificates from the Directory. Message recipient(s) addressing information can also be obtained from a local cache. The message preparation capability and the DMS messaging interfaces are integral parts of the office automation package on the workstation. If the message must be staffed, it can be done so electronically using the DMS capabilities. When the message, if organizational, is ready to be released, the OUA supports this action. SDNS protection is transparent to the users and the message content is encrypted end-to-end. When the message is delivered to the recipient it is decrypted for presentation. The message can be read, stored, forwarded or otherwise manipulated by the user's local office automation facilities. All DMS messaging will employ the ACP XXX Common Message Format (CMF) and procedures.

C.5.2 Message Exchange Scenarios. Typical message exchange scenarios are illustrated in Figure C-2. As noted in Appendix B, all diagrams use the same construct in presenting a scenario. The top line(s) connecting the two subscribers indicate which transport segments are involved in the message exchange. The center arrow indicates the DMS messaging components involved. The bottom line(s) indicates both the format and protocol used and where their conversion is performed.

a. Intra-base DMS Messaging. Scenarios 1 through 6 in Figure C-2 illustrate typical writer-to-reader target architecture intra-base flows for individual and organizational messages. Scenarios 3 and 6 depict the local distribution of an organizational message and the exchange and coordination of draft organizational messages. The ITU is expected to provide the required DMS security services, including the functionality of the Guard Gateway identified as a separate component for the IITS and MILNET/DISNET.

b. Inter-base Messaging. As noted in Scenarios 7 through 10, all inter-base messaging uses the ITU at both the base and network levels. Scenario 9 illustrates the inter-base "local" distribution of an organizational message as well as the coordination of draft organizational messages. Scenario 10 illustrates inter-base individual messaging with an Internet user.

c. Allied and Tactical Messaging. Organizational message exchange between the Allied and tactical communities and the DMS community is illustrated in Scenarios 11 and 12. The individual messaging scenario, not shown, would be identical. However, in the case of organizational messages, the Allied and tactical segments or interface devices, would have to be certified through

Figure C-2
PHASE 3 CONCEPTS OF OPERATION

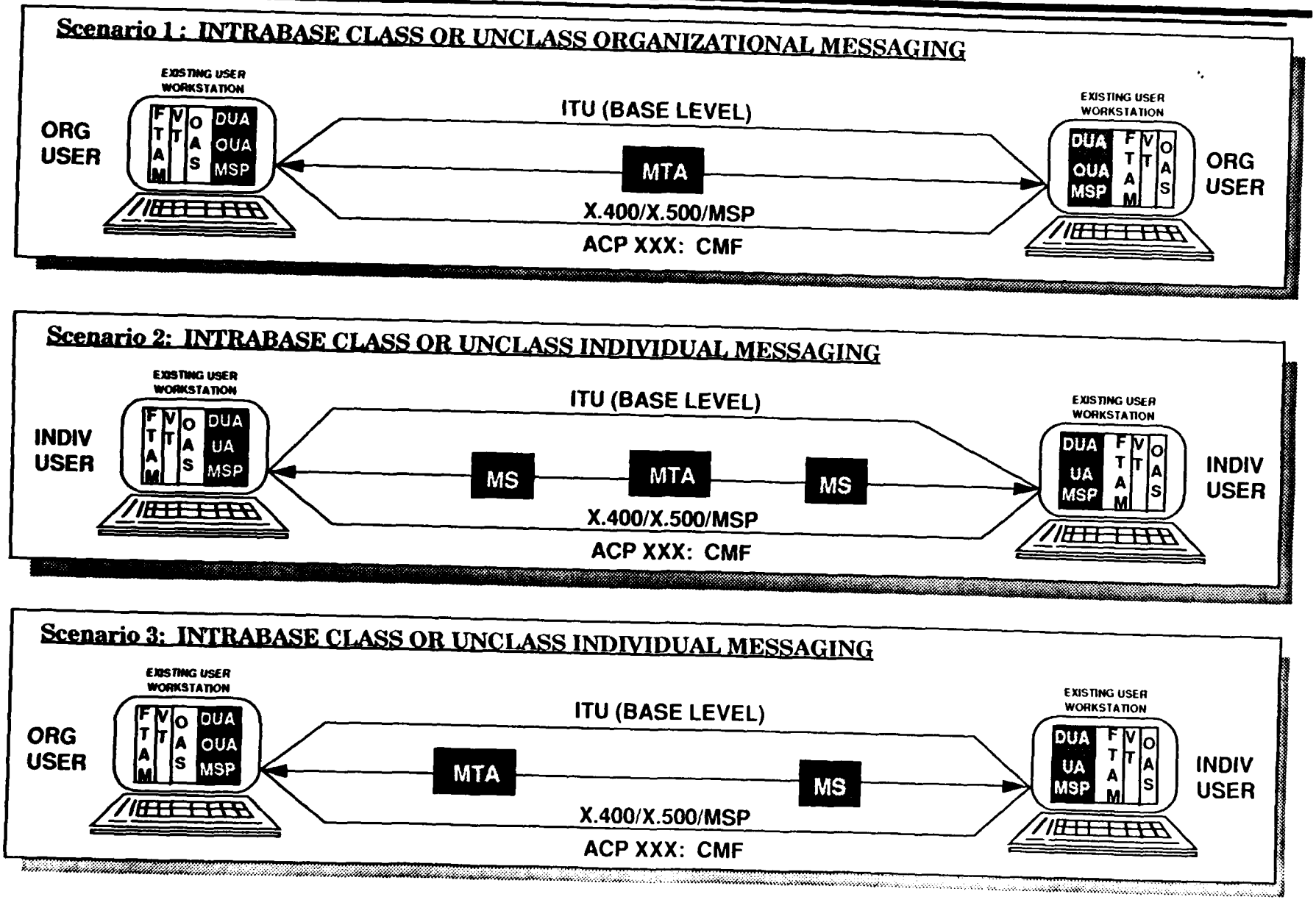


Figure C-2
PHASE 3 CONCEPTS OF OPERATION

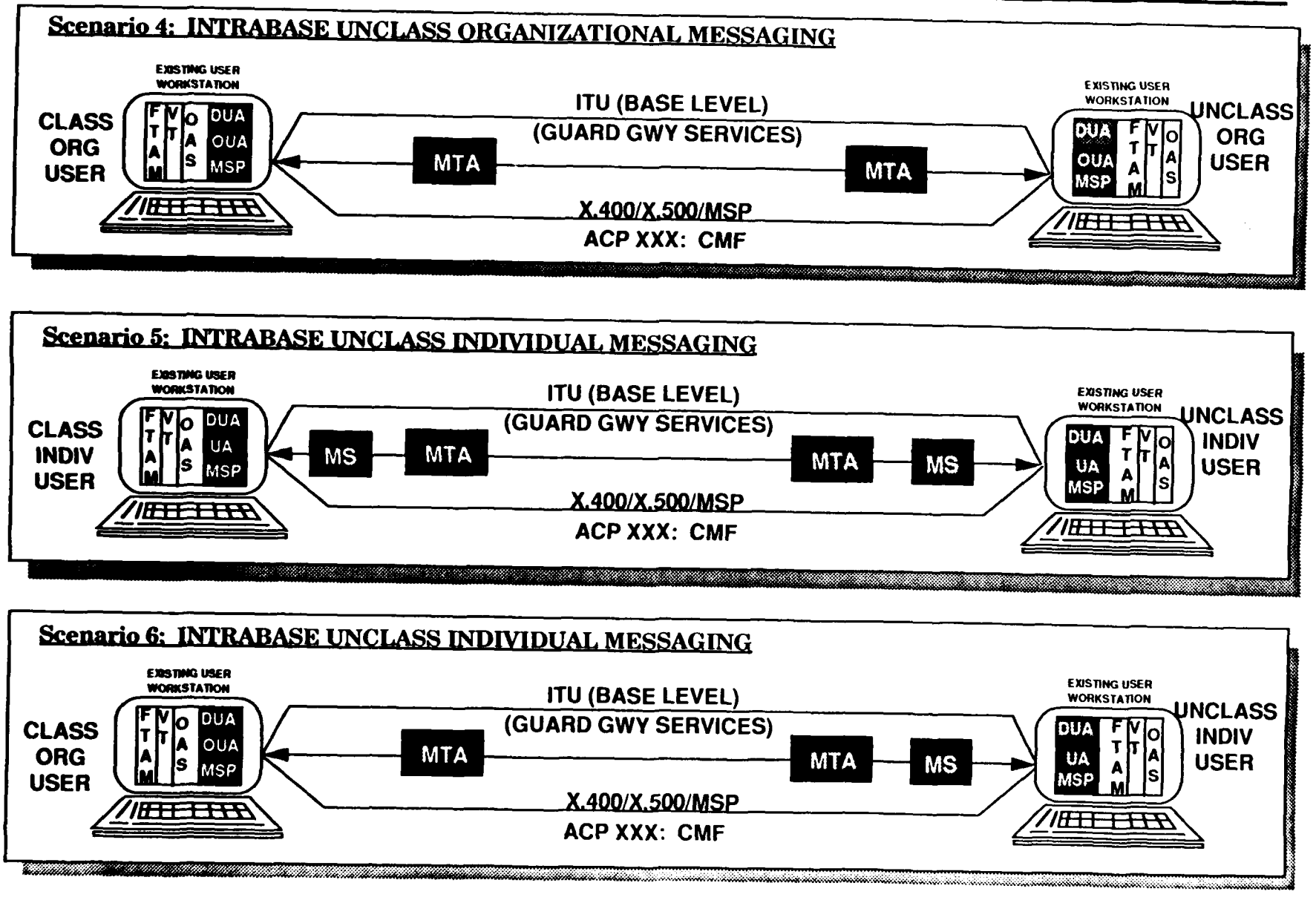


Figure C-2
PHASE 3 CONCEPTS OF OPERATION

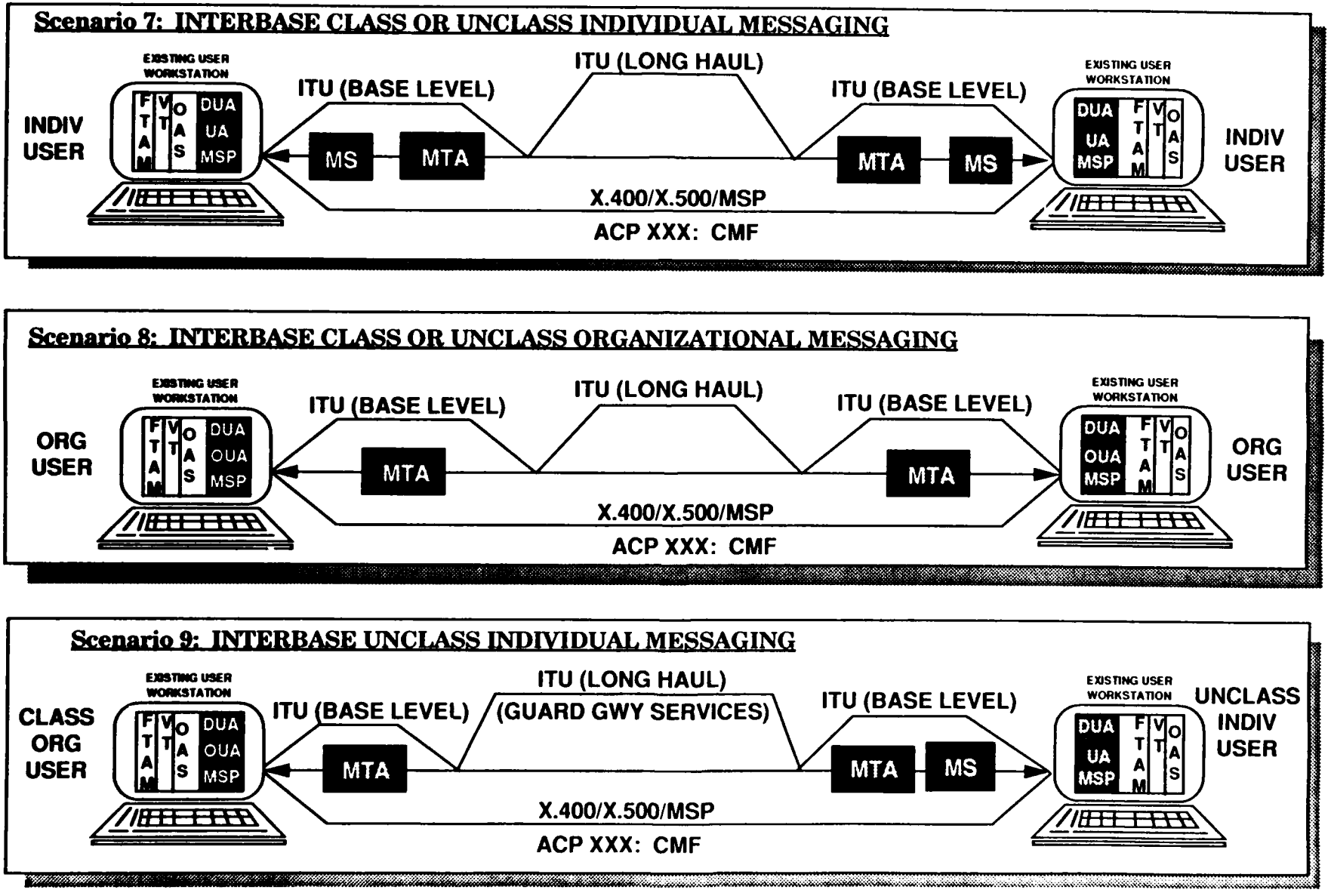
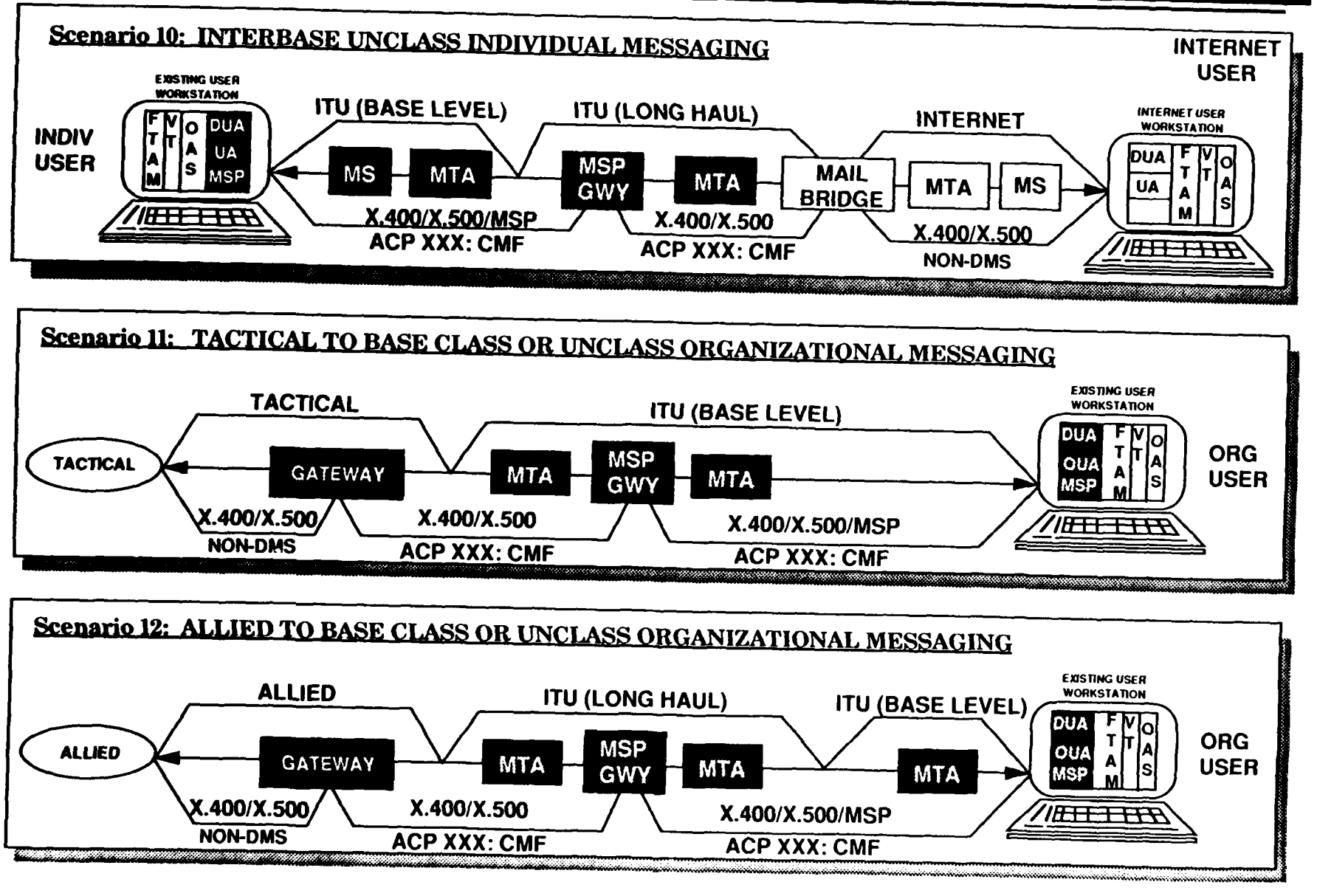


Figure C-2
PHASE 3 CONCEPTS OF OPERATION



the DMS certification process that was put in place during Phase 1. Scenario 12 illustrates Allied messages entering at the network level. Although not illustrated, Allied messages for a user at a base could also enter the DMS at the base level (as illustrated in Scenario 11 for tactical messages).

C.6 Comparison to Requirements. Phase 3 achieves the Target Architecture, and all MROC requirements are satisfied.

a. Connectivity/Interoperability. DMS writer-to-reader connectivity is provided at the user work spaces by using the DoD 5200.28, ISO OSI, CCITT, ISDN, and SDNS MSP standards, and communicating over the ITU. In particular, electronic messages are transferred from UA/OUA to UA/OUA using the CCITT X.400 series of protocols, as refined and implemented in ACP XXX. The use of these standards eliminates incompatible communications protocols and character sets. Interfaces are provided for interconnecting with the civil, tactical, allied, and commercial environments. The DMS requires that the ITU provide the reliable networking connectivity between DMS components.

b. Guaranteed Delivery/Accountability. The X.400 MTS for DMS delivers messages and provides non-delivery notification as required. A message originator is required to select the type(s) of service parameters appropriate for all messages, the MTS is robust enough to provide the message originator with these selected service(s). All organizational messages require non-delivery notification. Organizational messages also require that the message originator be held accountable for message delivery to all indicated recipients until an indication of message delivery is returned. After message delivery is complete, message accountability is provided as required by appropriate Joint Staff and DoD guidance. The guaranteed delivery and accountability capability of the DMS is dependant upon the reliability of the ITU.

c. Timely Delivery. Timely Delivery of messages in DMS is accomplished using the standard X.400 and X.500 facilities for delivery/non-delivery notices, precedence, and alternate recipients. The MTS holds routine messages until they can be delivered, or until a timeout parameter has expired and a non-delivery notice is returned to the message originator. For high priority messages, non-delivery notices are returned almost immediately (as set by X.400 timing parameters) and the message originator then sends the message to an alternate recipient for action, with a copy also being sent to the original intended recipient for informational purposes. Timely delivery of DMS messages depends on the availability of the ITU, and the appropriate DMS components (i.e., MGMT, DIR, DUA, MTA, UA, OUA, MS and MSP Gateway).

d. Confidentiality/Security. Confidentiality of message text and the association of the appropriate security label during transit through the DMS are provided by the SDNS MSP. Security of messages before transmission, and after receipt, are provided by a combination of the MSP confidentiality service and the trusted computer systems in which the DMS components exist. These mechanisms afford the appropriate level of security for the data being protected. The confidentiality of directory and message addressing information makes use of the confidentiality services of the lower ISO layer protocols (e.g., SP4). These lower layer confidentiality services depend on the ITU meeting these requirements.

e. Sender Authentication. Physical security requirements placed on the DMS components and the implementation of the SDNS MSP provides authentication of the DMS message originator. Release authority for organizational messages is also provided by these same means. Authentication of a request for directory information and the authentication of the requested directory information is provided by the transport network's lower layer security. The authentication of MTS components is also provided by lower layer security. These lower layer authentication services depend on the ITU meeting these requirements.

f. Integrity. The integrity of message text, addressing, and security parameters, during transit through the DMS, is provided by the SDNS MSP. The integrity of messages while in preparation, and after receipt, make use of a combination of the SDNS MSP provided confidentiality service and of the trusted computer systems in which the DMS components exist. These services are provided to a level appropriate for the data being protected. The integrity of directory and message addressing information make use of the integrity features of the lower ISO layer protocols (e.g., SP4). These lower layer integrity services depend on the ITU meeting these requirements.

g. Survivability. DMS components, and their connectivity, insure that the appropriate survivability levels are met. DMS components do not reduce the survivability of the communications facilities to which they are attached. DMS survivability relies on the ITU and the Service/agency locations which house DMS components. The connection of DMS components to ITU facilities will depend on the survivability characteristics of those locations.

h. Availability/Reliability. New or upgraded DMS components are expected to have little downtime and to be supported by inexpensive, highly reliable power and environmental support facilities. Those components requiring 24-hour-per-day availability (e.g., MGMT, DIR, MTA, MS, OUA) will be either

redundant or backed-up. ISDN technology allows for dynamic reconfiguration of the network which greatly enhances the availability/reliability of the DMS.

i. Ease of Use. The emergence of a simplified, X.400 based Common Message Format and procedures (ACP-XXX) will allow users to interact directly with the DMS using their own office automation capabilities with which they should be intimately familiar. Specialized communications skills will not be required. User interaction with the MHS, to include the security services and the directory and key management functions, will be for the most part, user transparent. Should the user need assistance in preparing or handling a message, automated help will be available for each step or procedure in use.

j. Identification of Recipients. The use of the SDNS MSP and DMS directory services support the users in the identification and location of authorized message recipients together with any restrictions placed on either users or recipients.

k. Preparation Support. The UA/OUA will provide the prompting and message formatting necessary for the user to easily prepare a message in the ACP XXX format with no special training. This function will be fully integrated into the office automation environment which will have appropriate message preparation capabilities. Throughout the DMS, standardized screens and menus will be employed, enabling easy portability of DMS messaging skills from one organization to another.

l. Storage and Retrieval Support. The requirements for message storage, specified by ACP XXX, will be met. The UA can use the X.400 Message Store (MS) functionality to provide a message storage capability for messages prior to delivery. For organizational messages, the storage capability is part of the OUA functionality. Messages can be stored on-line for a limited time period (e.g., 30 days) to allow for timely retrieval by the users at their PCs or workstations, and off-line storage may be much longer. Additional storage outside the DMS can be implemented locally to meet requirements for extended periods of storage. DMS compliant products can also provide message analysis and editing capabilities at the user's workstation.

m. Distribution Determination and Delivery. This function, which applies primarily to organizational messages, will be an automated capability of the OUA accomplished in accordance with the organization's policy. Distribution profiles reflecting the organization's distribution policy will be implemented at the OUA and maintained by the local organization. Message distribution will normally be accomplished electronically by sending

organizational messages from the OUA to the organization's subordinate OUAs and/or individual messages to the individual's UAs. Abnormal conditions (high precedence, high classification, OUA/UAs inoperable) will be handled by the submitting organizational element through alternate delivery, or handled by a receiving OUA through review and delivery by other means in accordance with applicable policy. For example, in the case of an urgent message, if delivery cannot be effected within a specified time period, this will result in a non-delivery notification and cause the message to be hand-delivered to the staff duty officer for action in accordance with local policy. The DMS security services can provide proof of delivery to the originator, provided both the originator and receiver subscribe to this service feature.

Appendix D

Acronyms

Acronym	Title
AC	Access Control
ACC	Access Control Center (for BLACKER)
ACP	Allied Communication Publication
ADI	AUTODIN-DDN Interface
ADP	Automatic Data Processing
AFAMPE	Air Force Automated Message Processing Exchange
AFCAC-251	Air Force Computer Acquisition Center Standard Multiuser Small Computer Requirements Contract
AID	AUTODIN Interface Device
AID-SS	AUTODIN Interface Device with Selective Splitting
AIG	Address Indicator Group
AIHS	Automated Information Handling System
AMF	Abbreviated Message Format
AMHS	Automated Message Handling System
AMIH	AUTODIN Mail Interface Host
AMME	Automated Multi-Media Exchange
AMPE	Automated Message Processing Exchange
AMS	AUTODIN Mail Server
ARPANET	Advanced Research Projects Agency Network
ASC	AUTODIN Switching Center
ASCII	American Standard Code for Information Interchange
AU	Access Unit (X.400)
AUTODIN	Automatic Digital Network
AWG	Architecture Working Group
BAWG	Baseline Assessment Working Group
BFE	BLACKER Front End
BIDS	Base Information Distribution System
BITS	Base level Information Transfer System
C3I	Command, Control, Communications and Intelligence
CAD	Collective Address Designator
CCEB	Combined Communications Electronic Board
CCEP	Commercial COMSEC Endorsement Program
CCITT	International Telegraph and Telephone Consultative Committee
CMF	Common Message Format
CMW	Compartmented Workstation
COMSEC	Communications Security
COTS	Commercial Off-the-Shelf

CP	Cryptographic Peripheral
CPU	Central Processing Unit
CPWG	Central Projects Working Group
CSIF	Communications Services Industrial Fund
CSP	Communications Support Processor
CSRF	Common Source Routing Files
CU	Cryptographic Unit
DAA	Designated Approving Authority
DAAS	Defense Automatic Addressing System
DAB	Defense Acquisition Board
DARPA	Defense Advanced Research Projects Agency
DCA	Defense Communications Agency
DCS	Defense Communications System
DCT	Digital Communications Terminal
DDN	Defense Data Network
DIA	Defense Intelligence Agency
DIB	Directory Information Base (X.500)
DINAH	Desktop Interface to AUTODIN Host
DIR	Directory
DIS	Defense Information System
DISNET	Defense Integrated Secure Network
DL	Distribution List
DLA	Defense Logistics Agency
DMS	Defense Message System
DMSIG	Defense Message System Implementation Group
DMSWG	Defense Message System Working Group (Now DMSIG)
DoD	Department of Defense
DPI	Data Processing Installation
DSA	Directory System Agent (X.500)
DSSCS	Defense Special Security Communications System
DSTE	Digital Subscriber Terminal Equipment
DT&E	Development Test and Analysis
DTG	Date Time Group
DUA	Directory User Agent (X.500)
E3	End-to-End Encryption
EDI	Electronic Data Interchange
E-Mail	Electronic Mail
FMHS	Formal Message Handling Service
FMS	Formal Message Service / Formal Message Server
FRCT	Fixed Record Communications Terminal (USAF)
FTP	File Transfer Protocol
GENSER	General Service
GOSIP	Government Open Systems Interconnection Profile
GW	Gateway
HAMPS	Host AUTODIN Message Processing System (USAF)

HARPS	Hybrid AUTODIN Red Patch Service
HDLC	High-Level Data Link Control
IAS	Integrated AUTODIN System
ICA	Integrated Communications Architecture
ID	Identifier/Identification
IDCS	Integrated Defence Communications System
IITS	Installation Information Transfer System
IEEE	Institute for Electrical and Electronic Engineers
INFOSEC	Information Security
I/O	Input/Output
IP	Internet Protocol
IPM	Interpersonel Message(X.400)
ISDN	Integrated Services Digital Network
I-S/A AMPE	Inter-Service/Agency Automated Message Processing Exchange
ISO	International Standards Organization
ITU	Information Transfer Utility
JANAP	Joint Army, Navy, Air Force Publication
JPWG	Joint Projects Working Group
JS	Joint Staff
JDL	Joint Development Laboratory
JINTACCS	Joint Interoperability of Tactical C2 Systems
JITC	Joint Interoperable Test Center (DCA)
KDC	Key Distribution Center (for BLACKER)
KMGMT	Key Management
KMS	Key Management Service
LAN	Local Area Network
LDMX	Local Digital Message Exchange
LEAD	Low-cost Encryption and Authentication Device
LMD	Lead Military Department
MAC	Message Authentication Code
MAD	Message Address Directory
MAN	Metropolitan Area Network
MART	Modular AMME Remote Terminal
MBI	Mail Box Interface
MCEB	Military Communications Electronics Board
MCS	Message Conversion System
MEPS	Message Entry and Preparation Software
MGMT	Management
MHS	Message Handling System (X.400)
MILNET	Military Network
MLS	Multi-level Secure
MOP	Memorandum of Policy (JCS)
MPDT	Message Preparation and Dissemination Terminal
MROC	Multicommand Required Operational Capability

MS	Message Store (X.400)
MSP	Message Security Protocol (SDNS)
MTA	Message Transfer Agent (X.400)
MTS	Message Transfer System (X.400)
NAMRADS	Naval Automated Message Reproduction and Delivery System
NBS	National Bureau of Standards (now NIST)
NDI	Non-Developmental Item
NIC	Network Information Center
NIST	National Institute for Standards and Technology (formerly NBS)
NMGMT	Network Management
NSA	National Security Agency
OAS	Office Automation System
OASD	Office of the Assistant Secretary of Defense
OCR	Optical Character Reader/Recognition
O&M	Operation and Maintenance
OJCS	Office of Joint Chiefs of Staff
O/R	Originator/Recipient (X.400)
OSD	Office of Secretary of Defense
OSI	Open Systems Interconnection
OSRI	Originating Station Routing Indicator
OSSN	Originating Station Serial Number
OTA	Operational Test Agency
OTC	Over-the-Counter
OT&E	Operational Test and Evaluation
OUA	Organizational User Agent
PC	Personal Computer
PCMT	Personal Computer Message Terminal (Navy)
PLA	Plain Language Address
POSIX	Portable Operating System Interface (UNIX)
PSN	Packet Switching Node
R&D	Research and Development
RFI	Request for Information
RI	Routing Indicator
RIXT	Remote Information Exchange Terminal
SARAH	Standard Automated Remote to AUTODIN Host
S/A	Service/agency
SBLC	Standard Base Level Computer (previously Phase IV) (USAF)
SC4	Standard Command, Control, Communications and Computers
SCI	Sensitive Compartmented Information
SCINET	Sensitive Compartmented Information Network
SDNS	Secure Data Network System

SMTP	Simple Mail Transfer Protocol
SPWG	Security Policy Working Group (DMSIG)
SRT	Standard Remote Terminal
ST&E	Security Test and Evaluation
TAC	Terminal Access Controller
TAIS	Target Architecture and Implementation Strategy
TCB	Trusted Computing Base
TCC	Telecommunications Center
TCP	Transmission Control Protocol
TEMP	Test and Evaluation Master Plan
TOUA	Trusted Organizational User Agent
TPWG	Test Planning Working Group
T&E	Test and Evaluation
TTY	Teletypewriter
UA	User Agent (X.400)
UC	User Component
USMCEB	United States Military Communications Electronics Board
VDT	Video Display Terminal
WINCS	WWMCCS (Worldwide Military Command and Control System) Information Network Communications System
WP	Wordprocessing
WS	Workstation
X.400	CCITT series of recommendations on electronic message handling system architecture and standards
X.500	CCITT series of recommendations on directory services architecture and standards

Appendix E

DMS Glossary

Access Control: The prevention of unauthorized use of a resource, incuding the prevention of use of a resource in an unauthorized manner (Definition source - DMS SPWG).

Accreditation: A formal declaration by the DAA that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards. It is the official management authorization for operation of an AIS and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security (Definition source - DMS SPWG).

Application layer: See Layer 7 definition.

Authentication: Verifies the identity of a communicating peer entity and the source of data. Example: Owners of bank accounts require assurance that money will only be withdrawn by the owner. (Definition source - SDNS).

Automated Information System (AIS): An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store and/or control data or information (Definition source - DoDD 5200.28)

Availability: The property of being accessible and usable upon demand by an authorized entity (Definition source - DMS SPWG).

Ada: Name of DoD high order programming language described in ANSI/MIL-STD 1815A.

AFCAC 251: Air Force Computer Acquisition Center (AFCAC) commodity buy personal computer contract. The AFCAC-251 Project is also known as the Standard Multiuser Small Computer Requirements Contract (SMSCRC).

Beta Testing: The measurement of the favorable and unfavorable impacts to users in a baseline environment that results from the addition of a new component to that environment. Users of the planned component actively participate in the Beta test and provide feedback on operational and technical issues. Feedback may be incorporated as changes to a future Beta version based on feasibility and need for such change. Beta testing results are

ultimately considered in deployment decisions.

BLACKER: A host-to-host protection (encryption) system used in conjunction with a set of PSNs to provide the basis for the DISNET. The components of the BLACKER are the BLACKER Front End (BFE), the Access Control Center (ACC), and the Key Distribution Center (KDC).

Body: The body of the message is the information the user wishes to communicate. In general, a body may consist of a number of different encoded information types such as voice, text, facsimile and graphics (Definition source - X.400 draft).

Bridge: A relatively simple and inexpensive device that passes data from one LAN segment to another without examining or altering the data. The bridged LAN segments must use the same protocol. (Definition source - Datapro Research).

Central Project: DMS policies; common procedures, formats and protocols; and centrally provided components which support all DMS users.

Certification: The formal technical evaluation of an AIS's security features and other safeguards, made in support of the accreditation process, which establishes the extent that a particular AIS design and implementation meet a set of specified security requirements (Definition source - DMS SPWG).

Commodity Buy: Large volume contract to provide hardware to a wide variety of users many of whom were not identified at the time of contract award.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes (Definition source - DMS SPWG).

Content: The piece of information that the originating UA wishes delivered to one or more recipient UAs. For IPM UAs, the content consists of either an interpersonal message or an IPM status report (Definition source - X.400, 1988).

Data Confidentiality: Protects data against unauthorized disclosure. Protecting the details of an attempted corporate takeover is an example of the need for confidentiality. (Definition source - SDNS).

Data Integrity: Protects against unauthorized modification, insertion and deletion. Example: Electronic funds transfer between banks requires protection against modification of the information. (Definition source - SDNS).

Datalink layer: See Layer 2 definition.

Defense Data Network (DDN): The set of DoD packet switching networks including the classified DDN (DSNET 1, DSNET 2 and DSNET 3) and the unclassified DDN (MILNET).

Defense Information System (DIS): The DIS reflects the merging of the telecommunications and computer industries over the past two decades. It consists of utilities which provide information transfer and information processing services that support the missions and functions of DoD elements such as the Military Services, Defense Agencies, the Joint Staff and the CINCs. (Definition Source - Defense Communications Agency Strategic Corporate Plan, 1989)

Defense Message System (DMS): The DMS consists of all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically between organizations and individuals in the Department of Defense. The DMS relies upon but does not include the DoD Internet.

Delivery: A transmittal step in which an MTA conveys a message or report to the MS or UA of a potential recipient of the message or of the originator of the report's subject message or probe. (Definition source - X.400, 1988).

Delivery Report: A report that acknowledges delivery, non-delivery, export, or affirmation of the subject message or probe, or distribution list expansion (Definition source - X.400, 1988).

Designated Approving Authority (DAA): The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA must be at an operational level, have authority to evaluate the overall mission requirements of the AIS and to provide definitive directions to AIS developers or owners relative to the risk in security posture of the AIS (Definition source - DoDD 5200.28).

Direct User: A user that engages in message handling by direct use of the MTS, i.e., via a UA, OUA (Definition source - X.400, 1988).

Directory: A collection of open systems cooperating to provide directory services (Definition source - X.400, 1988).

Directory Name: A Directory name is one component of an O/R name. It is the name of an entry in a directory. In the context of message handling, the entry in the directory will enable the

O/R address to be retrieved for submission of a message (Definition source - X.400, 1988).

Directory Services: All services are provided by the Directory in response to requests from DUAs. There are requests which allow interrogation of the Directory and those for modification. Requests for service can be qualified through a number of controls provided on, among other things: the amount of time, the size of results, the scope of search, the interaction modes, and on the priority of the request. Each request may be accompanied by information in support of security mechanisms for protecting the Directory information (Definition source - X.500, 1988).

Directory System Agent (DSA): An OSI application process which is part of the Directory, and whose role is to provide access to the directory information base to DUAs and/or other DSAs. A DSA may use information stored in its local database or interact with other DSAs to carry out requests. Alternatively, the DSA may direct a requestor to another DSA which can help carry out the request (Definition source- X.500, 1988).

Directory User Agent (DUA): An OSI application process which represents a user in accessing the Directory. Each DUA serves a single user so that the directory can control access to directory information on the basis of the DUA names. DUAs can also provide a range of local facilities to assist users to compose requests (queries) and interpret responses (Definition source - X.400, 1988).

DoD Internet: The long-haul data switching backbone networks (currently the DDN) and local post/camp/station electronic telecommunications distribution facilities/networks (LANs, IITS, BITS).

Envelope: In the context of message handling, an information object, part of a message, who composition varies from one transmittal step to another and that variously identifies the message originator and potential recipients, documents its past and directs its subsequent conveyance by the MTS, and characterizes its content (Definition source - X.400, 1988).

Facility: A DMS facility is an organizationally defined set of personnel, hardware, software, and physical environment, a function of which is to provide DoD messag handling service (Definition source - DMS SPWG).

Gateway: A protocol converter that restructures packets of information so they can pass between networks using different standards, e.g., between X.400 and SMTP networks. Gateways perform appropriate protocol and format conversion at all or most

of the layers of the network architecture to interconnect heterogeneous networks at the application layer.

Heading: Component of an interpersonal message. Other components are the envelope and the body (Definition source - X.400, 1988).

Individual Message: This type of message includes routine communications between individual DoD personnel within administrative channels, both internal and external to the individual organizational element. Informational messages and those requiring only a basic transport service (the electronic analogue of the telephone call) will be treated as a part of this class. The driving requirements on the communications system for this class of messages are those of far-reaching, fine grained connectivity and ease of use. (Definition Source - DMS MROC 3-88).

Information Transfer Utility (ITU): The long haul and base level telecommunication services of the DIS available to the DMS within Phase 3. The ITU is a result of the evolution of base and installation level information transfer systems and the long haul DCS (DDN and MILNET) to an ISDN-based, common-user information transfer capability. (Definition Source - DMS AWG)

Integrity: The property that a message or other data has not been altered or destroyed in an unauthorized manner (Definition source - DMS SPWG).

Interpersonal Message (IPM): The content of a message in the IPM service (Definition source - X.400,1988).

Interpersonal Messaging Service (IPM Service): Messaging service between users by means of message handling, based on the message transfer service (MTS) (Definition source - X.400, 1988).

Joint Project: DMS components which support activities at the base or local level and are intended for use by multiple services and agencies.

Layer 1: Layer 1 of the OSI Reference Model is called the physical layer and includes the functions required to activate, maintain, and deactivate the physical connection in a transmission circuit. It defines both the functional and procedural characteristics of the interface to the physical circuit (Definition source - Committee for Open Systems).

Layer 2: This is the Datalink layer of the OSI Reference Moed and covers the mechanism for synchronizing and error control of the information transmitted over the physical link, regardless of what that information represents. It includes error checking,

acknowledgment at the receive end, and control of the data flow into and out of the nodes on a particular link (Definition source - Committee for Open Systems).

Layer 3: This is the network layer of the OSI Reference Model. It provides the necessary switching and routing functions required to establish, maintain, and terminate any switched connections between the transmitting and receiving locations. It specifies the interface into a packet switched network and includes disassembly, reassembly, and error correction for the various segments of the network (Definition source - Committee for Open Systems).

Layer 4: This is the transport layer of the OSI Reference Model. It provides an end-to-end control for information interchange at the reliability and quality level required for the upper three layers (5-7). Layer 4 includes such functions as multiplexing and segmenting data into appropriate sized units for handling by the network layer, and provides a level of isolation designed to keep the user independent of the physical and operational functions of the network itself (Definition source - Committee for Open Systems).

Layer 5: This is the session layer of the OSI Reference Model. It provides the necessary interface to support the dialog between two separate applications. The functions that can be performedat thislevel are typically settingup synchronization points for intermediate checking and recovery of file transfers, providing abort and restarts, and priority data flows (Definition source - Committee for Open Systems).

Layer 6: This is the presentation layer of the OSI Reference Model. It insures that information is delivered in a form that the receiving system can understand and use, in other workds, the syntax or the physical representation of the data. This layer is not concerned with the meaning of the information, only to present it in a form that will be recognizable by the application layer, layer 7 (Definition source - Committee for Open Systems).

Layer 7: This is the application layer of the OSI Reference Model. It is concerned with the support of the end user's application. At this level the meaning of the information is important and its function is to support distributed applications as well as to manipulate information. This means it can provide file transfers, virtual filesand terminals, distributed processing, and other functions. The DMS OUA, UA, DUA and DSA functions are applications implemented at layer 7 (Definition source - Committee for Open Systems).

Mailbox: A computer file, queue or equivalent delivery point

which can be accessed by the host's E-Mail delivery process and by the user for reading the mail. In many ways, mailboxes are analogous to US Postal Service mailboxes.

Mailbox Host: Computer system that supports E-Mail and has storage for messages.

Message Handling System (MHS): The collection of interconnected UAs, MSs, AUs and MTAs that convey nessages from one user to another. The MHS is designed in accordance with the principles of the reference model of open systems interconnection for CCITT applications (Recommendation X.200) and uses the presentation layer (layer 6) services offered by other, more general, application service elements. (Definition source - X.400, 1988).

Message Handling Environment (MHE): The sum of all components of message handling systems, i.e., the collection of UA, MSs, AUs, and MTAs (Definition source - X.400, 1988).

Message Store (MS): A component of the MHS that provides a single direct user with capabilities for message storage (Definition source - X.400, 1988)

Message Transfer Agent (MTA): MTAs transfer messages and deliver them to the indended recipients (Definition source - X.400, 1988).

Message Transfer System (MTS): The MTS consists of one or more MTAs which provides store-and-forward message transfer between user agents, message stores and access units (Definition source - X.400, 1988).

Multilevel Security (MLS): A mode of operation which allows two or more classification levels of information to be processed simultaneously within the same system when not all users have a clearance or formal access approval for all data handled by the AIS (Definition source - DoDD 5200.28)

Network layer: See Layer 3 definition.

Non-repudiation: Non-repudiation with proof of origin provides to the recipient proof of the origin of data and protects against any attempt by the originator to falsely deny sending the data or its contents. For example, non-repudiation with proof of origin can be used to prove to a judge that a person signed a contract. (Definition source - SDNS).

Offnet Connection (OFC): A function addressing the DMS Allied, tactical and commercial refile interfaces (Definition source - DMSWG).

Open Systems Interconnect (OSI): A classification of standards for promoting global connectivity. OSI standards are generally promulgated by the International Standards Organization and used by a variety of standards-setting bodies (Definition source - Datapro Research)

Originator/Recipient (O/R) Address: An attibute list that distinguishes one user or DL from another and identifies the user's point of access to MHS or the distribution list's expansion point (Definition source - X.400, 1988).

Originatior/Recipient (O/R) Name: An identifier by means of which a user can be designated as the originator; or a user or DL designated as a potential recipient of a message or probe. An O/R name distinguishes one user or DL from another. AN O/R name comprises a Directory name, an O/R address, or both. Each user or DL will have one or more O/R name(s) (Definition source - X.400, 1988).

Organizational Message: This type of message includes command and control traffic and messages exchanged between organizational elements. These messages require release by the sending organization and distribution determination by the receiving organization. Due to their official and sometimes critical nature, such messages impose operational requirements on the communications systems for such capabilities as non-routine precedence, guaranteed timely delivery, high availability and reliability, and a specified level of survivability (Definition Source - DMS MROC 3-88).

Originator: A user, a person or a component of the message handling environment but not a DL, that is the ultimate source of the message or probe (Definition source - X.400, 1988).

OSI Reference Model: The Open Systems Interconnect model is a specification describing seven different protocol layers of interface by the International Standards Organization (ISO). With all the different vendors providing all kinds of different products it is very hard for any end user to connect products and/or services that are provided by different vendors. The aim of the OSI model is to provide a standardized set of parameters which, if followed by different vendors, would provide a methodology for communicating at all levels in the user's environment (Definition source - Committee for Open Systems).

Physical layer: See Layer 1 definition.

Presentation layer: See Layer 6 definition.

Probe: A probe is a message consisting of just the envelope.

This envelope contains much the same information as that for a message. A probe is sent from one user to the MTAs of of other users in order to determine the deliverability of a message (Definition source - X.400, 1988).

Protocol: A collection of rules, voluntarily agreed upon by vendors and users, to ensure that the equipment transmitting and receiving data understand each other. In general, protocols comprise three major areas: the method in which data is represented or coded; the method in which codes are received; and the methods used to establish control, detect failures or errors, and initiate corrective action (Definition source - Datapro Research).

Rapid Prototyping: Method to accelerate the availability of a new system to field by configuring and testing components in a Beta Test site environment.

Recipient: A user (a person, DL, or component of the message handling environment) the originator specifies as a message's or probe's intended destinations (Definition source - X.400, 1988).

Repudiation: The denial by one of the entities involved in a communication of having participated in all or part of the communication (Definition source - DMS SPWG).

SARAH: Standard Automated Remote to AUTODIN Host. AF developed software for personal computers to prepare and transmit DD173 and JANAP 128 formatted messages via AUTODIN.

Security Architecture: A description of the security services the DMS offers and how the services are implemented and ensured (Definition source - DMS SPWG).

Session layer: See Layer 5 definition.

SP 3: The SDNS lower layer security protocol(SP) residing in OSI layer 3, the network layer, which provides four major security services: connectionless confidentiality, integrity, identification/authentication andaccess control. Itis theonly layer in the SDNS architecture which provides for encipherment at gateways to support "red" networks (Definition source - DMS AWG).

SP 4: The SDNS lower layer security protocol (SP) residing in OSI layer 4, the transport layer. It can provide either connectionless or connection oriented confidentiality and integrity. Peer entity authentication and access control are also provided (Definition source - DMS AWG).

Traffic Flow Confidentiality: A special type of data

confidentiality; it protects the identities of the communicating parties and the amount of communication between them. Example: A marked increase in the communications between two companies could be an indication of a merger or joint product development project. (Definition source - SDNS).

Transport layer: See Layer 4 definition.

Trusted System: A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information (Definition source - DoD Standard 5200.28-STD).

Trusted Computing Base: The totality of protection mechanisms within a computer system, including hardware, firmware and software, the combination of which is responsible for enforcing a security policy (Definition source - DoD Standard 5200.28-STD).

User: A person or component of the message handling environment that engages in (rather than provides) message handling and that is a potential source or destination for messages. A user is referred to as either an originator (when sending a message) or a recipient (when receiving one) (Definition source - X.400,1988).

User Agent (UA): A component of the MHS through which a single direct user engages in message handling. The UA assists users in the preparation, storage, and display of messages (Definition source - X.400, 1988).

User Unique DMS Project: DMS components which support a single Service or agency or portion thereof.

X.200: Reference model of open systems interconnection for CCITT applications.

X.400: This refers to the CCITT set of Recommendations (X.400, X.402, X.403, X.407, X.408, X.411, X.413, X.419, and X.420) for message handling. This set provides a comprehensive blueprint for a message handling system realized by any number of cooperating open systems. Of special interest is recommendation X.400, "Message handling system and service overview" and X.402, "Message handling systems: Overall architecture".

X.500: This refers to the CCITT set of Recommendations which define the capabilities, structure and components of the Directory.

Appendix F

DMS References

F.0 Introduction.

This section identifies the documents and standards directly applicable to the Defense Message System.

F.1 DMS Specific Documents.

USD(A) Memorandum, Program Guidance on the Defense Message System (DMS), 3 August 1988

MJCS-20-89, Multicommand Required Operational Capability for the Defense Message System MROC 3-88, 6 February 1989

ASD(C3I) Memorandum, Interim Policy for Transition to the Defense Message System (DMS) Target Architecture, 2 November 1989

Charter, Defense Message System (DMS) Panel, Approved 22 August 1988.

Charter, Defense Message System (DMS) Implementation Group (DMSIG), Approved 22 August 1988.

Defense Message System Inplementation Group, The Defense Message System (DMS) Target Architecture and Implementation Strategy (TAIS), December 1988

F.2 DMS Pertinent Standards.

CCITT Recommendations X.400-X.420, Data Communication Networks, Message Handling Systems, IXth Plenary Assembly, Melbourne, 14-25 November 1988

CCITT Unofficial "Final" version of Recommendations X.500-X.521, The Directory, December 1988

FIPS Pub 146, Government Open Systems Interconnection Profile (GOSIP)

FIPS Pub 151, POSIX: Portable Operating System Interfacr for Computer Environments

DoD Standard 5200.28-STD, Trusted Computer System Evaluation Criteria, December 1985

F.3 Reference Documents.

DoD Directive 5200.28, Security Requirements for Automatic Information Systems (AISs), 21 March 1988

Appendix G

Distribution

G.0 Introduction.

This appendix describes the distribution mechanism used for the DMS Target Architecture and Implementation Strategy. The TAIS is authorized for unlimited distribution throughout Government and Industry, and generally available through the Defense Technical Information Center (DTIC) and the National Technical Information System (NTIS). The instructions for obtaining the TAIS from these sources is explained in paragraph G.1. Large Department of Defense organizations, e.g. the Services, receive photo-ready copies of the TAIS for further reproduction and distribution as needed. These organizations are listed in paragraph G.2. Other DoD Distribution (direct distribution of copies) is listed in paragraph G.3. These direct addressees receive either a low copy count or they are directly involved in the management of the DMS Program and therefore need copies as soon as possible. Addressees not covered in the preceding paragraphs are listed in paragraph G.4, which primarily lists non-DoD organizations currently authorized to use the DMS for organizational messaging.

G.1 Central Availability.

The DMS TAIS, subsequent revisions, and all future DMS documents will be provided to the Defense Technical Information Center (DTIC), Alexandria, Virginia. DTIC provides access to and transfer of scientific and technical information for registered DoD personnel, DoD contractors and potential contractors, and other U.S. Government agency personnel and their contractors. All DTIC account holders can obtain DMS documents upon request. For organizations not registered for DTIC services, unclassified/unlimited technical reports and bibliographic information, to include DMS documents, are released through the National Technical Information Service (NTIS). DTIC documents released through the NTIS are indexed in NTIS's Government Reports Announcements and Index, and are available online through the NTIS Bibliographic Data File. This file can be accessed through commercial database vendors. The Commerce Business Daily (CBD) will announce the availability of future revisions of the TAIS. For further information concerning access to DTIC or NTIS, for DMS documents, direct inquiries to:

DTIC

Defense Technical Information Center
ATTN: Registration and Services Section (DTIC-FDRB), Bldg. 5
Cameron Station, Alexandria, Virginia 22304-6145
(202) 274-6434/AUTOVON 284-6434

NTIS

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
(703) 487-4650

G.2 Photo-Ready Copies to DoD Distribution.

The following addresses receive photo-ready copies of the TAIS for reproduction and distribution to elements of their Service or agency. Organizations within these S/a should contact the address listed below for copies of the TAIS.

Distribution	Copies
ARMY	
Commander U.S. Army Information Systems Command Attn: ASPL-PS (Mr. Hersey) Fort Huachuca AZ 85613-5000 A/V 878-0850	1
NAVY	
Naval Telecommunications Automation Support Center C/O NAVCOMMUNIT Washington Attn: Code 44 (Mr. Atkinson) Washington DC 20397-5310 A/V 251-2176	1
AIR FORCE	
Headquarters Computer Systems Division Attn: AEF-D (Ms. Gove) Gunter AFB AL 36114-6343 A/V 446-3207/3510	1

DEFENSE COMMUNICATION AGENCY

Distribution	Copies
Director Defense Communications Agency ATTN: Code DISM (Mr. Clarke) Washington, D.C 20305-2000 A/V 356-3336	1

NATO CIS AGENCY

NATO CIS Agency Attn: J. Rex Reed APO New York, NY 09667-5381	1

G.3 Other Department of Defense Distribution.

The following addressees receive copies of the TAIS directly. These direct addressees receive either a low copy count or they are directly involved in the management of the DMS Program and therefore need copies as soon as possible.

Distribution	Copies
Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (Information Systems) The Pentagon, Room 3E187 Washington, DC 20301	5
Office of Joint Chiefs of Staff Attn: Code J6T Washington DC 20301	1

UNIFIED AND SPECIFIED COMMANDS

Commander-in-Chief U.S. Southern Command Attn: SCJ6-P APO Miami FL 34003-0226	1
Commander-in-Chief Strategic Air Command Attn: SC Offutt AFB NE 68113	1

Distribution	Copies
Commander-in-Chief Central Command Attn: CCJ-B MacDill AFB FL 33608	1
Commander-in-Chief Europe Attn: C3S-TSP APO NY 09131	1
Commander-in-Chief U.S. Special Operations Command Attn: SOJ6-I MacDill AFB FL 33608-6001	1
Commander-in-Chief Atlantic Attn: J62B Norfolk VA 23511-5100	1
Commander-in-Chief Pacific Attn: C3STM11 Camp Smith HI 96861-5025	1
Commander-in-Chief Aerospace Defense Command Attn: KRQR Peterson AFB CO 80914	1
Commander-in-Chief U.S. Forces Command Attn: FCJ6 Fort McPherson GA 30330-6000	1
Commander-in-Chief U.S. Transportation Command Attn: TCJ6 Scott AFB ILL 62225	1

ARMY

Distribution	Copies
Headquarters Department of the Army Attn: SAIS-PP Pentagon, 1D664 Washington DC 20310-0700	1
Program Manager Defense Communications and Army Switched Systems Attn: ASM-SW-B Fort Monmouth NJ 07703-5501	1
Commander USA Combined Arms Center Attn: ATZL-CAC-A Fort Leavenworth, KS 66027	2
Commander USASC&FG Attn: ATZH-CDM Fort Gordon, GA 30905	2
Director USAISC-Pentagon Room BD1028, The Pentagon ATTN: ASQNS-OS-PT Washington, DC 20310-3010	1

NAVY

Distribution	Copies
Chief of Naval Operations Attn: Director, Naval Communications Division (OP 941) Washington DC 20305-2000	1
Director Naval Telecommunications Automation Support Center c/o NAVCOMMUNIT Washington Attn: Code 44 Washington, DC 20397-5310	1
Commander Space and Naval Warfare Systems Command National Center I Attn: 110-2L, PDW 110-1425, PDW 120 Washington DC 20363-5100	3
Commander Naval Telecommunications Command Attn: N51 4401 Massachusetts Avenue, NW Washington DC 20390-5290	1
Naval Research Laboratory Attn: Code 5540 4555 Overlook Avenue, SW Washington, DC 20375-5000	1
Director Naval Telecommunications Systems Integration Center c/o NAVCOMMUNIT Attn: Code 05 Washington DC 20390-5340	1

AIR FORCE

Distribution	Copies
Headquarters Department of the Air Force Attn: SC Washington DC 20330-5190	1
Headquarters Department of the Air Force Attn: SCMM Washington DC 20330-5190	1
Headquarters Air Force Communications Command Attn: AI Scott AFB IL 62225-6001	1
Headquarters Air Force Communications Command Attn: DO Scott AFB IL 62225-6001	1

US MARINE CORPS

Distribution	Copies
Headquarters US Marine Corps ATTN: Code CMC(CC) Washington DC 20380-0001	1
Headquarters US Marine Corps ATTN: Code CCP-17 Washington DC 20380-0001	1
Headquarters US Marine Corps ATTN: Code CCT Washington DC 20380-0001	1

DEFENSE COMMUNICATIONS AGENCY

Distribution	Copies
Director Joint Tactical Command Control and Communications Agency Attn: Code C3A-DWS, C3A-MS, RORC, C3A-SEET Fort Monmouth NJ 07703-5513	4
Director Joint Tactical Command Control and Communications Agency Attn: C3A-ADW-S 11440 Issac Newton Square, North Reston, VA 22090-5006	2
Defense Communications Agency Attn: Code C4S/SMCA Washington DC 20305	2
Defense Communications Agency Attn: Code C4S/SCJE Washington DC 20305	1
Defense Communications Agency Attn: Code DISM Washington DC 20305-2000	6
Defense Communications Agency JDSSC Attn: Code C342 Washington DC 20305-2000	1
Defense Communications Agency European Area Attn: Code DES APO New York, NY 09131-4103	1
Defense Communications Agency Pacific Area Attn: Code Wheeler AFB, HI 96854-5000	1

Distribution	Copies
Defense Communications Engineering Center Attn: Code DRFF Fort Detrick MD 21701	1
Defense Communications Engineering Center Attn: Code DRFFE 1860 Wiehle Avenue Reston VA 22090-5500	1

NATIONAL SECURITY AGENCY

Distribution	Copies
Director National Security Agency Attn: Code T03 9800 Savage Road Fort George G. Meade MD 20755-6000	1
Director National Security Agency Attn: Code T137 9800 Savage Road Fort George G. Meade MD 20755-6000	1
Director National Security Agency Attn: Code T711 9800 Savage Road Fort George G. Meade MD 20755-6000	1
Director National Security Agency Attn: Code T744 9800 Savage Road Fort George G. Meade MD 20755-6000	1
Director National Security Agency Attn: Code V53 9800 Savage Road Fort George G. Meade MD 20755-6000	1
Director National Security Agency Attn: Code C207 9800 Savage Road Fort George G. Meade MD 20755-6000	1

DEFENSE INTELLIGENCE AGENCY

Distribution	Copies
Director Defense Intelligence Agency Attn: Codes DSE-2 3100 Clarendon Boulevard Washington, D. C. 22201-5324	2
Director Defense Intelligence Agency Attn: Code DSE-3 3100 Clarendon Boulevard Washington, D. C. 22201-5324	2

DEFENSE LOGISTICS AGENCY

Headquarters, Defense Logistics Agency Attn: DLA-A, DLA-ZW, DLA-W, DLA-T, DLA-ZP Cameron Station Alexandria VA 22304-6100	5
Defense Automatic Addressing System Office Attn: DAAS-VC S. Chrisman Rd Tracy CA 95376-5000	1
Defense Electronic Supply Center Attn: DESC-W 1507 Wilmington Pike Dayton OH 45444-5000	1
Defense Logistics Service Center Attn: DLSC-ZT Battle Creek MI 49016	1
Defense Automatic Addressing System Office Attn: DAAS-V 1507 Wilmington Pike Dayton OH 45444-5000	1
Defense Logistics Agency Systems Automation Center Attn: DSAC-R P.O. Box P1605 Columbus OH 43216	1

DEFENSE MAPPING AGENCY

Distribution	Copies
DMA Telecommunications Services Center ATTN: SRD 8613 Lee Highway Fairfax, VA 22031-2139	1

US MILITARY COMMUNICATIONS ELECTRONICS BOARD

HQ USMCEB Room 1B707 Washington, DC 20301-5000	7

* MCEB will distribute to CCEB members.

G.4 Other Distribution.

CENTRAL INTELLIGENCE AGENCY

Distribution	Copies
CIA Attn: Code SAN-L (Ms. Curwen) Washington, D.C. 20505	1
CIA Attn: Glen Albers Office of Communications Washington, D.C. 20505	1

ENVIRONMENTAL PROTECTION AGENCY

U.S. Environmental Protection Agency Attn: Telecommunications Manager Office of Administration and Resources Management Washington, D.C. 20460	1

FEDERAL EMERGENCY MANAGEMENT AGENCY

Federal Emergency Management Agency Attn: Darwin Smith Communications Center, Room 25 500 C Street SW Washington, DC 20472	1

U.S. DEPARTMENT OF COMMERCE

National Institute of Standards and Technology Institute for Computer Sciences and Technology Attn: K. Mills, TECH/B217 Gaithersburg, MD 20899	1

U.S. DEPARTMENT OF ENERGY

Department of Energy Mail Stop NA-251.3 Room GA-226 Attn: Curt Mackereth 1000 Independence Ave, SW Washington, DC 20585	1

U.S. DEPARTMENT OF STATE

Distribution	Copies
DOSTN Program Manager Department of State (SA-7) 7957 Cluny Court Springfield, VA 22153-1107	1
DOSTN Security Management Division Department of State 7197 Cluny Court Springfield, VA 22152	1

U.S. DEPARTMENT OF TRANSPORTATION

Chief, Telecommunications Systems Division (G-TTS) Attn: Captain Starkweather United States Coast Guard, Rm 6302 2100 2nd Street, S.W. Washington, DC 20593-0001	1

AMERICAN RED CROSS

American Red Cross Attn: Mr. Anderson/Mr. Gibb 18th and D Streets, NW Washington, DC 20006	1

MEDIA

Government Computer News Attn: Neil Munroe 1620 Elton Road Silver Springs, MD 20903	1