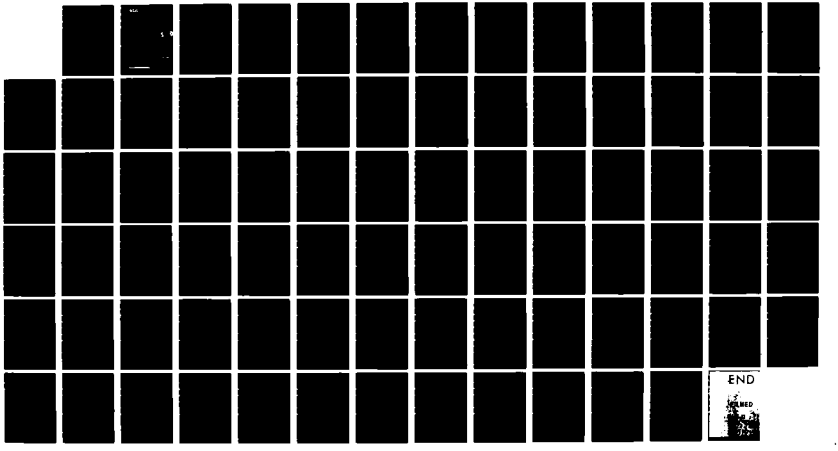
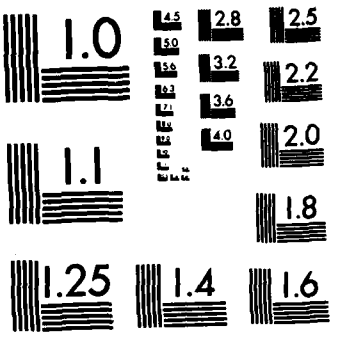
AD-A126 553 DOD MESSAGE PROTOCOL REPORT VOLUME II MESSAGE TRANSFER PROTOCOL REQUIREME..(U) SYSTEM DEVELOPMENT CORP SANTA MONICA CA C A ELDRIDGE 15 DEC 81 SDC-TM-7038/216/00 1/1

UNCLASSIFIED DCA100-80-C-0044 F/G 17/2 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

SDC
System Development Corporation
2500 Colorado Avenue, Santa Monica, CA 90406, Telephone (213) 820-4111

series base no./vol./reissue
TM- 7038/216/00

author
Charles A. Eldridge
technical
Douglas R. Price
release
Carl M. Switzky
for
Charles A. Savant

date
9/25/81

TM a working paper

This document was produced by
System Development Corporation in performance of Contract DCA100-80-C-0044

DCEC PROTOCOLS STANDARDIZATION PROGRAM

DoD MESSAGE PROTOCOL REPORT

VOLUME II

MESSAGE TRANSFER PROTOCOL REQUIREMENTS ANALYSIS

ABSTRACT

This document discusses requirements to be met by implementations of the DoD standard message transfer protocol. The protocol is indended to coordinate message transfer over networks. The requirements herein describe a minimum set of capabilities needed to allow application entities to exchange messages on a non-real-time basis. DoD objectives are reviewed in Section 1. Section 2 describes the architectural context; sections 3 and 4 describe requirements of the upper layer interface and of the protocol's processing capabilities. Section 5 discusses future requirements for extending message service capabilities. Appendices provide discussions of security, name service, and existing systems.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER 7038/216/00	2. GOVT ACCESSION NO. A126553	3. RECIPIENT'S CATALOG NUMBER
4. TITLE *(and Subtitle)* DoD Message Protocol Report Volume II Message Transfer Protocol Requirements Analysis		5. TYPE OF REPORT & PERIOD COVERED interim technical report 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Charles A. Eldridge		8. CONTRACT OR GRANT NUMBER(s) DCA100-80-C-0044
9. PERFORMING ORGANIZATION NAME AND ADDRESS System Development Corporation 2500 Colorado Ave. Santa Monica, CA 90406		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS P.E. 33126K Task 1053.558
11. CONTROLLING OFFICE NAME AND ADDRESS Defense Communications Engineering Center Switched Networks Engineering Directorate 1860 Wiehle Ave., Reston, VA 22090		12. REPORT DATE 25 Sep 81 13. NUMBER OF PAGES 45
14. MONITORING AGENCY NAME & ADDRESS*(if different from Controlling Office)* N/A		15. SECURITY CLASS. *(of this report)* Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A

16. DISTRIBUTION STATEMENT *(of this Report)*

Approved for Public release; distribution unlimited.

17. DISTRIBUTION STATEMENT *(of the abstract entered in Block 20, if different from Report)*

N/A

18. SUPPLEMENTARY NOTES

This document represents results of interim studies which are continuing at the DCEC of DCA.

19. KEY WORDS *(Continue on reverse side if necessary and identify by block number)*

Protocols, Data Communications, Data Networks, Protocol Standardization, Message Protocol

20. ABSTRACT *(Continue on reverse side if necessary and identify by block number)*

This document discusses requirements to be met by implementations of the DoD standard message transfer protocol. The protocol is intended to coordinate message transfer over networks. The requirements herein describe a minimum set of capabilities needed to allow application entities to exchange messages on a non-real-time basis. DoD objectives are reviewed in Section 1. Section 2 describes the architectural context; sections 3 and 4 describe requirements of the upper layer interface and of the protocol's processing capabilities. Section 5 discusses future requirements for extending message service capabilities.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE *(When Data Entered)*

ACKNOWLEDGEMENTS

Several members of the Department of Defense communications community have provided both access to literature and invaluable commentary complementing the available literature. The author would like to thank Mr. Don Clark, Dr. Clifford Guffee, Ms. Constance Heitmeyer, Dr. Casper DeFiore, and Mr. Mike Corrigan for their contributions.

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont'd)

TABLE OF CONTENTS (Cont'd)

LIST OF FIGURES

LIST OF TABLES

1. OVERVIEW

Transport of messages over digital communication systems is well established in military operations, but both hardware and software in military systems are undergoing extensive changes. As a consequence the services offered by military digital communication system are undergoing extensive redefinition. The DoD network architecture and data communication standard protocols will form the new definitions, furnishing a set of plans for communications services which will promote wide interoperability among DoD systems while meeting DoD communication service requirements for speed of service, reliability, survivability, and low probability of exploitation.

The computer and data communications industries have readily perceived the potential utility of computer-based message services, so that both production and developmental services have been fielded in such networks as Telenet, Tymnet and the Arpanet. However, these services meet civilian rather than military requirements. In addition to stressing the basic services which a message transfer protocol (MTP) must define, this document will attempt to make designers and specifiers of the military message transfer protocol sensitive to its particularly military requirements.

1.1 DEFINITIONS AND SCOPE

The MTP is intended to provide transfer service for narrative message traffic. A narrative message is one sent from one human to another, in a human readable form -- alphanumeric text. This clarification of the term message is included because in other message environments, such as AUTODIN I, messages may include data files and query/response traffic in addition to human-readable narrative ones. Future standards of the message protocol may encompass other message media such as graphics, facsimile, voice, code for processes, etc. In the interest of broad applicability and rapid achievability, the present requirements are limited to narrative messages.

The term transfer denotes the basic function of data communications -- to more information from one place to another. The movement does not necessarily remove information at the source, but it causes it to be registered at the receiver. In the case of the MTP, the unit of information to be moved is the narrative message.

A protocol defines the methods and rules by which the message transfer is accomplished. These rules and procedures depend upon how the information will be used by the receiver, and the pecularities of the communication media over which it is sent. The resulting protocol implementation will insulate users from these peculiarities.

The remainder of section 1 discusses the motivations for and significance of the MTP to military operations and concludes with goals to be addressed throughout the protocol design. Section 2 discusses the relationship between the MTP and the DoD data communications architecture. The DoD architecture defines a layered set of processes which cooperate to provide a total service. Therefore, Section 2 will discuss relations between the MTP and processes in adjacent layers. Section 3 discusses requirements of protocol in terms of specific services offered to upper-layer processes. Section 4 describes features which are transparent to the upper layer but are essential for implementing the required services. Section 5 describes services and features which are desirable but not absolutely required for initial provision of message transfer service. Appendix A discusses message transfer security issues; Appendix B discusses name service. Appendix C examines current computer-based message systems, including AUTODIN I-based systems and informal packet-switch network mail systems as found on the ARPANET and elsewhere. In particular the relationship of message header composition and services required is illustrated.

1.2 GENERAL MOTIVATIONS FOR AUTOMATED MESSAGE TRANSFER SERVICE

In any organization the communication of official messages (i.e. those relating to the function of the organization) is essential. Such communication gives the organization its strength and coordination. It also supports specification of functions so that individuals may concentrate effectively on limited tasks, while reporting to and receiving directions from others. For example, decision-making can be efficiently separated from taking action, removing interference each could have on the other.

The convenience, cost-effectiveness and speed of computer-based message systems are primary motivations for its use in organizations. There is convenience for the sender in not having to locate a difficult-to-reach receiver and establish direct contact. That is, it allows communication over disjoint time and space intervals. For the receiver there is the convenience of not being forced to listen to a long-winded or unwanted caller. Yet the speed of service can approach that of telephoning due to the high processing bandwidth of computer systems and communication media. Cost studies of computer message transfers show that it is competitive with either telephony or postal service. The computer-based message system can also provide an easily accessible record of the message to both the sender and the recipient.

Human error has played a significant part in the poor communications experienced in some military crises (see Section 1.3.3 below). These may have been caused in part by the pressure and stress generated by crises. Automated message exchange systems hold the promise of reducing these errors while providing the speed of service required for message communications during military crises.

1.3 MILITARY SIGNIFICANCE OF THE MESSAGE TRANSFER PROTOCOL

1.3.1 Command, Control, Communications and Intelligence (C^3I) Models

Planners within the US Department of Defense commonly use control system models to describe the way military objectives are met. Military decisions and planning are carried out in locations removed from the action centers and rely upon observations obtained from many action centers. These data are processed; decisions are made and then communicated to forces at the action centers. These commands are carried out by the forces, and their results are sensed and reported back to the Command Center. Actions resulting from other forces (enemy, natural forces, etc.) occur as well, and results are also reported to the Command Center. With the reporting of these data a cycle is completed, and the process can be iterated.

Timely, accurate, and non-exploitable communications are clearly necessary for Command Center objectives to be effectively met. If field reports are out-of-date or inaccurate, then the bases for decision-making are eroded, and decisions can be erroneous. Similarly if commands passed to forces are inaccurate or out-of-date, then the actions resulting can be useless or even harmful. If communications are absent altogether the forces may act in their separate fields, but there is no means to organize and coordinate to better meet an organized, coordinated enemy. If the communications are exploitable, enemy forces can gain both the advantage through anticipation of force actions and movements.

Another consequence of these models of military operations is the need for increasingly longer distance communications. This is due in part to ever-increasing speeds and ranges of weapons such as missiles and bombers. First the sensory and communication ranges need to be comparable to the range of friendly force actions; second they need to sense and report enemy weapons from further away. Long haul systems, such as satellites, are on hand to meet this need. However, interoperability is perhaps a more important

factor in meeting the challenges of coordination over long distances in response to high speed forces. Communication systems in different theatres which can interoperate provide definite advantages in global scale conflicts by allowing many different force units to talk to each other.

These C^3I principles apply as strongly to the flow of narrative message traffic as they do to the communications from many automated sensory, guidance and tracking systems. Narrative traffic supports a wide range of purposes with varying requirements for timeliness. Among these is the communication between command centers necessary for carrying out actions. The crises case histories described briefly below highlight the significance of timeliness and reliability in the communication of narrative messages.

1.3.2 Crisis Case Histories and C^3I

The capture of the Pueblo illustrated many problems with both communications and command/control procedures. First, the emergency messages sent from the Pueblo shortly before it was boarded required about one hour to reach the White House Situation Room. Inordinate delays were incurred in setting up secure voice links between command posts concerned with the incident. In addition, inter-service and Agency coordination was lacking, as various commands were uninformed as to the status and location of available forces and of the Pueblo itself.

Command, control and communications shortcomings were also central to the attack upon the Liberty by Israeli forces. The incident occurred only days after the ship had been assigned to the 6th fleet; the Liberty failed to receive a general fleet message to stand off from the area. The Liberty instead proceeded with its mission. However, the Joint Chiefs of Staff (JCS) perceived that the Liberty was out of position and in danger and issued orders to it to stand off. Unfortunately, delays and misroutes prevented messages carrying these orders from reaching the ship.

The lessons learned from such case histories are manifold, but here the emphasis has been on the consequences of unreliable message communications during crises. The mission loss potentials are real and very substantial, demonstrating the need for improvements to the communication equipment, procedures and processes. The message transfer protocol discussed in this document is intended to contribute to such improvement by providing a DoD-wide standard which directly supports the interoperability and further automation of narrative message handling systems.

1.3.3 Military Doctrine and Survivability

Military preparedness doctrine defines a spectrum of states of conflict, ranging from "day-to-day operations," "crises," "conventional (theatre) war," "theatre nuclear war," "strategic nuclear war," "reconstitution," "restrike," and "national recovery." These different stages pose different levels of stress on communication systems and pose different demands upon them as well. Most commercial systems are designed for day-to-day operations, for example; they are not severly stressed, and they provide for predictable traffic volumes. At the crisis level and above, communications systems may need to provide for unpredictable volumes of information over unpredictable routes. At the same time, they may be subject to attacks which bring down links and nodes or which interfere with or destroy other media. Survivability to these attacks and reconstitution after some evitable losses are essential attributes. Interoperability is again imperative, as survivors of attacks may need to make new connections with other survivors in subsequent reconstitution efforts.

1.4 GOALS OF THE MILITARY MESSAGE TRANSFER PROTOCOL

To serve military communication needs, the MTP must support DoD requirements for timeliness, accuracy, reliability, low probability of exploitation, interoperability and survivability. As a standard *per se* it can support the

last two of these; its design and implementation must support the remainder. Obviously all other elements of DoD message communications must also support these requirements. Issues of economics especially with respect to preservation of existing investments and smooth transitions between technologies, are important as well.

1.4.1 Functional Purpose

The MTP defines means of sending and receiving narrative messages over structured communication media. The structured communication media will be systems which supply standard digital data communication services, leaving users unconcerned with its details of operation. DoD's standard TCP is the archetypal structured medium, but interoperability and other special needs may require the use of other data transport services.

1.4.2 Support of Military C^3I Objectives

The protocol and the message communication-support provided by the protocol are intended to serve overall command control and communications in the military environment. First, as a standard DoD protocol, it supports the abilities of communicators in many different sectors to interoperate (and exchange information). This enhances the communication systems's survivability, it widens the connectivity and effectiveness range of the military reporting systems. Second, the protocol will be a means of organizing increasingly capable digital technology into a rapid, reliable system of message transfer. As a consequence the efficiency of day-to-day operations can also be increased.

1.4.3 Support of Investment Preservation and Smooth Transition

Even though digital communication-technology has undergone rapid advances in recent years, production-oriented systems, such as the Bell network and the military AUTODIN I, have not immediately incorporated all of the latest digital technology. This is due largely to their existing huge investments

in earlier technologies which still provide very capable service. In the military, the transition from present communications systems to advanced ones must preserve investments in training as well as facilities and hardware. The MTP must and can be designed to support several processing styles so that the AUTODIN I hardware phaseout need not impose overly severe impacts on communicators.

2. MESSAGE TRANSFER PROTOCOL ARCHITECTURAL CONTEXT

2.1 MESSAGE SERVICE AND TRANSFER PROTOCOL RELATIONSHIP

The message transfer protocol is an element within a layered set of communication services, ranging from the physical communication process to provision of services to end-users. The DoD [SYTEK81] and ISO/ANSI [ISO80] architectural models are examples of assignments of particular communication functions (e.g. link control, network routing, etc.) to specific layers. A central issue in defining message transfer protocol requirements is assigning which functions in the total message service should be assigned to which layers of the communication architecture.

The architecture described in this section is provisional and is provided for illustration purposes. In practice the assignment of required functions into layers of a standard architecture can require many iterations. One major reason for this is the fact that the functions in the upper layer are not yet well-defined. Therefore the architectural boundaries described in this section are not to be construed as implying particular requirements.

An overall message service architecture has been defined [BA79] for the Inter-Service AMPE environment: an upper-layer message service application provides capabilities for end-users, and it uses services of a message transfer protocol to send messages to other message-handling centers. The message transfer protocol in turn uses services provided a data transport protocol such as by the DoD standard TCP. A diagram of this suggested architecture is shown in Figure 2-1.

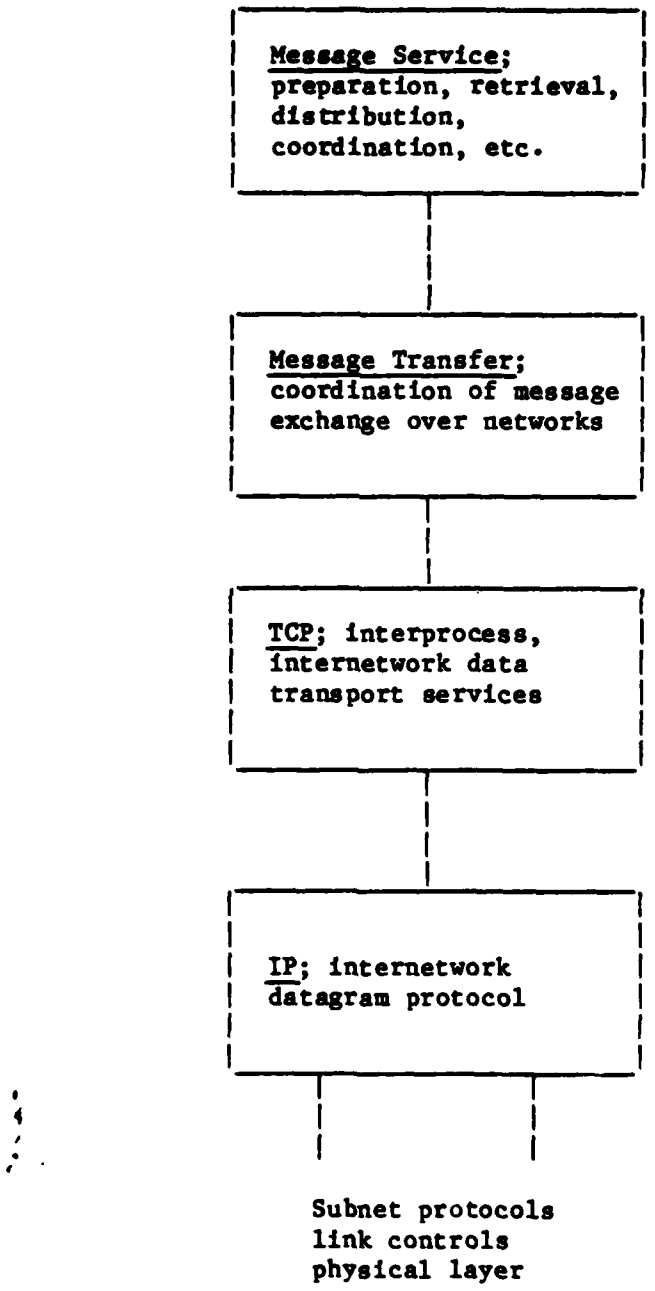


Figure 2-1. Suggested DoD Message Service Architecture

The message service in the application layer may also provide to users functions not directly involving message transport. These can include assistance in preparation and display, storage and retrieval of messages, provision of message summaries, provision of system management information, support of message draft coordination prior to formal release, etc.

The message service uses the services of the message transfer protocol to carry out user requests to send messages. The message transfer protocol uses the message's addressing information and other transmission instructions to establish an appropriate transport pathway to a peer message transfer protocol, and it transmits the message to the peer. The receiving peer uses the addressing information, transmission instructions or other information to deliver the message to one of possibly multiple message services. This scenario need not be limited to a single exchange between two peers; it could also involve forwarding or relaying.

In the requirements sections below, this division of functions is specifically preserved. Functions that do not involve necessary data transformations between network and local formats and that do not involve use of network data transport services belong outside of the message transfer protocol. Similarly, functions concerned with data transport other than connection management and use do not belong to the message transfer protocol.

This architecture serves several purposes. First it allows for diversity in message service offerings while providing uniform transport service; for example, message services with many resources and functions can communicate with those that have few. Second, it isolates message services from the data transport services providing needed modularity. Users need not

be concerned with the operation of internetwork data transport connections nor with the transport services of particular packet-switching networks. Finally, the architecture specifically allows extension of the services of basic data transport connections. For example, additional reliability features may be added, and message-specific presentation functions can be defined.

2.2 MTP CORRESPONDANCE WITH DOD's PRESENTATION LAYER

Under the DCEC Protocols contract, a standard protocol architecture is being produced. Its basis is the seven-layered model under development by ISO and ANSI, but needs specific to DoD are addressed as well. The document describing this model "DoD Standard Protocol Architecture Model (DRAFT)," describes the presentation layer [SYTEK80]:

> The primary model for presentation layer operation (at least implicitly) involves the concepts of 'transfer syntax' and 'local syntax'. In this model, a presentation-entity exchanges data with its local application-entity using a local syntax which they agree upon. For transfers between presentation-entities, data is represented in a transfer syntax which may or may not be different from the original local syntax. The receiving presentation-entity passes the data to its application-entity using a third syntax, local to that interface.

The above quote from the DoD architecture document describes the operation of message transfer when the following noun phrase substitutions are made:

"transfer syntax" becomes "network vertual message format;"
"local syntax" becomes "local message format" (e.g., JANAP 128);
"presentation-entity" becomes "message transfer entity;"
"data" becomes "message data;"
"application-entity" becomes "message service application entity."

2.3 LOWER-LAYER TRANSPORT PROTOCOL/SERVICE ASSUMPTIONS

An information channel is a fundamental requirement for an automated message transfer service. The DoD architecture addresses this need directly at the physical, link, sub-network, and inter-network levels. In other words, the architecture defines means of establishing communication channels based upon physical media but distributed over multiple digital processing centers. The transport and session layers of the DoD architecture address means of manipulating the information channel as a resource and of increasing its fidelity and reliability. Therefore, these needs are not addressed as message transfer protocol requirements.

A quality of service embodied in DoD's standard TCP is assumed to be available for communication between message transport protocol entities over packet-switched networks. TCP manages connections, provides full-duplex, error-free, guaranteed, ordered, flow controlled data transfer and reports errors to its users. TCP provides means of signaling to its upper-layer "users" that urgent data will follow, allowing processing to be expedited. (See "TCP Standard: Initial Version" [BERN81].)

The observations presented in Appendix C imply that end-to-end transport connections are not features of message-switching systems such as AUTODIN I. Data transport is provided only by link-control protocols, with message-transfer protocols running directly above. This differs fundamentally from the services which packet-switching technology can offer. Therefore, the concept of an end-to-end data transport protocol cannot be defined over all of the Integrated AUTODIN System (IAS). The conclusions presented in Section 2.1.5 imply that message transfers may be defined into and out of AUTODIN I and similar systems if some message transfer protocol entities has the capability to exchange properly prepared messages with ASC's via an appropriate interface protocol such as AUTODIN Mode I [DCA370]. (See also Section 5.1.3 below.)

2.4 MTP's NETWORK VIRTUAL MESSAGE FORMAT

A network virtual message format is the "transfer syntax" used between communicating message transfer protocol entities. As such, it can accomplish the following:

- Provide space for conveying transmission instructions and other administrative information.
- Avoid the "n x m" problem involved with transporting messages between local mail systems with differing formats.

Therefore, the MTP will define a standard message format. Postel [POST80] and NBS [NBS81] have specified standard message formats for use by interconnected networks. It is expected that the standard network format by which MTP modules exchange messages will be based upon one of these. To the end of developing such a format for use by the MTP, several requirements can be noted:

- The format must employ efficient yet flexible data structures so that economic upward compatibility is assured.
- The format must have a message construction scheme which facilitates rapid reliable parsing and error recovery.
- The sum of its fields must be capable of registering all information contained in a JANAP 128(H) and other currently used message formats, enabling one of these to be transformed to the network standard format for transmission and back again for delivery to the recipient.

- It must be capable of defining necessary message data types (e.g., ASCII characters, integer quantities etc.) and of providing content indicators for them.

Use of the virtual message format is not a requirement for interoperation with store-and-forward systems such as AUTODIN I. These systems use link-level protocols to transmit messages between switches. Switch software then processes messages, performing routing and other functions, based upon one of the "formal" message formats -- JANAP 128, DOI-103, ACP 127, ACP 126(M) , etc. The rendering of a message into a virtual message format would clearly be superfluous in this case.

2.5 CONCLUSIONS

The Message Transfer Protocol provides services which allow users' applications to exchange messages on the users' behalf. When the overall message service is fit to the DoD architectural model, the users' message service applications correspond to the "Application Layer," while the message transfer protocol encompasses the "Presentation Layer" and the "Session Layer." Figure 2-2 illustrates these architectural concepts.

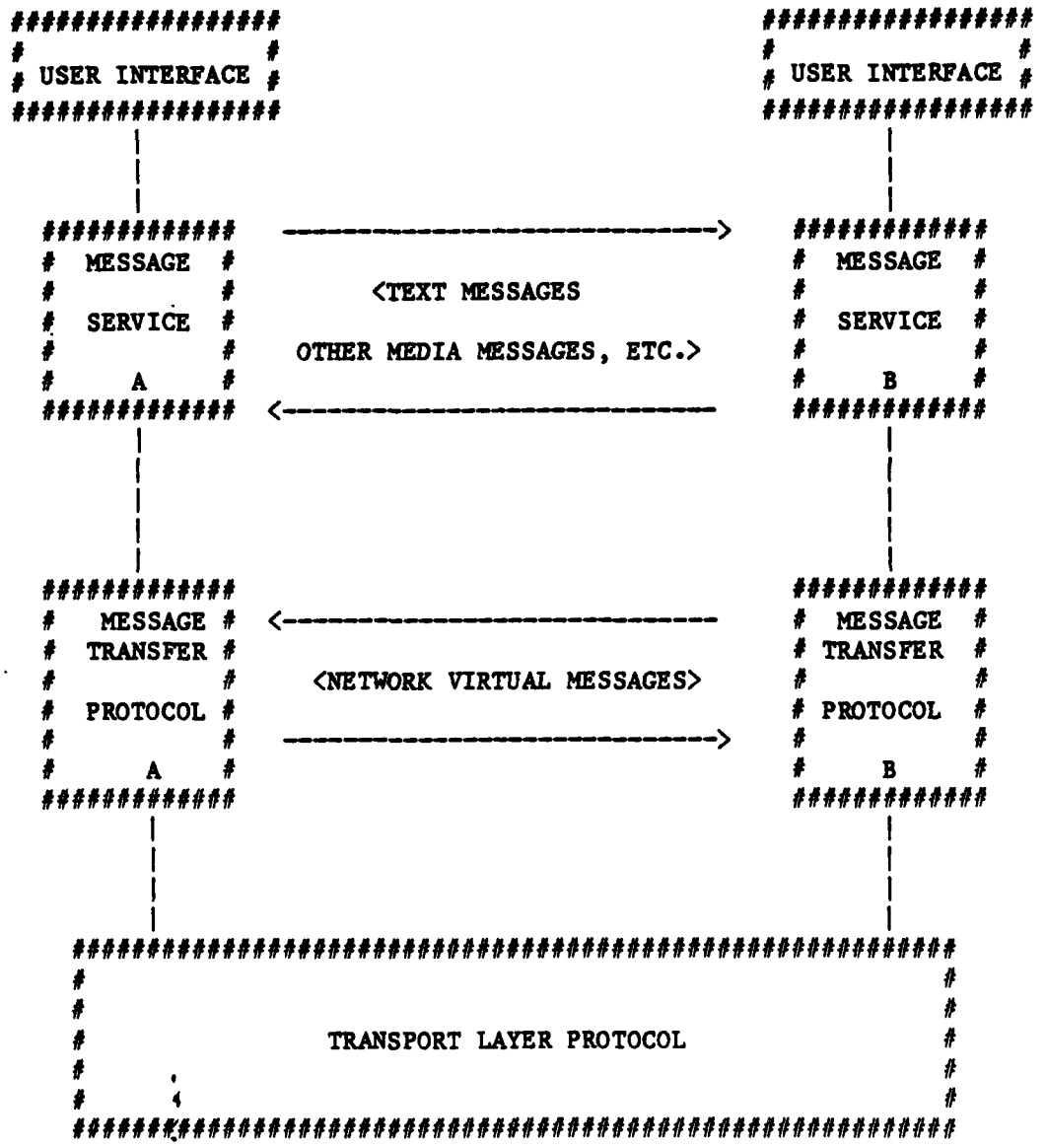


Figure 2-2. Message Service Architecture

3. REQUIRED PROTOCOL SERVICES

In a layered, modular computer communication environment, the exchange of messages involves communications between upper and lower layers at host sites and communications between peer levels at different host sites over media defined by the layer just below. Figure 3-1 depicts possible types of communications among the layers associated with the message transfer protocol, and it will be used to amplify descriptions of functional requirements which follow. Services represent primarily events which can take place at the interface with the upper-layer message service applications.

3.1 MESSAGE TRANSFER

3.1.1 Data Flow

The protocol must offer the capability to transfer messages from a sending message service application entity to one or more receiving message service application entities. The protocol carries out the send request based upon instructions supplied in the message header and upon the available communication pathways. Figure 3-1 suggests that such a transfer capability can be decomposed into several sub-functions:

1. Capability to receive the send instruction and the message from upper-layer message service application entity.

2. Capability to determine and effect transmission of the message to peer message transfer protocol.

3. Capability to deliver a message received from a peer to the recipient message service application entity.

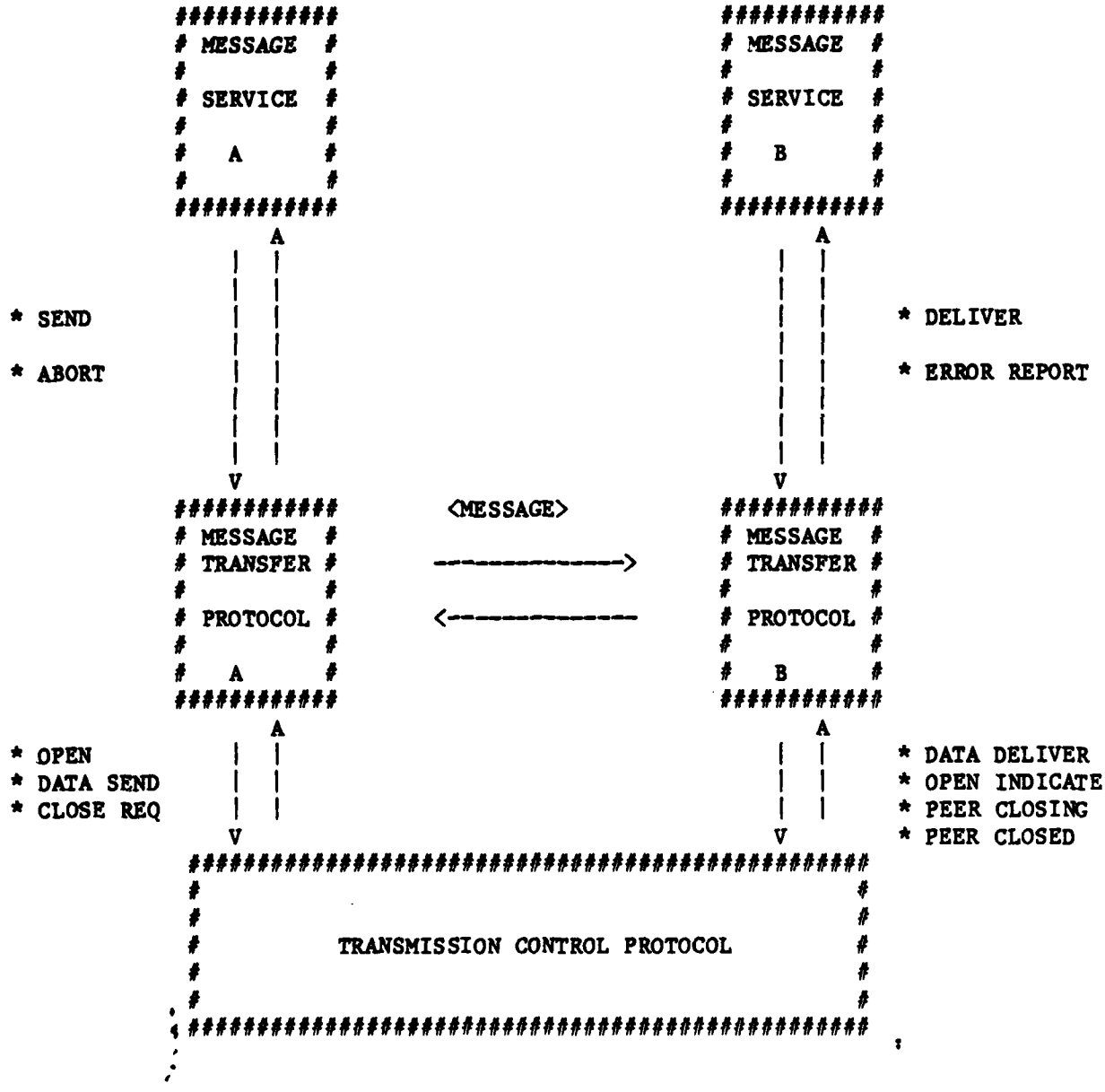


Figure 3-1. Possible Message Transfer Operations

In other words, the protocol must be capable of causing delivery of a message to a particular message service application entity whenever a message is submitted by any message service application entity, and the particular message service application entity's address occurs in a message addressee field.

3.1.2 The Data Unit

A message is the unit of data transferred between the message transfer protocol and its upper layer "user." When prepared according to local syntax, it will be recognizable as a message and will furnish transmission instructions in an unambiguous manner.

3.1.3 Extended Data Flow

A messaging network will be defined by a set of message transfer protocol peers capable of forming data transport connections between themselves. The message transfer protocol extends the data transport services in order to define message transfer pathways between message service application entities. Each message transfer entity must make data flow decisions to insure the eventual delivery of a message. No restrictions are placed upon the maximum number of different transfer protocol entities which handle a message, and the minimum number of message handlers is one. Therefore different routing scenarios are probable, depending upon the capabilities of the implementations.

3.2 CONTROL OF MESSAGE TRANSFERS

3.2.1 Starting and Halting Message Flow

The message transfer event is a one-way store and forward process; therefore, only simple controls are required. First, there must be "start" signals in both directions between the protocol and its upper layer; these allow one to begin transfer of a unit of data to the other. Second, there must be "stop" signals defined in both directions. Third, a means of aborting message

transfers between layers is required for use whenever this is possible. The "abort" is initiated by the sender and signals "cancellation" to the receiver.

3.2.2 Expedited Messages

The protocol must have capabilities to promote expedited transmission or delivery of urgent messages. Such messages will be recognized by either FLASH or CRITIC precedence. Appropriate technical means must be employed to attempt to process, transmit or deliver such messages without delays; otherwise the user is informed of the impending delays.

CRITIC messages are the most urgent, and as such have special requirements. For example, system operators require training in the handling of CRITICs, because of their urgency. CRITICs can be recognized by their unique precedence and destination and so need not be subjected to validation procedures required for non-CRITIC messages. (Specific descriptions of the format and some handling requirements are classified.)

3.3 MESSAGE STATUS REPORTING

The protocol must be capable of informing the upper layer about the status of a particular message delivery request. The types of results which are reported include but are not limited to:

3.3.1 Successful delivery to a peer protocol; the sending entity informs its upper layer user upon completion of a transmission to a peer.

3.3.2 Unsuccessful attempted delivery to a peer; the sending entity was uable to connect to and transmit a message to a peer entity servicing an addressee's message service.

3.4 MESSAGE QUALITY CONTROL

Some form of assurance is required that the protocol can carry out a message's transmission instructions. This assurance can, in principle, be provided by either the message service (where a message is prepared) or by the message transfer protocol. This document does not assume it is always practical for a message service to assure message correctness and so prescribes requirements for checking and sending error notifications to the upper layer user.

3.4.1 Syntax Checking

The message format must be correct in order that instructions may be correctly interpreted. Violations of message format syntax rules will result in task terminations and notification of error to the upper layer, except in the processing of CRITIC messages.

3.4.2 Valid Field Values

The indicators for sender, addressees, security and precedence must be recognizable and valid. Exceptions terminate the task and generate error notices to the upper layer, except in the processing of CRITIC messages.

3.5 CHOICES OF SERVICE

The following capabilities are not all essential to the operation of every message service, but all are essential to the provision of both "formal" and "informal" message service. Therefore, a "formal" message service may be based upon a particular set of choices, while "informal" service is based upon another.

3.5.1 Message Precedence Levels

In military communications some messages are more urgent than others, and a five-level precedence spectrum is currently defined for AUTODIN I and similar messages. The spectrum's purpose is two-fold: 1- to provide greater speed of service to more urgent message, and 2- to afford communication resource

access to urgent messages during saturation or other crises. The protocol must recognize the precedence spectrum and use appropriate technical means to assure service and speed to urgent messages. The protocol must also ensure aginst unauthorized access to high precedence service. When a message precedence option is not specified by a message service, as can be the case with "informal" messages, a default precedence may be assumed. A message service may use these levels if authorized by the local implementation. Otherwise, limited subsets or a single implicit default precedence are used.

3.5.2 Message Format Choices

The protocol must be capable of handling messages in several widely-used formats, including at least:

JANAP 128
ACP 127 (NATO Supp)
ACP 126 (M)
DD 173
Tactical Message Format

Each of these formats represents a context in which essential transmission instructions and message text are presented. They are all associated with "formal" messages, so that messages received in one of the above formats are most likely but not necessarily to be perceived as "formal" by users. Therefore, the protocol must be designed for flexibility in message format processing so that a standard for informal messages can also be added to the above list.

3.5.3 Message Security (Classification)

Senders may classify messages in order to protect information vital to national security; this limits the availability of messages to only those qualified for the designated classification. The set of message classifications, and receiver qualifications, along with rules governing access

to messages by receivers, are described in Appendix A. The protocol must preserve the integrity of this field throughout all message data transmissions, and the protocol implementation must be consistent and compatible with security policies and rules in force within a host operating system.

3.5.4 Multiple Addressees

The protocol must offer senders the option of specifying multiple addressees; AUTODIN I currently requires capabilities for 500, but future requirements may be higher. It must also support labeling addresses as "action" or "information" addressees. Finally, the protocol must support the use of address indicator groups so that groups of addressees may be denoted by a single name; it must also support specification of exemptions to group addresses.

It will also be necessary that the protocol recognize multiple families of addresses which reflect multiple user communities who exchange messages. At a minimum the protocol must recognize and process addresses currently used for AUTODIN I messages and "internet" addresses currently used to exchange messages between individuals over packet-switched networks. The former represents a community of formal organization and office/roles; the majority of "formal" messages will circulate in this community. The latter address community will exchange "informal" messages. Each such community can conveniently be served by a separate message service application entity having features and services tailored to community needs.

4. REQUIRED PROTOCOL FEATURES

Protocol features denote its capabilities which are not necessarily visible to the user but are still necessary for carrying out the specified services. As such, they address mechanisms. However, such mechanisms are predicated upon the anticipated operating environment and so are addressed in these requirements rather than in specifications. Performance goals are also addressed as features.

4.1 TRANSFER FEATURES

4.1.1 Minimum Addressing Domains

Users of DD-173 and to-be-defined informal message formats will employ addresses in "plain language", which are not the same as addresses used by network processes for routing and communication. Similarly full JANAP 128 (et al.) messages will contain address codes (RI's) now used by AUTODIN I Switching Centers (ASC's), but which do not correspond to the TCP address space. (Appendix C provides explanations and illustrations of JANAP 128 addresses.) Therefore the message transfer protocol will require several address interpretation features:

- the protocol must route messages based upon their plain language addresses found in DD173 and JANAP 128 formats;
- the protocol must route messages based upon their internet addresses used with "informal" messages -- user names, host names and network names;
- the protocol must route messages based upon their AUTODIN I routing indicators (RI's) and address indicator groups (AIGs).

4.1.2 Routing Decisions

The protocol either transmits each message it receives to a peer or delivers it to an upper layer entity. The choice of such an action is based upon the message address. Each valid message address must "map" to the address of a message transfer protocol peer for transmission or to the address of an upper layer message service application entity for delivery. The requirements in 5.1.1 above define the minimum mathematical "domains" of this mapping: plain language addresses, internet addresses and routing indicators.

The protocol must not exclude distributed address processing. A very large address base may preclude every protocol implementation from making precise routing decisions. Therefore, a sender protocol might transmit messages bearing addresses within a large class to a peer capable of making more accurate routing decisions. The dilemma can also be resolved by using name service (see Appendix B, for example).

4.1.3 Application to Interoperability

These activities are directly related to interoperability issues. One interoperability goal is to allow a non-AUTODIN I-connected user to send a message to a message to a AUTODIN I site. Correct interpretation of RI's would allow the non-AUTODIN I user to prepare a JANAP 128 message bearing an AUTODIN I RI and submit it to his own network via the message protocol. The sender protocol would perceive that the message was bound for AUTODIN I and would route it to a peer capable of presenting messages directly to AUTODIN I. Final routing would be carried out by AUTODIN I.

Two levels of addressing are similarly required to pass a message from an AUTODIN I site to a non-AUTODIN I site served by TCP and the message protocol. First, an RI must direct the message through AUTODIN I for eventual presentation to a message transfer protocol entity interfaced to AUTODIN I. Second, the standard message transfer protocol entities must interpret the message

address for suitable peer-to-peer exchanges and delivery to a message service. This second scenario requires no other changes to AUTODIN I ASC's than additions to standard routing tables.

The protocol must support such message transfers in and out of AUTODIN I and the NICS TARE system via address interpretation and use of compatible interface protocols such as AUTODIN Mode I.

4.1.4 Multiplexing Upper-Layer Message Services

Different user communities with different message-handling requirements (e.g. "formal" and "informal") will be represented by different message service application entities. The message transfer protocol must provide service between multiple pairs of compatible message services. (Compatibility implies that message service application entities may address messages to one another's users.)

4.1.5 Use of Transport Services

Extending the services of a reliable, secure data transport protocol to message handling processes is the primary purpose of the message transport protocol. It must isolate message service application entities from tasks associated with manipulation of the data transport connections, such as establishment, release, exception handling and fragmentation.

4.2 DATA STRUCTURE CONVERSIONS

As an interface between network resources and local message services, the message transfer protocol must perform needed data conversions. Protocol peers must exchange messages in a universal mutually recognizable form, (i.e. a transfer syntax) but this form may differ from that of the "local" messages handled by the message service application entities. Therefore data conversions must be performed as necessary both at the character level

and at the higher levels of data structure which comprise the structure of messages. In other words, the protocol must perform the translations between the local syntax and the transfer syntax.

4.2.1 Message-Level Conversions

The format of messages exchanged between protocol peers (i.e. the network virtual message format) must be capable of representing the types of information found in the JANAP 128 message format. The protocol must be capable of mapping any the of this message structure into the network virtual message, and it must also be capable of the inverse mapping.

4.2.2 Character-Level Conversions

The protocol must provide character-level code conversions as needed for upper-layer message services. The following list the minimal set of codes which must be converted by message transfer protocol implementations.

- o American Standard Code for Information Exchange; 8 bits (ASCII)
- o International Telegraph Alphabet; 5-level with 1 start bit, 5 information bits, 1 1/2 stop bits (ITA #2)
- o Extended Binary Coded Decimal Interchange Code; 8 bits (EBCDIC)

The first two ensure compatibility with existing DOD data communication interfaces; the third is the standard code for many computers (IBM, UNIVAC, etc.).

4.3 ROBUSTNESS FEATURES

Requirements for protocol features to provide robustness call for anticipation of circumstances which interface with the message transfer process. The specific mechanisms to counteract the interferences depend upon the

interference mechanisms themselves, as exemplified by the use of different types of error-correcting codes for different types of error patterns. The protocol must address following types of robustness provisions.

4.3.1 The protocol implementation must ensure against message loss; recording messages provides some assurance, but some form of loss detection (e.g. acknowledgements) is also required; when loss by the network is detected, the message must be retransmitted.

4.3.2 The protocol implementation must guard against unauthorized message modifications; however such events may be rendered unlikely by reliable and secure data transport services.

4.3.3 The protocol implementation must prevent message intermixture so that no portion of any message reaches a receiver for whom it is not intended.

4.3.4 The protocol implementation must prevent delivery of duplicate messages; unique message identification is an adjunct to this requirement.

4.3.5 The protocol implementation must guard against network overload, but must always provide network service for CRITIC messages; data transport service signals may assist in this requirement.

4.3.6 The protocol must validate message headers to ensure that transmission instructions are intelligible and valid and, it must assist users in error recovery otherwise.

4.4 PERFORMANCE GOALS

The message transfer protocol represents a link in a serial chain of service providing overall message transfer. The chain may be pictured, based upon the DOD architectural model, as:

message service/message transfer protocol/data transport protocol/ message transfer protocol/message service.

The message protocol can definitely affect the speed and accuracy of overall message transfers, but three other factors also limit performance -- the hardware and operating system on which the message transfer protocol is implemented, and the performance of the data transport service. As a result, neither a requirement for an overall message transfer bandwidth nor a requirement for a message transfer protocol-specific processing bandwidth can be stated.

Instead, the protocol must support in its design and implementation the achievement of the following overall message service performance goals:

1. mean speeds of service for average messages (2075 characters) by precedence class —

ECP/CRITIC	(1% or less of total traffic)	0.75 min.,
FLASH	(1% or less of total traffic)	1.0 min.,
IMMEDIATE	(approx. 15% of total traffic)	5.0 min.,
PRIORITY	(approx. 33% of total traffic)	30.0 min.,
ROUTINE	(approx. 40% of total traffic)	80.0 min.;

2. approximate overall processing rate (through-put) per Automated Message Processing Exchange (typically a host, attached to a packet-switched network, which supports a message service, message transfer protocol, and data transport protocol) --

16,600 bits/second, or 2075 characters/second;

3. frequency of message data errors --

   1 in 10^{12} or less;

4. frequency of misrouted messages

   1 in 10^{11} or less.

[These goals are based on discussions with DoD personnel.]

5. FUTURE REQUIREMENTS

The following services and features are identified as potential or future requirements rather than immediate ones. They have been identified as message transfer features by members of the computer-based message system R&D community. As future requirements, they address requirements which can arise in future message transfer scenarios; these are identified along with the requirements.

5.1 SERVICES OFFERED TO THE UPPER LAYER

5.1.1 Handling Stamps

Ideally, the overall handling of messages will remain simple enough so that the single indication of date/time by the message originator will satisfy users' needs for records of network message handling. However, should the process become more complex via relaying, forwarding, or physical separation of message service application entities from the message transfer protocol implementation, then the protocol must be capable of appending handling stamps to messages that it handles. This will allow users to continue to monitor the message service performance. Handling stamps indicate the identity of the process which handles the message and the time of handling. A sample format is described in [POST 80].

5.1.2 Posting Receipts

Physical separation of message service applications from message protocol entities can decrease users' confidence that messages have indeed entered the message transport system. Therefore, upon request in such cases, the protocol must generate a form receipt message to be issued to the originating message service. This feature will also support accountability requirements which user communities may impose upon themselves. Receipts do not guarantee delivery; they only validate the sending of a message.

5.1.3 Extended Status Tracking

When message transfer involves handling by more than two transfer protocol entities, a single status report cannot provide confidence that a message has reached a target protocol peer or recipient message service application. This confidence can be increased when each implementation of the transfer protocol which handles a message in turn transmits a status message to the sender. This effort should not be expended on non-urgent messages nor without the request of the sender. Therefore, upon request by the sender, the protocol will provide a message status report indicating time received, immediate sender, immediate transmission destination and time of transmission.

5.1.4 Source Routing

In cases where more than two protocol entities must handle a message, it can be necessary to avoid certain routes for administrative, political, or security reasons. To support this, the protocol must allow senders to specify intermediate handlers (protocol implementations at known sites) which must be avoided, to specify intermediates which must be used, or to specify a particular handling sequence.

5.1.5 Message Storage

Future message services (upper-layer applications) may be implemented on personal-sized machines as well as large mainframes. The personal machines may often be powered-down and off-line when attempts are made to transmit and deliver messages. Availability of larger machines may also be limited, for example, if periods processing is necessary. Other implementation factors may also limit availability. Therefore, messages must be held by a transfer protocol implementation when such host availability prevents deliveries or transmissions. This requirement raises several technical problems:

1. For what duration should a message be held? The practical limits depend upon the volumes of traffic intended for the inaccessible

host and the durations of its inaccessibility, and the urgency or perishability of the message.

2. By what means should the held message be delivered? The holder may try again to reach the inaccessible host, or the inaccessible host may call for its mail when it returns on-line.

3. Provision of longer holding times may necessitate special approaches to message encryptions, particularly due to key lifetimes. Under limited key lifetimes, a host may not be able to obtain a decryption key for a message which had been held.

5.2 PROTOCOL FEATURES

5.2.1 Multimedia Messages

As the capabilities of computing hardware and software grow, users will find needs for formats other than text characters in their messages. For example they may wish to exchange via messages the binary data required to direct graphics peripherals to produce line drawings or facsimile images, or the binary data which may be linked and interpreted directly as a process on the receiver's host machine. The message transfer protocol must support transfer of text and non-text messages. This capability presents additional technical requirements:

1. For non-text media the message transfer protocol must be indifferent to the actual data in the message "text" portion; data for other media may be non-recognizable under standard character codes, or they may contain apparent control sequences which must not be interpreted as such.

2. There must be means in the message syntax of indicating that a message has data bound for a particular medium, such as text,

graphics, facsimile, etc.; there must also be an option negotiation phase between the message protocol and message services to indicate availability of required devices and select default options in the case of unavailabilities.

3. A method of including more than one type of data in a single message is desirable; methods for "unbundling" multimedia messages and directing data to appropriate devices would be required.

4. Delay and throughput requirements may necessitate use of specialized multiple transport connections for multiple segment messages.

The third technical requirement implies a need for extended message structures to allow segregation of media into message segments and for protocol capabilities for segment-by-segment message handling. These features can be applied to another foreseeable multimedia message requirement -- to support handling of messages as multi-level security objects. Classification levels may be viewed as different media. Message segments are labeled as UNCLASSIFIED, SECRET, etc. and are handled accordingly depending upon the security levels of data transport services, transfer protocol peers and upper level message services and upon security rules in force.

5.2.2 Automatic Forwarding

Informal messages, addressed to individuals, may be addressed to recipients whose network "mail" addresses have since changed. It is quite feasible to leave forwarding instructions at the old "address" which can be automatically implemented, producing a re-addressed message to be carried by the several protocols to the recipient at the new network address. The protocol must support this capability.

5.2.3 Handling Perishable Messages

If the total message communication service is to support near-real-time applications, messages will often have time-dependent validity, becoming meaningless after their expiration.

The expiration time can be indicated in the message header. The message protocol must read this and compare to its own time, and discard the message if it's expired. This capability presents two technical problems:

1. Sufficient synchrony and resolution of the clocks so that certainty of out-datedness is assured before discarding.

2. The determination of whether notifications to senders are required upon message discarding; classified perishable message discards must generate notifications.

3. Allocation of responsibility for action between the message protocol and the application layer; either might hold messages for delivery.

5.2.4 Audit Trails

The architecture of DOD message services is expected to be based upon the AMPE concept; message service processes and message transfer protocol process will be implemented in the same hardware base. The protocol must support creation and maintenance of message audit trails showing transfers between message service application entities only. However should the message service application entity and message transfer protocol be physically separate, linked by a data transport protocol, such as TCP, then the audit trail must also show transfers involving the message transfer protocol. In this case, the protocol must write audit trail records showing receipts and transmissions of all messages.

APPENDIX A. MESSAGE TRANSFER SECURITY CONSIDERATIONS

A.1 Introduction

Determination of methods of governing access to classified messages by processes representing users cleared at different levels is a primary design issue in message systems. However, it is not practical to require that the message transfer protocol possess the qualities of and accept the responsibilities of a security kernel or a trusted process. The responsibilities for assuring that message security is preserved require determination of whether each information transfer is allowable (via the security model described below), as well as authentication of processes to which messages are transferred. These will be the responsibilities of and host operations systems rather than of the protocol itself.

The following paragraphs develop the concepts of the security model implicit in JANAP 128 (and similarly formatted messages) in terms of a partially-ordered clearance/classification lattice.

The lattice is a representation of the classes from which objects (i.e. messages) and subjects (e.g. human readers, processes, etc.) are selected. The relation described by the lattice tells both whether or not access to an object of one class may be had by a subject of another and whether a subject of one class may send information to a subject of another class. (The latter relation assumes implicitly that the first subject produces information classified at its same clearance level.) "Simple security" is the rule governing the accesses, and the "*-property" is the rule governing the information sending.

In order that the rules of this model be followed, there must be guarantees of both the proper marking (classification) of messages and of the correct clearances of the subjects which will access the messages. The former must be assured by enforcement of rules for message preparation and by assurance of message integrity during transmission (i.e. prevention of unauthorized modification). The latter must be assured by authentication procedures. These authentication procedures in turn require secure transfer or communication.

The enforcement of the lattice of access controls in an environment where both messages and subjects may be at many different classifications poses severe complexity problems. Many military ADP installations have used "system-high" or "periods" processing to limit the range of clearances and classifications which must be governed simultaneously. (This practice presents delays to users due to the exclusion and to lengthy system "color changes".) Submitted messages must be at the specified "period" level or at a level equal to or lower than the "system-high" level. Users are cleared at the "periods" level or higher than or equal to the "system-high" level. Examples:

- During the "secret" period all users are cleared at "secret" and all messages are "secret".

- During system-high "secret" processing, all users are cleared to "secret" or higher, and all messages are "secret" or lower.

Need-to-know categories are also enforced during "periods" and "system-high" processing.

The full potential of the lattice model must be exercised when both users and messages are present at multiple levels. The following explicitly describes message classifications, subject clearances (classmarking) and the rules for message reception (access). The locations of message classification labels are indicated, but the particular means of authenticating subjects, whether users or processes is beyond the scope of this note.

A.2 Message Transfer Security Model

1. The classification of a message is represented by a quadruplet:

(Security-level, TRC, TCC, SPECAT) .

A. The security-level may be one of the standard military classifications, TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED.

B. TRC represents the transmission control code required to release messages to foreign governments or regional defense centers. Symbols now used are

A - Australia
B - British Commonwealth and South Africa, except for Canada and New Zealand
C - Canada
Z - New Zealand
X - Any of Belguim, Denmark, France, FRG, Greece, Italy, Netherlands, Norway, Portugal, Turkey, NATO

Two TRC's may be present on a message.

C. SPECAT represents the special category indicator. Symbols now used are

A - SIOP-ESI messages
B - other SPECAT messages
F - messages for UK activities with special handling designators (e.g., US-UK EYES ONLY)

D. TCC represents the transmission control code trigraph (i.e., three alphabetic characters). These are used by particular communities of interest to enforce need-to-know restrictions.

2. Receivers bear classmarks corresponding to the same quadruplet, except that some receiving stations may possess more than one SPECAT or TCC qualification. Therefore, a receiver's qualifications may be expressed by a similar qudruplet:

(Security-level, Country, SPECAT , TCC),

where the "Country" represents the receivers location and may be implicit in the address.

3. In order for message transfer to be permitted, the following relations between the message classification and the receivers classmaking must all hold true:

Message	Relation	Receiver
o Security-level		Security-level
o TRC	contains	TRC of receiving country

(required only for release outside of US)

o SPECAT	is subset of	SPECAT
o TCC	is subset of	TCC

A.3 Location of Message Classification Indicators on JANAP 128 Messages

Format Line 2, space 4 gives security
" space 30 " "
" spaces 31-33 give redundant security markings, or else spaces 31-33 give TRC. If two or more TRC's appear must be in alphabetical order.

Format Line 4 spaces 5-9 give either

5 x security (e.g. UUUUU) or
3 x security + TRC (2) (e.g. UUUBC) or
2 x security + TCC (3) (e.g. UUNSH) .

Format Line 4 gives SPECAT immediately following spaces 5-9 and preceded by a slash (/).

A.4 Message Recording

Although message recording is a candidate for a required presentation protocol service, it could be implemented as well by the upper layer message service. This has the advantage of limiting the complexity of the protocol while allowing flexibility in this function at the upper layer.

AUTODIN I messages are presently recorded at all ASC sites and at most, if not all, tributary sites; but in practice it is extremely inconvenient and seldom necessary to recall a message from an ASC history tape. Although the widespread practice of message recording supports accountability, the need for it is offset by past plus expected reliable performance by the message transport system.

Because of the practice of recording AUTODIN I messages on centrally-administered media, it is anticipated that message recording will become a requirement of upper-layer message services supporting "formal" messages. The message services will also carry out retrievals of messages based upon the date/time of message issue, the sender, the addressees, and so forth.

A.5 Message Release Authorization

One of the virtues of the AUTODIN I message service and a definite candidate protocol requirement is message release authorization procedures and resulting assurance of message authenticity. However, it is primarily the administrative controls exercised in AUTODIN I which provide authenticity. (See Section 2.2.1 .) These procedures are indeed candidates for automation, but not at the message transfer protocol level. Drawing from the architectural correspondence of Section 2.1.5, the release authorization is initiated at the message service level. The problem of authentication of the message service to the message transfer protocol is beyond the intended scope of a single communications protocol and belongs to implementation considerations for system-wide security.

A.6 Secure Data Transport Service

In order for classified messages to be exchanged between message transfer protocol peers, a secure, non-exploitable data transport service (and networks) must be provided. "Secure" implies that means are provided to prevent the following:

- o unauthorized release of message contents
- o unauthorized modification of message contents
- o unauthorized denial of resources

Communication security measures (e.g. encryption) protect against attackers outside the user community, while access controls and authentication mechanisms protect against potential attackers within the user community. Access controls and authentications are tools for the implementations of military security policy at processing sites, and both depend, in turn, upon a secure communication service. Such a service will be provided by AUTODIN II and is assumed in the discussion of the security access model.

APPENDIX B. ADDRESSING ASSISTANCE

Provision of various forms of addressing assistance are candidate requirements for a message transfer protocol. For example, end-users may be relieved of the task of providing routing indicators or other direct addressing codes, such as socket numbers. Users may also need assistance in completing network addresses (i.e., network names and host names). This assistance can also take a distributed form, so that network servers can provide address information.

However, system designers are better served by placing such services with upper layer message services. This eliminates a source of considerable complexity and grants flexibility to message services. Furthermore, no additional protocol service need be specified for using distributed network address assistance. End users may send a form message to an address server, receiving a form reply; another method of communication with a network address server is via a TELNET connection.

This type of service presents two important technical problems. First, the data bases which furnish addressing information must be kept synchronously up-to-date. Second, there will be questions of access authorization to this information.

APPENDIX C. ANALYSES OF EXISTING MESSAGE SYSTEMS

The analysis of existing message system serves two purpose: 1) it points how basic functions are performed for users, giving designers systems to learn from, and 2) it points out where functional and performance shortcomings exist and suggests methods of correction. This section will explore existing hardware and software systems with these purposes in mind. It will also examine users' message-handling procedures with a view towards defining formal versus informal messages. Finally, existing message headers will be interpreted in detail to identify protocol requirements.

C.1 COMPUTER-BASED MESSAGE FACILITIES

C.1.1 The AUTODIN I System

C.1.1.1 Traffic Categories

AUTODIN I is a digital network based upon message-switching technology which today carries several forms of digital data traffic for military users. These include:

a. narrative messages
b. "data pattern" messages
c. "query/response" traffic
d. hybrid autodin redpatch service (HARPS).

Narrative messages will be the data objects transferred by the MTP; in the future the MTP may be required to transfer messages containing other than text character data.

"Data pattern" messages are generally large magnetic tape files or other very long segments of data. They are generally not intended to be read by humans upon receipt. Therefore, such transfers will be more appropriate for a file transfer protocol (FTP) when AUTODIN I tributaries become part of future DoD data communication networks.

"Query/response" traffic represents interactive dialogue carried between users at terminals and host computer systems. This type of traffic will be handled by terminal-to-host protocols in the future.

HARPS service is used by installations which have infrequent needs to transmit very large volumes of information. By agreement with recipients and intermediate switching centers a continuous circuit is "switched" in for a direct link between sender and receiver.

C.1.1.2 Communications Centers

Three general reference covering the operations of AUTODIN I are JANAP 128, [JAN128], and "Message Protocol Requirements Volume I, Annex C," [CLAR80], and [DCA370].

Many AUTODIN I tributary sites operate as batch-oriented communication-centers. Messages are submitted to operators who submit them into a batch-oriented system. A typical message handling operating system is queue- and interrupt-driven; basic tasks are queue management and I/O operations. The line to the AUTODIN I Switching Center (ASC) is treated as an I/O device. Information in the message header is used to route messages to I/O devices. Messages are received as print-outs, tapes or card decks and are picked up by the users from the operator. [SAT5] and [ATE81] describe operations of AUTODIN I tributaries; more than 70 such systems are presently operational.

C.1.1.3 AUTODIN I Communications Protocols

The message transfer protocols implementation in AUTODIN I rely on lower-level protocols, typically AUTODIN Mode I, to transmit messages (in JANAP 128, ACP 127, ACP 126 or DOI-103 format). A unit of transmission (a "block") for AUTODIN Mode I can be a line of teletype text or a card image, up to 80 characters in length. Mode I provides link control functions, such as synchronization, acknowledgements, and error control. Its control characters can also indicate the beginnings of message header and text sections, the ends of messages, and the target media for messages. Therefore it acts as more than a link-level protocol. ASCII character code is used, with seven information bits and one parity bit. Data may be transmitted at rates of 2^n x 75 bps, n = 0 - 7. Interfacing with NATO switches is carried out at 600, 1200 and 2400 bps only. See [DCA370] for description of other AUTODIN I link-oriented protocols that vary with respect to speeds and error and channel controls.

AUTODIN store-and-forward processes provide for the end-to-end transport of messages between two tributories. Each ASC node must receive a given message in entirety from a sender before it begins transmission to another ASC or tributary. Message routing indicators (RIs) indicate to ASC nodes upon which line the message should be transmitted. These processes for moving messages from the sender station to the receiver station form a message transfer protocol for AUTODIN I. Details of these processes are provided in Appendices to [CLAR80].

C.1.1.4 AUTODIN I Conclusions

An immediate intuitive comparison of AUTODIN I with packet-switched nets such as the ARPA net would suggest that ASC's and packet-switching nodes are analogous, because each performs data routing. From the point of view of message transfer, however, the ASCs are implementations of a message transfer protocol. Both transfer entire messages to and from either "peers" or message distribution systems. Within this analogy a major difference lies in the

communication between the message transfer "peers." In the AUTODIN I environment, only point-to-point lines exist between ASC "peers," often necessitating multiple hops. In the packet-switched environment, it is nearly always possible to define a single virtual pathway between two message transfer "peers," even across multiple packet-switched networks; rarely is storing and forwarding required.

The following correspondences can be drawn between the AUTODIN I architecture for message transfer and a packet-switching architecture for message transfer:

1. AUTODIN I tributaries can correspond to message service systems
2. AUTODIN I ASCs can correspond to message transfer protocol implementations
3. AUTODIN I Mode I can correspond to a data transport protocol implementations

The present AUTODIN I system and similar technologies present two major shortcomings:

1) the speed of service offered by message-switching is not competitive with that offered by packet-switching technology;

2) the manual submission and distribution of messages create delays on the order of minutes and hours; automated message handling can significantly reduce the delays.

The message transfer protocol is part of an overall remedy to these kinds of performance and functional shortcomings. It defines an interface between automated message handling entities and packet-switched data transport services.

C.1.2 User Terminal-Based Systems

Systems such as SIGMA, HERMES, and NMIC-SS have extended the basic message transfer service provided by AUTODIN I tributary/terminal systems into time-sharing environments. These individual user-oriented message services provide more direct user-to-message access via such features such as message retrieval, preparation, coordination, etc.

The military message experiment (MME), conducted in the late 70's, undertook to evaluate the feasibility and utility of extended automation of message handling. Three large-scale message-handling systems were initially evaluated, but only one, SIMGA, was retained for a field trial at CINCPAC Headquarters. SIGMA is a software system which supports many message handling functions for interactive users. Among these functions are message preparation, coordination, distribution, storage and retrieval. Many of SIGMA's design features were aimed at finding optimal trade-offs between acceptable human interfaces and enforcement of security policy. SIGMA was well-received by users, and the MME has lead to the definition of requirements for automated message handling in Command centers [ROCAMH]. References to the features, design and evaluation of SIGMA are found in [ROTH70], [TANG77], [WILS77] and [GOOD80].

The implementation of SIGMA illustrated how the message handling functions may be separated from network functions. SIGMA's interface to the AUTODIN I network was provided by the LDMX (local digital message exchange) system; the LDMX also provided message-handling functions such as format checking, distribution, storage and retrieval. Therefore, the implementation of SIGMA depended only upon a specified interface to the LDMX and not at all upon an interface to AUTODIN I.

C.1.3 The WWMCCS Intercomputer Network (WIN)

The WWMCCS Intercomputer Network (WIN) is telecommunication network, similar to the ARPA net, which interconnects WWMCCS sites. Its primary uses are in the support of joint force activities: planning, deployment coordination, post-exercise analysis, etc.

Two types of message services are available; point-to-point exchange and teleconferencing. (File transfers are also used extensively.) Teleconferencing involves establishment of a particular community/ conference of correspondents. The conference director admits participants on an exclusive basis. Proceedings then take place via message exchanges, typically over days, weeks or even longer. The conferences typically serve organizations who participate in exercises and need to plan (prior to the exercise) or conduct reviews.

Although conference proceedings are recorded, participants have often found a need for private, off-the-record exchanges. Therefore participants also use informal message exchange capabilities, which may optionally be recorded. However, considerable disagreement exists as to the appropriateness of this capability for military use.

The Joint Chiefs of Staff organization (JCS) is currently urging acceptance of WIN teleconferencing messages as formal messages. However many WIN users feel comfortable only with the message authenticity guarantee provided by DIN I formal messages.

C.1.4 Non-military Computer-Based Message Services

With the advent of resource sharing protocols for use between host computer systems, many computer-based message systems have now been developed. Organizations having developed these include ARPA, BBN, ISI, Texas Instruments, Bell Labs, Telenet, and Tymnet, to name a few.

Typically these systems are oriented towards time-sharing terminal users who control file storage areas on a shared disc or other storage device. Part of the file area serves as the user mailbox to which all messages are delivered. The user may examine the mailbox contents through standard file manipulation utilities or via a specialized message retrieval utility, such as Unix's MSG. Another utility (typically) allows users to compose and send the messages.

Such systems are models of the "informal" messaging being considered as part of the MTP service. However, the time-sharing file-system scenario is not a necessity, and informal messages could as well be exchanged via batch systems using paper tape or other data storage media.

The present computer-based message systems developed by the organizations mentioned above are unsuitable for "as is" processing of military message traffic. They can provide some degree of protection and privacy, but not to the degree required for classified data. Nor do they offer provision for the spectrum of urgency which military traffic encompasses.

The National Bureau of Standards (NBS) has issued a proposed Federal Information Processing Standard [NBS81] of message formats for computer-based message systems. The specification allows messages to identify a precedence level (e.g. routine, priority, immediate, etc.). Such a feature can support DoD requirements for message precedence groups. On the other hand, the specification totally omits any fields to indicate classification or other security markings. In this respect the specification precludes meeting DoD requirements.

C.1.5 User Acceptance Issues in Automated Message Handling

1. There are trade-offs between user convenience and security policy enforcements, but this is primarily message service rather than message transfer protocol issue.

2. In the MME, the extension of automated distribution, preparation, sending, reception to user terminals did expedite formal message delivery; however MME participants concluded that manual message handling will remain (especially, say, for draft coordination among colleagues in very close proximity).

3. Many in the military community treat only AUTODIN I messages as action items, because the administrative procedures assure message authenticity. Gaining conservative users' acceptance of automated authentication can be an unwritten design goal; the overt design goal is a reliable method of formal message authentication.

C.2 FORMAL AND INFORMAL MESSAGES

C.2.1 Present Procedures

The DoD standard form for originating AUTODIN I messages is the DD-173. An organization or officer sending a message fills out DD-173, indicating the message's precedence and classification, the plain language address(es) of recipient(s) (for action and/or for information), and the message text itself. Specific information items, such as classification, subject, references are expected in the text. Finally, a release authorization signature must appear on the bottom of DD-173.

The DD-173 is submitted over-the-counter to operations personnel at most AUTODIN I tributary sites. The release authorization signature is checked against that on a signature card on file at the communications center.

Operations personnel also look up the routing indicators (5-to-7 letter code(s)) of the message addressees. The message is either manually converted (i.e., typed) into JANAP 128 format (onto paper tape) or is automatically converted with the aid of OCR equipment. Some OCR systems can also supply well-known RI's. OCR systems also produce a paper tape with a JANAP 128 formatted message. Operations personnel then enter this paper tape into the network via the AUTODIN tributary hardware/software system.

The message is then transmitted through the AUTODIN I network to appropriate tributaries. Upon arrival it is transferred to printed media or to card, magnetic tape or other storage. Tributary processors notify operators of message arrivals. Operations personnel notify recipients by telephone or by courier or urgent (IMMEDIATE or higher depending upon standard operating procedures) messages. ROUTINE messages may be held for several hours, usually awaiting scheduled pick-ups.

The release authorization guaranteed by AUTODIN I is due to the administrative/operations procedures rather than to automated features. However, tributaries are automatically authorized up to certain precedence, security and need-to-know levels. The actual transmission of a message into AUTODIN I is not preceded by an automated authentication; this function has been performed by the operator processing the message.

Although the message service provided by AUTODIN I clearly differs from electronic mail services exemplified by ARPA net mail, there is no existing official definition of "formal" versus "informal" message service. These

terms are rapidly becoming common practice in the computer messaging community, with "formal" messages associated with the services offered by AUTODIN I. [HEIT80] provides an excellent discussion of formal/informal message distinctions.

This document proposes the following distinctions between formal and informal messages as operational concepts. In section IV, some specific functions associated with these concepts are called out as message options, allowing message service applications to meet varied user needs for "formal" or "informal" message service.

C.2.2 Formal/Informal Message Distinctions

1. Formal messages are presented in one of several prescribed formats: JANAP 128, ACP 127 (US or NATO supp's), ACP 126 (M) or DOI-103. Presentation in one of these formats necessarily implies that the message is formal.

2. Informal messages are not sent via formal message formats.

3. All formal messages are recorded onto history tapes.

4. Not all informal messages need be recorded.

5. A five-level precedence spectrum is defined for formal messages: ROUTINE, PRIORITY, IMMEDIATE, FLASH, CRITIC.

6. Occasional desire, but not need, has been expressed for precedence categories for informal messages.

7. The formal message sender/addressee universe is composed of organizations, not individudals. Individuals may be reached based upon their roles in organizations but not upon their identities as individuals.

8. Current AUTODIN I "comm center" administrative procedures guarantee authenticity of formal messages. Prior authorization to release messages exists in the form of signature cards on file in "comm center"; submitted messages must bear authorizing signatures before operations personnel will transmit them.

9. Informal message release authorization is less strictly controlled. All that the user needs is "mailbox" authorization.

10. Informal messages may still be classified.

C.2.3 Envisioned Procedures -- Automated Formal Message Handling

The military message experiment (MME) has furnished scenarios of formal message processing in an environment where message senders and recipients can submit and receive message "on-line" rather than in "batch" mode. An action officer can interact with a terminal to prepare, coordinate, receive, distribute and store messages. These functions are not automated in most present systems.

For example, an action officer using an Automated Message Handling (AMH) system (of which SIGMA is a prototype) may compose a message on-line, use local distribution capabilities or semi-formal messaging to circulate drafts and obtain comments or approval. If authorized by the AMH system, he may transmit the message. Any such authorization must be as reliable as the signature method.

The action officer also receives notifications of message arrival from the terminal. If he cannot attend the terminal he can assign a guard to the terminal to watch for incoming messages. Distribution to specific terminals within a local AMH is programmed by system managers; network distributions to other AMHs must be affected by re-addressal.

C.3 EXISTING MESSAGE HEADERS

The designers of the military MTP can obtain a similar knowledge of system requirements by detailed examinations of message headers which direct the actions of existing message systems. The repertoire of transmission instructions implies a similar repertoire of necessary capabilities. The following presents a detailed examination of the message structure prescribed by JANAP 128 [JAN128].

C.3.1 The JANAP 128(H) Message Structure

Message Structure Overview

JANAP 128(H) messages are composed of units called "format lines." A format line may be composed of one or more teletype records (lines of type). A normal line (of type) is terminated by a carriage return followed by a line feed (CR,LF), while a format line is terminated by two carriage returns followed by a line feed (CR,CR,LF). Although format lines have number names (e.g. "format line 2") these are not always implied by their order of appearance in a message.

For example, "CODRESS" and "ABBREVIATED PLAINDRESS" messages contain no format lines 6,7,8,9 nor 10. Therefore, unique characters or character groups near the beginning of each format line assist in identifying particular lines. For example, only format line 1 begins with the character quartet "ZCZC"; therefore "ZCZC" uniquely identifies format line 1.

Table C-1. Format Line Identification Patterns

Format Line	Identification Patterns
1	ZCZC in record columns 1-4
2	One of (Z,O,P,R,Y) in col. 1 (precedence), AND one of (A,B,C,D,F,I,R,S,T) in col. 2, col. 3 (language, media indicators), AND one of (T,S,C,R,E,U) in col. 4 (security); space in col. 9.
3	DE in cols. 1-2.
4	ZN in cols. 1-2 AND one of (R,Y) in col. 3. (Other special operating groups may be in cols. 1-3.)
5	One of (Z,O,P,R,Y) (precedence) in col. 1 AND space in col. 2.
6	FM in cols. 1-2.
7	TO in cols. 1-2.
8	INFO in cols. 1-4.
9	XMT in cols. 1-3.
10	Accounting symbol in cols. 1-2. (See JANAP 128(H) Annex C, Appendix I.)
11	BT in cols. 1-2. (Separator line.)
12	One of (T,S,C,R,E,U) in col. 1. Text line.
13	As in line 11 above.
14	not used.
15	C in col. 1, OR "#" in col. 1 AND four digits in cols. 2-5.
16	(CR,CR,8(LF),NNNN, 12(LTRS), OR repeat first 33 or 28 characters of line 2, then NNNN.

Table C-1 lists for format line the groups of characters which identify the line. It can be seen that each line (save #'s 11 and 13) has a unique identification pattern.

C.3.2 Detailed Format Line Structures

Each record contained in a format line may be up to 69 characters long. Multiple records may be needed for format lines 2 and 12, which contain the routing list and text message, respectively. The following table, C-2 shows the record structures of individual format lines.

Table C-2. Message Format Line Structures

Format Line	Column	Symbol	Explanation
1	1	Z+	
	2	C|	start-of-message (SOM) signal
	3	Z|	
	4	C+	
	5	D+	
	6	R|	channel name
	7	A+	
	8	1+	
	9	2|	sequence number
	10	3+	
2	1	P	.. precedence
	2	T+	language/media format indicator
	3	T+	
	4	T	.. security
	5	Z+	
	6	Y|	.. content indicator, action identifier
	7	U|	
	8	W+	
	9		.. separator
	10	Y+	
	11	E|	
	12	D|	.. originator routing indicator (RI)
	13	A|	
	14	D|	
	15	R+	
	16		.. separator

Table C-2. Message Format Line Structures (Cont'd.)

Format Line	Column	Symbol	Explanation
	17	O+	
	18	O|	.. station serial number
	19	2|	
	20	3+	
	21		.. separator
	22	1+	
	23	2|	
	24	3|	.. filing time
	25	1|	
	26	2|	
	27	3|	
	28	4+	
	29	-	.. security warning
	30	T	.. redundant security
	31	N+	
	32	S|	.. transmission control code
	33	H+	
	34	-	.. two hyphens indicate start-of-routing
	35	-	
	36	Y+	
	37	A|	
	38	H|	.. RI of first addressee
	39	H|	
	40	Q|	
	41	Q+	
	42		.. separator
	43	Y+	
	44	A|	.. RI of next addressee; follow by additional
	45	D|	RI's and separators as necessary, until
	46	R|	
	47	Z|	
	48	Q+	
	49	.	.. end-of-routing signal
4	1	Z+	
	2	N|	.. security warning signal
	3	Y+	
	4		.. separator
	5	M+	.. security indicatory
	6	M+	
	7	N+	
	8	S|	.. transmission control code trigraph
	9	H+	

Table C-2. Message Format Line Structure (Cont'd)

Format Line	Column	Symbol	Explanation
5	1	P	.. precedence
	2		.. separator
	3	0+	
	4	3|	
	5	1|	
	6	2|	
	7	2|	
	8	5|	.. date/time group
	9	Z|	
	10	|	
	11	M|	
	12	A|	
	13	Y|	
	14	|	
	15	7|	
	16	5+	
6	1	F+	.. "from" prosign
	2	M+	
	3		.. separator
	4	P+	
	5	I|	
	6	C|	
	7	K|	.. sender name
	8	E|	
	9	N|	
	10	S+	
7	1	T	.. "to" prosign
	2	O	
	3		.. separator
	4	K+	
	5	A|	
	6	U|	.. action addressee
	7	F|	
	8	M|	
	9	A|	
	10	N+	

Table C-2. Message Format Line Structure (Cont'd)

Format Line	Column	Symbol	Explanation
8	1	I+	
	2	N|	.. "information" prosign
	3	F|	
	4	O+	
	5		.. separator
	6	E+	
	7	L|	
	8	D|	
	9	R|	
	10	I|	.. information addressee
	11	D|	
	12	G|	
	13	E+	
9	1	X+	
	2	M|	.. "exempt" prosign
	3	T+	
	4		.. *separator*
	5	N+	
	6	O|	.. addressees exempted from delivery
	7	N|	
	8	-|	
	9	U|	
	10	S+	
10	1	S	.. NASA accounting symbol
	2	A	
	3		.. separator
	4	2+	
	5	5|	.. group count for encrypted text
	6	5+	
11	1	B	.. separation line
	2	T	

Table C-2. Message Format Line Structure (Cont'd)

Format Line	Column	Symbol	Explanation
12	1	U+	
	2	N|	
	3	C|	
	4	L|	
	5	A|	.. classification
	6	S|	
	7	|	
	8	E|	
	9	F|	
	10	T|	
	11	O+	
	12		
	13 ...	(TEXT)	
13	1	B	.. separator line
	2	T	
15	1	#+	
	2	0|	.. station serial number
	3	0|	
	4	2|	
	5	3+	
16		2 CR's 8 LF's NNNN 12 LTRS (End of Message)	

Table C-2. Message Format Line Structure (Cont'd)

Message Examples

1. Plaindress Message

Format Line	Contents	End of Line
1	supplied automatically	CR CR LF
2	RTTUZYUW RUEBABA1234 1081400-UUUU--RUKKLAA.	CR CR LF
4	ZNR UUUUU	CR CR LF
5	R 181230Z APR 69	CR CR LF
6	FM AFSC ANDREWS AFB MD	CR CR LF
7	TO ELMENDORF AFB ALASKA	CR CR LF
11	BT	CR CR LF
12	UNCLAS (TEXT)	CR CR LF
13	BT	CR CR LF
15	#1234	CR CR LF
16	CR CR LF LF LF LF LF LF LF LF NNNN	12 (LTRS)

2. Abbreviated Plaindress Message

2	PTTCZYUW RUCLDBA0123 1081400-CCCC--RUHHLFA.	CR CR LF
4	ZNY CCCCC	CR CR LF
11	BT	CR CR LF
12	C O N F I D E N T I A L (TEXT)	CR CR LF
13	BT	CR CR LF
15	#0123	CR CR LF
16	CR CR LF LF LF LF LF LF LF LF NNNN	12 (LTRS)

3. CODRESS Message

2	RTTUZYUW RUEOLGA0025 1081400-UUUU--RUCIABA.	CR CR LF
4	ZNR UUUUU	CR CR LF
5	R 181320Z APR 69	CR CR LF
10	GR55	CR CR LF
11	BT	CR CR LF
12	X FJKTUVBJVVKTHHAL:KWLRTJJ KKHGG (encrypted)	CR CR LF
13	BT	CR CR LF
15	#0025	CR CR LF
16	CR CR LF LF LF LF LF LF LF LF NNNN	CR CR LF

C.3.3 Requirement Interpretation from JANAP 128 Header Fields

Table C-3 presents a detailed interpretation of header fields and presents interpretations of resulting requirements. Fields not only carry transmission instructions, but also carry information in support of message accountability (registration) and distribution instructions (alt-routing pilots, addressees and CICs). Protocol requirements are suggested based on the requirement that initial protocol operating capability supports carrying of JANAP 128 (H) messages.

C.3.4 Tactical Message Format

The tactical message format is shown in schematic detail in Volume 1 of this study. It is more concise that the JANAP 128(H) no doubt because of its shorter history and its tactical application. Its fields again support transmission instructions and administration:

start-of message
precedence (C,A,B,Y,Z,O,P,R)
classification (T,S,C,U)
originator RI
message type (control, perishable, non-perishable)
station serial number
addressee RI's
EOR (end-of-routing)
EOM (end-of-message)

Absent are the date-time group, the addressees' name fields and other reader-writer information. Particular attention is still given to security and precedence, however. In summary, tactical messages indicate only the sender, receiver and transmission instructions.

Table C-3. Identification of Requirements from JANAP 128(H) Message Format

Item Reference	Format Line	Field	Explanation and Requirement
1	1	transmission identification (TI)	Indicates start-of-message, designates station/channel, indicates sequence modulo 1000 required for Mode II, IV, V terminals. (See p. 2-1, p. 2-2 of JANAP 128(H).) REQUIREMENT: Protocol must be capable of delimiting messages, and maintaining upper-layer-to-message bindings.
2	1	pilots	Automatically generated indicators of suspected duplicates and alternative routing of collectively routed messages. (See JANAP 128(H) p. 3-19, p. 3-5.) REQUIREMENT: Protocol must detect and identify message duplicates.
3	2	precedence	Indicates membership in precedence category with specific speed-of-service objective. See Vol. 7, pp. 17-19. REQUIREMENT: Protocol must preserve label, support speed of service by appropriate technical means.

Table C-3. Identification of Requirements from JANAP 128(H) Message Format (Cont'd)

Item Reference	Format Line	Field	Explanation and Requirement
4	2	Language Media Format	Code letters indicate message media (tape, cards, etc.). REQUIREMENT: Protocol must transfer parameter(s) for language media.
5	2	CIC/CAI	Content Indicator Code/Communication Action Identifier. (See Appendix B of JANAP 128(H).) CIC is for receiving terminal use to determine distribution actions. CAI code used by both communication terminals and ASC/relays stations for traffic handling actions (indicate presence errors, duplicates, forwarding; narrative message indication, service message indication). REQUIREMENT: Protocol must transfer CIC/CAI codes.
6	2	OSRI, SSN	Originating station routing indicator, station serial number. REQUIREMENT: Protocol transfers information and can perform needed address conversions.
7	2	date-time filed	Date and time of message submission. REQUIREMENT: Protocol must transfer date-time field on messages.

Table C-3. Identification of Requirements from JANAP 128(H) Message Format (Cont'd)

Item Reference	Format Line	Field	Explanation and Requirement
8	2	record count	Indicates number of records in message. REQUIREMENT: Protocol must transfer field.
9	2	Classification	Indicates sensitivity of message. REQUIREMENT: Protocol implementation must preserve message security via process authentication security marker protection, message security enforcement. Protocol must check classification redundancy; reject message on classification mismatch.
10	2	Classification (Cont'd)	
11	2	Called Stations	Routing indicators of "called stations," up to 500 per message. REQUIREMENT: Protocol must map RI to appropriate transport connection. Protocol must be capable of mapping multiple RI's to multiple transport connections. Protocol must also use RI's for delivery of codress, abbreviated plaindress messages.

Table C-3. Identification of Requirements from JANAP 128(H) Message Format (Cont'd)

Item Reference	Format Line	Field	Explanation and Requirement
12	3	Calling station, filing time	Not used in Autodin I; used with messages from other networks. See items 11, 7.
13	4	Classification fields	See above #9.
14	5	Precedence data-time group	See above #3, #7. Precedence applies to INFO addressees. REQUIREMENT: Protocol must support dual precedence for action and information addressees.
15	6	Originator's designation	Plain-language address, RI, address group or call sign of originator. Not used in CODRESS messages. REQUIREMENT: Protocol transfers field in plaindress messages; may use to determine deliveries to message services.
16	7	Action addressees	Action addressees indicated as in #15. REQUIREMENT: Protocol must attempt use of addressee names to effect correct delivery to user processes. Not used in CODRESS messages.
17	8	information addressees	Addressees of parties receiving message copies "for their information." REQUIREMENT: See #16 and #14.

Table C-3. Identification of Requirements from JANAP 128(H) Message Format (Cont'd)

Item Reference	Format Line	Field	Explanation and Requirement
18	9	exempt addressees	Used when collective address requires exemptions. REQUIREMENT: Protocol must have collective addressing capability and must be able to effect exemptions specified in format line 9.
19	10	Accounting sybmol group count	Used when text consists of countable encrypted groups.
20	15	Corrections	REQUIREMENT: Protocol transfer correction data.

C.3.5 ARPANET Mail Message Format

ARPANET mail can be exchanged among hosts with distinct but similar mailing and mail retrieval programs. Messages received from different mailing systems may contain different subsets of the following types of fields:

- o network mail title header identifying host and IMP
- o date of sending
- o message numerical identification
- o sender (user @ host)
- o receiver one or more (user @ host)
- o cc: receiver one or more (user @ host)
- o subj: any text
- o in-reply-to: any text

The subsets of these fields may also be placed in different order by different message systems.

The transmission instructions are mainly the identification of the addressees. The remainder of the fields support administrative and user retrieval functions. This message format is clearly adapted to an office-oriented non-military environment.

C.4 CONCLUSIONS

Existing computer-based message systems have been implemented using both message-switching and packet-switching technologies. The needs of military traffic are now being met by message-switching systems, while commercial and unclassified research communities are now served by packet-switching technology. Existing systems (such as AUTODIN I) which carry military traffic define a set of baseline functional requirements for the military

MTP; the MTP will define these services within the context of packet-switching technology and its associated architecture. It will also define an interface for sending and delivering which can be employed by a wide variety of message-handling application systems.

The detailed study of the existing message formats has revealed how user needs are being met by existing message handling systems. However, message headers such as that prescribed by JANAP 128 bear information for both message service applications as well as message transfer protocols. A detailed analysis of the impact of JANAP 128 header items on message transfer protocol requirements has been provided.

APPENDIX D. GLOSSARY

function	-- an activity on the part of a protocol implementation necessary for providing a specified service
lower-layer service	-- services provided by protocol residing in the next lower layer within the protocol hierarchy
mechanism	-- a particular method by which a protocol performs a function or service
message, narrative	-- a unit of data transferred between message-handling applications; when decoded it may be read and understood by a human reader
network virtual message	-- the format into which a message is encoded for data transmission
protocol	-- a set of rules and procedures for the transfer of data; specifically messages here
service	-- any activity on the part of the protocol which is visible to the user and directed at specific user needs
transfer	-- the process of moving a message from one location to another
upper-layer entity	-- any protocol or process which resides above the message transfer service in the protocol hierarchy

REFERENCES

ATE81 Executive Summary: DCT 9000 Automated Terminal Exchange (ATE) System. Ft. Huachuca, AZ: US Army Communication-Electronics Engineering Agency, Telecommunications Automation Directorate [1979].

BA79 Booz-Allen, IAS Overview and Functional Specifications of the Common Family of Terminals, Services and Protocols Annex: produced for Contract DCA-77-C-0057 [1979].

BERN81 Bernstein, M. "TCP Standard Initial Version". TM/7038/207/00 for Contract DCA-80-C-0044 [1981].

CLAR80 Clark, Don. Message Protocol Requirements. Volume 1. McLean, VA.: System Development Corporation [1981].

DCA370 DCS AUTODIN Interface and Control Criteria. DCA Circular 370-D175-1. Defense Communications Agency [1970].

GOOD80 Goodwin, N. C. and Hosmer, S. W. A User-Oriented Evaluation of Computer Aided Message-Handling (MTR-3920). Bedford, Mass: Mitre Corp. [1980].

HEIT80 Heitmeyer, C. L. and Wilson, S. H. Military Message Systems. Present Status and Future Directions IEEE Transactions on Communications, September, 1980, pp. 1645-1654.

ISO80 "Date Processing Open Systems Interconnection -- Basic Reference Model," Draft version of ISO/TC97/SC 16 N 537 Revised November, 1980.

JAN128 Automatic Digital Network (AUTODIN) Operating Procedures JANAP 128. Washington, DC: Joint Chiefs of Staff [1977].

NBS81 National Bureau of Standards, Specification for Message Format for Computer Based Message Systems. Institute for Computer Science and Technology [1981].

POST80 Postel, J. Internet Message Protocol (Internet Experiment Notebook #113). Information Sciences Institute [1981].

ROCAMH Required Operational Capability for Automated Message Handling (DRAFT). New York: WWMCCS System Engineering Organization, and USEUCOM [1980].

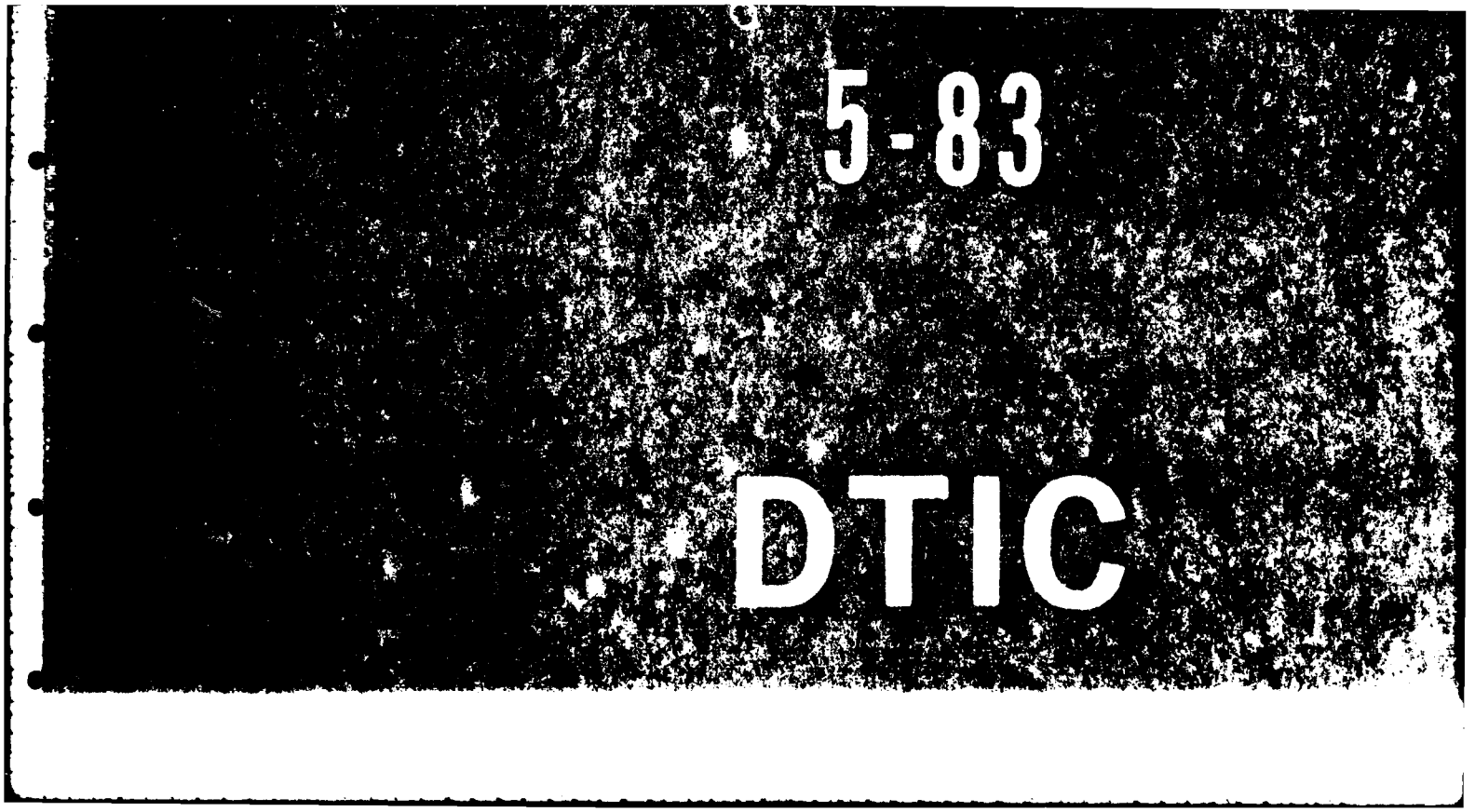
ROTH79 Rothenberg, J., SIGMA Message Service: Reference Manual Version 2.3 (ISI/TM-78-11.2). Los Angeles: Information Sciences Institute [1979].

SAT5 Executive Summary: DCT9000 Standard AUTODIN Terminal (SAT-5) System. Ft. Huachuca, AZ: US Army Communication-Electronics Engineering Agency, Telecommunications Automation Directorate [1979].

SYTEK81 Sytek, Inc., DoD Protocol Architectural Model (Draft). Submitted to System Development Corp. for Contract DCA-80-C-0044 [1981].

TANG77 Tangney, J. D., Ames, S. R., Jr. and Burke, E. L. Security Evaluation Criteria for MME Message Service Selection (MTR-3433). Bedford, Mass.: Mitre Corp. [1979].

WILS77 Wilson, S. H., Ames, S. R., Jr., Tangney, J. D. and Bunch, J. R., Jr. Security/Privacy Evaluation Subcommittee Report on the Candidate Message Service Systems for the Military Message Experiment. Washington, DC: NRL Report 8155 [1977].


5-83
DTIC