CCITT Recommendation X.400

In this report:

Datapro Summary

This report outlines the various segments of the X.400 Recommendation, notably X.409—syntax and notations; X.410—remote operations and Reliable Transfer Server (RTS); X.411—Message Transfer Layer (MTL); X.413—Message Store (MS); X.419—Message Handling System (MHS) application protocols; X.420—Interpersonal Message System (IPM) User Agent Layer (UAL); and X.430—integration of teletex terminals into an IPMS. There is also a discussion of X.500. Work is still being done on the X.400 standard, especially in the MHS area. The MHS applications are being extended, and new work is being done on MHS management—a very dynamic area. Users should recognize that there are two sets of implementation: one from 1984 (the prototype) and another from 1988. The latter standard encompasses over 50 service element additions, most of which address requirements that were not evident in 1984. The 1988 standard includes elements that are crucial for such important applications as Electronic Data Interchange (EDI), standardized mailboxes, and security. Unfortunately, many vendor offerings still reflect only the 1984 version, although there is evidence that this situation is gradually changing.

The Consultative Committee on International Telephony and Telegraphy (CCITT) Recommendation X.400 specifies a set of standards for Message Handling Systems. First formalized in 1984, and supplemented in 1988, X.400 is the first Application layer standard adopted by the industry that conforms to the ISO/OSI seven-layer reference model. The Recommendation assumes growing significance in the United States and Europe, as demand increases for interconnection products and services on both continents, and as vendors respond with applications that conform to the specifications. The most recent CCITT Study Group VII activity centered on the publication in the fall of 1990 of Draft Recommendation X.435, which offers standards for electronic data interchange (EDI).

—By Charles Haggerty
Associate Analyst

This report provides an overview of activity from the X.400 Application Program Interface Assoc. (XAPIA), and X/Open outlines the organizations' latest specifications for the development of electronic messaging applications. These programming interface specifications enable software developers to create electronic mail applications based on international standards, capable of operating independently of computer systems, operating systems, or communications networks.

Announced by XAPIA and X/Open in September 1990, the specifications, which cover X.400 messaging, X.500 directories, and object management, are Messaging Gateway Application Program Interface (API) Version 2, Messaging Application API, Directory Services API, and Object Management API.

The CCITT formally approved Recommendation X.400 for MHS in 1984. The recommendation specifies a set of standards for users and vendors to adopt to ensure global compatibility for electronic mail and other message-oriented information exchanges.

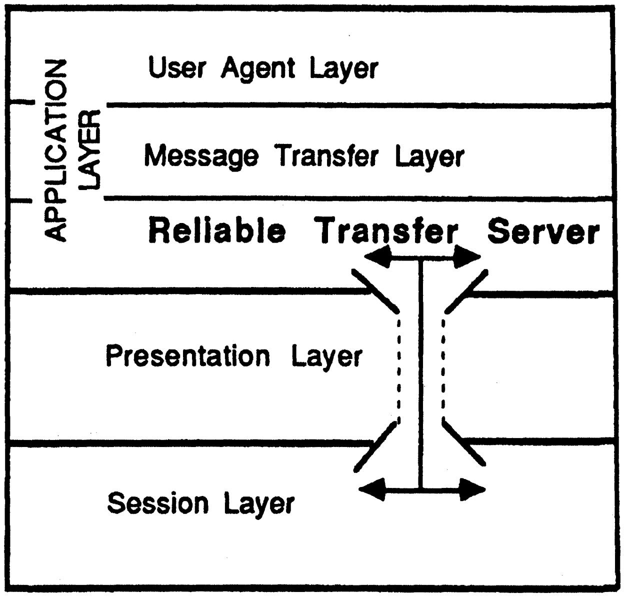
Most major computer system vendors have announced or demonstrated high-level interconnectivity based on X.400 protocols. In addition, a growing number of domestic network facilities vendors have added X.400 interfaces to product offerings in anticipation of new user demand. Together, these developments have provided network managers and integration specialists with sufficient functionality for coordinating private multivendor networks for electronic mail (E-Mail) exchange.

X.400 Standard Set

The X.400 standard is actually a collection of eight CCITT recommendations, ranging from X.400 through X.430. The full set, as published by the CCITT, consists of the following:

- X.400—System Model—Service Elements
- X.401—Basic Service Elements and Optional User Facilities
- X.408—Encoded Information Type Conversion Rules
- X.409—Presentation Transfer Syntax and Notation
- X.410—Remote Operations and Reliable Transfer Server
- X.411—Message Transfer Layer
- X.413—Message Store
- X.419—MHS Application Protocols
- X.420—Interpersonal Messaging User Agent Layer
- X.430—Access Protocol for Teletex Terminals
- X.435—(Draft Recommendation) EDI Messaging Systems

Figure 1.
RTS



The CCITT X.400 Reliable Transfer Server (RTS) is an adaptation of ISO conventions. Unlike pure ISO/OSI applications, it bypasses most of the Presentation layer, calling directly on Session layer services. This implementation has created some controversy, as it presumes the network addresses required for interprocess communications will be maintained in the Application layer. ISO conventions rely on Presentation Addresses to accomplish the same thing.

In addition, there is a separate but related standard—X.500 Directory, which provides "directory assistance" for X.400 communications.

The X.400 MHS is based on specific service protocols imbedded in ISO/CCITT Presentation (layer 6) and Session (layer 5) conventions and on specific refinements of the generalized OSI Application layer model. (See Figure 1.)

Specific features of the X.400 MHS are based on more generic layer 7 conventions, including the CCITT-defined RTS. The standardization of applications, such as X.400 and FTAM, has led to the pursuit of defined modules of functions that are common to those applications. Thus, the RTS has evolved as part of the Application layer for the MHS and represents a logical clustering of functions required for passing information from application to application, expediting access to the Session layer. Currently, this is accomplished by situating the RTS between the MHS's Message Transfer Layer and the Presentation layer, making minimal use of the latter.

Message Handling System Model

Recommendation X.400 describes the system model and service elements that administrations provide for subscribers to exchange messages on a store-and-forward basis. In essence, X.400 MHS conventions provide two fundamental types of Message Handling services—Interpersonal Messaging and Message Transfer (MT).

Interpersonal Messaging is a person-to-person communication of electronic mail. Message Transfer service supports general, application-independent message transfer. Message Handling System, which describes sublayers within the Application layer, supports both services.

An MHS user, depicted in Figure 2, can be either a person or computer application. A corresponding User Agent (UA) represents a user, classified as an originator or a recipient, in the MHS. UAs interact with Message Transfer Agents (MTAs) and with MTAs form the Message Transfer System (MTS). UAs are grouped into classes based on the types of messages they handle; each identifies its class by facilities in the MTS.

Collectively, all these elements make up the Message Handling Environment. Functions performed solely by the UA and not standardized as part of the MH services, such as those proprietary features of a vendor's UA implementation, are called local UA functions.

An originator prepares messages with the assistance of a local UA, which structures the information into envelope and content entities. After the envelope and contents are submitted to the MTS, the MTS initiates a generalized store-and-forward service. The MTS must support both submission and delivery interactions with the appropriate UAs.

Using the relaying interaction and its associated relaying envelope, each MTA passes an outbound message to another MTA until the message is received by the recipient's MTA, where it is delivered to the recipient UA via the delivery interaction. The relaying envelope contains information related to MTS operation, as well as the service elements requested by the originating UA. Generally,

Datapro Information Services Group. Delran NJ 08075 USA

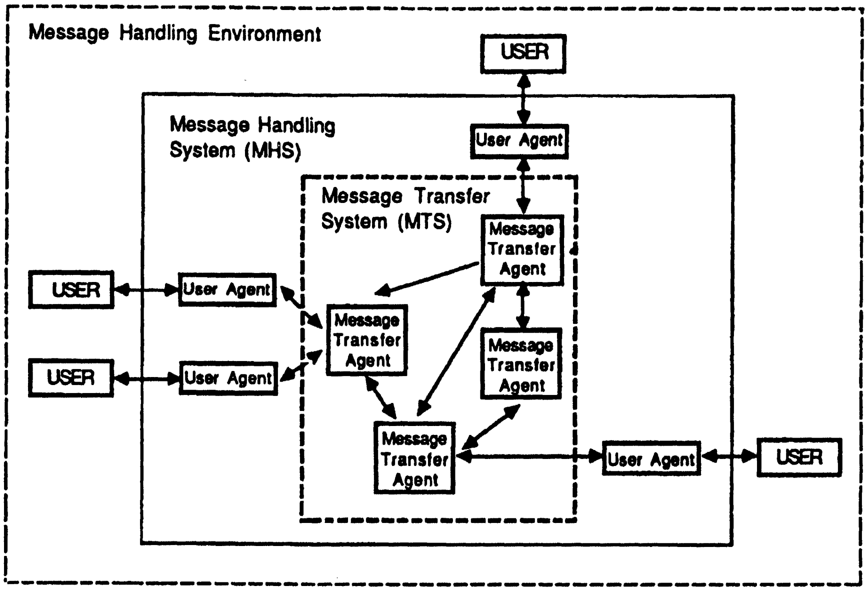


Figure 2.
MHS

The X.400 Message Handling System (MHS) is a conceptual model within the recommendation. The core of the model is the Message Transfer System (MTS), which is composed of Message Transfer Agents. The MHS represents a superset of MTS functionality by providing User Agents (UAs) that present information on behalf of an ISO Application layer user or process via specialized protocols.

MTAs transfer messages of binary information and do not alter or interpret the contents unless instructed by a service element to do so.

Physical Mapping

In addition to performing the various functions required to create, file, or present messages, a UA can also support storage that is useful for managing incoming or outgoing mail. Users interact within the UA via traditional input/output devices, including keyboards, video displays, printers, or facsimile equipment. A UA is thereby implemented as a set of processes in a computer system or intelligent terminal.

There are many valid configurations for UAs and MTAs. For example, a UA and MTA can coreside on a minicomputer system. Alternately, a UA can be implemented on a physically separate device as a standalone process. In this case, the UA communicates with its MTA through standardized protocols specified for Message Handling. An MTA can also exist as a standalone process. Figure 3 shows some of the possible combinations.

Organizational Mapping

Since a large-scale implementation of the MHS often links geographically and logically separate users, some means for distributing system administration tasks are necessary. A Management Domain (MD) fulfills that task. An MD consists of at least one MTA and can contain UAs owned by an organization or public administration. Domains managed by administrations are Administration Management Domains (ADMDs), and those maintained by a private organization are called Private Management Domains (PRMDs).

An administration can provide subscribers with access from combinations of UAs and MTAs, which can cross domain boundaries. Three scenarios are supported:

User to administration-supplied UA: The user's private I/O device, such as a telephone or teletype, interacts with a UA owned by the administration. Alternately, the administration can supply the user with an intelligent terminal.

Private UA to administration MTA: The user's private, standalone UA function in an intelligent workstation or a personal computer interacts with the administration MTA via the standard submission and delivery procedures, required for obtaining Message Transfer Agent service.

Private MTA to administration MTA: A PRMD subscriber owning one or more MTAs and one or more UAs interacts MTA to MTA. This interaction is one of peers, as it also represents an MD-to-MD relationship.

Although the X.400 Recommendation limits a PRMD to existence in one country, it can have access to one or more ADMDs. However, a PRMD cannot act as a relay between two ADMDs. When an ADMD interacts with a PRMD, the ADMD ensures that the PRMD provides valid Message Transfer Service before handing off a message and takes responsibility for the logging, accounting, quality, and other service elements in the transfer. Figure 4 offers a graphical overview of various ADMD and PRMD combinations.

Basic Message Transfer Service

Messages originated or received by the UA are handled in the form of an envelope plus content structure. The interactions are analogous to the ways individuals use public and private services to distribute mail and parcels.

The basic MT service provides the UAs with two-way access to the MTS and assigns each message a unique reference (tracking) identification code. When a message is undeliverable, the MTS informs the originating UA. The UA can specify the encoded types of information within a message, such as original encoded types (text, data, image); times of submission and delivery; and content conversion instructions, such as encryption.

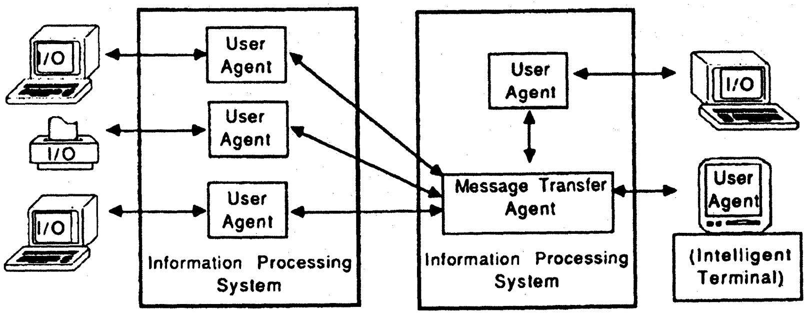
Optional service elements can also be selected: some on a per-message basis, others for a prearranged contractual time period. Table 1 lists basic MTS service elements, grouped according to the five major service types—Basic, Submission and Delivery, Conversion, Query, and Status and Inform. Table 2 lists optional user facilities by per-message and contractual availability. The international availability of service elements is further specified in Recommendation X.401.

Interpersonal Message System

The IPMS incorporates extensions to support its special requirements. It consists of the MTS, a specific class of

Figure 3.
UAs and MTAs

User Agents (UAs) and Message Transfer Agents (MTAs) can have a variety of physical implementations. An Information Processing System can include one or both within its bounds. The UA function could also reside in a dedicated intelligent terminal, such as a personal computer. For now, there are still some practical limitations to overcome before X.400 will support PC users desiring informal, dial-up access.



I/O = Nonintelligent input/output devices.

cooperating UAs (IPM UAs), and items supporting access to telex and CCITT Telematic services (further specified in Recommendation X.430). The general availability of service elements is further specified in Recommendation X.401. Tables 2 and 3 depict optional user facilities offered on a per-message or contractual basis. Table 4 lists basic IPMS service elements, grouped according to the seven major types: Basic, Submission and Delivery, Conversion, Cooperating IPM UA Action, Cooperating IPM UA Information Conveying, Query, and Status and Inform.

As in basic MT service, optional elements are available on a per-message or contractual basis. To assist users with sending and replying to IP messages, the IPM UA can provide a line or full-screen editing capability, as well as notification of pending messages. These and other enhancements to the UA, which can be implemented locally without affecting other UAs, are not subject to CCITT standardization.

The IPMS elaborates on the convention of structuring messages into envelope and content portions, further subdividing the content into heading and body portions, as shown in Figure 5. The resulting structure follows the format of a memo.

Naming Conventions

In order to facilitate the execution of various MTS and IPMS service elements, Recommendation X.400 specifies a naming convention, which defines originator/recipient (O/R) names, O/R name attributes, forms, routing, and distribution lists. A directory function is mentioned, and wish list attributes are enumerated.

Usernames, which are the basis for addressing messages, can be primitive and/or descriptive. A naming authority, which assigns primitives, must ensure that they are unique within that authority's administrative domain. An example of a primitive name is an employee number. A descriptive name must also denote exactly one user, as in The Executive Director of Data Processing for XYZ Hospital.

Descriptive names identify an entity by specifying one or more of its attributes and also specify a set known as an attribute list. Since users are outside the MHS, an originator's UA must provide the MTA with a descriptive name, used to route the message to the recipient's UA. Thus, an O/R name could also be an O/R address, and the MTS could use it to locate the UA's point of attachment.

The CCITT has defined four categories of standard O/R attributes: Personal, Geographical, Organizational, and Architectural. A base attribute set is a minimum grouping required to clearly identify a Management Domain. These attributes include the following:

- Personal—surname, given names, initials, generation qualifiers (Jr., Sr.).
- Geographical—street name and number, town, region, country.
- Organizational—company, decision, position/title.
- Architectural—X.121 address, unique UA identifier (numeric), ADMD name, PRMD name.

Several base attribute sets, with attributes chosen from each of the four categories, can be specified for the MHS. The choice of which one(s) to implement is left to the MD, but X.400 lists four that are of the most interest:

- Commercial—organization and country names.
- Residential—region and country names.
- Architectural—country and MD names.
- Terminal oriented—X.121 address, telex address, or Telematic terminal ID.

For initial service, each MD supports two base attribute sets: the Architectural and Terminal oriented. Support is specified as the ability to relay a message to a destination MD when passed from another MD, except for PRMDs, which are not required to relay between ADMDs; identification of the MD of the recipient UA by at least one base attribute set of the MD's choice; and user designation of recipients by either of the two base attribute sets.

Initially, two forms of O/R name (Form 1 and Form 2) are supported. The first form specifies the originator or recipient by means of the country or ADMD to which the user belongs. Three variants exist for the first form, using combinations of the various attributes found in the base attribute sets. A second form consists solely of the X.121 address and an optional Telematic terminal identifier.

Routing occurs only within the context of O/R addresses that provide the MTS with enough information to route the message between originating and receiving MDs.

Routing within an MD is cited as beyond the scope of Recommendation X.400. Routing is handled by the designer of the MD's communications architecture.

Relying on base attribute sets, the linking MDs route messages until they arrive at the destination MD. At this point, the user attributes in the O/R address are interpreted to allow further redirection to the recipient UA. The recipient UA checks the correctness of the attributes. If the message is undeliverable, the recipient UA must initiate procedures to notify the originator.

Since the logical routing and assignment of responsibilities are hierarchical, a Management Domain's MTAs and UAs relinquish responsibility as soon as they complete the handoff to the next functional layer. This procedure is the most efficient in terms of overhead and is dictated by the MHS's store-and-forward nature.

The naming convention also specifies distribution lists. The ability to simultaneously route E-Mail to multiple recipients is of obvious value, and it is an integral feature of the Message Handling Environment. Tables 1 through 3 list many distribution-oriented features.

Layered Representation of the MHS Model

Section 5 of X.400 presents a layered view of the MHS and defines protocols used between peer layers. All MHS entities and protocols reside within the Application layer of the OSI reference model and can be visualized as sublayers within layer 7. This structure gives X.400-oriented applications access to the underlying layers and accomplishes the following:

- Establishes connections between individual systems independently of network topologies or media.
- Establishes session connections for reliable message transfer.
- Signals the use of standardized Message Handling Presentation Transfer Syntax as defined in Recommendation X.409.

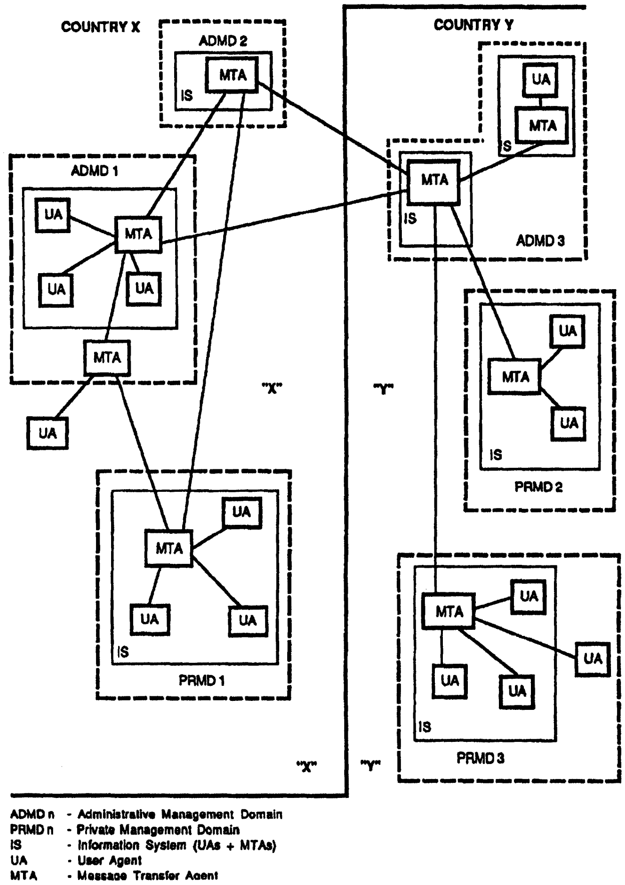
The Message Handling functions in layer 7 consist of two sublayers: a UAL, containing the UA functionality associated with message contents, and a Message Transfer Layer, containing Message Transfer Agent functions supporting the MTS. The layers can be directly related to the functional model, based on S1, S2, and S3 systems. S1 systems contain only UA functions, S2 systems contain only MTA functions, and S3 systems contain UA and MTA functions.

Figure 6 depicts the S1, S2, and S3 types and the protocols used with them. The User Agent Entity (UAE) represents the UA when some type of UA-to-UA protocol takes place. Technically, it is distinguished from the complete UA as being only the *functionality* in a UA that represents a user while interacting with another cooperating UA.

Similarly, the Message Transfer Agent Entity (MTAE) supports the layer services of the MTL in cooperation with other MTAEs. A Submission and Delivery Entity (SDE) makes the services of the MTL available to a UAE through the MTL boundary. The SDE does not provide the services, but interacts with the peer MTAE to provide access to the MTAE.

These entities require three peer protocols—P1, P2, and P3. The Message Transfer Protocol (P1) defines relaying of messages between MTAs and other interactions required for MTL services. P1 messages consist of the original message contents plus a relaying envelope. The X.411 Recommendation specifies P1 protocol in detail. Recommendation X.410 specifies how the Application layer uses the OSI layers for reliable transfer and defines the Reliable Transfer Server and remote operations protocols.

Figure 4.
X.400 Domains of Control



X.400 Domains of control are either Administrative or Private. An Administrative Management Domain (ADMD), essentially a public utility, provides MHS service to subscribers, which can reside as standalone UAs or within Private Management Domains (PRMDs). Note that an ADMD is the only MD specified to provide service between countries and between Private Domains.

The P1 protocol reports only between MTAs. Of the OSI Application layer protocols, it is the only one not using the Remote Operations Service Element (ROSE). As a result, an MTA cannot signal back problems or positively acknowledge an MTA-MTA receipt. Flow control, also, is not possible. It has, therefore, been suggested that P1 be updated and respecified as a ROSE-based protocol so these problems can be corrected. So far, however, no steps have been taken in this direction.

The Interpersonal Messaging Protocol (P2), specified in X.420, consists of a set of protocol elements with standardized syntax and semantics. These protocol elements form the contents of messages exchanged between IPM UAEs. The operations relating to the exchange of P2 protocol elements between an IPM UAE are also defined. P2 defines rules that an IPM UAE must follow when it requests MTL Service in the course of supporting IPM Service. Figure 7

Table 1. X.400 Message Transfer Service Elements

Service Group	Service Elements
Basic	Access Management Content Type Indication Converted Indication Delivery Time Stamp Indication Message Notification Nondelivery Notification Original Encoded Information Types Indication Registered Encoded Information Types Submission Time Stamp Indication
Submission and Delivery	Alternate Recipient Allowed Deferred Delivery Deferred Delivery Cancellation Delivery Notification Disclosure of Other Recipients Grade of Delivery Selection Multidestination Delivery Prevention of Nondelivery Notification Return of Contents
Conversion	Conversion Prohibition Explicit Conversion Implicit Conversion
Query	Probe
Status and Inform	Alternate Recipient Assignment Hold for Delivery

depicts the layered representation of the IPM.

The Submission and Delivery Protocol (P3) allows the SDE in an S1 system to provide its UAE with access to the MTL and its services. It is also defined in X.411. Its use of the ISO stack is defined in X.410.

Management Considerations

Work is only now beginning in managing MHS components within a standardized form using OSI Systems Management. One current proposal involves an MHS Management Overview to provide a top-level "driver" for MHS Management, complemented by an MHS Management Structure document that details the MHS management information structure and gives managed object definitions.

X.401

Recommendation X.401 defines the Basic Service Elements and Optional User Facilities of those services. Certain elements of each service, inherent in the MHS, are classified as basic MT or IPM services. Other service elements are optional, and the user can select them on a per-message or contractual (time period) basis. Of the optional elements, some are specified by X.401 as essential optional; others are additional optional. Essential optional items can be added to the inherent items but must be offered internationally by administrations, such as PTTs. Additional optional elements are truly optional, as administrations may or may not make them available nationally; they can also be available internationally via bilateral agreement.

X.408

Recommendation X.408 specifies rules for encoding various information types into a universal format that can be freely interchanged among the physical input/output devices covered in the MHS recommendation. Nine types of information are cited, but conversion between some of the combinations is cited "for further study." The nine information types are:

- Telex—Code defined in F.1; format in S.5.
- International Alphabet #5 (IA5) Text—Code defined in T.50.
- Teletex—Code defined in T.61; format defined in F.200 and T.60.
- G3 Facsimile—Code defined in T.4; signaling in T.30.
- Text Interchange Format 0 (TIF0)—Code and format defined in T.73.
- Videotex—Code defined in T.100 and T.101.
- Voice—Encoding for further study.
- Simple Formattable Document (SFD)—Code defined in T.61; format in X.420.
- Text Interchange Format 1 (TIF1)—Code and format defined in T.73.

Table 2. X.401 MT Optional User Facilities (per Message)

MT Optional User Facilities	Categorization
Alternate Recipient Allowed	E
Conversion Prohibition	E
Deferred Delivery	E
Deferred Delivery Cancellation	E
Delivery Notification	E
Disclosure of Other Recipients	E
Explicit Conversion	A
Grade of Delivery Selection	E
Multidestination Delivery	E
Prevention of Nondelivery Notification	A
Probe	E
Return of Contents	A

E—Essential optional facility.
A—Additional optional facility.

The rules also point out that any existing standards outside the recommendation are preserved in conversion implementations. Recommendation X.408 also includes several matrices of conversion detail.

X.409

This recommendation offers a methodology for the actual encoding of binary or character information, required before passage through the MHS. It defines a presentation transfer syntax for Application layer protocols used by the MHS and Telematic Services Document Interchange Protocol. Those familiar with IBM's DIA/DCA protocols will recognize X.409 as the CCITT's approach to similar requirements, but on an international, multivendor scale.

X.409 uses the Backus-Naur Form (BNF) notation for expressing information. The BNF description of any formal language comprises a series of replacement rules called productions. Adherence to the replacement rules produces valid instances of the language.

X.410

X.410 defines Remote Operations, used to structure interactive Application layer protocols such as P3 (Submission and Delivery). It also describes the Reliable Transfer Server mechanism between peer entities, which uses message handling protocols such as P1. In addition, it describes the notation of protocol data units used by Remote Operations, the service primitives used to describe reliable transfer, and the use of P1 and P3 protocols to access the OSI Presentation and Session layers.

The concept of remote operations and remote errors facilitates the specification and implementation of interactive protocols. These logical representations of any interactive communication action occur as one Application Entity (AE) requests another to perform an operation. The obliging AE, in turn, attempts to perform the operation and then reports the outcome as a success or failure. Operation Protocol Data Units (OPDUs) invoke, then return, result or return error conditions.

The Reliable Transfer Server is the part of the AE that creates and maintains associations between the AE and its peers and passes Application Protocol Data Units (APDUs) between them. The associated APDUs and OPDUs conform to the BNF notation described in Recommendation X.409. Service primitives describe the interactions between an RTS and its user. Based on Session layer services, they use sets of tokens to determine the sequence of turns at invoking services from the remote entity. For example, a PLEASE token can request a turn; a GIVE token can grant a turn. Service primitives, such as OPEN, CLOSE, TURN-PLEASE, TURN-GIVE, EXCEPTION, and RECOVER, thus translate into similar Session layer service requests. Other important facets of service primitives include the passing of additional session-related information, such as major and minor checkpoint (synchronization) sizes and initial token possession. Important features of the RTS are its support of session recovery and data transfer restart (from last checkpoint).

Recommendation X.410 specifies the subset of the OSI session tokens required for RTS operation and defines several valid states in which the RTS and its user can exist, depending on specific possession of various tokens at given times. Thus, the primitives are really abstractions representing logical uses of lower-level services.

X.411

Recommendation X.411 defines the Message Transfer Layer and the types of services it supports in a practical message handling system. The service primitives presented for the MT Layer are again abstractions and thus resemble X.410 RTS primitives in their form. Protocol data units are also described in BNF notation.

LOGON, LOGOFF, REGISTER, CHANGE PASSWORD, CONTROL, SUBMIT, PROBE, DELIVER,

Table 3. X.401 MT Optional User Facilities (Contractual)

MT Optional User Facilities	Categorization
Alternate Recipient Assignment	A
Hold for Delivery	A
Implicit Conversion	A

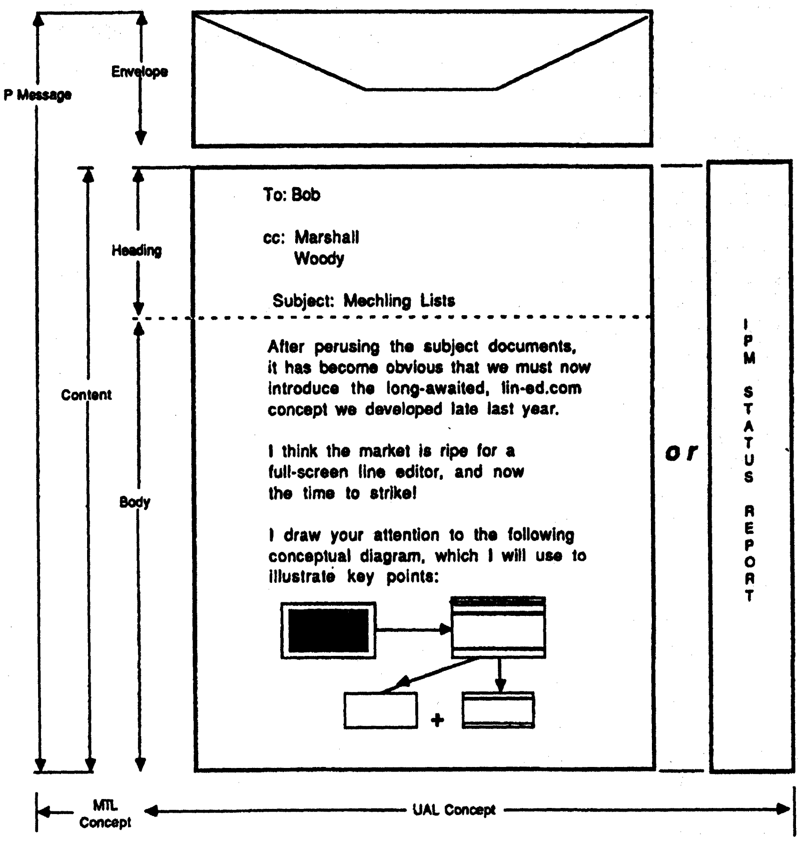
E—Essential optional facility.
A—Additional optional facility.

Table 4. Interpersonal X.400 Messaging Service Elements

Service Group	Service Elements
Basic	Basic MT Service Elements (MTS) IP-Message Identification Typed Body
Submission/Delivery and Conversion *(MTS)*	*(See Table 1)*
Cooperating IPM UA Action	Blind Copy Recipient Indication Nonreceipt Notification Receipt Notification Auto Forwarded Indication
Cooperating IPM UA Information Conveying	Originator Indication Authorizing Users Indication Primary and Copy Recipients Indication Expiry Date Indication Cross-Referencing Indication Importance Indication Obsoleting Indication Sensitivity Indication Subject Indication Replying IP-Message Indication Reply Request Indication Forwarded IP-Message Indication Body Part Encryption Indication Multipart Body
Query *(MTS)*	*(See Table 1)*
Status and Inform *(MTS)*	*(See Table 1)*

Figure 5.
Interpersonal Messages

Interpersonal Messages consist of Envelopes and Contents. The contents can be either the Heading and Body of a true IP message or a Status Report about the message. Note that text, data, and image can be mixed within an IP message. In cases where a user enables automatic forwarding, rerouting information is appended to the Heading to support successful delivery.



To: Bob

cc: Marshall
Woody

Subject: Mechling Lists

After perusing the subject documents, it has become obvious that we must now introduce the long-awaited, lin-ed.com concept we developed late last year.

I think the market is ripe for a full-screen line editor, and now the time to strike!

I draw your attention to the following conceptual diagram, which I will use to illustrate key points:

NOTIFY, and CANCEL primitives are defined. The concept of a PROBE is introduced, which effectively tests the validity of a service requested by an AE, before causing the MHS to incur the overhead associated with its transfer. In essence, it tests to see if there is a mailbox before licking the stamp.

NOTIFY sends an acknowledgment of the success or failure of a delivery attempt. CONTROL allows a user to specify the times for, and types of, messages being accepted. REGISTER allows users to change their subscription profiles for services and options.

The Message Transfer Protocol, P1, is specified as supporting services that require coordination between cooperating Message Transfer Agent Entities. It is used, therefore, for communications between different Administration Management Domains and between a Private Management Domain and an ADMD. The protocol elements of P1, called Message Protocol Data Units (MPDUs), can be User MPDUs (UMPDUs) or Service MPDUs (SMPDUs). UMPDUs carry messages submitted by a UAE for transfer and delivery to another UAE. SMPDUs convey information about the messages. Relaying and multiple delivery are supported.

An MTAE executing the P1 protocol has three logical parts. The Message Dispatcher performs the P1 protocol actions dictated by the MPDUs received from other MTAEs or those resulting from messages submitted by its own UAEs. The Association Manager, which compares with the ASE of Figure 1, manages the establishment, control, and release of associations provided by the Reliable Transfer Server. All three are shown in a layered model in Figure 8.

X.413

This recommendation defines the services of the Message Store, which serves in an intermediary role between the user agent and the MTS. A user agent is an application process that interacts with the MTS to submit messages. Its primary function is to accept delivery of messages on behalf of a single MHS end user and to retain them for subsequent retrieval by the end user's UA. The MS also provides indirect message submission and message administration services to the UA, via "pass-through" to the MTS. Like the UA, the MS acts on behalf of a single end user and does not provide a common or shared multiuser MS service.

Message Store (MS) Ports

An MS provides the Retrieval, Indirect-submission, and Administration ports to the MS service user. Although the indirect-submission and administration capabilities of the MS service are the same as those provided by other components of an MHS, the retrieval capabilities are unique to the MS. These capabilities include obtaining information on, fetching, and deleting messages residing in the MS. Additional capabilities register certain MS-provided automatic actions.

Before providing an MS user with any retrieval capabilities, the MS authenticates the user by means of the Bind-operation. Similarly, the MTS must authenticate the MTS service user before it extends its services. All the services provided by the MS, with the exception of the Alert service, are invoked by the user.

In addition to supplying the Retrieval port services to its user and acting as a surrogate MTS service provider, supplying the MTS submission and administration services to its user, the MS, acting as a surrogate UA, also uses the MTS Delivery port, Submission port, and Administration port services.

MS Information Model

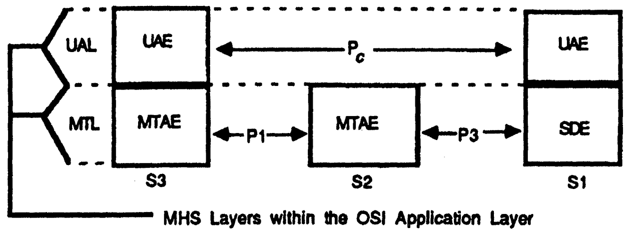
The MS stores and maintains *Information bases*, which consist of *entries* that, in turn, consist of *attributes*. An Information base in the MS is a database containing all the entries that represent constituent objects of a particular category or categories. There are various kinds of Information bases, but this recommendation describes the *Stored message Information base.*

Each Information base is organized as a sequence of entries, with each entry representing a single object, such as a delivered message, within the Information base. Each entry is identified by means of a sequence number, unique within the Information base, which is generated as new entries are created. The MS generates these sequence numbers in ascending order without cycling, and they are never reused.

All entries consist of a set of attributes, with each attribute providing a piece of information about, or derived from, the data to which the entry corresponds (e.g., the sequence number of the entry or the creation time). An attribute consists of an attribute type, which identifies the class of information given by an attribute (e.g., a message's priority), and the corresponding attribute value(s), which are particular instances of that class appearing in the entry (e.g., urgent). All attributes in an entry must be of distinct attribute type; attribute types that contain a single attribute value are said to be single valued, while those with more than one are multivalued. Certain general-purpose attribute types for the Stored messages Information base, defined in the X.413 recommendation, are called general attribute types, and their attributes are known as general attributes.

Although entries in a single Information base are generally independent of each other, the MS information model supports tree-structured relationships among entries, with one entry (a child entry) being the child of another (a parent entry). An entry that is not a child entry is termed a main entry. The operations of the MS service act by default only on main entries, although some can be directed to act on all entries.

Figure 6.
MHS Elements



S1 - Systems with only UA functions
S2 - Systems with only MTA functions
S3 - Systems with both UA and MTA functions
UAE - User Agent Entity
MTAE - Message Transfer Agent Entity
SDE - Submission and Delivery Entity
P1 - Message Transfer Protocol
P_C - Range of Protocols defining message content
P3 - Submission and Delivery Protocol

The generic MHS elements support the possible physical mappings of Figure 3 as a general structure on which specialized implementations can be built. Pc is, therefore, a range of protocols, any one of which will support protocol data transfer between Cooperating UAs.

The Stored message Information base acts as a repository for information obtained from the Message Delivery and Report Delivery operations of the Message Delivery Port. It contains entries for delivered messages and notifications. Entries are created by the MS when a message is delivered or a notification arrives at the MS.

Retrieval Port Operations

The **Summarize Operation** returns summary counts of selected entries in an Information base. In addition, a count of the entries selected and their lowest and highest sequence numbers are also returned. Zero or more individual summaries can be requested. This operation will be successful only when the Information base permits access according to the security context and enforced security policy. The attributes that can be used for summaries are restricted.

The **List Operation** searches a selected Information base for entries and returns selected information from them. This operation will be successful only when the Information base permits access according to the security context and enforced security policy.

The **Fetch Operation** returns selected information from a specific entry in the Information base. Alternately, it returns selected information from the first entry among several entries of interest. Information from an entry can be fetched several times until the entry is explicitly deleted via the Delete Operation. This operation will be successful only when the Information base permits access according to the security context and enforced security policy.

The **Delete Operation** is used to delete selected entries from an Information base. A main entry and all its child entries can be deleted together only by specifying the main entry as the argument of command. For specific Information bases, there may be restrictions on which entries can be deleted. For stored messages, no entry can be deleted if its entry status is new. This operation will be successful only when the Information base permits access according to the security context and enforced security policy.

The **Register-MS Operation** registers or deregisters auto actions, default lists of attribute types, new credentials, and new sets of user security labels.

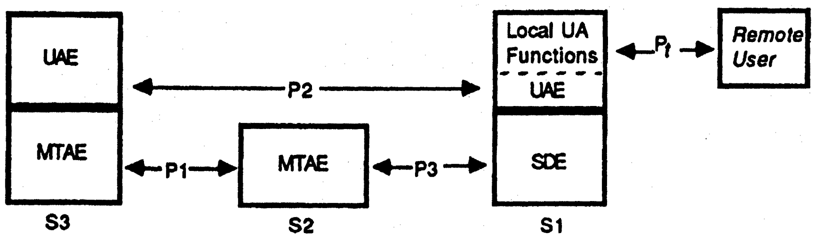
The **Alert Operation** enables the MS service provider to inform its user immediately of a new entry that has been entered into the MS, whose attributes match the selection criteria of one of the auto alert-registrations previously supplied using the Register Operation. This operation can be invoked during an existing association initiated by the UA, but only when new entries have been entered after the establishment of the association. This operation will be successful only when the Information base permits access according to the security context and enforced security policy.

Message Store Extension

Since its inception in 1988, the MS has been regarded as providing a rather limited set of protocols. Work to provide a more complete set of specifications has been ongoing and is referred to as the MS extension. Its main goal is

Figure 7.
IPMS

The IPMS is actually a special case of the generalized MHS depicted in Figure 7. The P2 protocol is the first protocol specified in the Pc range. Protocol Pt is not actually specified in X.400, but can be chosen from a suite of existing interactive terminal protocols from other CCITT recommendations.



P1 - Message Transfer Protocol
P2 - Interpersonal Messaging Protocol ***(from P_C)***
P3 - Submission and Delivery Protocol
P_t - Interactive Protocols unspecified within X.400

to let the user access a managed store of messages by standardized protocols. More specifically, with the MS extension, the user should be able to do the following: instruct the MS to store a message after it has been successfully submitted, then search for and retrieve submitted messages; place submitted and delivered messages into user-created message groups; specify in what order messages are stored; assign group names to messages based on the characteristics of the messages; determine that a stored messages may be deleted after a specified lifetime; stop composing a message and resume later, perhaps from another location; attach notes to messages; and store documents that have been conveyed via MHS in a document store.

Some draft work regarding these measures has been done, but none of them has yet been implemented.

X.419

This recommendation specifies the following MHS application protocols:

- The MTS Access Protocol (P3) used between a remote User Agent and the MTS to provide access to the MTS service,
- The MS Access Protocol (P7) used between a remote User Agent and an MS to provide access to the MS service, and
- The MTS Transfer Protocol (P1) used between MTAs to provide the distributed operation of the MTS.

The recommendation describes how the MTS service, the MS service, and the MTA service are supported by instances of OSI communications when a service user, a service provider, or (in the case of the MTA service) the MTAs are realized as *application processes* located in different open systems.

Protocols and Services

In the Open Systems Interconnection (OSI) environment, communication between applications processes is represented in terms of communication between a pair of *application entities (AEs)* that use the presentation service. These AEs consist of a set of one or more *application service elements (ASEs)*, and the interaction between AEs is described in terms of their use of the services provided by the ASEs. Access to the MTS service is supported by three ASEs, each of which supports a type of port paired between a user and the MTS (as defined in Recommendation X.411).

The **Message Submission Service Element (MSSE)** supports the services of the Submission-port.

The **Message Delivery Service Element (MDSE)** supports the services of the Delivery-port.

The **Message Administration Service Element (MASE)** supports the services of the Administration-port.

The MTS service is supported by only one ASE.

The **Message Transfer Service Element (MTSE)** supports the services of the Transfer-port (as defined in Recommendation X.411).

Access to the MS service is also supported by three ASEs, with the MSSE suppporting the services of the Indirect-submission-port, the MASE supporting the services of the Administration port, and the Message Retrieval Service Element (MRSE) supporting the services of the Retrieval-port (as defined in Recommendation X.413).

The MSSE, MDSE, MRSE, and MASE are asymmetric ASEs; i.e., the user ASEs act as the consumer, and the MTS and MS ASEs act as the supplier of the services. Along with the services provided by the ASEs, the three protocols also comprise the operations that provide the appropriate Bind and Unbind services.

Underlying Services

The ASEs previously described are in turn supported by other ASEs. The **Remote Operations Service Element (ROSE)** supports the request/reply functions of the remote operations that occur at the ports. The ROSE supports only the ASEs that provide access to the MTS and MS services, i.e., the MSSE, MDSE, MRSE, and MASE. These ASEs map the syntax notation of a service onto the services provided by the ROSE. The remote operations of the MTS Access Protocol (P3) are asynchronous operations (Class 2), and those of the MS Access Protocol (P7) are synchronous operations (Class 1).

The **Reliable Transfer Service Element (RTSE)** reliably transfers the *Application Protocol Data Units (APDUs)* that contain the parameters of the operations between AEs. The RTSE is mandatory for the support of the MTS Transfer Protocol (P1) since it does not use the ROSE, but it is optional for the P3 and P7 protocols. The RTSE recovers from communications and end-system failure and minimizes the amount of retransmission needed for recovery.

The **Association Control Service Element (ACSE)** supports the establishment and release of an application association between a pair of AEs. Associations between a user and the MTS can be established by either, while those between a user and the MS can be established only by the user.

The combination of one or more of the ASEs for the MTS and MS Access Protocols, together with their supporting ASEs, defines the application context for the MHS Access Protocols, while the MTSE and the supporting RTSE define that for the MTS Transfer Protocol. The MHS protocols also make use of the services provided by the lower levels of the OSI model.

Protocol Syntax

The syntax of the MHS protocols is defined by the syntax notation ASN.1 specified in CCITT Recommendation X.208 (ISO 8824) and the remote operation notation defined in the Recommendation X.218.

The syntax definition of the MTS Access Protocol (P3) has the following major parts:

- *Prologue:* declarations of the exports from, and imports to, the MTS Access protocol module,
- *Application Contexts:* definitions of the application contexts that can be used between an MTS user and the MTS,
- *Message Submission Service Element:* definitions of the MSSE, its remote operations, and errors,
- *Message Delivery Service Element:* definitions of the MDSE, its remote operations, and errors, and
- *Message Administration Service Element:* definitions of the MASE, its remote operations, and errors.

The syntax definition of the MS Access Protocol (P7) has the following major parts:

- *Prologue:* declarations of the exports from, and imports to, the MS Access Protocol module,
- *Application Contexts:* definitions of the application contexts that can be used between an MS user and the MS,
- *Message Submission Service Element:* definitions of the MSSE, its remote operations, and errors, and
- *Message Retrieval Service Element:* definitions of the MRSE, its remote operations, and errors.

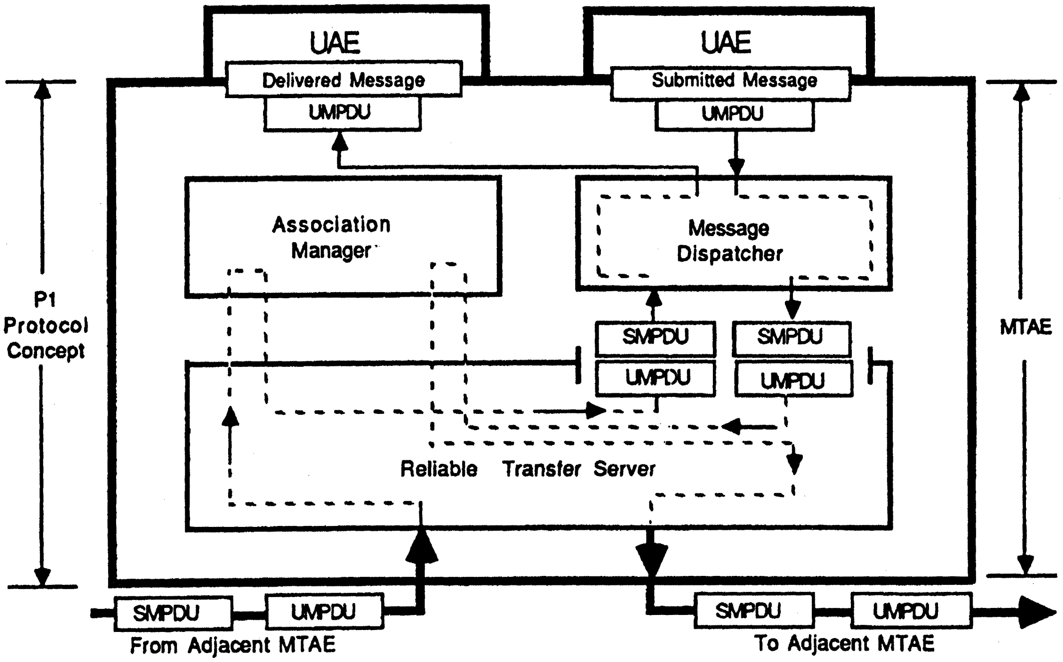
The syntax definition of the MTS Transfer Protocol (P1) has the following major parts:

- *Prologue:* declarations of the exports from, and imports to, the MTS Transfer Protocol module,
- *Application Contexts:* definitions of the application contexts used between MTAs,
- *Message Transfer Service Element:* definitions of the MTSE, and
- *MTS Application Protocol Data Units:* definitions of the MTS APDUs, i.e., Message, Probe, and Report.

X.420

Recommendation X.420 describes the Interpersonal Messaging User Agent Layer for the MHS and its associated protocol data units. It also specifies the representation used for transmitting Simple Formattable Documents (SFDs). The IPM Service provides the mechanisms through which users can exchange interpersonal messages.

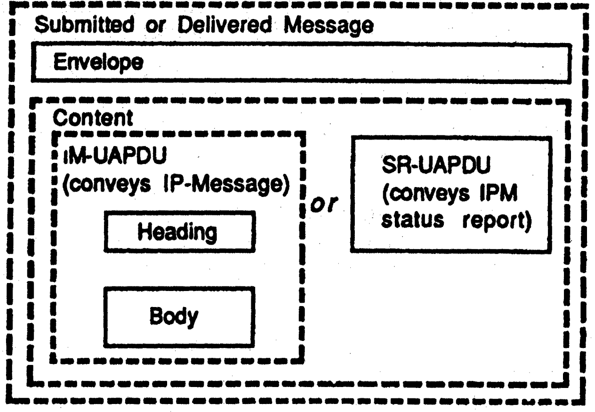
Figure 8.
The Association Manager



UMPDU-User Message Protocol Data Unit
SMPDU-Service Message Protocol Data Unit

The Association Manager manages the use of Session layer connections required for message transfer. The Message Dispatcher passes P1 protocol data to and from the Reliable Transfer Server and the involved User Agent Entities.

Figure 9.
Recommendation X.420



IM-UAPDU - Interpersonal Message User Agent Protocol Data Unit
SR-UAPDU - Status Report User Agent Protocol Data Unit

Recommendation X.420 goes into great detail to specify the Protocol Data Units required for Interpersonal Messaging Service. The items within solid boxes represent actual MTL or UAL defined elements. The items within the dashed boxes are abstractions of these items.

Certain additions to the basic MHS are incorporated to support IPMS, which is actually just a special case of MH System use.

The two types of IPM contents are described as User Agent Protocol Data Units (UAPDUs), IP-message (IM-UAPDUs), and IPM-status-report (SR-UAPDUs). IM-UAPDUs contain the actual message content, including the heading and body; SR-UAPDUs contain status and reporting information, including the success or failure of a delivery attempt. Figure 9 breaks out IPM components with respect to UAPDUs.

IPM UAEs access the MTL in much the same way as basic UAEs do, using a very similar set of primitives (LOGON, CHANGE PASSWORD, SUBMIT). Because of the nature of IPM service, a number of other parameters supporting postal and corporate memo-type services, such as deferred delivery, carbon copy, blind carbon, and forwarding, are also accommodated.

The SFD concept is analogous to IBM's revisable form document concept. SFDs are minimally formatted text segments that conform to prescribed standards, ensuring revisability by the receiving UA process. This is an important consideration, since it makes text exchange possible between otherwise incompatible systems. SFD implementation conforms to a number of structure and content notation conventions, which are also described via the BNF notation.

X.430

This recommendation deals with integrating Teletex (TTX) terminals into an IPMS. To facilitate this integration, special variants to IPMS service elements are defined. Figure 10 shows the relationships of IPMS components, including Teletex and Telematic elements.

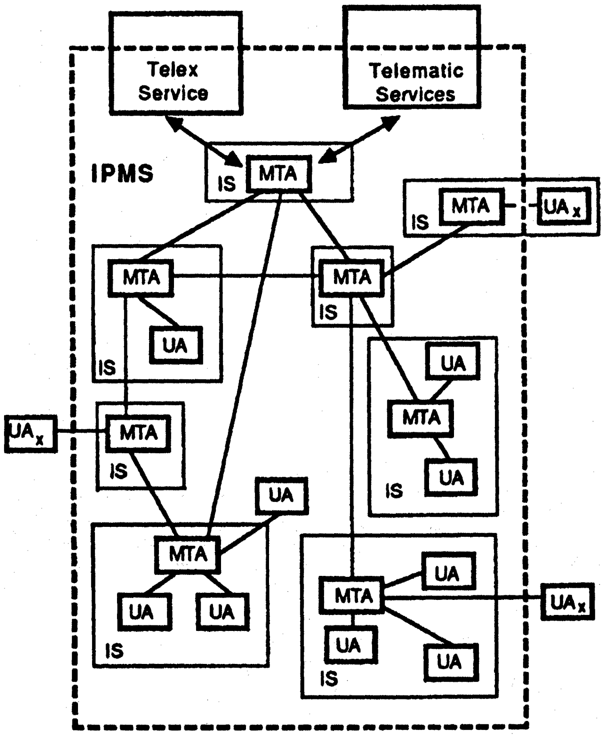
A Teletex Access Unit (TTXAU) is added to the Message Handling System model to give TTX units access to the Message Transfer System entities used by other IPMS terminals. It supports TTX terminals on a one-to-one basis, using the Teletex Access Protocol (P5). The TTXAU can also provide a Document Storage (DS) facility to accept delivery of messages from the MHS for the TTX terminal. Figure 11 shows the recommended relationship between the IPMS and existing Teletex networks.

X.435

Study Group VII published draft recommendations in the fall of 1990 that covered Electronic Data Interchange (EDI) messaging systems. Completing work begun in the spring of 1988, Study Group VII spent five meetings drafting Recommendation X.435. Since the group reached the decision to base the EDI/X.400 service on the concept of user agent services, the group defined a protocol and content type for EDI. Participants at the next to the last meeting decided to use Message Store (MS) to accommodate EDI transmissions. The draft recommendation enables originators in EDI transactions to be notified when EDI recipients have taken over the EDI message.

At the NIST OSI Implementors Workshop (OIW) in Gaithersburg, MD, in April 1992, the X.400 Special Interest Group discussed agreements for the X.435 standard for EDI messaging. X.435 facilitates the transmission of EDI between administrative management domains; this is the

Figure 10.
An Overview of the Complete IPMS Model



IS - Information System (UAs + MTAs)
UA - User Agent
MTA - Message Transfer Agent
UA_x - Non-Cooperating UA (outside of IPMS)

Note that some User Agents (UAs) are noncooperating: They support basic MHS service but not the specialized IPMS service. Also, note that the noncooperating UAs are not distinguished by any peculiarities of physical mapping; standalone UAs can be either cooperating or not cooperating.

first part of the International Standardized Profile for Message Handling Systems, and it is expected to be completed soon.

X.500

A directory service comprises a distributed database that runs on LAN servers. It should constantly update a list of network users and the equipment in the networks. This list may even be specific enough to include printers and individual files. A joint effort between CCITT and ISO, X.500 specifies which functions a directory service should provide; it also ensures interoperability among services from different vendors.

X.500 Components

X.500 consists of the following major elements:

Users: The X.500 Recommendation regards users as objects in the network. Although these "objects" can be people, they can also be computer processes or, indeed, anything that operates within the network.

Directory User Agent (DUA): The DUA is the interface between the user and the directory.

Directory System Agent (DSA): The DSA is the DUA's access point into the directory. Because the DSA compiles and owns directory data and maintains the entries in the database, the directory is, in effect, a collection of DSAs.

Directory Access Protocol (DAP): This protocol permits communication between the DUA and the DSA. Owing to the existence of the DAP, the DUA and DSA can be on either the same system or on different ones.

Directory System Protocol (DSP): DSP allows a server to forward requests over an Open Systems Interconnection network to other servers in the network. A company can create one central DSA or several distributed DSAs. Strictly speaking, equipment that is truly X.500 compatible has the DSP on the server.

Directory Information Tree (DIT): This structure makes it possible to maintain and locate information in the directory. It assigns each DSA a unique position. It also groups DSAs into Directory Management Domains.

Distinguished Names: Some central authority within an enterprise must assign a unique name to each object in a Directory Management Domain. This opens up a path along the Directory Information Tree to a specific object.

Directory Schema: Information in the directory is categorized, and the directory schema spells out the rules whereby categories are stored. This allows DUAs to talk to each other.

X-Open Development System: The X-Open Development System comprises application program interfaces for DUA services. With this system, applications that use or access X.500 on one vendor's computer can be used on another's.

Current Status

Generally regarded as a supporting mechanism for X.400, X.500 was first announced in 1988. The original specification, however, failed to define access control, nor did it describe how to replicate directories and data across multiple servers. There has also been criticism of X.500's general complexity and less-than-simple user interface. This has slowed acceptance and lead to some reluctance to accept the X.500 standard itself. It is true that, in 1992, additional X.500 specifications were released that address access control and replication. X.500, however, still falls short of defining the kind of functionality that many vendors want to offer, failing to define, for instance, the various types of objects that manufacturers might have to store in a directory. As a result, some vendors and users do not plan to wait for further X.500 developments, preferring instead to develop proprietary directory technologies. Even these companies, however, are hedging their bets by developing proprietary technologies that support migration to X.500.

So the question comes down to this: "Do I really need X.500?" Users who already have an adequate internal electronic mail directory probably do not require X.500 in the short term. Users who plan to replace their existing directory service, however, and those who currently do not

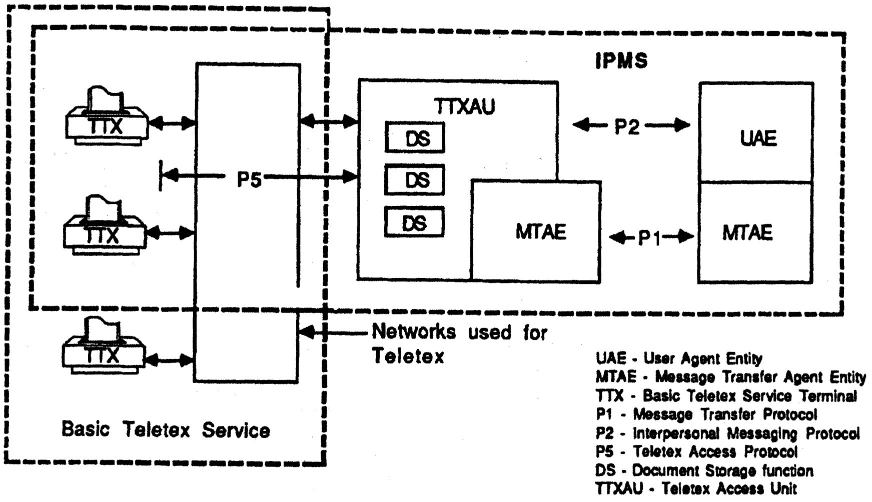

IPMS
TTX
TTX
TTX
P5
TTXAU
DS
DS
DS
MTAE
P2
P1
UAE
MTAE
Networks used for Teletex
Basic Teletex Service
UAE - User Agent Entity
MTAE - Message Transfer Agent Entity
TTX - Basic Teletex Service Terminal
P1 - Message Transfer Protocol
P2 - Interpersonal Messaging Protocol
P5 - Teletex Access Protocol
DS - Document Storage function
TTXAU - Teletex Access Unit

Figure 11.
TTXAU

The Teletex Access Unit (TTXAU) expands the functionality of the MTAE to support terminals of an existing TTX network. Special Document Storage entities spool messages between the TTX terminals and a conventional UAE.

Table 5. X.401 IPM Optional User Facilities

IPM Optional User Facilities (per Message)	Origination by UAs	Reception by USs
Alternate Recipient Allowed	A	A
Authorizing Users Indication	A	E
Auto Forwarded Indication	A	E
Blind Copy Recipient Indication	A	E
Body Part Encryption Indication	A	E
Conversion Prohibition	E	E
Cross-Referencing Indication	A	E
Deferred Delivery	E	Does not apply
Deferred Delivery Cancellation	E	Does not apply
Delivery Notification	E	Does not apply
Disclosure of Other Recipients	A	E
Expiry Date Indication	A	E
Explicit Conversion	A	Does not apply
Forwarded IP-Message Indication	A	E

E—Essential optional facility.
A—Additional optional facility.

have one but plan to implement one, would do well to purchase X.500-compliant products. One leading industry analysis group estimates that, within the next five years, nearly 50% of large companies will be using X.500 with their electronic mail systems.

The North American Directory Forum (NADF) is a vendor consortium that was founded in 1990. Currently comprising 16 members, the NADF includes such organizations as AT&T, IBM, MCI, the U.S. Postal Service, GE Information Services, and Sprint Intl. Early in 1992, the 16 members of the NADF conducted a pilot test of X.500 directory services. The software being tested involved the Directory User Agent and the Directory System Agent (discussed earlier in this section). NADF's ultimate goal is to fine-tune the software and technology related to X.500 to create a global directory that contains electronic mail addresses, telephone numbers, and other user information.

XAPIA and X/Open

In September 1990 the X.400 Application Program Interface Assoc. (XAPIA), an association of leading computer and communications vendors, and X/Open, the international open systems organization, jointly announced the availability of specifications for the development of electronic messaging applications. These programming interface specifications enable software developers to write electronic mail applications based on international standards, capable of operating independently of computer systems, operating systems, or communications networks. The specifications cover X.400 messaging, X.500 directories, and object management. They are the folowing:

Messaging Gateway Application Program Interface (API) Version 2—an API providing definitions for interfacing proprietary mail systems to an X.400 Message Transfer Agent.

Messaging Application API—an API that enables X.400 messaging capabilities, such as submission, delivery, and retrieval, to be incorporated directly into nonmessaging applications, such as word processing and spreadsheets.

Directory Services API—an API that enables global mail directories based on X.500 to be accessed from within these same applications.

Object Management API—an API used by other APIs to provide tools for manipulating complex information objects, such as messages and the results of directory inquiries.

Table 5. X.401 IPM Optional User Facilities (Continued)

IPM Optional User Facilities (per Message)	Origination by UAs	Reception by USs
Grade of Delivery Selection	E	E
Importance Indication	A	E
Multidestination Delivery	E	Does not apply
Multipart Body	A	E
Nonreceipt Notification	A	E
Obsoleting Indication	A	E
Originator Indication	E	E
Prevention of Nondelivery Notification	A	Does not apply
Primary and Copy Recipients Indication	E	E
Probe	A	Does not apply
Receipt Notification	A	A
Reply Request Indication	A	E
Replying IP-Message Indication	E	E
Return of Contents	A	Does not apply
Sensitivity Indication	A	E
Subject Indication	E	E

E—Essential optional facility.
A—Additional optional facility.

Formed in January 1989, the X.400 Application Interface Assoc. includes AT&T, Banyan Systems, British Telecommunications plc, cc:Mail, Data Access, Data Connecttion Ltd., Digital Equipment, Enable Software, GSI/Danet, Hewlett-Packard, Indisy Software, Lotus Development, Microsoft, NCR, Novell, NTT America, OSIware, Retix, Soft-Switch, Sun Microsystems, US Sprint Communications, Tandem, TITN, Touch Communications, and 3Com.

X/Open, founded in 1984, is made up of international computer systems vendors, user organizations, and software suppliers that are investing business, technical, and marketing resources in the specification of the X/Open Portability Guide (XPG), which is a vendor- and product-independent, open operating environment based on de facto and international standards. X/Open members include AT&T, Bull, Digital Equipment, Fujitsu Ltd., Hewlett-Packard, Hitachi, IBM, ICL, NCR, NEC, Nixdorf, Nokia Data, Olivetti, Open Software Foundation, Philips, Prime Computer, Siemens, Sun Microsystems, Unisys, and UNIX International.

European Perspectives

X.400 has had its critics, and even its most fervent adherents will not claim that it is perfect. Nevertheless, no other standard can surpass X.400's capabilities on an international basis.

ENV 41 201 has been the agreed-upon profile in Europe for MHS implementation. This profile covers P1 and P2; it is still used in installations in which 1984-only systems are interconnected. The National Institute of Standards and Technology OSI Implementors Workshop also developed a similar and compatible profile. These profiles form the basis for such government procurement profiles as the U.K. and U.S. GOSIPs.

The European Workshops for Open Systems (EWOS) has done a great deal of work toward developing profiles based on the 1988 recommendations. EWOS intends that there be a family of profiles encompassing the numerous possible interconnection scenarios. EWOS's intention is to create a "kernel" profile that describes basic functionality, supplemented by other profiles for "functionality groups." In other words, a basic set of features is supplemented by optional extensions. Users choose a system that supports the appropriate functions for their needs.

EWOS has specified profile families for P1, P3, and P7; there are variants for interpersonal message systems and electronic data interchanges. Functional groups have been defined for the following: redirection, distribution lists, conversions, physical delivery, use of directory, '84 interworking, and security.

It is expected that ENV 41 214 will soon be published, showing the results of work that has been done on these profiles. Similar work is being done in the NIST/OIW and the Asia/Oceanic Workshop. Attempts are being made to coordinate these efforts, and hopes exist that a single set of International Standardized Profiles will eventually be developed.

The MHS profiles followed by EWOS are rooted in peer-to-peer OSI concepts. They do not accurately reflect the store-and-forward nature of the Message Transfer Agents or the actions of a message store.

Unisource Business Networks is a joint venture between Televerket of Sweden and PTT Telecom Netherlands. Headquarted in Frankfurt, Germany, Unisource was introduced in the summer of 1992 and is offering a range of network services, including X.400, to business customers in Europe. The company has commenced services in Sweden, Germany, the United Kingdom, and the Netherlands. Services will soon be available in Belgium, France, Norway, Denmark, and Finland. Unisource has made a global interconnection agreement with SprintNet, which is Sprint's international data network.

X.400 Sources

Readers who want more complete details of the standards can order and examine copies of the CCITT documents that contain the X.400 MHS specifications. Recommendations X.400, X.401, X.408, X.409, and X.410 are published in Document AP VIII-66-E. Recommendations X.411, X.420, and X.430 are published in Document AP VIII-67-E. Both documents mention others; documents in the series AP VIII-(56-68) make up the complete set referenced. To order copies of CCITT standards in the United States, contact:

United States Department of Commerce
National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
Telephone (703) 487-4650 ■

CCITT Recommendation X.400

In this report:

Synopsis

Editor's Note
The CCITT Recommendation X.400 specifies a set of standards for Message Handling Systems. Formalized in 1984, X.400 is the first Application layer standard adopted by the industry that conforms to the ISO/OSI seven-layer reference model. The Recommendation assumes growing significance in the United States and Europe, as demand increases for interconnection products and services on both continents, and as vendors respond with applications that conform to the specifications. The most recent CCITT Study Group VII activity centered on the publication in the fall of 1990 of Draft Recommendation X.435, which offers standards for electronic data interchange (EDI).

Report Highlights
The report outlines the various segments of the X.400 Recommendation, notably X.409—syntax and notations; X.410—remote operations and reliable transfer server (RTS); X.411—message transfer layer; X.413—message store; X.419—MHS application protocols; X.420—IPM User Agent Layer; and X.430—integration of teletex terminals into an IPMS.

In the report, an overview of activity from the X.400 Application Program Interface Association (XAPIA) and X/Open outlines the organizations' latest specifications for the development of electronic messaging applications. These programming interface specifications enable software developers to create electronic mail applications based on international standards, capable of operating independently of computer systems, operating systems, or communications networks.

Announced by XAPIA and X/Open in September 1990, the specifications, which cover X.400 messaging, X.500 directories, and object management, are Messaging Gateway Application Program Interface (API) Version 2, Messaging Application API, Directory Services API, and Object Management API.

—By Barbara Callahan
Associate Editor

Datapro Information Services Group. Delran NJ 08075 USA

Analysis

The Consultative Committee on International Telephony and Telegraphy (CCITT) formally approved Recommendation X.400 for Message Handling Systems (MHS) in 1984. The recommendation specifies a set of standards for users and vendors to adopt to ensure global compatibility for electronic mail and other message-oriented information exchanges.

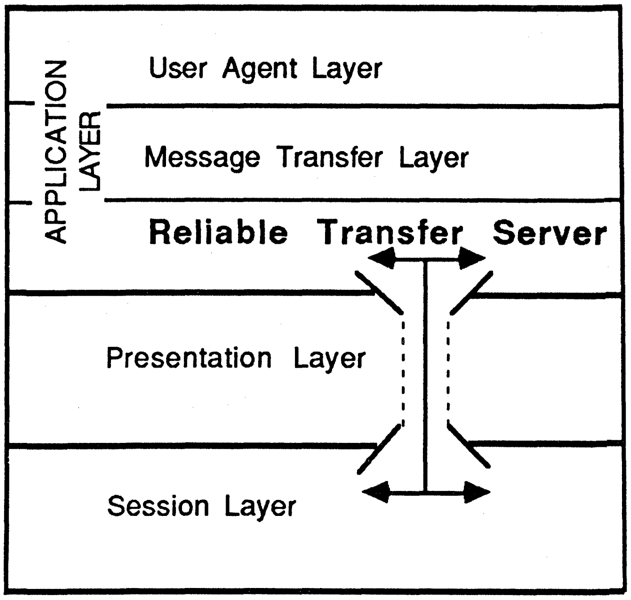
Most major computer system vendors have announced or demonstrated high-level interconnectivity based on X.400 protocols. In addition, a growing number of domestic network facilities vendors have added X.400 interfaces to product offerings in anticipation of new user demand. Together, these developments have provided network managers and integration specialists with sufficient functionality for coordinating private multivendor networks for electronic mail (E-Mail) exchange.

X.400 Standard Set

The X.400 standard is actually a collection of eight CCITT recommendations, ranging from X.400 through X.430. The full set, as published by the CCITT, consists of the following:

- X.400—System Model—Service Elements
- X.401—Basic Service Elements and Optional User Facilities
- X.408—Encoded Information Type Conversion Rules
- X.409—Presentation Transfer Syntax and Notation
- X.410—Remote Operations and Reliable Transfer Server
- X.411—Message Transfer Layer
- X.413—Message Store
- X.419—MHS Application Protocols
- X.420—Interpersonal Messaging User Agent Layer
- X.430—Access Protocol for Teletex Terminals

Figure 1.
RTS



The CCITT X.400 Reliable Transfer Server (RTS) is an adaptation of ISO conventions. Unlike pure ISO/OSI applications, it bypasses most of the Presentation layer, calling directly on Session layer services. This implementation has created some controversy, as it presumes the network addresses required for interprocess communications will be maintained in the Application layer. ISO conventions rely on Presentation Addresses to accomplish the same thing.

- X.435—(Draft Recommendation) EDI Messaging Systems

In addition, there is a separate but related standard—X.500 Directory, which provides "directory assistance" for X.400 communications.

The X.400 Message Handling System (MHS) is based on specific service protocols imbedded in ISO/CCITT Presentation (layer 6) and Session (layer 5) conventions and on specific refinements of the generalized OSI Application layer model. (See Figure 1.)

Specific features of the X.400 MHS are based on more generic layer seven conventions, including the CCITT-defined Reliable Transfer Server (RTS). The standardization of applications, such as X.400 and FTAM, has led to the pursuit of defined modules of functions that are common to those applications. Thus, the RTS has evolved as part of the Application layer for the MHS and represents a logical clustering of functions required for passing information from application to application, expediting access to the Session layer. Currently, this is accomplished by situating the RTS between the MHS' Message Transfer layer (MTL) and the Presentation layer, making minimal use of the latter.

Message Handling System Model

Recommendation X.400 describes the system model and service elements that administrations provide for subscribers to exchange messages on a store-and-forward basis. In essence, X.400 MHS conventions provide two fundamental types of Message Handling (MH) services—Interpersonal Messaging (IPM) and Message Transfer (MT).

Interpersonal Messaging (IPM) is a person-to-person communication of electronic mail (E-Mail). Message Transfer (MT) service supports general, application-independent message transfer. Message Handling System (MHS), which describes sublayers within the Application layer, supports both services.

An MHS user, depicted in Figure 2, can be either a person or computer application. A corresponding User Agent (UA) represents a user, classified as an originator or a recipient, in the MHS. UAs interact with Message Transfer Agents (MTAs) and with MTAs form the Message Transfer System (MTS). UAs are grouped into classes based on the types of messages they handle; each identifies its class by facilities in the MTS.

Collectively, all these elements make up the Message Handling Environment. Functions performed solely by the UA and not standardized as part of the MH services, such as those proprietary features of a vendor's UA implementation, are called local UA functions.

An originator prepares messages with the assistance of a local UA, which structures the information into envelope and content entities. After the envelope and contents are submitted to the MTS, the MTS initiates a generalized store-and-forward service. The MTS must support both submission and delivery interactions with the appropriate UAs.

Using the relaying interaction and its associated relaying envelope, each MTA passes an outbound message to another MTA until the message is received by the recipient's MTA, where it is delivered to the recipient UA via the delivery interaction. The relaying envelope contains information related to MTS operation, as well as the service elements requested by the originating UA. Generally, MTAs transfer messages of binary information and do not alter or interpret the contents unless instructed by a service element to do so.

Physical Mapping

In addition to performing the various functions required to create, file, or present messages, a UA can also support storage that is useful for managing incoming or outgoing mail. Users interact within the UA via traditional input/output devices, including keyboards, video displays, printers, or facsimile equipment. A UA is thereby implemented as a set of processes in a computer system or intelligent terminal.

There are many valid configurations for UAs and MTAs. For example, a UA and MTA can coreside on a minicomputer system. Alternately, a UA can be implemented on a physically separate device as a standalone process. In this case, the UA communicates with its MTA through standardized protocols specified for Message Handling. An MTA can also exist as a standalone process. Figure 3 shows some of the possible combinations.

Organizational Mapping

Since a large-scale implementation of the MHS often links geographically and logically separate users, some means for distributing system administration tasks are necessary. A Management Domain (MD) fulfills that task. An MD consists of at least one MTA and can contain UAs owned by an organization or public administration. Domains managed by administrations are Administration Management Domains (ADMDs), and those maintained by a private organization are called Private Management Domains (PRMDs).

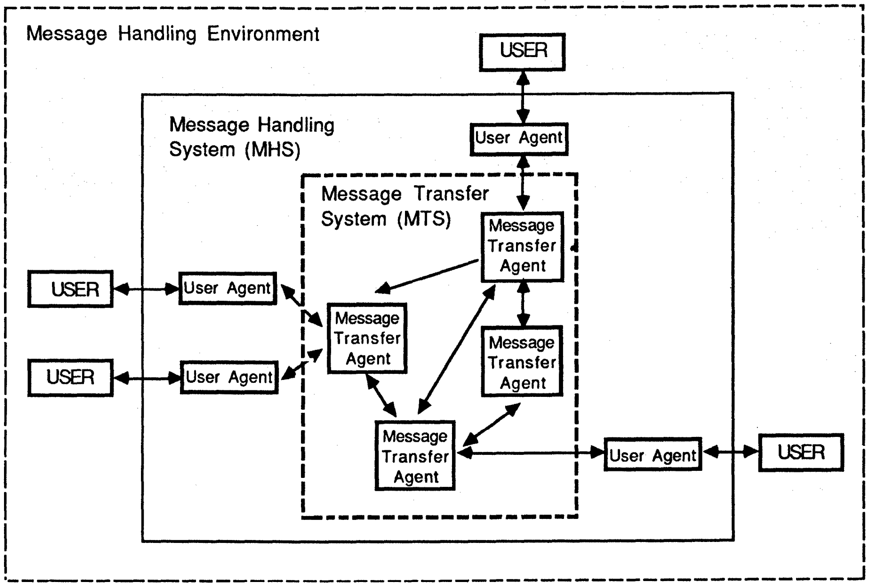
An administration can provide subscribers with access from combinations of UAs and MTAs, which can cross domain boundaries. Three scenarios are supported:

User to administration-supplied UA: The user's private I/O device, such as a telephone or teletype, interacts with a UA owned by the administration. Alternately, the administration can supply the user with an intelligent terminal.

Private UA to administration MTA: The user's private, standalone UA function in an intelligent workstation or a personal computer interacts with

Figure 2.
MHS

The X.400 Message Handling System (MHS) is a conceptual model within the recommendation. The core of the model is the Message Transfer System (MTS), which is composed of Message Transfer Agents. The MHS represents a superset of MTS functionality by providing User Agents (UAs) that present information on behalf of an ISO Application layer user or process via specialized protocols.



the administration MTA via the standard submission and delivery procedures, required for obtaining Message Transfer Agent service.

Private MTA to administration MTA: A PRMD subscriber owning one or more MTAs and one or more UAs interacts MTA to MTA. This interaction is one of peers, as it also represents an MD-to-MD relationship.

Although the X.400 Recommendation limits a PRMD to existence in one country, it can have access to one or more ADMDs. However, a PRMD cannot act as a relay between two ADMDs. When an ADMD interacts with a PRMD, the ADMD ensures that the PRMD provides valid Message Transfer Service before handing off a message and takes responsibility for the logging, accounting, quality, and other service elements in the transfer. Figure 4 offers a graphical overview of various ADMD and PRMD combinations.

Basic Message Transfer Service

Messages originated or received by the UA are handled in the form of an envelope plus content structure. The interactions are analogous to the ways individuals use public and private services to distribute mail and parcels.

The basic MT service provides the UAs with two-way access to the MTS and assigns each message a unique reference (tracking) identification code. When a message is undeliverable, the MTS informs the originating UA. The UA can specify the encoded types of information within a message, such as original encoded types (text, data, image); times of submission and delivery; and content conversion instructions, such as encryption.

Optional service elements can also be selected: some on a per-message basis, others for a prearranged contractual time period. Table 1 lists basic MTS service elements, grouped according to the five major service types—Basic, Submission and Delivery, Conversion, Query, and Status and Inform. Table 2 lists optional user facilities by per-message and contractual availability. The international availability of service elements is further specified in Recommendation X.401.

Interpersonal Message System

The Interpersonal Message System (IPMS) incorporates extensions to support its special requirements. It consists of the MTS, a specific class of cooperating UAs (IPM UAs), and items supporting access to telex and CCITT Telematic services (further specified in Recommendation X.430). The general availability of service elements is further specified in Recommendation X.401. Tables 2 and 3 depict optional user facilities offered on a per-message or contractual basis. Table 4 lists basic IPMS service elements, grouped according to the seven major types: Basic, Submission and Delivery, Conversion, Cooperating IPM UA Action, Cooperating UA Information Conveying, Query, and Status and Inform.

As in basic MT service, optional elements are available on a per-message or contractual basis. To assist users with sending and replying to IP messages, the IPM UA can provide a line or full-screen editing capability, as well as notification of pending messages. These and other enhancements to the UA, which can be implemented locally without affecting other UAs, are not subject to CCITT standardization.

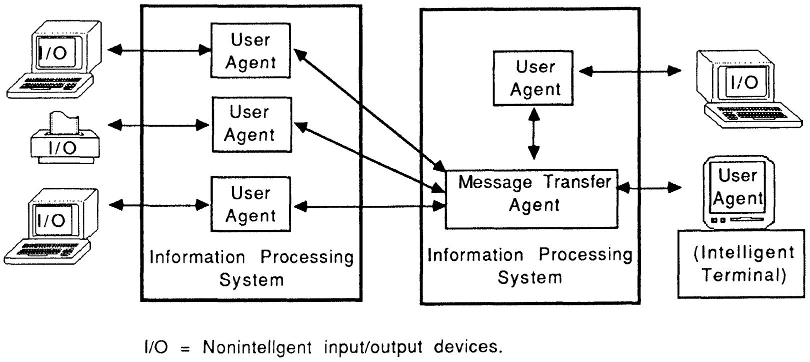


Figure 3.
UAs and MTAs
User Agents (UAs) and Message Transfer Agents (MTAs) can have a variety of physical implementations. An Information Processing System can include one or both within its bounds. The UA function could also reside in a dedicated intelligent terminal, such as a personal computer. For now, there are still some practical limitations to overcome before X.400 will support PC users desiring informal, dial-up access.

The IPMS elaborates on the convention of structuring messages into envelope and content portions, further subdividing the content into heading and body portions, as shown in Figure 5. The resulting structure follows the format of a memo.

Naming Conventions

In order to facilitate the execution of various MTS and IPMS service elements, Recommendation X.400 specifies a naming convention, which defines originator/recipient (O/R) names, O/R name attributes, forms, routing, and distribution lists. A directory function is mentioned, and wish list attributes are enumerated.

Usernames, which are the basis for addressing messages, can be primitive and/or descriptive. A naming authority, which assigns primitives, must ensure that they are unique within that authority's administrative domain. An example of a primitive name is an employee number. A descriptive name must also denote exactly one user, as in The Executive Director of Data Processing for XYZ Hospital.

Descriptive names identify an entity by specifying one or more of its attributes and also specify a set known as an attribute list. Since users are outside the MHS, an originator's UA must provide the MTA with a descriptive name, used to route the message to the recipient's UA. Thus, an O/R name could also be an O/R address, and the MTS could use it to locate the UA's point of attachment.

The CCITT has defined four categories of standard O/R attributes: Personal, Geographical, Organizational, and Architectural. A base attribute set is a minimum grouping required to clearly identify a Management Domain. These attributes include the following:

- Personal—surname, given names, initials, generation qualifiers (Jr., Sr.).
- Geographical—street name and number, town, region, country.
- Organizational—company, decision, position/title.
- Architectural—X.121 address, unique UA identifier (numeric), ADMD name, PRMD name.

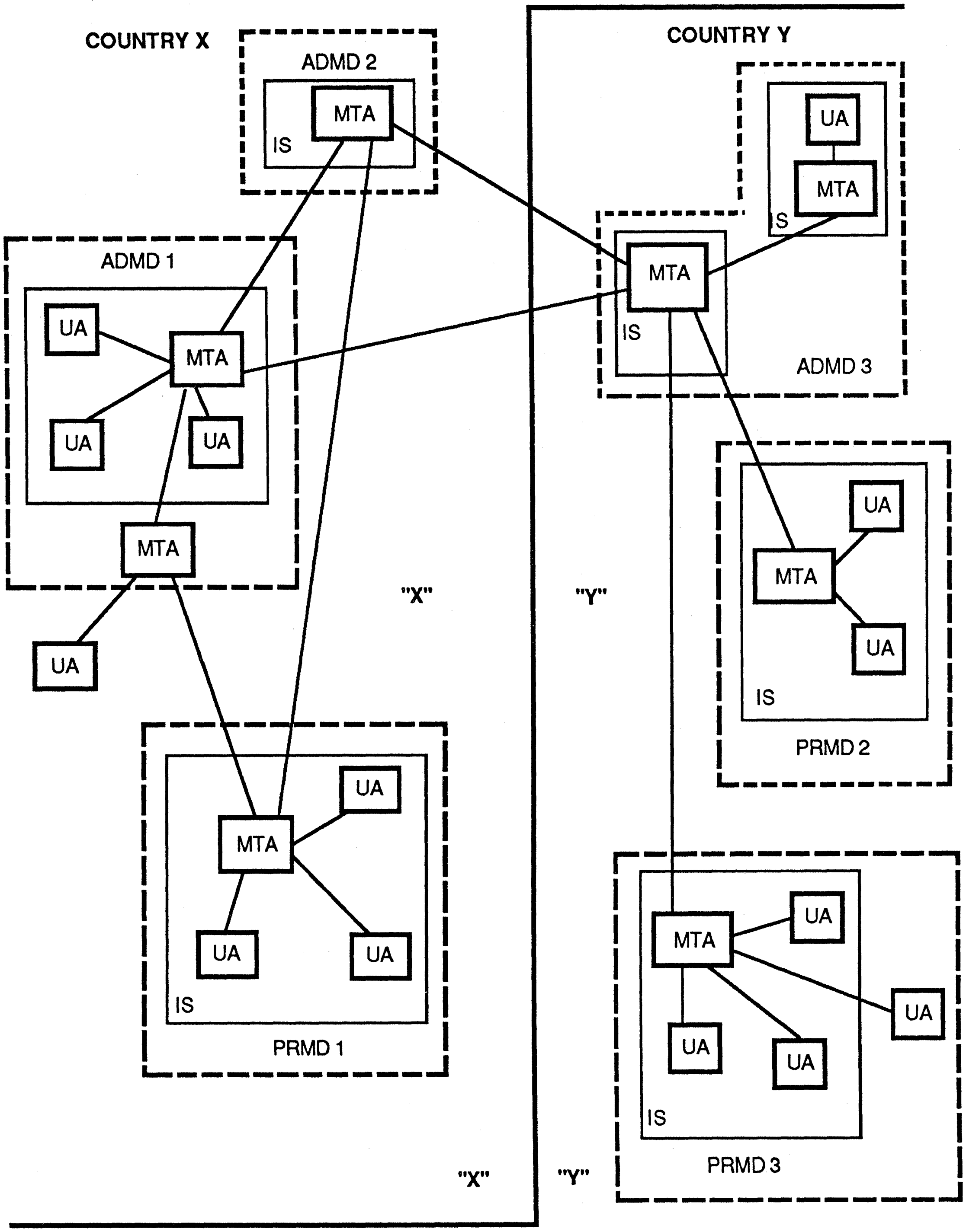
Several base attribute sets, with attributes chosen from each of the four categories, can be specified for the MHS. The choice of which one(s) to implement is left to the MD, but X.400 lists four that are of the most interest:

- Commercial—organization and country names.
- Residential—region and country names.
- Architectural—country and MD names.
- Terminal oriented—X.121 address, telex address, or Telematic terminal ID.

For initial service, each MD supports two base attribute sets: the Architectural and Terminal oriented. Support is specified as the ability to relay a message to a destination MD when passed from another MD, except for PRMDs, which are not required to relay between ADMDs; identification of the MD of the recipient UA by at least one base attribute set of the MD's choice; and user designation of recipients by either of the two base attribute sets.

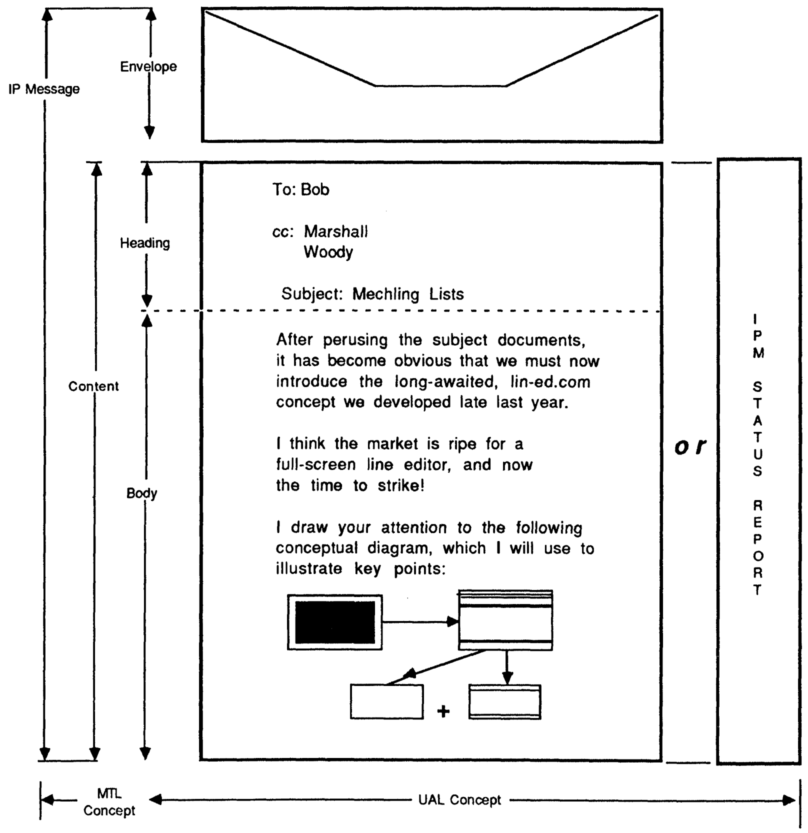
Initially, two forms of O/R name (Form 1 and Form 2) are supported. The first form specifies the

Figure 4.
X.400 Domains of Control



ADMD n	- Administrative Management Domain
PRMD n	- Private Management Domain
IS	- Information System (UAs + MTAs)
UA	- User Agent
MTA	- Message Transfer Agent

X.400 Domains of control are either Administrative or Private. An Administrative Management Domain (ADMD), essentially a public utility, provides MHS service to subscribers, which can reside as standalone UAs or within Private Management Domains (PRMD). Note that an ADMD is the only MD specified to provide service between countries and between Private Domains.



To: Bob

cc: Marshall
Woody

Subject: Mechling Lists

After perusing the subject documents, it has become obvious that we must now introduce the long-awaited, lin-ed.com concept we developed late last year.

I think the market is ripe for a full-screen line editor, and now the time to strike!

I draw your attention to the following conceptual diagram, which I will use to illustrate key points:

Figure 5.
Interpersonal Messages

Interpersonal Messages are comprised of Envelopes and Contents. The contents can be either the Heading and Body of a true IP message or a Status Report about the message. Note that text, data, and image can be mixed within an IP message. In cases where a user enables automatic forwarding, rerouting information is appended to the Heading to support successful delivery.

originator or recipient by means of the country or ADMD to which the user belongs. Three variants exist for the first form, using combinations of the various attributes found in the base attribute sets. A second form consists solely of the X.121 address and an optional Telematic terminal identifier.

Routing occurs only within the context of O/R addresses that provide the MTS with enough information to route the message between originating and receiving MDs. Routing within an MD is cited as beyond the scope of Recommendation X.400. Routing is handled by the designer of the MD's communications architecture.

Relying on base attribute sets, the linking MDs route messages until they arrive at the destination MD. At this point, the user attributes in the O/R address are interpreted to allow further redirection to the recipient UA. The recipient UA checks the correctness of the attributes. If the message is undeliverable, the recipient UA must initiate procedures to notify the originator.

Since the logical routing and assignment of responsibilities are hierarchical, a Management Domain's MTAs and UAs relinquish responsibility as soon as they complete the handoff to the next functional layer. This procedure is the most efficient in terms of overhead and is dictated by the MHS' store-and-forward nature.

The naming convention also specifies distribution lists. The ability to simultaneously route E-Mail to multiple recipients is of obvious value, and it is an integral feature of the Message Handling Environment. Tables 1 through 3 list many distribution-oriented features.

Layered Representation of the MHS Model

Section 5 of X.400 presents a layered view of the MHS and defines protocols used between peer layers. All MHS entities and protocols reside within the Application layer of the OSI reference model and can be visualized as sublayers within layer 7. This structure gives X.400-oriented applications access to the underlying layers and accomplishes the following:

- Establishes connections between individual systems independently of network topologies or media.
- Establishes session connections for reliable message transfer.

Table 1. X.400 Message Transfer Service Elements

Service Group	Service Elements
Basic	Access Management Content Type Indication Converted Indication Delivery Time Stamp Indication Message Notification Nondelivery Notification Original Encoded Information Types Indication Registered Encoded Information Types Submission Time Stamp Indication
Submission and Delivery	Alternate Recipient Allowed Deferred Delivery Deferred Delivery Cancellation Delivery Notification Disclosure of other Recipients Grade of Delivery Selection Multidestination Delivery Prevention of Nondelivery Notification Return of Contents
Conversion	Conversion Prohibition Explicit Conversion Implicit Conversion
Query	Probe
Status and Inform	Alternate Recipient Assignment Hold for Delivery

- Signals the use of standardized Message Handling Presentation Transfer Syntax as defined in Recommendation X.409.

The Message Handling functions in layer 7 consist of two sublayers: a User Agent Layer (UAL), containing the UA functionality associated with message contents, and a Message Transfer Layer (MTS), containing Message Transfer Agent functions supporting the MTS. The layers can be directly related to the functional model, based on S1, S2, and S3 systems. S1 systems contain only UA functions, S2 systems contain only MTA functions, and S3 systems contain UA and MTA functions.

Figure 6 depicts the S1, S2, and S3 types and the protocols used with them. The User Agent Entity (UAE) represents the UA when some type of UA-to-UA protocol takes place. Technically, it is distinguished from the complete UA as being only the *functionality* in a UA that represents a user while interacting with another cooperating UA.

Similarly, the Message Transfer Agent Entity (MTAE) supports the layer services of the MTL in cooperation with other MTAEs. A Submission and Delivery Entity (SDE) makes the services of the MTL available to a UAE through the MTL boundary. The SDE does not provide the services, but interacts with the peer MTAE to provide access to the MTAE.

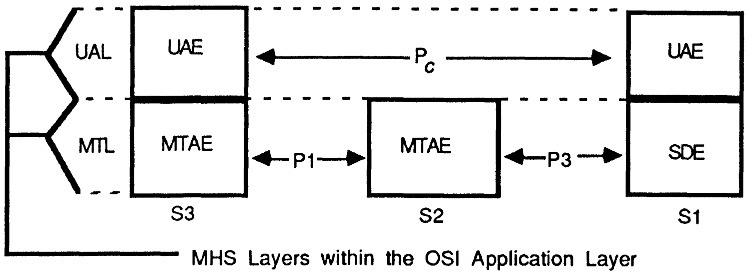
These entities require three peer protocols—P1, P2, and P3. The Message Transfer Protocol (P1) defines relaying of messages between MTAs and other interactions required for MTL services. P1 messages consist of the original message contents plus a relaying envelope. The X.411 Recommendation specifies P1 protocol in detail. Recommendation X.410 specifies how the Application layer uses the OSI layers for reliable transfer and defines the Reliable Transfer Server and remote operations protocols.

The Interpersonal Messaging Protocol (P2), specified in X.420, consists of a set of protocol elements with standardized syntax and semantics. These protocol elements form the contents of messages exchanged between IPM UAEs. The operations relating to the exchange of P2 protocol elements between an IPM UAE are also defined. P2 defines rules that an IPM UAE must follow when it requests MTL Service in the course of supporting IPM Service. Figure 7 depicts the layered representation of the IPM.

The Submission and Delivery Protocol (P3) allows the SDE in an S1 system to provide its UAE with access to the MTL and its services. It is also defined in X.411. Its use of the ISO stack is defined in X.410.

X.401

Recommendation X.401 defines the Basic Service Elements and Optional User Facilities of those services. Certain elements of each service, inherent in the MHS, are classified as basic MT or IPM services. Other service elements are optional, and the user can select them on a per-message or contractual (time period) basis. Of the optional elements, some are specified by X.401 as essential optional; others are additional optional. Essential optional items can be added to the inherent items but must be offered internationally by administrations, such as PTTs. Additional optional elements are truly optional, as administrations may or may not make them available nationally; they can also be available internationally via bilateral agreement.



S1 - Systems with only UA functions
S2 - Systems with only MTA functions
S3 - Systems with both UA and MTA functions
UAE - User Agent Entity
MTAE - Message Transfer Agent Entity
SDE - Submission and Delivery Entity
P1 - Message Transfer Protocol
P_c - Range of Protocols defining message content
P3 - Submission and Delivery Protocol

Figure 6.
MHS Elements

The generic MHS elements support the possible physical mappings of Figure 3 as a general structure on which specialized implementations can be built. Pc is, therefore, a range of protocols, any one of which will support protocol data transfer between Cooperating UAs.

X.408

Recommendation X.408 specifies rules for encoding various information types into a universal format that can be freely interchanged among the physical input/output devices covered in the MHS recommendation. Nine types of information are cited, but conversion between some of the combinations is cited "for further study." The nine information types are:

- Telex—Code defined in F.1; format in S.5.
- International Alphabet #5 (IA5) Text—Code defined in T.50.
- Teletex—Code defined in T.61; format defined in F.200 and T.60.
- G3 Facsimile—Code defined in T.4; signaling in T.30.
- Text Interchange Format 0 (TIF0)—Code and format defined in T.73.
- Videotex—Code defined in T.100 and T.101.
- Voice—Encoding for further study.
- Simple Formattable Document (SFD)—Code defined in T.61; format in X.420.
- Text Interchange Format 1 (TIF1)—Code and format defined in T.73.

The rules also point out that any existing standards outside the recommendation are preserved in conversion implementations. Recommendation X.408 also includes several matrices of conversion detail.

X.409

This recommendation offers a methodology for the actual encoding of binary or character information, required before passage through the MHS. It defines a presentation transfer syntax for Application layer protocols used by the MHS and Telematic Services Document Interchange Protocol. Those familiar with IBM's DIA/DCA protocols will recognize X.409 as the CCITT's approach to similar requirements, but on an international, multivendor scale.

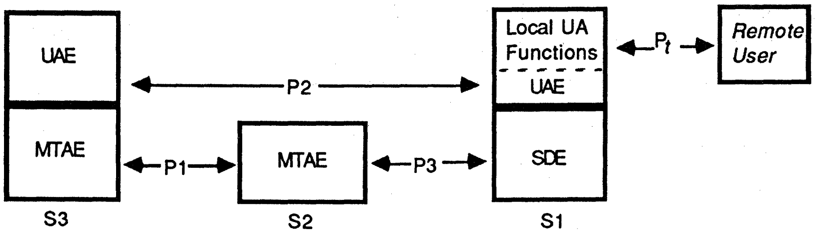
X.409 uses the Backus-Naur Form (BNF) notation for expressing information. The BNF description of any formal language comprises a series of replacement rules called productions. Adherence to the replacement rules produces valid instances of the language.

X.410

X.410 defines Remote Operations, used to structure interactive Application layer protocols such as P3 (Submission and Delivery). It also describes the Reliable Transfer Server (RTS) mechanism between peer entities, which uses message handling protocols such as P1. In addition, it describes the notation of protocol data units used by Remote Operations, the service primitives used to describe reliable transfer, and the use of P1 and P3 protocols to access the OSI Presentation and Session layers.

Figure 7.
IPMS

The IPMS is actually a special case of the generalized MHS depicted in Figure 7. The P2 protocol is the first protocol specified in the Pc range. Protocol Pt is not actually specified in X.400, but can be chosen from a suite of existing interactive terminal protocols from other CCITT recommendations.



P1 - Message Transfer Protocol
P2 - Interpersonal Messaging Protocol *(from P_c)*
P3 - Submission and Delivery Protocol
P_t - Interactive Protocols unspecified within X.400

The concept of remote operations and remote errors facilitates the specification and implementation of interactive protocols. These logical representations of any interactive communication action occur as one Application Entity requests another to perform an operation. The obliging AE, in turn, attempts to perform the operation and then reports the outcome as a success or failure. Operation Protocol Data Units (OPDUs) invoke, then return, result or return error conditions.

The Reliable Transfer Server is the part of the AE that creates and maintains associations between the AE and its peers and passes Application Protocol Data Units (APDUs) between them. The associated APDUs and OPDUs conform to the BNF notation described in Recommendation X.409. Service primitives describe the interactions between an RTS and its user. Based on Session layer services, they use sets of tokens to determine the sequence of turns at invoking services from the remote entity. For example, a PLEASE token can request a turn; a GIVE token can grant a turn. Service primitives, such as OPEN, CLOSE, TURN-PLEASE, TURN-GIVE, EXCEPTION, and RECOVER, thus translate into similar Session layer service requests. Other important facets of service primitives include the passing of additional session-related information, such as major and minor checkpoint (synchronization) sizes and initial token possession. Important features of the RTS are its support of session recovery and data transfer restart (from last checkpoint).

Recommendation X.410 specifies the subset of the OSI session tokens required for RTS operation and defines several valid states in which the RTS and its user can exist, depending on specific possession of various tokens at given times. Thus, the primitives are really abstractions representing logical uses of lower level services.

X.411

Recommendation X.411 defines the Message Transfer Layer and the types of services it supports in a practical message handling system. The service primitives presented for the MT Layer are again abstractions and thus resemble X.410 RTS primitives in their form. Protocol data units are also described in BNF notation.

LOGON, LOGOFF, REGISTER, CHANGE PASSWORD, CONTROL, SUBMIT, PROBE, DELIVER, NOTIFY, and CANCEL primitives are defined. The concept of a PROBE is introduced, which effectively tests the validity of a service requested by an AE, before causing the MHS to incur the overhead associated with its transfer. In essence, it tests to see if there is a mailbox before licking the stamp.

NOTIFY sends an acknowledgment of the success or failure of a delivery attempt. CONTROL allows a user to specify the times for, and types of, messages being accepted. REGISTER allows users to change their subscription profiles for services and options.

The Message Transfer Protocol, P1, is specified as supporting services that require coordination between cooperating Message Transfer Agent Entities. It is used, therefore, for communications between different Administration Management Domains and between a Private Management Domain and an ADMD. The protocol elements of P1, called Message Protocol Data Units (MPDUs), can be User MPDUs (UMPDUs) or Service MPDUs (SMPDUs). UMPDUs carry messages submitted by a UAE for transfer and delivery to another

Table 2. X.401MT Optional User Facilities (per Message)

MT Optional User Facilities	Categorization
Alternate Recipient Allowed	E
Conversion Prohibition	E
Deferred Delivery	E
Deferred Delivery Cancellation	E
Delivery Notification	E
Disclosure of Other Recipients	E
Explicit Conversion	A
Grade of Delivery Selection	E
Multidestination Delivery	E
Prevention of Nondelivery Notification	A
Probe	E
Return of Contents	A

E—Essential optional facility.
A—Additional optional facility.

UAE. SMPDUs convey information about the messages. Relaying and multiple delivery are supported.

An MTAE executing the P1 protocol has three logical parts. The Message Dispatcher performs the P1 protocol actions dictated by the MPDUs received from other MTAEs or those resulting from messages submitted by its own UAEs. The Association Manager, which compares with the ASE of Figure 1, manages the establishment, control, and release of associations provided by the Reliable Transfer Server. All three are shown in a layered model in Figure 8.

X.413

This recommendation defines the services of the Message Store (MS), which serves in an intermediary role between the user agent and the MTS. A user agent (UA) is an application process that interacts with the message transfer system (MTS) to submit messages. Its primary function is to accept delivery of messages on behalf of a single MHS end user and to retain them for subsequent retrieval by the end user's UA. The MS also provides indirect message submission and message administration services to the UA, via "pass-through" to the MTS. Like the UA, the MS acts on behalf of a single end user and does not provide a common or shared multiuser MS service.

Message Store (MS) Ports

An MS provides the Retrieval, Indirect-submission, and Administration ports to the MS service user. Although the indirect-submission and administration capabilities of the MS service are the same as those provided by other components of an MHS, the retrieval capabilities are unique to the MS. These capabilities include obtaining information on, fetching, and deleting messages residing in the MS. Additional capabilities register certain MS-provided automatic actions.

Before providing an MS user with any retrieval capabilities, the MS authenticates the user by means of the Bind-operation. Similarly, the MTS must authenticate the MTS service user before it extends its services. All the services provided by the MS, with the exception of the Alert service, are invoked by the user.

In addition to supplying the Retrieval port services to its user and acting as a surrogate MTS service provider, supplying the MTS submission and administration services to its user, the MS, acting as a surrogate UA, also uses the MTS Delivery port, Submission port, and Administration port services.

MS Information Model

The MS stores and maintains *Information bases,* which consist of *entries* that, in turn, consist of *attributes.* An Information base in the MS is a database containing all the entries that represent constituent objects of a particular category or categories. There are various kinds of Information bases, but this recommendation describes the *Stored message Information base.*

Table 3. X.401MT Optional User Facilities (Contractual)

MT Optional User Facilities	Categorization
Alternate Recipient Assignment	A
Hold for Delivery	A
Implicit Conversion	A

E—Essential optional facility.
A—Additional optional facility.

Table 4. Interpersonal X.400 Messaging Service Elements

Service Group	Service Elements
Basic	Basic MT Service Elements (MTS) IP-Message Identification Typed Body
Submission/Delivery and Conversion *(MTS)*	*(See Table 1)*
Cooperating IPM UA Action	Blind Copy Recipient Indication Nonreceipt Notification Receipt Notification Auto Forwarded Indication
Cooperating IPM UA Information Conveying	Originator Indication Authorizing Users Indication Primary and Copy Recipients Indication Expiry Date Indication Cross-Referencing Indication Importance Indication Obsoleting Indication Sensitivity Indication Subject Indication Replying IP-Message Indication Reply Request Indication Forwarded IP-Message Indication Body Part Encryption Indication Multipart Body
Query *(MTS)*	*(See Table 1)*
Status and Inform *(MTS)*	*(See Table 1)*

Each Information base is organized as a sequence of entries, with each entry representing a single object, such as a delivered message, within the Information base. Each entry is identified by means of a sequence number, unique within the Information base, which is generated as new entries are created. The MS generates these sequence numbers in ascending order without cycling, and they are never reused.

All entries consist of a set of attributes, with each attribute providing a piece of information about, or derived from, the data to which the entry corresponds (e.g., the sequence number of the entry or the creation time). An attribute consists of an attribute type, which identifies the class of information given by an attribute (e.g., a message's priority), and the corresponding attribute value(s), which are particular instances of that class appearing in the entry (e.g., urgent). All attributes in an entry must be of distinct attribute type; attribute types that contain a single attribute value are said to be single valued, while those with more than one are multivalued. Certain general-purpose attribute types for the Stored messages Information base, defined in the X.413 recommendation, are called general attribute types, and their attributes are known as general attributes.

Although entries in a single Information base are generally independent of each other, the MS information model supports tree-structured relationships among entries, with one entry (a child entry) being the child of another (a parent entry). An entry that is not a child entry is termed a main entry. The operations of the MS service act by default only on main entries, although some can be directed to act on all entries.

The Stored message Information base acts as a repository for information obtained from the Message Delivery and Report Delivery operations of the Message Delivery Port. It contains entries for delivered messages and notifications. Entries are created by the MS when a message is delivered or a notification arrives at the MS.

Retrieval Port Operations

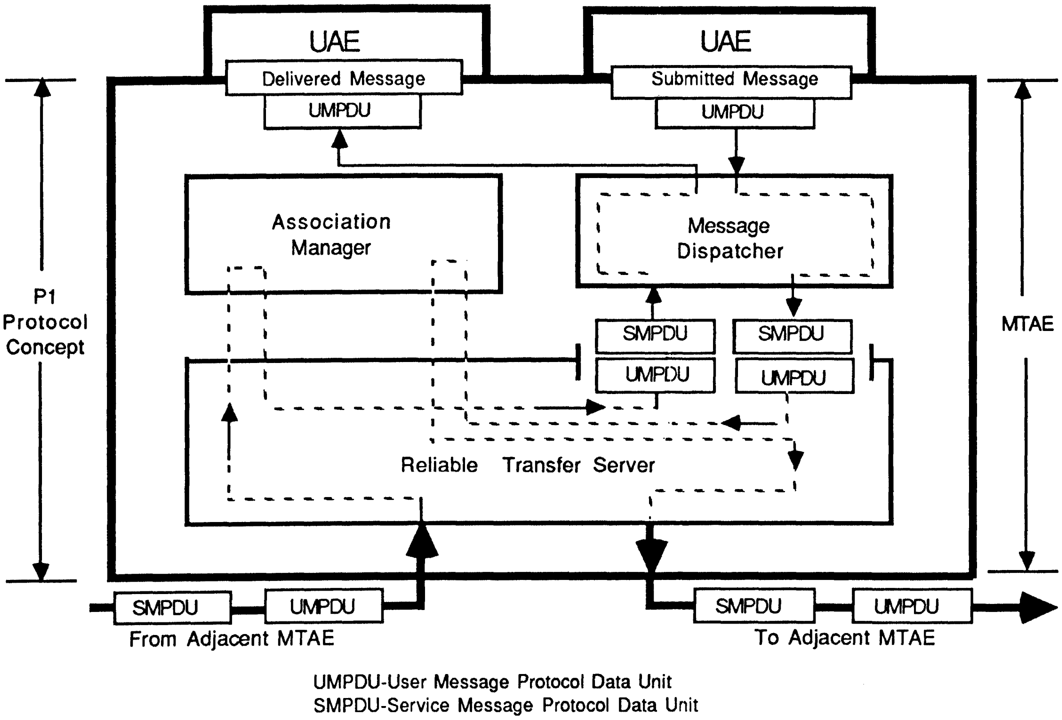
The **Summarize Operation** returns summary counts of selected entries in an Information base. In addition, a count of the entries selected and their lowest and highest sequence numbers are also returned. Zero or more individual summaries can be requested. This operation will be successful only when the Information base permits access according to the security context and enforced security policy. The attributes that can be used for summaries are restricted.

The **List Operation** searches a selected Information base for entries and returns selected information from them. This operation will be successful only when the Information base permits access according to the security context and enforced security policy.

The **Fetch Operation** returns selected information from a specific entry in the Information base. Alternately, it returns selected information from the first entry among several entries of interest. Information from an entry can be fetched several times until the entry is explicitly deleted via the Delete Operation. This operation will be successful only when the Information base permits access according to the security context and enforced security policy.

The **Delete Operation** is used to delete selected entries from an Information base. A main

Figure 8.
The Association Manager



The Association Manager manages the use of Session layer connections required for message transfer. The Message Dispatcher passes P1 protocol data to and from the Reliable Transfer Server and the involved User Agent Entities.

entry and all its child entries can be deleted together only by specifying the main entry as the argument of command. For specific Information bases, there may be restrictions on which entries can be deleted. For stored messages, no entry can be deleted if its entry status is new. This operation will be successful only when the Information base permits access according to the security context and enforced security policy.

The **Register-MS Operation** registers or deregisters auto actions, default lists of attribute types, new credentials, and new sets of user security labels.

The **Alert Operation** enables the MS service provider to inform its user immediately of a new entry that has been entered into the MS, whose attributes match the selection criteria of one of the auto alert-registrations previously supplied using the Register Operation. This operation can be invoked during an existing association initiated by the UA, but only when new entries have been entered after the establishment of the association. This operation will be successful only when the Information base permits access according to the security context and enforced security policy.

X.419

This recommendation specifies the following MHS application protocols:

- The MTS Access Protocol (P3) used between a remote User Agent and the MTS to provide access to the MTS service,
- The MS Access Protocol (P7) used between a remote User Agent and an MS to provide access to the MS service, and
- The MTS Transfer Protocol (P1) used between MTAs to provide the distributed operation of the MTS.

The recommendation describes how the MTS service, the MS service, and the MTA service are supported by instances of OSI communications when a service user, a service provider, or (in the case of

Table 5. X.401 IPM Optional User Facilities

IPM Optional User Facilities (per Message)	Origination by UAs	Reception by USs
Alternate Recipient Allowed	A	A
Authorizing Users Indication	A	E
Auto Forwarded Indication	A	E
Blind Copy Recipient Indication	A	E
Body Part Encryption Indication	A	E
Conversion Prohibition	E	E
Cross-Referencing Indication	A	E
Deferred Delivery	E	NA
Deferred Delivery Cancellation	E	NA
Delivery Notification	E	NA
Disclosure of Other Recipients	A	E
Expiry Date Indication	A	E
Explicit Conversion	A	NA
Forwarded IP-Message Indication	A	E
Grade of Delivery Selection	E	E
Importance Indication	A	E
Multidestination Delivery	E	NA
Multipart Body	A	E
Nonreceipt Notification	A	E
Obsoleting Indication	A	E
Originator Indication	E	E
Prevention of Nondelivery Notification	A	NA
Primary and Copy Recipients Indication	E	E
Probe	A	NA
Receipt Notification	A	A
Reply Request Indication	A	E
Replying IP-Message Indication	E	E
Return of Contents	A	NA
Sensitivity Indication	A	E
Subject Indication	E	E

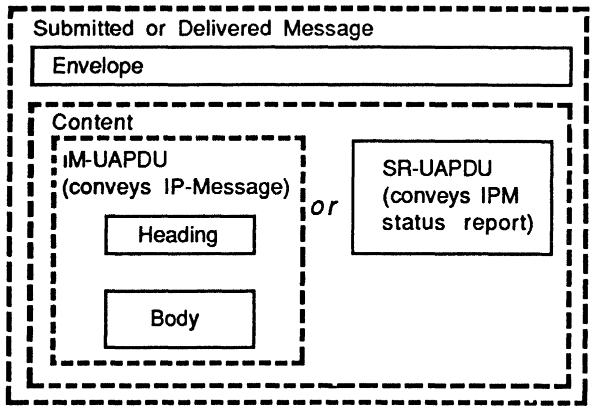
E—Essential optional facility.
A—Additional optional facility.
NA—Not applicable.

the MTA service) the MTAs are realized as *application processes* located in different open systems.

Protocols and Services

In the Open Systems Interconnection (OSI) environment, communication between applications processes is represented in terms of communication between a pair of *application entities (AEs)* that use the presentation service. These AEs consist of a set of one or more *application service elements (ASEs)*, and the interaction between AEs is described in terms of their use of the services provided by the ASEs. Access to the MTS service is supported by three ASEs, each of which supports a type of port paired between a user and the MTS (as defined in Recommendation X.411).

Figure 9.
Recommendation X.420



IM-UAPDU - Interpersonal Message User Agent Protocol Data Unit
SR-UAPDU - Status Report User Agent Protocol Data Unit

Recommendation X.420 goes into great detail to specify the Protocol Data Units required for Interpersonal Messaging Service. The items within solid boxes represent actual MTL or UAL defined elements. The items within the dashed boxes are abstractions of these items.

The **Message Submission Service Element (MSSE)** supports the services of the Submission-port.

The **Message Delivery Service Element (MDSE)** supports the services of the Delivery-port.

The **Message Administration Service Element (MASE)** supports the services of the Administration-port.

The MTS service is supported by only one ASE.

The **Message Transfer Service Element (MTSE)** supports the services of the Transfer-port (as defined in Recommendation X.411).

Access to the MS service is also supported by three ASEs, with the MSSE supporting the services of the Indirect-submission-port, the MASE supporting the services of the Administration port, and the Message Retrieval Service Element (MRSE) supporting the services of the Retrieval-port (as defined in Recommendation X.413).

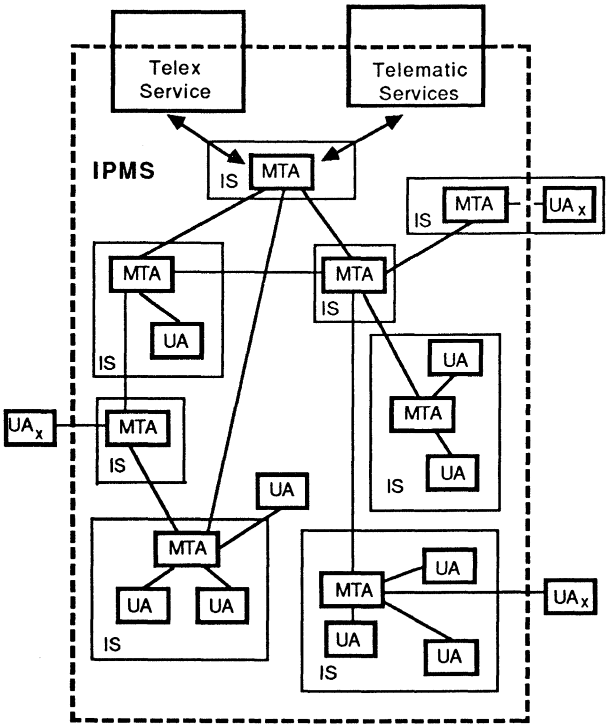
The MSSE, MDSE, MRSE, and MASE are asymmetric ASEs; i.e., the user ASEs act as the consumer, and the MTS and MS ASEs act as the supplier of the services. Along with the services provided by the ASEs, the three protocols also comprise the operations that provide the appropriate Bind and Unbind services.

Underlying Services

The ASEs previously described are in turn supported by other ASEs. The **Remote Operations Service Element (ROSE)** supports the request/reply functions of the remote operations that occur at the ports. The ROSE supports only the ASEs that provide access to the MTS and MS services, i.e., the MSSE, MDSE, MRSE, and MASE. These ASEs map the syntax notation of a service onto the services provided by the ROSE. The remote operations of the MTS Access Protocol (P3) are asynchronous operations (Class 2), and those of the MS Access Protocol (P7) are synchronous operations (Class 1).

The **Reliable Transfer Service Element (RTSE)** reliably transfers the *Application Protocol Data Units (APDUs)* that contain the parameters of

Figure 10.
An Overview of the Complete IPMS Model

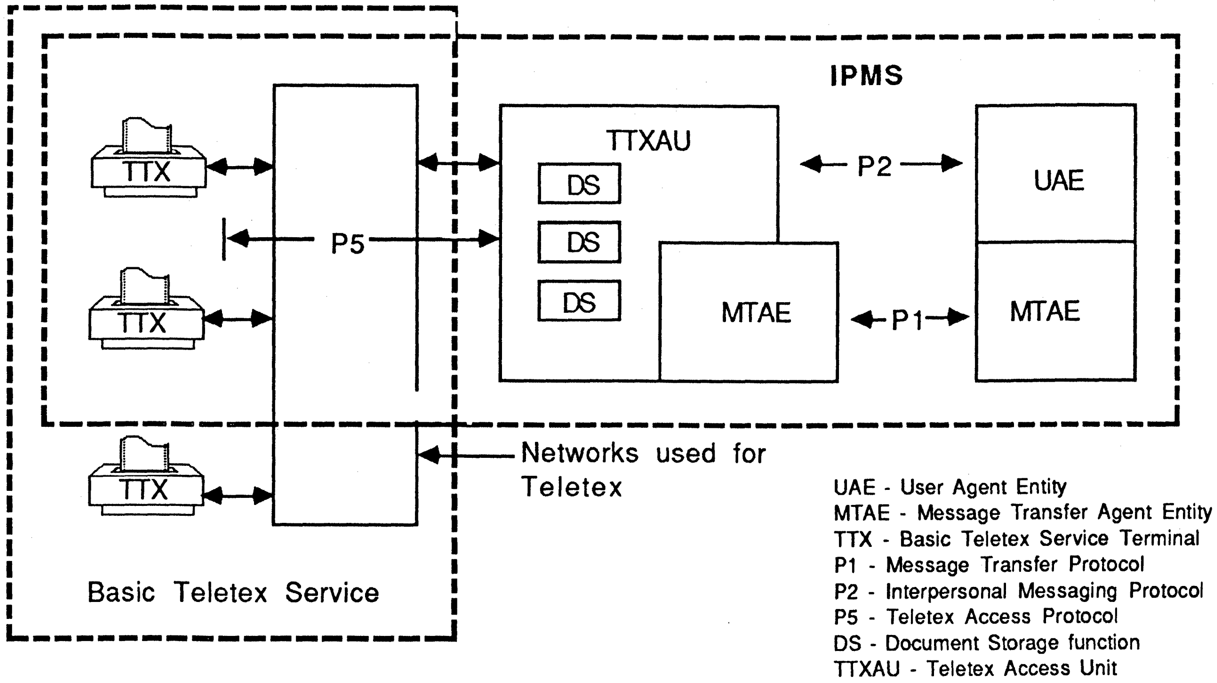


IS - Information System (UAs + MTAs)
UA - User Agent
MTA - Message Transfer Agent
UA$_x$ - Non-Cooperating UA (outside of IPMS)

Note that some User Agents (UAs) are noncooperating: They support basic MHS service but not the specialized IPMS service. Also, note that the noncooperating UAs are not distinguished by any peculiarities of physical mapping; standalone UAs can be either cooperating or not cooperating.

Datapro Information Services Group. Delran NJ 08075 USA

Figure 11.
TTXAU


IPMS
TTX
TTX
TTX
P5
TTXAU
DS
DS
DS
MTAE
P2
UAE
P1
MTAE
Networks used for Teletex
Basic Teletex Service
UAE - User Agent Entity
MTAE - Message Transfer Agent Entity
TTX - Basic Teletex Service Terminal
P1 - Message Transfer Protocol
P2 - Interpersonal Messaging Protocol
P5 - Teletex Access Protocol
DS - Document Storage function
TTXAU - Teletex Access Unit

The Teletex Access Unit (TTXAU) expands the functionality of the MTAE to support terminals of an existing TTX network. Special Document Storage entities spool messages between the TTX terminals and a conventional UAE.

the operations between AEs. The RTSE is mandatory for the support of the MTS Transfer Protocol (P1) since it does not use the ROSE, but it is optional for the P3 and P7 protocols. The RTSE recovers from communications and end-system failure and minimizes the amount of retransmission needed for recovery.

The **Association Control Service Element (ACSE)** supports the establishment and release of an application association between a pair of AEs. Associations between a user and the MTS can be established by either, while those between a user and the MS can be established only by the user.

The combination of one or more of the ASEs for the MTS and MS Access Protocols, together with their supporting ASEs, defines the application context for the MHS Access Protocols, while the MTSE and the supporting RTSE define that for the MTS Transfer Protocol. The MHS protocols also make use of the services provided by the lower levels of the OSI model.

Protocol Syntax

The syntax of the MHS protocols is defined by the syntax notation ASN.1 specified in CCITT Recommendation X.208 (ISO 8824) and the remote operation notation defined in the Recommendation X.218.

The syntax definition of the MTS Access Protocol (P3) has the following major parts:

- *Prologue:* declarations of the exports from, and imports to, the MTS Access protocol module,
- *Application Contexts:* definitions of the application contexts that can be used between an MTS user and the MTS,
- *Message Submission Service Element:* definitions of the MSSE, its remote operations, and errors,
- *Message Delivery Service Element:* definitions of the MDSE, its remote operations, and errors, and
- *Message Administration Service Element:* definitions of the MASE, its remote operations, and errors.

The syntax definition of the MS Access Protocol (P7) has the following major parts:

- *Prologue:* declarations of the exports from, and imports to, the MS Access Protocol module,
- *Application Contexts:* definitions of the application contexts that can be used between an MS user and the MS,
- *Message Submission Service Element:* definitions of the MSSE, its remote operations, and errors, and
- *Message Retrieval Service Element:* definitions of the MRSE, its remote operations, and errors.

The syntax definition of the MTS Transfer Protocol (P1) has the following major parts:

- *Prologue:* declarations of the exports from, and imports to, the MTS Transfer Protocol module,
- *Application Contexts:* definitions of the application contexts used between MTAs,
- *Message Transfer Service Element:* definitions of the MTSE, and
- *MTS Application Protocol Data Units:* definitions of the MTS APDUs, i.e., Message, Probe, and Report.

X.420

Recommendation X.420 describes the Interpersonal Messaging User Agent Layer for the MHS and its associated protocol data units. It also specifies the representation used for transmitting simple formattable documents (SFDs). The IPM Service provides the mechanisms through which users can exchange interpersonal messages. Certain additions to the basic MHS are incorporated to support IPMS, which is actually just a special case of MH System use.

The two types of IPM contents are described as User Agent Protocol Data Units (UAPDUs), IP-message (IM-UAPDUs), and IPM-status-report (SR-UAPDUs). IM-UAPDUs contain the actual message content, including the heading and body; SR-UAPDUs contain status and reporting information, including the success or failure of a delivery attempt. Figure 9 breaks out IPM components with respect to UAPDUs.

IPM UAEs access the MTL in much the same way as basic UAEs do, using a very similar set of primitives (LOGON, CHANGE PASSWORD, SUBMIT). Because of the nature of IPM service, a number of other parameters supporting postal and corporate memo-type services, such as deferred delivery, carbon copy, blind carbon, and forwarding are also accommodated.

The SFD concept is analogous to IBM's revisable form document concept. SFDs are minimally formatted text segments that conform to prescribed standards, ensuring revisability by the receiving UA process. This is an important consideration, since it makes text exchange possible between otherwise incompatible systems. SFD implementation conforms to a number of structure and content notation conventions, which are also described via the BNF notation.

X.430

This recommendation deals with integrating Teletex (TTX) terminals into an IPMS. To facilitate this integration, special variants to IPMS service elements are defined. Figure 10 shows the relationships of IPMS components, including Teletex and Telematic elements.

A Teletex Access Unit (TTXAU) is added to the Message Handling System model to give TTX units access to the Message Transfer System entities used by other IPMS terminals. It supports TTX terminals on a one-to-one basis, using the Teletex Access Protocol (P5). The TTXAU can also provide a Document Storage (DS) facility to accept delivery of messages from the MHS for the TTX terminal. Figure 11 shows the recommended relationship between the IPMS and existing Teletex networks.

X.435

Study Group VII published draft recommendations in the fall of 1990 that covered electronic data interchange (EDI) messaging systems. Completing work begun in the spring of 1988, Study Group VII spent five meetings drafting Recommendation X.435. Since the group reached the decision to base the EDI/X.400 service on the concept of user agent services, the group defined a protocol and content type for EDI. Participants at the next to the last meeting decided to use Message Store (MS) to accommodate EDI transmissions. The draft recommendation enables originators in

EDI transactions to be notified when EDI recipients have taken over the EDI message. Since Study Group VII is continuing its work on X.435, publications in 1992 will feature the outcome.

XAPIA and X/Open

In September 1990, the X.400 Application Program Interface Association (XAPIA), an association of leading computer and communications vendors, and X/Open, the international open systems organization, jointly announced the availability of specifications for the development of electronic messaging applications. These programming interface specifications enable software developers to write electronic mail applications based on international standards, capable of operating independently of computer systems, operating systems, or communications networks. The specifications cover X.400 messaging, X.500 directories, and object management. They are:

Messaging Gateway Application Program Interface (API) Version 2—an API providing definitions for interfacing proprietary mail systems to an X.400 Message Transfer Agent.

Messaging Application API—an API that enables X.400 messaging capabilities, such as submission, delivery, and retrieval, to be incorporated directly into nonmessaging applications, such as word processing and spreadsheets.

Directory Services API—an API that enables global mail directories based on X.500 to be accessed from within these same applications.

Object Management API—an API used by other APIs to provide tools for manipulating complex information objects, such as messages and the results of directory inquiries.

Formed in January 1989, the X.400 Application Interface Association includes AT&T, Banyan Systems, British Telecommunications plc, cc:Mail, Data Access, Data Connection Ltd., Digital Equipment, Enable Software, GSI/Danet, Hewlett-Packard, Indisy Software, Lotus Development, Microsoft, NCR, Novell, NTT America, OSIware, Retix, Soft-Switch, Sun Microsystems, US Sprint Communications, Tandem, TITN, Touch Communications, and 3Com.

X/Open, founded in 1984, is made up of international computer systems vendors, user organizations, and software suppliers that are investing business, technical, and marketing resources in the specification of the X/Open Portability Guide (XPG), which is a vendor- and product-independent, open operating environment based on de facto and international standards. X/Open members include AT&T, Bull, Digital Equipment, Fujitsu Ltd., Hewlett-Packard, Hitachi, IBM, ICL, NCR, NEC, Nixdorf, Nokia Data, Olivetti, Open Software Foundation, Philips, Prime Computer, Siemens, Sun Microsystems, Unisys, and Unix International.

X.400 Sources

Readers who want more complete details of the standards can order and examine copies of the CCITT documents that contain the X.400 MHS specifications. Recommendations X.400, X.401, X.408, X.409, and X.410 are published in Document AP VIII-66-E. Recommendations X.411, X.420, and X.430 are published in Document AP VIII-67-E. Both documents mention others; documents in the series AP VIII-(56-68) make up the complete set referenced. To order copies of CCITT standards in the United States, contact:

United States Department of Commerce
National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
Telephone (703) 487-4650 ■