Message Handling Systems
An Overview and Introduction into the X.400 Recommendations of 1984 and 1988

Dr. Pietro Schicker

Zellweger Telecommunications AG
CH-8634 Hombrechtikon

Message handling systems are the electronic equivalent to ordinary mail. First used in the academic world then within computer systems, IFIP set out to define the means to integrate these systems. However, due to the obvious usefulness of such a service, CCITT took over and by 1984 puplished a first set of recommendations for message handling systems, the X.400 series. A number of facilities were left undefined in this first set in order to have a standard published; work continued and led to the puplication of an enhanced set of recommendations in 1988.

The CCITT X.400 series recommendations of 1988 differ in appearance drastically from those of 1984. Although the model, on which the definitions are based, remains basically the same, subtle extensions were necessitated by the increase of functionality in the message handling services.

The most apparent change from 1984 to 1988 lies in the structure of the application (in the OSI sense). This modification is due to the fact that ISO has progressed work on the definition of the application layer structure and CCITT followed in their 1988 recommendations this new development.

A large number of service elements have been added to the recommendations many of which reflect the new functionality (e.g., postal delivery, distribution lists, secure messages, etc.). In the annex, a complete list of all service elements as defined in X.400 is given.

1. Introduction

Message handling systems often known under the name "computer based message systems" or simply "electronic mail" have many analogies to the regular mail system. In the regular mail system a message is composed first, then an envelope is addressed, the message is put as a content into the envelope and both thrown into a mailbox. The mail system transports this letter from office to office and eventually deposits it in the mail box of the addressee. The addressee on his part takes the letter out of the letter box, opens the envelope and consumes the message.

In the electronic message handling systems the same elements can be distinguished (c.f. figure 1-1), only these are not realized with paper content, letterbox and post office but by electronic means. The two persons involved are here called the originator and the recipient respectively. The terms content and evelope have been carried over to the electronic message handling systems, the elements mailbox and post office, however, received other terms which we will get to know shortly.

In the regular mail a large number of content types can be communicated, e.g., letter, picture, etc. The same is true for electronic message handling systems and, although the most used application is the communication of ASCII text files, there exists the possibility to communicate teletex or telefax messages,or a mixture of both. Even complete multi-media documents can be exchanged between originator and recipient (c.f. figure 1-2).

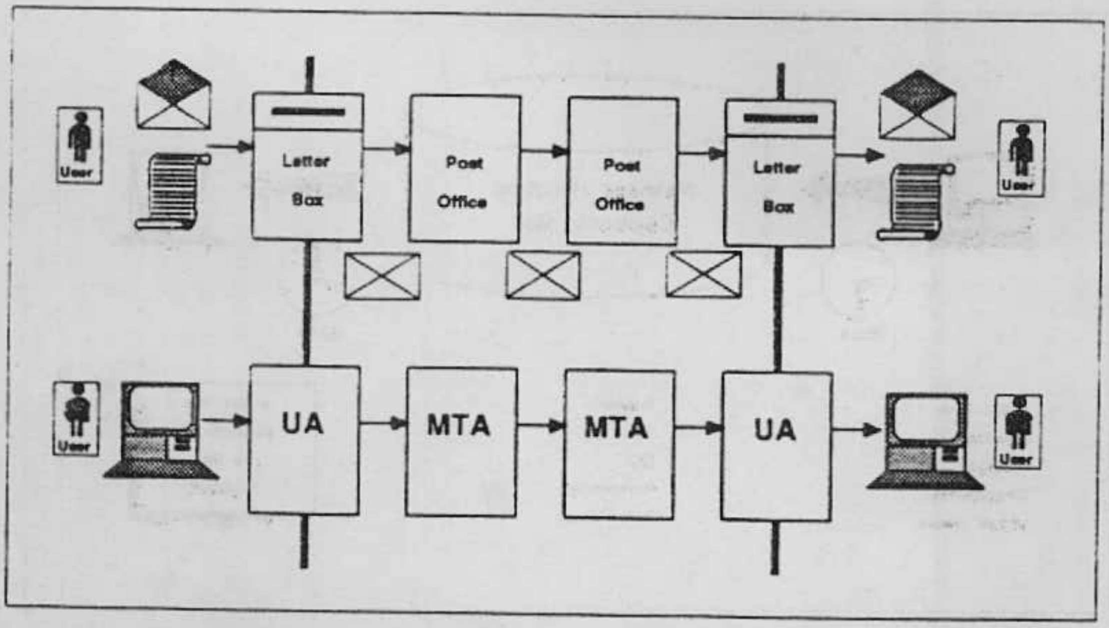


Figure 1-1: Analogy between the Regular Mail System and the Message Handling System

The name "Message Handling System" is derived from the primary use of the system, i.e., the exchange of interpersonal messages. Consequently the message handling standards define fields for the recipient(s), carbon copy recipients, date and time, subject as well as references to other messages.

Message handling services have a big advantage when compared with other communication services: they are a store and forward systems, e.g., originator and recipient are not taking part in the communication simultaneously. This characteric is especially useful when originator and recipient are living in different time zones and a common usage of the system is to compose a message late in the evening, hand it over to the system and the message is read by the recipient the following morning. Interruptions of ongoing work, as is common with the ringing of the telephone, no-longer prevails; the message is read by the recipient at his chosen time.

2. History

Electronic message systems are nothing new (consider the worldwide telex service). The telex service, however, is not a store and forward service but is based on circuit switching. In addition, the functionality of telex services is way below the services of a modern message handling system. On the other, hand requests for more functionality have only been awakened by the proliferation and interconnection of data networks and the ever decreasing costs of electronic processing power and storage mediums.

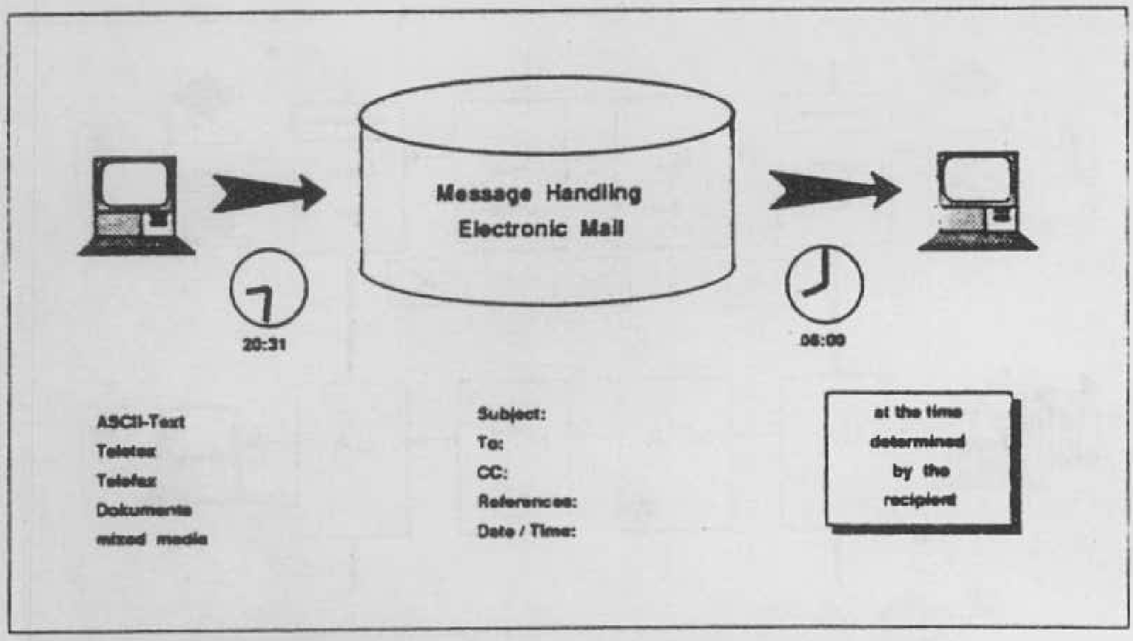


Figure 2-1: Message Handling Systems are Store and Forward Systems

The first data network, not used entirely for a closed application and in addition with a wide geographic distribrution, was the ARPA network in the USA. First the object of research itself, it soon was utilized for the information transfer between researchers. This transfer was excecuted mainly in the form of file transfers. The researchers soon felt the need to transmit next to the data in the file also messages. This need probably has been awakened to a large part because different researchers have been living in different time zones.

At first, files have been exchanged with specific bilaterally agreed names and as soon as such a specific name has been detected in a directory the recipient knew that it must be a message. However, this message system based on pure file transfers did not provide any ancillary functional services and soon a first version of a more functional message system was developped. For the actual message transfer, this system was still based on the file transfer mechanism. Through several revisions the functionality has been enhanced and the current definition (RFC 821 and RFC 822) has probably achieved more implementations in more operating systems and on more hardware types than any other message handling system.

Following the example of ARPA other networks, and in particular multi-access computer systems, have implemented message handling systems; however, none of these systems have reached the wide-spread importance as did the ARPA network (c.f. table 2-1).

1970-1975	**Development in the ARPA-Network**
1975-1980	**Introduction into Main Frame Computers**
1978	**Establishment of IFIP WG 6.5**
1979-1980	**IFIP develops MHS-Model (UA / MTA)**
1980	**CCITT proposes the MHS topic for the following study period (not an urgent study point)**
1980-1981	**Inofficial preparatory CCITT work**
1981-1983	**CCITT develops the X.400 recommendations**
1984	**Final adoption of the X.400 recommendations** **Splitting of the problem area into several study points for the new period**
1985-1987	**Collaboration with ISO** **Major restructuring of the recommendations**
1988	**Adoption of the Blue Book versions**

Table 2-1: The Evolution of the Message Handling Systems

Realizing that the different systems are imcompatible, and detecting the growing need for interconnecting the different electronic mail systems, the Technical Committee 6 (data communication) of IFIP (International Federation for Information Processing) established a working group (WG 6.5). The charter of this working group directed it to study international message handling systems. It is important to note that IFIP is not an organization that produces standards. In this case, the IFIP WG 6.5 was a forum for the open exchange of information between scientists working in the field, to develop conceptual models and architectures in anticipation of future standards work.

The North-American subgroup, in which a considerable expertise was concentrated in the years 1979 and 1980, defined a model that was adopted by CCITT. This model is still guiding the structure of message handling systems. The transfer of knowledge from the IFIP working group to CCITT was accomplished because many members of the IFIP working group became members of the CCITT group working on the message handling recommendations.

While CCITT was completing its work on message handling systems, the IFIP working group 6.5 worked out a scheme for a user friendly naming convention and researched the foundations for an international directory system. The two documents resulting from this research have both been introduced to CCITT which carried the work further. Recently, the IFIP working group 6.5 has finished the definition of a gateway between the RFC-822 and X.400 systems. Currently, the group is studying communication, the organization of communication within groups and has started research in multi-media multi-mode (real-time and non-real-time) conference systems.

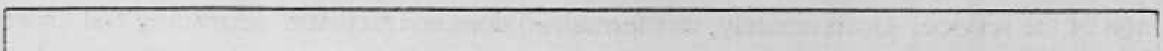
CCITT works in 4 year study periods, and at the end of each period new study points for the next period are formulated in the form of questions. Thus, at the end of the period 1977 to 1980, CCITT established a question to study message handling systems. However, because the end of a period is a major interruption of the standardization process, actual work on the definition of message handling systems could not be taken up before the end of 1981. For many members of CCITT anticipating to work on the message handling system this long delay between forming the question in the spring of 1980 and the actual start of work appeared too long. Thus, an unofficial group was formed to start work during the "interregnum" period. This preparatory work gave the group a good headstart and by spring of 1984 the first set of 8 recommendations were completed and subsequently published in the Red Book.

This series of recommendations, i.e., standards, that regulate the communication between public message handling systems as well as the communication between public and private message handling systems. These eight recommendations are issued in one volume (Fascicle is the CCITT term) of the Red Book and are commonly known under the name "X.400" (c.f. Table 2-2).

The 1984 standards are in some areas incomplete and after the completion of the 1984 version, CCITT continued to improve the standards. The study period 1985 to 1988 is marked by the fact that the problem of message handling systems has been divided into several study points (questions) and collaberation with ISO, the International Standards Organization, was achieved. The result of this collaboration is the fact that by 1988 both organizations will publish "aligned" texts as standards for message handling systems (they differ only in editorial conventions and some minor aspects reflecting the fact that CCITT produces "recommendations" for public service providers and ISO produces "standards" for general applications). It is worth noting that the collaboration between CCITT and ISO has not been restricted to message handling systems. It now includes open system interconnection (OSI) and the directory services as well.

The revisions are now being published in the Blue Book and represent a major expansion of the standard. The original eight recommendations have been restructured and now there exist twenty-two of them. During the restructuring some of the recommendations of the old X.400 series have received numbers in the X.200 series, i.e., they belong now to the general OSI communication model. Furthermore, the recommendations describing the services have received F-series numbers. The table 2-2 shows the relationship between the recommendations of 1984 and those of the new ones.

The recommendations that are now in the X.200 series will also be published as international standards by ISO. This fact indicates that the CCITT group that worked out the first recommendations between 1981 and 1984 did pioneering work for the application layer of the OSI model. On the other hand, ISO defined in the meantime a structure for the application layer.



1984	→	1988	
System Model - Service Elements	X.400	F.400	System and Service Overview
		F.401	Naming & Addressing for Public MH Sen
Basic Service Elements and Optional User Facilities	X.401	X.402	Overall Architecture
		X.403	Conformance Testing
		X.407	Abstract Service Definition Conventions
Encoded Information Type Conversion Rules	X.408	X.408	Encoded Information Type Conversion R
Presentation Transfer Syntax and Notation	X.409	X.208	Abstract Syntax Notation One (ASN.1)
		X.209	Basic Encoding Rules for ASN.1
Remote Operation and Reliable Transfer Server	X.410	X.218	Reliable Transfer Model and Service
		X.228	Reliable Transfer Protocol Specificatio
		X.219	Remote Operations Model, Service and Notation
		X.229	Remote Operations Protocol Specifica
Message Transfer Layer	X.411	F.410	Public Message Transfer Service
		X.411	Message Transfer System: Abstract Sen Definitions and Procedures
		X.413	Message Store: Abstract Service Definiti
		X.419	Protocol Specifications
		F.415	Physical Delivery Service Intercommunic
Interpersonal Messaging User Agent Layer	X.420	F.420	The Public IPM Service
		X.420	Interpersonal Messaging System
Access Protocol for Teletex Terminals	X.430	T.330	Telematic Access Protocol
		F.421	Intercommunication Telex / IPM Service
		F.422	Intercommunication Teletex / IPM Servio

Table 2-2: The CCITT Recommendations of 1984 and 1988

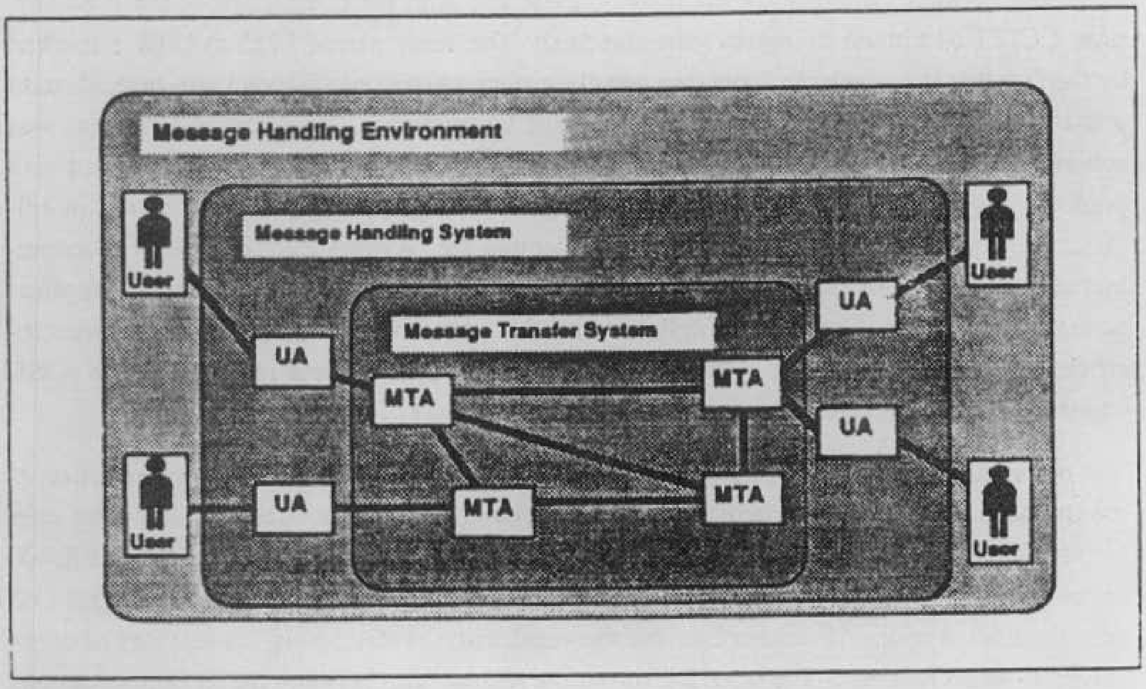


Figure 3-1: The Model of the Message Handling System (1984)

Unfortunately, this structure is not reflected in the recommendations of 1984 and was one of the main reasons for the major restructuring of the recommendations. The new texts have a complete new appearance to the reader and now contain also more precise and formal definition of the services. Unfortunately, this formalism does not facilitate the reading and understanding of the texts.

3. The Model

The recommendation X.400 defines a model that describes the basic relations between the components of the message handling systems. This model is an onion skin model. The innermost skin, the message transfer system, relays messages from MTA (message transfer agent) to MTA. Messages enter this transfer system via a submission protocol and leave it via a delivery protocol (c.f. figure 3-1).

The middle skin, the message handling system, contains the user agents (UA). The user agents assist the user of the message handling system on the one hand and they engage in submission and delivery actions with the message transfer agents.

The outermost skin, the message handling environment, is populated by the users who utilize the message handling system for the communication of messages.

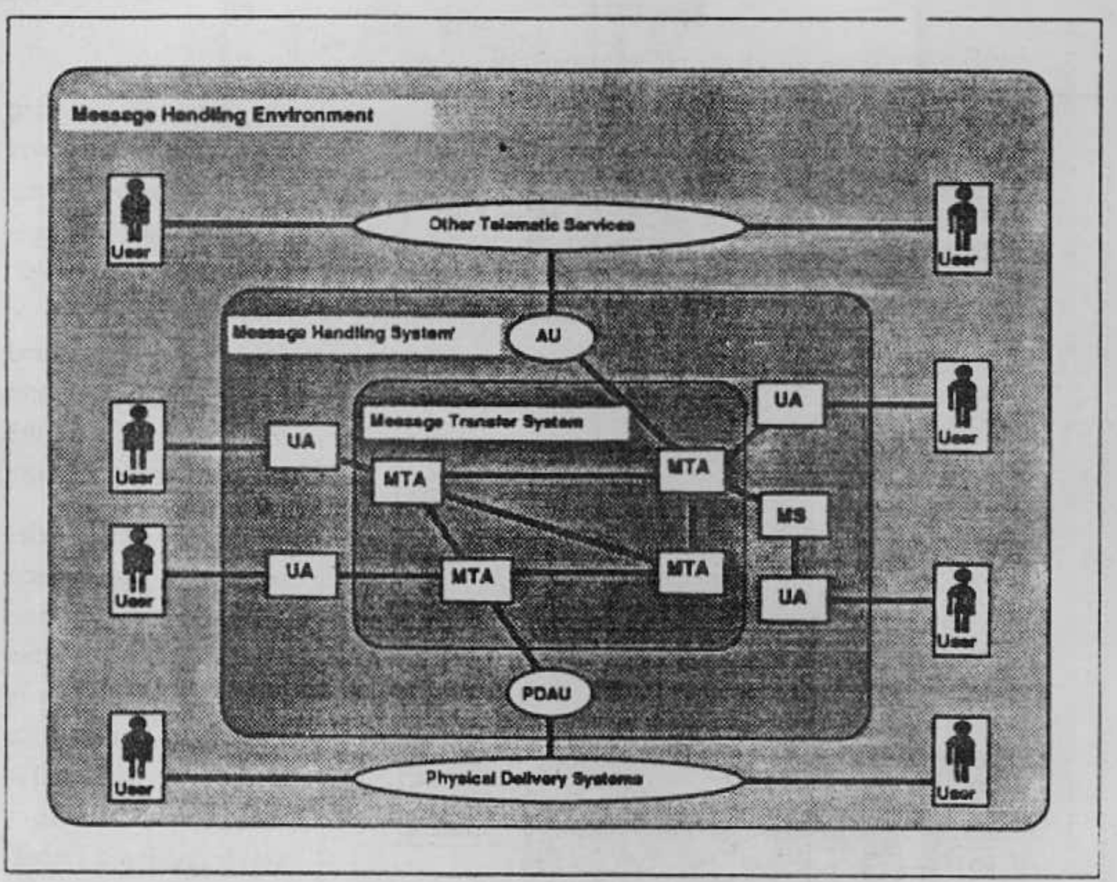


Figure 3-2: The Model of the Message Handling System (1988)

In the 1988 version, this model is enhanced and the message handling system now contains entities for message stores (MS) and access units (AU) for so-called indirect users. These indirect users normally employ other telematic services (e.g. teletex) for their daily communication. By means of the access units the message handling system is now open also for those users (c.f. figure 3-2).

A special access unit (PDAU = physical delivery access unit) establishes a connection with the regular mail service. The transition from the message handling systems to the regular mail system is defined extensively in the recommendations of 1988; these definitions provide that the special mail services (e.g. registered mail, special delivery, etc.) are employed consistently by all message handling systems.

Especially for the integration of small computers (e.g. PCs) a new entity "message store" has been defined. Considering the limited storage capacity of a PC and the fact that a PC acting as user agent or message transfer agent has no possibility to negociate the sequence of message transfers with an MTA results in the necessity of a system entity that can buffer messages. A definition of this entity has been repeatedly requested by users and implementors of the message handling system. CCITT was not very keen on the definition of the message store; however, under the pressure of ISO, CCITT defined the message store and integrated it into the new recommendations.

The onion skin model makes no assumption about the physical implementation of the different entities. It is therefore possible to implement an MTA and several UAs in a single computer system as shown on top in figure 3-3. In this case the users can communicate with the system via simple terminals e.g. VDUs of the VT100 class.

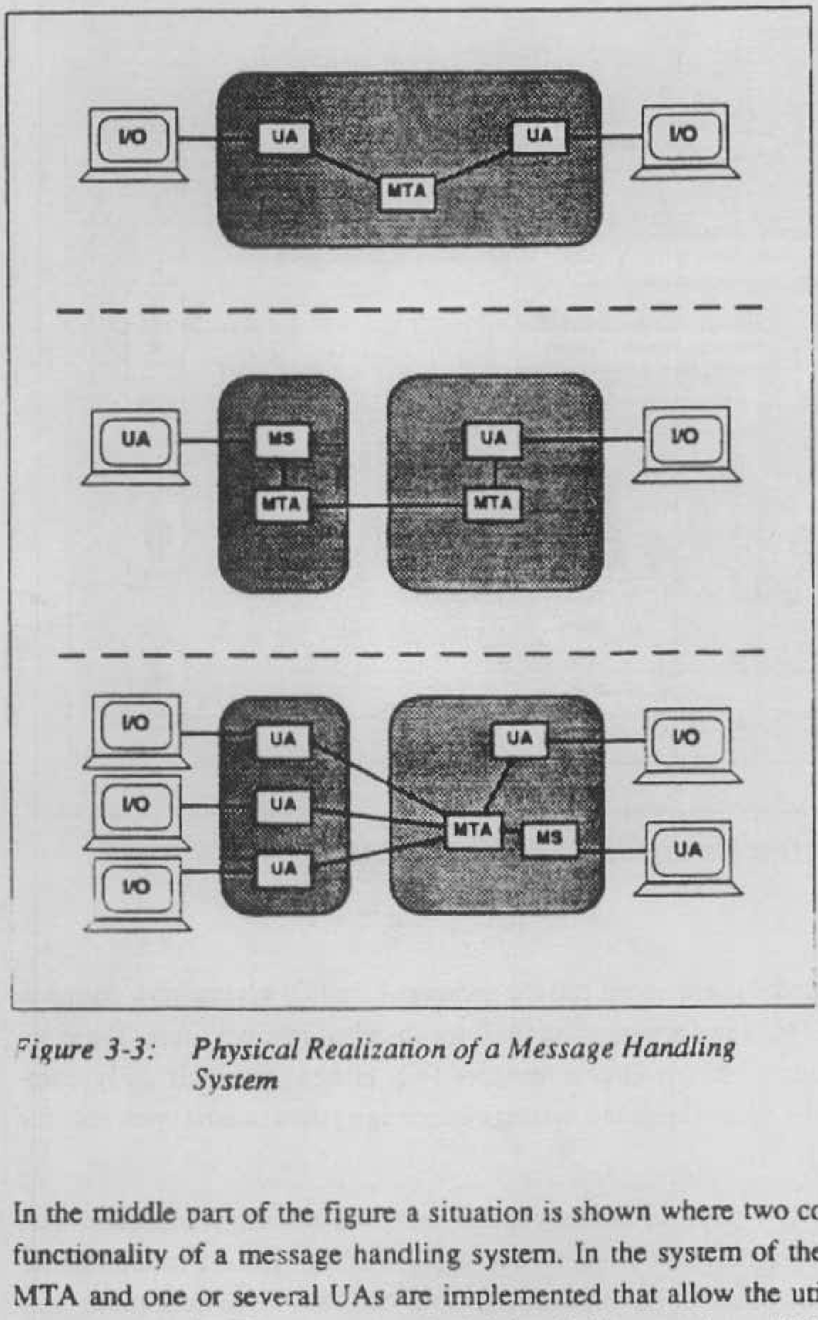
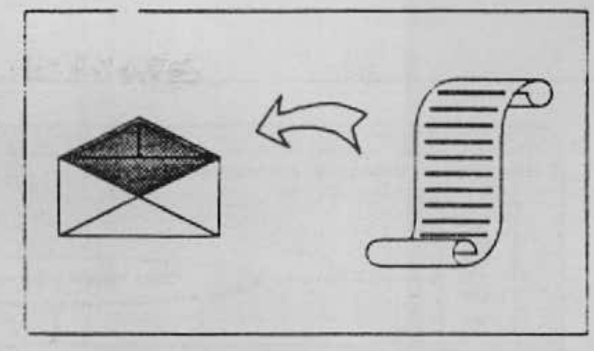


Figure 3-3: Physical Realization of a Message Handling System

In the middle part of the figure a situation is shown where two computer systems share the functionality of a message handling system. In the system of the right hand side again an MTA and one or several UAs are implemented that allow the utilization of the system via simple terminals. The system on the left hand side contains an MTA and one or several MSs (message store), the UA-functionality in this case is implemented in the terminal itself that therefore must contain some processing power (e.g., a PC).

On the bottom in the figure an implementation is shown where in the left hand computer system only UAs are implemented. The system on the right hand side contains an MTA as well as one or several MSs and UAs; this provides for the possibility of accessing the system with different classes of terminals.

The three examples shown in the figure are by no means an enumeration of all possible variants of implementations of a message handling system; the intent here is to demonstrate the unlimited variety of implementation possibilities.



As mentioned earlier a message is composed of an envelope and a content. The envelope part contains originator and recipient addresses as well as all indications necessary that influence the transfer of the message. In particular, indications are necessary to invoke the supplementary services of the message transfer system (e.g., request for a delivery notification). The content part of a message is not touched by the message transfer system except in the case where the supplementary service of a content conversion (e.g., text to facsimile) is requested.

4. Interpersonal Message System

The contents of messages that are carried by the message transfer system can be coded with any chosen method. The transfer system thus can be used to establish "connectionless" store and forward communication. However, the original need was for a system that transports messages from person to person. In order to meet with this need, the X.400 recommendations defined another skin (c.f. figure 4-1). So-called cooperating user agents that implement this recommendation establish for their users the interpersonal message service (IPMS).

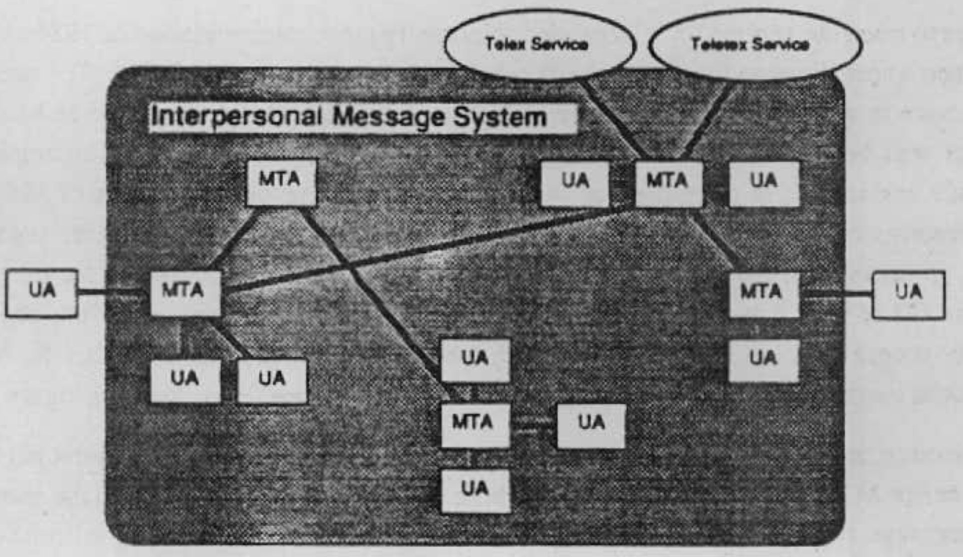


Figure 4-1: The Model of the Interpersonal Message Handling System (1984)

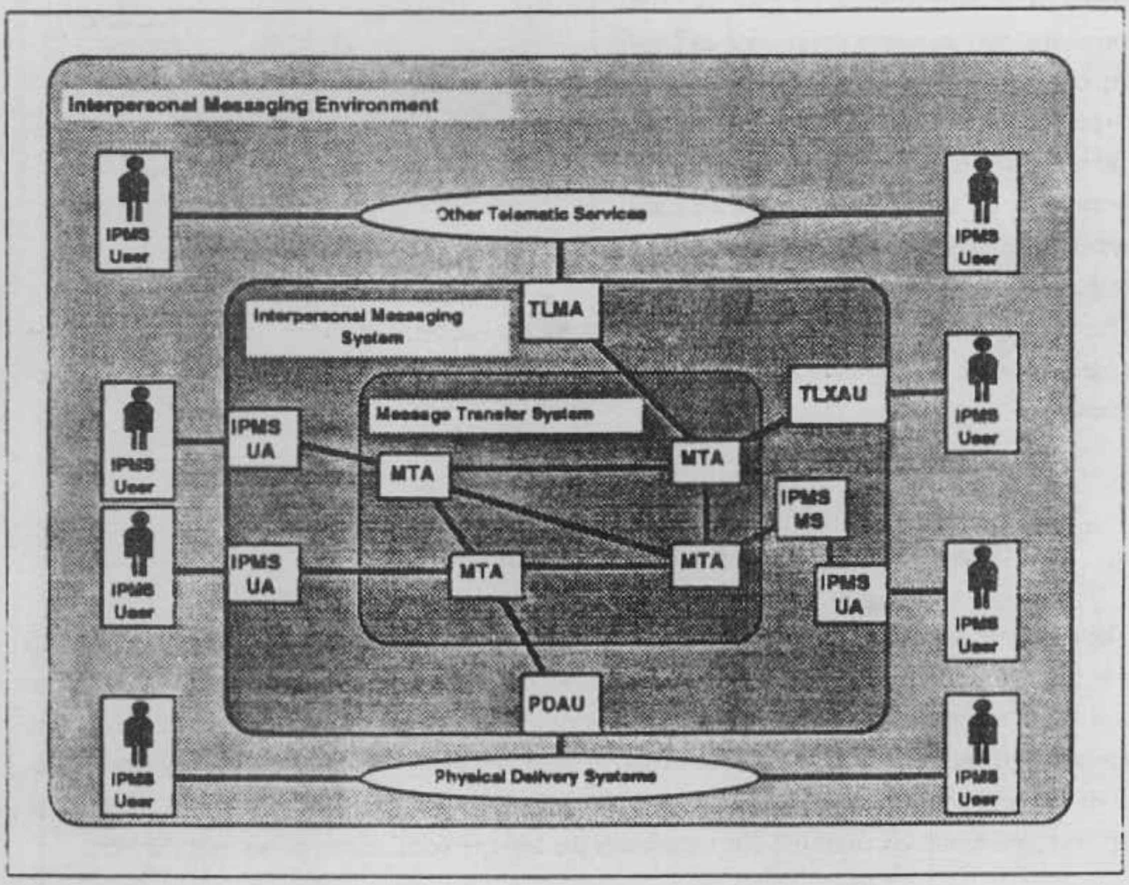


Figure 4-2: The Model of the Interpersonal Message Handling System (1988)

In order to open the service for a large user community the recommendation of 1984 already contained a specification for access protocolls for the teletex and telex service. The need for this service is still present. As a matter of fact, it is envisioned that the message handling systems will become the primary interworking facilities between otherwise incompatible telematic services. It is therefore not surprising that in the recommendations of 1988 the specifications concerning this service have been enhanced. Together with other enhancements, an access unit for telex (TLXAU = Telex Access Unit), an access unit for telematic services (TLMA = Telematic Access Unit) and respective enhancements to the physical delivery access unit, i.e., the connection with the regular mail, are defined. Also the newly introduced message store can be enhanced to an interpersonal message store (c.f. figure 4-2).

The message transfer system remains transparent for this application of interpersonal messages; hence MTAs can transfer messages whose content is coded according to the interpersonal message system as well as messages whose content is coded according to some other (even private) definition. In figure 4-1 two UAs have been drawn outside the interpersonal message system to allude to these possibilities; these UAs do not participate in the interpersonal message service, however, they make use of the message transfer system to store and forward data communication.

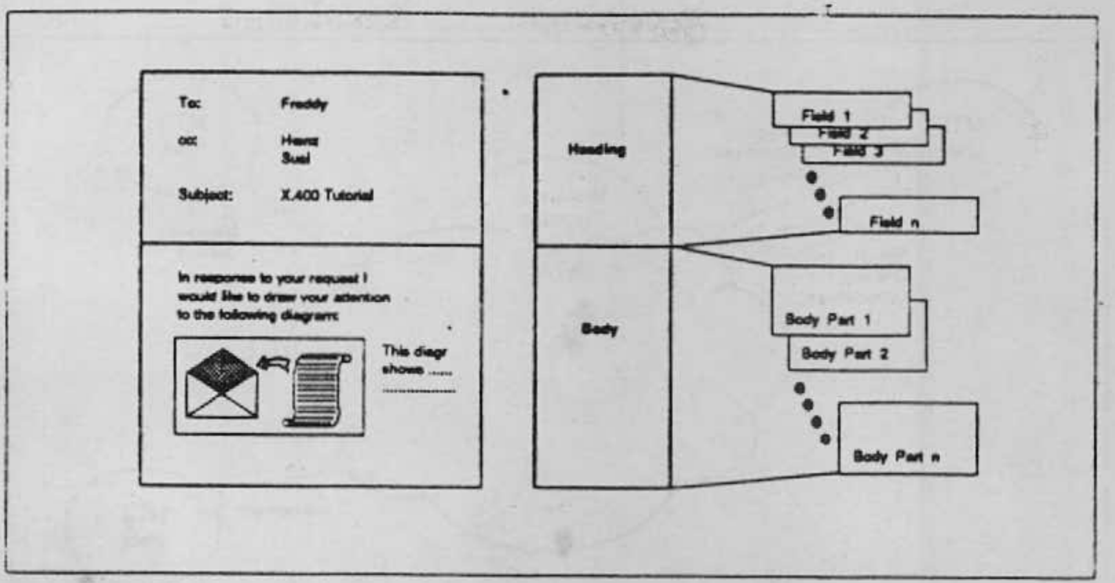


Figure 4-3: The Structure of an Interpersonal Message

The content that in the general message system model remained without further specification received the structure for the interpersonal message system. It is divided into a heading and a body. The heading is further sub-divided into fields with standard significance, e.g., "recipients", "carbon copy recipients", "subtract", "date and time", etc. (c.f. figure 4-3).

The body itself also can be structured into one or several body parts where every one of them can adhere to a different coding standard. In particular, it is possible for one such body part to contain a complete message consisting of envelope and content where the content again can be heading and body of an interpersonal message (c.f. figure 4-4). This message encapsulation is analoguous to the situation in the regular mail where a letter that has been received is put as a whole into a new envelope, possibly an extra sheet with comments added (a further body part), and the whole sent off as a new letter.

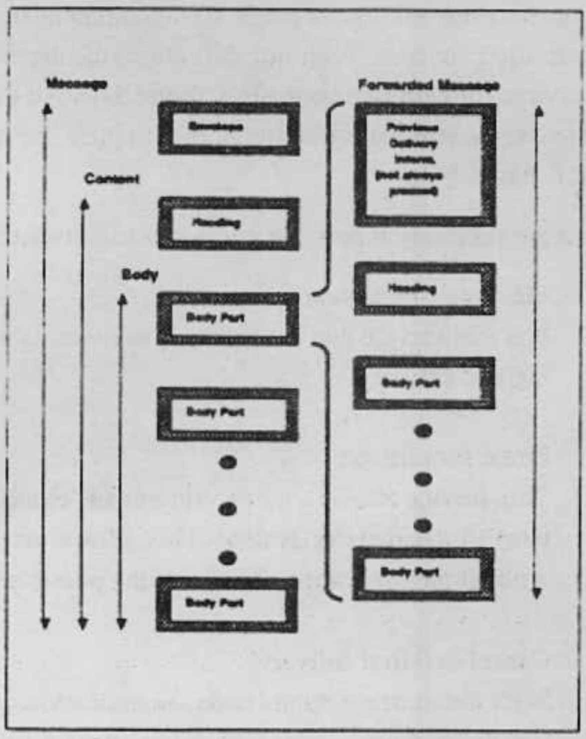


Figure 4-4: Message Encapsulation

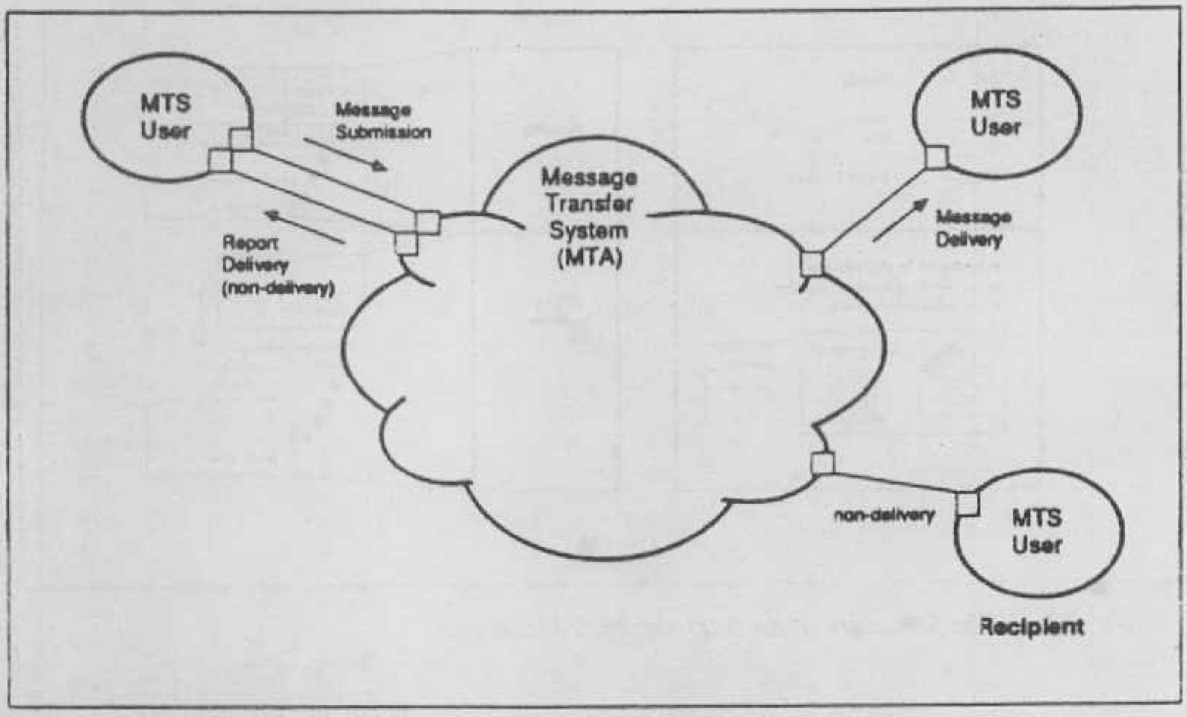


Figure 5-1: Abstract Service of the Message Transfer System

5. Abstract Service Definition

For the 1988 version of the X.400 recommendations, CCITT developed an abstract service definition concept. With this definition, the users of the message transfer system access the services through three ports (c.f. figure 5-1). All three ports are asymmetric, i.e., the message transfer system plays the role of the supplier, the user the role of the consumer of the service (c.f. figure 5-2).

On the submission port, the consumer can invoke:

- Message submission
  It is this service that is employed to submit a message to the transfer system for forwarding and delivery.

- Probe submission
  This service allows a user to submit an "empty" envelope (i.e., a message without a content) to the transfer system. This allows the testing of uncertain destination addresses without paying for the transfer of the possibly lengthy content.

- Cancel deferred delivery
  With the message submission, an indication can be given to the transfer system to begin transfer and delivery to a later time than the submission, i.e., to defer delivery. With the cancel service, such a message can be revoked.

Also on the submission port, the supplier can invoke:

- Submission control

  Via this service, the transfer system can restrict the user in the submission of messages. For example, the transfer system might instruct the user that only messages of a certain length are currently acceptable.

On the delivery port, the supplier can invoke:

- Message delivery

  Messages that have been submitted and transferred are delivered to the destination user via this service.

- Report delivery

  When submitting a message, the user can instruct the message transfer system to report on the outcome of the transfer of the message. In particular, a report can be requested for the delivery or non-delivery of the message.

Also on the delivery port, the consumer can invoke:

- Delivery control

  Similar to the submission control service but in the opposite direction, the user can instruct the transfer system to deliver only messages that fulfill certain criteria.

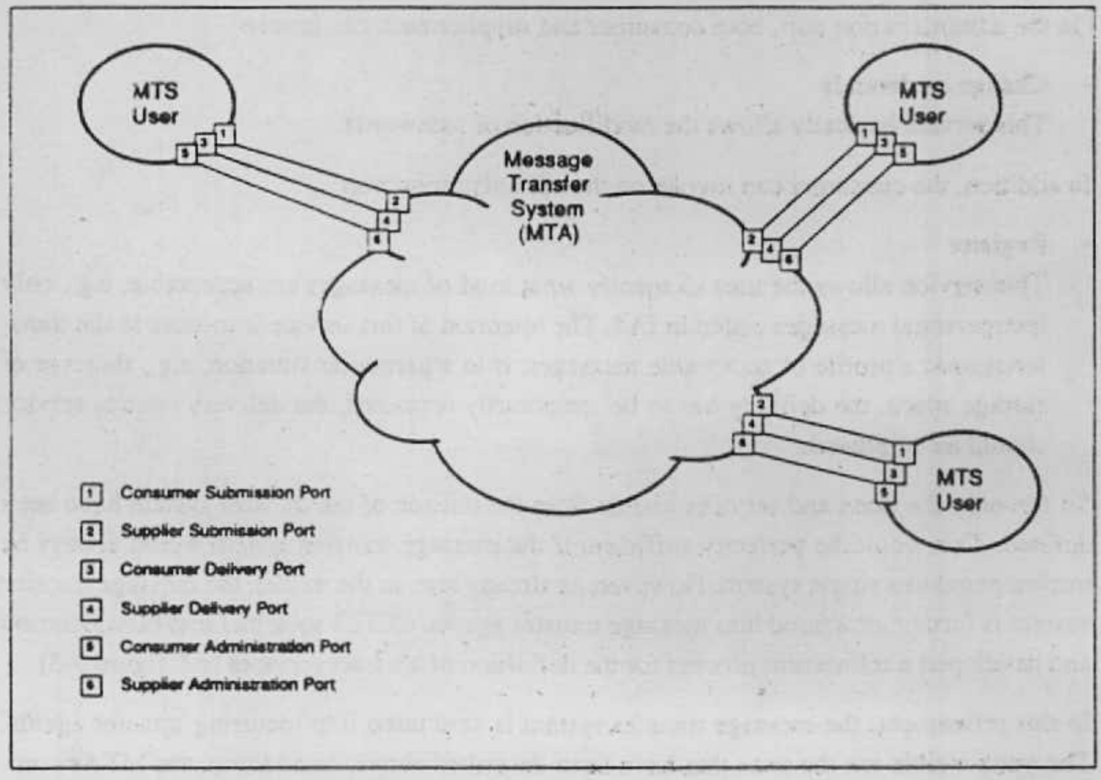

MTS User
MTS User
MTS User
Message Transfer System (MTA)
1 Consumer Submission Port
2 Supplier Submission Port
3 Consumer Delivery Port
4 Supplier Delivery Port
5 Consumer Administration Port
6 Supplier Administration Port

Figure 5-2: Port Services of the Message Transfer System

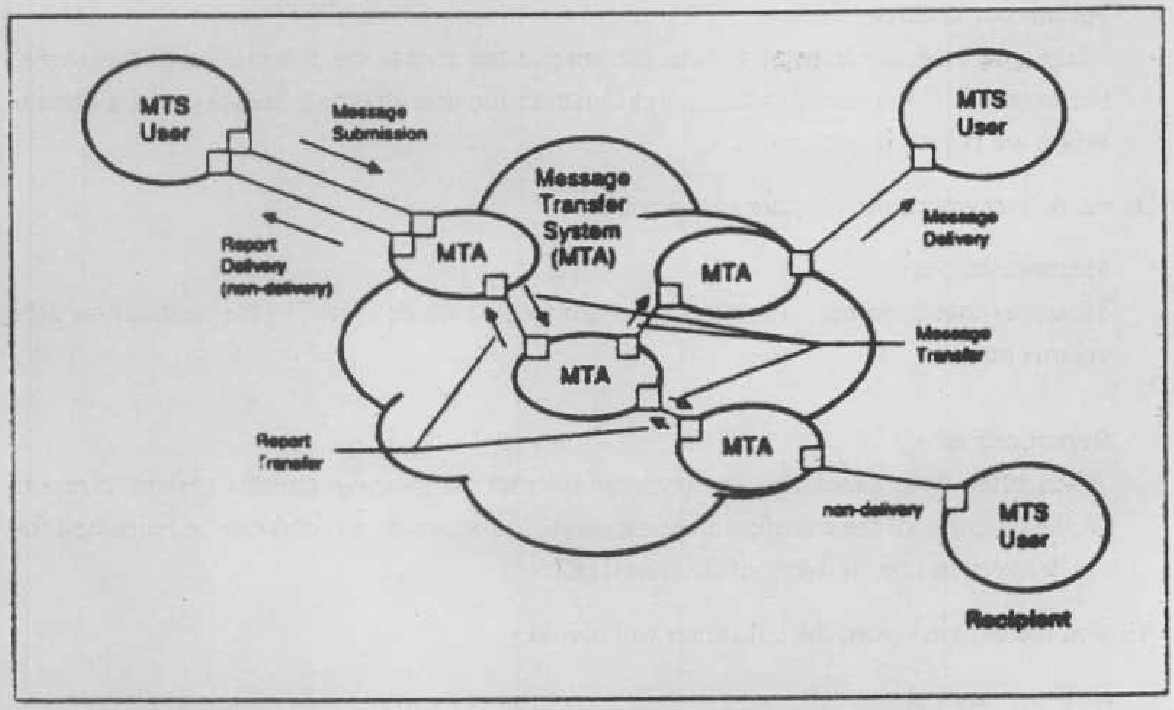


Figure 5-3: Refinement of the Abstract Service of the Message Transfer System

On the administration port, both consumer and supplier each can invoke:

- Change credentials
  This service basically allows the modification of passwords.

In addition, the consumer can invoke on the administration port:

- Register
  This service allows the user to specify what kind of messages are acceptable, e.g., only interpersonal messages coded in IA5. The intention of this service is to store in the transfer system a profile of acceptable messages; if in a particular situation, e.g., shortage of storage space, the delivery has to be temporarily restricted, the delivery control service should be employed.

So far, only the ports and services visible from the outside of the transfer system have been defined. This would be perfectly sufficient if the message transfer system would always be implemented in a single system. However, as already seen in the model, the message transfer system is further structured into message transfer agents. CCITT took this into consideration and developed a refinement process for the definition of abstract services (c.f. figure 5-3).

In this refinement, the message transfer system is structured into recurring transfer agents. The ports visible are the ones that have been described above. In addition, the MTAs communicate with each other via the symmetric transfer ports (c.f. figure 5-4); those ports are not visible from outside the transfer system.

On the transfer port, each MTA can invoke:

- Message transfer,
- Probe transfer, and
- Report transfer.

This refinement mechanism is a powerful tool. It makes extensive use of the macro capability of the ASN.1 (abstract syntax notation). Currently, ISO is reluctant to accept this mechanism as a general tool for the description of layer 7 services although it is accepted within the specification of the message handling system. CCITT, on the other hand, works on the elaboration of this concept; a special rapporteur is assigned this topic in the new study period (1989 to 1992).

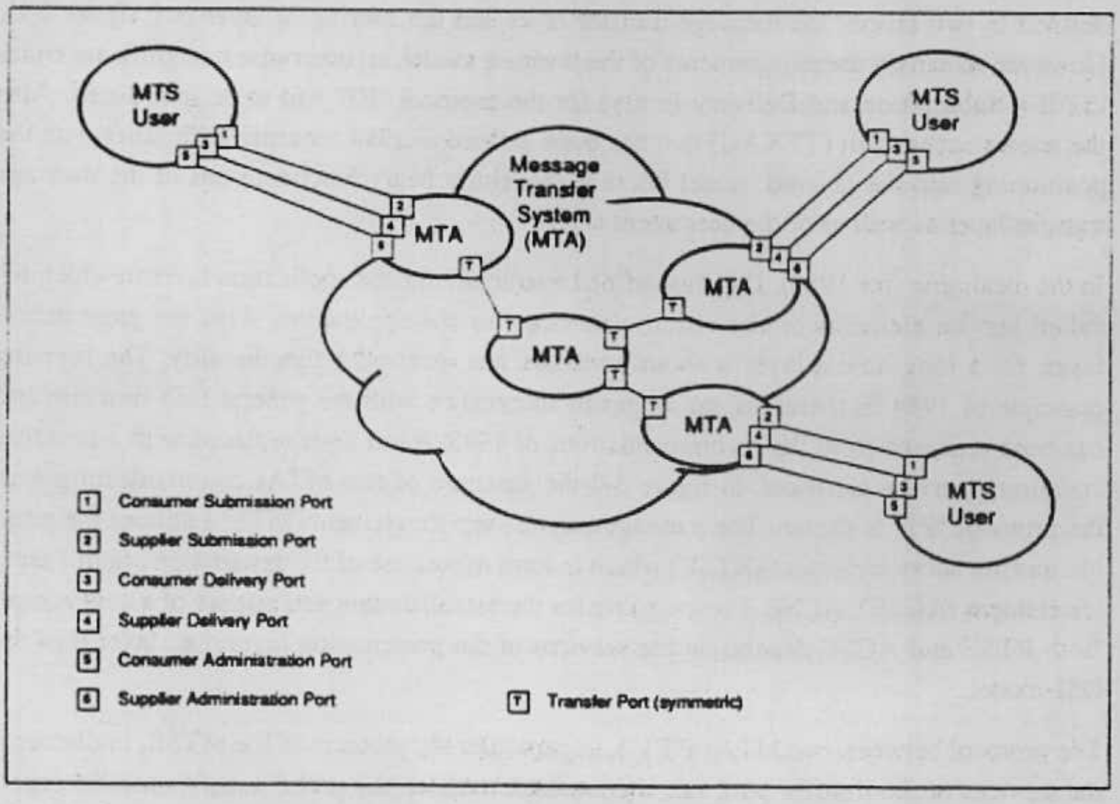

MTS User
MTS User
MTS User
Message Transfer System (MTA)
MTA
MTA
MTA
MTA
1 Consumer Submission Port
2 Supplier Submission Port
3 Consumer Delivery Port
4 Supplier Delivery Port
5 Consumer Administration Port
6 Supplier Administration Port
T Transfer Port (symmetric)

Figure 5-4: Refined Port Services of the Message Transfer System

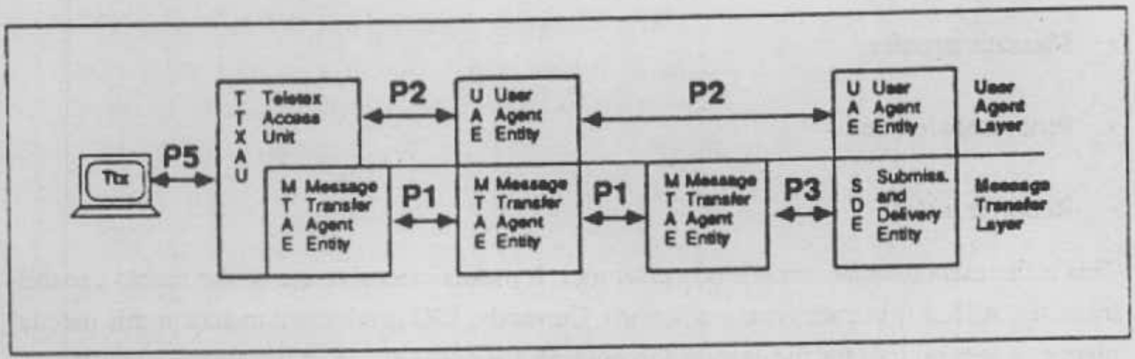


Figure 6-1: The Application Layer Structure (1984)

6. The Structure of the Application

In the recommendations of 1984 the protocol between two MTAs has been named "P1". The protocol between two cooperating user agents as "P2". A further protocol ("P3") has been defined for the communication between a remote user agent and a MTA (this protocol, however, was unsuitable for the task, has never been implemented, and hence achieved no significance).

In analogy to the layering principle of the OSI-model, the message handling service has been defined in two layers: the message transfer layer and the user agent layer (c.f. figure 6-1). However, to satisfy the requirements of the layering model, an otherwise unsignificant entity (SDE = Submission and Delivery Entity) for the protocol "P3" had to be introduced. Also the teletex access unit (TTXAU) that has been defined in 1984 presents difficulties with the positioning into the layered model because this entity bears functionalities of the message transfer layer as well as of the user agent layer.

In the meantime (for 1988), ISO has defined a structure for the application layer in which so-called service elements render specific services for the application. Also the presentation layer, for a long time a layer without portfolio, has received a functionality. The layering principle of 1984 is, therefore, no longer in accordance with the general ISO structure and has been removed from the recommendations of 1988. It has been replaced with a structure containing service elements. In figure 6-2 the structure of two MTAs communicating with the protocol "P1" is shown. The message transfer service element (MTSE) utilizes the reliable transfer service element (RTSE) which in term makes use of the association control service element (ACSE). ACSE is responsible for the establishment and release of a connection. Both RTSE and ACSE depend on the services of the presentation layer, i.e., layer 6 of the OSI-model.

The protocol between two MTAs ("P1"), in particular the protocol of the MTSE, implements the services of the transfer port, i.e., the message transfer, the probe transfer, and the report transfer service (c.f. figure 6-2).

The reliable transfer service is a service element that hides the particulars of the OSI protocols. The MTSE hands over to the RTSE a complete message; this message is then segmented by the RTSE and transmitted to the partner MTA through the OSI layer services. The RTSE assures that those services are employed correctly. In particular, even in the case of a complete disruption of the connection, the message, probe, or report is neither lost nor mutilated or doubled.

The protocols of "P3" and "P7" in addition make use of the remote operation service element (ROSE) (c.f. figures 6-3 and 6-4). ROSE is a simple protocol that permits the triggering of an action in the partner entity. Such an action is for example the receipt of a message. The action always responds to the initiator with either a result or an error message. In many cases the result contains proper message system data, e.g., if a message is requested from the store.

For these two protocols ("P3" and "P7") the recommendations allow the inclusion of the reliable transfer service element (RTSE), however, this is not mandatory.

The service elements specific to protocols "P3" and "P7" cater to the submission of messages and probes (submission port services) the delivery of messages or reports (delivery port services) as well as the administration of the connection (administration port services).

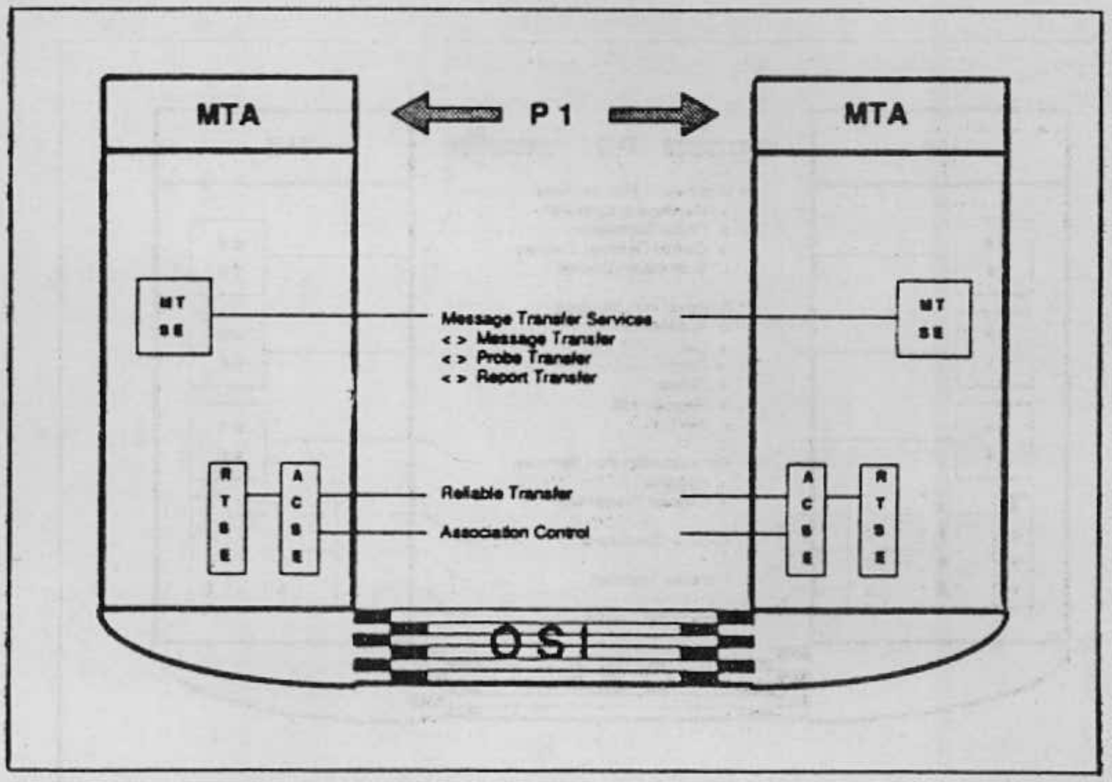


Figure 4-2: The Application Layer Structure for the Protocol "P1" (1988)

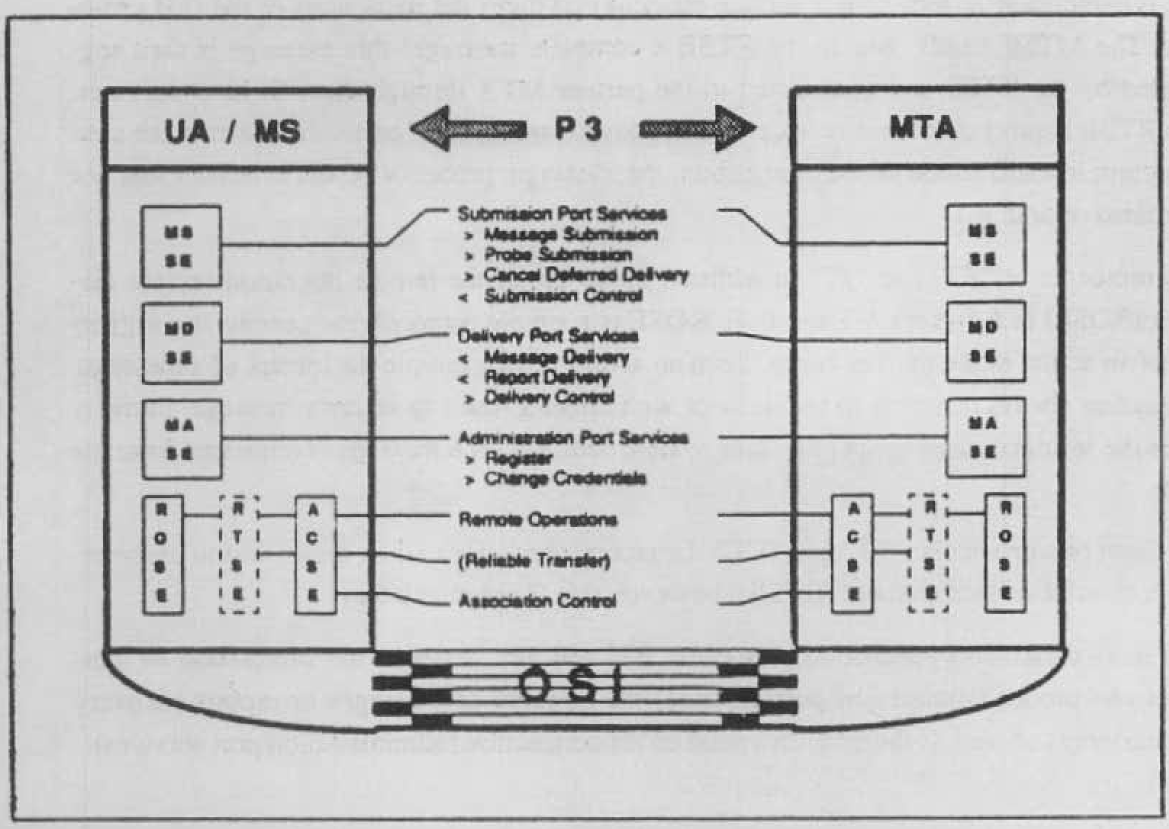


Figure 4-3: The Application Layer Structure for the Protocol "P3" (1988)

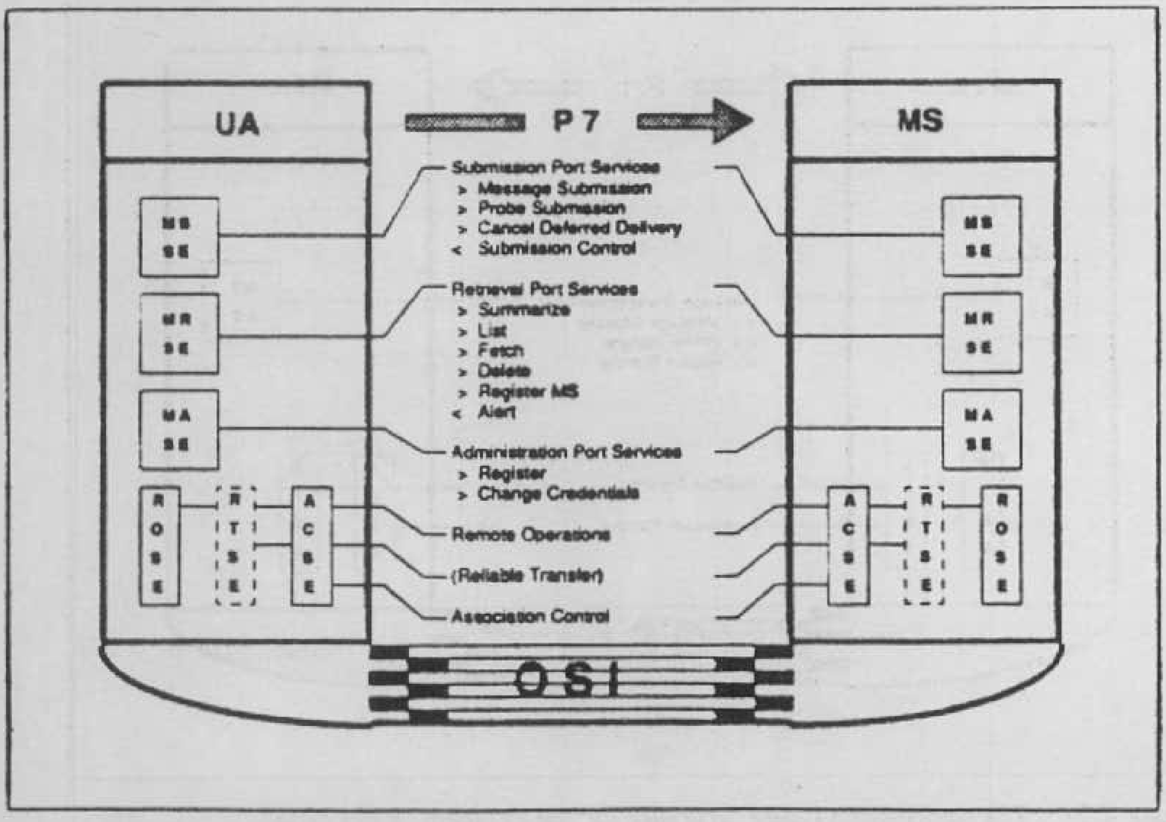


Figure 4-4: The Application Layer Structure for the Protocol "P7" (1988)

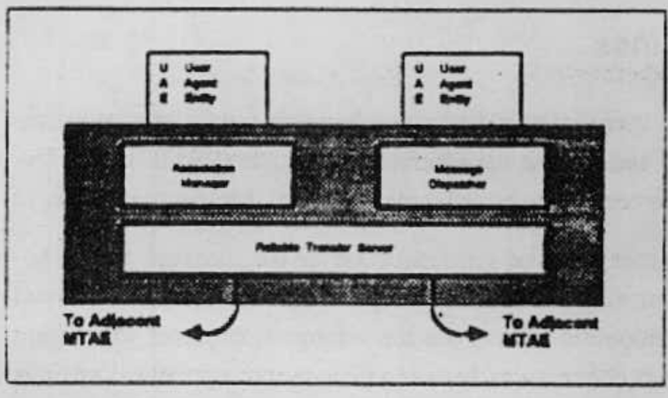


Figure 6-5: The intexnal Structure of an MTA (1984)

The protocol "P7" is nearly identical to the protocol "P3" except that delivery port services are replaced by the retrieval port services. This reflects the fact that the message transfer system delivers a message to the message store from where it has to be retrieved by a UA in part or as a hole.

The recommendations of 1984 knew a service element "hold for delivery". (Note: this is a service element of the message handling service and not of the application structure). With this service element an MTA could be instructed to hold messages back that would otherwise have been delivered. In the recommendations of 1988 this service has been refined and relegated to the administration port services. The transmission of messages (in particular, submission, transfer, or delivery) can be restricted with respect to their grade of service (three levels), their total length, as well as their coding of the content (e.g., text, facsimile, etc.). This service is no longer unidirectional but encompases next to the known "hold for delivery" also a "hold for submission" and "hold for transfer".

The progress of the standardisation effort between 1984 and 1988 shows clearly when the two sets of recommendations are compared with respect to the internal structure of an MTA and their respective procedural description. In 1984 some remarks about the presence of an association manager and a message dispatcher were sufficient (c.f. figure 6-5). In the recommendations of 1988, the enhanced functionality has been taken into account and the recommendations contain detailed procedural descriptions how messages, probes, and reports are treated within an MTA (c.f. figure 6-6).

The two figures illustrate the big step between the two cycles of recommendations: The first figure is taken out of the recommendations of 1984, the second one out of those of 1988. The figures serve only as an illustration here for the big step in the degree of details in the two sets of recommendations; an explanation of the details contained in the figures, however, is beyond the scope of this article.

7. Management Domaines

In the X.400 series recommendations there exists a distinction between public or administration management domains (ADMD) and private management domaines (PRMD). It is forseen that in some countries more than one administration management domain may exist.

The X.400 series recommendations cater for the stanardization of the message traffic between administration management domains (within a country or across country boundaries) as well as the message traffic between public and private management domaines (c.f. figure 7-1). This does not indicate that direct connections between private management domaines are not possible, however, such connections are beyond the scope of the CCITT standards and, therefore, are not included in the recommendations. Omission from the standard does not prohibit such transfers.

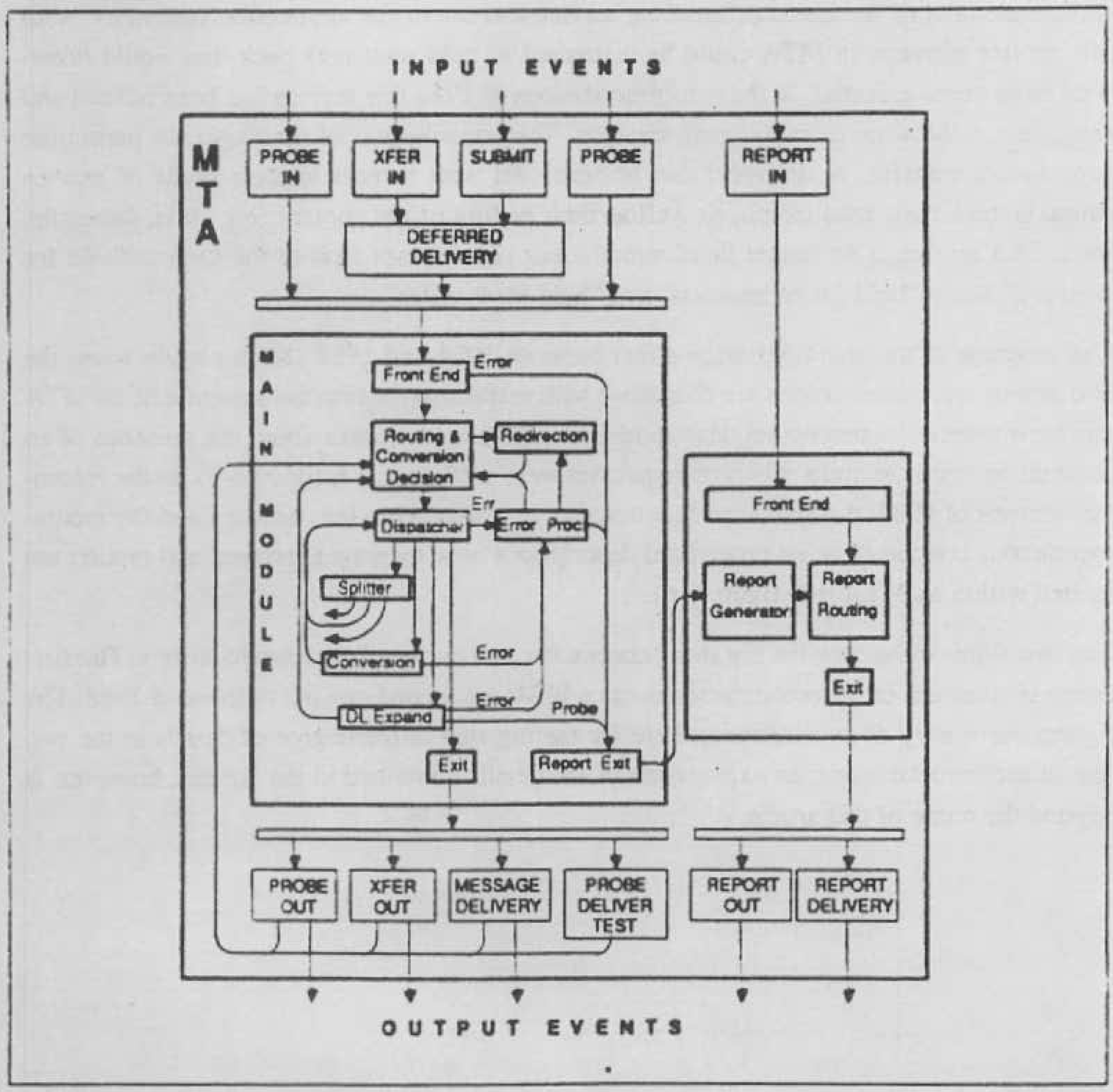


Figure 6-6: The internal Structure of an MTA (1988)

The administrations view the message transfer system in the administration management domain as a central switching system (ADMD). This system allows message communication between any two user agents in the world be they connected directly to an administration domain or indirectly via private management domain. However, as the addressing capabilities on the envelope of a message allow for naming only one private management domain, these must be connected directly to an administration management domain; any user agent that is connected to a private management domain that has no direct connection to an administration management domain is not seen by the latter, i.e., messages destined for such a user agent cannot be transferred through the public administration management domains as their addresses cannot be resolved into transfer routes.

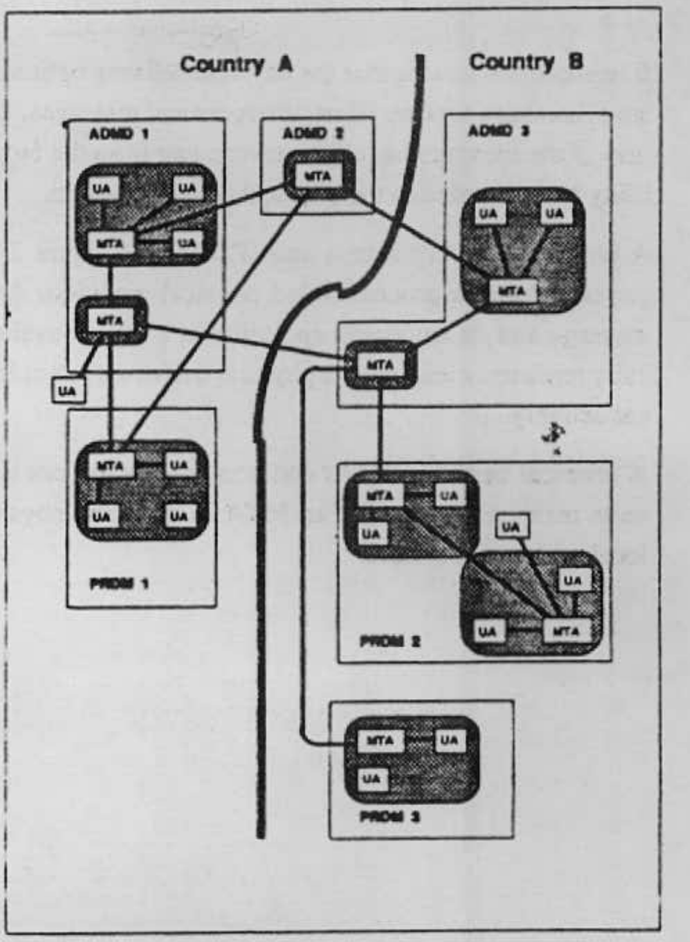


Figure 7-1: Management Domains

8. Physical Delivery

The value of the message handling service was increased by connecting it to physical delivery (PD) systems such as the traditional postal service. This will allow for hardcopy delivery of messages originated within the message handling system, and in some cases will aloow for the return of notifications from the physical delivery services to the message originator.

All users of the message handling service have the ability to generate messages for subsequent physical delivery. This is assured by a appropriate address form, the postal O/R address, that can be used as a recipient in the envelope part of any message.

It is important to note that the physical delivery option has also been defined for the interpersonal message service. Thus, interpersonal messages, the (currently) most important application of the message handling service, can from the beginning of the physical delivery possibility be forwarded to the physical delivery system.

A physical delivery access unit (PDAU, c.f. figure 3-2) converts an electronic message to physical form, a process called physical rendition. An example of this is the printing of a message and its automatic enclosure in a paper envelope. The access unit passes the physically rendered message to a physical delivery system for further relaying and eventual physical delivery.

A protocol between MTAs and access units has not been defined. It is assumed that access units reside together with an MTA in the same physical system and that all interfaces are local within this system.

9. Supplementary Services

The supplementary services that the transfer system can render are listed in the table 9-1 (1984 set). Only a few of them will be explained here in this section. A more complete list is found in the annex (1988 set) and all the services are described in the respective recommendations.

Compared to the regular mail service, it is a simple task for an electronic message handling systems to make multiple copies of a message. This supplementary service "multi-destination delivery", therefore, allows the submission of a message with several addresses on the envelope; the message handling system will create enough copies of the message to deliver one to each recipient mentioned on the envelope. For each recipient, the originator can set a flag, instructing the message system to hide all the other recipients or if the flag is not set allow the recipient to find on the delivered envelope the addresses of all other recipients.

The message handling system offers the supplementary service "content conversion": It is therefore possible for a recipient having only faximile capabilities to receive a message that originally was coded as a text message. The fact that a content conversion has been applied is reflected as an indication on the delivery envelope. The conversion is implicit and determined by the respective capabilities of the originator and recipient equipment; however, the originator can also ask for an explicit conversion or he can instruct the message handling system to perform no conversion at all. Prohibiting conversions might render a message undeliverable.

A further supplementary services is the possibility of transferring a probe. A probe is basically an envelope without any content. A possible usage of

Basic	**Access Management** **Content Type Identification** **Converted Identification** **Delivery Time Stamp Indication** **Message Identification** **Non-Delivery Notification** **Original Encoded Information Types** **Registered 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** **Multi-Destination Delivery** **Prevention of Non-Delivery Notification** **Return of Contents**
Conversion	**Conversion Prohibition** **Explicit Conversion** **Implicit Conversion**
Query	**Probe**
Status and Information	**Alternate Recipient Assignment** **Hold for Delivery**

Table 9-1: The Supplementary Services of the Message Transfer Service (1984)

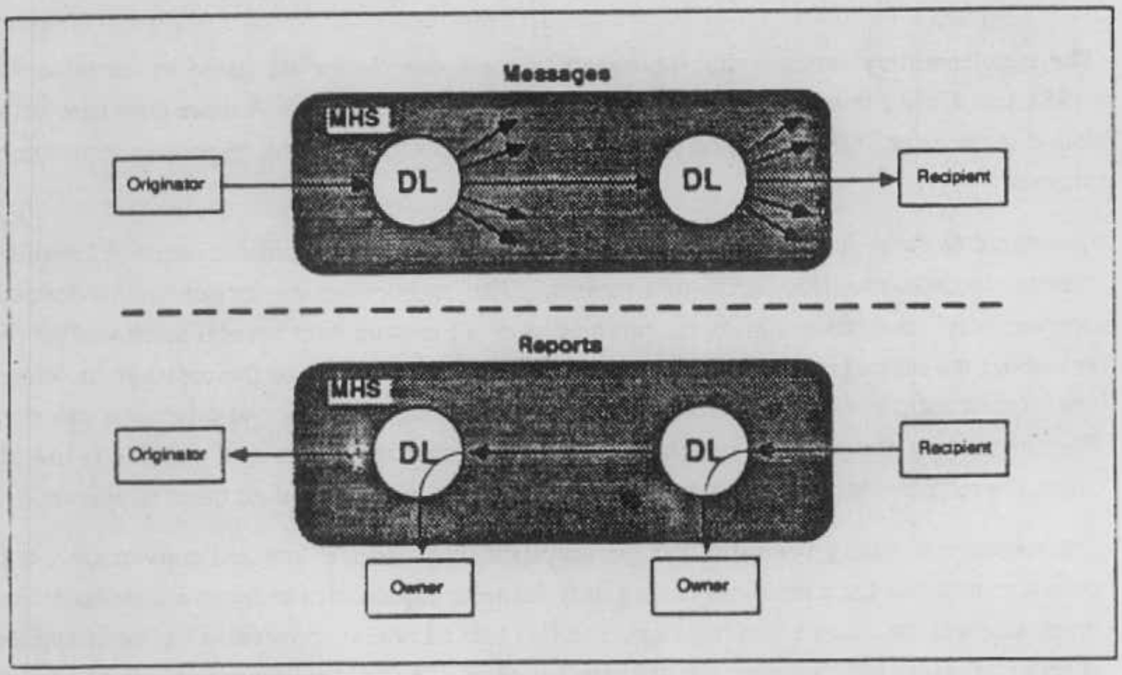


Figure 9-1: Distribution Lists

the probe is in the case where a long document should be transmitted to a recipiant with whom no prior communication has been taken part. The delivery or non-delivery notification returned as a result of the probe transmission indicates whether the recipient address is correct (i.e., whether the transfer system can deliver the message) and it also indicates whether content conversion would be necessary when the docoment is transferred.

The "probe recipient" itself is oblivious to the fact of such a probe transmission. The probe travels only up to the MTA that would perform the actual delivery of a real message; there it is converted into a report that is returned to the originator.

For the recommendations to be published in 1988 two essential new supplementary services have been defined: distribution lists and secure messages.

The address of a distribution list is in no way different from one of a normal recipient and an originator has no knowledge that the addresses in a message are to such a distribution list. However, when a message reaches the MTA responsible for the distribution list the MTA expands the distribution list onto the envelope, i.e., all member addresses of the distribution list are added as recipients to the envelope of the message.

Distribution lists can itself be members of other distribution lists. To safeguard against endless expansion loops an appropriate system has been implemented. However, because this system works only in the MTAs adhering to the 1988 recommendations and 1984 MTAs lack this mechanism, any message arriving from (or through) a 1984 MTA is prohibited from enacting an expansion. A non-delivery notification is returned to the originator.

As soon as a message reaches the first expansion point, a delivery notification (if requested) is returned to the originator. when the replicated messages travel further through the system, they may again trigger a notification. However, these notification are not relayed to the initial originator but are deflected to the "owner" of the distribution list (c.f. figure 9-1).

Security in the message handling system refers to the security of a message against casual or deliberate inspection by third parties. An authentication system based on the assymentric public key crypto system, originator and recipient can agree on a mutual key for encyphering and decyphering of a message. The MTAs have to be included in this security concept as they need the information on the envelope to route the message and perform the requested supplementary services.

Without further explanation of the details envolved, the table (c.f. Table 9-2) shows which supplementary services have been defined with respect to which security aspects. The table also gives an indication as to which security aspect can be employed between which system components.

Elements of Service	UA - MS	MS - MTA	UA - UA	UA - MTA	MTA - MTA	MTA - UA	MS - UA
Message Origin Authentication			o	o			
Report Origin Authentication					o	o	
Probe Origin Authentication				o			
Proof of Delivery			o				o
Proof of Submission						o	
Secure Access Management	o	o		o	o	o	o
Content Integrity			o				
Content Confidentiality			o				
Message Flow Confidentiality				o	o		
Message Sequence Integrity			o				
Non-Repudiation of Origin			o	o			
Non-Repudiation of Submission						o	
Non-Repudiation of Delivery			o				o
Message Security Labelling	o	o	o	o	o	o	o

Table 9-2: The Supplementary Services for Secure Messages

10. Electronic Business Data Interchange

Since several years, ISO has been working on the definition of formats to allow the exchange of business data (EDI, i.e., orders, invoices, etc.) from machine to machine. Trials of such EDI exchanges have for example taken place within the community of large chemical organizations in Europe.

CCITT is currently working on a recommendation of how such EDI data could be transported with the store and forward message handling system. There are many advantages to using the MHS for such a purpose. Today's implementations of EDI rely on access to the administrative computers via remote job entry facilities in those computers; however, those entries could be misused to gain other information from the systems involved. With the use of MHS, all messages arrive at the computers wrapped in an envelope and it is only the receiving computer that can open this envelope and perform necessary operations and always under its control.

An intermediate solution has been adopted under the guidance of the European communities. In this solution, the EDI data is coded as prescribed by the respective ISO standard (IA5 text) and transported like an interpersonal message. All header fields that otherwise are so useful for the communication between humans are to be ignored.

Basically, the direction CCITT is taking with its definition does not depart far from this intermediate solution. A new content type (PEDI) is being defined that consist of a header and a body. The body also contains the unaltered IA5 EDI text as specified by ISO. The header, on the other hand, is an extract of the EDI header in a format conforming to the X.400 world. Through this mechanism, it becomes possible to utilize already existing message handling services (especially retrieval by attributes from the message store).

11. Summary

Message handling systems with already a long tradition in the academic world are since a few years also being introduced in the commercial world. The 1984 set of recommendations of X.400 allow the interconnection of all those (so far) isolated message handling systems into one global system that can provide a service worldwide.

Having done pioneering work for application layer service elements (RTSE and ROSE), it was unfortunate that the complete application layer structure as now standardized by ISO has not been forseen correctly. This led to a complete restructuring of the 1988 set of recommendations. In addition to this restructuring, CCITT also complemented the recommendations especially in the area of interworking with the postal system and other telematic services as well as the provision for secure messages. , With the X.400 set of recommendations published in the blue book and also available as the ISO standard 10021, there exists now a complete and stable set of standards that will promote the implementation of a universal message handling service. Large private domain and administrative domain networks as well as small single user systems can cooperate to allow every message handling system user to reach any other user in the world.

However, much work still is needed in the content definition area. This will open the message handling system to other applications than interpersonal messages. For example, CCITT is currently defining recommendations to allow the transfer of business data (EDI) where the users are envisaged to be primarily administrative computer systems in large, medium, and small companies.

A. ANNEX — Definitions of Elements of Service

Note The abbreviations used in the title line have the following meanings:

MT	Message Transfer
IPM	Interpersonal Messaging
PD	Physical Delivery
MS	Message Store
PR	Per Recipient (available on a per-recipient basis)

A.1 Access Management MT

This element of service enables a UA and MTA to establish access to one another and to manage information associated with access establishment.

The element of service permits the UA and MTA to identify and validate the identity of the other. It provides a capability for the UA to specify its O/R Address and to maintain access security. When access security is achieved through passwords, these passwords can be periodically updated.

Note A more secure form of access management is provided by the element of service Secure Access Management.

A.2 Additional Physical Rendition PD PR

This element of service allows an originating user to request the PDAU to provide the additional rendition facilities (e.g., kind of paper, coloured printing, etc.). Bilateral agreement is required to use this element of service.

A.3 Alternate Recipient Allowed MT

This element of service enables an originating UA to specify that the message being submitted can be delivered to an alternate recipient as described below.

A destination MD will interpret all of the user attributes in order to select a recipient UA. Three cases can be distinguished:

1. All the attributes match precisely those of a subscriber UA. Delivery is attempted to that UA.

2. Either insufficient attributes are supplied or those supplied match those of more than one subscriber UA. The message cannot be delivered.

3. At least the minimum set of attributes required by the destination MD is supplied. Nevertheless, taking all of the other attributes into account, the attributes match those of no UA.

In case 3, an MD that supports the Alternate Recipient Assignment element of service can deliver the message to a UA that has been assigned to receive such messages. This UA will be notified of the O/R Address of the intended recipient as specified by the originator. Delivery to this UA will be reported in a delivery notification if requested by the originator.

A.4 Alternate Recipient Assignment MT

This element of service enables a UA to be given the capability to have certain messages delivered to it for which there is not an exact match between the recipient attributes specified and the name of the user. Such a UA is specified in terms of one or more attributes for which an exact match is required, and one or more attributes for which any value is acceptable. For example, an organization can establish a UA to receive all messages for which country name, Administration Management Domain name and organization name (for example, company name) are an exact match but the personal name of the recipient does not correspond to an individual known by an MHS in that organization. This permits the organization to manually handle the messages to these individuals.

In order for a message to be reassigned to an alternate recipient, the originator must have requested the Alternate Recipient Allowed Element of Service.

A.5 Authorizing Users Indication IPM

This element of service allows the originator to indicate to the recipient the names of the one or more persons who authorized the sending of the message. For example, an individual can authorize a particular action which is subsequently communicated to those concerned by another person such as a secretary. The former person is said to authorize its sending while the latter person is the one who sent the message (originator). This does not imply signature-level authorization.

A.6 Auto-Forwarded Indication IPM

This element of service allows a recipient to determine that a body of an incoming IP-message contains an IP-message that has been auto-forwarded. Thus the recipient can distinguish from that where an incoming IP-message contains a forwarded message (as described in B.32) in the body. As with a forwarded IP-message, an auto-forwarded IP-message can be accompanied by information (for example, time stamps, indication of conversion) associated with its original delivery.

Note The indication that auto-forwarding of an IP-message has occurred enables a recipient IPM UA, should it so choose, to prevent further auto-forwarding and thus the possibility of loops. In addition, a recipient IPM UA can choose whether or not to auto-forward based on other criteria (for example, sensitivity classification).

When an IPM UA auto-forwards an IP-message, it designates it as auto-forwarded. If receipt/non-receipt notification has been requested for the IP-message being auto-forwarded, the IPM UA generates a non-receipt notification informing the originator of the auto-forwarding of the IP-message. The notification optionally includes a comment supplied by the originally intended recipient. No further notification applying to the auto-forwarded IP-message is generated by any IPM UA.

A.7 Basic Physical Rendition PD PR

This element of service enables the PDAU to provide the basic rendition facilities for converting the MHS message into a physical message. This is the default action to be taken by the PDAU.

A.8 Blind Copy Recipient Indication IPM PR

This element of service allows the originator to provide the O/R name of one or more additional users, or DLs, who are intended recipients of the IP-message being sent. These names are not disclosed to either the primary or copy recipients. Whether or not these additional recipients are disclosed to one another is a local matter.

A.9 Body Part Encryption Indication IPM

This element of service allows the originator to indicate to the recipient that a particular body part of the IP-message being sent has been encrypted. Encryption can be used to prevent unauthorized inspection or modification of the body part. This element of service can be used by the recipient to determine that some body part(s) of the IP-message must be decrypted. This element of service, however, does not itself encrypt or decrypt any body part.

A.10 Content Confidentiality MT

This element of service allows the originator of a message to protect the content of the message from disclosure to recipients other than the intended recipient(s). Content Confidentiality is on a per-message basis, and can use either an asymmetric or a symmetric encryption technique.

A.11 Content Integrity MT PR

This element of service allows the originator of the message to provide to the recipient of the message a means by which the recipient can verify that the content of the message has not been modified. Content Integrity is on a per-recipient basis, and can use either an asymmetric or a symmetric encryption technique.

A.12 Content Type Indication MT

This element of service enables an originating UA to indicate the content type for each submitted message. A recipient UA can have one or more content types delivered to it. An example of a content type is the contents generated by the IPM class of cooperating UAs.

A.13 Conversion Prohibition MT

This element of service enables an originating UA to instruct the MTS that implicit encoded information type conversion(s) should not be performed for a particular submitted message.

A.14 Conversion Prohibition in Case of Loss of Information MT

This element of service enables an originating UA to instruct the MTS that encoded information type conversion(s) should not be performed for a particular submitted message if such conversion(s) would result in loss of information. Loss of information is discussed in detail in X.408.

Should this and the Conversion Prohibition element of service both be selected, the latter shall take precedence.

Note This element of service will not protect against possible loss of information in certain cases where the recipient is using an I/O device whose capabilities are unknown to the MTA.

A.15 Converted Indication MT PR

This element of service enables the MTS to indicate to a recipient UA that the MTS performed encoded information type conversion on a delivered message. The recipient UA is informed of the resulting types.

A.16 Counter Collection PD PR

This element of service allows an originating user to instruct the PDS to keep the physical message ready for counter collection at the post office specified by the originator, or at the post office which offers counter collection service closest to the given recipient's address.

A.17 Counter Collection with Advice PD PR

This element of service allows an originating user to instruct the PDS to keep the physical message ready for counter collection at the post office specified by the originator, or at the post office which offers counter collection service closest to the given recipient's address, and to inform the recipient via telephone, or telex, or teletex, using the number provided by the originator.

A.18 Cross-referencing Indication IPM

This element of service allows the originator to associate with the IP-message being sent, the globally unique identifiers of one or more other IP-messages. This enables the recipient's IPM UA, for example, to retrieve from storage a copy of the referenced IP-messages.

A.19 Deferred Delivery MT

This element of service enables an originating UA to instruct the MTS that a message being submitted shall be delivered no sooner than a specified date and time. Delivery will take place as close to the date and time specified as possible, but not before. The date and time specified for deferred delivery is subject to a limit which is defined by the originator's management domain.

Note Storage of the message shall be handled in the originating country.

A.20 Deferred Delivery Cancellation MT

This element of service enables an originating UA to instruct the MTS to cancel a previously successfully submitted deferred delivery message. The cancellation attempt may or may not always succeed. Possible reasons for failure are: deferred delivery time has passed, or the message has already been forwarded within the MTS.

A.21 Delivery Notification MT PR

This element of service enables an originating UA to request that the originating UA be explicitly notified when a submitted message has been successfully delivered to a recipient UA or Access Unit. The notification is related to the submitted message by means of the message identifier and includes the date and time of delivery. In the case of a multi-destination message, the originating UA can request this element of service on a per-recipient basis.

When a message is delivered after distribution list expansion, then, depending on the policy of the distribution list, the notification can be sent to either the list owner, the message originator, or both.

Delivery notification carries no implication that any UA or user action, such as examination of the message's content, has taken place.

A.22 Delivery Time Stamp Indication MT PR

This element of service enables the MTS to indicate to a recipient UA the date and time at which the MTS delivered a message. In the case of physical delivery, this element of service indicates the date and time at which the PDAU has taken responsibility for printing and further delivery of the physical message.

A.23 Delivery via Bureaufax Service PD PR

This element of service allows an originating user to instruct the PDAU and associated PDS to use the Bureaufax Service for transport and delivery.

A.24 Designation of Recipient by Directory Name MT PR

This element of service enables an originating UA to use a Directory Name in place of an individual recipient's O/R Address.

A.25 Disclosure of Other Recipients MT

This element of service enables the originating UA to instruct the MTS when submitting a multi-recipient message, to disclose the O/R names of all other recipients to each recipient UA, upon delivery of the message. The O/R names disclosed are as supplied by the originating UA. If distribution list expansion has been performed, then only the originator specified DL name will be disclosed, and not the names of its members.

A.26 DL Expansion History Indication MT

This element of service provides to a recipient, at delivery, information about the distribution list(s) through which the message has arrived. It is a local matter as to how much of this information is presented to the recipient.

A.27 DL Expansion Prohibited MT

This element of service allows an originating user to specify that if any of the recipients can directly or via reassignment refer to a distribution list, then no expansion shall occur. Instead, a Non-delivery Notification will be returned to the originating UA, unless Prevention of Non-delivery Notification has been requested.

A.28 EMS (Express Mail Service) PD PR

This element of service allows an originating user to instruct the PDS to transport and deliver the physical message produced from the MHS message through accelerated letter circulation and delivery service (such as EMS or the equivalent domestic service) in the destination country.

A.29 Expiry Date Indication IPM

This element of service allows the originator to indicate to the recipient the date and time after which he considers the IP-message to be invalid. The intent of this element of service is to state the originator's assessment of the current applicability of an IP-message. The particular action on behalf of a recipient by his IPM UA, or by the recipient himself, is unspecified. Possible actions might be to file or delete the IP-message after the expiry date has passed.

A.30 Explicit Conversion MT PR

This element of service enables an originating UA to request the MTS to perform a specified conversion, such as required when interworking between different Telematic Services. When a message is delivered after conversion has been performed, the recipient UA is informed of the original encoded information types as well as the current encoded information types in the message.

Note 1: This element of service is intended to support interworking with Telematic terminals/Services.

Note 2: When DL Names are used in conjunction with this element of service, conversion will apply to all members of the DL.

A.31 Forwarded IP-message Indication IPM

This element of service allows a forwarded IP-message, or a forwarded IP-message plus its "delivery information" to be sent as the body (or as one of the body parts) of an IP-message. An indication that the body part is forwarded is conveyed along with the body part. In a multi-part body, forwarded body parts can be included along with body parts of other types. "Delivery information" is information which is conveyed from the MTS when an IP-message is delivered (for example, time stamps and indication of conversion). However, inclusion of this delivery information along with a forwarded IP-message in no way guarantees that this delivery information is validated by the MTS.

The Receipt Notification Request Indication and the Non-receipt Notification Request Elements of Service are not affected by the forwarding of a IP-message.

A.32 Grade of Delivery Selection MT

This element of service enables an originating UA to request that transfer through the MTS be urgent or non-urgent , rather than normal. The time periods defined for non-urgent and urgent transfer are longer and shorter, respectively, than that defined for normal transfer. This indication is also sent to the recipient with the message.

A.33 Hold for Delivery MT

This element of service enables a recipient UA to request that the MTS hold its messages and returning notifications for delivery until a later time. The UA can indicate to the MTS when it is unavailable to take delivery of messages and notifications, and also, when it is again ready to accept delivery of messages and notifications from the MTS. The MTS can indicate to the UA that messages are waiting due to the criteria the UA established for holding messages. Responsibility for the management of this element of service lies with the recipient MTA.

Criteria for requesting a message to be held for delivery are: encoded information type, content type, maximum content length, and priority. The message will be held until the maximum delivery time for that message expires, unless the recipient releases the hold prior to its expiry.

Note The Hold for Delivery Element of Service is distinct from the message store facility. The Hold for Delivery Element of Service provides temporary storage to facilitate delivery and only after a message has been transferred to the recipient's UA, is delivery notification returned. The message store facility augments the storage of a UA and can be used to store messages for an extended period of time. Unlike the Hold for Delivery Element of Service, delivery notifications are returned as soon as the message is placed in (that is, delivered to) the message store.

A.34 Implicit Conversion MT

This element of service enables a recipient UA to have the MTS perform for a period of time any necessary conversion on messages prior to delivery. Neither the originating nor recipient UA explicitly requests this element of service on a per-message basis. If the encoded information type capabilities of the recipient UA are such that more than one type of conversion can be performed, the most appropriate conversion is performed. When a message is delivered after conversion has been performed, the recipient UA is informed of the original encoded information types as well as the current encoded information types in the message.

A.35 Importance Indication IPM

This element of service allows the originator to indicate to the recipients his assessment of the importance of the IP-message being sent. Three levels of importance are defined: low, normal, and high.

This element of service is not related to the Grade of Delivery Selection Element of Service provided by the MTS. The particular action taken by the recipient or his IPM UA based on the importance categorization is unspecified. It is the intent to allow the recipient IPM UA, for example, to present IP-messages in order of their importance or to alert the recipient of the arrival of IP-messages of high importance.

A.36 Incomplete Copy Indication IPM

This element of service allows an originator to indicate that this IP-message is an incomplete copy of an IP-message with the same IP-message identification in that one or more body parts, and/or heading fields of the original IP-message are absent.

A.37 IP-message Identification IPM

This element of service enables cooperating IPM UAs to convey a globally unique identifier for each IP-message sent or received. The IP-message identifier is composed of an O/R name of the originator and an identifier that is unique with respect to that name. IPM UAs and users use this identifier to refer to a previously sent or received IP-message (for example, in receipt notifications).

A.38 Language Indication IPM

This element of service enables an originating UA to indicate the language type(s) of a submitted IP-message.

A.39 Latest Delivery Designation MT

This element of service enables an originating UA to specify the latest time by which the message is to be delivered. If the MTS cannot deliver by the time specified, the message is not delivered and is cancelled. On multi-recipient messages, the latest delivery time can expire prior to delivery to all recipients, but this will not negate any deliveries which have already occurred.

A.40 Message Flow Confidentiality MT

This element of service allows the originator of the message to protect information which might be derived from observation of the message flow.

Note Only a limited form of this is supported.

A.41 Message Identification MT

This element of service enables the MTS to provide a UA with a unique identifier for each message or probe submitted or delivered by the MTS. UAs and the MTS use this identifier to refer to a previously submitted message in connection with Elements of Service such as Delivery and Non-delivery Notification.

A.42 Message Origin Authentication MT PR

This element of service allows the originator of a message to provide to the recipient(s) of the message, and any MTA through which the message is transferred, a means by which the origin of the message can be authenticated (i.e. a signature). Message Origin Authentication can be provided to the recipient(s) of the message, and any MTA through which the message is transferred, on a per-message basis using an asymmetric encryption technique, or can be provided only to the recipient(s) of the message, on a per-recipient basis using either an asymmetric or a symmetric encryption technique.

A.43 Message Security Labelling MT

This element of service allows the originator of a message (or probe) to associate with the message (and any reports on the message or probe) an indication of the sensitivity of the message (a security label). The message security label may be used by the MTS and the recipient(s) of the message to determine the handling of the message in line with the security policy in force.

A.44 Message Sequence Integrity MT PR

This element of service allows the originator of the message to provide to a recipient of the message a means by which the recipient can verify that the sequence of messages from the originator to the recipient has been preserved (without message loss, re-ordering, or replay). Message Sequence Integrity is on a per-recipient basis, and can use either an asymmetric or a symmetric encryption technique.

A.45 Multi-destination Delivery MT PR

This element of service enables an originating UA to specify that a message being submitted is to be delivered to more than one recipient UA. Simultaneous delivery to all specified UAs is not implied by this element of service.

A.46 Multi-part Body IPM

This element of service allows an originator to send to a recipient or recipients an IP-message with a body that is partitioned into several parts. The nature and attributes, or type, of each body part are conveyed along with the body part.

A.47 Non delivery Notification MT PR

This element of service enables the MTS to notify an originating UA if a submitted message was not delivered to the specified recipient UA(s). The reason the message was not delivered is included as part of the notification. For example, the recipient UA can be unknown to the MTS.

In the case of a multi-destination message, a non-delivery notification can refer to any or all of the recipient UAs to which the message could not be delivered.

When a message is not delivered after distribution list expansion, then, depending on the policy of the distribution list, the notification can be sent to either the list owner, the message originator, or both.

A.48 Non-receipt Notification Request IPM PR

This element of service allows the originator to ask that he be notified should the IP-message be deemed unreceivable. In the case of a multi-recipient IP-message, the originator can request this element of service on a per-recipient basis.

The originator's UA conveys his request to the recipient's UA. The UA automatically issues a non-receipt notification when any of the following events occur:

1. The recipient's UA auto-forwards the IP-message to another user.

2. The recipient's UA discards the IP-message prior to receipt.

3. The recipient's subscription is terminated before he receives the IP-message.

Since receipt can occur arbitrarily long after delivery, the recipient's failure to access the IP-message, even for a long period of time (for example, while on an extended business trip), does not constitute non-receipt and thus no notification is issued.

Note No legal significance can be adduced from this element of service.

A.49 Non-repudiation of Delivery MT PR

This element of service allows the originator of a message to obtain from the recipient(s) of the message irrevocable proof that the message was delivered to the recipient(s). This will protect against any attempt by the recipient(s) to subsequently deny receiving the message or its content. Non-repudiation of Delivery is provided to the originator of a message on a per-recipient basis using asymmetric encryption techniques.

A.50 Non-repudiation of Origin MT PR

This element of service allows the originator of a message to provide the recipient(s) of the message irrevocable proof of the origin of the message. This will protect against any attempt by the originator to subsequently revoke the message or its content. Non-repudiation of Origin is provided to the recipient(s) of a message on a per-message basis using asymmetric encryption techniques.

A.51 Non-repudiation of Submission MT

This element of service allows the originator of a message to obtain irrevocable proof that a message was submitted to the MTS for delivery to the originally specified recipient(s). This will protect against any attempt by the MTS to subsequently deny that the message was submitted for delivery to the originally specified recipient(s). Non-repudiation of Submission is provided to the originator of a message on a per-message basis, and uses an asymmetric encryption technique.

A.52 Obsoleting Indication IPM

This element of service allows the originator to indicate to the recipient that one or more IP-messages he sent previously are obsolete. The IP-message that carries this indication supersedes the obsolete IP-message.

The action to be taken by the recipient or his IPM UA is a local matter. The intent, however, is to allow the IPM UA or the recipient to, for example, remove or file obsolete messages.

A.53 Ordinary Mail PD PR

This element of service enables the PDS to transport and deliver the letter produced from the MHS message in the mode available through the ordinary letter mail service in the country of destination. This is the default action for the transport and delivery of a physical message.

A.54 Original Encoded Information Types Indication MT

This element of service enables an originating UA to specify to the MTS the encoded information types of a message being submitted. When the message is delivered, it also indicates to the recipient UA the encoded information types of the message specified by the originating UA.

A.55 Originator Indication IPM

This element of service allows the identity of the originator to be conveyed to the recipient. The intent of this IPM element of service is to identify the originator in a user friendly way. In contrast, the MTS provides to the recipient the actual O/R Address and directory name, if present, of the originator. DL Names should not be used in Originator Indication.

A.56 Originator Requested Alternate Recipient MT PR

This element of service enables an originating UA to specify, for each intended recipient, one alternate recipient to which the MTS can deliver the message, if delivery to the intended recipient is not possible. The alternate recipient can be a distribution list. For the purposes of determining success or failure (and hence delivery and non-delivery notifications), delivery to the originator requested alternate recipient is equivalent to delivery to the intended recipient. If the intended recipient has requested redirection of incoming messages, and if the originating UA has requested Redirection Allowed by the Originator, the system first tries to redirect the message. If this fails, the system then attempts to deliver the message to the designated alternate recipient.

A.57 Physical Delivery Notification by MHS PD PR

This element of service allows an originating user to request that an explicit notification, informing the originator of either successful or unsuccessful delivery of the physical message, be generated and returned by MHS. The notification provides information on delivery but no physical record is provided by the PDS.

Note 1: The notification includes the date and time of delivery based on the delivery confirmation given by the delivery person, the addressee or another authorized person. This is subject to national regulations in the destination country and is also dependent on the type of delivery requested (e.g., in the case of Registered Mail to Addressee in Person, the addressee would be the confirming person).

Note 2: This notification carries no implication that any action on the part of the recipient (such as examination of the message content) has taken place.

Note 3: When this element of service is requested, and the physical message is undeliverable, it either returned or destroyed depending on national regulations in the destination country, which means that the default action of the element of service B.91 is overridden.

A.58 Physical Delivery Notification by PDS PD PR

This element of service allows an originating user to request that an explicit notification, informing the originator of either successful or unsuccessful delivery of the physical message, be generated and returned by the PDS. The notification serves as a record of delivery for the originating user to retain for reference.

Note 1: The notification includes the date and time, and, in the case of successful delivery, the signature of the person confirming the delivery. The confirming person can be the delivery person, the addressee or another authorized person. This is subject to national regulations in the destination country and is also dependent on the type of delivery requested (e.g., in the case of Registered Mail to Addressee in Person, the addressee would be the confirming person).

Note 2: This notification carries no implication that any action on the part of the recipient (such as examination of the message content) has taken place.

Note 3: When this element of service is requested, and the physical message is undeliverable, it either returned or destroyed depending on national regulations in the destination country, which means that the default action of the element of service B.91 is overridden.

A.59 Physical Forwarding Allowed PD PR

This element of service enables the PDS to forward the physical message to a forwarding address if the recipient has changed his address and indicated this to the PDS. This is the default action taken by the PDS.

A.60 Physical Forwarding Prohibited PD PR

This element of service allows an originating user to instruct the PDS not to forward the physical message to a forwarding address.

A.61 Prevention of Non-delivery Notification MT PR

This element of service enables an originating UA to instruct the MTS not to return a non-delivery notification to the originating UA in the event that the message being submitted is judged undeliverable. In the case of a multi-destination message, the originating UA can request this element of service on a per-recipient basis.

A.62 Primary and Copy Recipients Indication IPM

This element of service allows the originator to provide the names of zero or more users, or DLs, who are the intended primary recipients of the IP-message, and the names of zero or more users, or DLs, who are the intended copy recipients of the IP-message. It is intended to enable a recipient to determine the category in which each of the specified recipients (including the recipient himself) was placed. The exact distinction between these two categories of recipients is unspecified. However, the primary recipients, for example, might be expected to act upon the IP-message, while the copy recipients might be sent the IP-message for information only.

Note As an example of this element of service in a typical memorandum, the primary recipients are normally designated by the directive "to:" while "cc:" identifies the copy recipients.

A.63 Probe MT

This element of service enables a UA to establish before submission whether a particular message could be delivered. The MTS provides the submission information and generates delivery and/or non-delivery notifications indicating whether a message with the same submission information could be delivered to the specified recipient UAs.

The Probe Element of Service includes the capability of checking whether the content size, content type, and/or encoded information types would render it undeliverable. The significance of the result of a Probe depends upon the recipient UA(s) having registered with the MTS the encoded information types, content type and maximum message size that it can accept. This element of service is subject to the same delivery time targets as for the urgent class. In the case of DLs, a Probe indicates nothing about the likelihood of successful delivery to the DL members, but only whether the originator has the right to submit to the DL.

A.64 Probe Origin Authentication MT

This element of service allows the originator of a probe to provide to any MTA through which the probe is transferred a means to authenticate the origin of the probe (i.e. a signature). Probe Origin Authentication is on a per-probe basis, and uses an asymmetric encryption technique.

A.65 Proof of Delivery MT PR

This element of service allows the originator of a message to obtain from the recipient(s) of the message the means to authenticate the identity of the recipient(s) and the delivered message and content. Message recipient authentication is provided to the originator of a message on a per-recipient basis using either symmetric or asymmetric encryption techniques.

A.66 Proof of Submission MT

This element of service allows the originator of a message to obtain from the MTS the means to authenticate that the message was submitted for delivery to the originally intended recipient. Message submission authentication is provided on a per-message basis, and can use symmetric or asymmetric encryption techniques.

A.67 Receipt Notification Request Indication IPM PR

This element of service allows the originator to ask that he be notified when the IP-message being sent is received. In the case of a multi-recipient message, the originator can request this element of service on a per-recipient basis. This element of service also implicitly requests Non-receipt Notification Request Indication.

The originator's UA conveys his request to the recipient's UA. The recipient can instruct his UA to honour such requests, either automatically (for example, when it first renders the IP-message on the recipient's terminal) or upon his explicit command. The recipient can also instruct his UA, either in blanket fashion or case by case, to ignore such requests.

A.68 Redirection Allowed by Originator MT

This element of service enables an originating UA to instruct the MTS, if the recipient has requested the Redirection of Incoming Messages element of service, that redirection can be applied to a particular submitted message.

A.69 Redirection of Incoming Messages MT

This element of service enables a UA to instruct the MTS to redirect incoming messages addressed to it, to another UA or to a DL, for a specified period of time, or until revoked.

Note 1 This is an MT element of service that does not necessitate delivery to the intended recipient before redirection can take place. It is therefore distinct from the IPM Auto-Forwarded Indication Element of Service.

Note 2 When security provisions are in force, different incoming messages, on the basis of their security labels, may be redirected to separate alternate recipients or not redirected at all

A.70 Registered Mail PD PR

This element of service allows an originating user to instruct the PDS to handle the physical message as registered mail.

A.71 Registered Mail to Addressee in Person PD PR

This element of service allows an originating user to instruct the PDS to handle the physical message as registered mail and to deliver it to the addressee only.

A.72 Reply Request Indication IPM PR

This element of service allows the originator to request that a recipient send an IP-message in reply to the IP-message that carries the request. The originator can also specify the date by which any reply should be sent, and the one or more users and DLs to whom the originator requests (but does not demand) be among the preferred recipients of any reply. The recipient is informed of the date and names but it is up to the recipient to decide whether or not, and if so, to whom to reply.

Note A blind copy recipient should consider carefully to whom he sends a reply, in order that the meaning of the Blind Copy Recipient Indication Element of Service is preserved.

A.73 Replying IP-message Indication IPM

This element of service allows the originator of an IP-message to indicate to the recipient(s) that this IP-message is being sent in reply to another IP-message. A reply can, depending on the wishes of the originator of the replied-to message, and the final decision of the originator of the reply, be sent to:

1. The recipients specified in the reply request indication of the replied-to message.

2. The originator of the replied-to message.

3. The originator and other recipients.

4. A distribution list, in which the originator of the replied-to message can be a receiving member.

5. Other recipients as chosen by the originator of the reply.

The recipients of the reply receive it as a regular IP-message, together with an indication of which IP-message it is a reply to.

A.74 Report Origin Authentication MT

This element of service allows the originator of a message (or probe) to authenticate the origin of a report on the delivery or non-delivery of the subject message (or probe), (a signature). Report Origin Authentication is on a per-report basis, and uses an asymmetric encryption technique.

A.75 Request for Forwarding Address PD PR

This element of service allows an originating user to instruct the PDS to provide the forwarding address if the recipient has changed his address and indicated this to the PDS.

This element of service can be used with either Physical Forwarding Allowed or Prohibited. The provision of the forwarding address by the PDS to an originating user is subject to national regulations in the destination country. The default action is no provision of the forwarding address.

A.76 Requested Delivery Method MT PR

This element of service allows a user to request, on a per-recipient basis, the preference of method or methods of message delivery (such as through an Access Unit). Non-delivery results if preference(s) cannot be satisfied.

A.77 Restricted Delivery MT

This element of service enables a recipient UA to indicate to the MTS that it is not prepared to accept delivery of messages from certain originating UAs or DLs.

Note This element of service can be requested in either of two ways;

1. Specification by the recipient UA of unauthorized senders, all other senders are considered as authorized.

2. Specification by the recipient UA of authorized senders, all other senders are considered to be unauthorized.

A.78 Return of Content MT

This element of service enables an originating UA to request that the content of a submitted message be returned with any non-delivery notification. This will not be done, however, if any encoded information type conversion has been performed on the message's content.

A.79 Secure Access Management MT

This element of service enables an MTS user to establish an association with the MTS, or the MTS to establish an association with an MTS user, or an MTA to establish an association with another MTA. It also establishes the strong credentials of the objects to interact, and the context and security-context of the association. Secure Access Management can use either an asymmetric or a symmetric encryption technique. When access security is achieved through strong credentials, they can be periodically updated.

A.80 Sensitivity Indication IPM

This element of service allows the originator of an IP-message to specify guidelines for the relative sensitivity of the message upon its receipt. It is the intent that the sensitivity indication should control such items as:

1. Whether the recipient should have to prove his identity to receive the IP-message.
2. Whether the IP-message should be allowed to be printed on a shared printer.
3. Whether an IPM UA should allow the recipient to forward the received IP-message.
4. Whether the IP-message should be allowed to be auto-forwarded.

The sensitivity indication can be indicated to the recipient or interpreted directly by the recipient's IPM UA.

If no sensitivity level is indicated, it should be assumed that the IP-message's originator has advised no restriction on the recipient's further disposition of the IP-message. The recipient is free to forward, print, or otherwise do as he chooses with the IP-message.

Three specific levels of sensitivity above the default are defined:

Personal:
The IP-message is sent to the recipient as an individual, rather than to him in his role. There is no implication that the IP-message is private, however.

Private:
The IP-message contains information that should be seen (or heard) only by the recipient, and not by anyone else. The recipient's IPM UA can provide services to enforce this intent on behalf of the IP-message's originator.

Company-confidential:
The IP-message contains information that should be according to company-specific procedures.

A.81 Special Delivery PD PR

This element of service allows an originating user to instruct the PDS to transport the letter produced from the MHS message through the ordinary letter mail circulation system and to deliver it by special messenger delivery.

A.82 Stored Message Alert MS

This element of service allows a user of an MS to register relevant sets of criteria that can cause an alert to be generated to the user when a message arrives at the MS satisfying the selected criteria. The generation of the alert can occur as follows:

1. If the UA is connected and on-line to the MS, the alert message will be sent to the UA as soon as a message arrives at the MS that satisfies the registered criteria for generating alerts. If the UA is off line then the next time the UA connects to his MS after a message arrives at the MS satisfying the registered criteria, the user will be informed that one or more alert cases have occurred, the details of which can be determined by performing a Stored Message Summary.
2. In addition to, or as an alternative to #1 above, the MS can use other mechanisms to inform the user.

A.83 Stored Message Auto-forward MS

This element of service allows a user of an MS to register requests that the MS auto-forward selected messages that are delivered to it. The user of the MS can select through registration several sets of criteria chosen from the attributes available in the MS, and messages meeting each set of criteria will be autoforwarded to one or more users or DLs. A text(s) can also be specified to be included with the auto-forwarded message(s).

A.84 Stored Message Deletion MS

This element of service enables a recipient UA to delete certain of its messages from the MS. Messages cannot be deleted if they have not been previously listed.

A.85 Stored Message Fetching MS

This element of service enables a recipient UA to fetch from the MS a message, or portions of a message. The UA can fetch a message (or message portion) based on the same search criteria that can be used for Stored Message Listing.

A.86 Stored Message Listing MS

This element of service provides a recipient UA with a list of information about certain of its messages stored in the MS. The information comprises selected attributes from a message's envelope and content and others added by the MS. The UA can limit the number of messages that will be listed.

A.87 Stored Message Summary MS

This element of service provides a recipient UA with a count of the number of its messages currently stored in the MS. The count of messages satisfying a specified criteria based on one or more attributes of the messages stored in the MS can be requested.

A.88 Subject Indication IPM

This element of service allows the originator to indicate to the recipient(s) the subject of an IP-message being sent. The subject information is to be made available to the recipient.

A.89 Submission Time Stamp Indication MT

This element of service enables the MTS to indicate to the originating UA and each recipient UA the date and time at which a message was submitted to the MTS. In the case of physical delivery, this element of service also enables the PDAU to indicate the date and time of submission on the physical message.

A.90 Typed Body IPM

This element of service permits the nature and attributes of the body of the IP-message to be conveyed along with the body. Because the body can undergo conversion, the body type can change over time.

A.91 Undeliverable Mail with Return of Physical Message PD PR

This element of service enables the PDS to return the physical message without delay, with reason indicated to the originator, if it cannot be delivered to the addressee. This is the default action to be taken by the PDS.

Note In the case of "poste restante" the return of the physical message will take place after some period of time.

A.92 Use of Distribution List MT PR

This element of service enables an originating UA to specify a distribution list in place of all the individual recipients (users or nested DLs) mentioned therein. The MTS will add the members of the list to the recipients of the message and send it to those members. Distribution lists can be members of distribution lists, in which case the list of recipients can be successively expanded at several places in the MTS.

A.93 User Capabilities Registration MT

This element of service enables a UA to indicate to its MTA, through registration, the unrestricted use of any or all of the following capabilities with respect to received messages;

1. the content type(s) of messages it is willing to have delivered to it,

2. the maximum content length of a message it is willing to have delivered to it,

3. the encoded information type(s) of messages it is willing to have delivered to it.

The MTA will not deliver to a UA a message or probe that does not match, or exceeds, the capabilities registered.