INTERNATIONAL STANDARD

ISO/IEC 10021-2

First edition
1990-12-01

Information technology — Text Communication — Message-Oriented Text Interchange Systems (MOTIS) —

Part 2: Overall Architecture

Technologies de l'information — Communication de texte — Systèmes d'échange de texte en mode message —

Partie 2: Architecture générale

Reference number
ISO/IEC 10021-2 : 1990 (E)

Contents

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Printed in Switzerland

List of Figures

List of Tables

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 10021-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

ISO/IEC 10021-2 consists of the following parts, under the general title: *Information technology — Text Communication — Message-Oriented Text Interchange Systems (MOTIS) —*

- *Part 1: System and Service Overview*
- *Part 2: Overall Architecture*
- *Part 3: Abstract Service Definition Conventions*
- *Part 4: Message Transfer System: Abstract Service Definition and Procedures*
- *Part 5: Message Store: Abstract Service Definition*
- *Part 6: Protocol Specifications*
- *Part 7: Interpersonal Messaging System*

Annexes A, B, C and E form an integral part of this part of ISO/IEC 10021. Annexes D, F and G are for information only.

Introduction

This part of ISO/IEC 10021 is one of a number of parts of ISO/IEC 10021 (the International Standards for Message-Oriented Text Interchange Systems (MOTIS)). ISO/IEC 10021 provides a comprehensive blueprint for a Message Handling System (MHS) realized by any number of cooperating open systems.

The purpose of an MHS is to enable users to exchange messages on a store-and-forward basis. A message submitted on behalf of one user, the originator, is conveyed by the Message Transfer System (MTS) and subsequently delivered to the agents of one or more additional users, the recipients. Access units (AUs) link the MTS to communication systems of other kinds (e.g., postal systems). A user is assisted in the preparation, storage, and display of messages by a user agent (UA). Optionally, he is assisted in the storage of messages by a message store (MS). The MTS comprises a number of message transfer agents (MTAs) which collectively perform the store-and-forward message transfer function.

This part of ISO/IEC 10021 specifies the overall architecture of the MHS and serves as a technical introduction to it.

The text of this part of ISO/IEC 10021 is the subject of joint CCITT-ISO agreement. The corresponding CCITT specification is Recommendation X.402.

Information technology - Text Communication - Message-Oriented Text Interchange Systems (MOTIS) - Part 2 : Overall Architecture

Section one - Introduction

1 Scope

This part of ISO/IEC 10021 defines the overall architecture of the MHS and serves as a technical introduction to it.

Other aspects of Message Handling are specified in other parts of ISO/IEC 10021. A non-technical overview of Message Handling is provided by ISO/IEC 10021-1. The conventions used in the definition of the abstract services provided by MHS components are defined in ISO/IEC 10021-3. The abstract service the MTS provides and the procedures that govern its distributed operation are defined in ISO/IEC 10021-4. The abstract service the MS provides is defined in ISO/IEC 10021-5. The application protocols that govern the interactions of MHS components are specified in ISO/IEC 10021-6. The Interpersonal Messaging System, an application of Message Handling, is defined in ISO/IEC 10021-7.

The ISO International Standards and CCITT Recommendations on Message Handling are summarized in Table 1.

Table 1
Specifications for Message Handling Systems

ISO/IEC	CCITT	SUBJECT MATTER
Introduction		
10021-1	X.400	Service and system overview
10021-2	X.402	Overall architecture
Various Aspects		
-	X.403	Conformance testing
10021-3	X.407	Abstract service definition conventions
-	X.408	Encoded information type conversion rules
Abstract Services		
10021-4	X.411	MTS Abstract Service definition and procedures for distributed operation
10021-5	X.413	MS Abstract Service definition
Protocols		
10021-6	X.419	Protocol specifications
Interpersonal Messaging System		
10021-7	X.420	Interpersonal Messaging System
-	T.330	Telematic access to IPMS

The Directory, the principal means for disseminating communication-related information among MHS components, is defined in ISO/IEC 9594, as summarized in Table 2.

Table 2
Specifications for Directories

ISO/IEC	CCITT	SUBJECT MATTER
9594-1	X.500	Overview
9594-2	X.501	Models
9594-3	X.511	Abstract service definition
9594-4	X.518	Procedures for distributed operation
9594-5	X.519	Protocol specifications
9594-6	X.520	Selected attribute types
9594-7	X.521	Selected object classes
9594-8	X.509	Authentication framework

The architectural foundation for Message Handling is provided by other International Standards. The OSI Reference Model is defined in ISO 7498. The notation for specifying the data structures of abstract services and application protocols, ASN.1, and the associated encoding rules are defined in ISO 8824 and 8825. The means for establishing and releasing associations, the ACSE, is defined in ISO 8649 and 8650. The means for reliably conveying APDUs over associations, the RTSE, is defined in ISO/IEC 9066. The means for making requests of other open systems, the ROSE, is defined in ISO/IEC 9072.

The ISO International Standards and CCITT Recommendations which form the foundation for Message Handling are summarized in Table 3.

Table 3
Specifications for MHS Foundations

ISO	CCITT	SUBJECT MATTER
Model		
7498	X.200	OSI Reference Model
ASN.1		
8824	X.208	Abstract syntax notation
8825	X.209	Basic encoding rules
Association Control		
8649	X.217	Service definition
8650	X.227	Protocol specification
Reliable Transfer		
9066-1	X.218	Service definition
9066-2	X.228	Protocol specification
Remote Operations		
9072-1	X.219	Service definition
9072-2	X.229	Protocol specification

This part of ISO/IEC 10021 is structured as follows. Section one gives a general overview. Section two presents abstract models of Message Handling. Section three specifies how one can configure the MHS to satisfy any of a variety of functional, physical, and organizational requirements. Section four describes the naming and addressing of users and distribution lists and the routing of information objects to them. Section five describes the uses the MHS may make of the Directory. Section six describes how the MHS is realized by means of OSI. Annexes provide important supplemental information.

No requirements for conformance to this part of ISO/IEC 10021 are imposed.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 10021. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO/IEC 10021 are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of ISO and IEC maintain registers of currently valid International Standards.

2.1 Open Systems Interconnection

This part of ISO/IEC 10021 and others in the set cite the following OSI specifications:

ISO 7498:1984, *Information processing systems - Open Systems Interconnection - Basic Reference Model.*

ISO 7498-2:1989, *Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.*

ISO 8649:1988, *Information processing systems - Open Systems Interconnection - Service definition for the Association Control Service Element.*

ISO 8650:1988, *Information processing systems - Open Systems Interconnection - Protocol specification for the Association Control Service Element.*

ISO 8822:1988, *Information processing systems - Open Systems Interconnection - Connection oriented presentation service definition.*

ISO 8824:1990, *Information processing systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1).*

ISO 8825:1990, *Information processing systems - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

ISO/IEC 9066:1989, *Information processing systems - Text communication - Reliable Transfer Part 1: Model and service definition.*

Part 2: Protocol specification.

ISO/IEC 9072:1989, *Information processing systems - Text communication - Remote operations Part 1: Model, notation and service definition.*

Part 2: Protocol specification.

2.2 Directory Systems

This part of ISO/IEC 10021 and others in the set cite the following Directory System specifications:

ISO/IEC 9594:1990, *Information technology - Open Systems Interconnection - The Directory*

Part 1: Overview of concepts, models, and services.

Part 2: Models.

Part 3: Abstract service definition.

Part 4: Procedures for distributed operation.

Part 5: Protocol specifications.

Part 6: Selected attribute types.

Part 7: Selected object classes.

Part 8: Authentication framework.

2.3 Message Handling Systems

This part of ISO/IEC 10021 and others in the set cite the following Message Handling System specifications:

ISO/IEC 10021:1990, *Information technology - Text communication - Message-Oriented Text Interchange Systems (MOTIS) -*

Part 1: Service and system overview.

Part 3: Abstract service definition conventions.

Part 4: Message transfer system : Abstract service definition and procedures.

Part 5: Message store : Abstract service definition.

Part 6: Protocol specifications.

Part 7: Interpersonal messaging system.

CCITT T.330:1988, *Telematic access to IPMS.*

CCITT X.403:1988, *Message handling systems: Conformance testing.*

CCITT X.408:1988, *Message handling systems: Encoded information type conversion rules.*

2.4 Country Codes

This part of ISO/IEC 10021 cites the following Country Code specification:

ISO 3166:1988, *Codes for the representation of names of countries.*

3 Definitions

For the purposes of this part of ISO/IEC 10021 and others in the set, the following definitions apply.

3.1 Open Systems Interconnection

This part of ISO/IEC 10021 and others in the set make use of the following terms defined in ISO 7498, as well as the names of the seven layers of the Reference Model:

a) abstract syntax;

b) application entity (AE);

c) application process;

d) application protocol data unit (APDU);

e) application service element (ASE);

f) distributed information processing task;

g) layer;

h) open system;

i) Open Systems Interconnection (OSI);

j) peer;

k) presentation context;

l) protocol;

m) Reference Model;

n) transfer syntax; and

o) user element (UE).

This part of ISO/IEC 10021 and others in the set make use of the following terms defined in ISO 8824 and 8825, as well as the names of ASN.1 data types and values:

a) Abstract Syntax Notation One (ASN.1);

b) Basic Encoding Rules;

c) explicit;

d) export;

e) implicit;

f) import;

g) macro;

h) module;

i) tag;

j) type; and

k) value.

This part of ISO/IEC 10021 and others in the set make use of the following terms defined in ISO 8649:

a) application association, association;

b) application context (AC);

c) Association Control Service Element (ACSE);

d) initiator; and

e) responder.

This part of ISO/IEC 10021 and others in the set make use of the following terms defined in ISO/IEC 9066-1:

a) Reliable Transfer (RT); and

b) Reliable Transfer Service Element (RTSE).

This part of ISO/IEC 10021 and others in the set make use of the following terms defined in ISO/IEC 9072-1:

a) argument;

b) asynchronous;

c) bind;

d) parameter;

e) remote error;

f) remote operation;

g) Remote Operations (RO);

h) Remote Operations Service Element (ROSE);

i) result;

j) synchronous; and

k) unbind.

3.2 Directory Systems

This part of ISO/IEC 10021 and others in the set make use of the following terms defined in ISO/IEC 9594:

a) attribute;

b) certificate;

c) certification authority;

d) certification path;

e) directory entry; entry;

f) directory system agent (DSA);

g) Directory;

h) hash function;

i) name;

j) object class;

k) object;

l) simple authentication; and

m) strong authentication.

3.3 Message Handling Systems

For the purposes of this part of ISO/IEC 10021 the terms indexed in annex G apply.

4 Abbreviations

For the purposes of this part of ISO/IEC 10021 the abbreviations indexed in annex G apply.

5 Conventions

This part of ISO/IEC 10021 uses the descriptive conventions identified below.

5.1 ASN.1

This part of ISO/IEC 10021 uses several ASN.1-based descriptive conventions in annexes A and C to define the Message Handling-specific information the Directory may hold. In particular, it uses the OBJECT-CLASS, ATTRIBUTE, and ATTRIBUTE-SYNTAX macros of ISO/IEC 9594-2 to define Message Handling-specific object classes, attributes, and attribute syntaxes.

ASN.1 appears both in annex A to aid the exposition, and again, largely redundantly, in annex C for reference. If differences are found between the two, a specification error is indicated.

ASN.1 tags are implicit throughout the ASN.1 module that annex C defines; the module is definitive in that respect.

5.2 Grade

Whenever this part of ISO/IEC 10021 describes a class of data structure (e.g., O/R addresses) having components (e.g., attributes), each component is assigned one of the following **grades**:

a) **mandatory** (**M**): A mandatory component shall be present in every instance of the class.

b) **optional** (**O**): An optional component shall be present in an instance of the class at the discretion of the object (e.g., user) supplying that instance. There is no default value.

c) **defaultable** (**D**): A defaultable component shall be present in an instance of the class at the discretion of the object (e.g., user) supplying that instance. In its absence a default value, specified by this part of ISO/IEC 10021, applies.

d) **conditional** (**C**): A conditional component shall be present in an instance of the class as dictated by this part of ISO/IEC 10021.

5.3 Terms

Throughout the remainder of this part of ISO/IEC 10021, terms are rendered in **bold** when defined, in *italic* when referenced prior to their definitions, without emphasis upon other occasions.

Terms that are proper nouns are capitalized, generic terms are not.

Section two - Abstract Models

6 Overview

This section presents abstract models of *Message Handling* which provide the architectural basis for the more detailed specifications that appear in other parts of ISO/IEC 10021.

Message Handling is a distributed information processing task that integrates the following intrinsically related sub-tasks:

a) **Message Transfer**: The non-real-time carriage of information objects between parties using computers as intermediaries.

b) **Message Storage**: The automatic storage for later retrieval of information objects conveyed by means of Message Transfer.

This section covers the following topics:

a) Functional model;

b) Information model;

c) Operational model;

d) Security model.

NOTE - **Message Handling has a variety of applications, one of which is Interpersonal Messaging, described in ISO/IEC 10021-7.**

7 Functional Model

This clause provides a functional model of Message Handling. The concrete realization of the model is the subject of other parts of ISO/IEC 10021.

The **Message Handling Environment** (MHE) comprises "primary" functional objects of several types, the *Message Handling System* (*MHS*), *users*, and *distribution lists*. The *MHS* in turn can be decomposed into lesser, "secondary" functional objects of several types, the *Message Transfer System* (*MTS*), *user agents*, *message stores*, and *access units*. The *MTS* in turn can be decomposed into still lesser, "tertiary" functional objects of a single type, *message transfer agents*.

The primary, secondary, and tertiary functional object types and selected *access unit* types are individually defined and described below.

As detailed below, functional objects are sometimes tailored to one or more applications of Message Handling, e.g., Interpersonal Messaging (see ISO/IEC 10021-7 and CCITT Recommendation T.330). A functional object that has been tailored to an application understands the syntax and semantics of the contents of messages exchanged in that application.

As a local matter, functional objects may have capabilities beyond those specified in ISO/IEC 10021. In particular, a typical *user agent* has message preparation, rendition, and storage capabilities that are not standardized.

7.1 Primary Functional Objects

The MHE comprises the *Message Handling System*, *users*, and *distribution lists*. These primary functional objects interact with one another. Their types are defined and described below.

The situation is depicted in Figure 1.

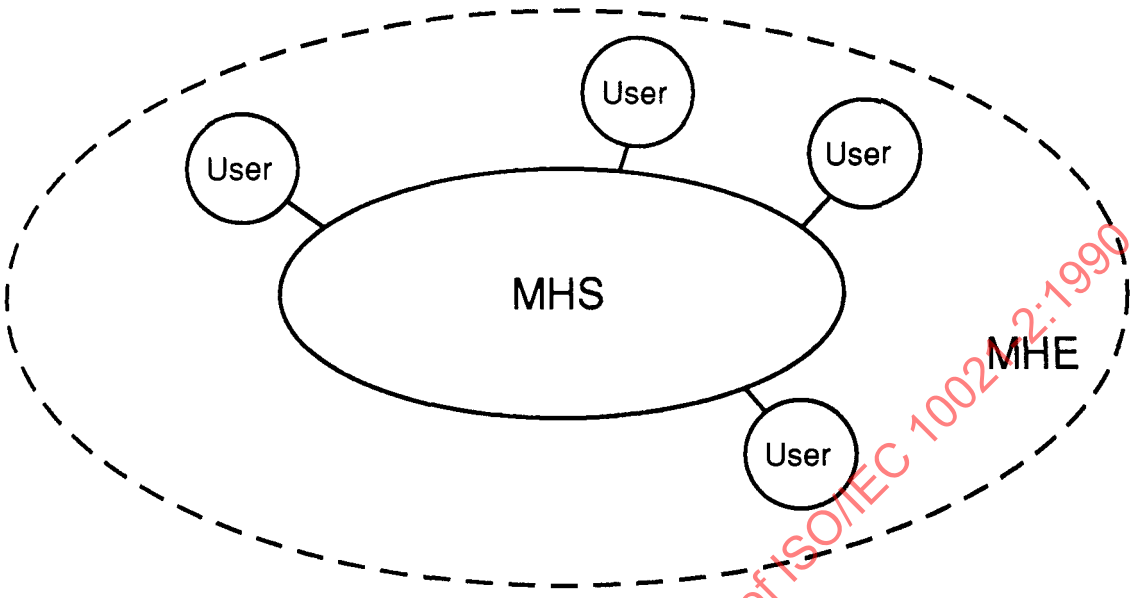

Figure 1
The Message Handling Environment

7.1.1 The Message Handling System

The principal purpose of Message Handling is to convey information objects from one party to another. The functional object by means of which this is accomplished is called the **Message Handling System** (**MHS**).

The MHE comprises a single MHS.

7.1.2 Users

The principal purpose of the MHS is to convey information objects between *users*. A functional object (e.g., a person) that engages in (rather than provides) Message Handling is called a **user**.

The following kinds of user are distinguished:

a) **direct user**: A user that engages in Message Handling by direct use of the MHS.

b) **indirect user**: A user that engages in Message Handling by indirect use of the MHS, i.e., through another communication system (e.g., a postal system or the telex network) to which the MHS is linked.

The MHE comprises any number of users.

7.1.3 Distribution Lists

By means of the MHS a user can convey information objects to pre-specified groups of users as well as to individual users. The functional object that represents a pre-specified group of users and other *DLs* is called a **distribution list** (**DL**).

A DL identifies zero or more users and DLs called its **members**. The latter DLs (if any) are said to be **nested**. Asking the MHS to convey an information object (e.g., a *message*) to a DL is tantamount to asking that it convey the object to its members. Note that this is recursive.

The right, or permission, to convey *messages* to a particular DL may be controlled. This right is called **submit permission**. As a local matter the use of a DL can be further restricted.

The MHE comprises any number of DLs.

NOTE - A DL might be further restricted, e.g., to the conveyance of *messages* of a prescribed *content type*.

7.2 Secondary Functional Objects

The MHS comprises the *Message Transfer System*, *user agents*, *message stores*, and *access units*. These secondary functional objects interact with one another. Their types are defined and described below.

The situation is depicted in Figure 2.

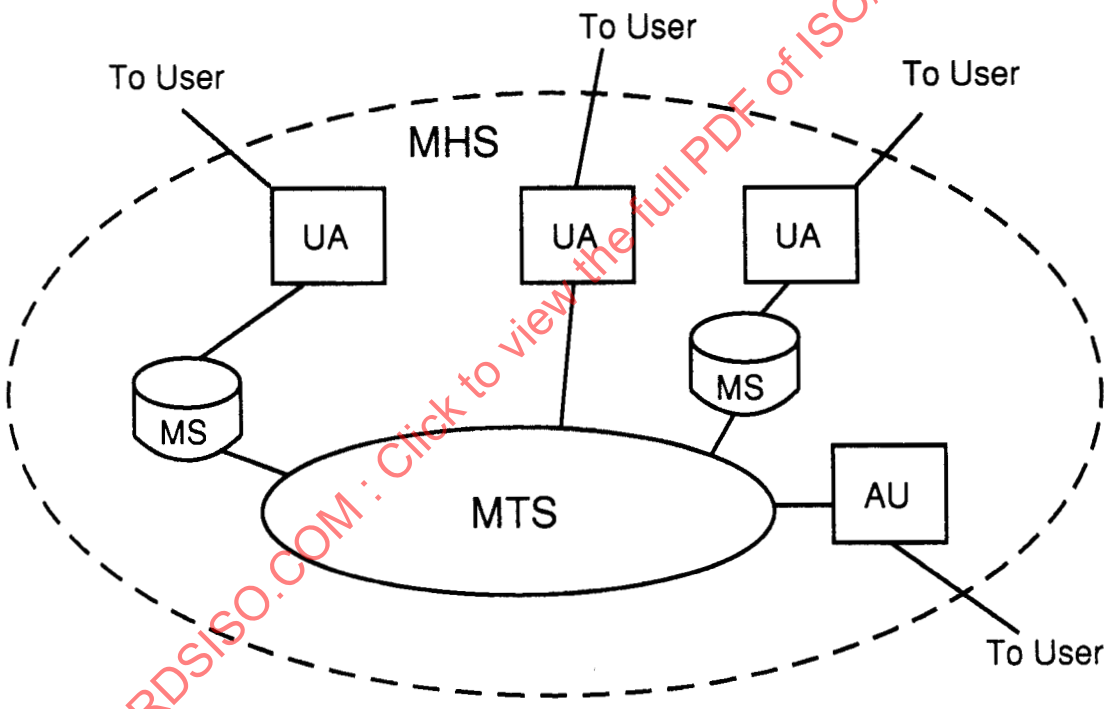

Figure 2
The Message Handling System

7.2.1 The Message Transfer System

The MHS conveys information objects to individual users and to the members of DLs. The functional object that actually does this is called the **Message Transfer System** (MTS). The MTS is a store-and-forward communication system and can be considered the backbone of the MHS.

The MTS is general-purpose, supporting all applications of Message Handling. Additionally, the MTS may be tailored to one or more particular applications so it can carry out *conversion*.

The MHS comprises a single MTS.

7.2.2 User Agents

The functional object by means of which a single direct user engages in Message Handling is called a **user agent** (UA).

A typical UA is tailored to one or more particular applications of Message Handling.

The MHS comprises any number of UAs.

NOTE - A UA that serves a human user typically interacts with him by means of input/output devices (e.g., a keyboard, display, scanner, printer, or combination of these).

7.2.3 Message Stores

A typical user must store the information objects it receives. The functional object that provides a (single) direct user with capabilities for Message Storage is called a **message store** (MS). Each MS is associated with one UA, but not every UA has an associated MS.

Every MS is general-purpose, supporting all applications of Message Handling. Additionally, an MS may be tailored to one or more particular applications so that it can more capably *submit* and support the *retrieval* of *messages* associated with that application.

The MHS comprises any number of MSs.

NOTE - As a local matter a UA may provide for information objects storage that either supplements or replaces that of an MS.

7.2.4 Access Units

The functional object that links another communication system (e.g., a postal system or the telex network) to the MTS and via which its patrons engage in Message Handling as indirect users is called an **access unit** (AU).

A typical AU is tailored to a particular communication system and to one or more particular applications of Message Handling.

The MHS comprises any number of AUs.

7.3 Tertiary Functional Objects

The MTS comprises *message transfer agents*. These tertiary functional objects interact. Their type is defined and described below.

The situation is depicted in Figure 3.

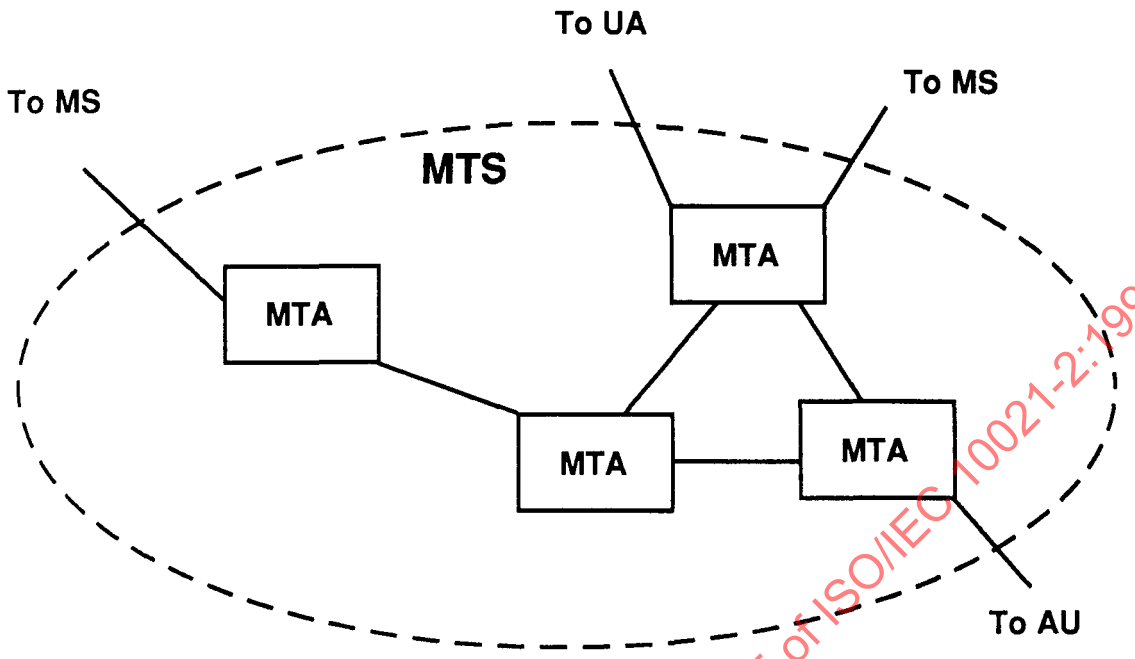

Figure 3
The Message Transfer System

7.3.1 Message Transfer Agents

The MTS conveys information objects to users and DLs in a store-and-forward manner. A functional object that provides one link in the MTS' store-and-forward chain is called a **message transfer agent** (MTA).

Every MTA is general-purpose, supporting all applications of Message Handling. Additionally, an MTA may be tailored to one or more particular applications so it can carry out *conversion*.

The MTS comprises any number of MTAs.

7.4 Selected AU Types

As described above, the MHS interworks with communication systems of other types via AUs. Several selected AU types--*physical delivery*, telematic, and telex--are introduced in the subclauses below.

7.4.1 Physical Delivery

A **physical delivery access unit** (**PDAU**) is an AU that subjects *messages* (but neither *probes* nor *reports*) to *physical rendition* and that conveys the resulting *physical messages* to a *physical delivery system*.

The transformation of a *message* into a *physical message* is called **physical rendition**. A **physical message** is a physical object (e.g., a letter and its paper envelope) that embodies a *message*.

A **physical delivery system** (**PDS**) is a system that performs *physical delivery*. One important kind of PDS is postal systems. **Physical delivery** is the conveyance of a physical message to a patron of a PDS, one of the indirect users to which the PDAU provides Message Handling capabilities.

Among the applications of Message Handling supported by every PDAU is Interpersonal Messaging (see ISO/IEC 10021-7).

7.4.2 Telematic

Telematic access units, which support Interpersonal Messaging exclusively, are introduced in ISO/IEC 10021-7.

7.4.3 Telex

Telex access units, which support Interpersonal Messaging exclusively, are introduced in ISO/IEC 10021-7.

8 Information Model

This clause provides an information model of Message Handling. The concrete realization of the model is the subject of other parts of ISO/IEC 10021.

The MHS and MTS can convey information objects of three classes: *messages*, *probes*, and *reports*. These classes are listed in the first column of Table 4. For each listed class, the second column indicates the kinds of functional objects--users, UAs, MSs, MTAs, and AUs--that are the ultimate sources and destinations for such objects.

Table 4
Conveyable Information Objects

Information Object	Functional Object: user	UA	MS	MTA	AU
message	SD	-	-	-	-
probe	S	-	-	D	-
report	D	-	-	S	-

Legend
S ultimate source
D ultimate destination

The information objects, summarized in the table, are individually defined and described in the subclauses below.

8.1 Messages

The primary purpose of Message Transfer is to convey information objects called **messages** from one user to others. A message has the following parts, as depicted in Figure 4:

a) **envelope**: An information object whose composition varies from one *transmittal step* to another and that variously identifies the message's *originator* and *potential recipients*, documents its previous conveyance and directs its subsequent conveyance by the MTS, and characterizes its *content*.

b) **content**: An information object that the MTS neither examines nor modifies, except for *conversion*, during its conveyance of the message.

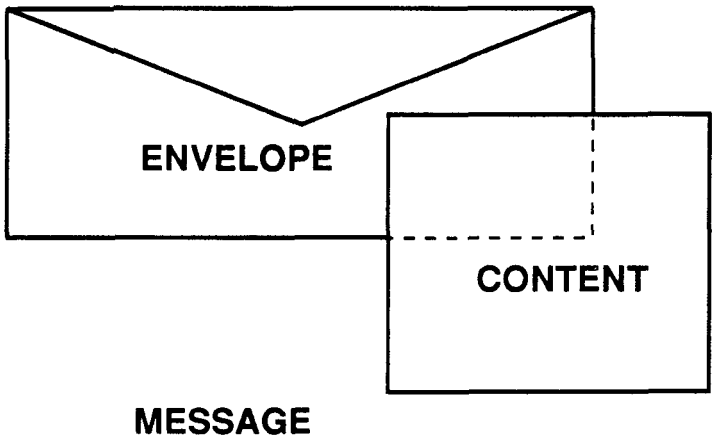

Figure 4
A Message's Envelope and Content

One piece of information borne by the envelope identifies the type of the content. The **content type** is an identifier (an ASN.1 Object Identifier or Integer) that denotes the syntax and semantics of the content overall. This identifier enables the MTS to determine the message's *deliverability* to particular users, and enables UAs and MSs to interpret and process the content.

Another piece of information borne by the envelope identifies the types of encoded information represented in the content. An **encoded information type** (**EIT**) is an identifier (an ASN.1 Object Identifier or Integer) that denotes the medium and format (e.g., IA5 text or Group 3 facsimile) of individual portions of the content. It further enables the MTS to determine the message's deliverability to particular users, and to identify opportunities for it to *make* the message deliverable by converting a portion of the content from one EIT to another.

8.2 Probes

A second purpose of Message Transfer is to convey information objects called **probes** from one user up to but just short of other users (i.e., to the MTAs serving those users). A probe describes a class of message and is used to determine the *deliverability* of such messages.

A message described by a probe is called a **described message**.

A probe comprises an envelope alone. This envelope contains much the same information as that for a message. Besides bearing the content type and encoded information types of a described message, the probe's envelope bears the length of its content.

The *submission* of a probe elicits from the MTS largely the same behaviour as would *submission* of any described message, except that *DL expansion* and *delivery* are forgone in the case of the probe. In particular, and apart from the consequences of the suppression of *DL expansion*, the probe provokes the same *reports* as would any described message. This fact gives probes their utility.

8.3 Reports

A third purpose of Message Transfer is to convey information objects called **reports** to users. Generated by the MTS, a report relates the outcome or progress of a message's or probe's *transmittal* to one or more *potential recipients*.

The message or probe that is the subject of a report is called its **subject message** or **subject probe**.

A report concerning a particular *potential recipient* is conveyed to the *originator* of the subject message or probe unless the *potential recipient* is a *member recipient*. In the latter case, the report is conveyed to the DL of which the *member recipient* is a member. As a local matter (i.e., by policy established for that

particular DL), the report may be further conveyed to the DL's owner; either to another, containing DL (in the case of nesting) or to the originator of the subject message (otherwise); or both.

The outcomes that a single report may relate are of the following kinds:

a) **delivery report**: *Delivery*, *export*, or *affirmation* of the subject message or probe, or *DL expansion*.

b) **non-delivery report**: *Non-delivery* or *non-affirmation* of the subject message or probe.

A report may comprise one or more delivery and/or non-delivery reports. A message or probe may provoke several delivery and/or non-delivery reports concerning a particular *potential recipient*. Each marks the passage of a different transmittal *step* or *event*.

9 Operational Model

This clause provides an operational model of Message Handling. The concrete realization of the model is the subject of other parts of ISO/IEC 10021.

The MHS can convey an information object to individual users, DLs, or a mix of the two. Such conveyance is accomplished by a process called *transmittal* comprising *steps* and *events*. The process, its parts, and the roles that users and DLs play in it are defined and described below.

9.1 Transmittal

The conveyance or attempted conveyance of a message or probe is called **transmittal**. Transmittal encompasses a message's conveyance from its *originator* to its *potential recipients*, and a probe's conveyance from its *originator* to MTAs able to *affirm* the described messages' *deliverability* to the probe's *potential recipients*. Transmittal also encompasses the conveyance or attempted conveyance to the *originator* of any reports the message or probe may provoke.

A transmittal comprises a sequence of *transmittal steps* and *events*. A **transmittal step** (or **step**) is the conveyance of a message, probe, or report from one functional object to another "adjacent" to it. A **transmittal event** (or **event**) is processing of a message, probe, or report within a functional object that may influence the functional object's selection of the next transmittal step or event.

The information flow of transmittal is depicted in Figure 5. The figure shows the kinds of functional objects--direct users, indirect users, UAs, MSs, MTAs, and AUs--that may be involved in a transmittal, the information objects--messages, probes, and reports--that may be conveyed between them, and the names of the transmittal steps by means of which those conveyances are accomplished.

The figure highlights the facts that a message or report may be retrieved repeatedly and that only the first conveyance of a retrieved object from UA to user constitutes *receipt*.

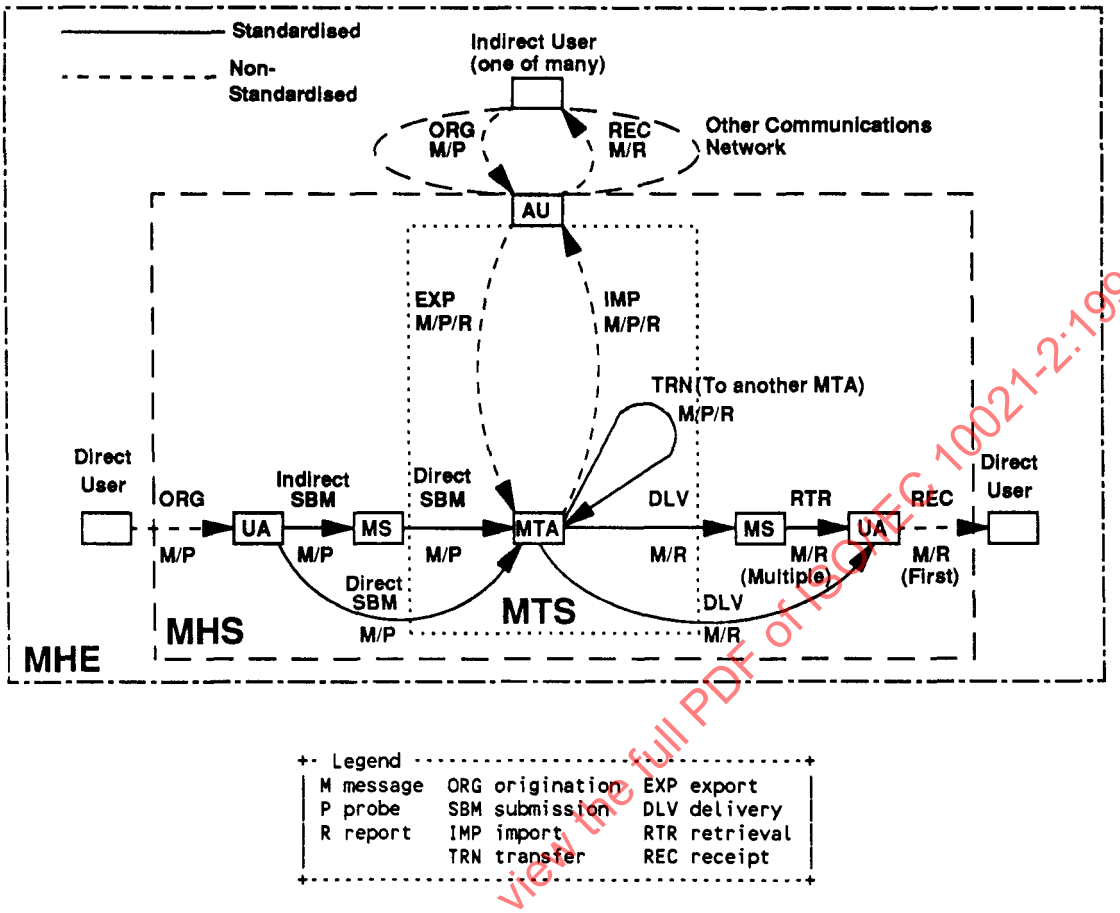

Figure 5
The Information Flow of Transmittal

One event plays a distinguished role in transmittal. *Splitting* replicates a message or probe and divides responsibility for its *immediate recipients* among the resulting information objects. The potential recipients associated with a particular instance of a message or probe are called the **immediate recipients**. An MTA stages a splitting if the next step or event required in the conveyance of a message or probe to some immediate recipients differs from that required in its conveyance to others. Each of the step and event descriptions which follow assumes that the step or event is appropriate for all immediate recipients, a situation that can be created, if necessary, by splitting.

9.2 Transmittal Roles

Users and DLs play a variety of roles in a message's or probe's transmittal. These roles are informally categorized as "source" roles, "destination" roles, or statuses to which users or DLs can be elevated.

A user may play the following "source" role in the transmittal of a message or probe:

a) **originator**: The user (but not DL) that is the ultimate source of a message or probe.

A user or DL may play any of the following "destination" roles in the transmittal of a message or probe:

a) **intended recipient**: One of the users and DLs the originator specifies as a message's or probe's intended destinations.

b) **originator-specified alternate recipient**: The user or DL (if any) to which the originator requests that a message or probe be conveyed if it cannot be conveyed to a particular intended recipient.

c) **member recipient**: A user or DL to which a message (but not a probe) is conveyed as a result of *DL expansion*.

d) **recipient-assigned alternate recipient**: The user or DL (if any) to which an intended, originator-specified alternate, or member recipient may have elected to *redirect* messages.

A user or DL may attain any of the following statuses in the course of a message's or probe's transmittal:

a) **potential recipient**: Any user or DL to (i.e., toward) which a message or probe is conveyed at any point during the course of transmittal. Necessarily an intended, originator-specified alternate, member, or recipient-assigned alternate recipient.

b) **actual recipient** (or **recipient**): A potential recipient for which *delivery* or *affirmation* takes place.

9.3 Transmittal Steps

The kinds of steps that may occur in a transmittal are listed in the first column of Table 5. For each listed kind, the second column indicates whether ISO/IEC 10021 standardizes such steps, the third column the kinds of information objects--messages, probes, and reports--that may be conveyed in such a step, the fourth column the kinds of functional objects--users, UAs, MSs, MTAs, and AUs--that may participate in such a step as the object's source or destination.

The table is divided into three sections. The steps in the first section apply to the "creation" of messages and probes, those in the last to the "disposal" of messages and reports, and those in the middle section to the "relaying" of messages, probes, and reports.

Table 5
Transmittal Steps

Transmittal Step	Standardized?	Information Objects			Functional Objects				
		M	P	R	user	UA	MS	MTA	AU
origination	No	x	x	-	S	D	-	-	-
submission	Yes	x	x	-	-	S	SD	D	-
import	No	x	x	x	-	-	-	D	S
transfer	Yes	x	x	x	-	-	-	SD	-
export	No	x	x	x	-	-	-	S	D
delivery	Yes	x	-	x	-	D	D	S	-
retrieval	Yes	x	-	x	-	D	S	-	-
receipt	No	x	-	x	D	S	-	-	-

Legend
M message S source x permitted
P probe D destination
R report

The kinds of transmittal steps, summarized in the table, are individually defined and described in the subclauses below.

9.3.1 Origination

In an **origination** step, either a direct user conveys a message or probe to its UA, or an indirect user conveys a message or probe to the communication system that serves it. This step gives birth to the message or probe and is the first step in its transmittal.

The user above constitutes the message's or probe's originator. In this step, the originator identifies the message's or probe's intended recipients. Additionally, for each intended recipient, the originator may (but need not) identify an originator-specified alternate recipient.

9.3.2 Submission

In a **submission** step, a message or probe is conveyed to an MTA and thus entrusted to the MTS. Two kinds of submission are distinguished:

a) **indirect submission**: A transmittal step in which the originator's UA conveys a message or probe to its MS and in which the MS effects *direct submission*. Such a step follows origination.

   This step may be taken only if the user is equipped with an MS.

b) **direct submission**: A transmittal step in which the originator's UA or MS conveys a message or probe to an MTA. Such a step follows origination or occurs as part of indirect submission.

   This step may be taken whether or not the user is equipped with an MS.

Indirect and direct submission are functionally equivalent except that additional capabilities may be available with the former. Indirect submission may differ from direct submission in other respects (e.g., the number of open systems with which that embodying a UA must interact) and for that reason be preferable to direct submission.

The UA or MS involved in direct submission is called the **submission agent**. A submission agent is made known to the MTS by a process of registration, as a result of which the submission agent and MTS keep one another informed of their names, their locations, and any other characteristics required for their interaction.

9.3.3 Import

In an **import** step, an AU conveys a message, probe, or report to an MTA. This step injects into the MTS an information object born in another communication system, and follows its conveyance by that system.

NOTE - The concept of importing is a generic one. How this step is effected varies, of course, from one type of AU to another.

9.3.4 Transfer

In a **transfer** step, one MTA conveys a message, probe, or report to another. This step transports an information object over physical and sometimes organizational distances and follows direct submission, import, or (a prior) transfer.

This step may be taken, of course, only if the MTS comprises several MTAs.

The following kinds of transfer are distinguished, on the basis of the number of *MDs* involved:

a) **internal transfer**: A transfer involving MTAs within a single *MD*.

b) **external transfer**: A transfer involving MTAs in different *MDs*.

9.3.5 Export

In an **export** step, an MTA conveys a message, probe, or report to an AU. This step ejects from the MTS an information object bound for another communication system. It follows direct submission, import, or transfer.

As part of this step, the MTA may generate a delivery report.

NOTE - The concept of exporting is a generic one. How this step is effected varies, of course, from one type of AU to another.

9.3.6 Delivery

In a **delivery** step, an MTA conveys a message or report to an MS or UA. The MS and UA are those of a potential recipient of the message, or the originator of the report's subject message or probe. This step entrusts the information object to a representative of the user and follows direct submission, import, or transfer. It also elevates the user in question to the status of an actual recipient.

As part of this step, in the case of a message, the MTA may generate a delivery report.

The MS or UA involved is called the **delivery agent**. A delivery agent is made known to the MTS by a process of registration, as a result of which the delivery agent and MTS keep one another informed of their names, their locations, and any other characteristics required for their interaction.

9.3.7 Retrieval

In a **retrieval** step, a user's MS conveys a message or report to its UA. The user in question is an actual recipient of the message or the originator of the subject message or probe. This step non-destructively retrieves the information object from storage. This step follows delivery or (a prior) retrieval.

This step may be taken only if the user is equipped with an MS.

9.3.8 Receipt

In a **receipt** step, either a UA conveys a message or report to its direct user, or the communication system that serves an indirect user conveys such an information object to that user. In either case, this step conveys the object to its ultimate destination.

In the case of a direct user, this step follows the object's delivery or first retrieval (only). In the case of an indirect user, it follows the information object's conveyance by the communication system serving the user. In either case, the user is a potential recipient (and, in the case of a direct user, an actual recipient) of the message in question, or the originator of the subject message or probe.

9.4 Transmittal Events

The kinds of events that may occur in a transmittal are listed in the first column of Table 6. For each listed kind, the second column indicates the kinds of information objects--messages, probes, and reports--for which such events may be staged, the third column the kinds of functional objects--users, UAs, MSs, MTAs, and AUs--that may stage such events.

All the events occur within the MTS.

Table 6
Transmittal Events

Transmittal Event	Information Objects			Functional Objects				
	M	P	R	user	UA	MS	MTA	AU
splitting	x	x	-	-	-	-	x	-
joining	x	x	x	-	-	-	x	-
name resolution	x	x	-	-	-	-	x	-
DL expansion	x	-	-	-	-	-	x	-
redirection	x	x	-	-	-	-	x	-
conversion	x	x	-	-	-	-	x	-
non-delivery	x	-	x	-	-	-	x	-
non-affirmation	-	x	-	-	-	-	x	-
affirmation	-	x	-	-	-	-	x	-
routing	x	x	x	-	-	-	x	-

Legend
M message x permitted
P probe
R report

The kinds of transmittal events, summarized in the table, are individually defined and described in the subclauses below.

9.4.1 Splitting

In a **splitting** event, an MTA replicates a message or probe, dividing responsibility for its immediate recipients among the resulting information objects. This event effectively allows an MTA to independently convey an object to various potential recipients.

An MTA stages a splitting when the next step or event required in the conveyance of a message or probe to some immediate recipients differs from that required in its conveyance to others.

9.4.2 Joining

In a **joining** event, an MTA combines several instances of the same message or probe, or two or more delivery and/or non-delivery reports for the same subject message or probe.

An MTA may, but need not stage a joining when it determines that the same events and next step are required to convey several highly related information objects to their destinations.

9.4.3 Name Resolution

In a **name resolution** event, an MTA adds the corresponding *O/R address* to the *O/R name* that identifies one of a message's or probe's immediate recipients.

9.4.4 DL Expansion

In a **DL expansion** event, an MTA resolves a DL among a message's (but not a probe's) immediate recipients to its members which are thereby made member recipients. This event removes indirection from the immediate recipients' specification.

A particular DL is always subjected to DL expansion at a pre-established location within the MTS. This location is called the DL's **expansion point** and is identified by an *O/R address*.

As part of this event, the MTA may generate a delivery report.

DL expansion is subject to submit permission. In the case of a nested DL, that permission must have been granted to the DL of which the nested DL is a member. Otherwise, it must have been granted to the originator.

9.4.5 Redirection

In a **redirection** event, an MTA replaces a user or DL among a message's or probe's immediate recipients with an originator-specified or recipient-assigned alternate recipient.

9.4.6 Conversion

In a **conversion** event, an MTA transforms parts of a message's content from one EIT to another, or alters a probe so it appears that the described messages were so modified. This event increases the likelihood that an information object can be delivered or affirmed by tailoring it to its immediate recipients.

The following kinds of conversion are distinguished, on the basis of how the EIT of the information to be converted and the EIT to result from the conversion are selected:

a) **explicit conversion**: A conversion in which the originator selects both the initial and final EITs.

b) **implicit conversion**: A conversion in which the MTA selects the final EITs based upon the initial EITs and the capabilities of the UA.

9.4.7 Non-delivery

In a **non-delivery** event, an MTA determines that the MTS cannot deliver a message to its immediate recipients, or cannot deliver a report to the originator of its subject message or probe. This event halts the conveyance of an object the MTS deems unconveyable.

As part of this event, in the case of a message, the MTA generates a non-delivery report.

An MTA stages a non-delivery, e.g., when it determines that the immediate recipients are improperly specified, that they do not accept delivery of messages like that at hand, or that the message has not been delivered to them within pre-specified time limits.

9.4.8 Non-affirmation

In a **non-affirmation** event, an MTA determines that the MTS could not deliver a described message to a probe's immediate recipients. This event partially or fully determines the answer to the question posed by a probe.

As part of this event, the MTA generates a non-delivery report.

An MTA stages a non-affirmation, e.g., when it determines that the immediate recipients are improperly specified or would not accept delivery of a described message.

9.4.9 Affirmation

In an **affirmation** event, an MTA determines that the MTS could deliver any described message to a probe's immediate recipients. This event partially or fully determines the answer to the question posed by a probe, and elevates the immediate recipients to the status of actual recipients.

As part of this event, the MTA may generate a delivery report.

An MTA stages an affirmation once it determines that the immediate recipients are properly specified and, if the immediate recipients are users (but not DLs), would accept delivery of any described

message. If the immediate recipients are DLs, an MTA stages an affirmation if the DL exists and the originator has the relevant submit permission.

9.4.10 Routing

In a **routing** event, an MTA selects the "adjacent" MTA to which it will transfer a message, probe, or report. This event incrementally determines an information object's route through the MTS and (obviously) may be taken only if the MTS comprises several MTAs.

The following kinds of routing are distinguished, on the basis of the kind of transfer for which they prepare:

a) **internal routing**: A routing preparatory to an internal transfer (i.e., a transfer within an *MD*).

b) **external routing**: A routing preparatory to an external transfer (i.e., a transfer between *MDs*).

An MTA stages a routing when it determines that it can stage no other event, and take no step, regarding an object.

10 Security Model

This clause provides an abstract security model for Message Transfer. The concrete realization of the model is the subject of other parts of ISO/IEC 10021. The security model provides a framework for describing the security services that counter potential threats (see annex D) to the MTS and the security elements that support those services.

The security features are an optional extension to the MHS that can be used to minimise the risk of exposure of assets and resources to violations of a security policy (threats). Their aim is to provide features independently of the communications services provided by other lower or higher entities. Threats may be countered by the use of physical security, computer security (COMPUSEC), or security services provided by the MHS. Depending on the perceived threats, certain of the MHS security services will be selected in combination with appropriate physical security and COMPUSEC measures. The security services supported by the MHS are described below. The naming and structuring of the services are based on ISO 7498-2.

NOTE - Despite these security features, certain attacks may be mounted against communication between a user and the MHS or against user-to-user communication (e.g., in the case of users accessing the MHS through an access unit, or in the case of users remotely accessing their UAs).

In many cases, the broad classes of threats are covered by several of the services listed.

The security services are supported through use of service elements of the Message Transfer Service message envelope. The envelope contains security relevant arguments as described in ISO/IEC 10021-4. The description of the security services takes the following general form. In clause 10.2 the services are listed, with, in each case, a definition of the service and an indication of how it may be provided using the security elements in ISO/IEC 10021-4. In clause 10.3 the security elements are individually described, with, in each case, a definition of the service element and references to its constituent arguments in ISO/IEC 10021-4.

Many of the techniques employed rely on encryption mechanisms. The security services in the MHS allow for flexibility in the choice of algorithms. However, in some cases only the use of asymmetric encryption has been fully defined in this part of ISO/IEC 10021. A future addenda to this part of ISO/IEC 10021 may allow use of alternative mechanisms based on symmetric encipherment.

NOTE - The use of the terms "security service" and "security element" in this clause are not to be confused with the terms "service" and "element of service" as used in ISO/IEC 10021-1. The former terms are used in the present clause to maintain consistency with ISO 7498-2.

10.1 Security Policies

Security services in the MHS must be capable of supporting a wide range of security policies which extend beyond the confines of the MHS itself. The services selected and the threats addressed will depend on the individual application and levels of trust in parts of the system.

A security policy defines how the risk to and exposure of assets can be reduced to an acceptable level.

In addition, operation between different domains, each with their own security policy, will be required. As each domain will be subject to its own overall security policy, covering more than just the MHS, a bilateral agreement on interworking between two domains will be required. This must be defined so as not to conflict with the security policies for either domain and effectively becomes part of the overall security policy for each domain.

10.2 Security Services

This subclause defines the Message Transfer security services. The naming and structuring of the services are based on ISO 7498-2.

Message Transfer security services fall into several broad classes. These classes and the services in each are listed in Table 7. An asterisk (*) under the heading of the form *X*/*Y* indicates that the service can be provided from a functional object of type *X* to one of type *Y*.

Table 7
Message Transfer Security Services

SERVICE	UA/UA	MS/MTA UA/MS	MTA/MS UA/MTA	MTA/UA MTA/MTA	MS/UA
ORIGIN AUTHENTICATION					
Message Origin Authentication	*	*	*	-	-
Probe Origin Authentication	-	-	*	*	-
Report Origin Authentication	-	-	-	-	*
Proof of Submission	-	-	-	-	-
Proof of Delivery	*	-	-	-	-
SECURE ACCESS MANAGEMENT					
Peer Entity Authentication	-	*	*	*	*
Security Context	-	*	*	*	*
DATA CONFIDENTIALITY					
Connection Confidentiality	-	*	*	*	*
Content Confidentiality	*	-	-	-	-
Message Flow Confidentiality	*	-	-	-	-
DATA INTEGRITY SERVICES					
Connection Integrity	-	*	*	*	*
Content Integrity	*	-	-	-	-
Message Sequence Integrity	*	-	-	-	-
NON-REPUDIATION					
Non-repudiation of Origin	*	-	-	*	-
Non-repudiation of Submission	-	-	-	-	*
Non-repudiation of Delivery	*	-	-	-	-
MESSAGE SECURITY LABELLING					
Message Security Labelling	*	*	*	*	*
SECURITY MANAGEMENT SERVICES					
Change Credentials	-	*	-	*	*
Register	-	*	-	*	-
MS-Register	-	*	-	-	-

Note - This service is provided by the recipient's MS to the originator's UA.

Throughout the security service definitions that follow, reference is made to Figure 6, which reiterates the MHS functional model in simplified form. The numeric labels are referenced in the text.

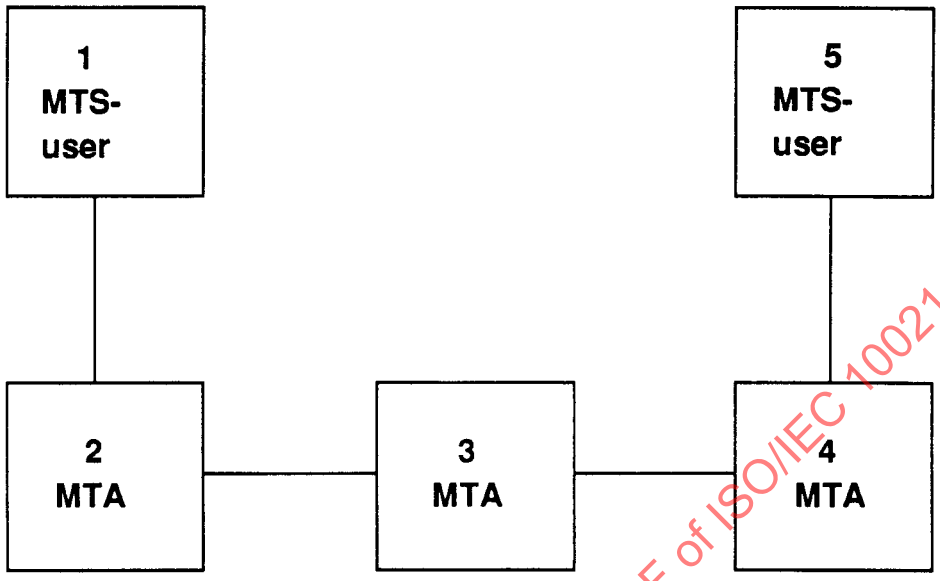

Figure 6
Simplified MHS Functional Model

10.2.1 Origin Authentication Security Services

These security services provide for the authentication of the identity of communicating peer entities and sources of data.

10.2.1.1 Data Origin Authentication Security Services

These security services provide corroboration of the origin of a message, probe, or report to all concerned entities (i.e., MTAs or recipient MTS-users). These security services cannot protect against duplication of messages, probes, or reports.

10.2.1.1.1 Message Origin Authentication Security Service

The Message Origin Authentication Service enables the corroboration of the source of a message.

This security service can be provided using either the Message Origin Authentication or the Message Argument Integrity security element. The former can be used to provide the security service to any of the parties concerned (1-5 inclusive in Figure 6), whereas the latter can only be used to provide the security service to MTS-users (1 or 5 in Figure 6). The security element chosen depends on the prevailing security policy.

10.2.1.1.2 Probe Origin Authentication Security Service

The Probe Origin Authentication security service enables the corroboration of the source of a probe.

This security service can be provided by using the Probe Origin Authentication security element. This security element can be used to provide the security service to any of the MTAs through which the probe is transferred (2-4 inclusive in Figure 6).

10.2.1.1.3 Report Origin Authentication Security Service

The Report Origin Authentication security service enables the corroboration of the source of a report.

This security service can be provided by using the Report Origin Authentication security element. This security element can be used to provide the security service to the originator of the subject message or probe, as well as to any MTA through which the report is transferred (1-5 inclusive in Figure 6).

10.2.1.2 Proof of Submission Security Service

This security service enables the originator of a message to obtain corroboration that it has been received by the MTS for delivery to the originally specified recipient(s).

This security service can be provided by using the Proof of Submission security element.

10.2.1.3 Proof of Delivery Security Service

This security service enables the originator of a message to obtain corroboration that it has been delivered by the MTS to its intended recipient(s).

This security service can be provided by using the Proof of Delivery security element.

10.2.2 Secure Access Management Security Service

The Secure Access Management security service is concerned with providing protection for resources against their unauthorised use. It can be divided into two components, namely the Peer Entity Authentication and the Security Context security services.

10.2.2.1 Peer Entity Authentication Security Service

This security service is provided for use at the establishment of a connection to confirm the identity of the connecting entity. It may be used on the links 1-2, 2-3, 3-4, or 4-5 in Figure 6 and provides confidence, at the time of usage only, that an entity is not attempting a masquerade or an unauthorised replay of a previous connection.

This security service is supported by the Authentication Exchange security element. Note that use of this security element may yield other data as a result of its operation that in certain circumstances can be used to support a Connection Confidentiality and/or a Connection Integrity security service.

10.2.2.2 Security Context Security Service

This security service is used to limit the scope of passage of messages between entities by reference to the Security Labels associated with messages. This security service is therefore closely related to the Message Security Labelling security service, which provides for the association of messages and Security Labels.

The Security Context security service is supported by the Security Context and the Register security elements.

10.2.3 Data Confidentiality Security Services

These security services provide for the protection of data against unauthorised disclosure.

10.2.3.1 Connection Confidentiality Security Service

The MHS does not provide a Connection Confidentiality security service. However, data for the invocation of such a security service in underlying layers may be provided as a result of using the Authentication Exchange security element to provide the Peer Entity Authentication security service. The security service may be required on any of links 1-2, 2-3, 3-4, or 4-5 in Figure 6.

10.2.3.2 Content Confidentiality Security Service

The Content Confidentiality security service provides assurance that the content of a message is only known to the sender and recipient of a message.

It may be provided using a combination of the Content Confidentiality and the Message Argument Confidentiality security elements. The Message Argument Confidentiality security element can be used to transfer a secret key which is used with the Content Confidentiality security element to encipher the message content. Using these security elements the service is provided from MTS-user 1 to MTS-user 5 in Figure 6, with the message content being unintelligible to MTAs.

10.2.3.3 Message Flow Confidentiality Security Service

This security service provides for the protection of information which might be derived from observation of message flow. Only a limited form of this security service is provided by the MHS.

The Double Enveloping Technique enables a complete message to become the content of another message. This could be used to hide addressing information from certain parts of the MTS. Used in conjunction with traffic padding (which is beyond the current scope of ISO/IEC 10021) this could be used to provide message flow confidentiality. Other elements of this service, such as routing control or pseudonyms, are also beyond the scope of ISO/IEC 10021.

10.2.4 Data Integrity Security Services

These security services are provided to counter active threats to the MHS.

10.2.4.1 Connection Integrity Security Service

The MHS does not provide a Connection Integrity security service. However, data for the invocation of such a security service in underlying layers may be provided by using the Authentication Exchange security element to provide the Peer Entity Authentication security service. The security service may be required on any of links 1-2, 2-3, 3-4, or 4-5 in Figure 6.

10.2.4.2 Content Integrity Security Service

This security service provides for the integrity of the contents of a single message. This takes the form of enabling the determination of whether the message content has been modified. This security service does not enable the detection of message replay, which is provided by the Message Sequence Integrity security service.

This security service can be provided in two different ways using two different combinations of security elements.

The Content Integrity security element together with the Message Argument Integrity security element and, in some cases, the Message Argument Confidentiality security element can be used to provide the security service to a message recipient, i.e., for communication from MTS-user 1 to MTS-user 5 in Figure 6. The Content Integrity security element is used to compute a Content Integrity Check as a function of the entire message content. Depending on the method used to compute the Content Integrity Check, a secret key may be required, which may be confidentially sent to the message recipient using the Message Argument Confidentiality security element. The Content Integrity Check is protected

against change using the Message Argument Integrity security element. The integrity of any confidential message arguments is provided using the Message Argument Confidentiality security element.

The Message Origin Authentication security element can also be used to provide this security service.

10.2.4.3 Message Sequence Integrity Security Service

This security service protects the originator and recipient of a sequence of messages against re-ordering of the sequence. In doing so it protects against replay of messages.

This security service may be provided using a combination of the Message Sequence Integrity and the Message Argument Integrity security elements. The former provides a sequence number to each message, which may be protected against change by use of the latter. Simultaneous confidentiality and integrity of the Message Sequence Number may be provided by use of the Message Argument Confidentiality security element.

These security elements provide the service for communication from MTS-user 1 to MTS-user 5 in Figure 6, and not to the intermediate MTAs.

10.2.5 Non-Repudiation Security Services

These security services provide irrevocable proof to a third party after the message has been submitted, sent, or delivered, that the submission, sending, or receipt did occur as claimed. Note that for this to function correctly, the security policy must explicitly cover the management of asymmetric keys for the purpose of non-repudiation services if asymmetric algorithms are being used.

10.2.5.1 Non-repudiation of Origin Security Service

This security service provides the recipient(s) of a message with irrevocable proof of the origin of the message, its content, and its associated Message Security Label.

This security service can be provided in two different ways using two different combinations of security elements. Note that its provision is very similar to the provision of the (weaker) Content Integrity security service.

The Content Integrity security element together with the Message Argument Integrity security element and, in some cases, the Message Argument Confidentiality security element can be used to provide the service to a message recipient, i.e., for communication from MTS-user 1 to MTS-user 5 in Figure 6. The Content Integrity security element is used to compute a Content Integrity Check as a function of the entire message content. Depending on the method used to compute the Content Integrity Check, a secret key may be required, which may be confidentially sent to the message recipient using the Message Argument Confidentiality security element. The Content Integrity Check and, if required, the Message Security Label are protected against change and/or repudiation using the Message Argument Integrity security element. Any confidential message arguments are protected against change and/or repudiation using the Message Argument Confidentiality security element.

If the Content Confidentiality security service is not required, the Message Origin Authentication security element may also be used as a basis for this security service. In this case the security service may be provided to all elements of the MHS, i.e., for all of 1-5 in Figure 6.

10.2.5.2 Non-Repudiation of Submission Security Service

This security service provides the originator of the message with irrevocable proof that the message was submitted to the MTS for delivery to the originally specified recipient(s).

This security service is provided using the Proof of Submission security element in much the same way as that security element is used to support the (weaker) Proof of Submission security service.

10.2.5.3 Non-Repudiation of Delivery Security Service

This security service provides the originator of the message with irrevocable proof that the message was delivered to its originally specified recipient(s).

This security service is provided using the Proof of Delivery security element in much the same way as that security element is used to support the (weaker) Proof of Delivery security service.

10.2.6 Message Security Labelling Security Service

This security service allows Security Labels to be associated with all entities in the MHS, i.e., MTAs and MTS-users. In conjunction with the Security Context security service it enables the implementation of security policies defining which parts of the MHS may handle messages with specified associated Security Labels.

This security service is provided by the Message Security Label security element. The integrity and confidentiality of the label are provided by the Message Argument Integrity and the Message Argument Confidentiality security elements.

10.2.7 Security Management Services

A number of security management services are needed by the MHS. The only management services provided within ISO/IEC 10021-4 are concerned with changing credentials and registering MTS-user security labels.

10.2.7.1 Change Credentials Security Service

This security service enables one entity in the MHS to change the credentials concerning it held by another entity in the MHS. It may be provided using the Change Credentials security element.

10.2.7.2 Register Security Service

This security service enables the establishment at an MTA of the Security Labels which are permissible for one particular MTS-user. It may be provided using the Register security element.

10.2.7.3 MS-Register Security Service

This security service enables the establishment of the security label which are permissible for the MS-user.

10.3 Security Elements

The following subclauses describe the security elements available in the protocols described within ISO/IEC 10021-4 to support the security services in the MHS. These security elements relate directly to arguments in various services described in ISO/IEC 10021-4. The objective of this subclause is to separate out each element of the ISO/IEC 10021-4 service definitions that relate to security, and to define the function of each of these identified security elements.

10.3.1 Authentication Security Elements

These security elements are defined in order to support authentication and integrity security services.

10.3.1.1 Authentication Exchange Security Element

The Authentication Exchange security element is designed to authenticate, possibly mutually, the identity of an MTS-user to an MTA, an MTA to an MTA, an MTA to an MTS-user, an MS to a UA, or a UA to an MS. It is based on the exchange or use of secret data, either passwords, asymmetrically encrypted tokens, or symmetrically encrypted tokens. The result of the exchange is corroboration of the identity of the other party, and, optionally, the transfer of confidential data which may be used in providing the Connection Confidentiality and/or the Connection Integrity security service in underlying layers. Such an authentication is only valid for the instant that it is made and the continuing validity of the authenticated identity depends on whether the exchange of confidential data, or some other mechanism, is used to establish a secure communication path. The establishment and use of a secure communication path is outside the scope of this part of ISO/IEC 10021.

This security element uses the Initiator Credentials argument and the Responder Credentials result of the MTS-bind, MS-bind, and MTA-bind services. The transferred credentials are either passwords or tokens.

10.3.1.2 Data Origin Authentication Security Elements

These security elements are specifically designed to support data origin authentication services, although they may also be used to support certain data integrity services.

10.3.1.2.1 Message Origin Authentication Security Element

The Message Origin Authentication security element enables anyone who receives or transfers message to authenticate the identity of the MTS-user that originated the message. This may mean the provision of the Message Origin Authentication or the Non-repudiation of Origin security service.

The security element involves transmitting, as part of the message, a Message Origin Authentication Check, computed as a function of the message content, the message Content Identifier, and the Message Security Label. If the Content Confidentiality security service is also required, the Message Origin Authentication Check is computed as a function of the enciphered rather than the unenciphered message content. By operating on the message content as conveyed in the overall message (i.e., after the optional Content Confidentiality security element), any MHS entity can check the overall message integrity without the need to see the plaintext message content. However, if the Content Confidentiality security service is used, the Message Origin Authentication security element cannot be used to provide the Non-repudiation of Origin security service.

The security element uses the Message Origin Authentication Check, which is one of the arguments of the Message Submission, Message Transfer, and Message Delivery services.

10.3.1.2.2 Probe Origin Authentication Security Element

Similar to the Message Origin Authentication security element, the Probe Origin Authentication security element enables any MTA to authenticate the identity of the MTS-user which originated a probe.

This security element uses the Probe Origin Authentication Check, which is one of the arguments of the Probe Submission service.

10.3.1.2.3 Report Origin Authentication Security Element

Similar to the Message Origin Authentication security element, the Report Origin Authentication security element enables any MTA or MTS-user who receives a report to authenticate the identity of the MTA which originated the report.

This security element uses the Report Origin Authentication Check, which is one of the arguments of the Report Delivery service.

10.3.1.3 Proof of Submission Security Element

This security element provides the originator of a message with the means to establish that a message was accepted by the MHS for transmission.

The security element is made up of two arguments: a request for Proof of Submission, sent with a message at submission time, and the Proof of Submission, returned to the MTS-user as part of the Message Submission results. The Proof of Submission is generated by the MTS, and is computed as a function of all the arguments of the submitted message, the Message Submission Identifier, and the Message Submission Time.

The Proof of Submission argument can be used to support the Proof of Submission security service. Depending on the security policy in force, it may also be able to support the (stronger) Non-repudiation of Submission security service.

The Proof of Submission Request is an argument of the Message Submission service. The Proof of Submission is one of the results of the Message Submission service.

10.3.1.4 Proof of Delivery Security Element

This security element provides the originator of a message with the means to establish that a message was delivered to the destination by the MHS.

The security element is made up of a number of arguments. The message originator includes a Proof of Delivery Request with the submitted message, and this request is delivered to each recipient with the message. A recipient may then compute the Proof of Delivery as a function of a number of arguments associated with the message. The proof of delivery is returned by the MTS to the message originator, as part of a report on the results of the original Message Submission.

The Proof of Delivery can be used to support the Proof of Delivery security service. Depending on the security policy in force, it may also be able to support the (stronger) Non-repudiation of Delivery security service.

The Proof of Delivery Request is an argument of the Message Submission, Message Transfer, and Message Delivery services. The Proof of Delivery is both one of the results of the Message Delivery service and one of the arguments of the Report Transfer and Report Delivery services.

NOTE - Non-receipt of a Proof of Delivery does not imply non-delivery.

10.3.2 Secure Access Management Security Elements

These security elements are defined in order to support the Secure Access Management security service and the security management services.

10.3.2.1 Security Context Security Element

When an MTS-user or an MTA binds to an MTA or MTS-user, the bind operation specifies the security context of the connection. This limits the scope of passage of messages by reference to the labels associated with messages. Secondly, the Security Context of the connection may be temporarily altered for submitted or delivered messages.

The Security Context itself consists of one or more Security Labels defining the sensitivity of interactions that may occur in line with the security policy in force.

Security Context is an argument of the MTS-bind and MTA-bind services.

10.3.2.2 Register Security Element

The Register security element allows the establishment at an MTA of an MTS-user's permissible security labels.

This security element is provided by the Register service. The Register service enables an MTS-user to change arguments, held by the MTS, relating to delivery of messages to that MTS-user.

10.3.2.3 MS-Register Security Element

The MS-Register security element allows the establishment of the MS-user's permissible security labels.

This security element is provided by the MS-Register service. The MS-Register service enables an MS-user to change arguments held by the MS relating to the retrieval of messages to that MS-user.

10.3.3 Data Confidentiality Security Elements

These security elements, based on the use of encipherment, are all concerned with the provision of confidentiality of data passed from one MHS entity to another.

10.3.3.1 Content Confidentiality Security Element

The Content Confidentiality security element provides assurance that the content of the message is protected from eavesdropping during transmission by use of an encipherment security element. The security element operates such that only the recipient and sender of the message know the plaintext message content.

The specification of the encipherment algorithm, the key used, and any other initialising data are conveyed using the Message Argument Confidentiality and the Message Argument Integrity security elements. The algorithm and key are then used to encipher or decipher the message contents.

The Content Confidentiality security element uses the Content Confidentiality Algorithm Identifier, which is an argument of the Message Submission, Message Transfer, and Message Delivery services.

10.3.3.2 Message Argument Confidentiality Security Element

The Message Argument Confidentiality security element provides for the confidentiality, integrity, and, if required, the irrevocability of recipient data associated with a message. Specifically, this data will comprise any cryptographic keys and related data that is necessary for the confidentiality and integrity security elements to function properly, if these optional security elements are invoked.

The security element operates by means of the Message Token. The data to be protected by the Message Argument Confidentiality security element constitutes the Encrypted Data within the Message Token. The Encrypted Data within the Message Token is unintelligible to all MTAs.

The Message Token is an argument of the Message Submission, Message Transfer, and Message Delivery services.

10.3.4 Data Integrity Security Elements

These security elements are provided to support the provision of data integrity, data authentication, and non-repudiation services.

10.3.4.1 Content Integrity Security Element

The Content Integrity security element provides protection for the content of a message against modification during transmission.

This security element operates by use of one or more cryptographic algorithms. The specification of the algorithm(s), the key(s) used, and any other initialising data are conveyed using the Message Argument Confidentiality and the Message Argument Integrity security elements. The result of the application of the algorithms and key is the Content Integrity Check, which is sent in the message envelope. The security element is only available to the recipient(s) of the message as it operates on the plaintext message contents.

If the Content Integrity Check is protected using the Message Argument Integrity security element then, depending on the prevailing security policy, it may be used to help provide the Non-repudiation of Origin security service.

The Content Integrity Check is an argument of the Message Submission, Message Transfer, and Message Delivery services.

10.3.4.2 Message Argument Integrity Security Element

The Message Argument Integrity security element provides for the integrity, and, if required, the irrevocability of certain arguments associated with a message. Specifically, these arguments may comprise any selection of the Content Confidentiality Algorithm Identifier, the Content Integrity Check, the Message Security Label, the Proof of Delivery Request, and the Message Sequence Number.

The security element operates by means of the Message Token. The data to be protected by the Message Argument Integrity security element constitutes the signed-data within the Message Token.

The Message Token is an argument of the Message Submission, Message Transfer, and Message Delivery services.

10.3.4.3 Message Sequence Integrity Security Element

The Message Sequence Integrity security element provides protection for the sender and recipient of a message against receipt of messages in the wrong order, or duplicated messages.

A Message Sequence Number is associated with an individual message. This number identifies the position of a message in a sequence from one originator to one recipient. Therefore each originator-recipient pair requiring to use this security element will have to maintain a distinct sequence of message numbers. This security element does not provide for initialisation or synchronisation of Message Sequence Numbers.

10.3.5 Non-repudiation Security Elements

There are no specific Non-repudiation security elements defined in ISO/IEC 10021-4. The non-repudiation services may be provided using a combination of other security elements.

10.3.6 Security Label Security Elements

These security elements exist to support security labelling in the MHS.

10.3.6.1 Message Security Label Security Element

Messages may be labelled with data as specified in the prevailing security policy. The Message Security Label is available for use by intermediate MTAs as part of the overall security policy of the system.

A Message Security Label may be sent as a message argument, and may be protected by the Message Argument Integrity or the Message Origin Authentication security element, in the same manner as other message arguments.

Alternatively, if both confidentiality and integrity are required, the Message Security Label may be protected using the Message Argument Confidentiality security element. In this case the Message Security Label so protected is an originator-recipient argument, and may differ from the Message Security Label in the message envelope.

10.3.7 Security Management Security Elements

10.3.7.1 Change Credentials Security Element

The Change Credentials security element allows the credentials of an MTS-user or an MTA to be updated.

The security element is provided by the MTS Change Credentials service.

10.3.8 Double Enveloping Technique

Additional protection may be provided to a complete message, including the envelope parameters, by the ability to specify that the content of a message is itself a complete message, i.e., a Double Enveloping Technique is available.

This technique is available though the use of the Content Type argument which makes it possible to specify that the content of a message is an Inner Envelope. This Content Type means that the content is itself a message (envelope and content) for forwarding by the recipient named on the outer envelope to the recipient named on the Inner Envelope.

The Content Type is an argument of the Message Submission, Message Transfer, and Message Delivery services.

Section three - Configurations

11 Overview

This section specifies how one can configure the MHS to satisfy any of a variety of functional, physical, and organizational requirements.

This section covers the following topics:

a) Functional configurations;

b) Physical configurations;

c) Organizational configurations;

d) The *Global MHS*.

12 Functional Configurations

This clause specifies the possible functional configurations of the MHS. The variety of such configurations results from the presence or absence of the Directory, and from whether a direct user employs an MS.

12.1 Regarding the Directory

With respect to the Directory, the MHS can be configured for a particular user, or a collection of users (e.g., see clause 14.1), in either of two ways: with or without the Directory. A user without access to the Directory may lack the capabilities described in section five.

NOTE - A partially, rather than fully interconnected Directory may exist for an interim period during which the (global) Directory made possible by International Standards for Directories is under construction.

12.2 Regarding the Message Store

With respect to the MS, the MHS can be configured for a particular direct user in either of two ways: with or without an MS. A user without access to an MS lacks the capabilities of Message Storage. A user in such circumstances depends upon his UA for the storage of information objects, a capability that is a local matter.

The two functional configurations identified above are depicted in Figure 7 which also illustrates one possible configuration of the MTS, and its linkage to another communication system via an AU. In the figure, user 2 is equipped with an MS while user 1 is not.

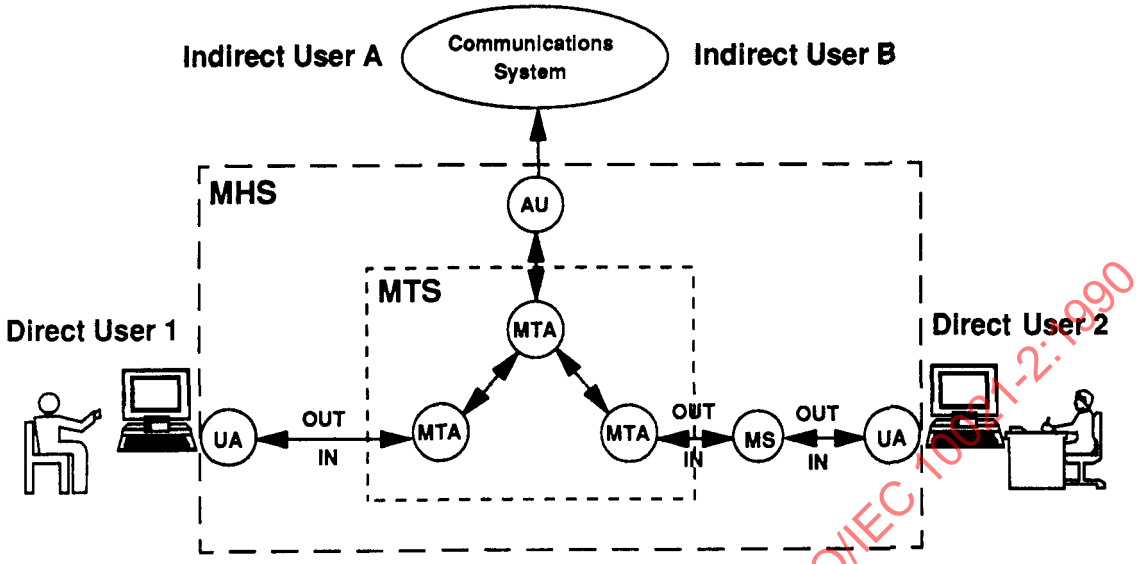

Figure 7
Functional Configurations Regarding the MS

NOTE - While the users depicted in the figure are people, the figure applies with equal force and validity to users of other kinds.

13 Physical Configurations

This clause specifies the possible physical configurations of the MHS, i.e., how the MHS can be realized as a set of interconnected computer systems. Because the number of configurations is unbounded, the clause describes the kinds of *messaging systems* from which the MHS is assembled, and identifies a few important representative configurations.

13.1 Messaging Systems

The building blocks used in the physical construction of the MHS are called *messaging systems*. A **messaging system** is a computer system (possibly but not necessarily an open system) that contains, or realizes, one or more functional objects.

Messaging systems are of the types depicted in Figure 8.

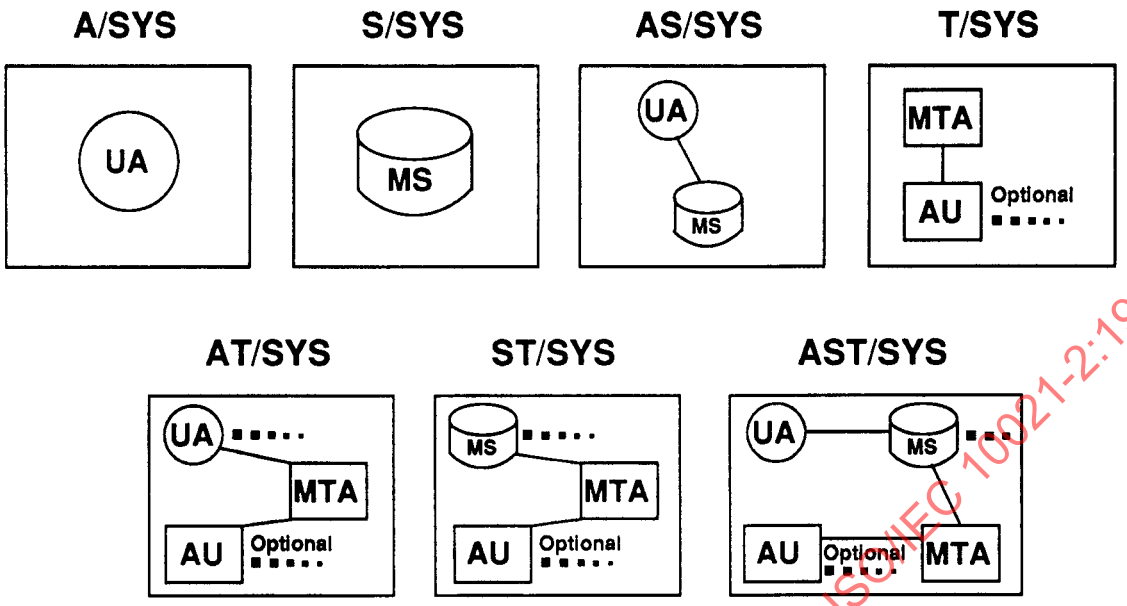

Figure 8
Messaging System Types

The types of messaging system, depicted in the figure, are listed in the first column of Table 8. For each type listed, the second column indicates the kinds of functional object--UAs, MSs, MTAs, and AUs--that may be present in such a messaging system, whether their presence is mandatory or optional, and whether just one or possibly several of them may be present in the messaging system.

The table is divided into two sections. Messaging systems of the types in the first section are dedicated to single users, those of the types in the second can (but need not) serve multiple users.

Table 8
Messaging Systems

Messaging System	Functional Objects			
	UA	MS	MTA	AU
A/SYS	1	-	-	-
S/SYS	-	1	-	-
AS/SYS	1	1	-	-
T/SYS	-	-	1	[M]
AT/SYS	M	-	1	[M]
ST/SYS	-	M	1	[M]
AST/SYS	M	M	1	[M]

Legend: M multiple [...] optional

The messaging system types, summarized in the table, are individually defined and described in the subclauses below.

NOTE - The following major principles governed the admission of messaging system types:

a) An AU and the MTA with which it interacts are typically co-located because no protocol to govern their interaction is standardized.

b) An MTA is typically co-located with multiple UAs or MSs because, of the standardized protocols, only that for transfer simultaneously conveys a message to multiple recipients. The *serial* delivery of a message to multiple recipients served by a messaging system, which the delivery protocol would require, would be inefficient.

c) No purpose is served by co-locating several MTAs in a messaging system because a single MTA serves multiple users, and the purpose of an MTA is to convey objects between, not within such systems. (This is not intended to exclude the possibility of several MTA-related processes co-existing within a single computer system.)

d) The co-location of an AU with an MTA does not affect that system's behaviour with respect to the rest of the MHS. A single messaging system type, therefore, encompasses the AU's presence and absence.

13.1.1 Access Systems

An **access system** (A/SYS) contains one UA and neither an MS, an MTA, nor an AU.

An A/SYS is dedicated to a single user.

13.1.2 Storage Systems

A **storage system** (S/SYS) contains one MS and neither a UA, an MTA, nor an AU.

An S/SYS is dedicated to a single user.

13.1.3 Access and Storage Systems

An **access and storage system** (AS/SYS) contains one UA, one MS, and neither an MTA nor an AU.

An AS/SYS is dedicated to a single user.

13.1.4 Transfer Systems

A **transfer system** (T/SYS) contains one MTA; optionally, one or more AUs; and neither a UA nor an MS.

A T/SYS can serve multiple users.

13.1.5 Access and Transfer Systems

An **access and transfer system** (AT/SYS) contains one or more UAs; one MTA; optionally, one or more AUs; and no MS.

An AT/SYS can serve multiple users.

13.1.6 Storage and Transfer Systems

A **storage and transfer system** (ST/SYS) contains one or more MSs; one MTA; optionally, one or more AUs; and no UA.

An ST/SYS can serve multiple users.

13.1.7 Access, Storage, and Transfer Systems

An **access, storage, and transfer system** (AST/SYS) contains one or more UAs; one or more MSs; one MTA; and optionally, one or more AUs.

An AST/SYS can serve multiple users.

13.2 Representative Configurations

Messaging systems can be combined in various ways to form the MHS. The possible physical configurations are unbounded in number and thus cannot be enumerated. Several important representative configurations, however, are described below and in Figure 9.

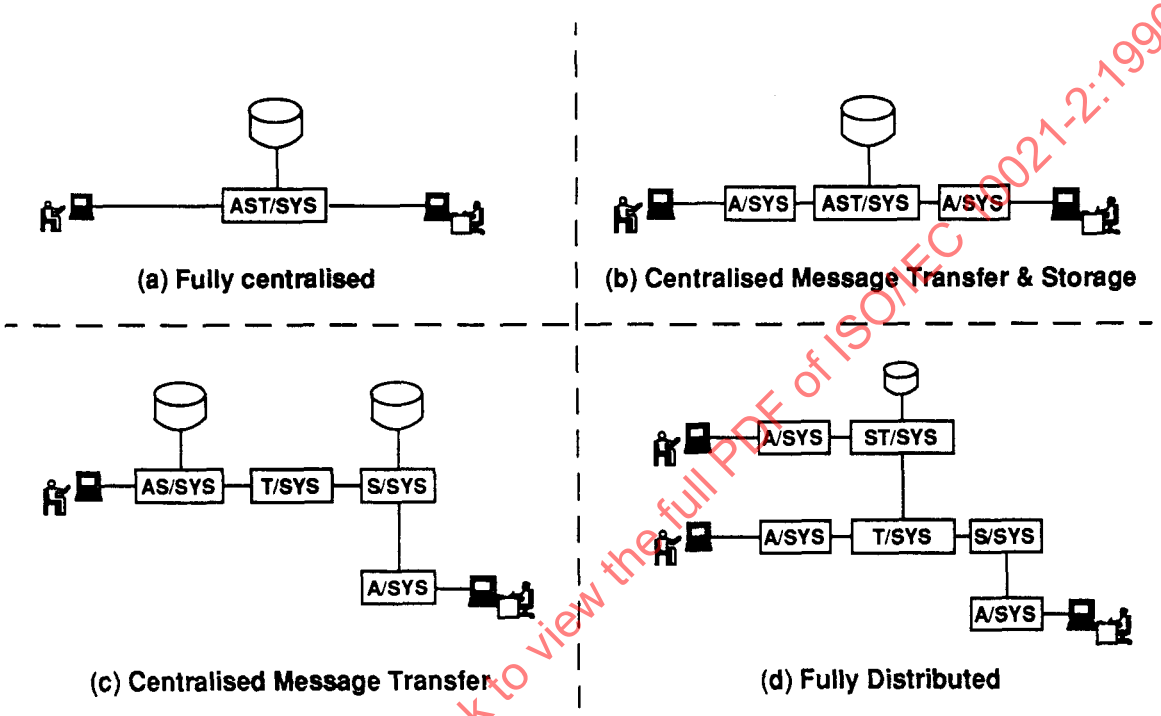

Figure 9
Representative Physical Configurations

NOTES

1. While the users depicted in the figure are people, the figure applies with equal force and validity to users of other kinds.

2. Besides the physical configurations that result from the "pure" approaches below, many "hybrid" configurations can be constructed.

13.2.1 Fully Centralized

The MHS may be fully centralized (panel *a* of the figure). This design is realized by a single AST/SYS which contains functional objects of all kinds and which can serve multiple users.

13.2.2 Centralized Message Transfer and Storage

The MHS may provide both Message Transfer and Message Storage centrally but distributed user access (panel *b* of the figure). This design is realized by a single ST/SYS and, for each user, an A/SYS.

13.2.3 Centralized Message Transfer

The MHS may provide Message Transfer centrally but Message Storage and distributed user access (panel *c* of the figure). This design is realized by a single T/SYS and, for each user, either an AS/SYS alone or an S/SYS and an associated A/SYS.

13.2.4 Fully Distributed

The MHS may provide even distributed Message Transfer (panel *d* of the figure). This design involves multiple ST-SYSs or T-SYSs.

14 Organizational Configurations

This clause specifies the possible organizational configurations of the MHS, i.e., how the MHS can be realized as interconnected but independently managed sets of messaging systems (which are themselves interconnected). Because the number of configurations is unbounded, the clause describes the kinds of *management domains* from which the MHS is assembled, and identifies a few important representative configurations.

14.1 Management Domains

The primary building blocks used in the organizational construction of the MHS are called *management domains*. A **management domain** (**MD**) (or **domain**) is a set of messaging systems--at least one of which contains, or realizes, an MTA--that is managed by a single organization.

The above does not preclude an organization from managing a set of messaging systems (e.g., a single A/SYS) that does not qualify as an MD for lack of an MTA. Such a collection of messaging systems, a secondary building block used in the MHS' construction, "attaches" to an MD.

MDs are of several types which are individually defined and described in the subclauses below.

14.1.1 Administration Management Domains

An **administration management domain** (**ADMD**) comprises messaging systems managed by a CCITT Administration.

NOTE - An ADMD provides Message Handling to the public.

14.1.2 Private Management Domains

A **private management domain** (**PRMD**) comprises messaging systems managed by an organization other than a CCITT Administration.

NOTE - A PRMD provides Message Handling, e.g., to the employees of a company, or to those employees at a particular company site.

14.2 Representative Configurations

MDs can be combined in various ways to form the MHS. The possible organizational configurations are unbounded in number and thus cannot be enumerated. Several important representative configurations, however, are described below and in Figure 10.

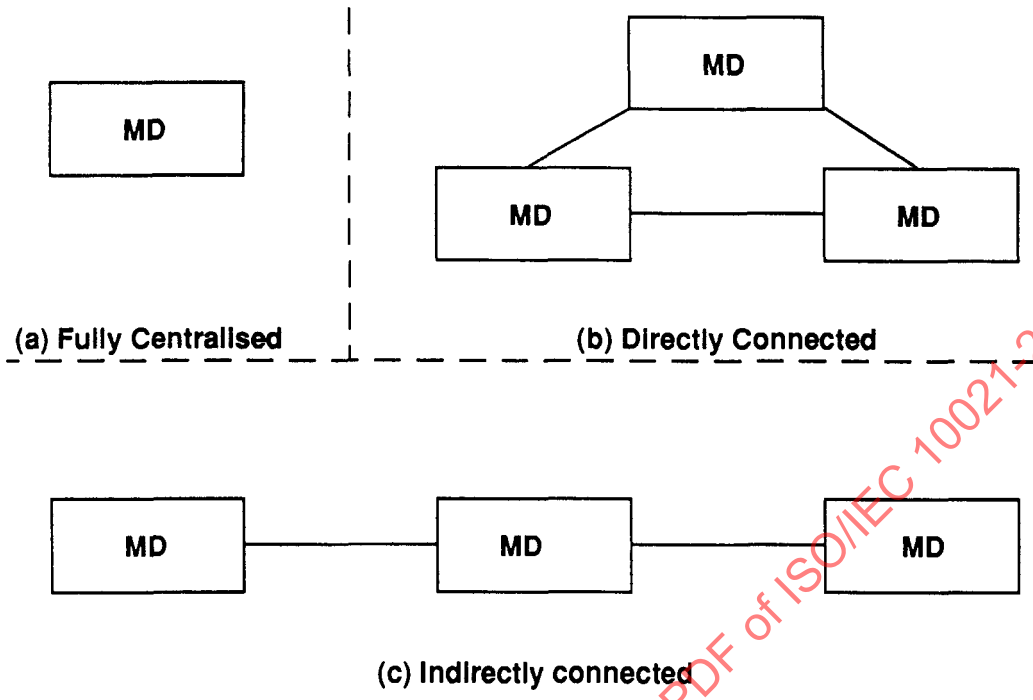

Figure 10
Representative Organizational Configurations

NOTE - Besides the organizational configurations that result from the "pure" approaches below, many "hybrid" configurations can be constructed.

14.2.1 Fully Centralized

The entire MHS may be managed by one organization (panel *a* of the figure). This design is realized by a single MD.

14.2.2 Directly Connected

The MHS may be managed by several organizations, the messaging systems of each connected to the messaging systems of all of the others (panel *b* of the figure). This design is realized by multiple MDs interconnected pair-wise.

14.2.3 Indirectly Connected

The MHS may be managed by several organizations, the messaging systems of one serving as intermediary between the messaging systems of the others (panel c of the figure). This design is realized by multiple MDs one of which is interconnected to all of the others.

15 The Global MHS

A major purpose of ISO/IEC 10021 is to enable the construction of the **Global MHS**, an MHS providing both intra- and inter-organizational, and both intra- and international Message Handling world-wide.

The Global MHS almost certainly encompasses the full variety of functional configurations specified in clause 12.

The physical configuration of the Global MHS is a hybrid of the pure configurations specified in clause 13, extremely complex and highly distributed physically.

The organizational configuration of the Global MHS is a hybrid of the pure configurations specified in clause 14, extremely complex and highly distributed organisationally.

Figure 11 gives an example of possible interconnections. It does not attempt to identify all possible configurations. As depicted, ADMDs play a central role in the Global MHS. By interconnecting to one another internationally, they provide an international Message Transfer backbone. Depending upon national regulations, by interconnecting to one another domestically, they may also provide domestic backbones joined to the international backbone.

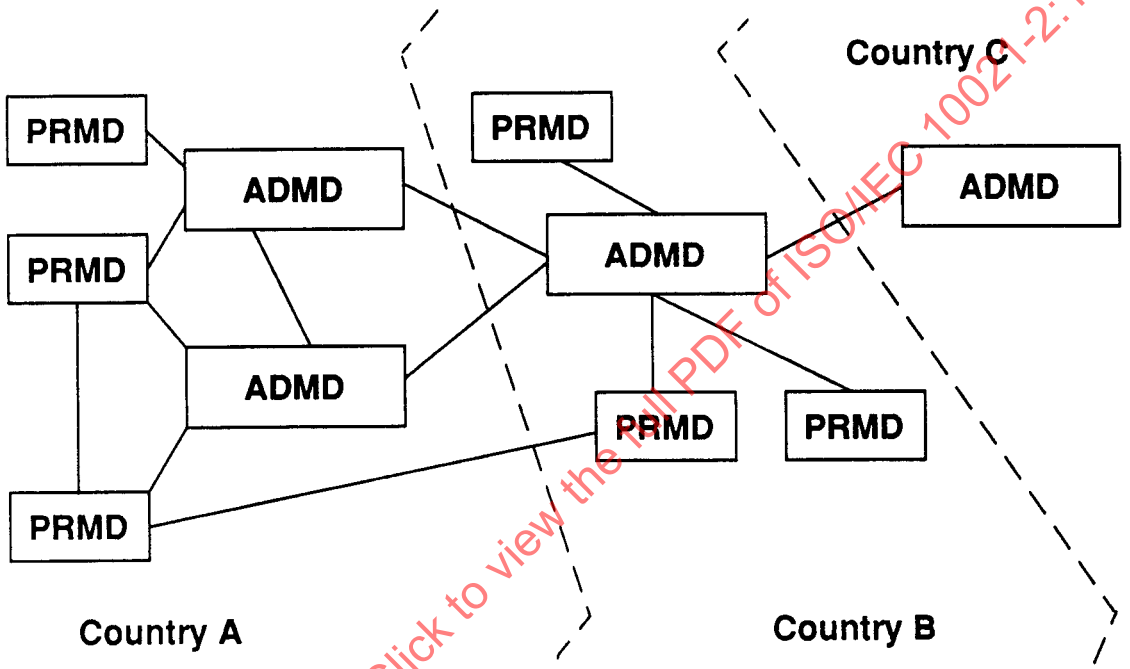

Figure 11
The Global MHS

Section four - Naming, Addressing, and Routing

16 Overview

This section describes the naming and addressing of users and DLs and the routing of information objects to them.

This section covers the following topics:

a) Naming;

b) Addressing;

c) Routing.

17 Naming

This clause specifies how users and DLs are named for the purposes of Message Handling in general and Message Transfer in particular. It defines *O/R names* and describes the role that Directory names play in them.

When it directly submits a message or probe, a UA or MS identifies its potential recipients to the MTS. When the MTS delivers a message, it identifies the originator to each recipient's UA or MS. *O/R names* are the data structures by means of which such identification is achieved.

17.1 Directory Names

A Directory name is one component of an *O/R name*. A Directory name identifies an object to the Directory. By presenting such a name to the Directory, the MHS can access a user's or DL's Directory entry. From that entry the MTS can obtain, e.g., the user's or DL's *O/R address*.

Not every user or DL is registered in the Directory and, therefore, not every user or DL possesses a Directory name.

NOTES

1. Many users and DLs will lack Directory names until the Directory is widely available as an adjunct to the MHS. Many indirect users (e.g., postal patrons) will lack such names until the Directory is widely available as an adjunct to other communication systems.

2. Users and DLs may be assigned Directory names even before a fully interconnected, distributed Directory has been put in place by pre-establishing the naming authorities upon which the Directory will eventually depend.

3. The typical Directory name is more user-friendly and more stable than the typical *O/R address* because the latter is necessarily couched in terms of the organizational or physical structure of the MHS while the former need not be. Therefore, it is intended that over time, Directory names become the primary means by which users and DLs are identified outside the MTS (i.e., by other users), and that the use of *O/R addresses* be largely confined to the MTS (i.e., to use by MTAs).

17.2 O/R Names

Every user or DL has one or more *O/R names*. An **O/R name** is an identifier by means of which a user can be designated as the originator, or a user or DL designated as a potential recipient of a message or probe. An O/R name distinguishes one user or DL from another and may also identify its point of access to the MHS.

An O/R name comprises a Directory name, an *O/R address*, or both. If present, the Directory name (if valid) unambiguously identifies the user or DL (but is not necessarily the only name that would do so). If present, the *O/R address* does the same and more (again see clause 18.5).

At direct submission, the UA or MS of the originator of a message or probe may include either or both components in each O/R name it supplies. If the *O/R address* is omitted, the MTS obtains it from the Directory using the Directory name. If the Directory name is omitted, the MTS does without it. If both are included, the MTS relies firstly upon the *O/R address*. Should it determine that the *O/R address* is invalid (e.g., obsolete), it proceeds as if the *O/R address* had been omitted, relying upon the Directory name.

At delivery the MTS includes an *O/R address* and possibly a Directory name in each O/R name it supplies to a message's recipient or to the originator of a report's subject message or probe. The Directory name is included if the originator supplied it or if it was specified as the member of an expanded DL.

NOTE - Redirection or DL expansion may cause the MTS to convey to a UA or MS at delivery, O/R names the UA or MS did not supply at direct submission.

18 Addressing

This clause specifies how users and DLs are addressed. It defines *O/R addresses*, describes the structure of the *attribute lists* from which they are constructed, discusses the character sets from which individual *attributes* are composed, gives rules for determining that two *attribute lists* are equivalent and for the inclusion of conditional *attributes* in such lists, and defines the *standard attributes* that may appear in them.

To convey a message, probe, or report to a user, or to expand a DL specified as a potential recipient of a message or probe, the MTS must locate the user or DL relative to its own physical and organizational structures. *O/R addresses* are the data structures by means of which all such location is accomplished.

18.1 Attribute Lists

The *O/R addresses* of both users and DLs are attribute lists. An **attribute list** is an ordered set of *attributes*.

An **attribute** is an information item that describes a user or DL and that may also locate it in relation to the physical or organizational structure of the MHS (or the network underlying it).

An attribute has the following parts:

a) **attribute type** (or **type**): An identifier that denotes a class of information (e.g., personal names).

b) **attribute value** (or **value**): An instance of the class of information the attribute type denotes (e.g., a particular personal name).

Attributes are of the following two kinds:

a) **standard attribute**: An attribute whose type is bound to a class of information by this part of ISO/IEC 10021.

The value of every standard attribute except *terminal-type* is either a string or a collection of strings.

b) **domain-defined attribute**: An attribute whose type is bound to a class of information by an MD.

Both the type and value of every domain-defined attribute are strings or collections of strings.

NOTE - The widespread use of standard attributes produces more uniform and thus more user-friendly O/R addresses. However, it is anticipated that not all MDs will be able to employ such attributes immediately. The purpose of domain-defined attributes is to permit an MD to retain its existing, native addressing conventions for a time. It is intended, however, that all MDs migrate toward the use of standard attributes, and that domain-defined attributes be used only for an interim period.

18.2 Character Sets

Standard attribute values and domain-defined attribute types and values are constructed from Numeric, Printable, and Teletex Strings as follows:

a) The type or value of a particular domain-defined attribute may be a Printable String, a Teletex String, or both. The same choice shall be made for both the type and value.

b) The kinds of strings from which standard attribute values may be constructed and the manner of construction (e.g., as one string or several) vary from one attribute to another (see clause 18.3).

The value of an attribute comprises strings of one of the following sets of varieties depending upon its type: Numeric only, Printable only, Numeric and Printable, and Printable and Teletex. With respect to this, the following rules govern each instance of communication:

a) Wherever both Numeric and Printable Strings are permitted, strings of either variety (but not both) may be supplied equivalently.

b) Wherever both Printable and Teletex Strings are permitted, strings of either or both varieties may be supplied, but Printable Strings should be supplied as a minimum whenever attributes are conveyed internationally. If both Printable and Teletex Strings are supplied, the two should convey the same information so that either of them can be safely ignored upon receipt.

NOTES

1. Teletex Strings are permitted in attribute values to allow inclusion, e.g., of the accented characters commonly used in many countries.

2. The downgrading rules in Annex B of ISO/IEC 10021-6 state that an O/R address cannot be downgraded if only the Teletex String has been supplied.

18.3 Standard Attributes

The standard attribute types are listed in the first column of Table 9. For each listed type, the second column indicates the character sets--numeric, printable, and teletex--from which attribute values may be drawn.

The table has three sections. Attribute types in the first are of a general nature, those in the second have to do with *routing to* a PDS, and those in the third have to do with *addressing within* a PDS.

Table 9
Standard Attributes

Standard Attribute Type	Character Sets NUM	PRT	TTX
General			
administration-domain-name	x	x	-
common-name	-	x	x
country-name	x	x	-
network-address	x(*)	-	-
numeric-user-identifier	x	-	-
organization-name	-	x	x
organizational-unit-names	-	x	x
personal-name	-	x	x
private-domain-name	x	x	-
terminal-identifier	-	x	-
terminal-type	-	-	-
Postal Routing			
pds-name	-	x	-
physical-delivery-country-name	x	x	-
postal-code	x	x	-
Postal Addressing			
extension-postal-O/R-address-components	-	x	x
extension-physical-delivery-address-components	-	x	x
local-postal-attributes	-	x	x
physical-delivery-office-name	-	x	x
physical-delivery-office-number	-	x	x
physical-delivery-organization-name	-	x	x
physical-delivery-personal-name	-	x	x
post-office-box-address	-	x	x
poste-restante-address	-	x	x
street-address	-	x	x
unformatted-postal-address	-	x	x
unique-postal-name	-	x	x

Legend
NUM numeric — x permitted
PRT printable — * Under prescribed circumstances
TTX teletex — a Sequence of Octet Strings

The standard attribute types, summarized in the table, are individually defined and described in the subclauses below.

18.3.1 Administration-domain-name

An **administration-domain-name** is a standard attribute that identifies an ADMD relative to the country denoted by a country-name.

The value of an administration-domain-name is a Numeric or Printable String chosen from a set of such strings that is administered for this purpose by the country alluded to above.

The attribute value comprising a single space (" ") shall be reserved for the following purpose. If permitted by the country denoted by the country-name attribute, a single space shall designate any (i.e., all) ADMDs within the country. This affects both the identification of users within the country and the routing of messages, probes, and reports to and among the ADMDs of that country. Regarding the former, it requires that the O/R addresses of users within the country be chosen so as to ensure their unambiguousness, even in the absence of the actual names of the users' ADMDs. Regarding the latter, it permits both PRMDs within, and ADMDs outside of the country, to route messages, probes, and reports to any of the ADMDs within the country, and requires that the ADMDs within the country interconnect themselves in such a way that the messages, probes, and reports are conveyed to their destinations.

18.3.2 Common-name

A **common-name** is a standard attribute that identifies a user or DL relative to the entity denoted by another attribute (e.g., an organization-name).

The value of a common-name is a Printable String, Teletex String, or both. Whether Printable or Teletex, the string is chosen from a set of such strings that is administered for this purpose (and perhaps others) by the entity alluded to above.

NOTE - Among many other possibilities, a common-name might identify an organizational role (e.g., "Director of Marketing").

18.3.3 Country-name

A **country-name** is a standard attribute that identifies a country.

The value of a country-name is a Printable String that gives the character pair assigned to the country by ISO 3166, or a Numeric String that gives one of the numbers assigned to the country by CCITT Recommendation X.121.

18.3.4 Extension-postal-O/R-address-components

An **extension-postal-O/R-address-components** is a standard attribute that provides, in a postal address, additional information necessary to identify the addressee (e.g., an organizational unit).

The value of an extension-postal-O/R-address-components is a Printable String, Teletex String, or both.

18.3.5 Extension-physical-delivery-address-components

An **extension-physical-delivery-address-components** is a standard attribute that specifies, in a postal address, additional information necessary to identify the exact point of delivery (e.g., room and floor numbers in a large building).

The value of an extension-physical-delivery-address-components is a Printable String, Teletex String, or both.

18.3.6 Local-postal-attributes

A **local-postal-attributes** is a standard attribute that identifies the locus of distribution, other than that denoted by a physical-delivery-office-name attribute (e.g., a geographical area), of a user's physical messages.

The value of a local-postal-attributes is a Printable String, Teletex String, or both.

18.3.7 Network-address

A **network-address** is a standard attribute that gives the network address of a terminal.

The value of a network-address is any one of the following:

a) A Numeric String governed by CCITT Recommendation X.121.

b) Two Numeric Strings governed by CCITT Recommendations E.163 and E.164.

c) A PSAP address.

NOTE - Among the strings admitted by CCITT Recommendation X.121 is a Telex number preceded by the Telex escape digit (8).

18.3.8 Numeric-user-identifier

A **numeric-user-identifier** is a standard attribute that numerically identifies a user relative to the MD denoted by a private-domain-name, or an administration-domain-name, or both.

The value of a numeric-user-identifier is a Numeric String chosen from a set of such strings that is administered for this purpose by the MD alluded to above.

18.3.9 Organization-name

An **organization-name** is a standard attribute that identifies an organization. As a national matter, this identification may be either relative to the country denoted by a country-name (so that organization names are unique within the country), or relative to the MD identified by a private-domain-name, or an administration-domain-name, or both.

The value of an organization-name is a Printable String, Teletex String, or both. Whether Printable or Teletex, the string is chosen from a set of such strings that is administered for this purpose (and perhaps others) by the country or MD alluded to above.

NOTE - In countries choosing country-wide unique organization-names, a national registration authority for organization-names is required.

18.3.10 Organizational-unit-names

An **organizational-unit-names** is a standard attribute that identifies one or more units (e.g., divisions or departments) of the organization denoted by an organization-name, each unit but the first being a sub-unit of the units whose names precede it in the attribute.

The value of an organizational-unit-names is an ordered sequence of Printable Strings, an ordered sequence of Teletex Strings, or both. Whether Printable or Teletex, each string is chosen from a set of such strings that is administered for this purpose (and perhaps others) by the organization (or encompassing unit) alluded to above.

18.3.11 Pds-name

A **pds-name** is a standard attribute that identifies a PDS relative to the MD denoted by a private-domain-name, or an administration-domain-name, or both.

The value of a pds-name is a Printable String chosen from a set of such strings that is administered for this purpose by the MD alluded to above.

18.3.12 Personal-name

A **personal-name** is a standard attribute that identifies a person relative to the entity denoted by another attribute (e.g., an organization-name).

The value of a personal-name comprises the following four pieces of information, the first mandatory, the others optional:

a) The person's surname.

b) The person's given name.

c) The initials of all of his names but his surname.

d) His generation (e.g., "Jr").

The above information is supplied as Printable Strings, Teletex Strings, or both.

18.3.13 Physical-delivery-country-name

A **physical-delivery-country-name** is a standard attribute that identifies the country in which a user takes delivery of physical messages.

The value of a physical-delivery-country-name is subject to the same constraints as is the value of a country-name.

18.3.14 Physical-delivery-office-name

A **physical-delivery-office-name** is a standard attribute that identifies the city, village, etc. in which is situated the post office through which a user takes delivery of physical messages.

The value of a physical-delivery-office-name is a Printable String, Teletex String, or both.

18.3.15 Physical-delivery-office-number

A **physical-delivery-office-number** is a standard attribute that distinguishes among several post offices denoted by a single physical-delivery-office-name.

The value of a physical-delivery-office-number is a Printable String, Teletex String, or both.

18.3.16 Physical-delivery-organization-name

A **physical-delivery-organization-name** is a standard attribute that identifies a postal patron's organization.

The value of a physical-delivery-organization-name is a Printable String, Teletex String, or both.

18.3.17 Physical-delivery-personal-name

A **physical-delivery-personal-name** is a standard attribute that identifies a postal patron.

The value of a physical-delivery-personal-name is a Printable String, Teletex String, or both.

18.3.18 Post-office-box-address

A **post-office-box-address** is a standard attribute that specifies the number of the post office box by means of which a user takes delivery of physical messages.

The value of a post-office-box-address is a Printable String, Teletex String, or both chosen from the set of such strings assigned for this purpose by the post office denoted by a physical-delivery-office-name attribute.

18.3.19 Postal-code

A **postal-code** is a standard attribute that specifies the postal code for the geographical area in which a user takes delivery of physical messages.

The value of a postal-code is a Numeric or Printable String chosen from the set of such strings that is maintained and standardized for this purpose by the postal administration of the country identified by a physical-delivery-country-name attribute.

18.3.20 Poste-restante-address

A **poste-restante-address** is a standard attribute that specifies the code that a user gives to a post office in order to collect the physical messages that await delivery to him.

The value of a poste-restante-address is a Printable String, Teletex String, or both chosen from the set of such strings assigned for this purpose by the post office denoted by a physical-delivery-office-name attribute.

18.3.21 Private-domain-name

A **private-domain-name** is a standard attribute that identifies a PRMD. As a national matter, this identification may be either relative to the country denoted by a country-name (so that PRMD names are unique within the country), or relative to the ADMD identified by an administration-domain-name.

The value of a private-domain-name is a Numeric or Printable String chosen from a set of such strings that is administered for this purpose by the country or ADMD alluded to above.

NOTE - In countries choosing country-wide unique PRMD names, a national registration authority for private-domain-names is required.

18.3.22 Street-address

A **street-address** is a standard attribute that specifies the street address (e.g., house number and street name and type (e.g., "Road")) at which a user takes delivery of physical messages.

The value of a street-address is a Printable String, Teletex String, or both.

18.3.23 Terminal-identifier

A **terminal-identifier** is a standard attribute that gives the terminal identifier of a terminal (e.g., a Telex answer back or a Teletex terminal identifier).

The value of a terminal-identifier is a Printable String.

18.3.24 Terminal-type

A **terminal-type** is a standard attribute that gives the type of a terminal.

The value of a terminal-type is any one of the following: *Telex*, *Teletex*, *G3 facsimile*, *G4 facsimile*, *IA5 terminal*, and *Videotex*.

18.3.25 Unformatted-postal-address

An **unformatted-postal-address** is a standard attribute that specifies a user's postal address in free form.

The value of an unformatted-postal-address is a sequence of Printable Strings, each representing a line of text; a single Teletex String, lines being separated as prescribed for such strings; or both.

18.3.26 Unique-postal-name

A **unique-postal-name** is a standard attribute that identifies the point of delivery, other than that denoted by a street-address, post-office-box-address, or poste-restante-address, (e.g., a building or hamlet) of a user's physical messages.

The value of a unique-postal-name is a Printable String, Teletex String, or both.

18.4 Attribute List Equivalence

Several O/R addresses, and thus several attribute lists, may denote the same user or DL. This multiplicity of O/R addresses results in part (but not in full) from the following attribute list equivalence rules:

a) The relative order of standard attributes is insignificant.

b) Where the value of a standard attribute may be a Numeric String or an equivalent Printable String, the choice between them shall be considered insignificant.

NOTE - This rule applies even to the country-name standard attribute, where the choice between X.121 or ISO 3166 forms shall be considered insignificant. Where X.121 allocates more than one number to a country the significance of which number is used has not been standardised by this part of ISO/IEC 10021.

c) Where the value of a standard attribute may be a Printable String, an equivalent Teletex String, or both, the choice between the three possibilities shall be considered insignificant.

d) Where the value of a standard attribute may contain letters, the cases of those letter shall be considered insignificant.

e) In a domain-defined attribute type or value, or in a standard attribute value, all leading, all trailing, and all but one consecutive embedded spaces shall be considered insignificant.

NOTES

1. An MD may impose additional equivalence rules upon the attributes it assigns to its own users and DLs. It might define, e.g., rules concerning punctuation characters in attribute values, the case of letters in such values, or the relative order of domain-defined attributes.

2. As a national matter, MDs may impose additional equivalence rules regarding standard attributes whose values are given as Teletex Strings, in particular, the rules for deriving the equivalent Printable Strings.

18.5 O/R Address Forms

Every user or DL is assigned one or more O/R addresses. An **O/R address** is an attribute list that distinguishes one user from another and identifies the user's point of access to the MHS or the DL's expansion point.

An O/R address may take any of the forms summarized in Table 10. The first column of the table identifies the attributes available for the construction of O/R addresses. For each O/R address form, the second column indicates the attributes that may appear in such O/R addresses and their grades (see also clause 18.6).

The table has four sections. Attribute types in the first are those of a general nature, attribute types in the second and third those specific to physical delivery. The fourth section encompasses domain-defined attributes.

Table 10
Forms of O/R Address

Attribute Type	O/R Address Forms				
	MNEM	NUMR	POST F	POST U	TERM
General					
administration-domain-name	M	M	M	M	C
common-name	C	-	-	-	-
country-name	M	M	M	M	C
network-address	-	-	-	-	M
numeric-user-identifier	-	M	-	-	-
organization-name	C	-	-	-	-
organizational-unit-names	C	-	-	-	-
personal-name	C	-	-	-	-
private-domain-name	C	C	C	C	C
terminal-identifier	-	-	-	-	C
terminal-type	-	-	-	-	C
Postal Routing					
pds-name	-	-	C	C	-
physical-delivery-country-name	-	-	M	M	-
postal-code	-	-	M	M	-
Postal Addressing					
extension-postal -O/R-address-components	-	-	C	-	-
extension-physical-delivery -address-components	-	-	C	-	-
local-postal-attributes	-	-	C	-	-
physical-delivery-office-name	-	-	C	-	-
physical-delivery-office-number	-	-	C	-	-
physical-delivery-organization-name	-	-	C	-	-
physical-delivery-personal-name	-	-	C	-	-
post-office-box-address	-	-	C	-	-
poste-restante-address	-	-	C	-	-
street-address	-	-	C	-	-
unformatted-postal-address	-	-	-	M	-
unique-postal-name	-	-	C	-	-
Domain-defined					
domain-defined (one or more)	C	C	-	-	C

Legend

MNEM mnemonic	F formatted	M mandatory
NUMR numeric	U unformatted	C conditional
POST postal		
TERM terminal		

The forms of O/R address, summarized in the table, are individually defined and described in the subclauses below.

18.5.1 Mnemonic O/R Address

A **mnemonic O/R address** is one that provides a memorable identification for a user or DL. It identifies an MD, and a user or DL relative to it.

A mnemonic O/R address comprises the following attributes:

a) One country-name, one administration-domain-name and conditionally one private-domain-name, which together identify an MD.

b) One organization-name, one organizational-unit-names, one personal-name or common-name, or a combination of the above; and optionally one or more domain-defined attributes; which together identify a user or DL relative to the MD in item *a* above.

18.5.2 Numeric O/R Address

A **numeric O/R address** is one that numerically identifies a user. It identifies an MD, and a user relative to it.

A numeric O/R address comprises the following attributes:

a) One country-name, one administration-domain-name and conditionally one private-domain-name, which together identify an MD.

b) One numeric-user-identifier which identifies the user relative to the MD in item *a* above.

c) Conditionally, one or more domain-defined attributes which provide information additional to that which identifies the user.

18.5.3 Postal O/R Address

A **postal O/R address** is one that identifies a user by means of its postal address. It identifies the PDS through which the user is to be accessed and gives the user's postal address.

The following kinds of postal O/R address are distinguished:

a) **formatted**: Said of a postal O/R address that specifies a user's postal address by means of several attributes. For this form of postal O/R address, this part of ISO/IEC 10021 prescribes the structure of postal addresses in some detail.

b) **unformatted**: Said of a postal O/R address that specifies a user's postal address in a single attribute. For this form of postal O/R address, this part of ISO/IEC 10021 largely does not prescribe the structure of postal addresses.

A postal O/R address, whether formatted or unformatted, comprises the following attributes:

a) One country-name, one administration-domain-name and conditionally one private-domain-name, which together identify an MD.

b) Conditionally, one pds-name which identifies the PDS by means of which the user is to be accessed.

c) One physical-delivery-country-name and one postal-code, which together identify the geographical region in which the user takes delivery of physical messages.

A formatted postal O/R address comprises, additionally, one of each postal addressing attribute (see Table 9), except unformatted-postal-address, that the PDS requires to identify the postal patron.

An unformatted postal O/R address comprises, additionally, one unformatted-postal-address attribute.

NOTE - The total number of characters in the values of all attributes but country-name, administration-domain-name, and pds-name in a postal O/R address should be small enough to permit their rendition in 6 lines of 30 characters, the size of a typical physical envelope window. The rendition algorithm is PDAU-specific but is likely to include inserting delimiters (e.g., spaces) between some attribute values.

18.5.4 Terminal O/R Address

A **terminal O/R address** is one that identifies a user by means of the network address and, if required, the type of his terminal. It may also identify the MD through which that terminal is accessed. In the case of a Telematic terminal, it gives the terminal's network address and possibly its terminal identifier and terminal type. In the case of a Telex terminal, it gives its Telex number.

A terminal O/R address comprises the following attributes:

a) One network-address.

b) Conditionally, one terminal-identifier.

c) Conditionally, one terminal-type.

d) Conditionally, both one country-name and one administration-domain-name and conditionally one private-domain-name which together identify an MD.

e) Conditionally, one or more domain-defined attributes, all of which provide information additional to that which identifies the user.

The private-domain-name and the domain-defined attributes shall be present only if the country-name and administration-domain-name attributes are present.

18.6 Conditional Attributes

The presence or absence in a particular O/R address of the attributes marked conditional in Table 10 is determined as follows.

All conditional attributes except those specific to postal O/R addresses are present in an O/R address at the discretion of, and in accordance with rules established by, the MD denoted by the country-name, administration-domain-name and private-domain-name attributes.

All conditional attributes specific to postal O/R addresses are present or absent in such O/R addresses so as to satisfy the postal addressing requirements of the users they identify.

19 Routing

To convey a message, probe, or report toward a user or the expansion point of a DL, an MTA must not only locate the user or DL (i.e., obtain its O/R address) but also select a route to that location. Routing is thus the process of selecting, given an O/R address, the MTA to which the message, probe or report should be transferred.

This clause is tutorial in nature: it is envisaged that a future Addendum to this International Standard will be developed standardising the mechanisms for dissemination of and use of the information required for routing decisions.

Where no other considerations apply, the optimal routing is to transfer the message as directly as possible to the MTA to which the recipient's UA is connected. However, there may be factors making a more indirect route appropriate such as: less direct routes utilising higher bandwidth links between MTAs; using late fan-out to give optimisation of transmission costs; and needing to access an intermediate MTA for a service such as conversion. The costs of disseminating and storing routing information possibly combined with the undesirability for some domains of disclosing internal structure means that frequently routing directly to the ultimate MTA will not be possible, even when desirable.

The first part of the routing decision that an MTA must make is whether this recipient is in its own MD. To do this, the MTA must know all the combinations of country-name, administration-domain-name and private-domain-name attributes which identify its own domain. A PRMD may have as many combinations of these as there are entry points from ADMDs to that PRMD, although for PRMDs existing entirely within countries adopting nationally unique private-domain-names a single pair of values of country-name and private-domain-name attributes will be sufficient to identify that PRMD internally regardless of whether or not semantic absence of the administration-domain-name is permitted at entry points from ADMDs.

If the recipient is identified as within the same MD the values of other attributes of the recipient's O/R address are examined to determine whether the recipient is a UA served by that MTA, in which case local delivery will occur, or whether an appropriate MTA within the MD can be identified to which the message can be relayed. Failing either of these, a non-delivery event must occur.

Not all MTAs within an MD necessarily need be configured with the capability to relay to or receive from other MDs, but there must be at least one MTA within the MD with such capabilities if the MD is

not to remain isolated from all other MDs. Every MTA within a (non-isolated) MD must be capable of routing to an MTA within that MD which can relay to other MDs, if not possessing this capability itself. So, even if the recipient is identified as being outside the MD, relaying to another MTA within the MD may still be necessary.

If the external MD is identified as one to which a direct connection exists, then this direct connection will often be used. The external MD may also be identified as one reached by relaying through one or more intermediate MD. If these intermediate MDs are PRMDs then this option can only be exercised by bilateral agreement. Alternatively, the external MD may be unknown and then the services of an ADMD will be required.

The role of an ADMD within the MHS is to provide, directly or indirectly, relaying to all other ADMDs, and to relay messages to all PRMDs directly connected to that ADMD. Thus a PRMD always has the option of choosing to use the services of an ADMD for routing to other PRMDs.

When more than one entry point to an external MD can be identified, additional O/R address attributes or other considerations may be used to determine the most appropriate entry point. In the extreme case of the originating MD having complete information about the recipient's MD this would allow direct communication between originator's MTA and recipient's MTA.

Section five - Use of the Directory

20 Overview

This section describes the uses to which the MHS may put the Directory if it is present. If the Directory is unavailable to the MHS, how, if at all, the MHS performs these same tasks is a local matter.

This section covers the following topics:

a) Authentication;

b) Name resolution;

c) DL expansion;

d) Capability assessment.

21 Authentication

A functional object may accomplish authentication using information stored in the Directory.

22 Name Resolution

A functional object may accomplish name resolution using the Directory.

To obtain the O/R address(es) of a user or DL whose Directory name it possesses, an object presents that name to the Directory and requests from the Directory entry the following attributes:

a) *MHS O/R Addresses.*

b) *MHS Preferred Delivery Methods.*

To do this successfully, the object must first authenticate itself to the Directory and have access rights to the information requested.

23 DL Expansion

A functional object may accomplish DL expansion using the Directory, first verifying that the necessary submit permissions exist.

To obtain the members of a DL whose Directory name it possesses, the object presents that name to the Directory and requests from the Directory entry the following attributes:

a) *MHS DL Members.*

b) *MHS DL Submit Permissions.*

c) *MHS Preferred Delivery Methods.*

To do this successfully, the MTA must first authenticate itself to the Directory and have access rights to the information requested.

24 Capability Assessment

A functional object may assess the capabilities of a user or MS using the Directory.

The following Directory attributes represent user capabilities of possible significance in Message Handling:

a) *MHS Deliverable Content Length.*

b) *MHS Deliverable Content Types.*

c) *MHS Deliverable EITs.*

d) *MHS Preferred Delivery Methods.*

The following Directory attributes represent MS capabilities of possible significance in Message Handling:

a) *MHS Supported Automatic Actions.*

b) *MHS Supported Content Types.*

c) *MHS Supported Optional Attributes.*

To assess a particular capability of a user or MS whose Directory name it possesses, the object presents that name to the Directory and requests from the Directory entry the attribute associated with that capability.

To do this successfully, the MTA must first authenticate itself to the Directory and have access rights to the information requested.

Section six - OSI Realization

25 Overview

This section describes how the MHS is realized by means of OSI.

This section covers the following topics:

a) Application service elements;

b) Application contexts.

26 Application Service Elements

This clause identifies the application service elements (ASEs) that figure in the OSI realization of Message Handling.

In OSI the communication capabilities of open systems are organized into groups of related capabilities called ASEs. The present clause reviews this concept from the OSI Reference Model, draws a distinction between *symmetric* and *asymmetric* ASEs, and introduces the ASEs defined for or supportive of Message Handling.

NOTE - Besides the ASEs discussed, the MHS relies upon the Directory Access Service Element defined in ISO/IEC 9594-6. However, since that ASE does not figure in the *ACs* for Message Handling (see ISO/IEC 10021-6), it is not discussed here.

26.1 The ASE Concept

The ASE concept is illustrated in Figure 12, which depicts two communicating open systems. Only the OSI-related portions of the open systems, called AEs, are shown. Each AE comprises a UE and one or more ASEs. A UE represents the controlling or organizing portion of an AE which defines the open system's role (e.g., that of an MTA). An ASE represents one of the communication capability sets, or services (e.g., for message submission or transfer), that the UE requires to play its role.

The relationship between two AEs in different open systems is called an application association. The ASEs in each open system communicate with their peer ASEs in the other open system via a presentation connection between them. That communication is what creates and sustains the relationship embodied in the application association. For several ASEs to be successfully combined in a single AE, they must be designed to coordinate their use of the application association.

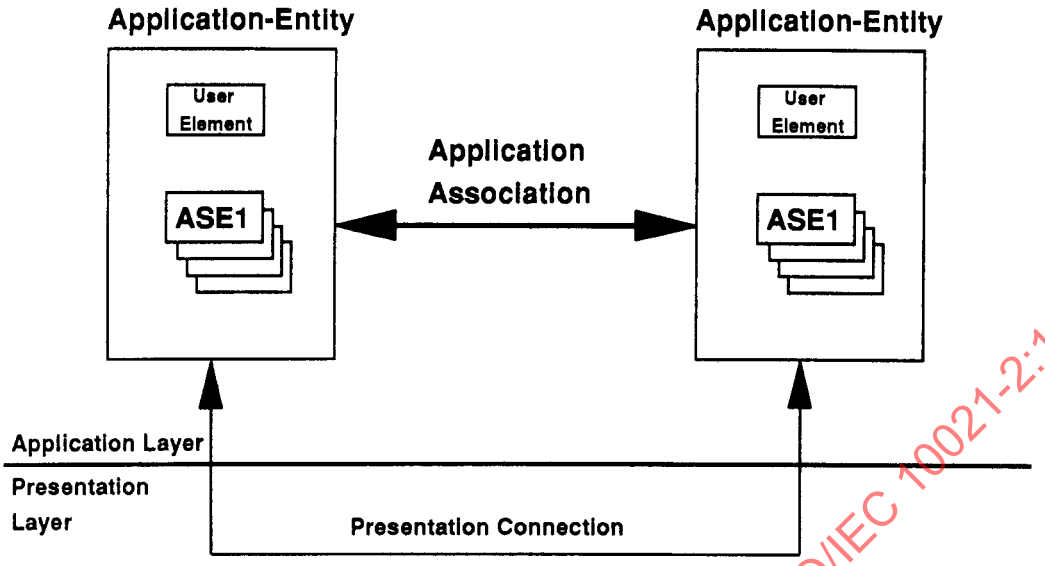

Figure 12
The ASE Concept

An ASE plays the largely mechanical role of translating requests and responses made by its UE to and from the form dictated by the application protocol that governs the ASE's interaction with its peer ASE in the open system to which the association connects it. The ASE realizes an abstract service, or a part thereof, for purposes of OSI communication (see ISO/IEC 10021-3).

NOTE - Strictly speaking, an open system's role is determined by the behaviour of its application processes. In the Message Handling context an application process realizes a functional object of one of the types defined in clause 7. A UE in turn is one part of an application process.

26.2 Symmetric and Asymmetric ASEs

The following two kinds of ASE, illustrated in Figure 13, can be distinguished:

a) **symmetric**: Said of an ASE by means of which a UE both supplies and consumes a service. The ASE for message transfer, e.g., is symmetric because both open systems, each of which embodies an MTA, offer and may consume the service of message transfer by means of it.

b) **asymmetric**: Said of an ASE by means of which a UE supplies or consumes a service, but not both, depending upon how the ASE is configured. The ASE for message delivery, e.g., is asymmetric because only the open system embodying an MTA offers the associated service and only the other open system, which embodies a UA or MS, consumes it.

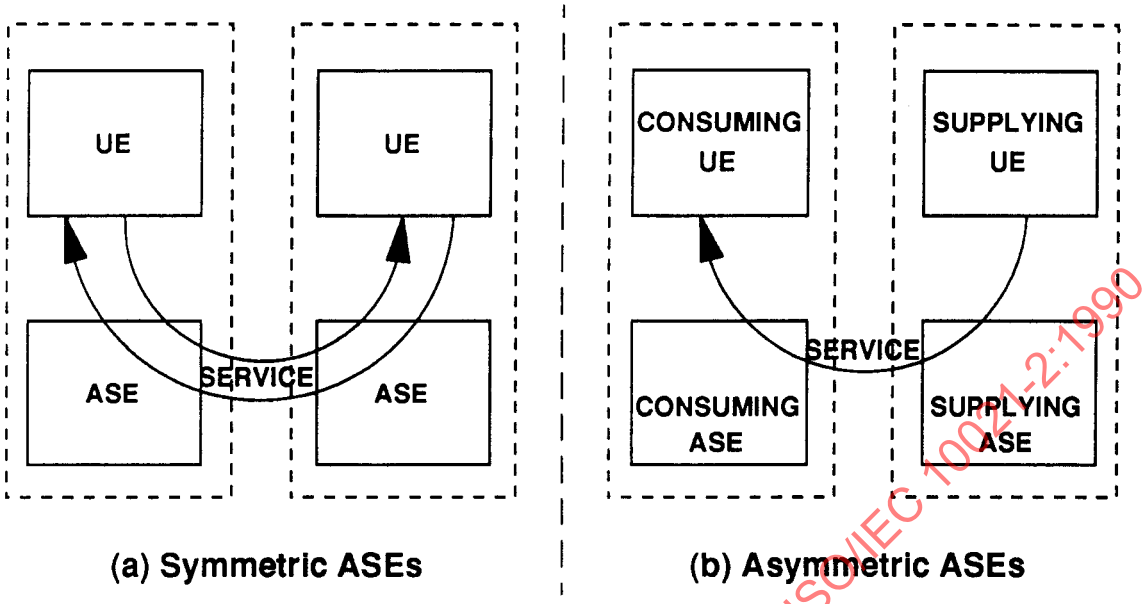

Figure 13
Symmetric and Asymmetric ASEs

With respect to a particular asymmetric ASE, one UE supplies a service which the other consumes. The ASEs co-located with the UEs assist in the service's supply and consumption. The resulting four roles are captured in Figure 14 and in the following terminology:

a) *x*-**supplying UE**: An application process that supplies the service represented by asymmetric ASE *x*.

b) *x*-**supplying ASE**: An asymmetric ASE *x* configured for co-location with an *x*-supplying-UE.

c) *x*-**consuming UE**: An application process that consumes the service represented by asymmetric ASE *x*.

d) *x*-**consuming ASE**: An asymmetric ASE *x* configured for co-location with an *x*-consuming-UE.

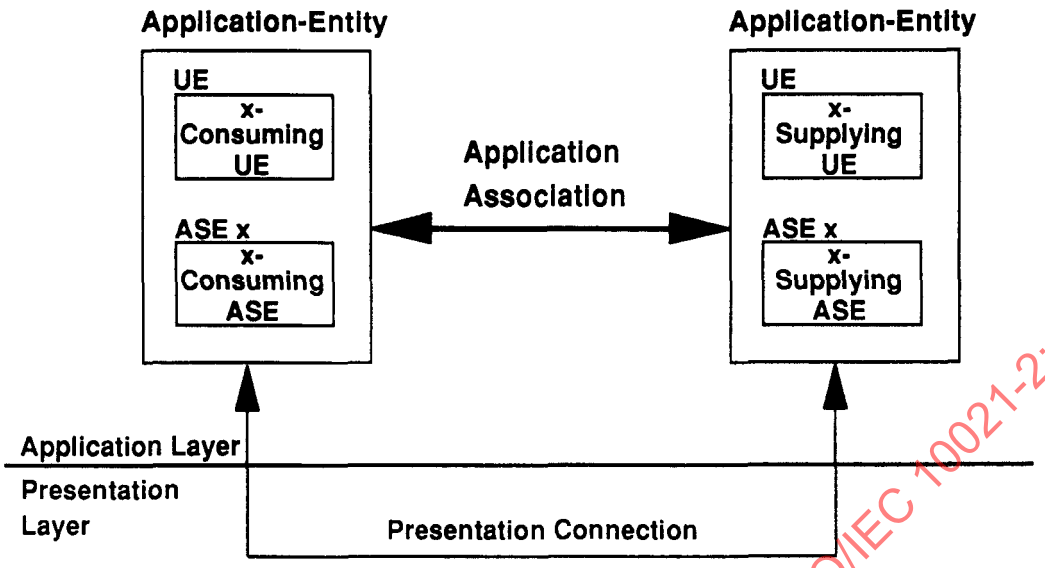

Figure 14
Terminology for Asymmetric ASEs

As indicated, the four roles described above are defined relative to a particular ASE. When an AE comprises several asymmetric ASEs, these roles are assigned independently for each ASE. Thus, as shown in Figure 15, a single UE might serve as the consumer with respect to one ASE and as the supplier with respect to another.

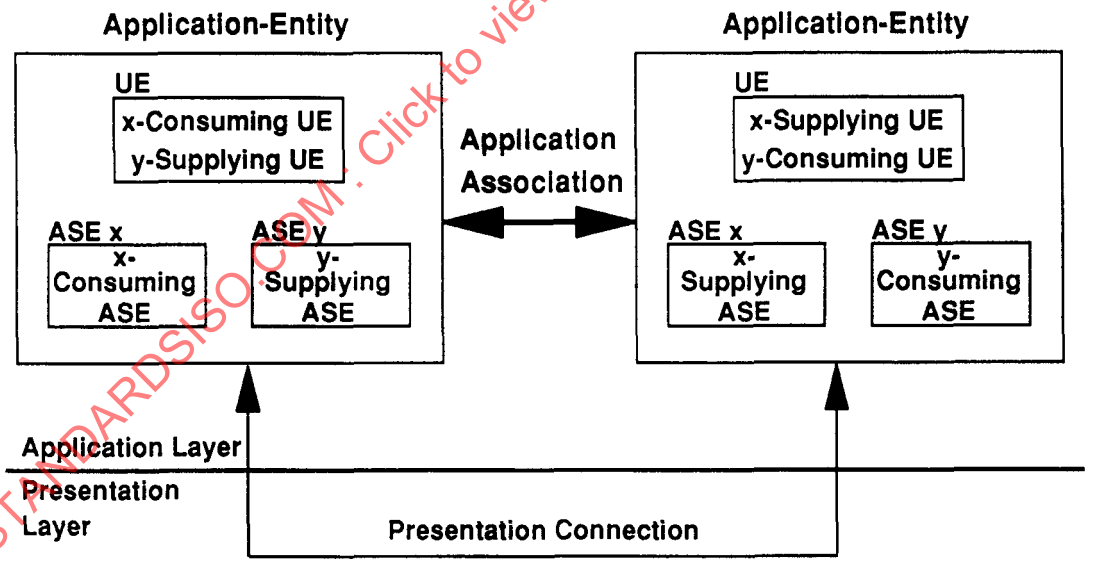

Figure 15
Multiple Asymmetric ASEs

26.3 Message Handling ASEs

The ASEs that provide the various Message Handling services are listed in the first column of Table 11. For each ASE listed, the second column indicates whether it is symmetric or asymmetric. The third column identifies the functional objects--UAs, MSs, MTAs, and AUs--that are associated with the ASE, either as consumer or as supplier.

Table 11
Message Handling ASEs

ASE	Form	Functional Objects UA	MS	MTA	AU
MTSE	SY	-	-	CS	-
MSSE	ASY	C	CS	S	-
MDSE	ASY	C	C	S	-
MRSE	ASY	C	S	-	-
MASE	ASY	C	CS	S	-

Legend
SY symmetric C consumer
ASY asymmetric S supplier

The Message Handling ASEs, summarized in the table, are individually introduced in the subclauses below. Each is defined in ISO/IEC 10021-6.

26.3.1 Message Transfer

The Message Transfer Service Element (MTSE) is the means by which the transfer transmittal step is effected.

26.3.2 Message Submission

The Message Submission Service Element (MSSE) is the means by which the submission transmittal step is effected.

26.3.3 Message Delivery

The Message Delivery Service Element (MDSE) is the means by which the delivery transmittal step is effected.

26.3.4 Message Retrieval

The Message Retrieval Service Element (MRSE) is the means by which the retrieval transmittal step is effected.

26.3.5 Message Administration

The Message Administration Service Element (MASE) is the means by which a UA, MS, or MTA places on file with one another information that enables and controls their subsequent interaction by means of the MSSE, MDSE, MRSE, and MASE.

26.4 Supporting ASEs

The general-purpose ASEs upon which Message Handling ASEs depend are listed in the first column of Table 12. For each listed ASE, the second column indicates whether it is symmetric or asymmetric.

Table 12
Supporting ASEs

ASE	Form
ROSE	SY
RTSE	SY
ACSE	SY

Legend
SY symmetric
ASY asymmetric

The supporting ASEs, summarized in the table, are individually introduced in the subclauses below.

26.4.1 Remote Operations

The Remote Operations Service Element (ROSE) is the means by which the asymmetric Message Handling ASEs structure their request-response interactions between consuming and supplying open systems.

The ROSE is defined in ISO/IEC 9072-1.

26.4.2 Reliable Transfer

The Reliable Transfer Service Element (RTSE) is the means by which various symmetric and asymmetric Message Handling ASEs convey information objects--especially large ones (e.g., facsimile messages)--between open systems so as to ensure their safe-storage at their destinations.

The RTSE is defined in ISO/IEC 9066-1.

26.4.3 Association Control

The Association Control Service Element (ACSE) is the means by which all application associations between open systems are established, released, and in other respects managed.

The ACSE is defined in ISO 8649.

27 Application Contexts

In OSI the communication capabilities (i.e., ASEs) of two open systems are marshalled for a particular purpose by means of application contexts (ACs). An AC is a detailed specification of the use of an association between two open systems, i.e., a protocol.

An AC specifies how the association is to be established (e.g., what initialization parameters are to be exchanged), what ASEs are to engage in peer-to-peer communication over the association, what constraints (if any) are to be imposed upon their individual use of the association, whether the initiator or responder is the consumer of each asymmetric ASE, and how the association is to be released (e.g., what finalization parameters are to be exchanged).

Every AC is named (by an ASN.1 Object Identifier). The initiator of an association indicates to the responder the AC that will govern the association's use by conveying the AC's name to it by means of the ACSE.

An AC also identifies by name (an ASN.1 Object Identifier) the abstract syntaxes of the APDUs that an association may carry as a result of its use by the AC's ASEs. Conventionally one assigns a name to the set of APDUs associated either with each individual ASE or with the AC as a whole. The initiator of an

association indicates to the responder the one or more abstract syntaxes associated with the AC by conveying their names to it via the ACSE.

The abstract syntax of an APDU is its structure as an information object (e.g., an ASN.1 Set comprising an Integer command code and an IA5 String command argument). It is distinguished from the APDU's transfer syntax which is how the information object is represented for transmission between two open systems (e.g., one octet denoting an ASN.1 Set, followed by one octet giving the length of the Set, etc.).

The ACs by means of which the various Message Handling services are provided are specified in ISO/IEC 10021-6. These protocols are known as P1, P3, and P7.

NOTE - The nature of a message's content does not enter into the definition of Message Handling ACs because the content is encapsulated (as an Octet String) in the protocols by means of which it is conveyed.

Annex A

(normative)

Directory Object Classes and Attributes

Several Directory object classes, attributes, and attribute syntaxes are specific to Message Handling. These are defined in the present annex using the OBJECT-CLASS, ATTRIBUTE, and ATTRIBUTE-SYNTAX macros of ISO/IEC 9594-2, respectively.

A.1 Object Classes

The object classes specific to Message Handling are those specified below.

NOTE - The Directory object classes described in this annex can be combined with other object classes, e.g., the ones defined in ISO/IEC 9594-7. See also ISO/IEC 9594-2, clause 9 for an explanation of how Directory object classes can be combined in one Directory entry. Annex B of ISO/IEC 9594-7 gives some further information about Directory name forms and possible Directory Information Tree structures.

A.1.1 MHS Distribution List

An **MHS Distribution List** object is a DL. The attributes in its entry identify its common name, submit permissions, and O/R addresses and, to the extent that the relevant attributes are present, describe the DL, identify its organization, organizational units, and owner; cite related objects; and identify its deliverable content types, deliverable EITs, members, and preferred delivery methods.

```
mhs-distribution-list OBJECT-CLASS
        SUBCLASS OF top
        MUST CONTAIN {
                commonName,
                mhs-dl-submit-permissions,
                mhs-or-addresses}
        MAY CONTAIN {
                description,
                organization,
                organizationalUnitName,
                owner,
                seeAlso,
                mhs-deliverable-content-types,
                mhs-deliverable-eits,
                mhs-dl-members,
                mhs-preferred-delivery-methods}
        ::= id-oc-mhs-distribution-list
```

A.1.2 MHS Message Store

An **MHS Message Store** object is an AE that realizes an MS. The attributes in its entry, to the extent that they are present, describe the MS, identify its owner, and enumerate the optional attributes, automatic actions, and content types it supports.

```
mhs-message-store OBJECT-CLASS
        SUBCLASS OF applicationEntity
        MAY CONTAIN {
                description,
                owner,
                mhs-supported-optional-attributes,
                mhs-supported-automatic-actions,
                mhs-supported-content-types}
        ::= id-oc-mhs-message-store
```

A.1.3 MHS Message Transfer Agent

An **MHS Message Transfer Agent** object is an AE that implements an MTA. The attributes in its entry, to the extent that they are present, describe the MTA and identify its owner and its deliverable content length.

```
mhs-message-transfer-agent OBJECT-CLASS
        SUBCLASS OF applicationEntity
        MAY CONTAIN {
                description,
                owner,
                mhs-deliverable-content-length}
        ::= id-oc-mhs-message-transfer-agent
```

A.1.4 MHS User

An **MHS User** object is a generic MHS user. (The generic MHS user can have, for example, a business address, a residential address, or both.) The attributes in its entry identify the user's O/R address and, to the extent that the relevant attributes are present, identify the user's deliverable content length, content types, and EITs; its MS; and its preferred delivery methods.

```
mhs-user OBJECT-CLASS
        SUBCLASS OF top
        MUST CONTAIN {
                mhs-or-addresses}
        MAY CONTAIN {
                mhs-deliverable-content-length,
                mhs-deliverable-content-types,
                mhs-deliverable-eits,
                mhs-message-store,
                mhs-preferred-delivery-methods}
        ::= id-oc-mhs-user
```

A.1.5 MHS User Agent

An **MHS User Agent** object is an AE that realizes a UA. The attributes in its entry, to the extent that they are present, identify the UA's owner; its deliverable content length, content types, and EITs; and its O/R address.

```
mhs-user-agent OBJECT-CLASS
        SUBCLASS OF applicationEntity
        MAY CONTAIN {
                owner,
                mhs-deliverable-content-length,
                mhs-deliverable-content-types,
                mhs-deliverable-eits,
                mhs-or-addresses}
        ::= id-oc-mhs-user-agent
```

A.2 Attributes

The attributes specific to Message Handling are those specified below.

A.2.1 MHS Deliverable Content Length

The **MHS Deliverable Content Length** attribute identifies the maximum content length of the messages whose delivery a user will accept.

A value of this attribute is an Integer.

```
mhs-deliverable-content-length ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX integerSyntax
        SINGLE VALUE
        ::= id-at-mhs-deliverable-content-length
```

A.2.2 MHS Deliverable Content Types

The **MHS Deliverable Content Types** attribute identifies the content types of the messages whose delivery a user will accept.

A value of this attribute is an Object Identifier.

```
mhs-deliverable-content-types ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
        MULTI VALUE
        ::= id-at-mhs-deliverable-content-types
```

A.2.3 MHS Deliverable EITs

The **MHS Deliverable EITs** attribute identifies the EITs of the messages whose delivery a user will accept.

A value of this attribute is an Object Identifier.

```
mhs-deliverable-eits ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX objectIdentifierSyntax
        MULTI VALUE
        ::= id-at-mhs-deliverable-eits
```

A.2.4 MHS DL Members

The **MHS DL Members** attribute identifies a DL's members.

A value of this attribute is an O/R name.

```
mhs-dl-members ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX mhs-or-name-syntax
        MULTI VALUE
        ::= id-at-mhs-dl-members
```

A.2.5 MHS DL Submit Permissions

The **MHS DL Submit Permissions** attribute identifies the users and DLs that may submit messages to a DL.

A value of this attribute is a DL submit permission.

```
mhs-dl-submit-permissions ATTRIBUTE
        WITH ATTRIBUTE-SYNTAX mhs-dl-submit-permission-syntax
        MULTI VALUE
        ::= id-at-mhs-dl-submit-permissions
```