NBSIR 88-3824

Ongoing Implementation Agreements for Open Systems Interconnection Protocols Volume 2: Continuing Agreements

Based on the Proceedings of the
NBS/OSI Implementor's Workshop
Plenary Assembly Held May 6, 1988
National Bureau of Standards
Gaithersburg, MD 20899

Robert Rosenthal, Editor

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Institute for Computer Sciences and Technology
Gaithersburg, MD 20899

July 1988

RTMENT OF COMMERCE
UREAU OF STANDARDS

NBSIR 88-3824

ONGOING IMPLEMENTATION AGREEMENTS FOR OPEN SYSTEMS INTERCONNECTION PROTOCOLS VOLUME 2: CONTINUING AGREEMENTS

Based on the Proceedings of the
NBS/OSI Implementor's Workshop
Plenary Assembly Held May 6, 1988
National Bureau of Standards
Gaithersburg, MD 20899

Robert Rosenthal, Editor

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Institute for Computer Sciences and Technology
Gaithersburg, MD 20899

July 1988

U.S. DEPARTMENT OF COMMERCE, C. William Verity, *Secretary*
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Director*

Table of Contents

List of Figures

List of Tables

1. GENERAL INFORMATION

1.1 PURPOSE OF THIS DOCUMENT

This document records ongoing implementation specification agreements of OSI protocols among the organizations participating in the NBS/OSI Workshop Series for Implementors of OSI Protocols. This work is not considered advanced enough for use in product development or procurement reference.

The companion document, "Stable Implementation Agreements for Open Systems Interconnection Protocols," records mature agreements considered advanced enough for use in product development or procurement reference.

As each protocol specification is completed, it is moved from this ongoing document to the stable companion document.

1.2 PURPOSE OF THE WORKSHOP

At the request of industry, the National Bureau of Standards organized the NBS Workshop for Implementors of OSI to bring together future users and potential suppliers of OSI protocols. The Workshop accepts as input the specifications of emerging standards for protocols and produces as output agreements on the implementation and testing particulars of these protocols. This process is expected to expedite the development of OSI protocols and promote interoperability of independently manufactured data communications equipment.

1.3 USE AND ENDORSEMENT BY OTHER ENTERPRISES

The Workshops are held for those organizations expressing an interest in implementing or procuring OSI protocols and open systems. However, there is no corporate commitment to implementations associated with workshop participation.

The agreements contained in earlier versions of this document were used for OSI demonstrations at the National Computer Conference in 1984 and at the AUTOFACT conference in 1985.

The agreements from several versions of this document have been adopted for use in implementations running on OSINET.

The MAP/TOP Steering Committee has endorsed these agreements and will "continue the use of the most current, applicable Implementors Workshop Agreements in all releases of the MAP and TOP specifications."

The COS Strategy Forum has "adopted a resolution stating that as a matter of policy COS should select as its sources of Implementation

Agreements organizations or forums that are: (1) Broadly open, widely recognized OSI workshops (NBS/OSI Workshops are first preference) ..."

The U.S. Government OSI User's Committee is using the implementation specifications from the "Stable Implementation Agreements for Open System Interconnection Protocols" in its Federal procurement specification, "Government OSI Profile (GOSIP)."

1.4 RELATIONSHIP OF THE WORKSHOP TO THE NBS LABORATORIES

As resources permit, NBS, with voluntary assistance from industry, develops formal protocol specifications, reference implementations, tests and test systems for the protocols agreed to in the workshops. This is work made available to the industry volunteers and to others making valid commitments to organized events and activities such as NCC, AUTOFACT, and OSINET. As soon as this work can be adequately documented, it is placed in the public domain through submission to the National Technical Information Service. Any organization may then obtain the work at nominal charge.

The NBS laboratories bear no other relationship to the workshop.

1.5 STRUCTURE AND OPERATION OF THE WORKSHOP

1.5.1 Plenary

The main body of the workshop is a plenary assembly. Any organization may participate. Representation is international. NBS prefers for the business of workshops to be conducted informally, since there are no corresponding formal commitments within the workshop by participants to implement the decisions reached. The guidelines we follow are: 1) one vote per company or independent division, 2) only companies that regularly attend should vote, 3) only companies that plan to sell or buy a protocol should vote on its implementation decisions, 4) only companies knowledgeable of the issues should vote, and 5) no proxy votes are admissible.

1.5.2 Special Interest Groups

Within the workshop there are Special Interest Groups (SIGs). The SIGs receive their instructions for their technical program of work from the plenary. The SIGs meet independently, usually during the workshop. As technical work is completed by a SIG, it is presented to the plenary for disposition. Companies participating in a SIG are expected to participate in the plenary. Voting rules for SIGS are the same as voting rules for the plenary.

Special Interest Groups sometimes correspond with organizations performing related work, such as ANSI committees. Such

correspondence should be sent through the plenary to the parent committee, such as ANSC X3T5 or ANSC X3S3. When SIG meetings take place between workshops, the correspondence from these meetings should be addressed directly to the parent committee and copied to the workshop plenary.

Following are procedures for cooperative work among Special Interest Groups.

- Any SIG (SIG 1) or individual having issues to discuss with or requirements of another SIG (SIG 2) should bring the matter to the attention of the chairperson of that SIG (SIG 2).

- The SIG 2 chairperson should bring the matter before SIG 2 for action.

- SIG 2 should respond to the concerns or needs of SIG 1 or the individual in a timely manner.

- If the matter cannot be satisfactorily resolved or if the request is outside the charter assigned to SIG 1, then it should be brought before the plenary.
- SIGs are expected to complete work in a timely manner and bring the results before the plenary for disposition. However, the plenary may elect to act on any issue within the scope of the workshop at any time.

Following are the charters of the ten Special Interest Groups.

FTAM SIG

Scope

- to develop stable FTAM Agreements between vendors and users for the implementation of interoperable products

- in particular to develop the FTAM Phase 2 product-level specifications and maintain these specifications with respect to experiences from implementations and from testing

- to define further FTAM functionality in the Phase 3 specifications. These will contain only extensions of FTAM Phase 2. It is a goal that Phase 3 will be backward compatible with FTAM Phase 2. The set of future work items listed below may be changed by the plenary if the work is more appropriate for other SIGs.

- to liaise with and contribute to other bodies working on FTAM harmonization such as CEN/CENELEC, POSI, and the ISO activities to define Functional Standards

and

to liaise with vendor/user groups such as COS, MAP, TOP, and SPAG

High priority work items:

- Complete and maintain FTAM Phase 2 Agreements
- Specify implementation of Error Recovery control procedures, specifically
- Error Recovery and Restart Data Transfer functional units
- Specify Concurrency Control parameter.
- Specify implementation of Character Set ISO 6937
- Specify requirements of FTAM to a Directory Service
- Specify use of Presentation Context Management functional unit.

Low priority work items:

- Add new Document Types/Constraint Sets
- Define use of Access Control
- Specify FADU Locking functional unit
- Specify File Store management (e.g., file directories)
- Specify File Name conventions
- Specify use of Overlapped Access

X.400 SIG

Develop product-level specifications for Message Handling Systems using the CCITT X.400 Recommendations.

Develop abstract tests for X.400, as requested by the ad hoc rapporteur for this study question in CCITT. This work is to be submitted by the plenary (after its approval) to the U.S. Department of State as a proposed U.S. contribution to CCITT Study Group VII.

Lower Layer SIG

The Lower Layer SIG will study OSI layers 1-4 and produce recommendations for implementations to support the projects undertaken by the workshop and the work of the other SIGs. Both connectionless and connection-oriented modes of operation will be studied. The SIG will accept direction from the plenary for work undertaken and the priority which it is assigned.

The objectives of the Lower Layer SIG are:

- Study OSI layers 1-4 as directed by the plenary,
- Produce and maintain recommendations for implementation of these layers,
- Where necessary, provide input to the relevant standards bodies concerning layers 1-4, in the proper manner, and
- Begin work on the implementation specification of the ISO Network Layer Routing Exchange Protocol prior to the ISO draft achieving DIS status.

The Lower Layer SIG will study both existing and emerging ISDN standards pertaining to user access and user services. The SIG will:

- Develop implementation agreements for user-network interfaces
- Develop conformance requirements
- Liaise with other standards/interest groups

OSI Security Architecture SIG

GOAL: To develop an overall OSI Security Architecture which is consistent with the OSI reference model and which economically satisfies the primary security needs of both the commercial and Government sectors.

APPROACH: To define a security architecture encompassing the security addenda presently being specified at certain OSI layers, the required cryptographic algorithms and related key management functions, and the security management functions which must be performed between the layers and the peer entities defined in the OSI architecture.

Directory Services SIG

Produce functional implementation agreements based on ISO/CCITT specifications for Directory Services in accordance with the objectives and goals of the plenary.

- Provide a subset for NBS publication which is functional and

forward compatible to further work by this Special Interest Group.

- Define stable core functionality which can be implemented in the near term.

Virtual Terminal SIG

This Special Interest Group's charter is based upon the implementation of Draft International Standards 9040 and 9041 and their respective addenda, in providing Basic Virtual Terminal Service.

This group will develop agreements for the implementation and testing of the following terminal types.

- X.29 PAD
- TELNET
- Basic Scrolling
- Basic Paging
- Basic Forms

Upper Layers SIG

The charter of the Upper Layers SIG is as follows.

- Develop product level specifications for the implementation of:
  - Session service and protocol,
  - Presentation service and protocol,
  - ACSE service and protocol.
  - Remote Operations Service Element (ROSE)
  - Reliable Transfer Service Element (RTSE)

- In addition, the specifications to be developed by the Upper Layers SIG will address issues that are common to layers 5-7 such as addressing, registration, etc. This SIG will review output and proposals from other SIGs to ensure consistency with international standards regarding Upper Layer Architecture.

- The specifications developed will be done to support the requirements of all ASE SIGs.

The objectives of the Upper Layers SIG are to:

- Study OSI Session, Presentation, ACSE, ROSE, and RTSE

- Incorporate implementor's agreements in the 1987 NBS standing document,

- Produce and maintain recommendations for implementations of these layers,

- Where necessary provide input to the relevant standards bodies concerning Session, Presentation, ACSE, ROSE, and RTSE

- React in a timely manner (i.e., to develop corresponding implementor's agreements) to technical changes in ISO documents.

The following are the guidelines under which the Upper Layers SIG will operate:

- Align implementation agreements with other organizations such as ANSI and ISO,

- Develop implementor's agreements that promote the efficiency of protocols,

- Develop implementor's agreements that promote ease in the verification of interoperability,

- Develop necessary conformance statements.

Network Management SIG

Will use phased workload approach to accommodate volume of emerging OSI management-related standards,

The SIG will:

- Agree upon NBS Implementors OSI systems management reference model

- Develop product level specifications for implementations, relating to common services/protocols for exchanging management information between OSI nodes

- Develop product level specifications for implementations relating to specific management services for exchanging fault management (FM), Security Management (SM), Configuration Management (CM), Accounting Management (AM), and Performance Management (PM) information between OSI nodes

- Initiate and coordinate with appropriate layer SIGs product level specifications of layer-specific management information to support FM, SM, CM, AM, and PM.

As necessary, the SIG will:

- Establish liaisons with various standards bodies

- Provide feedback for additional/enhanced services and protocols for OSI management

Office Document Architecture and Office Document Interchange Format SIG

The SIG will:

- develop one or more product level specifications for implementations of ISO/DIS 8613, i.e., the SIG will define one or more Document Application Profiles (DAP's)

- develop requirements for conformance testing of products purporting conformance to the (se) DAP (s)

- specify and describe requirements for services that manage the generation and interpretation of the ODA/ODIF document representation

- determine preferred relationships between ODA/ODIF and other document interchange formats

- promote the SIG's agreements (e.g., presentations, product demonstrations, press releases)

As necessary, the SIG will:

- establish liaison with required SIG's (e.g., X.400, FTAM, and Upper Layers SIG's) to seek efficient transfer capability for document interchange based on the ODA/ODIF SIG agreements

- provide feedback and liaison to groups working on ISO/DIS 8613 related activities

1.6 POINTS OF CONTACT

OSI Workshop - Chairman	Rob Rosenthal	NBS	(301) 975-3603
OSI Workshop - Registration	Larry Keys	NBS	(301) 975-3604
FTAM SIG	Klaus Truoel	GMD/DFN	49-615-1869312
X.400 SIG	Charles Fox	DEC	44-734-854885
Lower Layers SIG	Mike Gering	IBM	(919) 543-0481
Security SIG	Denny Branstad	NBS	(301) 975-2913
DS SIG	Anthony Hodson	ICL	44-344-424842
VT SIG	Rick Wilder	Mitre	(703) 883-6174
Upper Layers SIG	David Chappell	Cray Research	(612) 825-7928
ODA/ODIF SIG	Frank Dawson	IBM	(214) 556-5073
Network Management	Paul Brusil	Mitre	(617) 271-7632
Technical Liaison Committee	J.J. Cinecoe	Wang	(617) 967-5514
MAP	Gary Workman	GM	(313) 947-0599
TOP	Laurie Bride	BCS	(206) 763-5719
Government OSI Profile	Jerry Mulvenna	NBS	(301) 975-3631
OSINET			
Steering Committee	Jerry Mulvenna	NBS	(301) 975-3631
Technical Committee	Carol Edgar	NBS	(301) 975-3613
SME (MAP/TOP Sponsorship)	Mark Shaw		(313) 271-1500
U.S. Government OSI User's Committee	Jerry Mulvenna	NBS	(301) 975-3631

2.6 WIDE AREA NETWORKS

2.6.1 X.25 Wide Area Networks

The procedures required to describe the DTE side of a DTE/DCE interface for systems attached to sub-networks providing an X.25 interface shall be as defined in ISO 7776 and ISO 8202 and as supplemented below. (These procedures a/shall also apply to a DTE operating on a DTE/DTE interface).

2.6.1.1 ISO 7776

ISO 7776 is used as the Layer 2 Protocol with the following agreements:

- the address assignments are:

  DTE = A (=11000000 binary)
  DCE = B (=10000000 binary)

  On a DTE/DTE interface, on of the DTEs, by a prior agreement, shall use the DCE address.

- the modules shall be 8.

- a window size (k) of 7 shall be supported. Other window sizes may be supported.

- the Multilink Procedures are excluded.

2.6.1.2 ISO 8208

The elements of ISO 8208 applicable for use depend on the OSI role of ISO 8208 (ie., provisions of CONS, support of CLNP). Independent of the role, ISO 8208 is used as the Layer 3 protocol, with the following agreements:

- Virtual Call Service;

- any window and packet size mutually agreed;

- a DTE must be cable of receiving the Flow Control Parameter Negotiation Facility and responding appropriately (per ISO 8208).

When ISO 8208 is used to support CONS, the optional user

facilities in Section 5.1 of ISO 8278 shall also be supported.

When ISO 8298 is used to support CLNP (when providing the CLNS), Permanent Virtual Circuit Service may also be used.

2.7 INTEGRATED SERVICES DIGITAL NETWORKS (ISDN)

2.7.1 Introduction

This section defines Implementation Agreements based on the 1988 CCITT Recommendations Q.920/921 and Q.930/931. These agreements provide a set of procedures for accessing and ISDN so that systems implemented according to these agreements can successfully inter-operate. This is not meant to preclude vendors from implementing additional procedures specified in the ISDN protocols, as long as it does not create system inter-operability problems.

The CCITT Recommendations Q.920/921 and Q.930/931 specify the protocols for access to data services and transport that may be supported by an ISDN. The procedures supported in this document are consistent with the ANSI version of ISDN protocols.

This section presumes that the reader is familiar with these standards, and possesses technical knowledge appropriate to implementing of testing them. This section provides guidance for the implementor; it is not an ISDN tutorial.

2.7.2 Scope and Field of Application

Capabilities will vary from ISDN to ISDN and procedures beyond those included here may be necessary to more effectively utilize of request those network services. Further procedures for Layer 3 are contained in CCITT Recommendations Q.930/931/932.

2.7.3 Services

ISDN services are described in CCITT I Series Recommendations; I.210 discusses the principles of telecommunications services supported by ISDN; I.211 describes the bearer services to be provided by an ISDN; and I.212 describes the tele-services supported by ISDN.

Layer 2 of ISDN is specified in CCITT Recommendation Q.920/921 and provides the functions and services summarized below:

- o provision of one or more data link connections
- o frame delimiting, alignment, and transparency

- sequence control
- detection of transmission, format, and operational errors on a data link
- recovery from detected errors and notification of unrecoverable errors
- flow control
- support of multiple Layer 3 entities.

Layer 3 for ISDN is specified by CCITT Recommendation Q.930/931 and utilizes functions and services provided by the data link layer as summarized below:

- establishment of data link connections
- notification of unrecoverable data link errors
- release of data link connections
- notification of data link failures
- recovery from certain error conditions
- indication of data link layer status

Layer 3 of ISDN provides the functions and services summarized below:

- processing of primitives for communication with the data link layer
- generation and interpretation of Layer 3 messages for peer-to-peer communications
- administration of timers and logical entities (ie., call references) used in the call control procedures
- administration of access resources including B-channels
- error detection and recovery
- sequence and flow control

2.7.4 Implementation Agreements

This section gives Implementation Agreements for individual ISDN-related protocols and the protocol stacks and arrangements for using these protocols.

Figures 1 and 2 give the agreed stacks for X.25 packet transfer over the D and B channels respectively. ISO 8878 and ISO DIS 9574 are included to show support of CONS via ISDN; actual Implementation Agreements for these two ISO standards are in Section 3, Network Layer, of this document.

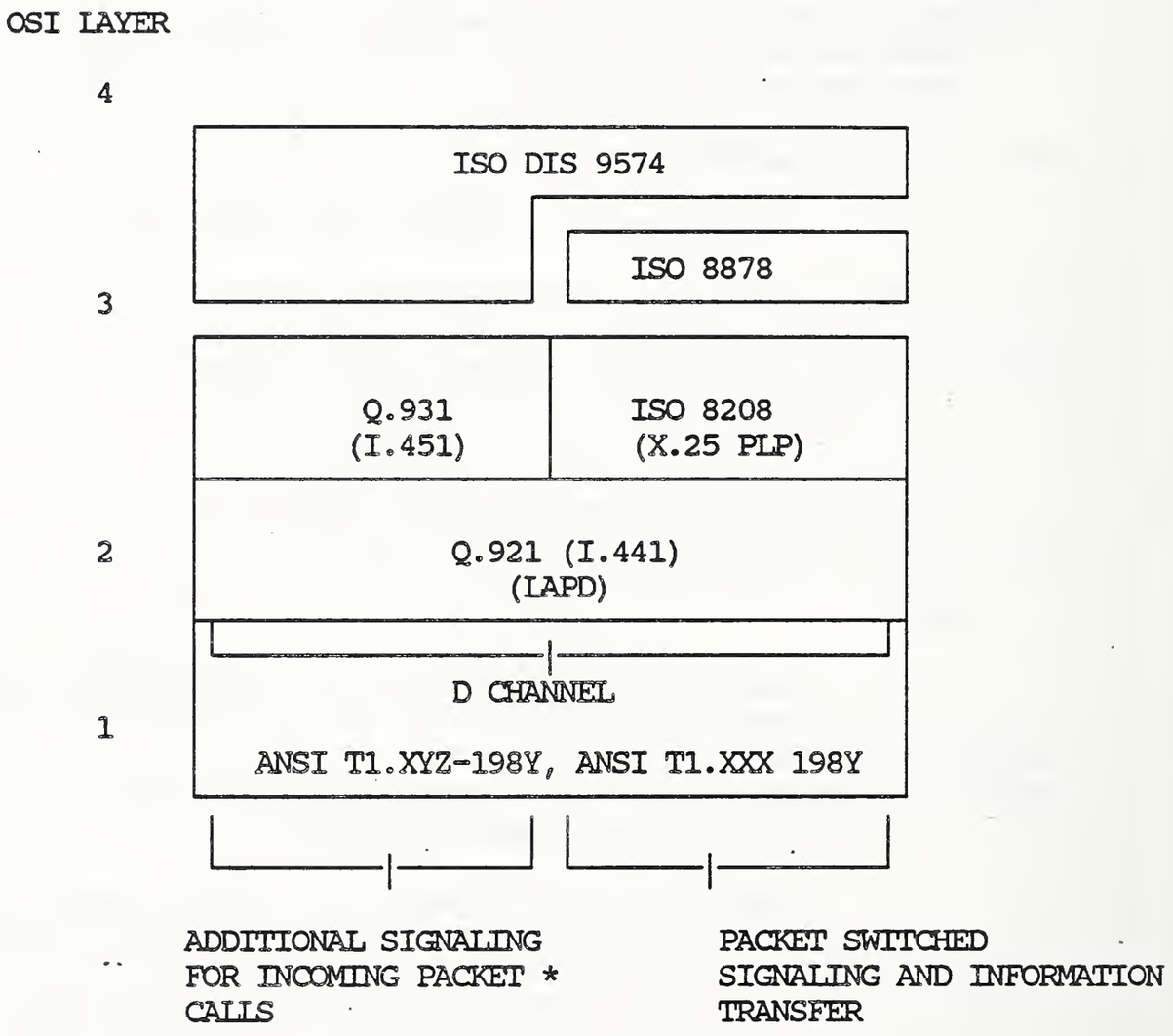


Figure 2.1 Protocol Layers at S and T reference points when D Channel is used in ISDN

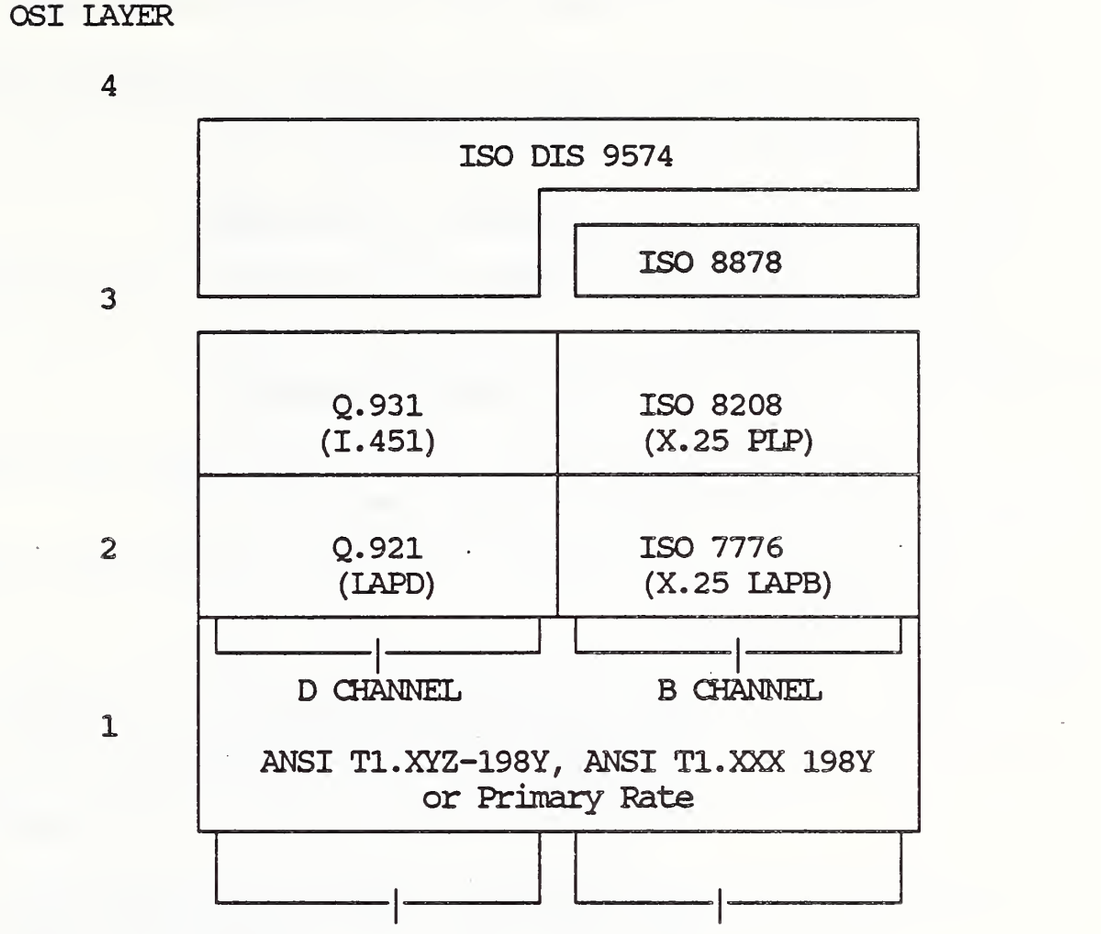


Figure 2.2 Protocol Layers at S and T reference points when B Channel is used in ISDN

2.7.4.1 Physical Layer, Basic Access at "U"

(To be based on ANSI T1. XXX-198Y, "Integrated Services Digital Network-Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT-Layer 1 Specification")

2.7.4.2 Physical Layer, Basic Access at S and T

(To be based on ANSI T1. XYZ-198Y, "Integrated Services Digital Network-Basic Access Interface at S and T Reference Points-Layer 1 Specifications.")

2.7.4.3 Physical Layer, Primary Rate

(To be based on CCITT Recommendation I.431 and related standards.)

2.7.4.4 Data Link Layer, D-Channel

CCITT Recommendation Q.921 (I.441), "ISDN User-Network Interface Data Link Layer Specification".

The following decisions have been reached with respect to this protocol:

1. For TEI assignment, the preferred type of TEI for user equipment to operate in a passive bus arrangement should be an automatic TEI. It is the responsibility of the user to ensure that non-automatic TEI values are uniquely assigned.

2. The Data Link Layer Monitor Function is an optional procedure for supervising the operation of a data link. This procedure is to detect a faulty data link connection condition, or a user equipment having been unplugged, when no Layer 2 frames are being exchanged on the data link connection. It is recommended that this procedure be implemented on all SAPI=0, D-Channel links using multiframe acknowledged information transfer.

2.7.4.5 Signaling

CCITT Recommendations Q.931 (I.451), "ISDN User-Network Interface Layer 3 Specification".

The following agreements have been reached concerning the use of Q.931.

- On a Basic Rate Interface supporting the ISDN virtual circuit service, all of Q.931 Section 6 except for 6.1.1 and 6.2.1 (the sections covering the circuit-switched access case) shall apply. The following sections also apply: 2.2, packet mode access connection states; 3.2, messages for packet mode access connection control; 4-4.5, section specifying general

information element handling and encoding; 4.7, information elements for packet communications.

- On a Primary Rate Interface supporting the ISDN virtual circuit service all of Q.931 Section 6 shall apply except for 6.1.1 and 6.2.1 and 6.4.2 (the sections specifying D-Channel ISDN virtual circuit service case). The following sections also apply: 2.2, packet mode access connection states; 3.2, messages for packet mode access connection control; 4-4.5, sections specifying general information element handling and encoding; 4.7, information elements for packet communications.

- On a Basic or Primary Rate Interface supporting the circuit-switched access to PSPDN service, Q.931 sections 6.1.1, 6.2.1, 6.3.1 and 6.4.3 shall apply. The following sections also apply; 2.1, circuit mode connection states; 3.1, messages for circuit mode connection control; 4-4.5, sections specifying general information element handling and encoding.

2.7.4.6 Data Link Layer B-Channel

The agreements on ISO 7776 specified in section 2.6.1.1 shall apply here.

2.7.4.7 Packet Layer

The agreements on ISO 8208 specified in section 2.6.1.2 shall apply here. When ISO 8208 is used on the D-Channel, the maximum size of the user data field of a data packet shall be limited to 256 octets.

3.5.3.1 ISO 8473

1. Subsets of the protocol:

- Implementations will not transmit PDUs encoded using the inactive subset. Received PDUs encoded using the inactive subset will be discarded.

- The non-segmenting subset will not be used. Implementations will not generate data PDUs without a segmentation part. However, implementations will receive and correctly process PDUs which do not contain the segmentation part.

2. Mandatory Functions:

- The lifetime parameter shall be used as specified in section 6.4 of ISO 8473. The parameter shall have an initial value of at least three times the network span or ~~of~~ three times the maximum transit delay (in units of 500 milliseconds), whichever is greater.

- The reassembly timer for an initial PDU at the reassembly point shall be no greater than the largest value of all lifetime parameters contained in all derived PDUs.

3. Optional Functions:

- The Security parameter is not defined by these Agreements. Implementations shall not transmit the parameter except where defined by bilateral agreements.

- Partial and complete source Routing will not be supported.[1]

- Partial record of Route will be supported by Intermediate systems.

- ISO 8473 will be followed with respect to QOS.

---

[1] A problem exists with the Partial Source Routing option which can cause PDUs to loop in the network until their lifetime expires.

- For systems implementing the congestion avoidance scheme.

A Globally Unique QOS Maintenance parameter shall be included in all PDU originated by End Systems. As specified in ISO 8473, the initial value of the Congestion Experienced flag (CE flag) within the Globally Unique QOS Maintenance Parameter shall be set by the originating End System to zero. All other flags within the Globally Unique QOS Maintenance Parameter shall be set based on the specific local needs of the originating End System.

Intermediate systems not implementing queue length averaging shall leave the CE flag in the same state as it was received. In particular, no intermediate system (IS) shall ever clear (set to zero) the CE flag.

All intermediate systems shall monitor all incoming and outgoing queues and compute average queue lengths as shown in box 1. The averaging is done from the beginning of the previous cycle to the current time. A cycle begins at the instant of the first NSDU arrival after an idle period.

An IS should set the CE flag in all NSDUs forwarded on a queue which has an average queue length greater than one.

The queue length averaging algorithm computes the average queue length over two cycles, where the two cycles are:

1) the "previous cycle", which is the interval from when the IS becomes busy, until it becomes idle and the idle ends (indicated by the instant the first packet arrives to the idle IS).

2) the "current cycle", which is the interval from the end of the idle interval to the current time instant when the average queue length is computed.

An embodiment of the averaging algorithm is shown in the following box:

Table 3.1 Queue Length Averaging Algorithm

The algorithm makes use of the following variables:

t = Current time
t_i = time of i^{th} arrival or departure event
q_i = number of packets in the system after the event
T_0 = time at the beginning of the previous cycle
T_1 = time at the beginning of the current cycle

The algorithm consists of three components:

1. Queue Length Update: Beginning with $q_0 = 0$,
   If the i^{th} event is an arrival event, $q_i = q_{i-1}+1$
   If the i^{th} event is a departure event, $q_i = q_{i-1}-1$

2. Queue Area (integral) update:

$$\text{Area of the previous cycle} = \sum_{t_i \epsilon (T_0, t_1)} q_{i-1}(t_i - t_{i-1})$$

$$\text{Area of the current cycle} = \sum_{t_i \epsilon (T_1, t)} q_{i-1}(t_i - t_{i-1})$$

3. Average Queue Length Update:

$$\text{Average Queue length over the two cycles} = \frac{\text{Area of the two cycles}}{\text{Time of the two cycles}} = \frac{\text{Area of the two cycles}}{t - T_0}$$

3.6.1 Mandatory Method of Providing CONS

3.6.1.1 General

Independent of the subnetwork type (of Section 2), when providing the CONS using X.25-1984, the following shall apply:

- The definition of the CONS is as specified in ISO 8348, Network Service Definition.

- The mapping of the elements of the CONS to the elements of the X.25 Packet Level Protocol (PLP) is as specified in ISO 8878, Use of X.25 to Provide the Connection-mode Network Service.

- The general procedures and formats of the X.25 PLP are as specified in ISO 8208, X.25 Packet Level Protocol for Data Terminal Equipment.

- CONS may be provided as part of the subnetwork types mentioned in section 2. In particular, when CONS is provided in a Local Area Network, ISO/DIS 8881, in addition to the documents listed above, shall apply.

3.6.1.2 X.25 WAN

No additional provisions apply in an X.25 WAN.

3.6.1.3 LANs

When providing the CONS in a Local Area Network, the following aspects of ISO/DIS 8881, in addition to the documents listed shall apply:

- clauses 1-6 and 9-11 for LLC Type 1 operation, including the additional nonstandard default packet size listed in clause 6.3, Note 2

Note: Operation of ISO 8208 in conjunction with LLC Type 2 requires agreement on LLC Type 2 procedures.

3.6.1.4 ISDN

When providing the CONS in an ISDN, the considerations for control of a B and D channel in ISO/DIS 9574, in addition to those provided in Section 3.6.1.1, shall apply.

3.8.2 End System to Intermediate System

9. The multicast addresses corresponding to "All Intermediate Systems on the network" (All_ISN) and "All End Systems on the network" (All_ESN) shall default to the following:

All_ESN = 0900 2B00 0004
All_ISN = 0900 2B00 0005

3.9 PROCEDURES FOR OSI NETWORK SERVICE/PROTOCOL IDENTIFICATION

3.9.1 General

The protocol identifiers specified in ISO PDTR 9577 ("Protocol Identification in the OSI Network Layer") provide a basis from which OSI systems (both End Systems and Intermediate Systems) may derive a set of procedures for indicating which OSI protocols are used in a particular instance of communication. As such, these procedures are only concerned with IPIs and SPIs that identify OSI protocols and pertain to the following types of systems:

A. systems providing/supporting only CONS (using ISO 8208/8878),
B. systems providing/supporting only CLNS (using ISO 8473), and
C. systems providing/supporting both CONS and CLNS.

From this set of definitions, the following possibilities for success (S) or failure (F) of an instance of communication can be defined, as shown in the table below:

Originating End System Type	Destination End System Type A	B	C
A	S	F	S
B	F	S	S
C	S	S	S

3.9.2 Processing of Protocol Identifiers

The usage of Protocol Identifiers in Network Protocol Data Units (NPDUs) depends on several factors:

- the OSI Network Service to be provided
- the protocol to be used in providing this service
- the role the protocol is to be used in (per the Internal Organization of the Network Layer)
  and
- the type of subnetwork to which the system is connected.

3.9.2.1 Originating NPDUs

The selection of a particular OSI Network Service depends on the capabilities of both the origination and destination end systems. It is not the intent of this section to provide guidelines on how to make this choice except for simple obvious criteria; rather, it is intended only to provide guidance on how to convey this choice to the destination system.

Where a prior knowledge exists in the originating End System about the capabilities (with respect to OSI Network Services available) of the destination End System, it should be used. This may result in no communication if the two End Systems involved only provide Network Services of different types. Alternatively, where a prior knowledge does not exist, then the selection of a Service to use in an instance of communication depends solely on the capabilities of the originating End System:

- if only CONS-related protocols (e.g., ISO 8208 are available, then this should be used and the Protocol Identifier specified so as to reflect the chosen protocol(s)

- if only CLNS-related protocols (e.g., 8473) are available, then this should be used and the Protocol Identifier specified so as to reflect the chosen protocol(s)

- if both Services are available, then other criteria are used in deciding which to use in an instance of communication.

Note: The choice of OSI Network Service to be used in an instance of communication is reflected in the Network Service primitives issued by the Network Service user.

Once a selection of Network Service has been made, the use of particular protocols depend on, for example, the subnetwork to which the originating End System is attached. Some specific cases are given in Annex A of ISO PDTR 9677. Another case involves use of the Protocol for Providing the Connectionless Network Service directly over the Data Link Service, as given in ISO 8473 (e.g., in a LAN). In this case, the IPI indicates ISO 8473.

3.9.2.2 Destination System Processing

A system receiving an NPDU must first be concerned with the protocol identified by the IPI. Valid values are given in Table 2 of ISO PDTR 9577. If the protocol is recognized as one supported by the system, further processing of the protocol is preformed according to the rules of that protocol. If not, an error is recognized and may be conveyed to the originating peer entity. With respect to ISO 8208 and ISO 8473, the following would apply for such error conditions.

1. For ISO 8208, the condition is classified as an "invalid General format Identifier", for which a DIAGNOSTIC packet may be returned. If DIAGNOSTIC packets are not used by the system, the NPDU is discarded without any further action.

2. For ISO 8473, the NPDU is discarded without any further action.

Given acceptance of the protocol identified by the IPI, the system must also determine the acceptability of the OSI Network Service being requested. Use of ISO 8473 implies CLNS; however, use of ISO 8208 can imply either CONS or CLNS, as identified by the SPI. In the case of ISO 8208, therefore, further processing is needed to determine the acceptability of the requested Service. If this Service is not acceptable (e.g., not supported by the system), a diagnostic code should be "Connection Rejection - unrecognizable protocol identifier in user data" (decimal 249).

Note: In ISO 8208, a call may be refused for reasons other than non-support of the requested OSI Network Service.

3.9.2.3 Further Processing in Originating End System

Further processing on receipt of an NPDU in response to an initial attempt to communicate may be necessary/useful to determine the success of such an attempt.

For ISO 8473, when used directly over the Date Link Service, the success of failure of an attempt to communicate may not be visible/obvious within the Network Layer. On the other hand, use of ISO 8473 over ISO 8208 may provide, via the diagnostic code in a received CLEAR INDICATION packet, an indication of failure to communicate (e.g., the remote system does not support CLNS).

When using ISO 8208 to provide the CONS, the diagnostic code in a received CLEAR INDICATION packet may provide the necessary indication of why a call was refused.

In cases where an ISO 8208 call is refused with diagnostic #249, it would not be desirable to re-attempt such calls with the exact same set of parameters; however, how the origination system ensures this is a local matter.

In cases where an origination system is capable of supporting both OSI Network Services, it may wish to re-attempt communications using the other mode of Network Service than that initially attempted.

3.10 MIGRATION CONSIDERATIONS

This section considers problems arising from evolving OSI standards and implementations based on earlier versions of OSI standards.

3.10.1 X.25-1980

Until there is widespread availability of 1984 X.25 service, it will be necessary for X.400 systems to use those existing packet-switched public data networks which offer only pre-1984 X.25 service. While 1980 X.25 does not provide the CONS as defined by ISO 8348, there is no implication of non-conformance to these Agreements resulting there from for systems using 1980 X.25 to interchange data at the Network Layer, provided they conform in all other respects.

This is an exception to the Agreements for providing the OSI Network Service, granted temporarily for practical reasons. This exception will be removed when it is deemed to be no longer necessary, in the judgement of the Workshop. While this provision is in effect, it provides an alternative method of using 1980 X.25 to the provisions of 3.6.2

3.11 CONFORMANCE

4. TRANSPORT LAYER

4.2 SCOPE AND FIELD OF APPLICATION

The connection-mode transportation protocols have been identified for implementation. Transport classes 0 and 4 of X.224 (1988) have been endorsed for use over CONS. Transport class 4 of 8073 AD2 has been endorsed for use over CLNS.

4.4 ERRATA

4.4.1 OSI Defect Reports

This section lists the defect reports from ISO which are currently recognized to be valid for the purpose of NBS conformance.

4.5 TRANSPORT CLASS 4

4.5.1 Transport Class 4 Overview

Transport class 4 is mandatory for connection oriented communication between systems using the OSI CLNS and may also be used for systems using the OSI CONS (i.e., a private MHS, etc.).

4.5.2.1 Rules for Negotiation

- The use of checksums shall be as specified in ISO 8073 section 6.5.4., i.e., checksum shall be used unless both transports explicitly negotiate its non-use. Requesting its non-use is an implementation choice. All implementations must be able to operate with checksums.

- A transport entity shall accept a DR TPDU and a corresponding DC TPDU with or without a checksum in response to a CR or CCTPDU.

- Transmitted DR TPDUs shall carry a disconnect reason code as specified in OSI 8073 which pertains to the actual cause of the disconnect. A DR TPDU may carry a reason code of "0" (unspecified) if the cause is not listed in ISO 8073 reason codes.

4.5.2.5 Congestion Avoidance Policies

For systems implementing a congestion avoidance policy the following rules shall be used:

RECEIVING TRANSPORT ENTITY (RTE) RULES:

Rule 1: Initialization of Window

Initially, the receiving window (WR) granted to a new transport connection (TC) is based on the local buffer management policy (which may be a window size WR). This window is sent to the sending transport entity (STE) in the next CDT field transmitted.

Rule 2: Required Sampling Period

All RTEs shall maintain a fixed value for WR until the next 2WR DT TPDU arrive since the last CDT field was transmitted by the RTE.

Rule 3: Required Counting of Received TPDUs in a Sampling Period

All RTEs shall maintain a count, N equal to the total number of TPDUs received and a count, NC equal to the total number of TPDUs received which had the CE Flag set. All types of TPDUs are included in the counts for N and NC, not just DT TPDUs.

Rule 4: Required Action upon the end of a Sampling Period

All RTEs shall take the following action at the end of each sampling period:

- If the count NC is less than fifty percent of the count N, the RTE shall increase WR by adding 1 up to a maximum, WR (that is based on the local buffer management policy) otherwise, it shall decrease WR by multiplying by 0.875 (a minimum of 1).
- Reset N and NC to zero.
- Transmit the new window WR in the next CDT field sent to the sending transport entity.

SENDING TRANSPORT ENTITY (STE) RULES:

Rule 1: Initialization of Window

All STEs shall maintain a sending window size (WS). Initially and also as long as there is no loss, WS is set equal to the receiving window value WR received from the remote RTE in the last CDT field.

Rule 2: Required Action on a Timeout

All STEs shall reset WS to one when the retransmissions timer expires and indicates a lost TPDU. WS now limits the number of DT TPDUs that may be transmitted or retransmitted without further acknowledgements.

Rule 3: Required Counting of Acknowledged TPDU

All STEs shall maintain a count, ACKRCVD of the number of DT TPDUs acknowledged, by the RTE, since WS was last adjusted. Therefore each time WS is adjusted, the count ACKRCVD shall be reset to zero.

Rule 4: Increase Window Policy

All STEs shall increase WS by one each time ACKRCVD is equal to of greater than the current value of WS, unless WS exceeds the window permitted by the remote RTE.

4.7 CONNECTIONLESS TRANSPORT

Document ISO IS 8072/DAD1 is the Transport Service Definition covering Connectionless-mode Transmission. Document ISO DIS 8602 is the Protocol for providing the Connectionless-mode Transport service.

4.7.1 Connectionless Transport Overview

The connectionless transport protocol shall be implemented as specified in ISO DIS 8602.

4.7.2 Protocol Agreements

The connectionless transport protocol is a relatively simple protocol providing little opportunity for conflicting interpretations. A few relevant agreements follow.

- The optional elements of procedure for use of CLTS over CONS (i.e., section 6.2 of DIS 8602) will not be supported.

- A Unitdata TPDU that is received that contains a protocol error or an unknown destination TSAP ID shall be discarded.

4.7.2.1 Connectionless Transport Service Access Points or Selectors

The TSAP selector field in the UD TPDU shall be encoded as a variable length field and will be interpreted as an octet string. The length of the string cannot exceed 32 octets.

5. MESSAGE HANDLING SYSTEMS

5.1 INTRODUCTION

This is an Implementation Agreement developed by the Implementor's Workshop sponsored by the U.S. National Bureau of Standards to promote the useful exchange of data between devices manufactured by different vendors. This Agreement is based on, and employs protocols developed in accord with, the OSI Reference Model. While this Agreement introduces no new protocols, it eliminates ambiguities in interpretations.

This is an Implementation Agreement for Message Handling Systems (MHS) based on both the CCITT X.400(1988) series of Recommendations and the similar (but not identical) ISO MOTIS standard (see References). The term `MHS' is used to refer to both sources where a distinction is unnecessary. Similarly, `1984' and `1988' are often used to distinguish between the CCITT X.400(1984) series of Recommendations and the later sources. Figure 5.1 shows the layered structure of this Agreement.

It is the objective of the NBS OSI Workshop to promote global interoperability. Regrettably, the CCITT and ISO versions of the 1988 MHS standards have diverged in respect of certain conformance requirements. This Implementation Agreement seeks to establish a common specification which is conformant with both CCITT and ISO with a view to:

- Preventing a proliferation of incompatible communities of MHS systems which are isolated for protocol reasons;
- Achieving interworking with implementations conforming to the NBS Stable Implementation Agreements for CCITT 1984 X.400-based Message Handling Systems (NBS);
- Facilitating integration of other OSI-based services (e.g. Directory) within a single real system.

This initial Implementation Agreement is designed to encourage early upgrade of existing 1984-based systems:

- To add useful 1988 functionality (Message Store, remote UA, etc);
- To provide a minimal conformant 1988 MHS as a firm basis for the introduction of further 1988 services and features. Subsequent versions of this Agreement will define such additional 1988 aspects as incremental enhancements.

However, it is <u>not</u> considered that the existing NBS Stable Implementation Agreements for CCITT 1984 X.400-based Message Handling Systems should be withdrawn at this stage and it can be anticipated that X.400(1984) implementations will continue to provide a viable

alternative for applications that do not require the additional 1988 functionality for some time.

Interpersonal Messaging System	CCITT X.420	ISO 10021-7
Message Store	CCITT X.413	ISO 10021-5
Message Transfer System	CCITT X.411/419	ISO 10021-4
Remote Operations Service Element	CCITT X.219/229	ISO 9072
Reliable Transfer Service Element	CCITT X.218/228	ISO 9066
Association Control Service Element	See Chapter ..	
Presentation Layer	See Chapter ..	
Session Layer	See Chapter ..	

Figure 5.1 The Layered Structure of this Implementation Agreement

5.2 SCOPE

This Agreement specifies the requirements for MHS implementations based on the 1988 MHS standards (see Figure 5.1 above).

This Agreement applies to Private Management Domains (PRMDs) and Administration Management Domains (ADMDs). Six boundary interfaces are specified:

(A) PRMD to PRMD;
(B) PRMD to ADMD;
(C) ADMD to ADMD;
(D) MTA to MTA (within a PRMD, e.g., for MTAs from different vendors);
(E) MTA to remote MS or UA;
(F) MS to remote UA.

In case A, the PRMDs do not make use of MHS services provided by an ADMD. In cases B and C, UAs associated with an ADMD can be the source or destination for messages. Furthermore, in cases A and B, a PRMD can serve as a relay between MDs, and in cases B and C an ADMD can serve as a relay between MDs. In cases E and F, the UA is located remotely from the MTA. Figure 5.2 illustrates the interfaces to which this Agreement applies.

MHS protocols other than the Message Transfer Protocol (P1), the Message Transfer System Access Protocol (P3), the Interpersonal Messaging Protocol (P2), and the Message Store Access Protocol (P7)

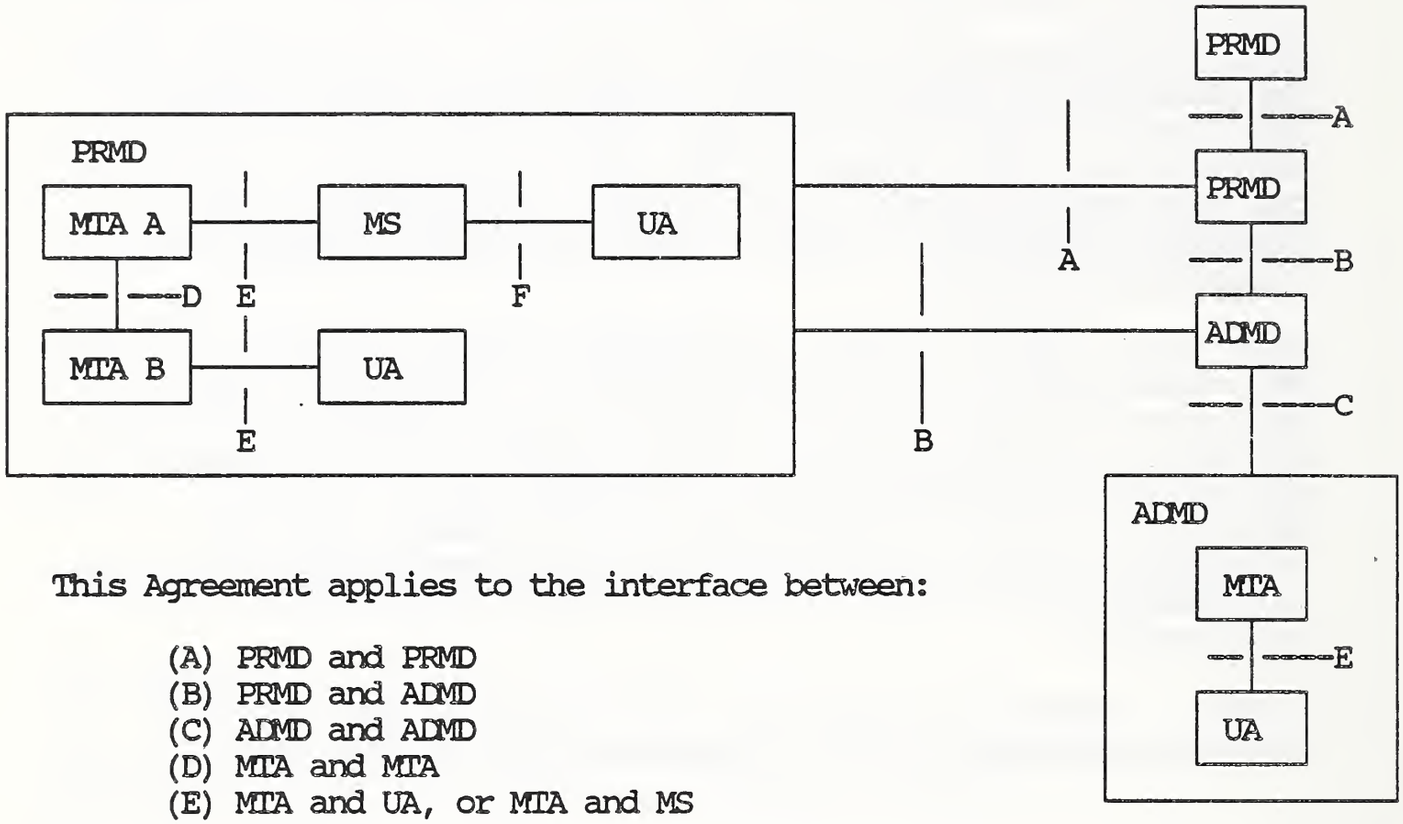
are beyond the scope of this Agreement. Issues arising from the use of other protocols or relating to P1 components in support of other protocols are outside the scope of this document. This Agreement describes the minimum level of services provided at each interface shown in Figure 5.2. Provision for the use of the remaining services defined in the MHS standards is outside the scope of this document.

With the exception of intra-domain connections, this Agreement does not cover message exchange between communicating entities within a domain even if these entities communicate via P1, P2, P3, and P7. Bilateral agreements between domains may be implemented in addition to the requirements stated in this document. Conformance to this Agreement requires the ability to exchange messages without use of bilateral agreements.

The initial version of this Agreement will define a minimal conformant MHS implementation which will be capable of interworking with implementations based on the CCITT X.400(1984) Recommendations as defined in Chapter 7 of the NBS Stable Implementation Agreements for OSI Protocols (Version 1 Edition 1, December 1987), and will additionally define the minimum set of requirements which are necessary to provide useful remote UA and/or Message Store services, independent of the level (i.e. 1984 or 1988) of the MTA implementation.

Figure 5.3 shows the categories of MHS service covered by this Agreement and indicates where they are defined in this Chapter.

PRMD = Private Management Domain
ADMD = Administration Management Domain



This Agreement applies to the interface between:

(A) PRMD and PRMD
(B) PRMD and ADMD
(C) ADMD and ADMD
(D) MTA and MTA
(E) MTA and UA, or MTA and MS
(F) UA and MS

Figure 5.2 Scenario Definition

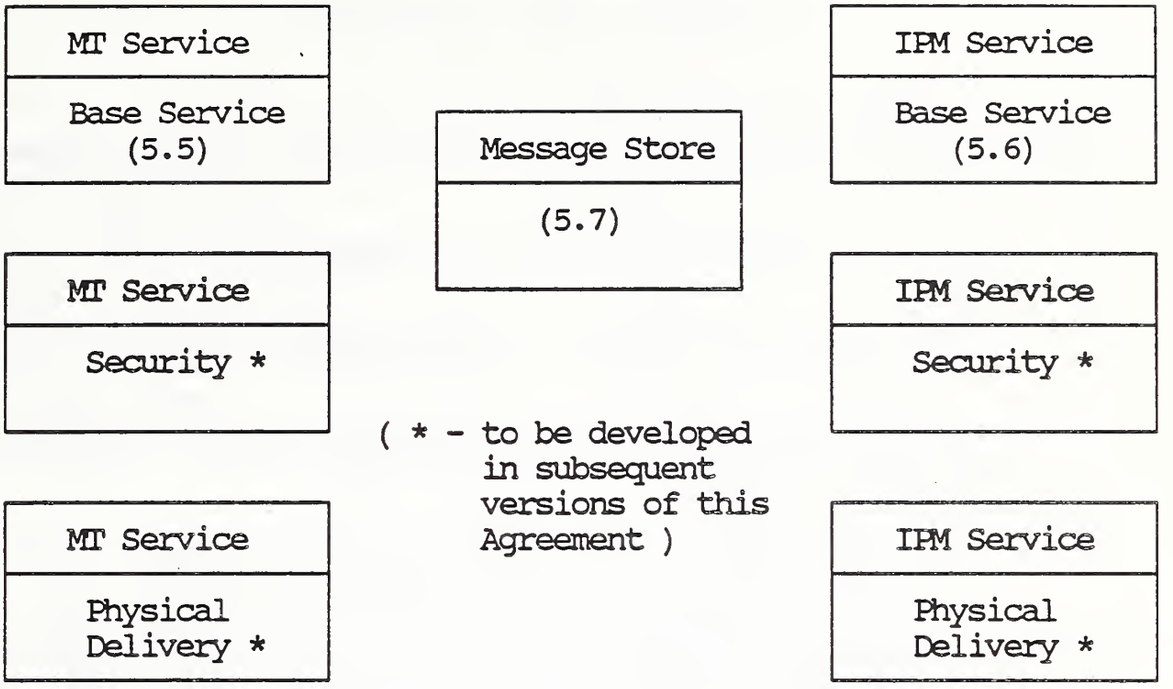


Figure 5.3 MHS Service Categories

5.3 STATUS

This version of the Implementation Agreements for Message Handling Systems (MHS) based on the CCITT X.400(1988) Recommendations and ISO MOTIS standards is under development.

It is intended that the Stable Implementation Agreements to be published in December 1988 will include an Agreement which specifies a minimal 1988-based MHS implementation and support for Message Stores and remote User Agents, and which addresses interworking with 1984-based implementations. The remaining features specified in the 1988 standards will be covered in subsequent versions of this Agreement.

5.4 ERRATA

5.5 MESSAGE TRANSFER (MT) SERVICE

5.5.1 Introduction

This section specifies the requirements for a minimal 1988-based MTS implementation (i.e., MTA) which is capable of interworking with 1984-based MTAs. The `base' MT Service specified in this section does not include support for:

- Message Store (see 5.7)
- Remote UA (see 5.8)
- Security (see 5.12)

- o Interworking with Physical Delivery systems or Specialized Access (see 5.13)

Such a minimal 1988-based MTA will have the following capabilities in order to achieve interworking with 1984-based MTAs and to facilitate migration to full 1988 operation:

- o It will be protocol-conformant to 1988 P1;
- o It will downgrade 1988 P1 to 1984 P1 when relaying to 1984-based MTAs, as specified in Appendix B of X.419;
- o It will relay the contents of 1988 P1 messages unchanged, even when relaying to 1984-based MTAs;

Note: It has yet to be determined whether `normal mode' or `X.410 mode' or both protocol stacks (i.e., as currently required by ISO and CCITT respectively) will be required for conformance to this Agreement. This issue will be resolved by the time of the December 1988 NBS X.400 SIG meeting.

5.5.2 Elements of Service

This section specifies the requirements for support of MT Elements of Service by an MTA conforming to this Agreement.

The classification scheme for support of Elements of Service is as follows:

Mandatory (M) - the Element of Service must be supported and made available to the service user;

Optional (O) - the Element of Service may be supported, but is not required for conformance to this Agreement;

Not Defined/Not Applicable (-) - the Element of Service is not defined by this Agreement or is otherwise not applicable in the particular context;

To Be Determined (*) - the support classification for the Element of Service has yet to be determined (temporary).

The requirements for support of MT Elements of Service for origination and reception and (where relevant) relaying are distinguished. Elements of Service which are new in the 1988 MHS standards are indicated as (1988).

Table 5.1 Basic MT Service

Element of Service	Origination	Reception	Relaying
Access Management	M[1]	M[1]	-
Content Type Indication	M	M	-
Converted Indication	M	M	M
Delivery Time Stamp Indication	-	M	-
Message Identification	M	M	-
Non-delivery Notification	M	M	M
Original Encoded Information Types Indication	M	M	-
Submission Time Stamp Indication	M	M	-
User Capabilities Registration (1988)	-	M[2]	-

Table 5.2 MT Service Optional User Facilities

Element of Service	Origination	Reception	Relaying
Alternate Recipient Allowed	M	*	-
Alternate Recipient Assignment	-	O	-
Conversion Prohibition	M	M	M
Conversion Prohibition in Case of Loss of Information (1988)	*	*	*
Deferred Delivery	O	-	-
Deferred Delivery Cancellation	O	-	-
Delivery Notification	M	M	-
Designation of Recipient by Directory Name (1988)	*	*	*
Disclosure of Other Recipients	O	M	M
DL Expansion History Indication (1988)	*	*	*
DL Expansion Prohibited (1988)	*	*	*
Explicit Conversion	O	O	O
Grade of Delivery Selection	M	M	M
Hold for Delivery	-	O/M[3]	-
Implicit Conversion	O	O	O
Latest Delivery Designation (1988)	*	*	*
Multi Destination Delivery	M	M	M
Originator Requested Alternate Recipient (1988)	*	*	*
Prevention of Non-delivery Notification	O	O	O
Probe	O	M	M
Redirection Allowed by Originator (1988)	*	*	-
Redirection of Incoming Messages (1988)	-	*	-
Requested Delivery Method (1988)	O	M	-
Restricted Delivery (1988)	-	*	-
Return of Content	O	O	O
Use of Distribution List (1988)	*	*	*

Notes: 1) Not applicable in the case of a co-located MTA/UA.

2) Required in order to provide a common MT Service, regardless of whether UAs are co-located or remote.

3) Required in the case of a remote UA (where the MTA does not support MSs) or a remote UA/MS.

5.5.3 Application Contexts

5.5.4 MTS Transfer Protocol (P1)

5.5.5 Reliable Transfer Service Element (RTSE)

5.5.6 Intra Domain Considerations

5.5.7 Error Handling

5.6 Interpersonal Messaging (IPM) Service

5.6.1 Introduction

This section specifies the requirements for a minimal 1988-based IPMS implementation (i.e., UA) which is capable of interworking with 1984-based UAs. The 'base' IPM Service specified in this section does not include support for:

- Message Store (see 5.7)
- Remote UA (see 5.8)
- Security (see 5.12)
- Interworking with Physical Delivery systems or Specialized Access (see 5.13)

Such a minimal 1988-based UA will have the following capabilities in order to achieve interworking with 1984-based UAs and to facilitate migration to full 1988 operation:

- It will continue to support content type P2 (encoded as integer 2) on submission and delivery;

- It will support receipt of P2 (encoded as integer 22);

- It may only originate P2 (22) by bilateral agreement (even in this case, the guidelines specified in section 20.2 of X.420(1988) are to be followed, i.e. the content type shall be encoded as P2 (2) unless 1988 P2 protocol elements are present).

Subsequent versions of this Agreement will allow 1988-based MHS implementations to submit P2 (22) content without requiring the

use of bilateral agreement, but the guidelines specified in section 20.2 of X.420(1988) will continue to be observed.

5.6.2 Elements of Service

This section specifies the requirements for support of IPM Elements of Service by a UA conforming to this Agreement.

The classification scheme for support of Elements of Service is as defined in section 5.5.1.

The requirements for support of IPM Elements of Service for origination and reception are distinguished. Elements of Service which are new in the 1988 MHS standards are indicated as (1988).

Table 5.3 Basic IPM Service

Element of Service	Origination	Reception
Access Management	M[1]	M[1]
Content Type Indication	M	M
Converted Indication	-	M
Delivery Time Stamp Indication	-	M
IP-message Identification	M	M
Message Identification	M	M
Non-delivery Notification	M	-
Original Encoded Information Types Indication	M	M
Submission Time Stamp Indication	M	M
Typed Body	-	M
User Capabilities Registration (1988)	-	M

Table 5.4 IPM Service Optional User Facilities

Element of Service	Origination	Reception
Alternate Recipient Allowed	O	*
Alternate Recipient Assignment	-	O
Authorizing Users Indication	O	M
Auto-forwarded Indication	*	M
Blind Copy Recipient Indication	O	M
Body Part Encryption Indication	O	M
Conversion Prohibition	M	M
Conversion Prohibition in Case of Loss of Information (1988)	*	-
Cross Referencing Indication	O	M
Deferred Delivery	O	-
Deferred Delivery Cancellation	O	-
Delivery Notification	M	-
Designation of Recipient by Directory Name (1988)	*	-
Disclosure of Other Recipients	O	M
DL Expansion History Indication (1988)	-	*
DL Expansion Prohibited (1988)	*	*
Expiry Date Indication	O	M
Explicit Conversion	O	-
Forwarded IP-message Indication	O	M
Grade of Delivery Selection	M	M
Hold for Delivery	-	O/M[2]
Implicit Conversion	-	O
Importance Indication	O	M
Incomplete Copy Indication (1988)	*	*
Language Indication (1988)	*	*
Latest Delivery Designation (1988)	*	-
Multi Destination Delivery	M	-
Multi-part Body	O	M
Non-receipt Notification Request	O	*
Obsoleting Indication	O	M
Originator Indication	M	M
Originator Requested Alternate Recipient (1988)	*	-

Table 5.4 IPM Service Optional User Facilities (contd)

Element of Service	Origination	Reception
Prevention of Non-delivery Notification	O	-
Primary and Copy Recipients Indication	M	M
Probe	O	-
Receipt Notification Request Indication	O	O
Redirection Allowed by Originator (1988)	*	-
Redirection of Incoming Messages (1988)	-	*
Reply Request Indication	O	M
Replying IP-message Indication	M	M
Requested Delivery Method (1988)	*	*
Restricted Delivery (1988)	-	*
Return of Content	O	-
Sensitivity Indication	O	M
Subject Indication	M	M
Use of Distribution List (1988)	*	*

Notes: 1) Not applicable in the case of a co-located MTA/UA.

2) Required in the case of a remote UA (where the MTA does not support MSs) or a remote UA/MS.

5.6.3 Interpersonal Messaging Protocol (P2)

5.6.4 Body Part Support

5.6.5 Error Handling

5.7 MESSAGE STORE

5.7.1 Introduction

This section specifies Agreements for implementation of the Message Store (MS). The MS is responsible for accepting delivery of messages on behalf of a single end-user, and retaining the messages until the end-user's UA is able to retrieve them. Message submission and administration services are provided via "pass-through" to the MTS. Figure 5.4 illustrates the logical relationship of the MS to the UA and MTS.

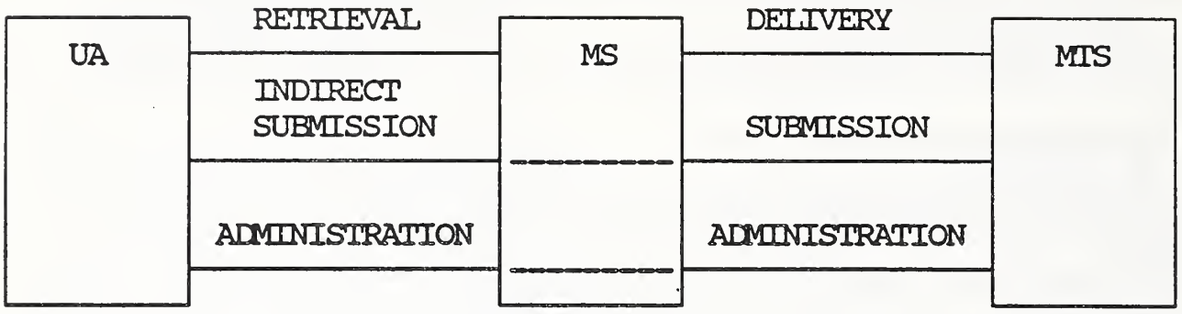


Figure 5.4 Message Store Model

The Agreements in this section specify the Message Store's use of the retrieval, delivery, and administration services. Agreements on submission services are specified in section 5.8, which describes support for the remote UA. Agreements on the use of message management services defined in ISO 10021-5 are for future study.

The goal of the Agreements in this section is to define the minimal set of features which are necessary to provide useful Message Store services, independent of the MTA implementation version (i.e., 1984 or 1988).

5.7.2 Scope

The scope of the Agreements in this section is depicted in Figure 5.5 below, and is confined to the services and protocols between the boundaries shown (marked with asterisks). Requirements for the UA and MTA are addressed only to the extent that they affect the Message Store and remote User Agent services and protocols. This reflects the additional services required at the UA to support MS access and at the MTA to support a remote MS.

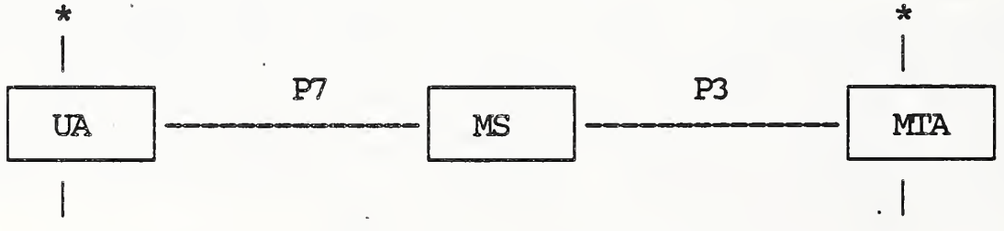


Figure 5.5 Scope of Message Store Agreements

5.7.3 Elements of Service

This section specifies the requirements for support of Elements of Service to provide a Message Store conforming to this Agreement.

The classification scheme for support of Elements of Service is as defined in section 5.5.1.

Support for Elements of Service is specified both for the Message Store itself and for the User Agent.

Table 5.5 Message Store Elements of Service

Element of Service	UA	MS
Stored Message Deletion	M	M
Stored Message Fetching	M	M
Stored Message Listing	M	M
Stored Message Summary	O	M
Stored Message Alert	O	O
Stored Message Auto Forward	O	O

5.7.4 Attribute Types

Requirements for support of attributes used in the Message Store are defined in section 11 of X.413(1988) and in Annex C of X.420(1988).

5.7.5 Pragmatic Constraints for Attribute Types

5.7.6 Implementation of the MS with 1984 Systems

While the Message Store is part of the 1988 MHS standards, implementation of MS services with a 1984 MTA is possible. In order to interoperate with other 1984 MHS systems, implementations with this configuration must adhere to the following guidelines:

- The UA must generate 1984 P2 PDUs;
- The UA must identify the content protocol as integer 2 to the MS;
- The MS must be co-located with the MTA unless 1988 P3 support is provided on the 1984 MTA as well.

To meet these guidelines, the UA may be implemented as follows:

- The UA could conform to X.420(1984), with 1988 UA extensions for utilizing the MS services;

- The UA could be a 1988 UA with restrictions on protocol elements generated and by identifying the content type as integer 2 rather than 3. No 1988-specific elements should be generated.

Details of the interface between the 1988 MS and the 1984 MTA are beyond the scope of these agreements.

5.7.7 Application Contexts

5.7.8 MS Access Protocol (P7)

5.7.9 MTS Access Protocol (P3)

5.7.10 Error Handling

5.8 REMOTE USER AGENT

5.8.1 Introduction

This section specifies Agreements for implementation of a remote User Agent (UA) that is not co-located with its MTA.

The goal of the Agreements in this section is to define the minimal set of features which are necessary to provide useful remote User Agent services, independent of the MTA implementation version (i.e., 1984 or 1988).

5.8.2 Scope

The scope of the Agreements in this section is depicted in Figure 5.6, and is confined to the services and protocols between the boundaries shown (marked with asterisks). Requirements for the UA and MTA are addressed only to the extent that they affect the remote User Agent services and protocols. Access to a Message Store by a remote User Agent is covered in section 5.7.

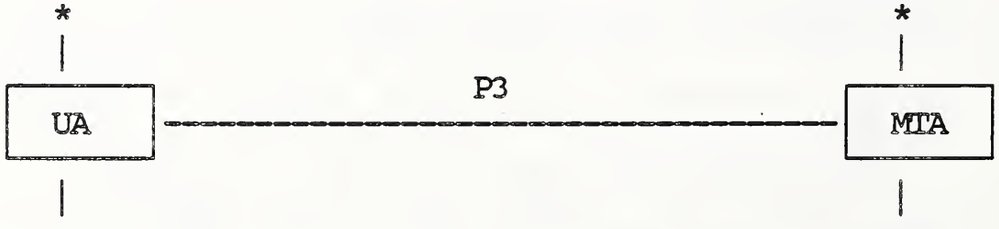


Figure 5.6 Scope of Remote User Agent Agreements

5.8.3 Service Support

5.8.4 Application Contexts

5.8.5 MTS Access Protocol (P3)

5.8.6 Error Handling

5.9 NAMING, ADDRESSING & ROUTING

5.9.1 MHS Use of Directory

5.9.2 Use of Names & Addresses

5.9.3 Distribution Lists

5.10 CONFORMANCE

5.10.1 Introduction

5.10.2 Configuration Options

MHS implementations may be configured as any single or multiple occurrence or combination of MTA, MS and UA, as illustrated in Figure 5.7. It is not intended to restrict the types of system that may be configured for conformance to these Agreements (although it is equally recognized that not all configuration types may be commercially viable).

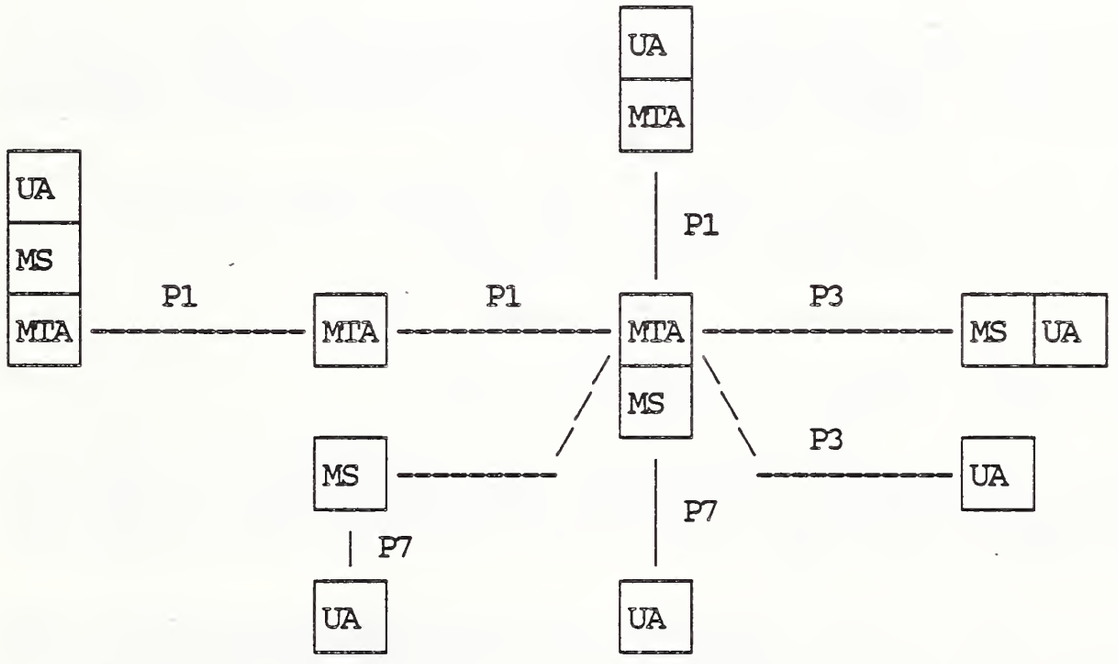


Figure 5.7 Configuration Options

5.10.3 Definition of Conformance

5.10.4 Conformance Requirements

5.11 MHS MANAGEMENT

5.12 MHS SECURITY

5.13 SPECIALIZED ACCESS

5.14 CONVERSION

5.15 USE OF UNDERLYING LAYERS

5.15.1 MT Transfer (P1)

The Session Service is defined in [ref.1].

The use of the RTSE requires the use of the Kernel, Half-Duplex, Exceptions, Minor Synchronize and Activity Management functional units.

Session Layer addressing is not used for the MT Transfer protocol (P1). That is, a Session-Address shall not be passed in the connect SPDU of the Session Layer.

The Transport Service is defined in [ref.2].

The choice of the class of Transport used by the Session Layer depends on the requirements for multiplexing and error recovery. For class 0 support see section 4.6 of the NBS Stable Agreements. Transport expedited service is not used.

The use of an error recovery class together with the RTSE duplicates mechanisms for error recovery.

5.15.2 MT Access (P3) and MS Access (P7)

The Session Service is defined in [ref.1].

If the RTSE is included in the Application-Association, the Kernel, Half-Duplex, Exceptions, Minor Synchronize and Activity Management functional units of the Session Service are used by the Presentation Layer.

If the RTSE is not included in the Application-Association, the Kernel and Duplex functional units of the Session Service are used by the Presentation Layer.

The Transport Service is defined in [ref.2].

For support of Transport class 0 see section 4.6 of the Stable Agreements. Transport expedited service is not used.

5.16 ERROR HANDLING

5.17 APPENDIX A: MHS PROTOCOL SPECIFICATIONS

5.17.1 MTS Transfer Protocol (P1)

5.17.2 Interpersonal Messaging Protocol (P2)

5.17.3 MTS Access Protocol (P3)

5.17.4 MS Access Protocol (P7)

5.18 APPENDIX B: RECOMMENDED PRACTICES

5.19 APPENDIX C: LIST OF ASN.1 OBJECT IDENTIFIERS

5.19.1 Content Types

5.19.2 Body Part Types

6. ISO FILE TRANSFER, ACCESS AND MANAGEMENT PHASE 3

6.1 INTRODUCTION

This section contains Implementors Agreements based on ISO 8571 File Transfer, Access and Management. These Agreements define enhancements to the Stable FTAM Implementation Agreements for OSI Protocols, Version 1, Edition 1, December 1987 (FTAM Phase 2 Agreements).

Therefore it is assumed that the reader is familiar both with the contents of the base standard ISO 8571 and its underlying layers, and also with the above mentioned NBS FTAM Phase 2 specifications.

These Phase 3 Agreements specify only the functionality which is additional to the Phase 2 Agreements.

Phase 2 Agreements define six Implementation Profiles, T1, T2, T3, A1, A2, M1. In order to avoid ambiguity when referring to these Implementation Profiles the above designations will apply only to Phase 2 functionality, references to Phase 3 enhanced Implementation Profiles will be by the addition of a'+', i.e. T1+, T2+, T3+, A1+, A2+, M1+.

6.2 SCOPE AND FIELD OF APPLICATION

These Phase 3 Agreements specify additional functionality to the FTAM Phase 2 Agreements. These additional functions include:

- Specification for Restart Data Transfer and Recovery functional units
- More details on Access Control and Concurrency Control
- Additional support of Character Sets

All Phase 2 systems are upward compatible to an Phase 3 system and can therefore interwork with it, if the additional functions are negotiated out (e.g. use of Recovery) or not used for the interconnection (e.g. additional features for document types).

6.3 STATUS

These FTAM Phase 3 Agreements are at working paper status, reflecting the results from the FTAM SIG Meeting, May 3-5. They are expected to be completed by March 1989.

6.4 ERRATA

6.5 ASSUMPTIONS

FTAM Phase 3 Agreements specify additional functionality to the Implementation Profiles T1, T2, T3, A1, A2, M1 as defined in the FTAM Phase 2 Agreements. So all definitions and requirements as for these Implementation Profiles apply also to the Phase 3 Agreements.

6.6 FILESTORE AGREEMENTS

6.6.1 Document types

In addition to the Phase 2 document type agreements the document type FTAM-4 is defined as per ISO 8571-2, Annex B.

The following Table 6.1 gives the support levels for document types with respect to the Implementation Profiles together with the supported parameter values. No restriction is defined for the <maximum string length> parameter.

Table 6.1 Implementation Profiles and Document Types

Implementation Profile	Document Type	Universal Class Number	String Significance
T1+, T2+, T3+, A1+, A2+	FTAM-1	Graphic String (25)	'variable' 'fixed'
		VisibleString (26)	'variable' 'fixed'
		GeneralString (27)	'not-significant'
		IA5String (22)	'not-significant'
T2+, T3+, A1+, A2+	FTAM-2	GraphicString (25)	'not-significant'
		VisibleString (26)	'not-significant'
		GeneralString (27)	'not-significant'
		IA5String (22)	'not-significant'
T1+, T2+, T3+, A1+, A2+	FTAM-3	-	'not-significant'
T2+, T3+, A1+, A2+	FTAM-4	-	'not-significant'

Notes:

1. The support level for document types in Implementation Profile M1+ depends on the T- of A- Implementation Profile, in conjunction with which M1+ is implemented.

2. In addition to the Phase 2 Agreements the character set ISO 6937-2 is also supported for GraphicString and GeneralString.
(full 6937-2? Or which subrepertoires?)

6.6.2 Character Sets

(More on character sets? Subrepertoires of 6937-2?)

6.7 SERVICE AGREEMENTS

6.7.1 FTAM Service Level Agreements

Recovery and Restart Data Transfer are defined for FTAM Phase 3 implementations.

FADU locking is optionally supported for Implementation Profiles A1+ and A2+.

6.8 PROTOCOL AGREEMENTS

6.8.1 Functional Unit Agreements

For FTAM Phase 3 implementations Recovery and Restart Data Transfer are optionally supported.

FADU locking is optionally supported for Implementation Profiles A1+ and A2+.

6.8.2 Error Recovery

Procedures for Class I, II and III errors are defined and supported for FTAM Phase 3 implementations. It is the implementor's choice whether to handle class I errors using F-RESTART PDUs or whether to use the class II error procedure.

6.8.2.1 Docket Handling

For class I or II errors the docket will always be present as long as the association is not terminated. Once the association is terminated, recovery from a class I, II error is not possible.

When a class III error occurs, the length of time a docket is maintained is determined by the local system. Recovery from a class III error is only possible as long as both end systems maintain the docket.

It is also a local decision how many dockets can be maintained simultaneously.

6.8.2.2 Parameters for Error Recovery

- <functional units> parameter of F-INITIALIZE includes 'restart data transfer' and 'recovery' if these are selected by the Initiator and the Responder.
- The semantics of the <FTAM quality of service> parameter is as defined in ISO 8571-2, including the local knowledge of FERPM.
- No minimum requirement for the <checkpoint window> parameter of the checkpoint size is defined.

- o For the <recovery mode> parameter of F-OPEN all three values 'none', 'at-start-of-file' and 'at-any-active-checkpoint' are supported If recovery mode 'at-start-of-file' is negotiated no F-CHECK shall be issued. When recovering at the start of the file, the <recovery point> value of 0 shall be used.

Note: This Agreement is because of a deficiency of the standard. All other behaviors would lead to unpredictable results, because text and state tables in 8571-4 are ambiguous.

- o For the <diagnostic> parameter of F-CANCEL/F-U-ABORT/F-P-ABORT the term <suggested delay> is supported and shall always be present when Restart/Recovery is negotiated. The Basic FERPM should wait at least the amount of time as given by the <suggested delay> term before attempting to recover.

6.8.3 Concurrency Control

6.8.3.1 Concurrency Control to whole file

The <concurrency control> parameter of F-SELECT, F-CREATE and F-OPEN either in conjunction with of without the <access control> attribute of Security Group are supported for Initiators and optionally supported for Responders.

If supported by a Responder details of their possible usage is a local matter and shall be specified in the PICS.

Default values for concurrency control are specified for FTAM Phase 2 Agreements.

For a first access either the specified concurrency locks or the default values are assigned. For a subsequent request shall be rejected.

6.8.3.2 FADU Locking

FADU locking functional unit and the respective <FADU lock> parameters are optionally supported for the Implementation Profiles A1+, A2+.

It is understood that ISO 8571-4 clause 18.4 also applies to FADU locks, that means, as long as a docket is maintained, FADU locks locking any FADUs recorded in that docket should be maintained.

6.9 CONFORMANCE

In addition to the specific requirements specified in the following subsections, conformance to this Phase 3 specification requires

- conformance to ISO 8571
- conformance to Phase 2 FTAM, as of December 1987 including all agreed errata changes.

6.9.1 Initiators

Every implementation of an FTAM Phase 3 Initiator shall support

- Document types as specified in section 6.6.1
- optionally the Recovery procedure and the Restart Data Transfer procedure as specified in section 6.8.2
- the use of <concurrency control> parameters and FADU locking functionality as specified in section 6.8.3

6.9.2 Responders

Every implementation of an FTAM Phase 3 Responder shall support

- Document types as specified in section 6.6.1
- optionally the Recovery procedure and the Restart Data Transfer procedure as specified in section 6.8.2
- optionally the use of <concurrency control> parameters and FADU locking functionality as specified in section 6.8.3

6.10 APPENDIX A:

PICS PROFORMA FOR FTAM PHASE 3

This PICS Proforma lists only the Phase 3 functions which are additions to the FTAM Phase 2 Agreements.

7. UPPER LAYERS

7.1 INTRODUCTION

This section specifies agreements for the implementation of OSI upper layer protocols, including Session, Presentation, ACSE, ROSE, and RTSE.

7.2 SCOPE AND FIELD OF APPLICATION

The agreements in this section apply to all ASE agreements in this document, including FTAM, X.400, Directory Services, Virtual Terminal, and OSI Network Management. All upper layer agreements specified in chapter 5 of the NBS Special Publication 500-150, "Stable Implementation Agreements for Open Systems Interconnection Protocols" (with errata) are also implicitly included in these agreements.

7.3 STATUS

This version of the upper layer agreements is under development.

7.4 ERRATA

7.5 ACSE

7.6 ROSE

7.7 RTSE

7.8 PRESENTATION

7.8.1 General

7.8.1.1 Presentation Data Value (PDV)

- A presentation data value (PDV) is a value of a type in an abstract syntax, e.g., a value of an ASN.1 type.
- A PDV may contain embedded PDVs in different contexts. A change of context within a PDV is indicated by an EXTERNAL. EXTERNAL implies an embedded PDV.

- o A PDV cannot be split across PDV-lists in fully-encoded user data.

- o Fully encoded data that is a series of PDVs in the same presentation context should be encoded as one PDV-list.

7.8.2 Connection Oriented

7.8.3 Connectionless

Agreements in this area are currently being pursued.

7.9 SESSIONS

7.9.1 General

7.9.2 Connection Oriented

7.9.3 Connectionless

Agreements in this area are currently being pursued.

7.10 SPECIFIC ASE REQUIREMENTS

7.10.1 Virtual Terminal

Note: This section is an ongoing-stable agreement.

7.10.1.1 VT

7.10.1.1.1 Phase 1a

ACSE Requirements:
all

Application Contexts:
- o "ISO VT" - implies the use of the ACSE and the VT ASE

Abstract Syntaxes:
- o "ISO 8650-ACSE1"

Associated Transfer Syntax:
o "Basic Encoding of a single ASN.1 type"

Presentation Requirements:

Presentation Functional Units:
o kernel

Presentation Contexts:
o 2

Abstract Syntaxes:
o "VT Basic"

Associated Transfer Syntax:
o "Basic Encoding of a single ASN.1 type"

Session Requirements:

Session Functional Units:
o kernel
o duplex
o expedited data
o major synchronize
o resynchronize
only a Resynchronize Type value of "abandon"
o typed data

Version Number: 2

Maximum size of User Data parameter field: 10,240

Session Options:
o expedited data

7.11 REFERENCES

The following documents are referenced in these ongoing NBS agreements on the OSI Upper Layers. Other document references may be found in the Stable Implementation Agreements for OSI Protocols of December, 1987.

7.11.1 Session Layer

[S1] Information Processing Systems - Open Systems Interconnection - Addendum to the Session Service Definition Covering Connectionless-Mode Transmission, ISO/DAD3 8326.

[S2] Information Processing Systems - Open Systems Interconnection - Session Connectionless Protocol to provide the Connectionless-Mode Session Service, ISO/DIS 9548.

7.11.2 Presentation Layer

[P1] Information Processing Systems - Open Systems Interconnection - Addendum to ISO 8822 Covering Connectionless Presentation Service, ISO/PDAD1 8822.

[P2] Information Processing Systems - Open Systems Interconnection - Connectionless Presentation Protocol, ISO/DP 9576.

8. NETWORK MANAGEMENT

8.1 Introduction

In progressing work on OSI Management in the NBS/OSI Network Management SIG, the OSI Management framework specified in ISO 7498/Part 4 (as presented in [ref.1]) shall be used as the basis for concepts and terminology relevant to OSI Management activities and to management services supported by OSI Management Protocols.

8.1.1 References

ISO/TC97/SC21/WG4 - Tokyo-25, DIS 7498/4, 9 June 1987, "Information Processing Systems - Open Systems Interconnection - Basic Reference Model Part 4 - OSI Management Framework - Revised following DP ballot."

8.2 SCOPE AND FIELD OF APPLICATION

8.2.1 Use of Evolving Standards

8.2.2 Management Architecture

8.2.3 Management Requirements and Scenarios

8.3 STATUS

8.4 ERRATA

8.4.1 Implementation Agreements Corrections

8.4.2 ISO Defects/Interim Resolutions

8.5 SERVICES OFFERED

8.5.1 Common Management Services

8.5.2 Specific Management Functional Areas

8.6 SERVICES REQUIRED

8.6.1 Use of Services of Other ASEs

8.6.1.1 ACSE Requirements

9. SECURITY

9.1 INTRODUCTION

9.1.1 References

9.1.2 Assumptions

9.1.3 Definitions

9.1.4 Motivation

9.1.5 Security Chapter Structure

9.2 SCOPE AND FIELD OF APPLICATION

9.3 STATUS

9.4 ERRATA

9.5 GENERAL OSI SECURITY MODEL

9.5.1 General Matrix from 7498-2

9.5.2 Selected Matrix of Services/Layers

9.5.3 Security Domain Model

9.6 OSI MANAGEMENT SECURITY AND SECURITY MANAGEMENT

9.7 PHYSICAL LAYER

9.7.1 Introduction

9.7.1.1 References

9.7.1.2 Definitions

9.7.1.3 Assumptions

9.7.1.4 Motivation

9.7.2 Scope and Field of Application

9.7.3 Specific Security Model

9.7.4 Services Offered

9.13.7 Management Elements Required/Impacted

9.13.8 Conformance Class Definitions

9.13.9 Conformance Class Specifications

9.13.10 Registration Issues Requirements

9.14 FTAM

9.14.1 Introduction

9.14.1.1 References

9.14.1.2 Definitions

9.14.1.3 Assumptions

9.14.1.4 Motivation

9.14.2 Scope and Field of Application

9.14.3 Specific Security Model

9.14.4 Services Offered

9.14.5 Services Required

9.14.6 Protocols

9.14.7 Management Elements Required/Impacted

9.14.8 Conformance Class Definitions

9.14.9 Conformance Class Specifications

9.14.10 Registration Issues Requirements

9.15 Message Handling System Security

The following definitions of the elements of security service are based on the 1988 CCITT Recommendations on the Message Handling System (X.400). The fourteen (14) elements of security service are refinements of the five (5) primary security services as defined in IS 7498 Part 2 (Security Architecture). The Implementor's Workshop prepared Table 9.2 that summarizes where in the MHS the element of security service may be performed (the check marks) as stated in the MHS Recommendations. The Special Interest Group in Security (SIG-SEC) then examined each of the 14 elements of security service and placed a priority rating (1-5) next to one of the checkmarks in each row representing the priority that should be given for consideration of standardization and implementation of that element of service. The

SIG-SEC reviewed the User Agent (UA) to User Agent peer entities as the first (perhaps preferred) place to implement security and used the check mark in that column if one was present. The SIG-SEC then reviewed the Message Transfer Agent (MTA) to Message Transfer Agent as the second place to implement security if it has not been implemented in the UA-UA protocol. Finally, the interface between the UA and the MTA was investigated for implementing security.

The Implementor's Workshop will be using this table and the set of definitions as a basis upon which future work in MHS security may be performed. The table is and subject to change during future meetings.

Table 9.1 X.400 Relationship between Elements of Security Service and MHS Components

	UA-MS	MS-MTA	UA-UA	UA-MTA	MTA-MTA	MTA-UA	MS-UA
Message Origin Authentication			√1	√			
Report Origin Authentication					√4	√	
Probe Origin Authentication		√		√5			
Proof of Delivery			√2				√
Proof of Submission						√5	
Peer Entity Authentication	√	√		√	√4	√	√
Content Integrity			√1				
Content Confidentiality			√1				
Message Flow Confidentiality			√4				
Message Sequence Integrity			√2				
Non Repudiation of Origin			√1				
Non Repudiation of Submission						√5	
Non repudiation of Delivery			√3				
Access Control	√	√	√1	√	√	√	√

UA: User Agent
MS: Message Store
MTA: Message Transfer Agent

9.15.1 Definitions of Elements of Security Service

Message Origin Authentication MT

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

Report Origin Authentication MT

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

Probe Origin Authentication MT

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

Proof of Delivery MT

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

Proof of Submission MT

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

Peer Entity Authentication MT

This element of service provides confirmation of the identity of the Entity (UA, MTA, MS). It provides confidence at the time of usage only that an entity is not attempting to masquerade as an unauthorized entity.

Content Confidentiality MT

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

Content Integrity MT

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

Message Flow Confidentiality MT

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

Message Sequence Integrity MT

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

Non Repudiation of Origin MT

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

Non Repudiation of Submission MT

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

Non Repudiation of Delivery **MT**

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

Access Control **MT**

This element of service provides protection against unauthorized use of the resources accessed via MHS. Access decisions are directed by a security policy which may be identity and/or role based.

9.16 DIRECTORY

9.16.1 Introduction

9.16.1.1 References

9.16.1.2 Definitions

9.16.1.3 Assumptions

9.16.1.4 Motivation

9.16.2 Scope and Field of Application

9.16.3 Specific Security Model

9.16.4 Services Offered

9.16.5 Services Required

9.16.6 Protocols

9.16.7 Management Elements Required/Impacted

9.16.8 Conformance Class Definitions

9.16.9 Conformance Class Specifications

9.16.10 Registration Issues Requirements

9.17 VTP

9.17.1 Introduction

9.17.1.1 References

9.17.1.2 Definitions

9.17.1.3 Assumptions

9.17.1.4 Motivation

9.17.2 Scope and Field of Application

9.17.3 Specific Security Model

9.17.4 Services Offered

9.17.5 Services Required

9.17.6 Protocols

9.17.7 Management Elements Required/Impacted

9.17.8 Conformance Class Definitions

9.17.9 Conformance Class Specifications

9.17.10 Registration Issues Requirements

10. OBJECT IDENTIFIERS: STRUCTURE AND ALLOCATION

All upper layer agreements specified in chapter 10 of the NBS Special Publication 500-150, "Stable Implementation Agreements for Open Systems Interconnection Protocols" (with errata) are also implicitly included in these agreements.

The following objects need to be administered by an ad hoc registration authority:

Application Context Name
Abstract Syntax Name
Transfer Syntax Name
Document Type Name
Constraint Set Name
File Model
VT Profile
VT Control Object

Since all objects to be administered by the NBS Workshop SIGs are identified by the ASN.1 type OBJECT IDENTIFIER, the following structure shall be used:

Using the NameAndNumberForm (::= identifier (NumberForm)) for an ObjIdComponent we have:

```
ObjectIdentifierValue ::= { identifier1 (NumberForm1)
     identifier2 (NumberForm2)
     identifier3 (NumberForm3)
     identifier4 (NumberForm4)
     identifier5 (NumberForm5)
     identifier6 (NumberForm6) }
```

The assignment of identifiers and NumberForms is as follows:

identifier1	NumberForm1
iso	1
identifier2	**NumberForm2**
identified-organization	3
identifier3	**NumberForm3**
issuing-organization	9999
identifier4	**NumberForm4**
organization-code	1
identifier5	**NumberForm5**
application-context	1
abstract-syntax	2
file model	3

constraint-set	4
document-type	5
transfer-syntax	6
ftam-nil-ap-title	7
VT profile	8
VT control object	9

Note 1: The value of NumberForm3 is selected for use by implementors of these agreements: it has <u>not</u> been assigned by ISO or by any official Registration Authority. It does correspond to an "ad hoc" issuing organization with an ICD of 9999, as specified by ISO 6523. We intend to use the procedure designated in D.7 of the Specification of ASN.1, ISO 8824 once the appropriate Registration Authority has been established. This mechanism is subject to change dependent upon ISO standards.

Note 2: Specific values for identifier6 and NumberForm6 are chosen as needed by the NBS UL SIG. A table of the currently allocated values is given later.

Note 3: The NBS UL SIG will assign values for identifier5 and NumberForm5 as required by other SIGs.

Note 4: Companies wishing to interoperate may designate themselves with an organization code other than 1 under { iso (1) identified-organization (3) issuing-organization (9999) } for the purpose of defining private OBJECT IDENTIFIERs.

TABLE OF ALLOCATED OBJECT DESCRIPTORS and OBJECT IDENTIFIERS

The values of the first 4 NumberForms are constant, so the following value is defined for use in the table below.

```
nbs-ad-hoc OBJECT IDENTIFIER ::= { 1 3 9999 1 }
```

Note that the only OBJECT IDENTIFIERS herein defined are flagged with an '*'; all other OBJECT IDENTIFIERs and their associated ObjectDescriptor's are reproduced here solely for the convenience of implementors. The standards defining these OBJECT IDENTIFIERs and ObjectDescriptor's take precedence over the values specified below.

Application Context

Abstract Syntax

File Model

Constraint Set

Document Type

Transfer Syntax

VT Profile

```
"ISO VT VTE-profile NBS generic root"
     { nbs-ad-hoc nbs-vte-profile (8) } *
```

Note: used only with a subsidiary leaf as a specific VTE profile identifier.

```
"NBS VTE-Profile Telnet-1988"
     { nbs-vte-profile telnet-1988 (0) } *

"NBS VTE-Profile Transparent-1988"
     { nbs-vte-profile transparent-1988 (1) } *
```

Miscellaneous

READER RESPONSE FORM

Please retain my name for the next mailing of the NBS/OSI Implementors Workshop.

NAME _____

ADDRESS _____

_____

_____

PHONE NO. _____

Mail this page to:

National Bureau of Standards
NBS Workshop for Implementors of OSI
Bldg. 225/B-217
Gaithersburg, MD 20899

NBS-114A (REV. 2-8C)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET (See instructions)	1. PUBLICATION OR REPORT NO. NBSIR 88-3824	2. Performing Organ. Report No.	3. Publication Date July 1988

4. TITLE AND SUBTITLE

Ongoing Implementation Agreements for Open Systems Interconnection Protocols
Volume 2:
Continuing Agreements

5. AUTHOR(S)

Robert Rosenthal, Editor

6. PERFORMING ORGANIZATION (If joint or other than NBS, see instructions)

NATIONAL BUREAU OF STANDARDS
U.S. DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.

8. Type of Report & Period Covered

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP)

10. SUPPLEMENTARY NOTES

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)

This document records current agreements on implementation details of Open Systems Interconnection Protocols among the organizations participating in the NBS/OSI Workshop Series for Implementors of OSI Protocols. These decisions are documented to facilitate organizations in their understanding of the status of agreements. This is a standing document that is updated after each workshop (about 4 times a year).

12. KEY WORDS (Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)

local area networks; NBS/OSI Workshop; network protocols; Open Systems Interconncetion OSINET; testing protocols

13. AVAILABILITY

☒ Unlimited

☐ For Official Distribution. Do Not Release to NTIS

☐ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

☒ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES

87

15. Price

$13.95