INTERNATIONAL TELECOMMUNICATION UNION

ITU-T Q.812

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03/93)

SPECIFICATIONS OF SIGNALLING SYSTEM No. 7
Q3 INTERFACE

UPPER LAYER PROTOCOL PROFILES FOR THE Q3 INTERFACE

ITU-T Recommendation Q.812

(Previously "CCITT Recommendation")

FOREWORD

The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the International Telecommunication Union. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, established the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

ITU-T Recommendation Q.812 was prepared by the ITU-T Study Group XI (1988-1993) and was approved by the WTSC (Helsinki, March 1-12, 1993).

NOTES

1 As a consequence of a reform process within the International Telecommunication Union (ITU), the CCITT ceased to exist as of 28 February 1993. In its place, the ITU Telecommunication Standardization Sector (ITU-T) was created as of 1 March 1993. Similarly, in this reform process, the CCIR and the IFRB have been replaced by the Radiocommunication Sector.

In order not to delay publication of this Recommendation, no change has been made in the text to references containing the acronyms "CCITT, CCIR or IFRB" or their associated entities such as Plenary Assembly, Secretariat, etc. Future editions of this Recommendation will contain the proper terminology related to the new ITU structure.

2 In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

© ITU 1994

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

CONTENTS

			Page
1	Introduction		1
	1.1	Scope	1
	1.2	Abbreviations and symbols	1
	1.3	Terms	2
2	Upper layer protocol profiles		2
	2.1	Introduction	2
	2.2	Upper layer protocol profile for transaction type services	3
	2.3	Upper layer protocol profile for file transfer type services	4
3	Upper layer protocol profile for transaction type services		4
	3.1	Transport-layer profile for use over connection-mode network services	4
	3.2	Transport layer profile for use over connectionless-mode network services	7
	3.3	Session layer profile	8
	3.4	Presentation layer	9
	3.5	Application layer profile	10
4	Upper layer profile for file transfer type functions		13
	4.1	Session layer profile	13
	4.2	Application layer profile	14
5	Conformance		14
References			15

ABSTRACT

This Recommendation provides the upper layer (4-7) protocol profiles for the Q3 interface as defined in Recommendation M.3010.

Keywords

ACSE, ASN.1, CMISE, FTAM, Protocol Profiles, Q3 Interface, TMN.

UPPER LAYER PROTOCOL PROFILES FOR THE Q3 INTERFACE

(Helsinki, 1993)

1 Introduction

1.1 Scope

This Recommendation defines the characteristics of protocol profiles for the Q3 interface, as defined in Recommendation M.3010 [1]. The interface will support bidirectional data transfer for the management of telecommunications systems.

This Recommendation defines:

- the layer services profiles;
- the layer protocols profiles;
- the application service and protocols profiles;
- the conformance requirements to be met by an implementation of this interface.

This Recommendation does not define:

- the structure or meaning of the management information that is transmitted by means of the protocol suite;
- the manner in which management is accomplished as a result of the application protocol exchanges;
- the interactions which result in the use of the application layer protocols.

It is the intention to move the specification of the upper layers to International Standard Profiles (ISP) format. As the ISPs become standard, they will be reviewed for applicability and definition.

1.2 Abbreviations and symbols

1.2.1 Abbreviations

For the purpose of this Recommendation, the following abbreviations are used:

AC	Publication Context
ACSE	Association Control Service Element
AE	Application Entity
AEI	Application Entity Invocation
AFI	Authority and Format Identifier
APDU	Application-protocol-data-unit
ASN.1	Abstract Syntax Notation One
ASO	Application Service Object
CD	Collision Detection
CF	Control Function
CMISE	Common Management Information Service Element

Conf	Confirm
DCN	Data Communication Network
DIS	Draft International Standard
DLS	Data Link Service
DSP	Domain Specific Part
FTAM	File Transfer, Access and Management
IDI	Initial Domain Identifier
IDP	Initial Domain Part
Ind	Indication
ISO	International Organization for Standardization
LME	Layer Management Entity
MAC	Media Access Control
NE	Network Element
NS	Network Service
OSI	Open Systems Interconnection
PICS	Protocol Implementation Conformance Statement
QOS	Quality of Service
Req	Request
Res	Result
ROSE	Remote Operations Service Element
SMASE	Systems Management Application Service Element
TMN	Telecommunications Management Network

1.2.2 Symbols and abbreviations used in tables[1)]

M Mandatory

– The parameter is not present in the interaction described by the service or primitive concerned.

(=) The value of the parameter is equal to the value of the parameter in the column to the left.

1.3 Terms

Under study.

2 Upper layer protocol profiles

2.1 Introduction

The communication services and protocols referred to in this Recommendation are in accordance with the Open System Interconnection (OSI) Reference Model [2].

The protocols for the different layers are based on CCITT Recommendations and/or ISO standards.

---

1) The requirements are as defined in the referred standards or Recommendations.

Two types of protocol profiles are defined in this Recommendation:

- upper layer protocol profile for transaction type services;
- upper layer protocol profile for file transfer type services.

The two protocol profiles can be applied to applications using DCN, as defined by Recommendation M.3010 [1].

Interface Q3 is defined to intend to connect MDs to OSs, OAs to OSs, NEs to OSs, and OSs to OSs via a DCN.

Other ASEs will be added in the identified protocol profiles as new requirements develop.

2.2 Upper layer protocol profile for transaction type services

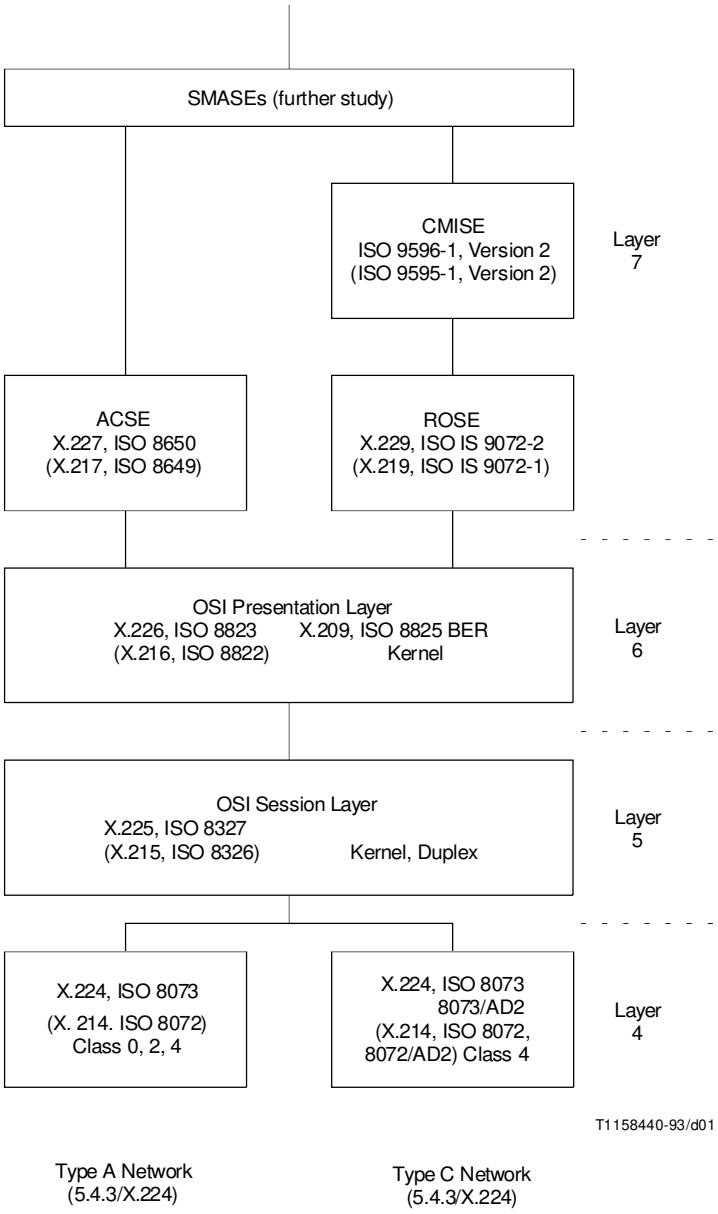

FIGURE 1/Q.812

Protocol profile for network management which uses transaction function

2.3 Upper layer protocol profile for file transfer type services

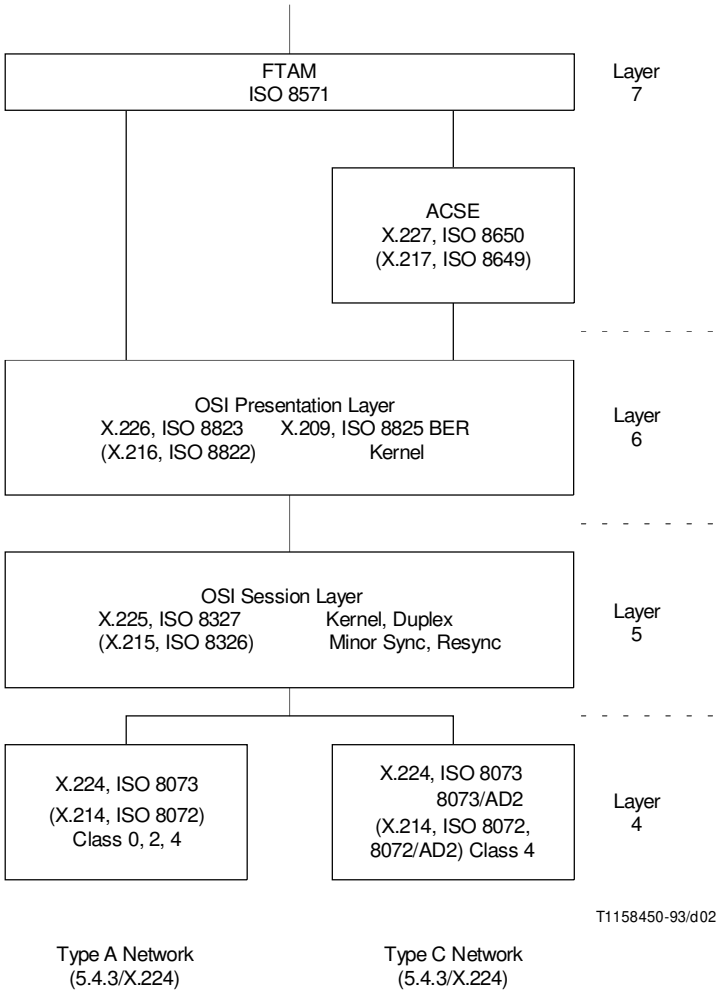

FIGURE 2/Q.812

Protocol profile for network management which uses file transfer

3 Upper layer protocol profile for transaction type services

3.1 Transport-layer profile for use over connection-mode network services

3.1.1 Services profiles

It is mandatory that for the connection-mode network service, the transport service shall conform to Recommendation X.214 [16] and to those provisions of ISO 8072 [18] that apply to the use of the Connection-Mode Network Service (CONS).

3.1.1.1 Splitting

Responders may refuse network connections which could impose an unnecessary restriction on the ability to establish outgoing network connections. To prevent repeated ineffective attempts during splitting, initiators shall refrain from immediately requesting additional network connections for a transport connection after a network connection has been refused. The time delay before requesting additional network connections is for further study.

3.1.1.2 Quality of Service negotiation

Quality of Service negotiation is outside the scope of this Recommendation. If Quality of Service negotiation is not supported, receipt of the parameters “throughput”, “residual error rate”, “priority” and “transit delay” in the CR and CC TPDUs shall be ignored.

3.1.1.3 TPDU size negotiation

Interoperability is achieved by having the initiator propose a TPDU size from the set specified in Table 1 and by the responder selecting the most appropriate TPDU size between 128 and the proposed TPDU size. The rules for negotiation of the size of the TPDU to be used in a given instance of communication are specified in ISO 8073 [19].

The choice of TPDU size is a local implementation issue.

3.1.1.4 Negotiation of protection

Negotiation of protection is outside the scope of this Recommendation. If negotiation of protection is not supported, receipt of the protection parameters in any CR TPDU and any CC TPDU shall be ignored.

3.1.2 Protocol profile

It is mandatory that for the connection-mode network service, the transport protocol shall conform to Recommendation X.224 [17] and to those provisions of ISO 8073 [19] that apply to the use of the Connection-Mode Network Service (CONS).

3.1.2.1 Class of service

Classes 4, 2 and 0 shall be supported as shown in Table 1 in countries requiring the features of transport layer Class 4. The conformance rules of Recommendation X.224 [17] require that Classes 0 and 2 be supported as well when Class 4 is specified. For existing equipment and in countries not requiring Class 4, support of Class 0 is mandatory and Class 2 is optional.

The default values shall be part of a vendor's offering. That is, unless otherwise specified by the user, the default parameters shall be the initial values supplied. They can be subsequently changed by the user within the specified range.

In addition to the requirements specified in Recommendation X.224 [17], equipment shall meet the following requirement: if a responder receives an alternate class of “none”, it shall respond with the preferred class. Rules for responders are specified in Table 2.

User options shall be provided to designate the preferred and alternate classes (see Table 3/X.224) [17]. When all of the classes are supported, the preferred class for connection is Class 4.

3.1.2.2 Protocol identification

For the purpose of transport layer protocol identification, the procedures specified in Annex B/X.224 [17] and ISO 8073/AD 1 [15] shall be used. The conventions for protocol identification given in ISO TR 10172 [25] should be followed. Selection of codes not specified in the referenced standards is for further study. The absence of call user data in a call request or call accept packet of Recommendation X.25 [13] and ISO 8208 [14] indicates the operation of the transport layer procedures of ISO 8073 [19] and Recommendation X.224 [17].

3.1.2.3 Attributes

Attributes of the transport layer for use with CONS are summarized in Table 1. The selection of values within required and optional ranges depends on characteristics of the messages.

NOTE – The need to support high priority messages that require low transit delay on a given transport connection must be reflected in the Quality of Service parameters requested when the transport connection is established. A properly implemented transport entity should not multiplex high priority messages that require low transit delay if it cannot provide the requested Quality of Service. Since this is an implementation detail, it is not subject to standardization.

TABLE 1/Q.812

Transport layer attributes
[for connection-mode network service (CONS)]

	Range	Default
Maximum TPDU (octets)	128, 256, 512, 1024 (2048, 4096, 8192 optional)	(128)
Class of Service	4, 2, 0	
Preferred Class	4, 2, 0	(4)
Alternative Class	4, 2, 0, none	(None
Expedited Data	Non-use	
Options for Class 4		
Data TPDU numbering (Note 2)	Normal, extended	(Normal)
Options for Class 2		
Data TPDU numbering (Note 2)	Normal, extended	(Normal)
Flow control	Explicit	
Parameters for Class 4		
T1 – Retransmission time	0.25-64 seconds (Note 4)	(8)
N – Retransmissions	2 (other values for further study)	
L Bound on reference	1-256 seconds	(32)
I Inactivity time	2-512 seconds	(64)

NOTES

1 Some systems may require TSAP-IDs. However, all systems shall be capable of generating called TSAP-IDs in CR TPDUs and capable of receiving calling and called TSAP-IDs in received CR and CC TPDUs, respectively.

2 Extended format option shall be implemented. Non-use of this option shall be negotiable. The responder shall honour the initiator's request whenever possible. Negotiation to other than what has been requested shall only occur under abnormal conditions, for example, severe congestion, as determined by the implementor. Initiators shall be prepared to operate in the mode confirmed by the responder.

3 Use of the checksum is required for the CR TPDU. An additional requirement is that all implementations shall support the negotiated "non-use" of the checksum. Initiators shall request and responders shall agree to "non-use" of the checksum.

4 The transport layer T1 timer should always be greater than the link layer T1 timer.

TABLE 2/Q.812

Valid response corresponding to preferred
and any alternative class proposed in the CR TPDU

Preferred Class	Alternative Class			
	0	2	4	None
0	Class 0	Not valide	NV	Class 0
2	Classes 0, 2	Class 2	NV	Class 2
4	Classes 0, 2, 4	Classes 2 or 4	Class 4	Classes 2 or 4

3.1.2.4 User data in connection request and connection confirm TPDUs

User data in the connection request and connection confirm TPDUs are optional in Recommendation X.224 [17]. No transport service user shall send it: all protocol implementations shall be prepared to receive it and all implementations may ignore it, i.e. it shall not cause a disconnect.

3.1.2.5 Class 0 error TPDU

When transport Class 0 has been negotiated, the error transport protocol data unit (ER-TPDU) may be used at any time and upon receipt requires that the recipient disconnect the network connection and, by extension, the transport connection.

3.1.2.6 Unknown CR TPDU parameters

An unknown parameter in any received CR TPDU shall be ignored.

When all of the classes are supported, the preferred class, when initiating a CR TPDU, shall be Class 4.

If a responder receives an alternative class of "none", implicit negotiation is enforced.

3.1.2.7 Invalid values of known CR TPDU parameters

Known parameters with valid lengths but with invalid values in a CR TPDU shall be handled as depicted in Table 3.

TABLE 3/Q.812

TPDU parameters

Parameter	Action
TASP id	Send DR TPDU
TPDU size	Ignore parameter, use default
Version	Ignore parameter, use default
Checksum	Discard CR TPDU
Alternate protocol classes	Protocol error

3.1.2.8 Additional options parameter

Unrecognized or not applicable bits of the "additional options" shall be ignored.

3.2 Transport layer profile for use over connectionless-mode network services

3.2.1 Services profile

It is mandatory that for the connectionless mode network services, the transport service shall conform to ISO 8072 [18] and ISO 8072/AD 2.

3.2.2 Protocol profile

Operation of the transport protocol over the connectionless-mode network layer service (CLNS), as described in ISO 8348/AD 1 [3], shall use the elements of ISO 8073/AD 2 [20], Class 4 operation over the CLNS.

3.2.2.1 Class of service

Support of Class 4 operation of ISO 8073/AD 2 [20] is mandatory.

3.2.2.2 Transport layer attributes

Transport layer attributes for Class 4 operation over the connectionless mode network layer service shall be as shown in Table 4.

TABLE 4/Q.812

Transport layer attributes
[for use with Connectionless-Mode Network Service (CLNS)]

	Value/Range/Option	Default
Maximum TPDU (Octets)	128, 256, 512, 1024 (2048, 4096 optional)	(128)
TSAP-ID (Note 1)	Up to 32 octets	–
Class of service	4	–
Preferred class	4	–
Alternative Class	None	–
Expedited Data	Non-use	–
Options:		
Security Parameters	Optional	–
Data TPDU numbering (Note 2)	Normal, extended	(Normal)
Checksum (Note 3)	Use, non-use	(Non-use)
Parameters:		
T1 – Retransmission time	0.25-64 seconds (Note 4)	(8)
N – Retransmissions	2-15	(2)
L – Bound on reference	1-256 seconds	(32)
I – Inactivity time	2-512 seconds	(64)

NOTES

1 Some systems may require TSAP-IDs. However, all systems shall be capable of generating called TSAP-IDs in CR TPDUs and capable of receiving calling and called TSAP-IDs in received CR and CC TPDUs, respectively.

2 Extended format option shall be implemented. Non-use of this option shall be negotiable. The responder shall honour the initiator's request whenever possible. Negotiation to other than what has been requested shall only occur under abnormal conditions, for example; severe congestion, as determined by the implementor. Initiators shall be prepared to operate in the mode confirmed by the responder.

3 Use of checksum is required for the CR TPDU. An additional requirement is that all implementations shall support the negotiated "non-use" of the checksum. Initiators shall request and responders shall agree to "non-use" of the checksum.

4 The transport layer T1 timer value should always be greater than the link layer T1 timer value.

3.3 Session layer profile

3.3.1 Service profile

The session layer conforms to the service definition in Recommendation X.215, ISO 8326 [21].

The default values shall be part of a vendor's offering. That is, unless otherwise specified by the user, the default parameters shall be the initial values supplied. They can be subsequently changed by the user within the specified range.

A conflict in the code values for subsequent number and flow control confirmation exists between ISO and CCITT. The conflict is expected to be resolved as specified in ISO 8073.

3.3.1.1 Functional units

Two session layer functional units (FU) are required in this Recommendation:

1) Kernel;

2) Duplex.

Restrictions applied to parameters and their values are specified in the following subclauses.

3.3.1.2 Transport expedited service

The use of the transport expedited service is as stated in Recommendation X.225: if available, it must be used. When the transport expedited service is available, the Prepare (PR), Session Protocol Data Unit (SPDU) shall be supported as in Recommendation X.225. The "Prepare Type" parameter value in the PR SPDU, to indicate the arrival of an Abort (AB) SPDU, is ABORT.

3.3.2 Protocol profile

The session layer conforms to the protocol definition in Recommendation X.225, ISO 8327 [22]. Support of Version 2 of the session protocol is mandatory.

3.3.2.1 Parameters

All mandatory parameters defined in Recommendation X.225 for the SPDUs required by the Kernel and Duplex FUs are mandatory parameters for this Recommendation.

3.3.2.2 User data

The maximum length of the session user data shall be 10240 octets. This restriction implies that the Overflow Accept (OA) and Connect Data Overflow (CDO) SPDUs are not required to be supported. "Session-selector" (s-selector) parameter values shall have a maximum length of 16 octets.

3.3.2.3 Session protocol data units

Session Protocol Data Units (SPDUs), associated with the Kernel and Duplex functional units, shall be supported as described in Table 9.

3.3.2.4 Reuse

Reuse of the transport connection is not required. The transport disconnect parameter value (PV) field may be absent or set to "transport connection is released" in appropriate SPDUs. Furthermore, on receipt of a transport disconnect PV field indicating "transport connection is kept", the transport connection can be released.

3.3.2.5 Segmentation

The "segmentation" feature in the session layer is not required. Support for extended concatenation of SPDUs is not required.

3.3.2.6 Invalid SPDUs

Upon receipt of an invalid SPDU, the session protocol machine shall take any action specified in A.4.3.2/X.225 [22] with the exception of action "d" (take no action).

3.4 Presentation layer

3.4.1 Services profile

It is mandatory that the presentation layer conform to the services specified in Recommendation X.216 [4] and ISO 8822.

3.4.1.1 Functional units

One presentation layer functional unit (FU) is required in this Recommendation:

1) Kernel

Restrictions applied to parameters and their values are specified in the following subclauses.

3.4.2 Protocol profile

It is mandatory that the presentation layer conform to the protocols specified in Recommendation X.226 [23] and ISO 8823 (normal mode).

3.4.2.1 Presentation protocol units

The following Presentation Protocol Units (PPDU) associated with the Kernel functional unit shall be supported as depicted in Table 5.

TABLE 5/Q.812

Presentation PPDU

(1) Connect Presentation	(CP PPDU)
(2) Connect Presentation Accept	(CPA PPDU)
(3) Connect Presentation Reject	(CPR PPDU)
(4) Abnormal Release Provider	(ARP PPDU)
(5) Abnormal Release User	(ARU PPDU)
(6) Presentation Data	(TD PPDU)

3.4.2.2 Parameters

All mandatory parameters defined in Recommendation X.226 [23] for the above PPDUs are mandatory for this Recommendation. The "presentation context identifier" value shall be encoded in no more than 2 octets. Also, the value(s) in the parameter "presentation context definition list" shall be consistent with the value(s) defined in the application-specific standards. "Presentation-selector" (p-selector) parameter values shall have a maximum length of 4 octets.

3.4.3 Encoding rules for transfer syntax

The encoding rules defined in Recommendation X.209 [8] shall be applied to derive the transfer syntax for the Application Protocol Data Units (APDUs). The ASN.1 OBJECT IDENTIFIER [joint-ISO-CCITT ASN.1 (1) basic-encoding (1)] shall be used as the value for the transfer syntax name. The maximum value of an ASN.1 basic encoding tag that needs to be handled for conformance to this Recommendation is 16 383. This is the largest unsigned integer that can be represented in 14 bits. Hence the identifier octets shall consist of an initial octet and up to two more octets, thus occupying a maximum of three octets. Also, the largest number of octets in the "contents octets" component of an ASN.1 data value encoding that needs to be handled for conformance to this Recommendation is 4,294,967,295. This is the largest unsigned integer that can be represented in 32 bits. Hence in the "long form" encoding, the length octets shall consist of an initial octet and up to four more octets, thus occupying a maximum of five octets. (Note that this restriction does not apply to "indefinite length" encodings.)

3.5 Application layer profile

The application layer protocol data unit presentation is described by using Abstract Syntax Notation One (ASN.1), as defined in Recommendation X.208 [7].

3.5.1 Application layer architecture

It is mandatory that the application layer conforms to the architecture for the application layer outlined in ISO 9545.

The concepts of Application Entity (AE), Application Entity Invocation (AEI), Application Service Object (ASO), Control Function (CF) and Application Context will be used to describe the relationship between ROSE, ACSE, CMISE, SMASE.

3.5.2 Association control service element

3.5.2.1 Services profile

The ACSE service description is detailed in Recommendation X.217 [11], ISO 8649. All of the defined ACSE services (see Table 6) are mandatory. The value of mode parameter of A-ASSOCIATE shall be "normal".

3.5.2.2 Protocol profile

The protocol specification for ACSE shall follow Recommendation X.227 [12], ISO 8650. All five APDUs (see Table 6) specified in the standard are mandatory.

TABLE 6/Q.812

ACSE services and associated APDUs

ACSE Service	Associated APDUs	Related P-Service
A-ASSOCIATE	AARQ, AARE	P-CONNECT
A-RELEASE	RLRQ, RLRE	P-RELEASE
A-ABORT	ABRT	P-U-ABORT
A-P-ABORT	(None)	P-P-ABORT

3.5.2.3 Use of the SACF for association control

The CF is defined to control the interactions among ASEs and/or ASO within the containing ASO in ISO/IEC 9545 with DAM 1.

Thus it controls the association establishment, release and abort in respect to the rules defined in the Application Context available for the association.

Then it allows the joint use of several ASEs on the same association.

3.5.2.4 Abstract Syntax Name

The ACSE abstract syntax name has the ASN.1 type OBJECT IDENTIFIER. The following value shall be used to identify the ACSE abstract-syntax-definition:

{

joint-ISO-CCITT association-control (2)
abstract-syntax (1) apdu's (0) version (1)

}

3.5.3 Remote operations

3.5.3.1 Services profile

The Remote Operations Service Element (ROSE) shall be a mandatory service element. The ROSE service description is detailed in Recommendation X.219, ISO 9072-1 [6]. All of the defined ROSE services (see Table 7) are mandatory.

3.5.3.2 Protocol profile

The protocol specification for ROSE shall follow Recommendation X.229 [10] and ISO 9072-2. All four APDUs specified in the standard (see Table 7) are mandatory. In addition, the ability to support correct origination and reception of the linked-id protocol element is required.

The requirement specified in Table 7 implies association Class 3 in ROSE.

TABLE 7/Q.812

ROSE services and associated APDUs

ROSE Service	Associate APDUs	Relate Underlying Service
RO-INVOKE	ROIV	P-DATA
RO-RESULT	RORS	P-DATA
RO-ERROR	RORE	P-DATA
RO-REJECT-U	RORJ	P-DATA
RO-REJECT-P	RORJ	P-DATA

3.5.4 Common management information

Network management applications shall use the Common Management Information Service Element (CMISE).

3.5.4.1 Services profile

The CMISE service description is detailed in ISO 9595-1 version 2 [5]. The CMISE services are listed in Table 8.

Multiple object selection, filter and multiple reply functional units as defined in ISO 9595-1 version 2 [5] are optional. Their use is application dependent. The negotiation during association establishment to use or not use the functional units shall be supported.

Support of the extended service functional unit defined in ISO 9595 [5] is not required for conformance to this Recommendation and negotiation shall be supported, at association establishment, for its non-use.

TABLE 8/Q.812

CMISE services

Service	Type
M-EVENT-REPORT	Confirmed/non-confirmed
M-GET	Confirmed
M-SET	Confirmed/non-confirmed
M-ACTION	Confirmed/non-confirmed
M-CREATE	Confirmed
M-DELETE	Confirmed
M-CANCEL-GET	Confirmed

3.5.4.2 Protocol profile

Implementations shall support those operations defined in ISO 9596-1 version 2 [9], that are required by specific applications. All mandatory parameters defined in ISO 9596-1 version 2 [9] for the required operations are mandatory parameters for this Recommendation.

4 Upper layer profile for file transfer type functions

The profiles for each layer are the same as described in clause 3; this clause only documents the differences required for FTAM support.

4.1 Session layer profile

4.1.1 Service profile

4.1.1.1 Functional units

Four session layer functional units (FUs) are required in this Recommendation:

1) Kernel;
2) Duplex;
3) Minor Synchronize;
4) Resynchronize.

Restrictions applied to parameters and their values are the same as specified in 3.3.2.

4.1.2 Protocol profile

4.1.2.1 Parameters

All mandatory parameters defined in Recommendation X.225 for the SPDUs required by the Kernel, Duplex, Minor Synchronize and Resynchronize FUs are mandatory parameters for this Recommendation.

4.1.2.2 Session Protocol Data Units

Session Protocol Data Units (SPDUs), associated with the Kernel, Duplex, Minor Synchronize and Resynchronize, shall be supported as described in Table 9.

TABLE 9/Q.812

Session PDU

(1) Connect	(CN SPDU)
(2) Accept	(AC SPDU)
(3) Refuse	(RF SPDU)
(4) Finish	(FN SPDU)
(5) Disconnect	(DN SPDU)
(6) Abort	(AB SPDU)
(7) Abort Accepted	(AA SPDU)
(8) Data Transfer	(DT SPDU)

4.2 Application layer profile

4.2.1 Application layer architecture

The description of ACSE and FTAM as part of the application layer architecture is to be provided.

4.2.2 File transfer, access and management

The FTAM conforms to the service definition and protocol specification in ISO 8571 [26-29]. Restrictions applied to parameters and their values are specified in the following subclauses.

4.2.2.1 Service profile

The mandatory file service class is file transfer class.

In this class the following functional units are mandatory:

- the kernel functional unit;
- both the read and write functional units;
- the limited file management functional unit;
- the grouping functional unit;
- and, in the internal file service, the recovery functional unit and optionally the restart functional unit.

4.2.2.2 Protocol profile

The functional units of the file protocol are equivalent to the functional units of the supported service described above.

The functional units retained and their PDUs associated are listed in Table 10.

This file protocol assumes the session services described in 4.1.1.1 with the following details:

- the recovery or restart functional unit implicates the use of minor synchronize session service;
- the restart functional unit implicates in addition to minor synchronize session service the resynchronize session service.

4.2.2.3 Support of document types

The nature of the file structures to be transferred involves the use of the suitable document types.

Three types of file structures are retained:

- unstructured binary files;
- unstructured text files;
- sequentially ordered files (these files are made of a sequence of records without any possibility of having direct access to a given record, each record is made of fields of different type).

So three document types at least are mandatory:

- ISO FTAM unstructured text (FTAM.1);
- ISO FTAM unstructured binary (FTAM.3);
- NBS sequential file (NBS-6).

FTAM.1 and FTAM.3 are allowed by FTAM hierarchical file model defined in ISO 8571-2 as constrained by the unstructured constraint set.

NBS-6 is allowed by FTAM hierarchical file model defined in ISO 8571-2 as constrained by the sequential flat constraint set.

5 Conformance

To be provided.

TABLE 10/Q.812

FTAM functional units and PDUs associated

Name	Functional units
F-INITIALIZE request	Kernel
F-INITIALIZE response	Kernel
F-TERMINATE request	Kernel
F-TERMINATE response	Kernel
F-P-ABORT request	Kernel
F-U-ABORT request	Kernel
F-SELECT request	Kernel
F-SELECT response	Kernel
F-DESELECT request	Kernel
F-DESELECT response	Kernel
F-CREATE request	Limited file management
F-CREATE response	Limited file management
F-DELETE request	Limited file management
F-DELETE response	Limited file management
F-READ-ATTRIB request	Limited file management
F-READ-ATTRIB response	Limited file management
F-OPEN request	Read, write
F-OPEN response	Read, write
F-CLOSE request	Read, write
F-CLOSE response	Read, write
F-READ request	Read
F-WRITE request	Write
F-DATA-END request	Read, write
F-TRANSFER-END request	Read, write
F-TRANSFER-END response	Read, write
F-CANCEL request	Read, write
F-CANCEL response	Read, write
F-BEGIN-GROUP request	Grouping
F-BEGIN-GROUP response	Grouping
F-END-GROUP request	Grouping
F-END-GROUP response	Grouping
F-RECOVER request	Recovery
F-RECOVER response	Recovery
F-RESTART request	Restart
F-RESTART response	Restart

References

[1] CCITT Recommendation *Principles for a Telecommunications Management Network (TMN)*, Rec. M.3010.

[2] CCITT Recommendation *Reference Model of Open System Interconnection for CCITT Applications*, Rec. X.200 (see also ISO 7498; first edition 1984-10-15).

[3] ISO 8348/Addendum 1 *Information processing systems – Data communications – Network service definition, Addendum 1: Connectionless-mode transmission*, April, 1987.

[4] CCITT Recommendation *Presentation Service Definition for Open System Interconnection for CCITT Applications*, Rec. X.216 (ISO 8822).

[5] ISO 9595-1 version 2 *Information Processing Systems – Open Systems Interconnection – Common Management Information Service Definition (CMIS)*.

[6] CCITT Recommendation *Remote Operations: Model, Notation and Service Definition*, Rec. X.219 (see also ISO IS 9072-1).

[7] CCITT Recommendation *Specification of Abstract Syntax Notation One (ASN.1)*, Rec. X.208 (see also ISO 8824).

[8] CCITT Recommendation *Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*, Rec. X.209 (see also ISO 8825).

[9] ISO 9596-1 version 2 *Information Processing Systems – Open Systems Interconnection – Common Management Information Protocol Specification (CMIP)*.

[10] CCITT Recommendation *Remote Operations: Protocols Specification*, Rec. X.229 (see also ISO IS 9072-2).

[11] CCITT Recommendation *Association Control Service Definition for Open System interconnections for CCITT applications*, Rec. X.217.

[12] CCITT Recommendation *Association Control Protocol Specification for Open System interconnections for CCITT applications*, Rec. X.227.

[13] CCITT Recommendation *Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit*, Rec. X.25.

[14] ISO 8208 *Information Processing Systems Data Communications – X.25 Packet Level Protocol for Data Terminal Equipment*, 1987.

[15] ISO/IEC 8073/AD 1 *Information Processing Systems - Open Interconnection – Connection Oriented Transport Protocol Specification - Addendum 1 - Network Connection Management Sub-protocol*, 1988.

[16] CCITT Recommendation *Transport Service Definition for Open Systems Interconnection for CCITT Applications*, Rec. X.214 (ISO 8072).

[17] CCITT Recommendation *Transport Protocol Specification for Open Systems Interconnection for CCITT Applications*, Rec. X.224 (ISO 8073).

[18] ISO 8072 *Information Processing Systems – Open Systems Interconnection – Transport Service Definition*, 1986.

[19] ISO/IEC 8073 *Information Processing Systems – Open Systems Interconnection – Connection-Oriented Transport Protocol Specification*, 1988.

[20] ISO/IEC 8073/AD 2 *Information Processing Systems – Open Systems Interconnection – Connection-Oriented Transport Protocol Specification – Addendum 2: Class 4 Operation over Connectionless Network Service*, 1988.

[21] CCITT Recommendation *Session service definition for Open System Interconnection (OSI) for CCITT applications*, Rec. X.215. (ISO 8326, 8326/AD 1, 8326/AD 3.)

[22] CCITT Recommendation *Session Protocol Specification for Open System Interconnection (OSI) for CCITT applications*, Rec. X.225. (ISO 8327, 8327/AD 1, 8327/AD 3.)

[23] CCITT Recommendation *Presentation Protocol specification for Open System Interconnection for CCITT Applications*, Rec. X.226. (ISO 8823.)

[24] ISO IS 9545 *Information Processing Systems, Open System Interconnection and Application Layer Structure (ALS)*, 1989.

[25] ISO TR 10172 *Information Processing System – Data Communications – Network/Transport Protocol Inter-working Specification.*

[26] ISO 8571-1 *Information Processing Systems – Open Systems Interconnection – File Transfer, Access and Management – Part 1: General Introduction*, 1988.

[27] ISO 8571-2 *Information Processing Systems – Open Systems Interconnection – File Transfer, Access and Management – Part 2: Virtual Filestore Definition*, 1988.

[28] ISO 8571-3 *Information Processing Systems – Open Systems Interconnection – File Transfer, Access and Management – Part 3: File Service Definition*, 1988.

[29] ISO 8571-4 *Information Processing Systems – Open Systems Interconnection – File Transfer, Access and Management – Part 4: File Protocol Specification*, 1988.