ATNP/WG3/WP 16-15

ATNP/WG1/JSG-SM/WP 11-15

Version DRAFT 1.3 (MS Word 6/7)
1 March 1999

AERONAUTICAL TELECOMMUNICATION NETWORK PANEL

WORKING GROUP 1 (System Planning and Concepts)

Joint Sub Group on System Management

ATN Systems Management

Draft SV6 Guidance Material

Editor: A. J. Kerr

SUMMARY

This is the draft ATN Systems Management Guidance Material relating to Sub-Volume 6 of the ICAO Manual prepared by the ICAO Aeronautical Telecommunication Network Panel (ATNP).

This working draft is an update based on developments in the System Management subgroup since June 1998. It should be noted that the whole area of MIB standardisation is under review, and the provisions in this draft may change fundamentally when the Concept of Operations for ATN systems management stabilises. The Working Group is invited to review this document and to provide comments for inclusion in the next version.

CONFIGURATION SHEET

Title : ATN Systems Management -
Sub-Volume 6 Guidance Material

Version : DRAFT 1.3 (MS Word 6/7)

Date: 1 March 1999

Contact: Sub-Volume editor: Tony.Kerr@ecsoft.co.uk
JSG chairman: Moulton@mailons.ons.com

Status: Draft

Change History :

Version	Description	Affected Parts	Date
0.1	Initial outline for SG3 review	All	07/10/97
0.2	Minor updates from WG3/SG3 Toulouse meeting. Presented at WG3-11 Redondo Beach, October 1997	All	24/10/97
1.0	First substantive version. Input to WG3-12, Rio de Janeiro, March 1998	All	March 1998
1.1	Updated working draft incorporating editing instructions from WG3-12. Input to WG3-13, Utrecht, June 1998	All	June 1998
1.2	Updated working draft reflecting discussions of JSG-SM. SARPs and GM split into 2 documents. Input to ATNP WG meetings, Honolulu, January 1999.	All	December 1998
1.3	Post Honolulu. Editorial cleanup. MOs replaced with references to Convergent MIB. Transport layer mapping added.	All	March 1999

Preface

This draft represents work in progress within the ICAO ATNP Working Groups and should not be taken as stable. It should be noted that the whole area of MIB standardisation is under review, and the guidance in this draft may change fundamentally when the Concept of Operations for ATN systems management stabilises.

This draft is based on the following assumptions:

a) that System Management (including in scope both Network Management, Applications and higher level functions) will be essential for world-wide ATN operation.

b) that cross-domain management will be required, and therefore Provisions are required to ensure interworking between management domains. Within domains, system management is a local issue.

c) that system management data traffic will flow over the air-ground data link, if not in the short term then at some time in the future. The management protocol must therefore not preclude such traffic.

d) that a flexible, extensible System Management infrastructure is needed, as it is not possible to predict all future System and Network Management scenarios.

e) that a Concept of Operations for ATN Systems Management will be defined, and this will specify the operational requirements more closely.

This Working Draft contains the draft technical Guidance Material corresponding to Sub-Volume 6 of the ATN ATN Technical Provisions. As this document reaches maturity, it will be forwarded for inclusion in the Comprehensive ATN Manual (CAMAL). Note that the Guidance Material included here is technical material which relates directly to the technical provisions - it does not include the Operational Requirements nor the Concept of Operations, which are assumed to be defined elsewhere.

Cross-references:

[1] Draft Sub-Volume 1 and Core Guidance Material

[2] Draft ATNSI CONOPS

[3] Draft ACI/ProATN Convergent MIB

Table of Contents

ATN SYSTEMS MANAGEMENT GUIDANCE MATERIAL

1. INTRODUCTION

Note.— Chapter 1 contains introductory material and an overview of the Guidance Material structure.

1.1 Scope and Objectives

The ICAO ATN Panel instructed its Working Groups to identify and define standards and recommended practices (SARPs) necessary for the management and administration of the ATN and its hosted applications.

The ATN System Management Guidance Material presented here is intended to assist States in their technical planning for ATN System Management deployment, as well as aiding implementors to understand the rationale behind the technical provisions.

There are no requirements or recommendations (shalls or shoulds) in this Guidance Material.

A MIB structure is proposed which will provide a capability for domain management in order to monitor and maintain the Quality of Service (QoS) offered by the ATN infrastructure to its hosted applications. Implementation of the detailed MIB exactly as presented is not mandated.

1.2 Structure of ATN Systems Management Guidance

There are several distinct aspects to the ATN systems management guidance presented here. This material is structured as follows:

a) Introduction (1) describes the purpose and structure of the ATN Systems Management guidance material.

b) Naming and Addressing Guidance (2) gives guidance on constructing and navigating the Management Information Base (MIB) and identifying particular attributes within individual Managed Object (MO) instances, or groups of MOs.

c) Management Information Guidance (3) contains general material related to the method used to define management information in terms of MOs, MO Classes, and MIB structure (inheritance and containment hierarchies) and specifies conventions which are used in the rest of the management information material..

d) Managed Objects for ATN Applications (4) gives guidance on MOs for ground-ground and air-ground ATN Applications, including MOs for ATN systems management applications (CMIP) and MOs for ATN upper layers (Session, Presentation, ACSE, ATN-App-AE).

e) Managed Objects for ATN ICS (5) gives guidance on the set of MOs required for management of the ATN Internet Communications Service in order to ensure that the required QoS metrics can be observed.

f) Detailed Technical Guidance and Rationale (6) explains some of the choices that have been made in selecting the two ATN systems management communication profiles, and gives technical guidance to planners and implementors. It includes a description of scenarios for accommodating and interworking with various other systems management approaches that may be adopted internally within management domains.

1.3 Systems Management Functionality

ATN systems management is based on the ISO/IEC and ITU-T international standards for OSI management.

Editor's note.— This section will provide an overview of ATN systems management functionality, i.e. the management framework and what can be exchanged between Manager and Agent Processes. Such an overview currently resides in the draft Guidance Material for Core/SV1 Systems Management - WG1-10 WP 16.

The OSI Systems Management framework has been chosen to standardise the ATN SM application. The OSI SMA based on the OSI Basic Reference Model is conceptualised by an application entity relying on the connection-oriented communication service offered by the OSI presentation service provider. The System Management Application Entity (SMAE) is the component of the SM Application carrying out the communication activities between remote SM entities.

The SMAE comprises three ISO-specified ASEs: the ACSE for the establishment and the control of the application-associations, the CMISE providing the basic SM operations for handling remotely managed objects and the ROSE supporting the concept of remote operations. Other ASEs may be included to support the protocols related to specific SM Functions.

2. NAMING AND ADDRESSING GUIDANCE

Editor's note.— To be defined. This chapter will contain guidance on Managed Object addressing and registration requirements. It will specify the requirements for navigating the Management Information Base and identifying particular attributes within individual Managed Object (MO) instances, or groups of MOs.

3. MANAGEMENT INFORMATION GUIDANCE

Editor's note.— Provisions for encoding MO attributes in PER need to be considered. Potentially all MOs need to be augmented with PER-visible constraints and extensibility markers.

ATN Management Information is defined by specifying:

a) the containment (naming) hierarchy of the MO Classes that characterise the ATN MIB.

b) the inheritance hierarchy of the defined MO Classes.

c) the MO Class definition of ATN MOs, using a simplified MO template

d) the action type operations on the attributes of ATN MOs that are available to ATN System Management.

3.1 Symbols, abbreviations and terms

In each MO table, the "ISO Status" column indicates the conformance requirement as specified in the ISO/IEC base standard that defines the MO. A hierarchy exists, so that the conformance requirements of a dependent feature only apply if the "parent" feature is supported (e.g. if an MO class is not supported, then none of the attributes will be supported, even if classified as "M"). Possible values for ISO Status are:

M - Mandatory to implement

O - Optional to implement

C - Dependent upon some Condition explained in a footnote to the table

A - Feature is ATN-specific, i.e. not present in base standard.

The "ATN Status" column indicates the conformance requirement as specified in the ATN Provisions. Notes may be used to expand on the support requirement, e.g. to differentiate between different types of ATN system. Possible values for ATN Status are:

M - Mandatory to implement (equivalent to a "shall" statement)

R - Recommended to implement (equivalent to a "should" statement)

O - Optional to implement (i.e. an implementation is free to implement the feature or not)

X - Prohibited to implement.

3.2 Global Containment Tree for One System

The upper part of the global containment tree (naming hierarchy) for one system is as illustrated in Figure 3-1.

Note.— The subordinate nodes in the containment tree are defined in subsequent chapters.

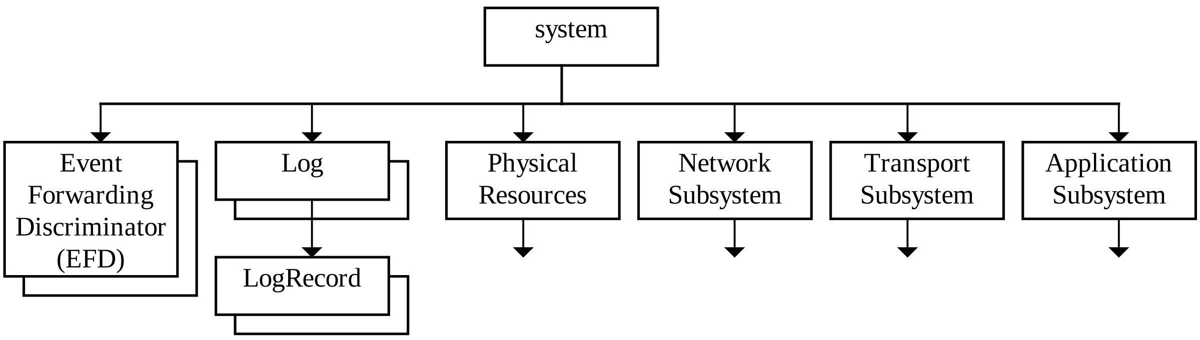

Figure 3-1. Global MO Containment Tree for One System

3.3 "System" MO Classes

The generic attributes "**objectClass**", "**nameBinding**" and "**packages**" (inherited from "**top**") are implicitly included in every object class; thus they are not shown in other MO classes.

4. MANAGED OBJECTS FOR ATN APPLICATIONS

Note 1.— This chapter contains guidance on MOs for ground-ground and air-ground ATN Applications, including MOs for ATN systems management applications (CMIP) and MOs for ATN upper layers (Session, Presentation, ACSE, ATN-App-AE).

Note 2.— Systems management in the applications can be used:

a) to monitor the quality of service available to end-users,

b) to convey alarms to notify equipment failures and other exception conditions

Note 3.— Analysis of the applications has determined where systems management could be useful in monitoring the QoS as seen by end-users. For example, for ADS, statistical information could be gathered on the operation of ADS contracts (contract type, reporting rate, etc.) which would allow some optimisation of communications bandwidth. For CM, the response time to complete a Logon operation at various ground centres can be monitored, and any anomalies identified.

Note 4.— Systems management may be utilised to convey alarms to notify equipment failures and other exception conditions. For example, in ADS the validity and availability of data required in an ADS Report may be called into question if there is a failure after the contract has been agreed. Systems management notifications could be used to report the failure, thus allowing remedial action to be taken.

Note 4.— Configuration related MOs are considered out of the scope of the standardisation. The resources to be configured and the way they are configured (management protocol, file exchanges, etc...) is defined on a management domain basis. As configuration parameters are not supposed to be exchanged between system management authorities, no standardisation is required in this area.

4.1 Summary of Managed Object Classes

The following managed object classes are defined for the ATN Application layer:

- applicationSubsystem
- aTNcMae
- aTNcMaeInstance
- aTNaDSae
- aTNaDSaeInstance
- aTNaRFae
- aTNaRFaeInstance
- aTNcPDLCae
- aTNcPDLCaeInstance
- aTNfISae
- aTNfISaeInstance
-

Editor's Note.— MOs for ground-ground applications (ATSMHS, AIDC) are To Be Defined.

4.2 Containment hierarchy

The containment hierarchy is illustrated in Figure 4-1. Managed Objects which can have multiple instances are illustrated by shadowed boxes. These objects are defined in detail in the following sections.

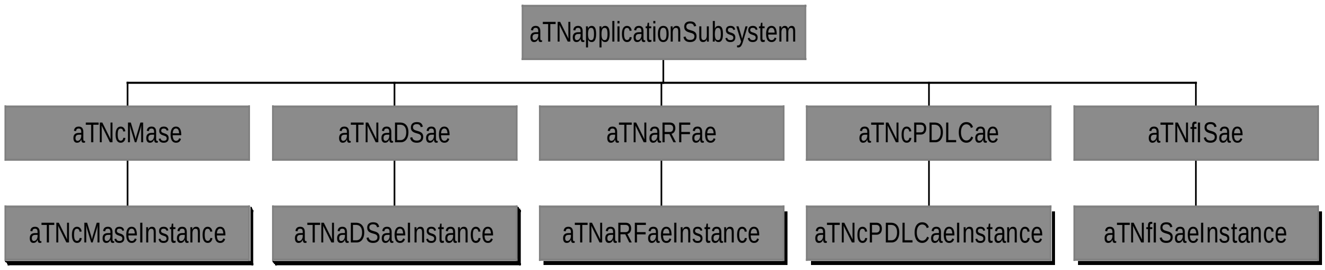

Figure 4-1. Containment Sub-tree for Air-Ground Application MOs

The two levels of MOC identified in the containment hierarchy **-** i.e. AE MOC and AE Instance MOC **-** allow for distinguishing between management of the static aspects of the ATN application entities and dynamic aspects related to application association (e.g., per invocation).

Editor's Note.— Previous drafts of this document contained detailed MO definitions corresponding to the above containment tree. ***The MOs for the ATN Applications were extracted from WG3/ WP12-11: "Elements of management information related to the ATN application layer" by F Picard. These MO templates*** *have been removed from this version because:*

a) *they are now considered to be out of date as they have not been maintained for some considerable time;*
b) *they were not "Summary MIB" MOs, rather proposed MOs for a single ATN End System;*
c) *the requirements leading to the MO definitions had not been validated;*
d) *it is not agreed within ATNP working groups that it is appropriate to include MO definitions in the ICAO material, as it may inadvertently constrain implementations unnecessarily.*

The best current example of an ATN MIB is considered to be the ProATN/ACI "Convergent MIB" V1.4. Work is in progress to validate the MOs defined in the Convergent MIB against the identified system management requirements.

4.3 Managed Objects for Systems Management Applications

ISO 10165-9, "Systems management protocol machine managed objects" is under development within ISO, and should be assessed for utility within the ATN architecture.

5. MANAGED OBJECTS FOR ATN ICS

Note 1.— For OSI lower layers, there exist a number of international standards which specify MOs for layer management. These standardised MOs have been adapted and extended for ATN management.

Editor's note.— The MOs defined here may move to the ICS Sub-Volume in due course, but for now this chapter serves as a "home" for these systems management requirements without disrupting the CNS/ATM-1 Provisions.

5.1 Introduction

5.2 Elements of Management Information for ATN Transport Layer

Editor's Note.— This working draft only covers system management aspects pertaining to fault and performance management. Accounting and Security management for the ATN Transport Layer will be considered in a future version of this document.

Note 1.— Configuration management is a system management functional area that has been considered to be out of the scope of the ATN provisions.

5.3 Summary of managed objects

The following set of managed object classes are defined for the ATN Transport layer:

- aTNtransportSubsystem
- aTNtransportEntity
- aTNcomodeTPM
- aTNtransportConnection
- aTNclmodeTPM

5.4 Containment hierarchy

The containment hierarchy is illustrated in Figure 5-1. Managed Objects which can have multiple instances are illustrated by shadowed boxes. These objects are defined in detail in the following sections.

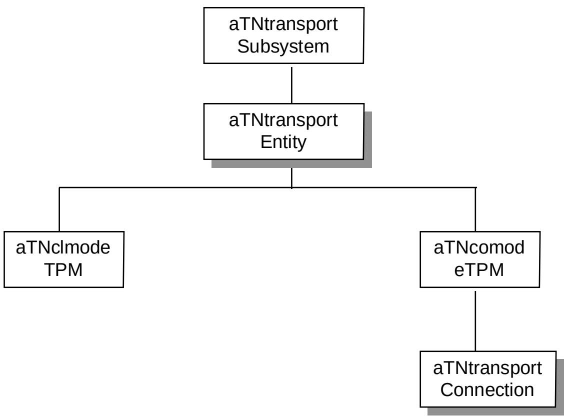

Figure 5-1. Containment Sub-tree for ATN Transport layer MOs

Editor's Note.— Previous drafts of this document contained detailed MO definitions corresponding to the above containment tree. ***The MOs for the ATN Transport Layer were extracted from WG2/14 WP 441: "Elements of management information related to the ATN transport layer" by S. Tamalet. These MO templates*** *have been removed from this version because:*

a) *they are now considered to be out of date as they have not been maintained for some considerable time;*
b) *they were not "Summary MIB" MOs, rather proposed MOs for a single ATN End System;*
c) *the requirements leading to the MO definitions had not been validated;*
d) *it is not agreed within ATNP working groups that it is appropriate to include MO definitions in the ICAO material, as it may inadvertently constrain implementations unnecessarily.*

The best current example of an ATN MIB is considered to be the ProATN/ACI "Convergent MIB" V1.4. Work is in progress to validate the MOs defined in the Convergent MIB against the identified system management requirements.

5.5 Elements of Management Information for ATN Network Layer

Editor's Note.— *This working draft only covers system management aspects pertaining to fault and performance management. Accounting and Security management for the ATN Network Layer will be considered in a future version of this document.*

Note 1.— Configuration management is a system management functional area that has been considered to be out of the scope of the ATN provisions.

5.6 Summary of managed objects

The following set of managed object classes are defined for the ATN Network layer:

- aTNnetworkSubsystem
- aTNnetworkEntity
- aTNcLNS
- aTNlinkage
- aTNmobileConnection
- aTNfIB
- aTNidrpConfig
- aTNadjacentBIS
- aTNrIB
- aTNiSSME
- aTNmobileAdjacency
- x25PLE-DTE
- virtualCall-DTE

Editor's Note.— Text to be extracted from the latest version of ATNP/WG2 WP "Elements of management information related to the ATN network layer" by S. Tamalet. *In fact, the best current example of an ATN MIB is considered to be the ProATN/ACI "Convergent MIB" V1.4. Work is in progress to validate the MOs defined in the Convergent MIB against the identified system management requirements.*

6. DETAILED TECHNICAL GUIDANCE AND RATIONALE

6.1 Communications Protocols

A profile is a selected set of standards with various choices made for those elements which are optional in the standards. The aim of this section is to consider the requirements for communications profiles for general ATN systems management, and to define the provisions necessary for ATN standardisation.

Two distinct non-interoperable communication profiles are specified for ATN systems management:

a) There exist well-defined internationally standardised communication profiles for general systems management, and one such profile is specified in Sub-Volume 6. This is the default systems management profile for general ground-ground inter-domain management communication, and must be supported by all boundary management systems.

b) For air-ground management communication, a lightweight efficient protocol mechanism is specified in order to optimise the use of the bandwidth-limited air-ground data links. This can also optionally be used for ground-ground management communication.

6.1.1.1 Summary of Requirements

It is necessary to produce key technical provisions and guidance material which:

a) Define a CMIP communications profile based on identified functional requirements for ATN systems management, bearing in mind the need for future extensibility and the potential for interworking both with existing CMIP products and with other systems management technologies. It is probable that one of the existing internal standardised profiles AOM 1x will satisfy these requirements.

b) For bandwidth-limited environments, such as mobile subnetworks, define a mapping of the selected profile to the efficient upper layer protocol stack specified in the ULCS Provisions, which in turn maps to the lower layer stack specified in the ICS Provisions.

c) Specify a presentation context and a new application context based on PER encoding of all systems management and ACSE APDUs.

Note.— The existence of COTS products implementing the CMIP profile must be taken into consideration.

6.1.2 Default Inter-domain Standard CMIP profile

To maximise the use of established management software solutions, an international standardised profile (ISP) is adopted for cross-domain ground-ground management communications using CMIP. This is adapted slightly for use over the ATN Transport Service rather than the standard OSI Transport Service.

The candidate ISPs which could potentially be adopted for ATN system management are ISO/IEC ISP 11183 parts 1 and 2.

ISO/IEC ISP 11183-1 specifies how the Association Control Service Element (ACSE), the Presentation layer and the Session layer are used to provide the required upper layer functions for the CMISE/ROSE functions. In addition, requirements for abstract and transfer syntax handling are specified.

Part 2 of ISP 11183 specifies how the OSI Common Management Information Service Element (CMISE) combined with the OSI Remote Operation Service Element (ROSE) are used to provide the complete set of operation and notification services to the CMISE-service-users of two end systems. It specifies the CMIP / ROSE protocol features for the definition of the Enhanced Management Communications profile, identified as AOM 12.

Part 2 of ISP 11183 defines the support level of all of the OSI management communication features needed by implementations, and it includes the common Part 1 provisions by reference. It specifies general purpose management communication capabilities by requiring the support of all CMIP Functional Units (FUs) except the extended services FU.

The support of the complete set of operation and notification services, and of the corresponding protocol elements does not imply that all these features must be used in all instances of communications. The selection of the features depends on the needs and dynamic requirements of the CMISE-service-users who may choose between:

- application entity roles
- functional units
- operation / notification services
- optional parameters.

6.1.3 Efficiency-enhanced “FastMIP” profile

For systems management communication between ground-based manager applications and airborne agent applications, or vice-versa, an efficient data encoding mechanism and minimal protocol overheads are required. The efficiency-enhanced CMIP profile defined for the ATN is designated the “FastMIP” profile, to distinguish it from the default “Full CMIP” profile.

In summary, the "FastMIP" protocol stack consists of utilising the "Fast Byte" stack specified in the ULCS Provisions. This requires the short connect / null encoding options of Session and Presentation layers, PER-encoded ACSE edition 2, and PER-encoded application information.

The rationale for this decision is based on a number of factors, including:

a) bit-efficient protocol for limited bandwidth air-ground datalinks,

b) avoidance of multiple parallel protocol stacks in ATN systems,

c) simplified certification requirements,

d) compatibility with the existing air-ground applications,

e) lightweight ATN upper layers in ISs.

ATN applications in general are specified to utilise the protocol stack defined in the Internet Communications Service (ICS) and Upper Layer Communications Service (ULCS) provisions. There are requirements:

a) to avoid multiple protocol stacks in ATN systems, and

b) to use highly bit-efficient protocols over mobile subnetworks.

Therefore, for ATN systems management, a CMIP profile is required which is based on the ULCS and ICS provisions.

Existing international standardised profiles (ISPs) for the OSI systems management protocol CMIP (e.g. references [2] and [3]) assume that:

a) basic session and presentation layer functionality is present, and

b) CMIP and ACSE APDUs are encoded for transfer using the Basic Encoding Rules of ASN.1.

Neither of these assumptions is true for the profile defined in Sub-Volume 4 for the ATN ULCS.

The ISPs also assume a standard connection-oriented Transport service, and as such there is no provision for ATN-specific parameters defined in Sub-Volume 5 for the ATN ICS, such as traffic type and class.

The ULCS provisions specify that all data transferred between applications uses the Packed Encoding Rules (PER) for information which is defined using the ASN.1 notation. The CMIP standard assumes that ASN.1 Basic Encoding Rules (BER) will be used. Hence, the CMIP abstract syntax definitions are not currently specified to take full advantage of ASN.1 extensibility features and optimal PER encoding. To this end, it may be necessary to augment CMIP and ROSE ASN.1 definitions to add PER-visible constraints and extensibility markers.

The following steps are necessary:

- If major efficiency gains can be made, augment the CMIP abstract syntax specification in ISO/IEC 9596-1 with PER-visible constraints and extensibility markers, in order to allow optimal encoding efficiency and provision for backwards compatibility in the future.
- Specify that CMISE APDUs are to be encoded for interchange using PER.
- Specify MO attribute syntaxes using PER-visible constraints and extensibility markers
- Specify that attribute values are to be encoded for interchange using PER
- As ULCS supports only a single presentation context, ensure that a mechanism is in place to distinguish PDUs from different abstract syntax modules.

6.1.3.1 Extensibility and Encoding

The ATN profile requires the following features:

a) The abstract syntax module defined in clause 9 of the ACSE protocol specification is augmented with the ASN.1 extensibility notation, as specified in ISO/IEC 8650-1 Amendment 1.

b) The system supports that encoding which results from applying the ASN.1 packed encoding rules (basic, unaligned variant), as specified in ISO/IEC 8825-2, to the abstract syntax module specified in ISO/IEC 8650-1 Amendment 1.

c) Packed encoding rules (basic, unaligned) are used for encoding all ACSE Protocol Control Information (PCI) for interchange.

The encoding issue thus applies at two levels:

a) the encoding of CMIP/ROSE/ACSE APDUs, and

b) the encoding of the MIB information.

6.1.3.1.1 Encoding of CMIP/ROSE APDUs

Given the existing ULCS architecture, the "Fast Byte" presentation profile requires all presentation data to be taken from a single presentation context. This implies that all application data must be treated as part of a single abstract syntax definition. The ULCS Provisions contain mechanisms for routing received application data to the correct ASE, which are independent of the presentation context.

6.1.3.1.2 Encoding of Embedded Management Information

The CMIP syntax encapsulates MO information by means of definitions such as:

```
Attribute ::= SEQUENCE {
        attributeId             AttributeId,
        attributeValue      ANY DEFINED BY attributeId
}
```

The actual type used in the ANY DEFINED BY will depend upon the definition of the attribute. For example, a counter attribute may be defined as an INTEGER type, in which case the transfer syntax would be a PER-encoded unconstrained INTEGER value.

In principle it would be possible to re-define all attributes to have EXTERNAL syntax at the CMISE level. This could then encapsulate the attribute value encoded using BER. In this way, standard BER could be used by the Manager and Agent applications. However, there are a number of drawbacks:

a) non-standard attribute definitions,
b) loss of encoding efficiency,
c) dual encoder/decoders per SM stack.

This approach is therefore rejected, and it is assumed that the management information in the MIB will belong to the same presentation context as used for ACSE and other ATN applications.

6.1.3.2 Suitability of Existing International Standardised Profiles

As discussed for the Full CMIP proofile above, the candidate ISPs which could potentially be adopted for ATN system management are ISO/IEC ISO 11183 parts 1 and 2.

ISP 11183-1 is based on a full OSI upper layer stack. It does not take into account the efficiency option of the presentation and the session protocols, nor does it take into account the second edition of the ACSE protocol. ISP 11183-1 section 8 requires ISP conforming systems to encode PDUs with the Basic Encoding Rules. ISP 11183-1 does not require the compliance to ISO/IEC 8650-1 Amendment 1.

The ISP requires conforming implementation to support at least 2 simultaneous presentation contexts. The ATN specification is non-conformant to the ISP proforma, in that only one presentation context is supported. In the case of the System Management Application, the presentation context should identify a single abstract syntax formed by ACSE and ROSE/CMISE abstract syntaxes and a single transfer syntax.

Reference [6] compares ISP 11183-1 with the functionality specified in the ULCS Provisions and concludes that the efficient ULCS profile is capable of supporting either of the AOM 11 and AOM 12 CMIP profiles. It also proposes an extension to the current ISP 11183-1 which would include this new protocol functionality.

It has thus been shown in [6] that the ULCS Provisions fully support ISP 11183-2 (AOM 12) for CMIP support.

6.1.3.3 Changes Required to AOM 12

Having selected an ISP, the specification of the FastMIP stack still needs some additional detailed work. It has been shown [6] that the internationally standardised AOM 12 profile can be used, if references to ISP 11183-1 (ACSE, presentation and session for use by CMISE/ROSE) are replaced by references to the ICAO ULCS stack.

Some optimisation of AOM 12 will also be required. For example, the CMIP standard defines the following type to identify MO attributes:

```
AttributeId ::= CHOICE {
        globalForm      [0] IMPLICIT OBJECT IDENTIFIER,
        localForm       [1] IMPLICIT INTEGER
}
```

AOM 12 specifies that all MO attributes are identified using the global Object Identifier form. This entails a very large overhead for systems management operations which involve several separate attributes. For a specific application context, such as ATN systems management, it is permissible to define INTEGER values instead of Object Identifiers, and to use the localForm of identification, which is much more bit-efficient. However, the local form is defined in AOM 12 as "out of scope" for that profile.

The communication profile for ATN system management will therefore be as specified in ISO/IEC ISP 11183-2 (CMISE/ROSE for AOM 12) [3], with the following general modifications:

- All references to ISP 11183-1 to be replaced by references to the ULCS Provisions
- Local forms of identification to be allowed where this will make a large difference to the overhead.

6.2 Interworking Provisions

Note 1.— Requirements have been expressed for a systems management architecture which will accommodate and facilitate interworking with other management technologies such as SNMP. This could involve the definition of Proxies and interworking units.

Note 2.— One aspect of this is the specification of standard APIs which are independent of any particular technology. Thus, requirements for standard Systems Management interfaces (APIs, Data Formats and Protocols) *should be explored, and documented in this chapter (may be empty). Guidance should be developed on the implementation of a Systems Management API based on industry standards (e.g. X/Open).*

6.2.1 Dual-Stack Managers

The decision to use an efficiency-enhanced communications protocol stack for ATN management implies the need for bilingual Manager implementations, which will be able to manage both ATN-specific entities using the "FastMIP" protocols and also standard CMISE entities using the conventional CMIP stack. This is illustrated in the following Figure.

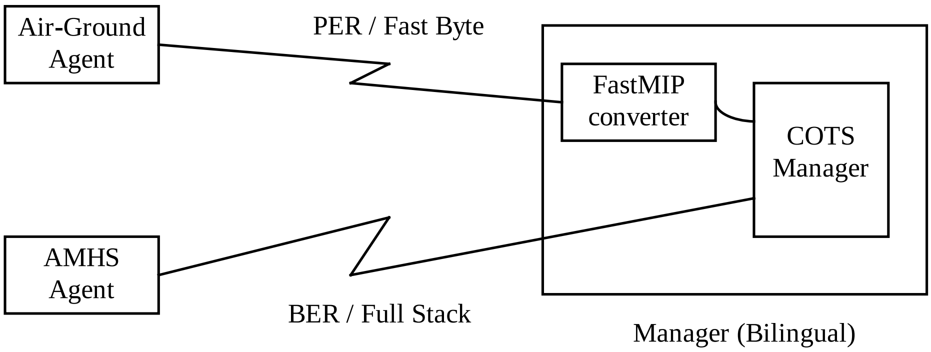

Figure 6-1. Co-existence of "FastMIP" and Standard CMIP Profiles

6.2.2 Integration of Manager Products with FastMIP ATN Agents

A large amount of the development of system manager applications is concerned not with the communications stack and attribute encoding but with the provision of sophisticated system management functions (e.g. fault management application) and the presentation of management information to the end user by means of ergonomic graphical interfaces. Thus, it is desirable for COTS manager products to be able to be used in the ATN system management environment.

A number of options have been investigated for utilising a typical COTS management application suite. The manager product is assumed to have suffiicient modularity to interface with different protocol stacks and management information encodings.

Four technical options have been analysed, all assuming that the airborne Agent has a FastMIP stack using PER (meaning that, given the MIB elements are encapsulated in the CMISE PDUs, that these MIB elements are PER encoded as well), as illustrated in Figure 6-2.

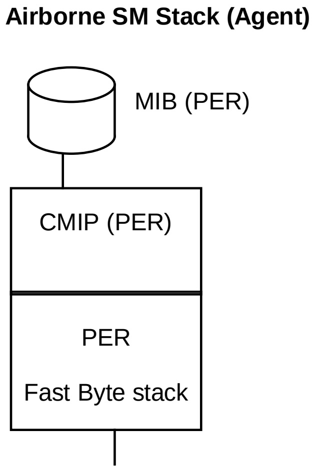

Figure 6-2. Airborne SM Stack

6.2.2.1 Option 0: PER-encoded MIB

In this option, the contents of the MIB would be exclusively encoded in PER in both Manager and Agent. For most COTS managers, this would probably require an expensive product modification, as these products are aimed at the market for traditional SM Managers which use BER encoding as defined in current standards, BER thus being pervasive throughout the Manager components.

Therefore the PER encoding defined for ATN management information must be decoded before it reaches the proprietary management applications, and management information generated by the proprietary manager applications must be re-encoded into the PER equivalent for transmission over ATN.

6.2.2.2 Option I: Full Application Gateway

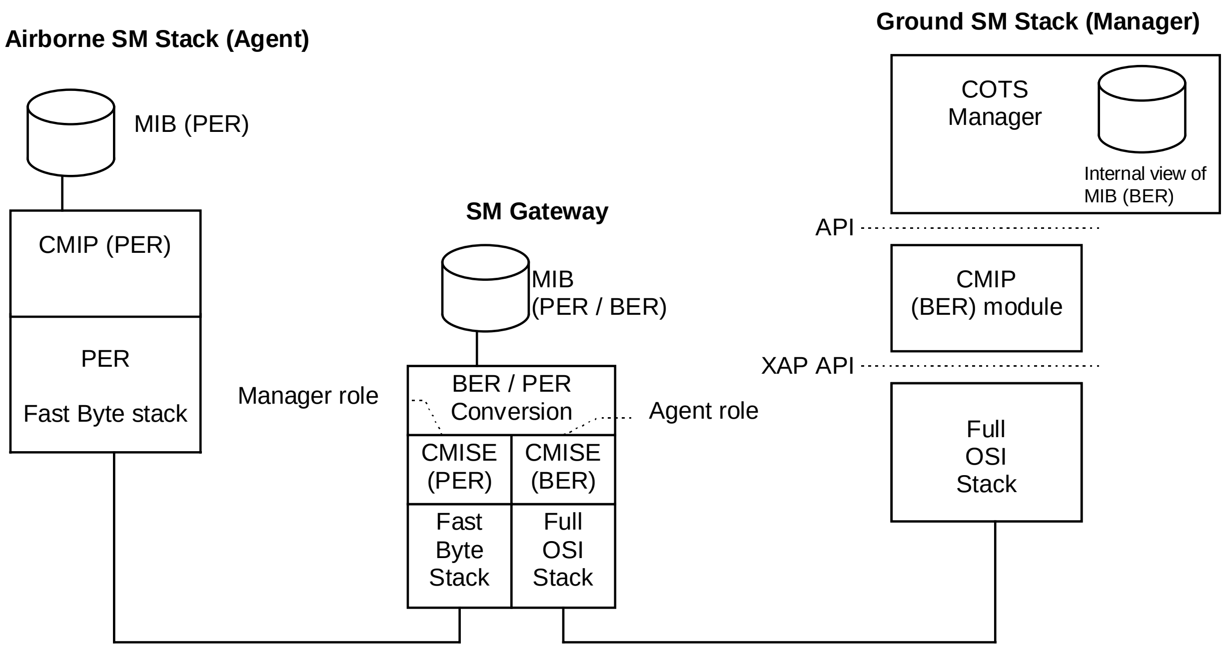

Figure 6-3. Ground SM stack - Option I: Full Application Gateway

In Option I, illustrated in Figure 6-3, a full application Gateway at CMISE level is produced, as a separate "Black Box". This requires no change at all to the COTS manager product, or the OSI/CMIP module. The Gateway appears to the Manager as a Full-Stack Agent, but is actually a proxy acting on behalf of the "real" remote Agent. The Gateway performs BER/PER conversion and acts in the Manager role towards the airborne Agent. It has an internal representation of the MIB in both PER and BER forms.

It should be noted that this Option requires the MIB and CMISE abstract syntaxes used in the COTS Manager product to be 100% compatible with those of the Gateway and Agent, meaning that, although the ASN.1 may be different to allow for encoding efficiency reasons, lossless conversion should be possible.

Advantages:

a) No change is required to existing manager products
b) Gateway design is independent of Manager architecture - can be used with different OSI Manager products

Disadvantages:

a) Likely high development/procurement costs
b) Inefficiency and complexity of dual stacks
c) Possible performance problems
d) Naming and addressing issues

6.2.2.3 Option II: Translation within CMISE

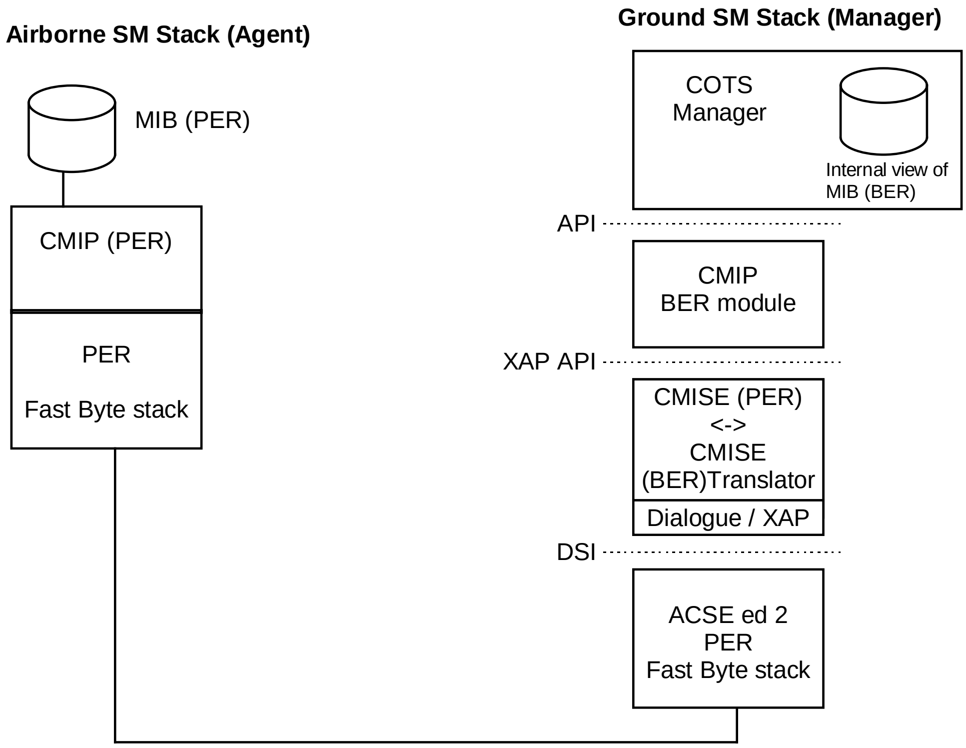

Figure 6-4. Ground SM stack - Option II: Translation within CMISE

In Option II, illustrated in Figure 6-4, the COTS module for CMIP/BER is used. Under the XAP interface, a CMISE translator is defined, converting between PER and BER at the CMISE level. Thus the MIB objects are retrieved/stored using BER and converted to/from PER within the translator. This would then run over a Provisions-compliant ULCS communications stack.

As with Option I, it should be noted that this Option requires the MIB and CMISE abstract syntaxes used in the Manager product to be 100% compatible with those of the translator and Agent, meaning that, although the ASN.1 may be different to allow for encoding efficiency reasons, lossless conversion should be possible.

Advantages:

a) Existing Agent Integrator is retained
b) Uses publicly available XAP interface

Disadvantages:

a) Solution is product-specific

6.2.2.4 Option III: Translation by CMISE User

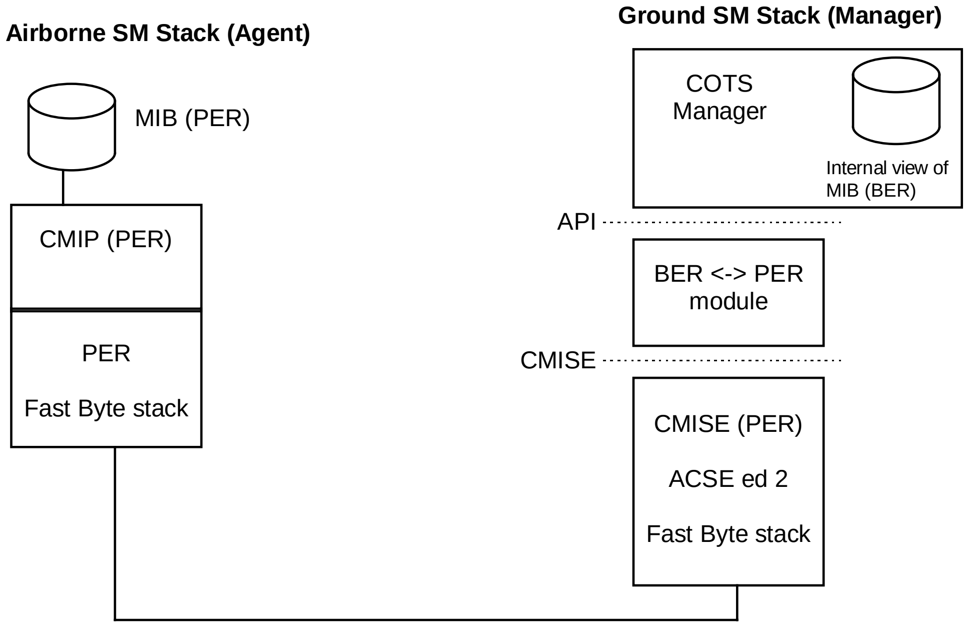

Figure 6-5. Ground SM stack - Option III: Translation by CMISE User

In option III, illustrated in Figure 6-5, a new COTS module is specified, which performs the BER - PER translation of the MIB elements, i.e. above the CMISE.

As with Options I and II, it should be noted that this Option requires the MIB and CMISE abstract syntaxes used in the Manager product to be 100% compatible with those of the Agent, meaning that, although the ASN.1 may be different to allow for encoding efficiency reasons, lossless conversion should be possible.

Advantages:

a) BER/PER conversion is done at the highest level, i.e. only for the MIB elements, emulating a PER-encoded MIB
b) Problem is contained in a single module

Disadvantages:

a) Solution is product-specific
b) SMK interface is not openly available
c) Likely cost implications of developing a new proprietary system manager component

6.3 Rationale for ATN Systems Management Architecture

The ATN System Management Application (SMA) is based on the internationally standardised OSI System Management Framework. The SM application allows remote management of resources of all kinds. The SM application provides the manager system with the capability to communicate with a managed system in order to manage a resource that is contained in or controlled by the managed system.

The Provisions for System Management in the ATN cover on the one hand the interface between manager and agent and on the other hand the identification of the managed object which must be accessible via System Management on ATN Intermediate Systems and End Systems.

In the OSI SM framework, manager and agent systems communicate with one another, using an OSI protocol stack and the application layer protocol CMIP. The protocol stack is denoted "Full-stack", in that the full functionality of both Session and Presentation protocols are assumed to be implemented.

In the ATN environment, the identification of the upper layers services required by the air-ground applications and the consideration of the constraints of the air-ground communication segment has led to the selection of a minimum upper layer stack, the "Fast Byte" stack, included as a base component of the ATN Upper Layer Architecture (ULA).

From this situation emerged the idea to specify the ATN SM application composed of the OSI service elements responsible for handling the application protocol (CMISE, ROSE and ACSE) and relying on the ATN upper layer stack (Fast Byte).

The different aspects of this option, identified as the “Fast MIP” solution, are discussed in the following subsections, which:

a) explain why the Full Stack is not always appropriate for supporting the communications of the ATN SM application,

b) recall the main characteristics of the ATN ULA. The objective is to check that the SM application is compatible with this architecture,

c) identify the most important tasks needed to port a Full Stack based SM application onto a Fast Byte stack.

The next section contains a comparison between the upper layer communication profile required by the full stack based SM application (ISP 11183-1) compared to the upper layer communication services effectively provided by the ATN upper layers.

The section after that analyses the possible internal architectures of the SM Application Entity.

6.3.1 Rationale for implementing the SMA on a "light" upper layer stack

The SM Application operates in connection-oriented mode, i.e. the application-association established by the CMIS-users is mapped onto a Presentation connection before that any management activity occurs.

In fact, the SMAE makes use of a limited set of Presentation services in order to open a connection and send data on this connection:

- The CMIS-user uses the A-ASSOCIATE, A-RELEASE and A-ABORT services from ACSE,
- CMISE requires services from ROSE only. It does not use Presentation services directly,
- ACSE uses the P-CONNECT, P-U-ABORT, and P-P-ABORT services, whilst ROSE uses the P-DATA service only.

Therefore, it is not necessary to implement the full presentation and session functions in the systems supporting the SM application. In particular, all the traditional Session services to handle synchronisation, activities, expedited data, etc. are not used. These functions were designed to support upper layer communication functionality for general-purpose applications (e.g. X.400, FTAM, etc). The already-defined ATN applications do not require these powerful functions (e.g. the session synchronisation and activity services or the presentation re-negotiation of presentation contexts). The integration of the SM application in the ATN routers and ES does not justify by itself the provision of the full presentation and session services. The additional services would lead to the installation of a dual-stack (full stack and fast byte stack) in the ESs and of a full stack in the ISs whereas the services of the full stack actually used for SM activities are limited to the services provided by the Fast Byte stack.

It should be noted that the SM application is unlike operational applications, in that the SM application is required to operate in degraded situations, i.e. when the use of certain resources becomes critical. Complex operations such as those provided by the full OSI session layer are not required during these periods of time. The establishment of the connection between the agent and the manager and the transmission of the data should be as efficient as possible. This is precisely the service offered by the ATN Upper Layer Stack.

In addition to these technical reasons which show that the full upper layer stack is not required by the OSI-based SM application[1], another consideration specific to the aeronautical environment is the problem of the certification of on-board systems. A full stack implemented for supporting the communication activities of the SM application would require to go through the complex and costly process of certification. Knowing that most of the implemented functions would not be used by the avionics, the effort needed for the certification does not seem justified.

6.3.1.1 ATN Upper Layer Architecture (ULA)

This section revisits the main characteristics of the ATN Upper Layer architecture. Comments in italics evaluate the impact of these characteristics on the ATN SM Application.

The ATN ULA provides a framework for the standardisation of ATN applications. This framework is based on the concept that a set of common communication services are provided by the "Upper Layer" on which ATN application protocols can be developed. The ATN ULA conforms to the OSI XALS architecture ISO 9545.

> *The ATN SM application should be considered as a particular air-ground ATN application. There is no reason why the methodology used for specifying the CNS/ATM-1 applications could not be used for the ATN SM application.*

The task of the "Upper Layer" services is two-fold: to compensate the deficiency of the transport service provided by the ATN Internet to its users and to provide high-level services required by the applications to carry out the application protocols.

Compensate the transport service. For instance, the ATN Transport Service Provider does not guarantee the delivery of all submitted data in case of connection release. Neither does it allow its users to reject a connection release requested by the peer. It is up to the applications to control the reception of all data before to request the connection release and to implement an application-level protocol handling the release negotiation.

Enhance the transport service. The ATN transport service is used to send unstructured data over the ATN. The applications using this service need to negotiate to some extent the nature of the data exchanged in terms of data types and encoding rules. The data flow on the connection need to be structured as a dialogue for which the rules of establishment, release and data transfer should be defined and controlled.

The SM Application needs the following Upper Layer services:

- *graceful release,*
- *optimisation of the use of the Transport service (use of the T-CONNECT user data),*
- *negotiation of the encoding rules used during the communication,*
- *PDU delivery to the relevant ASE, and*
- *management of all release collision situations.*

OSI standards recognise that the two categories of functions listed above have to be implemented by <u>any</u> transport service user, whatever the operational purpose of the application is. Layers 5 to 7 of the Basic Reference Model (Session, Presentation and Application) have been designed to implement the protocols needed to provide these functions in a consistent and efficient way. These layers prevent the applications from needing to be concerned with these functions. Implementing an application directly onto the transport service is possible but this would mean implementing in the application some of the upper layer services.

[1] The use of a reduced upper layer stack for SM was recognised as early as 1988. In the attempt to use the OSI network management protocol and framework to manage TCP/IP based internets, a "Lightweight Presentation Protocol" (LPP) was specified in order for systems to be able to run the CMIP protocol over a transport service without implementing the full upper layer stack. It was recognised that the session service was superfluous for the SMAE and that the presentation protocol could be limited to the negotiation of the presentation context for ACSE and ROSE. The Fast Byte option of the Presentation and the Session protocol may be considered as a variant of the LPP.

Porting an OSI SM Application over the ATN Transport service would necessitate a "glue layer" between the TSP and the SM Application. This glue is functionally equivalent to the ATN Upper Layers (i.e. Fast Byte Session and Presentation, and the CF). It is logical to use them instead of developing a specific interface module.

An ATN application which conforms to the ICAO Technical Provisions is composed of the functional elements illustrated in Figure 6-6:

a) The Application Process (AP) is the element in a real Open System which performs the processing for a particular application.

b) The Application Entity (AE) is that part of the AP which performs the communication functions needed by the application using defined application protocols and the underlying presentation service.

c) The Application Service Element (ASE) provides a set of communication functions for a particular purpose. Some ASEs have been defined by ICAO to handle ATN-specific protocols. Some others - more generic, useful for a number of applications - have been specified by ISO.

d) The Control Function (CF) exists within the AE to co-ordinate the use of the different services provided in the constituent ASEs and the use or the provision of the external services (AE service and presentation service).

An abstract service has been "artificially" defined in the middle of the ATN AE. The Dialogue service provides a simplified connection-oriented communication service to the ASEs hiding from them the complexity of the ACSE and the Presentation service primitives and parameters. The specification of the protocol handled by the ASEs is made simpler. There is no requirement for a product to implement a concrete dialogue interface (i.e. an Application Programmatic Interface, API). This approach has been chosen for the CNS/ATM-1 air-ground applications. For the AIDC application, the dialogue service has been replaced by a connectionless communication service, making the AIDC protocol a step simpler.

The SM Application Entity contains ISO-defined ASEs which have been designed in the initial ALS structure. The underlying service of these ASEs is directly the service of another ASE (ROSE service for CMIP) or the Presentation service itself (Presentation service for ACSE and ROSE protocols). These ASEs will be integrated in the ATN SM AE as standardised by ISO. Three types of internal structure may be envisaged for the SM AE:

- *the dialogue service is used by the CF,*
- *the dialogue service is not used at all by the CF,*
- *the dialogue service is enhanced to provide the CMIS service.*

The three structures are discussed later, and it is concluded that the dialogue approach is the more appropriate for the SM application.

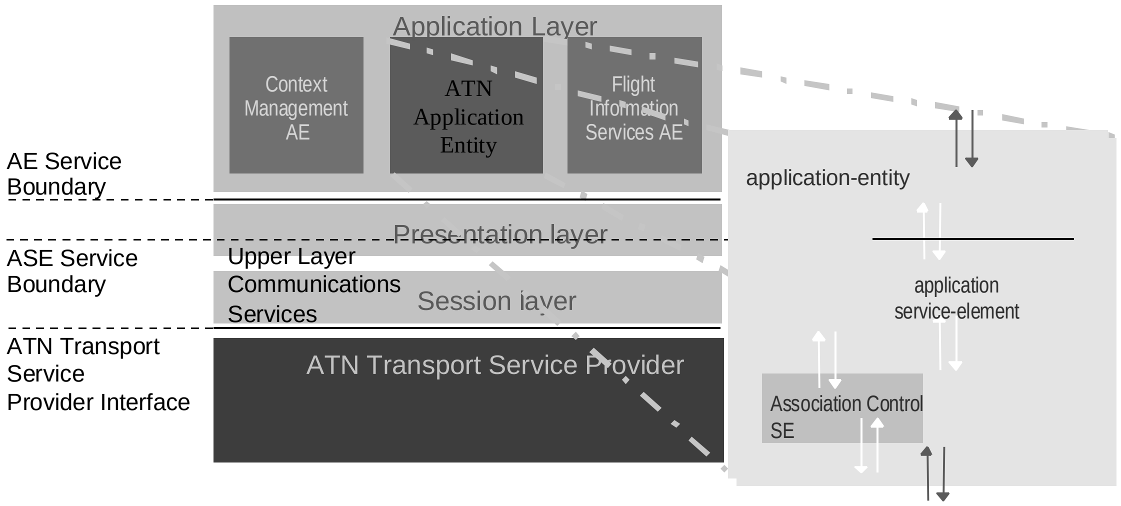

Figure 6-6. The ATN Upper Layer Architecture

An ATN application entity is fully designed when the constituent ASEs and the Control Function are specified. The AEs specified in the scope of the CNS/ATM-1 Package include at least the Association Control Service Element (edition 2) and an application-specific ASE. ACSE is used to create and maintain an application-association between the communicating AEs. The rules of use of the associations are defined in the application context. It defines the communications behaviour, how the ASE association can be started and finished and a set of rules and state information.

> *The ATN SM Application will rely on ACSE Edition 2, and CMISE combined with ROSE. Other ASEs may be added (SMASEs) to handle specific SM functions. The application-context defined in the OSI standard for the SM application is not valid any more. A new application-context will be modified to support PER as encoding rules.*

In addition, the ATN Upper Layer Architecture provides a global naming scheme used to identify unambiguously any ATN application in any End System. A unique name can be built from the type of the AE (System Management is a specific type) and the location of the ES where the application is run (either an aircraft or a ICAO ground facility).

> *The ATN Naming scheme allows for the identification of a single application of the same type within an aircraft or a ground system. There is a problem here in the CNS/ATM-1 provisions if two instances of the SM applications need to be identifiable (for instance, in an aircraft, one SM application in the ES and one SM application in the IS). The problem is solved by the naming and addressing extensions in Sub-Volume 4, which allow a System-ID to be specified unambiguously.*

6.3.1.2 "Fast Byte" Stack

The "Fast Byte" concept designates a subset of the efficiency options of the session and presentation protocols. This allows the service users to negotiate in a very efficient way the non-use of the protocol during the data transfer phase and the connection release phase but to use the connection establishment phase to negotiate some communication parameters. In addition, the fast byte session optimises the use of the transport service by sending user data directly in the T-CONNECT request when the data size allows for it.

The following assumptions are made on the applications using the "Fast Byte" option (comments in italics check the applicability of each assumption in the SM application):

- The applications are identified within the ES by the Transport selector. Both session and presentation selector are null.

  The SM Application does not need Session and Presentation selectors. ATN addresses need to be assigned to SM applications hosted in ESs and in ISs.

- The applications do not invoke presentation services other than the P-CONNECT, P-DATA and P-ABORT services. If the constituent ASEs make use of other services (e.g. P-RELEASE), the CF is responsible for mapping them onto available services. The P-ABORT service will be invoked without user data.

  CMISE assumes the use of the A-RELEASE of the ACSE. The CF for the SM application will provide the mapping mechanism P-RELEASE/P-DATA+P-ABORT. The P-ABORT is invoked by ACSE to abort the connection and send the ABRT APDU. The CF for the SM application will provide the mapping mechanism P-ABORT(data)/P-DATA(data)+P-ABORT.

- The orderly release function provided by the basic session protocol is not available to the session service users. This orderly release capacity has to be handled by an application level component. The CF specified in the ULCS Provisions supports this functionality in co-operation with ACSE.

  The mapping mechanism A-RELEASE/P-DATA(RLRQ)+P-DATA(RLRE)+P-ABORT performed by the CF guarantees the graceful release.

- An ATN application supports a single abstract syntax indirectly identified by the type and the version number of the application. Actually, this "unique" abstract syntax is the collection of the abstract syntaxes of the constituent ASEs. The implicit identification avoids the initiator presentation entity sending the AS reference to the receptor and subsequently the need to identify for each data sent the presentation context the data refer to. The drawback is that the receiving AE is no longer able to deduce (from the presentation context) which ASE is the actual recipient of the PDU. PCI data is sent by the initiator CF to receptor CF to identify recipient ASE.

  It will be assumed that ACSE, ROSE and CMISE ASN.1 specifications are part of the same abstract syntax. The CF will be able to send PDUs to the relevant ASE (ACSE or ROSE)

- As a consequence of the "unique" abstract syntax, all the PDUs generated by the AE are encoded using the same set of encoding rules. The connection establishment phase is used by the peers to negotiate the actual encoding rules.

  This means that the user data of CMIS must be encoded in PER. CMIS user data are the arguments of the CMIS operations.

6.3.1.3 The Control Function

The "Fast Byte" stack provides the minimum protocol offering a limited presentation transfer-syntax negotiation and removal of the session orderly release functionality.

As indicated above, some useful functions previously provided by the OSI upper layers have been allocated to the Control Function of the AE:

a) identification of the recipient of the received PDU,

b) mapping of the presentation service expected by the constituent ASEs onto the "Fast Byte" presentation service", in particular the P-RELEASE and the P-ABORT with user data,

in addition to standard CF functions:

a) management of the release collision situation,

b) transfer of the ASE version number.

All these functions are performed by the CNS/ATM-1 Package CF.

6.3.1.4 Porting OSI SM Protocols to the ATN Upper Layer Environment

Porting CMISE, ROSE and ACSE on a Fast Byte Stack

The International Profiles AOM11 (or AOM12) specify how CMISE combined with ROSE and based upon ACSE, Presentation layer protocol and Session layer protocol are used to provide a basic subset (or an enhanced subset) of operation and notification services to the CMSIE-service users of the two end systems.

Both profiles require the support of part 1 of ISO/IEC ISP 11183 (specification of ACSE, presentation and session protocols for the use by ROSE and CMISE).

A subsequent section compares the upper layer services required by ISP 11183-1 to support the operation of a CMISE/ROSE AE to the upper layers services effectively provided a "Fast Byte" ATN stack. The following table highlights the main differences and identifies what has to be done when porting the CMISE/ROSE AE over the ATN stack to compensate for these differences (in addition to the development of a CF).

Full Stack	ATN Stack	What has to be done to port a full stack-based SMA to a fast byte-based SMA
ACSE		
Includes ACSE edition 1 and Amd1 (authentication)	Includes ACSE edition 2	*The main difference comes from additional fields in the ACSE ASN.1 (e.g. application-context-name-list), new PER-visible constraints and extensibility markers[2]. The minimum task is an re-compilation of the ACSE ASN.1*
A conformant implementation shall support both roles (initiator and responder)	A conformant implementation shall support at least one role (initiator or responder)	
A conformant implementation shall encode ACSE PDUs in BER	A conformant implementation shall encode ACSE PDUs in PER	*An analysis of the Full Stack SMA should be carried out to determine how easy/difficult it is to switch from the BER encoder to the PER encoder.*
If the Authentication FU is supported, the "authentication-mechanism name" parameter shall be supported in the AARQ	The "authentication-mechanism-name" parameter of the AARQ is not supported	*An analysis of the Full Stack SMA should be carried out to determine whether the field "authentication mechanism name" is used when building the AARQ*
The "implementation information" parameter shall be supported in the AARQ for the receiver	The "implementation information" parameter is optionally supported in the AARQ for the receiver	*An analysis of the ATN Stack SMA should be carried out to check that the field "Implementation information" is supported by the receiver.*
The Form1 (Directory Name) shall be supported by a conformant implementation	The Directory Name form is not supported at all by the ATN stack	*There is a potential blocking problem here if the Full Stack SMA supports uniquely this form of AE Title*

[2] A detailed discussion of differences in ACSE editions is available in the CAMAL - Part IV - ATN Communication Services - Section 2.6.2. The discussion indicates that the initial version of ATN ULA requires none of the changes that distinguish ACSE edition 1 from ACSE edition 2, apart from, optionally, authentication

Full Stack	ATN Stack	What has to be done to port a full stack-based SMA to a fast byte-based SMA
The "other" Authentication Value Form shall be supported by any receiving conformant implementation	The "other" Authentication Value Form is not supported for receiving	*An analysis of the Full Stack SMA should be carried out to check that the authentication value can not take the form "other"*
CMISE/ROSE		
A conformant implementation shall encode CMISE/ROSE PDUs in BER	A conformant implementation shall encode CMISE/ROSE PDUs in PER	*An analysis of the Full Stack SMA should be carried out to determine how easy/difficult it is to switch from the BER encoder to the PER encoder..*
PRESENTATION		
	A conformant implementation shall implement the short-connect and the null-encoding options	*The SMA shall be able to select these options.*
A conformant implementation shall be able to support at least 2 presentation contexts.	An ATN conformant implementation does not handle more than one presentation context	*The management of the presentation contexts shall be simplified (in particular the presentation context definition list shall not be used).*
	An ATN conformant implementation shall allow the presentation service user to select the session "no-orderly release" FU.	*The SMA shall be able to select this FU.*
	An ATN conformant implementation shall support the "Fast Byte" specific PDUs (SHORT-CP, SHORT-CPA, SHORT-CPR)	
A conformant implementation shall encode the presentation user data with the Fully Encoded option	An ATN implementation shall encode the presentation user data (not for the P-CONNECT) with the Fully Encoded option augmented of PER-visible constraints.	*The encoding of the presentation user data shall be performed in the CF of the SMA AE.*
A conformant implementation shall encode the EXTERNAL type with the choice "single-ASN.1-type"	An ATN conformant implementation shall encode the EXTERNAL type with the choice "arbitrary"	*?*
SESSION		
	An ATN conformant implementation shall support the "no-orderly release" FU.	*The "no-orderly release" functionality shall be implemented in the CF of the SMA*
	An ATN conformant implementation shall support the null-encoding and short-connect options	*The SMA shall be able to select these options.*
	An ATN conformant implementation shall support the "Fast Byte" specific PDUs (SCN, SAC, SRF, NL, …)	

This analysis shows that the Fast Byte stack can support the communication activities of an AE containing CMISE and ROSE. However, as for the other ATN applications, a SMA CF will have to be developed to identify the ASE within the AE source or destination of a AE PDU, to redirect non available P-services used by CMSIE/ROSE, to manage collision situations. It is very likely that the CF specified in the CNS/ATM-1 Package is suitable for the SM AE.

6.3.1.5 PER encoding

PCI encoding

Annex B of ISO/IEC 9596-1 contains the expanded ASN.1 syntax of the combined CMISE and ROSE PDUs. Once encoded, these PDUs constitute the overhead generated by the CMISE and ROSE ASEs. As indicated above, the Upper Layer Architecture mandates the use of PER for the encoding of all the PDUs generated by an ATN application. At the association establishment time, the PER transfer syntax is negotiated by the AEs using the negotiation mechanisms of the "Fast Byte" Presentation.

Standardised ASN.1 for CMISE and ROSE

The first encoding approach is to keep the ASN.1 defined for the CMISE/ROSE APDUs.

Optimised ASN.1 for CMISE and ROSE

This section analyses how the ASN.1 could be modified in such a way the PER encoding is fully optimised. The principle is to add PER-visible constraints to the maximum extent possible. The information provided by the PER-visible constraints increases the a-priori knowledge of both the encoder and the decoder and reduces the amount of information to encode. PER-visible constraints usually affect the PER encoding of the value or the length of a data field.

<u>Extensibility Markers</u>

Extensibility markers may be used in an ASN.1 specification to allow future modifications of the data structure while keeping a certain level of compatibility between systems implementing the old and the new ASN.1.

The addition in the ASN.1 of extensibility markers does not impact the BER encoding. Such a modification can be proposed on the base standard without impacting BER-based developed products.

As far as the SM application is concerned, it is likely that the base protocols (i.e. CMISE and ROSE) will not evolve. Modifications will probably be needed in the object definition (i.e. the MIB) when experience will be gained from the operational service of the ATN.

<u>Value constraint on Integer types</u>

Some ASN.1 types are defined as non-constrained length INTEGER. This results in PER in the coding of the length of the value in 1 octet (at least) in front of the coding of the value itself. When the range of the integer is known, the length of the value is forced to the number of bits needed to encode all the possible values. As this length can be deduced from the ASN.1 by both the encoder and the decoder, there is no need to encode it in the data flow.

InvokeIDType ::= INTEGER

The difficulty is to define an upper bound to these types (e.g. INTEGER (0..256)). An extensibility marker may solve the problem (e.g. INTEGER(0..256,…)).

The addition in the abstract syntax of value constraints on integer types does not impact the BER encoding. Such a modification can be proposed on the base standard without impacting BER-based developed products.

<u>Redefinition of Integer types with Named values</u>

Named values attached to Integers are given for information purposes only but do not impact the encoding (BER and PER). The encoding of such a type is strictly identical to the encoding of an integer without named values. Non identified values may be provided to the encoder without causing an encoding error.

Since a list of values is defined for these integers, a more efficient encoding would be possible by integrating the range of values in the encoding.

The following example illustrates the 2 alternate solutions:

```
GeneralProblem ::= INTEGER {   unrecognisedAPDU      (0),
                               mistypedAPDU          (1),
                               badlyStructuredAPDU   (2) }
```

This definition could be replaced by

```
GeneralProblem ::= INTEGER (0..2) {   unrecognisedAPDU      (0),
                                      mistypedAPDU          (1),
                                      badlyStructuredAPDU   (2) }
```

or

```
GeneralProblem ::= ENUMERATED {   unrecognisedAPDU      (0),
                                  mistypedAPDU          (1),
                                  badlyStructuredAPDU   (2) }
```

The advantage of the first solution is to keep the BER encoding unchanged since the data type remains the same (INTEGER) and the value constraint is not used by the BER encoders. The second solution is more elegant but causes a compatibility problem with older stacks based on the previous definitions.

CMISE/ROSE integer types defined with named values are the following: GeneralProblem, InvokeProblem, ReturnResultProblem, ReturnErrorProblem

This analysis suggests that the encoding of very few parameters could be optimised by upgrading the ASN.1 with PER-visible constraints. The compression between BER and PER will come from the non-encoding of the data types (the top level CHOICE (ROSEapdus) and for each ROSE operation the SEQUENCE of parameters) and from the encoding of some integers. It is questionable whether the data compression rate obtained is worthwhile or not compared to the problems raised (new version of the ASN.1, standardisation process required, compatibility not guaranteed, etc…).

6.3.1.6 CMISE User data encoding

The user data of the CMISE/ROSE PDUs contains the arguments of the CMISE operations (action, create, delete, get, cancel-get, event-report, linked-reply, set, etc.).

The ASN.1 definition of these arguments is known from the agent and the manager. The ASN.1 is usually generated by automatic tools making easier the specification of the managed objets and the corresponding ASN.1 definition (GDMO tools).

The user data of the CMISE/ROSE PDUs are defined as an "ANY DEFINED BY" ASN.1 type. This means that the content is identified by another field close to the user data field and that the content is encoded with the same encoding rules as the PDUs themselves, i.e. PER.

In order to increase as much as possible the compression rate of PER, it is necessary to impose on the GDMO tools (or on ASN.1 designers when the ASN.1 is generated manually) some composition rules of the ASN.1 texts, as for instance:

- SEQUENCE OF and SET OF should be defined with a size constraint,
- INTEGER should be defined with a value constraint,
- ENUMERATED should be preferred over INTEGER with Named Values,
- etc…

6.3.1.7 Conclusion and Recommendations

Unlike the other CNS/ATM-1 applications, all the SM ASEs (CMISE, ROSE and ACSE) are already fully specified over the full session and presentation OSI protocols. On the other hand, the SM AE should fit the ATN Upper Layer framework defined in the ATN Technical Provisions.

The migration of the SM application from the full stack to the ATN upper layer stack (Fast MIP)

a) forces the specification of a kind of "convergence function", the Control Function, between the existing ASEs and the ATN Presentation service.

b) raises the problem of the data encoding since the encoding rules usually used up to now for SM data are replaced by the Packet Encoding Rules.

In order to take into account existing implementations of CMISE products and ATN Upper Layers products, the air-ground application approach is selected for the SM AE in the air-ground environment. The AE would be made of two parts. The AE lower part would be composed of ACSE edition 2 with the CF providing the dialogue service as specified in the ULA Provisions. The upper part would be composed of CMISE and ROSE with a CF using the dialogue service. The CMIS-user would use the D-START/END/ABORT services instead of the A-ASSOCIATE/RELEASE/ABORT services.

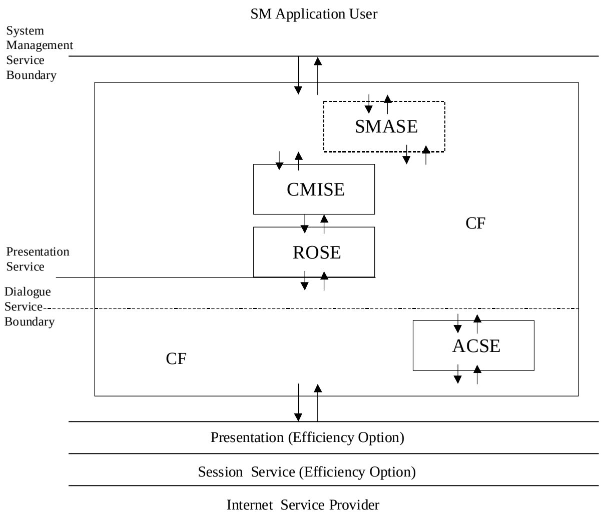

Figure 6-7

Given the poor compression rate obtained by adding PER-visible constraints in the CMISE ASN.1, it was decided to keep the CMISE and ROSE ASN.1 unchanged. The ASN.1 defining the MOs is however to be optimised for PER.

6.3.2 Comparison Between ISP 11183-1 and the ATN Upper Layer Profile

This section compares ISP 11183-1 (ACSE, Presentation and Session profile for use by CMISE/ROSE) and the ATN Upper Layer Profile (ACSE, Presentation and Session provided by the ATN).

ISO/IEC ISP 11183-1 (International Standardized Profiles AOM1n OSI Communication - Management Communications - Part1) specifies how the Association Control Service Element (ACSE), the Presentation layer and the Session layer are used to provide the required upper layer functions for the CMISE/ROSE functions. In addition, requirements for abstract and transfer syntax handling are specified.

The model used in the ISP is one of two end systems running an end-to-end association using the ACSE, Presentation and Session services and protocols as illustrated in Figure 6-8.

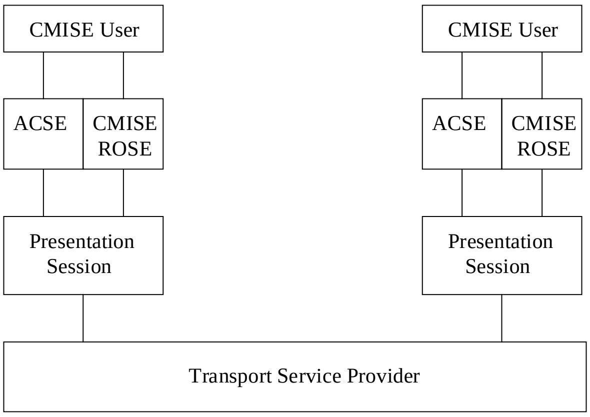

Figure 6-8. ISP Communication Model for SM Applicaion

The model proposed in the ATN Upper Layer Architecture is compatible with this, but uses the concepts introduced in the extended application architecture (XALS) of the OSI Basic Reference Model, as illustrated in Figure 6-9.

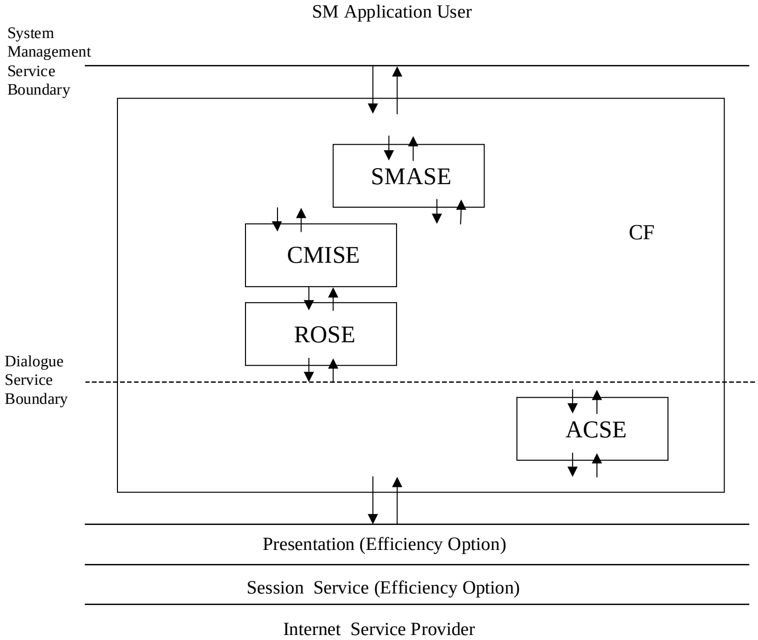

Figure 6-9 ATN Communication Model for SM Application

ISP 11183-1 is based on a full OSI upper layer stack. It does not take into account the efficiency options of the presentation and session protocols, nor it takes into account the second edition of the ACSE protocol. This section indicates how ISP 11183-1 could be extended to include the new protocol functionality.

This section highlights the differences between the ATN upper layer profile and the ISP 11183-1 profile.

6.3.2.1 ACSE

Annex A of ISP 11183-1 specifies the ACSE profile required to support the operation of CMISE and ROSE.

6.3.2.1.1 Protocol details

The reference to ACSE protocol in ISP 11183-1 is ISO 8650:1988 - CCITT Recommendation X.227:1988 and ISO 8650/Amendment 1 (Authentication during association establishment). The ATN upper layer profile is based on the second edition of ACSE.

Table 6-1. Identification of ACSE Protocol Specification

Identification of Protocol Specification	ATN Support	ISP 11183-1
ISO/IEC 8650-1:1995 (note)	M	-

Note. — This is the second edition of the ACSE protocol specification.

The ATN specification is non-conformant to the ISP proforma, in that the version of ACSE required to be supported is ACSE edition 2.

6.3.2.1.2 Protocol versions

There is no explicit reference in the ISP to the ACSE protocol version. Based on the baseline ACSE document used for the ISP, it is assumed that version 1 is mandated.

Table 6-2. Identification of ACSE Protocol version

ISP Index	Version	ISP 11183-1 Status	ATN Support	Mnemonic
-	Version 1	M	M	A-V1
-	Version 2	-		

The ATN specification is aligned with the ISP 11183-1 for the ACSE protocol version.

6.3.2.1.3 Supported roles

Association establishment

Table 6-3. ACSE Roles for Association Establishment

ISP Index	Capability	ISP Status	ATN Support	Mnemonic
A.2.2/1	Association initiator	C(1)	C(2)	A-CON_initiator
A.2.2/2	Association responder	C(1)	C(2)	A-CON_responder

(1) The ISP requires a conforming implementation to support at least one of the roles.

(2) The ATN profile requires either one or both of the ACSE roles “Association initiator” or “Association responder” to be supported.

The ATN specification is aligned with the ISP 11183-1 for the role during association establishment.

Normal Release procedure

Table 6-4. ACSE Roles for Normal Release

ISP Index	Role	ISP 11183-1 Status	ATN Support	Mnemonic
6.2	Initiator	M	C(1)	A-REL_requestor
6.2	Responder	M	C(1)	A-REL_acceptor

(1) The ATN profile requires either one or both of the ACSE Normal Release roles "Initiator" or "Responder" to be supported. The ACSE Release Responder is allowed to give a negative response, despite the fact that the session Negotiated Release functional unit is not selected for the association.

An ISP conforming implementation shall be able to request and accept an orderly release of the association, whatever its role, initiator or responder. The ATN specification is less constraining since it allows that only one side be initiator of the association release.

Abnormal Release procedure

Table 6-5. ACSE Roles for Abnormal Release

ISP Index	Role	ISP Status	ATN Support	Mnemonic
-	Initiator	M	M	
-	Responder	M	M	

The ATN specification is aligned with the ISP 11183-1 for the role during abnormal release procedure.

6.3.2.1.4 Protocol mechanisms

Table 6-6. ACSE Protocol Mechanisms Supported

ISP Index	Protocol Mechanism	ISP Status	ATN Support	Mnemonic
A.2.1/1	Normal mode	M	M	
A.2.1/2	X.410-1984 mode	I	X	
A.2.1/3	Rules for extensibility	M	M	
A.2.1/4	Supports operation of Session version 2	M	M	S-O-SESS-V2

The ATN specification is aligned with the ISP 11183-1 for the protocol mechanisms to be supported by the ACSE PMs.

Extensibility and Encoding

The ATN profile requires the following features:

a) For the purposes of this specification, the abstract syntax module defined in clause 9 of the ACSE protocol specification is augmented with the ASN.1 extensibility notation, as specified in ISO/IEC 8650-1 Amendment 1.

b) The system is to support that encoding which results from applying the ASN.1 packed encoding rules (basic, unaligned variant), as specified in ISO/IEC 8825-2, to the abstract syntax module specified in ISO/IEC 8650-1 Amendment 1.

c) Packed encoding (basic, unaligned) to be used for encoding all ACSE Protocol Control Information (PCI) for interchange.

ISP 11183-1 section 8 requires ISP conforming systems to encode PDU with the Basic Encoding Rules. ISP 11183-1 does not require compliance to ISO/IEC 8650-1 Amendment 1.

6.3.2.1.5 ACSE Functional units

Table 6-7. Selection of ACSE Functional Units

ISP Index	Role	ISP Status	ATN Support	Mnemonic
A.2.3/1	Normal mode	M	M	
A.2.3/2	Authentication	O	C(1)	A-FU(AU)

(1) If the Dialogue Service user requires the use of the Security Requirements parameter of the D-START primitives, then M, else O.

The ATN specification is aligned with the ISP 11183-1 for the functional units to be supported by the ACSE PMs.

6.3.2.1.6 Supported APDUs

Table 6-8. Supported ACSE Protocol Data Units

ISP Index	APDU	Sender		Receiver		Comment
		ISP Status	ATN Support	ISP Status	ATN Support	
A.3/1	AARQ	C(1)	M	M	M	
A.3/2	AARE	C(2)	M	M	M	
A.3/3	RLRQ	M	M	M	M	
A.3/4	RLRE	M	M	M	M	
A.3/5	ABRT	M	M	M	M	

(1) If [A-CON_initiator] then M else N/A
(2) If [A-CON_responder] then M else N/A

The ATN specification is aligned with the ISP 11183-1 for the protocol data units to be supported by the ACSE PMs.

6.3.2.1.7 Supported APDU parameters

AARQ

Table 6-9. Supported AARQ Parameters

		Sender		Receiver	
ISP Index	Parameter	ISP Status	ATN Support	ISP Status	ATN Support
A.4.1/1	Protocol Version	C(1)	X	M	M
A.4.1/2	Application Context Name	M	M	M	M
A.4.1/3	Calling AP title	O	O	M	M
A.4.1/4	Calling AE qualifier	O	O	M	M
A.4.1/5	Calling AP invocation-identifier	O	O	M	M
A.4.1/6	Calling AE invocation-identifier	O	O	M	M
A.4.1/7	Called AP title	O	X	M	M
A.4.1/8	Called AE qualifier	O	X	M	M
A.4.1/9	Called AP invocation-identifier	O	X	M	C(6)
A.4.1/10	Called AE invocation-identifier	O	X	M	C(6)
A.4.1/11	ACSE-requirements	C(2)	C(4)	M(3)	M(5)
A.4.1/12	Authentication-mechanism name	C(2)	X	M(3)	N/A
A.4.1/13	Authentication-value	C(2)	C(4)	M(3)	M(5)
A.4.1/14	Implementation information	I	X	M	O
A.4.1/15	User information	O	M	M	M

(1) If ACSE version 2 or above is supported m else o
(2) If A-FU(AU) M else -
(3) If the authentication FU is not supported, based on the extensibility rules, these tagged values shall be received and ignored. The "Authentication-mechanism-name" and "Authentication-value" fiels shall only be present if the "ACSE requirements" field includes the authentication FU. The "Mechanism-name" field shall be present if "Authentication-value" is of type ANY DEFINED BY.
(4) The AARQ parameters "ACSE-Requirements" and "Authentication-value" shall([173]) be supported, for sending, only if the connection initiator role (A-CON_initiator) and the Authentication functional unit (A-FU(AU)) are supported.
(5) The AARQ parameters "ACSE-Requirements" and "Authentication-value" shall([174]) be supported for receiving if the connection responder role (A-CON_responder) is supported, but are ignored if the Authentication functional unit (A-FU(AU)) is not supported by the responder.
(6) The AARQ parameters "Called AP invocation-identifier" and "Called AE invocation-identifier" shall([175]) be supported, for receiving, if the Association Responder role is supported.

The ATN specification is non-conformant to the ISP proforma, in that the "Authentication-mechanism-name" parameter is not supported for sending an AARQ.

The ATN specification is non-conformant to the ISP proforma, in that the "Implementation information" parameter is optionally supported for receiving an AARQ.

AARE

Table 6-10. Supported AARE Parameters

		Sender		Receiver	
ISP Index	**Parameter**	**ISP Status**	**ATN Support**	**ISP Status**	**ATN Support**
A.4.2/1	Protocol Version	C(1)	X	M	M
A.4.2/2	Application Context Name	M	M	M	M
A.4.2/3	Responding AP title	O	X	M	M
A.4.2/4	Responding AE qualifier	O	X	M	M
A.4.2/5	Responding AP invocation-identifier	O	X	M	M
A.4.2/6	Responding AE invocation-identifier	O	X	M	M
A.4.2/7	Result	M	M	M	M
A.4.2/8	Result source - diagnostic	M	M	M	M
A.4.2/9	ACSE-requirements	C(2)	(4)	M(3)	(5)
A.4.2/10	Authentication-mechanism name	C(2)	X	M(3)	N/A
A.4.2/11	Authentication-value	C(2)	(4)	M(3)	(5)
A.4.2/12	Implementation information	I	X	M	O
A.4.2/13	User information	M	M	M	M

(1) If ACSE version 2 or above is supported m else o
(2) If A-FU(AU) M else -
(3) The "Authentication-mechanism-name" and "Authentication-value" fields shall only be present if the "ACSE-requirements" fields includes the authentication FU. The "Authentication-mechanism-name" shall be present if "Authentication-value" is of type ANY DEFINED BY.
(4) The AARE parameters "ACSE-Requirements", Authentication-mechanism-name" and "Authentication-value" shall([177]) be supported, for sending, only if the connection responder role (A-CON_responder) and the Authentication functional unit (A-FU(AU)) are supported.
(5) The AARE parameters "ACSE-Requirements" and "Authentication-value" shall([178]) be supported, for receiving, only if the connection initiator role (A-CON_initiator) and the Authentication functional unit (A-FU(AU)) are supported.

The ATN specification is non-conformant to the ISP proforma, in that the "Authentication-mechanism-name" parameter is not supported for sending an AARE.

The ATN specification is non-conformant to the ISP proforma, in that the "Implementation information" parameter is optionally supported for receiving an AARE.

RLRQ

Table 6-11. Supported RLRQ Parameters

		Sender		Receiver	
ISP Index	**Parameter**	**ISP Status**	**ATN Support**	**ISP Status**	**ATN Support**
A.4.3/1	Reason	O	M	M	M
A.4.3/2	User information	O	M	M	M

The ATN specification is aligned with the ISP 11183-1 for the parameters to be supported by the ACSE PMs in the RLRQ APDU.

RLRE

Table 6-12. Supported RLRE Parameters

		Sender		Receiver	
ISP Index	**Parameter**	**ISO Status**	**ATN Support**	**ISO Status**	**ATN Support**
A.4.4/1	Reason	O	M	M	M
A.4.4/2	User information	O	M	M	M

The ATN specification is aligned with the ISP 11183-1 for the parameters to be supported by the ACSE PMs in the RLRE APDU.

ABRT

Table 6-13. Supported ABRT Parameters

		Sender		Receiver	
ISP Index	**Parameter**	**ISP Status**	**ATN Support**	**ISP Status**	**ATN Support**
A.4/1	Abort source	M	M	M	M
A.4/2	Diagnostic	C1	M	C1	M
A.4/3	User information	M	M	M	M

(1) If [A-FU(AU)] then M else N/A

The ATN specification is aligned with the ISP 11183-1 for the parameters to be supported by the ACSE PMs in the ABRT APDU.

6.3.2.1.8 Supported parameter forms

AE Title Name Form

Table 6-14. AE Title Name Form

		Sender		Receiver	
ISP Index	Syntax form	ISP Status	ATN Support	ISP Status	ATN Support
A.5/1	Form 1 (Directory name)	M	X	M	O
A.5/2	Form 2 (Object identifier and integer)	M	M	M	M

The ATN specification is non-conformant to the ISP proforma, in that the "Form 1 (Directory name)" AE Title Name Form is not supported for sending and is optionally supported for receiving.

Authentication Value Form

Table 6-15. Authentication Value Form

Prerequisite: A-FU(AU)

		Sender		Receiver	
ISP Index	Authentication value form	ISP Status	ATN Support	ISP Status	ATN Support
A.6/1	GraphicString	O	C(1)	M	M
A.6/2	BIT STRING	O	C(1)	M	M
A.6/3	EXTERNAL	O	C(1)	M	M
A.6/4	Other	O	X	M	N/A

(1) If the authentication functional unit is supported, at least one of the Authentication-value forms listed in Table 2-15 shall be implemented for sending.

The ATN specification is non-conformant to the ISP proforma, in that the "Other" Authentication Value Form is not supported for receiving.

6.3.2.1.9 Summary for ACSE

The ATN ACSE is conformant to the part of the ISO/IEC ISP 11183 related to ACSE with the following exceptions:

a) In AARQ/AARE, "Authentication-mechanism-name" and "Implementation information" are not supported as described in the ISO standard for ACSE and in the ISP.

b) The "Directory Name" form is not supported for sending an AE Title.

c) The "Other" form is not supported for receiving an "Authentication-value" parameter in AARQ and AARE APDUs.

These differences do not preclude the use of the ATN ACSE for supporting the communication protocols required for System Management.

6.3.2.2 Presentation Layer

Annex B of ISP 11183 specifies the Presentation profile required to support the operation of CMISE and ROSE. The ISP does not take into account the efficiency enhancements option of the Presentation protocol required by the ATN profile.

6.3.2.2.1 Protocol mechanisms

Table 6-16. Presentation Protocol Mechanisms Supported

ISP Index	Protocol Mechanism	ISO Status	ATN Support	Mnemonic
B.2.2/2	Normal mode	M	M	
B.2.2/1	X.410-1984 mode	I	X	
See note	Nominated context	-	N/A	
See note	Short encoding	-	N/A	
See note	Packed encoding rules	-	N/A	
See note	Short-connect	-	M	
See note	Null-encoding	-	M	

Note. — Optional protocol mechanisms defined in ISO/IEC 8823-1 Amendment 1.

It is proposed to align the ISP specification to the ATN profile.

6.3.2.2.2 Use of null-encoding and short-connect protocol options

The use of null-encoding and short-connect protocol options requires that some requirements be met. This section checks that these requirements are fulfilled in the System Management context.

Table 6-17. Use of the null encoding and short-connect Presentation protocol options

Ref.	Requirement	ATN Requirement	SM context
a	The presentation context definition list contains precisely one item in which the abstract syntax is known to the responding Presentation Protocol machine (PPM) by bilateral agreement.	N/A	C(1)
b	The presentation context definition list is empty and the default context is known by bilateral agreement	M	C(1)
c	The presentation context definition list is empty and the abstract syntax of the default context is known to the responding PPM by bilateral agreement and is specified in ASN.1	M	C(1)
d	The calling and called presentation selectors are null	M	C(2)
e	The presentation-requirements parameter in the P-CONNECT service includes the kernel functional unit only.	M	C(2)
f	When initiating a connection, there shall be no parameters of the S-CONNECT request service primitive issued by the Presentation layer other than, optionally, user data. *Note. — This enables the initiating Session Protocol Machine to use the short-connect protocol option.*	To be checked	
g	The user of the presentation service shall not issue any presentation primitives other than P-CONNECT request, P-CONNECT response, P-DATA request and P-U-ABORT request.	ok	
h	When it is required to release the presentation connection, the presentation service user shall issue a P-U-ABORT request	The SM CF is responsible for mapping the P-RELEASE service onto the P-DATA and P-U-ABORT service	
i	Any user data in a P-U-ABORT request shall be ignored by the presentation service provider.	The SM CF is responsible for first sending the data of a P-U-ABORT request with P-DATA and then to abort the connection	

(1) The null-encoding protocol option is available for use on an established connection only if at least one of the conditions a, b and c in Table 3-2 is true.

The ISP requires conforming implementation to support at least 2 simultaneous presentation contexts. The ATN specification is non-conformant to the ISP proforma, in that only one presentation context is supported. In the case of the System Management Application, the presentation context should identify a single abstract syntax formed by ACSE and ROSE/CMISE abstract syntaxes and a single transfer syntax.

(2) The short-connect protocol option is used only in connection establishment to establish a connection on which the null-encoding option will be used; it can only be used if both of the conditions d and e in Table 3-2 is true.

Conditions d and e are true for implementations conforming the ISP. ISP 11183-1 allows conforming implementation to request the short-connect option of the Presentation protocol.

6.3.2.2.3 Functional units

ISP 11183 only requires the Kernel functional unit. The support of the Context Management and of the Context Restoration FUs is outside the scope of the ISP.

Table 6-18. Selection of Presentation functional units

ISP Index	Presentation functional unit	ISP Status	ATN Support	Mnemonic
B.2.3/1	Kernel	M	M	
B.2.3/2	Presentation Context Management	I	X	P-FU(CM)
B.2.3/3	Presentation Context Restoration	I	X	P-FU(CR)

The ATN specification is aligned with the ISP 11183-1 for the functional units to be supported by the Presentation PMs.

Table 6-19. Selection of Presentation pass-through Session functional units

ISP Index	Pass through to Session functional units	ISP Status	ATN Support	Mnemonic
C.2.1/2	Negotiated release	I	X	S-FU(NR)
C.2.1/3	Half Duplex	I	X	S-FU(HD)
C.2.1/4	Duplex	M	M	S-FU(FD)
C.2.1/5	Expedited Data	I	X	S-FU(EX)
C.2.1/6	Typed Data	I	X	S-FU(TD)
C.2.1/7	Capability Data Exchange	I	X	S-FU(CD)
C.2.1/8	Minor Synchronize	I	X	S-FU(SY)
C.2.1/9	Symmetric Synchronize	I	X	S-FU(SS)
	Data Separation		X	S-FU(DS)
C.2.1/10	Major Synchronize	I	X	S-FU(MA)
C.2.1/11	Resynchronise	I	X	S-FU(RESYNC)
C.2.1/12	Exceptions	I	X	S-FU(EXCEP)
C.2.1/13	Activity Management	I	X	S-FU(ACT)
See note	No-orderly release (NOR)	-	M	S-FU(NOR)

Note. — The NOR Session functional unit is defined in ISO/IEC 8326 Amendment 1.

It is proposed to align the ISP specification to the ATN profile.

6.3.2.2.4 Elements of procedure

Supported roles

Presentation Connection

Table 6-20. Presentation Connection roles

ISP Index	Role	ISP Status	ATN Support	Mnemonic
B.2.1/1	Initiator	C(1)	M	P-CON_initiator

B.2.1/2	Responder	C(1)	M	P-CON_responder

(1) The ISP requires a conforming implementation to support at least one of these roles.

The ATN specification is aligned with the ISP 11183-1 for the role of the PPMs during connection establishment.

Supported Presentation Protocol Data Units (PPDUs)

Note.— This section specifies the PPDUs associated with the supported Presentation functional units. There are no additional PPDUs or additional pass through functionality associated with the supported Session functional units.

Supported PPDUs associated with the Kernel services

Table 6-21. Supported Presentation Protocol Data Units

		Sender		Receiver		
ISP Index	**PPDU**	**ISP Status**	**ATN Support**	**ISP Status**	**ATN Support**	**Mnemonics**
B.3.1/1	Connect presentation (CP)	M	N/A (Note 2)	M	N/A (Note 2)	
B.3.1/2	CPtype	M	N/A (Note 2)	M	N/A (Note 2)	
B.3.1/3	CPCtype	I	N/A	I	N/A	
B.3.1/4	Connect presentation accept (CPA)	M	N/A (Note 2)	M	N/A (Note 2)	S-OA_SDR / S-OA_RCV
B.3.1/5	Connect presentation reject (CPR)	M	N/A (Note 2)	M	N/A (Note 2)	S-CDO_SDR / S-CDO_RCV
B.3.1/6	Abnormal release provider (ARP)	M	N/A (Note 2)	M	N/A (Note 2)	
B.3.1/7	Abnormal release user (ARU)	M	N/A (Note 2)	M	N/A (Note 2)	
B.3.1/8	Presentation Data (TD)	M	N/A (Note 2)	M	N/A (Note 2)	
Note 1	Short Connect (SHORT-CP)	?	M	?	M	
Note 1	Short Connect Accept (SHORT-CPA)	?	M	?	M	
Note 1	Short Connect Reject (SHORT-CPR)	?	M	?	M	

Note 1. — PDUs defined in efficiency enhancement ISO/IEC 8823-1 Amendment 1.

Note 2. — PPDUs not applicable, as the short-connect and null-encoding protocol options are selected.

It is proposed to align the ISP specification to the ATN profile.

6.3.2.2.5 Presentation Context Identifier

The ATN specification is non-conformant to the ISP proforma, in that it does not support at least 2 simultaneous presentation context and it uses the concept of default presentation context. However, in the ATN ULA, only one presentation context is required, even when several ASEs are included in the AE. It is assumed that the abstract syntaxes are identified in a single abstract syntax in the default presentation context and that all abstract syntaxes are encoded with the same transfer syntax identified in the default presentation context.

6.3.2.2.6 Encoding of User data parameter

The ISP mandates the "user data" value of each PPDU to be encoded as a "Fully-encoded-data" type. In addition, the "single-ASN.1-type" component has to be selected in the PDV-list and in all EXTERNAL fields.

The ATN specification is non-conformant to the ISP proforma, in that it assume the Fully Encoding option of the presentation protocol as required by the ISP but augmented with the PER-visible constraints defined in ISO/IEC 8823-1:1994/AM 2. In addition, the ATN profile mandates the selection of the "arbitrary" component.

6.3.2.2.7 Support of Syntaxes

Transfer Syntaxes Supported

The ATN specification is non-conformant to the ISP proforma, in that the transfer syntax selected for the System Management application is the Packet Encoding Rules (PER) instead of the Basic Encoding Rules (BER).

As a consequence, requirements specified in ISP chapter 8.1 to 8.7 are not applicable.

Abstract Syntaxes Supported

The abstract syntax is known by bilateral agreement and does not need to be exchanged and negotiated. It is specified in the application context defined for the System Management application.

6.3.2.2.8 Summary for Presentation Layer

The ATN profile for the presentation protocol and the support of the abstract and transfer syntaxes deviates from the requirements specified in the ISP. However, the ISP allows (see ISP sections 8.5 and 8.7) exceptions to these rules when clearly specified. When assuming the integration of CMISE and Rose in the ULCS architecture and the use of the efficiency enhancement option of the Presentation protocol, the requirements defined by the ISP being in conflict with the ATN profile are not valid any more. A new version of the ISP for this option should be released.

6.3.2.3 Session Layer

Annex C of ISP 11183 specifies the Session profile required to support the operation of CMISE and ROSE. The ISP does not take into account the efficiency enhancements option of the Session protocol required by the ATN profile.

6.3.2.3.1 Protocol versions implemented

Table 6-22. Session Protocol Versions Supported

ISP Index	Version	ISP Status	ATN Support
	Version 1	-	-
9.2	Version 2 (use of unlimited user data)	M	M

The ATN specification is aligned with the ISP 11183-1 for the protocol version to be supported by the SPMs.

6.3.2.3.2 Session Functional units

Table 6-23. Selection of Session functional units

ISP Index	Functional unit	ISP Status	ATN Support
C.2.1/1	Kernel (K)	M	M
C.2.1/2	Negotiated release (NR)	I	X
C.2.1/3	Half Duplex (HD)	I	X
C.2.1/4	Duplex (FD)	M	M
C.2.1/5	Expedited Data (EX)	I	X
C.2.1/6	Typed Data (TD)	I	X
C.2.1/7	Capability Data Exchange (CD)	I	X
C.2.1/8	Minor Synchronize (SY)	I	X
C.2.1/9	Symmetric Synchronize (SS)	I	X
	Data Separation		X
C.2.1/10	Major Synchronize (MA)	I	X
C.2.1/11	Resynchronise (RESYN)	I	X
C.2.1/12	Exceptions (EXCEP)	I	X

C.2.1/13	Activity Management (ACT)	I	X
See note	No-orderly release (NOR)	?	M
See note	Special User-data	?	X

Note. — Functional units added by efficiency enhancement ISO/IEC 8327-1 Amendment 1.

The ATN specification is non-conformant to the ISP proforma, in that the No-Orderly release functional unit shall be selected in addition to the Kernel and Duplex FUs. It is proposed to align the ISP to the ATN profile.

6.3.2.3.3 Protocol mechanisms

Table 6-24. Session Protocol Mechanisms Supported

ISP Index	Mechanism	ISP Status	ATN Support	Associated mnemonic
C.2.2/1	Use of transport expedited data (Extended control Quality of Service)	I	X	S-EXP_T
C.2.2/2	Reuse of transport connection (sending)	I	O	S-REUSE_T
C.2.2/3	Reuse of transport connection (receiving)	I	O	S-REUSE_T
C.2.2/4	Basic concatenation	M	N/A (Note 2)	
C.2.2/5	Extended concatenation (sending)	I	X	
C.2.2/6	Extended concatenation (receiving)	I	X	S-XCONC_RCV
C.2.2/7	Segmenting (sending)	I	X	S-SEG_SDR
C.2.2/8	Segmenting (receiving)	I	X	S-SEG_RCV
	Max. size of SS-user-data (S-CONNECT) > 512		O	S-MAXSIZE_512
C.2.2/9&10 5.3	Max. size of SS-user-data (S-CONNECT) > 10240	I	O	S-MAXSIZE_10240
	Max. size of SS-user-data (S-ABORT) >9		X	S-MAXSIZE_9
See note 1	Null-encoding protocol option	-	M	
See note 1	Short-connect protocol option	-	M	
See note 1	Short-encoding protocol option	-	X	

Note 1. — Protocol options added by efficiency enhancement ISO/IEC 8327-1 Amendment 1.
Note 2.— Only Category 1 SPDUs are used for this ATN profile. By definition, these are never concatenated. Therefore, Basic concatenation is not applicable to this specification, but is supported to the extent necessary for compliance with the ISO PICS.

It is proposed to align the ISP to the ATN profile.

6.3.2.3.4 Supported Roles

Session Connection

Table 6-25. Session Connection Roles Supported

ISP Index	Role	ISO Status	ATN Support	Mnemonic
C.2.3/1	Connection initiator	C(1)	M	S-CON_initiator
C.2.3/2	Connection responder	C(1)	M	S-CON_responder

(1) The ISP requires a conforming implementation to support at least one of these roles as required by the implementation.
The ATN specification is aligned with the ISP 11183-1 for the role of the SPMs during connection establishment.

6.3.2.3.5 Supported SPDUs

Support for the SPDUs associated with the Kernel functional unit

Table 6-26. Supported Session Protocol Data Units

		Sender		Receiver		
ISP Index	**SPDU**	**ISP Status**	**ATN Support**	**ISP Status**	**ATN Support**	**Mnemonics**
C.3.1.1/1 C.3.1.2/1	Connect (CN)	M	N/A (Note 4)	M	N/A (Note 4)	
C.3.1.1/2 C.3.1.2/2	Overflow Accept (OA)	I	N/A (Note 4)	I	N/A (Note 4)	S-OA_SDR / S-OA_RCV
C.3.1.1/3 C.3.1.2/3	Connect Data Overflow (CDO)	I	N/A (Note 4)	I	N/A (Note 4)	S-CDO_SDR / S-CDO_RCV
C.3.1.1/4 C.3.1.2/4	Accept (AC)	M	N/A (Note 4)	M	N/A (Note 4)	
C.3.1.1/5 C.3.1.2/5	Refuse (RF)	M	N/A (Note 4)	M	N/A (Note 4)	
C.3.1.1/6 C.3.1.2/6	Finish (FN)	M	N/A (Note 2)	M	N/A (Note 2)	
C.3.1.1/7 C.3.1.2/7	Disconnect (DN)	M	N/A (Note 2)	M	N/A (Note 2)	
C.3.1.1/8 C.3.1.2/8	Abort (AB)	M	N/A (Note 3)	M	N/A (Note 3)	
C.3.1.1/9 C.3.1.2/9	Abort Accept (AA)	I	N/A (Note 3)	I	N/A (Note 3)	
C.3.1.1/10 C.3.1.2/10	Data Transfer (DT)	M	N/A (Note 3)	M	N/A (Note 3)	
C.3.1.1/11 C.3.1.2/11	Prepare (PR)	I	X	I	X	S-PR_SDR / S-PR_RCV
See note 1	Short Connect (SCN)	C(2)	M	C(2)	M	
See note 1	Short Accept (SAC)	C(2)	M	C(2)	M	
See note 1	Short Refuse (SRF)	C(2)	M	C(2)	M	
See note 1	Null (NL)	C(3)	M	C(3)	M	
See note 1	Short Connect Continue (SCNC)	C(1)	N/A	C(1)	N/A	
See note 1	Short Accept Continue (SACC)	C(2)	M	C(2)	M	
See note 1	Short Refuse Continue (SRFC)	C(2)	M	C(2)	M	
See note 1	Short Finish (SFN)	C(1)	N/A	C(1)	N/A	
See note 1	Short Disconnect (SDN)	C(1)	N/A	C(1)	N/A	
See note 1	Short Data Transfer (SDT)	C(1)	N/A	C(1)	N/A	
See note 1	Short Abort (SAB)	C(1)	N/A	C(1)	N/A	

Note 1. — PDUs defined in efficiency enhancement ISO/IEC 8327-1 Amendment 1.
Note 2. — Not applicable, as the no-orderly-release functional unit is selected.
Note 3. — Not applicable, as the null-encoding protocol option is selected.
Note 4. — Not applicable, as the short-connect protocol option is selected.

(1) Used only if the short-encoding protocol option is selected.
(2) Used if short-encoding or null-encoding is used.
(3) Used only if the null-encoding protocol option is supported.

SCN, SAC, SRF, SACC and SRFC SPDUs shall([188]) be encoded such that the parameter bit of the SI&P octet is set to the value 0, indicating that all following octets are User-information (i.e. no SPDU parameters are present).

Note. — This is a requirement of the null-encoding protocol option.

It is proposed to align the ISP to the ATN profile.

6.3.2.3.6 Use of null-encoding and short-connect protocol options

The null-encoding and short-connect session protocol options are to be selected for use, with requirements as specified in Table 6-27.

Table 6-27. Use of the null encoding and short-connect Session protocol options

Ref.	Requirement	ATN Requirement	SM context
A	The calling and called session selectors are null	M	ok
B	The session-requirements parameter in the S-CONNECT service includes the kernel, full-duplex and no-orderly-release functional units only.	M	ok

6.3.2.3.7 Summary for Session Layer

ISP 11183-1 specific does not apply to the ATN profile since it covers the full session presentation. However, once the ISP upgraded to take into account the efficiency option of the session protocol, there is nothing that makes the ATN session profile incompatible with of the use of the Session service by an Application Entity including CMISE and ROSE.

6.3.2.4 Conclusion

This analysis shows that there is no objection to the integration of the System Management Application (SMA) within the ICAO-specified ATN Upper Layer Architecture. ISP 11183-1 specifies the constraints put on the upper layer systems claiming the support of CMISE and ROSE communication requirements. The more restrictive constraints are placed on the Presentation layer to allow the handling of several ASEs within the Application Entity. The ATN ULA has been defined to handle such Application Entities (see air-ground and ground-ground applications). Therefore, these constraints are not relevant. The ISP should be reviewed to integrate the efficiency option of the Session and Presentation protocols.

6.3.3 Alternative Internal Architectures for the System Management Application

The ATN ULA provides a framework for the specification of the applications based on the OSI extended application layer structure. However, the internal organisation of the application entities is not predefined. Thus, the air-ground CNS/ATM-1 applications (CM, ADS, CPDLC and FIS(ATIS)) are not structured the same way the AIDC application is. A third alternative is even suggested by the ULCS Provisions (Sub-Volume IV), which consists in inserting some new Application Service Elements (ASE) in the lower part of the AE enhancing the dialogue service.

This chapter reviews the generic ULCS framework applied to Systems Management and analysis the alternative solutions.

The assumptions made in this chapter are that SM exchanges are likely to occur during the flight between an airborne agent and a ground manager and that the ATN Upper Layer Architecture has been selected for hosting the SM Application. The selection of Systems Management Functions (SMF) and the definition of the Management Information Base (MIB) for the ATN environment is not taken into account in this chapter.

Note.— The justification of these assumptions and the selection of the SMFs is out of the scope of this discussion.

6.3.3.1 Functional Model

The functional model used to represent the Systems Management Application and the supporting Upper Layers is depicted in Figure 6-10. The functional modules are described below.

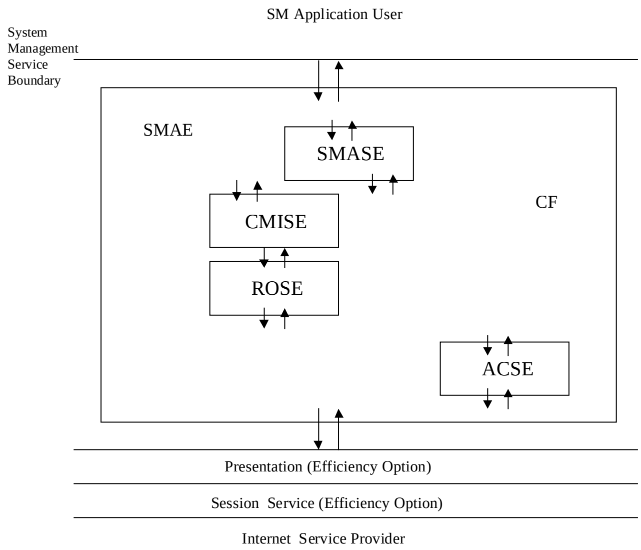

Figure 6-10. Functional Model of the SM Application and Supporting Upper Layers

The SMAEs provide the OSI communication services required by the SM Agent and the SM Manager. The SM Agent is a specific SM-user taking the role in which it is capable of performing management operations on managed objects and emitting notifications on behalf of managed objects. The SM Manager is a specific SM-user taking the role in which it is capable of issuing management operations and receiving notifications.

The ACSE provides services to establish, maintain and release application-association between application entities.

The CMISE negotiates with the peer the protocol version and the protocol functional units supported on the SM association. It provides CMIS-users with services handling Managed Objects (emission of notifications, operations on MOs such as creation, operation, attribute setting or retrieval, etc…) and the actions of requesting filtering and scoping. CMISE is not aware of the availability of an association. The management of the association is outside the scope of the CMISE protocol and shall be handled by the CMISE service user, i.e. the SM-user (in mode "explicit") or the CF (in mode "implicit").

The ROSE materialises the concept of remote operations by defining a common notation between the system requesting a action and the system performing this action.

The SMASE provides service to the users of the Systems Management AE (SMAE). The SMASEs negotiate during the association establishment the SM Functions activated on this association.

SMF negotiation is defined in ISO/IEC 10040 as an optional procedure. This negotiation is usually not performed by off-the-shelf SM products. An a-priori knowledge of the supported SMFs could be sufficient. It is proposed that the ATN SM AEs do not negotiate the SMFs.

As a consequence, the SMASE could be omitted in the SM ULA since it does not carried out actual protocol and only provides a pass-through service to CMIS and Dialogue services. However, if it is decided to implement a specific protocol for handling ATN dedicated SM functions (e.g. file transfer exchanges or the manager to manger communications), a SMASE could be useful.

The SMASE, CMISE and ROSE share a single abstract syntax. The merged abstract syntax {joint-iso-ccitt ms(9) cmip(1) cmip-pci(1) abstractSyntax(4)} is defined in ISO/IEC 9596-1.

The SM CF is responsible for the mapping of the service primitives issued/received by/from the SM Application User, the ASEs of the SMAE and the Presentation Service Provider. It is also responsible for initiating the association release when requested by the SM-users.

The SM CF provides CMISE and ROSE with the means to exchange data during association establishment and association abort:

a) the initiator CMISE is requested to build the initial APDU sent to the peer to negotiate the protocol options ("CMIPUserInfo" type as defined in 9596-1). The initiator CF sends this APDU as an EXTERNAL element of the "user information" parameter of an A-ASSOCIATE. The responder CF makes available this APDU to the responder CMISE.

b) likewise, CMISE is requested to build the abortive APDU sent to the peer when aborting the association. The CF sends this APDU as an EXTERNAL element of the "user information" of an A-ABORT.

6.3.3.2 The SM Abstract Service

The SM Abstract Service is the service provided by the SM AE to the SM-Users. This abstract service is described in ATN Technical Provisions Sub-Volume 6.

This section provides an example of what this abstract service could be. It is assumed that the "explicit" mode is selected for the AE, i.e. the SM-users are responsible for triggering the establishment and the release of the association with the peer.

SM Communication Management

SM-OPEN Service

Parameter Name	Req	Ind	Rsp	Cnf
SM Called Peer Id	M			
SM Calling Peer Id	U	C(=)		
CMISE Funtional Units				
AccessControl	U	C(=)	U	C(=)
UserInfo	U	C(=)	U	C(=)
Result			M	M(=)

Note 1. If the receiving CMISE rejects the association based on protocol version or access control check, there is no indication issued to nor response expected from the peer SM-user.
Note 2. No Class Of Communication parameter is defined since the value for the Routing Class is predefined for Systems Management communications.

SM-CLOSE Service

Parameter Name	Req	Ind	Rsp	Cnf
Result (?)			M	C(=)
SM-user data (?)	U	C(=)	U	C(=)

SM-ABORT

Parameter Name	Req	Ind
SM-User Data (?)	U	C(=)

SM-P-ABORT

Parameter Name	Ind
Reason	M

SM Information Exchange

The following services are deduced from the corresponding CMIS services:

a) SM-CANCEL-GET service,

b) SM-EVENT-REPORT service,

c) SM-GET service,

d) SM-SET service,

e) SM-ACTION service,

f) SM-CREATE service, and

g) SM-DELETE service.

SM File Transfer

Additional services could be added to the SM service if they can't be provided through existing SM services and the definition of MOs. The corresponding protocol is carried out by the ATN SMASE. For instance, if it is decided to not use the CMIS stack to transfer log or configuration files, the following services could be defined as part of the SM service:

a) SM-GETFILE

b) SM-PUTFILE

6.3.3.3 The SM AE Architecture

The functional model described above could fit in the Upper Layer Architecture described in ATN Technical Provisions Sub-Volume 6 as one of the three following options:

a) architecture #1 is based on the ATN air-ground application model. The Dialogue service is "used" in the AE to communicate with the peer.

b) architecture #2 is based on the AIDC application model. The CF manages the association on behalf of the App-ASE. The App-ASE simply sends data without knowledge of the status of the association.

c) architecture #3 defines a new concept, the "managed dialogue service". This architecture is a variant of Architecture #1 where the dialogue service provided to the App-ASE includes also SM services.

These 3 architectures are discussed below.

Architecture #1: The ATN Air-Ground Application model

The Dialogue Service defined in the CNS/ATM-1 ULA is provided unchanged. Likewise the CNS/ATM-1 ATN applications were designed, the lower part of the SMAE CF hides the ACSE and Presentation services by providing the Dialogue service. The Dialogue service identifies the artificial boundary between the "Upper CF" and the "Lower CF". The "Lower CF" is fully specified in Sub-Volume 6. A SMASE is present if required. In the following, it is assumed that there is no SMASE.

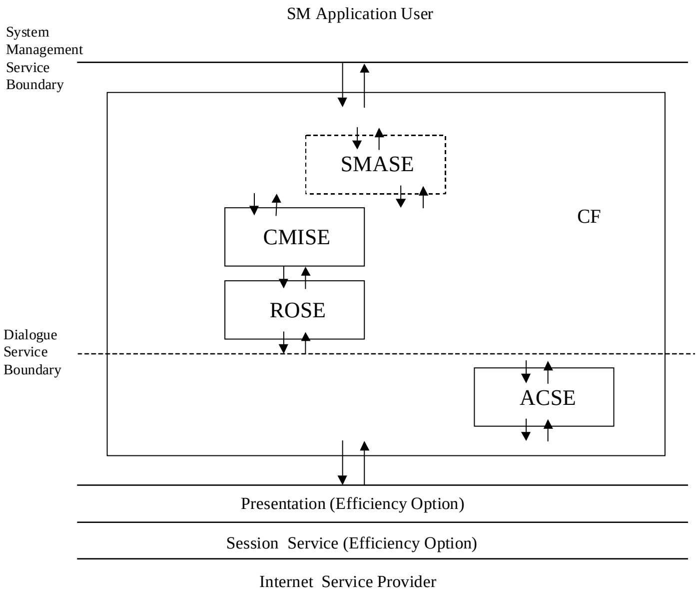

Figure 6-11. Architecture #1 - Use of the CNS/ATM-1 Dialogue Service

The "Upper CF" uses the Dialogue service to establish, release and abort the application-association with the peer SMAE and to exchange SM information when requested by CMISE and ROSE. The CMIS service is provided unchanged to the SM-users as part of the SM service.

The actions of the "Upper CF" shall be specified in Sub-Volume 6, in particular the actions to handle the primitive exchanges between the SM-users and CMISE, between the SM-users and the DSP and between ROSE and DSP. In particular, the CF is responsible for mapping the Presentation service primitives (P-DATA request and indication) used by ROSE at its lower interface to the Dialogue service interface.

Note.— The "Upper CF" was empty in the specification of the air-ground applications since the ASE service and the AE service were identical and since the ASEs were designed to use directly the Dialogue service. This is not the case here since CMSE/ROSE expects from the communication service provider a Presentation service.

The "Dialogue Abstract Service" and the "Lower CF" specified for the CNS/ATM-1 ULA remain unchanged. The Sub-Volume 6 sections describing the "Upper CF" (e.g. 4.3.3.2 "Services Invoked by the Application User") shall be made "non-effective".

This approach permits to not touch the ULA Provisions. The Sub-Volume 6 section describing the SM Application could be based on the Sub-Volume 2 layout (introduction, abstract service description, ASN.1 description, protocol specification, communication requirements, user requirements) with an additional section for the "Upper CF".

Note.— The main problem of this architecture when used for the ATN air-ground application was the induced complexity of the App-ASE protocol, because the states of the underlying dialogue (e.g. pending establishment, established, pending release, collision) should be handled by the ASE protocol itself. For the SMAE, CMISE and ROSE assume the association established and invoke only a data transfer primitive. This problem will therefore not be encountered for the specification of the SM application.

Architecture #2: The AIDC Application model

The Dialogue Service defined in the CNS/ATM-1 ULA is not used as such in the SMAE specification. In the same way as the CNS/ATM-1 AIDC application was designed, the entire SM CF is fully specified. An SMASE is present if required. In the following, it is assumed that there is no SMASE.

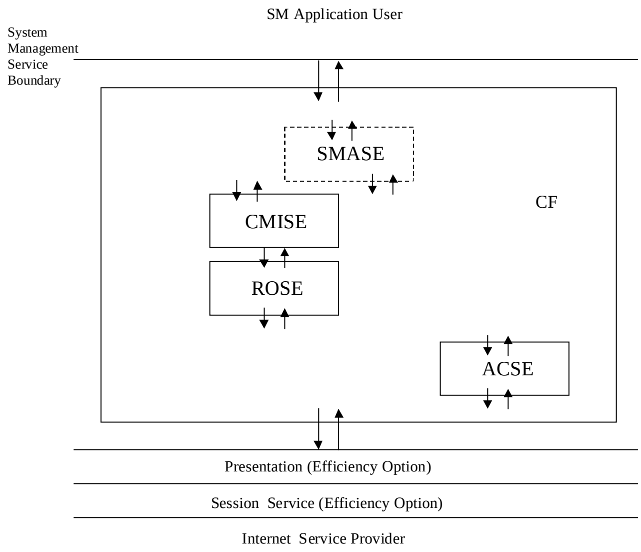

Figure 6-12. Architecture #2 - AIDC Model

In this architecture, the CF uses the ACSE Service to establish, release and abort the association with the peer SM and the Presentation service to exchange SM information when requested by CMISE and ROSE. The CMIS service is provided unchanged to the SM-users.

The main interest of this architecture is the simplification of the ASE protocol since the ASE is not responsible for tracking the state of the underlying association (the drawback being the inverse complexity added to the CF specification…). This is the case for the SM application, since CMISE and ROSE assume the presence of an association.

This approach permits the ULCS Provisions to be unchanged. Sub-Volume 6 will include the specification of the SM abstract service and the specification of the full CF. However, this implies a duplication of specification for the generic functions provided by the DSP as the mapping of the P-RELEASE and P-ABORT primitives onto the Dialogue primitives or the CF APDU management. This duplication not justified and potential source of errors could be avoided by using the Dialogue service, i.e. selecting the architecture #1 described above. It is therefore proposed to not choose this architecture.

<u>Architecture #3: "Managed Dialogue Service"</u>

This architecture is identified in Sub-Volume 4 section 4.3.1.1 as a possible evolution of the current ULA. This evolution consists in the addition of new ASE ("Future ASE") in the Dialogue Service Provider. The proposed architecture is to combine CMISE/ROSE with ACSE in the lower part of the AE. The CMIS service becomes part of the provided Dialogue service. An SMASE is present if required. In the following, it is assumed that there is a SMASE.

The rationale for proposing this approach is that the CMIS service can be viewed as a generic service which should be made available to a large number of SM applications: configuration, performance, accounting and security related applications are candidates for using the CMIS service.

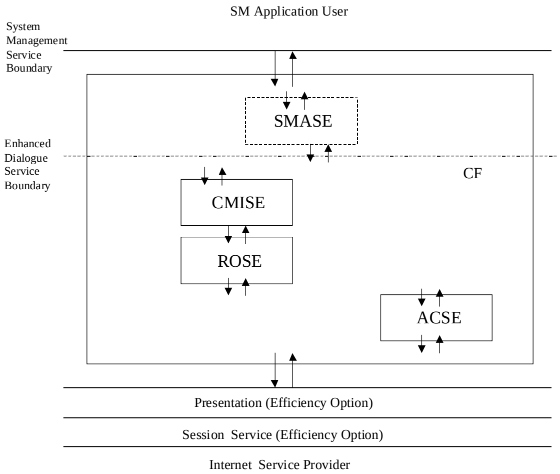

Figure 6-13. Architecture #3 - Managed Dialogue Service

In this architecture, the SMASE uses the Dialogue Service for both dialogue establishment and SM data communication.

The "Upper CF" provides a pass-through service between the SM AE service and the SMASE service. Depending on the lower interface defined for the SMASEs (i.e. does the SMASE use the Dialogue service?), the "Upper CF" is empty or not. The specification of the "Upper CF" is therefore straightforward.

The following additional service primitives would need to be added to the Dialogue Abstract Service:

a) D-CANCEL-GET service,

b) D-EVENT-REPORT service,

c) D-GET service,

d) D-SET service,

e) D-ACTION service,

f) D-CREATE service, and

g) D-DELETE service.

The "Lower CF" described in Sub-Volume 4 would need to be upgraded as follows:

a) The START and ABORT actions performed by the CF shall be slightly modified in order to include CMISE initial/abortive data in the user data of the A-ASSOCIATE and A-ABORT service primitives.

b) The new Dialogue request/response primitives shall be mapped to the peer CMIS request/response primitives. CMISE indication/confirmation primitives shall be mapped to the peer new Dialogue indication/confirmation primitives.

c) A Presentation Context identifier shall be assigned to ROSE/CMISE APDUs (e.g. the reserved value "2").

Attention must be given to backward compatibility. A ULCS stack providing the managed dialogue service must be able to interact with a remote ULCS stack providing the basic dialogue service, given that none of the SM services is used.

Attention must also be given to keeping the Dialogue Service Provider as generic as possible. In particular, the CF would not perform actions specific to a given ASE (here CMISE/ROSE).

Conclusion

Architectures 1 and 3 are the most serious candidates for SM Application. However, architecture 3 impacts the existing Provisions much more than architecture 1, since the CF specified in Sub-Volume 4 is modified. Architecture 1 is therefore the preferred solution.

6.4 Use of the ATN Transport Service

6.4.1 The ATN specific parameters

The ATN upper layers make use of the Transport Service provided by the ATN Internet. This service differs from the ISO standard TS, as it provides the applications with the visibility of parameters used by the ATN internet for data routing, depending directly of the type of application and the quality of service requirements of the communication service users. In addition to the usual QOS transport service parameters (Transport checksum, priority), an ATN specific parameter has been defined at the transport interface level (Security Label). All these parameters have to be handled by the AE.

Use of the Transport checksum

The TS-User specifies whether the transport checksum is required on a particular instance of communication. In the Sub-Volume 4 ULCS this is done by the Dialogue Service user specifying the required residual error rate in the T-CONNECT quality of service parameter.

> *As for the other air-ground applications, the residual error rate requested for the SM application will be "low", meaning that the transport checksum mechanism is to be operated.*

Transport connection priority

The application belongs to an application category to which a priority is assigned. The value of the priority parameter is therefore not given by the application user but is a given per application.

> *The priority value assigned to the SM Application is "Network/Systems Administration".*

ATN Security Label

The TS-user is responsible for passing the ATN security label parameter to the TS-provider with the format specified in the ATN internet Provisions. It defines for an instance of communication the traffic type (ATSC, AOC) and the category (class 'A' to 'H' for ATSC, representing the requested transit delay). The value of the traffic type is given per application (e.g. the CNS/ATM-1 applications are ATSC applications). The category is provided by the application user through the 'Class of Communication" parameter.

> *The SM Application will be assigned a traffic type dedicated to system management exchanges "ATN SM Communications: No Traffic Type Policy Preference". There is no category for this traffic type.*

Editor's Note.— The following text has been adapted from the equivalent section of the AMHS Guidance Material in the Comprehensive ATN Manual (CAMAL) Part III, section 6.2.2.

An ATN Manager or Agent application by definition uses the ATN Transport Service to communicate with peer systems management entities.

Several parameters need to be given to the transport service provider when requesting a transport connection to be established. These parameters are specified in Sub-Volume 5 of the ATN Technical Provisions. For most of these parameters, a single value is selected, either in the Technical Provisions or as a local matter, to be used when establishing a transport connection between two ATN SM applications.

More specifically, the base SM standards used in these Technical Provisions do not allow for the establishment of different transport connections with different quality of service parameters, based on the distinction between application level priorities. Thus a single transport priority is used.

The way to request the use of the specified parameters at the Transport Service provider is an implementation matter which is out of the scope of the ATN Technical Provisions.

6.4.2 Use of the Transport Service for the AOM 12 Profile

If profile AOM 12 is supported, then the profile is intended to be capable of using any supporting T- profile for the connection-mode ISO transprt service. This would include for example an ISO 8073 Class 0 Transport protocol (TP0) over X.25. This cannot be implemented over the ATN, it is therefore out of the scope of the ATN Technical Provisions. However it may be required, for example, if interconnection with a public managed network is the local policy of a given Management Domain.

In such a situation, the co-existence of the support of Classes 0 and 4 of the ISO 8073 Transport protocol is an implementation matter, which is out of the scope of the ATN Technical Provisions.

Furthermore, the parameters specified concerning the use of the ATN Transport Service are not applicable in such a context.

6.4.3 Implementation options

For those off-the-shelf SM applications which do not intrinsically support the use of the ATN Transport Service, the otherwise compliant upper layers and application entities may be integrated as follows with the lower layers of an ATN end system.

At the lower boundary below the upper layers and application implementation, a transport service interface may be specified to intercept the transport service primitives, and to map these onto ATN Transport Service primitives using the intercepted data and additional parameter values which cannot be passed from the upper layers.

The consolidated ATN Transport Service primitive can then be passed to the transport service provider which provides the ATN Internet Communication Services.

The parameters required by the ATN Transport Service Provider for the establishment of an ATN transport connection are specified in section 5.5.1 of the ATN Technical Provisions. They are as follows:

a) called and calling TSAP addresses;

b) whether or not the expedited data option is required;

c) the required residual error rate (RER) to determine whether or not non-use of the transport checksum is allowed;

d) the Transport Connection Priority to be mapped into the resulting CLNP (Connectionless Network Protocol) NPDUs (Network Protocol Data Units); and

e) the ATN Security Label.

The ATN Security Label and the requested Transport Connection Priority are examples of additional parameters which cannot be passed from the non-ATN specific upper layers.

Such an implementation architecture is depicted in Figure 6-14.

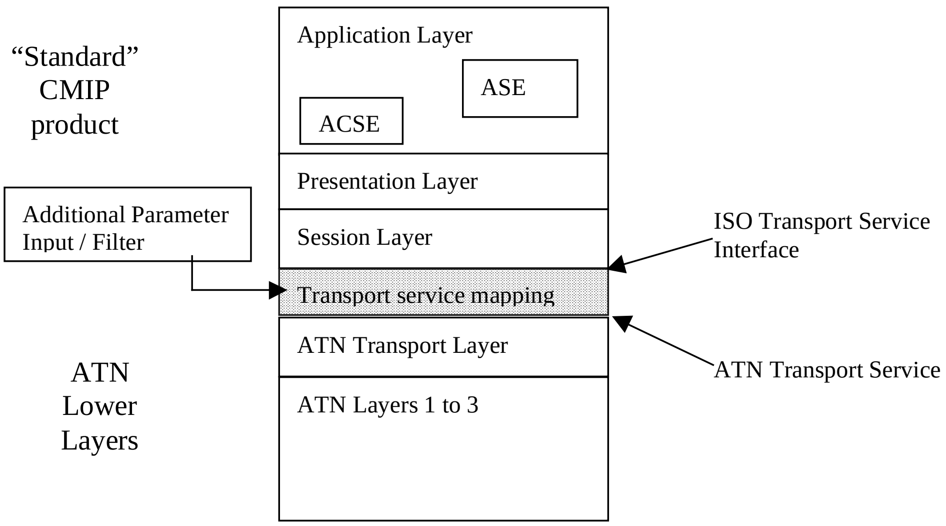

Figure 6-14. Transport Service Mapping

A similar mapping mechanism between a lower boundary interface and the transport service interface offered by the actual transport service providers may also be implemented in case of co-existence of different transport protocol stacks within a single system (e.g. ATN Transport Service and ISO TP0 over X.25 for connectivity towards a public managed network).

6.5 Requirements for Application Management

Editor's Note.— The text for this section is extracted from WG3 WP12-10: "System management requirements for air-ground CNS/ATM-1 package applications" by F. Picard..

6.5.1 Assumptions on the System management environment

6.5.1.1 Administrative Authorities

Management operations are usually performed by Administrative Authority (AA). An AA is an administrative unit responsible for the correct functioning of a set of systems and resources involved in the ATN data link operations.

As far as the application resources management is concerned, two types of AAs are of interest: the airline AA and the ATC AA respectively responsible for the management of the applications on-board and of the ground-based applications.

The Management Domain assigned to these AAs considered is limited - in the scope of this document - to communication resources implemented by the ATS CNS/ATM-1 air-ground applications, although other Management Domains could be defined for other types of applications (e.g. AOC). It is assumed in this document that the scope of the AAs is limited to the resources related to the applications hosted in the air and ground ATN ESs. The management of resources controlled by the lower layers (1-4) of both ESs and ISs and by the upper layers (5, 6 and part of 7 up to the dialogue service) of the ESs is outside the scope of this document.

6.5.1.2 SM Managers

An airline AA monitors and controls the operation of the airborne part of the air-ground applications. An airline AA operates several distributed SM managers or a centralised SM manager on the ground. As the distribution of the management centres on the ground does not impact the application SM requirements, the assumption is made that there is a single Airline SM Centre per airline from which all SM data related to the aircraft is sent and processed.

The assumption is taken here that there is no SM manager installed in the aircraft. If there is one, the communications between the air manager and the air agents is a local matter.

The ATC AA may have distributed SM managers or a centralised SM manager on the ground. An ATC AA monitors and controls the operation of the ground part of the air-ground applications. The assumption is made here that **there is a single Management ATC SM Centre per ATC Authority**. ATC AAs do not communicate directly with airborne SM agents.

Airline and ATC SM Centres may need to exchange SM information. This will be done through exchanges between SM Managers based on bilateral agreements defining the nature of the exchanges (types of information, triggering events, frequency, etc…). The SM information exchanged between SM Centres shall be covered by an ICAO standard.

This document focuses on the exchange of management information between agent and managers belonging to the same AA. In theory, this contents of this information is to be defined by each AA, independently of the other AAs. Actually it is not required to standardise this information nor the communication protocols needed to exchange this information on a world-wide basis. Only communications between managers of different AAs are required to be normalised. These communications are not covered by this document.

6.5.1.3 SM Agents

Each airborne ES implements a SM agent. The airborne SM Application Entity has a direct visibility of the Managed Objects (MOs) which have been defined in order to model the application resources implemented in the ES.

Each ground ES implements a SM agent. The ground SM Application Entity has a direct visibility of the Managed Objects (MOs) which have been defined in order to model the application resources implemented in the ES.

6.5.2 System Management Requirements of ATN Upper Layers and ATN Applications

System Management activities are usually grouped into the five following areas:

a) Fault management,

b) Configuration management,

c) Accounting management,

d) Performance management, and

e) Security management.

The SM Application provides services supporting one or several areas. This section aims at identifying precisely the nature of these services, limiting the scope of the managed objects to the air-ground ASEs.

6.5.2.1 Fault Management

6.5.2.1.1 High Level Requirements for Fault Management

Fault management concerns the detection of a problem, fault isolation and correction to normal operation. Although fault management can to a certain extent be achieved by polling the managed objects, and searching for error conditions, fault management deals most commonly with notifications as they occur. Data reporting mechanisms to report alarms or alerts is the best way to accomplish health checks of specific managed object's performance without having to double the amount of polling being accomplished. ISO has defined a specific notification (communicationAlarm) for reporting alarm conditions.

The ATN Provisions shall cover the management of faults which affect the ATN communication between organisations and between the air and the ground.

Faults detected and notified to SM managers reflect communication errors that occurred in the communication part of the ATN applications, i.e. the Application Entities. Faults indicate the abnormal behaviour of the ASE. It should be clear that operational fault detection and management are under the responsibility of the application service users and are therefore outside the scope of the ATN SM application (e.g. user actions not conforming to user requirements (ATN Technical Provisions chapter 7).

Faults identified shall reflect a failure of the communication system. 'Operational' faults are not relevant for the SM managers.

ASE communication faults shall be tracked in the following conditions:

a) inability of an application entity to establish communications with a peer application entity,

b) loss of end-to-end communication between peer application entities, and

c) inability of the application entity to provide correctly the application service.

When the fault can be detected before it becomes serious, an alarm should be produced. This alarm is needed only if the application user or the SM manager is able to react in such a way that the fault is avoided. Otherwise, the alarm is useless.

An alarm should be sent when the fault occurrence is detectable.

Likewise, a detected fault shall be notified on-line to a SM manager if and only if this SM manager is able to react to the fault and improve the fault situation. Otherwise, a log of the fault notification (via SM log procedures) or a local log of the event (via local trace procedures) is sufficient.

A fault notification shall be sent only to managers that can correct the fault situation immediately. Otherwise a trace in a log is sufficient.

6.5.2.1.2 Faults in the CNS/ATM-1 ASEs

This section identifies amongst the faults occurring in the CNS/ATM-1 applications (CM, ADS, CPDLC and FIS(ATIS)) the ones which have to be tracked by the SM application. Basically, they are three types of errors affecting the ASEs: faults generated by the application-users, by the ASE and by the dialogue service provider.

6.5.2.1.3 Application-user faults

Local faults initiated by the application-users (e.g. invalid primitive or primitive parameter, primitive out of sequence) are detected locally by the ASE. The peer ASE is not informed of the fault. The fault is indicated via a local means to the application-user which should log the fault notification and take the appropriate corrective action (redo or user-abort). A remote SM manager would be unable to intervene, so there is no need to inform him on-line.

User-generated abort reflect the detection by the user of a serious error. Such abort causes the brutal termination of the pending application communications.

The failure of an instance of communication due to a user abort shall be logged.

6.5.2.1.4 Dialogue Service Provider faults

When a fault occurs in the dialogue service provider, a provider abort primitive is indicated to the application-users. Such abort causes the brutal termination of the pending application communications. Very likely the fault has been also detected in the communication layer where it occurred and notified to the SM manager according to its severity. There is no need to send at the application level a fault notification to the SM manager.

The failure of an instance of communication due to a failure of the communication service provider shall be logged.

6.5.2.1.5 ASE-generated faults

These faults are identified in the application Provisions under the heading "Exception Handling". They identify either an error in the local ASE (e.g. an unrecoverable error) or in the peer ASE (e.g. reception of an invalid or not permitted PDU, time-out, etc.).

It is assumed that ATC AAs are interested in being informed of these kind of errors as soon as possible. The ASEs constitute the critical path of the operational data link information. On the ground, they provide communication services to a wide range of users: controllers, surveillance systems, safety-related systems, meteorological systems, etc… Switch to a backup system could be a corrective action when such an error is experienced.

The airline AAs are less interested to get the fault notification on-line since a ground controlled action would be difficult to implement.

The failure of an instance of communication due to an error within the application shall be

a) logged when detected in the aircraft,

b) notified to the SM manager when detected on the ground.

In most cases, ASE level faults detected at one side are indicated to the other side via the exchange of an ABORT PDU. In other words, a resource in the air ES and a resource in the ground ES are able to detect the same ASE fault. By looking at the abort reason, both ESs are aware of the nature of the fault, except when the transmission of the ABORT PDU is not possible (e.g. when an unrecoverable error is detected, it is likely that the system can not communicate any more). The only exception to this rule is when the application-association can not be established due to a problem of the peer ASE not detectable in the peer ASE (e.g. invalid TSEL, unrecoverable error in the Transport, Session, Presentation, the ACSE or the CF). However, this error is detected in the transport or in the upper layers of the peer ES.

Based on the fact that both sides are aware of the ASE-generated fault, there is no need to downlink fault notification in real-time to the airline SM manager. The ATC SM manager can forward the notification to the airline SM manager.

The fault notifications issued by airborne agent are logged locally. The fault notifications issued by ground agents are sent to the ground ATC managers which can forward these notifications to the airline managers, based on bilateral agreements between the airline AA and the ATC AA.

6.5.2.2 Configuration Management

6.5.2.2.1 General Requirements

Some configuration parameters inherent to the ASEs may have to be known and/or modified by the SM manager. Two types of parameters exist:

- configuration parameters defined in the ATN Technical Provisions.

The static configuration of an ES is determined by the identification of the applications actually installed in the ES, the subsetting rules of each ASE and the ASE version number. These parameters are fixed for a given aircraft or a given ground system. They are defined based on operational requirements and local choices of the airline or the ATC authority.

There is actually no need to change the ASE static configuration before or during the flight. However, the knowledge of the values taken by these parameters may be very useful to understand the global behaviour of the ASE.

The SM manager shall be able to assess the data link application capability of an ES and to get the functional configuration of each application.

Very few parameters are defined in the ASE Provisions as variable configuration parameters. Actually, only the technical timers may be configurable in the ASE. Values indicated in the ATN Technical Provisions are only indications of reasonable values. In some operational contexts, the timer values may have to be customised. Some implementations may choose to have fixed values for the timers whereas others will allow to configure them.

- Implementation dependent parameters.

Each implementation defines its own configuration parameters. The way the value of these parameters can be changed (locally or remotely, via operator commands or command files, etc...) is very dependent of the design of the implementations. Moreover, the configuration parameters are visible only within a management domain. It is unlikely that an AA will allow an other AA to retrieve and modify the configuration of its systems.

The definition of the configuration parameters and the configuration means are outside the scope of the ATN Technical Provisions.

6.5.2.3 Accounting

6.5.2.3.1 General Requirements

Accounting management is responsible for collecting and processing data related to resource consumption in the system. The historical record of the usage of the resources may be necessary to understand how a problematic situation occurred.

The usage of the application resources can be measured by the user activity. Two levels of measures may be required. Global statistics should permit to evaluate the amount of activity for a given application and detailed statistics should allow to understand the activity with a particular peer system.

The number of invocations of each application service shall be made available for off-line analysis at application level and instance of communication level.

The amount of resources in use for a given application is also characterised by the number of simultaneous instances of the ASEs, and for each instance the identity of the peer system, the mode of the ASE when modes are defined (e.g. CPDLC/DSC/Forward), the mode of termination of each instance and, when relevant, the way the communication resources are managed by the users (e.g. the maintain dialogue option).

The ES shall notify every creation and deletion of instance of communications with the associated parameters.

6.5.2.4 Performance Management

Performance management shall allow monitoring the end-to-end performance of the ATN system provided to the application users. It enables evaluation of the effectiveness of the communication resources during the operational functioning thanks to statistical information and logs of system state histories.

The workload of the applications is already measured - globally or on a connection basis - by the parameters identified in the previous section for the accounting functional area (number and type of service invocations by the users).

The ADSP Manual defines in Part I, Chapter 3 Appendix A three types of communication systems performance requirements related to the ATS data link applications:

- General Performance Requirements

The general performance requirements on the air-ground applications are the following:

a) the probability of non-receipt of a message will be equal to or less than 10^{-6},

b) the probability that non-receipt of a message will fail to be notified to the originator will be equal to or less than 10^{-9}, and

c) the probability that a message will be misdirected will be equal to or less than 10^{-7}.

These performance requirements can not be monitored at application level. These performance metrics could be evaluated at transport level.

- Application Specific Performance Requirements

The performance requirements specific to each air-ground application is also defined in the ADSP Manual, as shown below for the CM application.

Table 6-28. Application Specific Performance Requirements

APPLICATION	AVAILABILITY	INTEGRITY	RELIABILITY	CONTINUITY
CM	99.9%	10-6	99.9%	99.9%

It seems difficult to monitor these performance requirements at application level.

- Transfer Delay Requirements

Table 6-29. Transfer Delay Performance Requirements

PERFORMANCE LEVELS	MEAN END-TO-END TRANSFER DELAY	95% END-TO-END TRANSFER DELAY (SECONDS)	99.996% END-TO-END TRANSFER DELAY (SECONDS)
A	0.5	0.7	1
B	1	1.5	2.5
C	2	2.5	3.5
D	3	5	8
E	5	8	12.5
F	10	15	22
G	12	20	31.5
H	15	30	51
I	30	55	90
J	60	110	180

It is proposed to measure the transit delay at the application level. As the transit delay is indirectly dependant of the requested class of communication service, this parameter should be made available with the transit delay measurements.

As the messages are not time-stamped and there is no clock synchronisation mechanisms, the measurement of the transit delay shall be performed on a round trip exchange. The measure includes the transmission time of the request message, the message computation time by the remote system, the human response time and the transmission time of the corresponding response message. If no dialogue was in place, the delay includes the connection establishment delay and the transfer delay for the two messages. Otherwise, the delay includes the data transfer delay for the two messages only.

The mean and max values shall be measured for each confirmed application service.

6.5.2.5 Security Management

Security management is responsible for controlling access to the system resources through the use of authentication techniques and authorisation policies. Security functions are performed by the upper layers on behalf of the applications. It is likely that a specific ASE will be designed to handle security mechanisms.

The ASEs themselves will probably not perform security related actions. As a consequence, no resources will be defined at present in the ASE MIB to cover security.

7. REFERENCES

[1] ISO/IEC 9596-1 (X.711) - Information Technology - Open Systems Interconnection - Common Management Information Protocol - Part 1: Specification

[2] ISO/IEC ISP 11183-1 - Information Technology - International Standardized Profiles AOM1n, OSI Management - Management Communications - Part 1: Specification of ACSE, presentation and session protocols for use by ROSE and CMISE

[3] ISO/IEC ISP 11183-2 - Information Technology - International Standardized Profiles AOM1n, OSI Management - Management Communications - Part 2: CMISE/ROSE for AOM 12: Enhanced Management Communications.

[4] ISO/IEC 9072-2 (X.229) - Information Processing Systems - Text Communication - Remote Operations - Part 2: Protocol Specification

[5] ISO/IEC 8825-2 (X.691) - Information Technology - ASN.1 Encoding Rules: Specification of Packed Encoding Rules (PER)

[6] ATNP/WG3/SG3/WPxxx - System Management Application (SMA) - The Fast MIP Option - draft paper by F. Picard, February 1998

8. Issues / Work In Progress

1. Should inter-domain MO definitions be given in Guidance Material, and if so, to what level of specification? It may be desirable to adopt a common framework in order to reduce procurement and deployment costs, but should States be encouraged to build a specified GDMO MIB?

2. None of the MOs defined to date can be considered as stable. Detailed technical review is needed. Also consistency check with ACI/ProATN Convergent MIB.

3. There may be significant bandwidth savings if the CMIP APDUs were augmented with PER-visible constraints and extensibility markers. The resulting abstract syntax would be input to the ISO/IEC and ITU standardisation process. Studies of encoded CMIP PDUs are in progress.

4. Does there need to be a separate containment tree per class of Router?

5. What does the distinguished name of “system” look like?

6. How should the requirements for “full stack” management, such as ATSMHS be documented. ATSMHS will make use of ISO standards and profiles (see WG3/IP12-06)
   For example:
   ISO/IEC 11588-3 Information technology - Message Handling Systems (MHS) management - Part 3: Logging information
   ISO/IEC 11588-8 Information technology - Message Handling Systems (MHS) management - Part 8: Message Transfer Agent management.

7. What are the requirements for subnetwork management - there are no MOs currently defined at this level.

8. Coding examples of CMIP / ROSE / PER to be developed for a typical CMIP exchange, for Guidance Material.

9. Some MOs for Security are specified in WG3/WP 12-25 “ATN Upper Layers Security” by G. Mittaux-Biron. These need to be incorporated into SV6 once stable.

10. Rationale for MOs and SM actions for Fault, Performance and Accounting management functions is given in the “hot trio” documents. Should this material be included here?