ATNP/WG3/WP 16-14

ATNP/WG1/JSG-SM/11-11

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 Systems Management

ATN Systems Management

Sub-Volume 6 of ATN Technical Provisions

Editor: A. J. Kerr

SUMMARY

This is the current draft of ATN Systems Management provisions, for inclusion as Sub-Volume 6 of the Manual of Technical Provisions for the ATN, prepared by the ICAO Aeronautical Telecommunication Network Panel (ATNP).

This working draft is an update based on developments in the Systems 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 of ATNP Manual

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. All Convergent MIB layer MOs moved to Guidance. Input to ATNP WG and JSG/SM meetings, Honolulu, January 1999	All	December 1998
1.3	Post Honolulu. Restructuring to better reflect two CMIP profiles. Fig 6.1-1 from CONOPS.	All	March 1999

Preface

This working draft has been formatted as Sub-Volume 6 of the detailed ATN technical provisions. For this reason, section numbering starts at 6.0.

This draft represents work in progress within the ICAO ATNP Working Groups and should not be taken as a stable set of requirements. 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.

This draft is based on the following assumptions:

a) that Systems 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 SARPs are required to ensure interworking between management domains. Within domains, systems management is a local issue.

c) that systems 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 Systems 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 is structured such that the draft technical provisions are presented in the style of ICAO SARPs

Cross-references:

[1] Draft ATNP Sub-Volume 1 and Core SARPs amendment

[2] Draft CONOPS

[3] Draft ACI/ProATN Convergent MIB

Table of Contents

6.0 ATN SYSTEMS MANAGEMENT PROVISIONS

6.0 ATN SYSTEMS MANAGEMENT PROVISIONS

6.1. INTRODUCTION

Note.— 6.1 contains introductory material and an overview of the Sub-Volume structure. There are no requirements or recommendations (shalls or shoulds) in this section.

6.1.1 Scope and Objectives

6.1.1.1 The minimum requirements for ATN systems management are specified in this Sub-Volume.

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

6.1.1.3 ATN systems management activities may be performed:

a) internally by the ATN systems themselves (e.g. use of Echo within IDRP, delay monitoring within applications). Such activities are specified in the relevant Sub-Volume for the ATN element in question and are outside the scope of this Sub-Volume.

b) by local management / operator activity. Such activities are outside the scope of the ATN Technical Provisions.

c) by specified systems management operations external to the ATN systems themselves. Such activities are specified in this Sub-Volume.

6.1.1.4 There are some fundamental systems management requirements which must be satisfied by all ATN systems if the ATN is to remain demonstrably within its defined operational parameters (see 6.3).

6.1.1.5 However, most of the technical provisions in this Sub-Volume are concerned with the standardisation of the formats and protocols necessary to support cross-domain systems management (CDSM), as illustrated in Figure 6.1-1. Thus they are mainly relevant to systems management systems at the boundary between management domains, referred to as “Boundary Management Systems”.

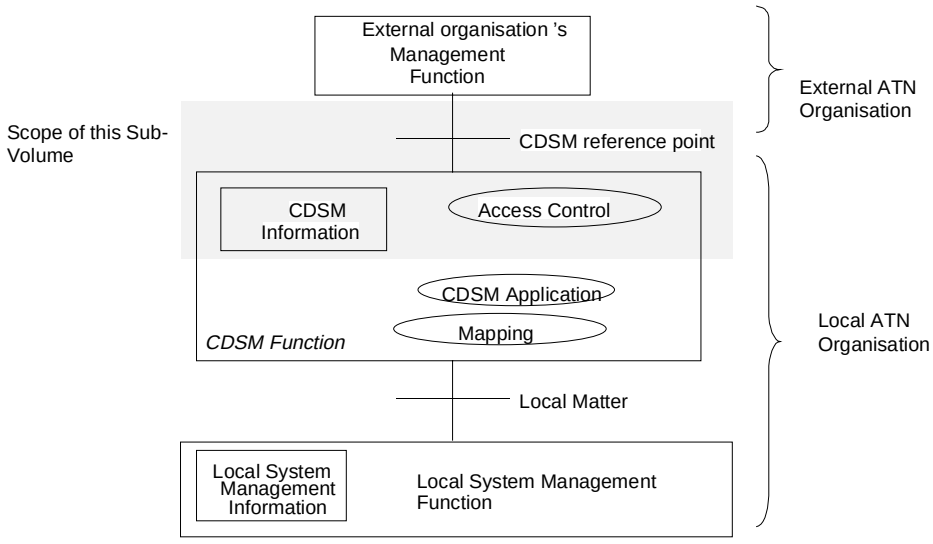

Figure 6.1-1. Functional Architecture of Cross-Domain Systems Management (CDSM)

6.1.1.6 Systems Management provisions broadly apply to two distinct areas: the definition of management information, and mechanisms for the interchange of such information.

6.1.1.7 Within a management domain, the detailed specification of systems management information is a local matter. Where such information is intended to cross domain boundaries, its format and encoding are subject to the technical provisions in this Sub-Volume.

6.1.1.8 Within a management domain, the mechanisms to convey systems management information between separate ATN systems are a local choice. Where there are exchanges of management information across domain boundaries, including over air-ground links, then the protocol requirements specified in this Sub-Volume apply.

6.1.1.9 Two distinct non-interoperable communication profiles are specified in this Sub-Volume:

a) There exist well-defined internationally standardised communication profiles for general systems management, and one such profile is specified in this Sub-Volume. 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.

6.1.2 Structure of ATN Systems Management Specification

6.1.2.1 This specification is structured as follows:

a) Introduction (6.1) describes the purpose and structure of the ATN Systems Management provisions, and the background to the functionality defined herein.

b) Naming and Addressing Provisions (6.2) specifies the requirements for navigating the Management Information Base and identifying particular attributes within individual Managed Object (MO) instances, or groups of MOs.

c) ATN Systems Management General Requirements (6.3) specifies requirements to be satisfied by all ATN systems.

d) ATN Systems Management Communication (6.4) specifies provisions for data communications subsystems in boundary management systems to support ATN systems management exchanges between management domains. The scope includes secure systems management application exchanges and access control to systems management resources.

e) Management Information (6.5) specifies common provisions for systems management information which is made available between management domains by ATN entities.

Note.— Managed Object (MO) specifications related to the intra-domain management of ATN resources are outside the scope of the technical provisions defined here. Guidance on a suitable Management Information Base (MIB) structure and composition for local management within a domain is given in the Guidance Material associated with these technical provisions.

6.1.3 Systems Management Model

6.1.3.1 The ATN Systems Management model is based on the OSI model described in ISO/IEC 10040, Systems Management Overview. In this model, a system is made up of at least the following components:

a) The Managed Resources, which can include network devices such as ATN routers, as well as other equipment and applications (software) which requires management.

b) A set of Managed Objects (MO). MOs are abstractions of the actual managed resources. These software abstractions provide the management interface to the real resources being managed. For

example, a set of MOs can be defined for the management of ATN routers. Each ATN router MO represents specific data associated with the router “managed resource”.

c) A management database in the form of a Management Information Base (MIB). The MIB is composed of the MOs, organised in an efficient manner to allow ease of retrieval of the data contained in each object.

d) A management Agent. The Agent is an application which accesses management data from the managed device and converts this raw data into a MIB-compatible format. Agents respond to queries (from managers) regarding management data. Agents may also notify managers when significant events take place.

e) A Manager application, which is responsible for receiving and responding to event notifications, initiating queries to accomplish the retrieval of management data, and providing an interface (usually a graphical interface) to the personnel in the operations control center.

6.1.3.2 To facilitate management communication between disparate managed systems, the Common Management Information Service (CMIS) and associated Common Management Information Protocol (CMIP) defined in ISO/IEC 9595 and ISO/IEC 9596, respectively are adopted for cross-boundary ATN management interchanges.

6.1.4 Ground-ground ATN Management Communications

6.1.4.1 Within the boundaries of an ATN portion managed by a single State or Organisation, there are no constraints on systems management mechanisms.

6.1.4.2 For management communications to be possible between separately managed domains of the global ATN, all ATN domains are required to support CMIP at the domain boundary.

6.1.4.3 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.

6.1.5 Air-ground ATN Management Communications

6.1.5.1 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.

6.1.5.2 The ATN air-ground applications in Sub-Volume 2 are specified to make use of the ULCS Dialogue Service, which is defined in [ULCS] 4.2. The Dialogue Service hides the ACSE and Presentation services from the application ASEs, and is provided by the control function (CF). The "Lower CF," which supports the Dialogue Service, is fully specified in the ULCS provisions.

6.1.5.3 The architecture, as applied to ATN air-ground management communication, is illustrated in Figure 6.1-2.

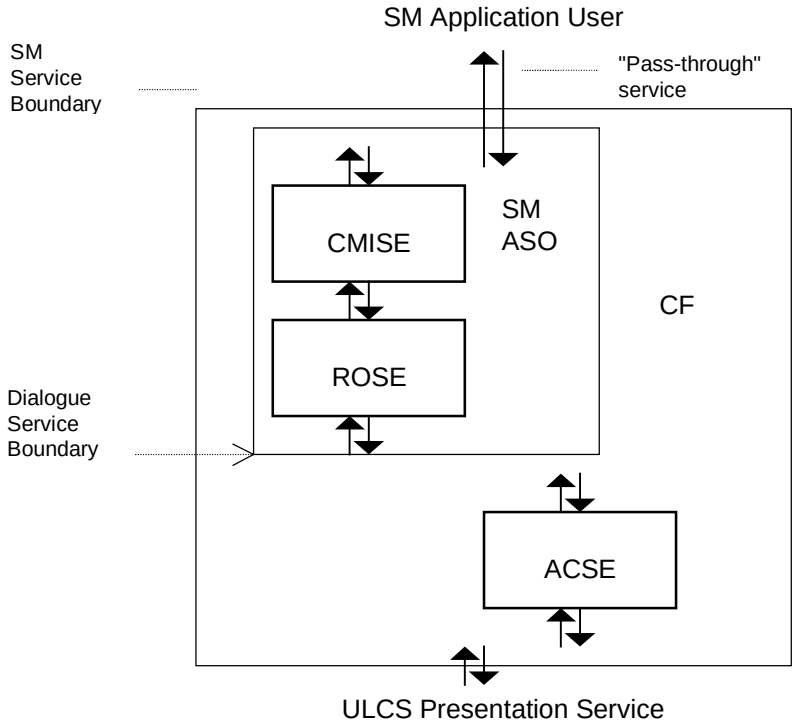

Figure 6.1-2. Use of the Dialogue Service

6.1.5.4 The CF provides a "pass-through" service to the SM Application User, allowing the SM Application User to invoke services offered by the Common Management Information Service Element (CMISE) and also to establish and release associations.

6.1.5.5 For modelling purposes, a "conceptual SM ASO" envelopes CMISE and the Remote Operations Service Element (ROSE) and invokes association establishment and termination services on behalf of the Application User. Thus, the Dialogue service is used to establish, release and abort the application-association with the peer Systems Management Application Entity (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.

6.1.5.6 The definition of the "conceptual SM ASO" is required only for modelling purposes. It avoids any need to modify the existing ULCS Provisions, which assume a one-to-one service mapping between the application ASE and the AE. The SM-User is provided with a service consisting of all the CMIS service primitives, plus a pass-through to the D-START, D-END and D-ABORT services. There is no requirement to implement any physical entity corresponding to the "conceptual SM ASO."

Note.—A problem of the ULCS architecture as used by the ATN air-ground application specifications is the induced complexity of the App-ASE protocol, because the states of the underlying dialogue (e.g. pending establishment, established, pending release, collision) are handled by the ASE protocol itself. For the SMAE this problem is avoided, as CMISE and ROSE assume the association handling is performed elsewhere, and invoke only a data transfer primitive.

6.1.5.7 The CMIS standard states that the user of the CMISE service uses ACSE services for the establishment and release of associations. The CF maps such ACSE service invocations by the CMISE user onto appropriate Dialogue Service requests. For example, when the CMISE user requests an association, the CF constructs the A-ASSOCIATE user information, adds the required D-START parameters, and invokes the D-START service. Thus, from the point of view of CMISE / ROSE, an “implicit start” service is provided.

6.1.5.8 The actions of the "conceptual SM ASO" are implicitly specified in the provisions of 6.4.4, in particular the actions to handle the primitive exchanges:

a) between the SM-users and CMISE,
b) between the SM-users and the Dialogue Service Provider, and
c) between ROSE and Dialogue Service Provider.

6.1.5.9 In particular, the specification in 6.4.4 is responsible for re-mapping the Presentation service primitives (P-DATA request and indication) used by ROSE at its lower interface to the Dialogue service interface, and also for mapping ACSE service invocations by the CMISE user onto appropriate Dialogue Service requests.

6.1.6 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"). 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. 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.

6.2. NAMING AND ADDRESSING PROVISIONS

Note.— This section specifies Managed Object addressing and registration requirement and requirements for navigating the Management Information Base and identifying particular attributes within individual Managed Object (MO) instances, or groups of MOs. Presentation context identifiers are also assigned.

6.2.1 Assignment of Object Identifiers

6.2.1.1 The ATN MIB shall be identified by an Object Identifier of the form:

Editor's note.— To be defined.

6.3. ATN SYSTEMS MANAGEMENT GENERAL REQUIREMENTS

6.3.1 General Provisions

Editor's note.— General provisions which affect all ATN systems, not just boundary management systems, are specified here. Since the ATN is dependent upon systems management to monitor and maintain the provided quality of service, there is a minimum set of SM requirements which applies to each type of ATN system (ES, BIS, IS, …).

6.3.2 General Requirements for Fault Management

Editor's note.— The following general requirements are the result of discussions on Fault Management in the ATN. The Notifications listed here will be more formally specified as part of the MIB definition, but it seems useful to extract out the basic functions required.

Editor's note.— More requirements are listed in the Working Paper "Fault Management Requirements Analysis" and could be inserted here after review by the ATNP SM subgroup.

6.3.2.1 An ATN system shall have the ability to emit a systems management notification when an ECHO Request (ERQ) NPDU is delivered to that system.

6.3.2.2 An ATN system shall have the ability to emit a systems management notification when an ECHO Response (ERP) NPDU is delivered to that system.

6.3.3 General Requirements for Performance Management

Editor's note.— Requirements are listed in the Working Paper "Performance Management Requirements Analysis" and could be inserted here after review by the ATNP SM subgroup.

6.3.4 General Requirements for Accounting Management

Editor's note.— Requirements are listed in the Working Paper "ATN Accounting Management Requirements" and could be inserted here after review by the ATNP SM subgroup.

6.3.5 General Requirements for Configuration Management

6.3.6 General Requirements for Security Management

Editor's note.— The Security requirements come from WG3/SG3.

6.3.6.1 An ATN system shall have the ability to emit a systems management notification when the Security ASO detects an authentication or data integrity security failure.

6.4. ATN SYSTEMS MANAGEMENT COMMUNICATION

6.4.1 General Provisions

Note 1.— The general requirements for SM communication are specified by reference to internationally standardised profiles (ISPs) to the extent possible. A basic level of SM functionality is specified in profiles AOM211, AOM 221 and AOM 231. Each of these profiles includes by reference a subset of the Enhanced Management Communications profile AOM 12 that is required to support the specified services.

Note 2.— AOM 211 specifies a combination of standards, which collectively provide a set of "General Management Capabilities". It supports the capabilities to create and delete any MO instance, retrieve and modify any attribute, report any event and initiate any action. These capabilities further include a specific set of: Reporting Services (for object creation, object deletion, attribute value change, relationship change and alarms); and Attribute Modification and Retrieval Services (for a specific set of state and relationship attributes and attribute groups). A system implementing this profile can interwork with: a system implementing the same profile in a complementary role, or a system implementing profiles AOM 212 and/or AOM 213 in a complementary role in the mode of operation specified by those profiles.

Note 3.— AOM 221 specifies a combination of standards, which collectively provide "General Event Report Management". It provides a means for selecting which notifications (generated by MOs) are sent by a managed system, and where they are sent to. This process of selection is referred to as "discrimination", and the criteria for selection are specified in the Event Forwarding Discriminator (EFD) support MO. The profile also provides a means for initiating, terminating, suspending and resuming the sending of event reports as well as modification of the selection criteria. These capabilities are achieved by a set of operations upon, and a set of notifications generated by, the EFD MO. This profile also specifies use of a combination of standards that collectively provide the subset of CMIS required for General Event Management. It does not include any specification of the notifications that are discriminated upon, nor the MOs generating them. A system implementing this profile can interwork with a system implementing the same profile in a complementary role. A system implementing the AOM 12 profile will be compatible with the communications aspects of this profile.

Note 4.— AOM 231 specifies a combination of standards, which collectively provide "General Log Control". This provides a means for selecting which notifications (generated by MOs) or incoming event reports are logged within a managed system, and the criteria for selection are specified in the Log support MO. The profile also provides a means for initiating, terminating, suspending and resuming the logging process as well as modification of the logging selection criteria and retrieving information from the logs. These capabilities are achieved by a set of operations upon, and a set of notifications generated by, the Log MO. This profile also specifies use of a combination of standards that collectively provide the subset of CMIS required for General Log Control. A system implementing this profile in the Agent role must support a mechanism to ensure that the notifications emitted by the log can be sent to a system implementing the same profile in a complementary role. A system implementing the AOM 12 profile will be compatible with the communications aspects of this profile.

6.4.1.1 Manager implementations shall conform to all the mandatory requirements for the manager role of profiles AOM211, AOM221 and AOM 231 as specified by ISO/IEC ISP 12060-1, 12060-4 and 12060-5 respectively, except as explicitly stated otherwise in the following provisions.

6.4.1.2 Agent implementations shall conform to all the mandatory requirements for the agent role of profiles AOM211 and AOM221 as specified by ISO/IEC ISP 12060-1 and 12060-4 respectively, except as explicitly stated otherwise in the following provisions.

6.4.1.3 Managed systems with sufficient resources to support a log shall conform to all the mandatory requirements for the agent role of profile AOM231 as specified by ISO/IEC ISP 12060-6, except as explicitly stated otherwise in the following provisions.

6.4.1.4 Implementations acting in the agent role shall provide the event time parameter in all CMIP M-EVENT-REPORT PDUs sent.

6.4.1.5 Implementations acting in the agent role shall be capable of requesting confirmation of all CMIP M-EVENT-REPORT PDUs sent.

6.4.1.6 The CMIP implementation shall be capable of being configured to establish an association for the purposes of ATN systems management.

Note.— The above provision is necessary because the standards do not mandate the responsibility of establishing communication to either the manager role system or the agent role system but leaves the particular style of management to be determined by the implementor or user. It is therefore necessary to ensure that all implementations are capable of establishing communications.

6.4.1.7 Peer entity authentication at time of association establishment

6.4.1.7.1 Implementations shall conform to all the requirements for the peer entity authentication option in agent role or manager role (as appropriate) of profile AOM 211 as specified by ISO/IEC ISP 11183-1 as referenced from ISO/IEC ISP 12060-1.

6.4.1.8 Systems Management functional unit negotiation

6.4.1.8.1 Implementations shall conform to all the requirements for Systems Management Functional Unit negotiation of profile AOM 211 as specified by ISO/IEC ISP 12060-1.

6.4.2 Inter-domain Communication between Manager Applications

Editor's note.— Discussions to date suggest that there are no special profile requirements for Manager to Manager communications. The CMIP profiles defined in 6.4 will fulfil all requirements, with one of the managers taking a "supra-manager" role and the other taking the Agent role for a given instance of communication.

Note.— The information exchanged between Managers is likely to be limited to cross-domain statistical or aggregate information e.g. for accounting purposes. Work is ongoing to define MOs to support this level of communication, in the context of a Concept of Operations for ATN Systems Management.

6.4.2.1 Manager-to-Manager communication shall be achieved by one of the Managers adopting the Agent role for a particular interchange.

6.4.2.2 Thus Manager implementations shall support both Manager and Agent roles.

6.4.3 Ground-Ground Management Communications Profile

6.4.3.1 Where it is required to perform ATN systems management communication using a "full" CMIP protocol stack (i.e. BER-encoded CMIP and ACSE PDUs transferred using the full Session and Presentation protocols), then the communication profile shall be as specified for AOM 12 in ISO/IEC ISP 11183-2, except as specified in 6.4.5.

6.4.4 Air-Ground Management Communications Profile

6.4.4.1 Where it is required to perform ATN systems management communication using an "efficient" CMIP protocol stack (i.e. PER-encoded CMIP and ACSE PDUs transferred using the short-connect, null-encoding Session and Presentation protocol options), then the communication profile shall be as specified in this subsection.

Note 1.— This section specifies requirements for an efficient CMIP profile for general ATN systems management (Manager to Agent) communications. It is not applicable to "full stack" applications such as ATSMHS, where a conventional full stack CMIP profile is more appropriate.

Note 2.— For efficient use of air-ground data links, and to avoid multiple protocol stacks in ATN systems, this CMIP profile is based on the ULCS and ICS Provisions. The profile specified here references the international

standardised profile (ISP) AOM 12, modified to take account of the null-encoding session and presentation layer protocols, and ACSE APDUs encoded for transfer using the Packed Encoding Rules of ASN.1.

6.4.4.2 The complete communication requirements between Manager and Agent for ATN systems management over the air-ground link shall be as specified here, taken together with the profile defined for the ULCS in 4 and the connection-mode Transport service defined for the ICS in 5.

6.4.4.3 The complementary communications interactions between CMISE-service-users within two end Management Information systems shall comply with the provisions specified here, with scope as shown in Figure 6.4-1.

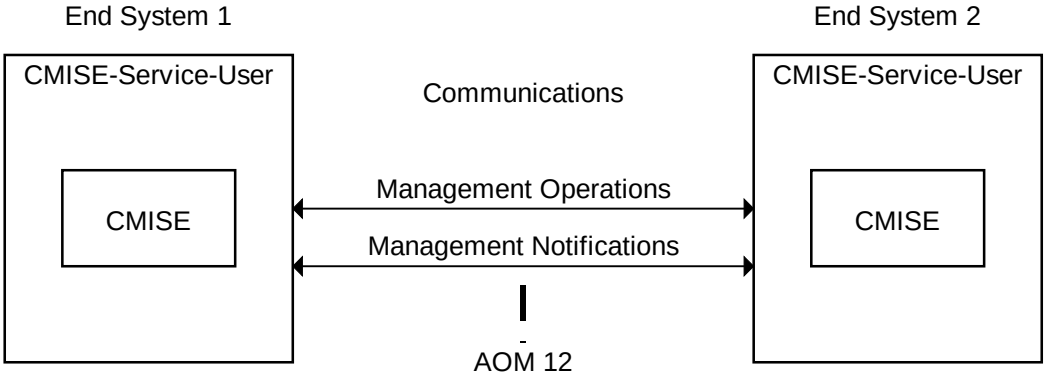

Figure 6.4-1. Scope of the SM Communications Profile

6.4.4.4 The supporting protocols shall be as specified in the international standards indicated in Table 6.4-1, subject to the constraints and options specified in this profile.

Table 6.4-1. Profile supporting stack

Application Layer	ISO 9595, 9596-1 (CMIS, CMIP v2) ISO 9072-1, 9072-2 (ROSE) ISO 8649, 8650-1 Amd.1 (ACSE ed.2) ULCS (CF, encoding)
Presentation Layer	ISO 8822, 8823-1 Amd.1 (Service, "Fast Byte" protocol) ISO 8824, 8825-2 (ASN.1, PER)
Session Layer	ISO 8826, 8327-1 Amd.1 (Service, "Fast Byte" protocol)

6.4.4.5 The profile requirements shall be as specified for profile AOM 12 in ISO/IEC ISP 11183-2, with modifications as specified in Table 6.4-2.

Table 6.4-2 - Modifications to ISP 11183-2

ISP 11183-2 clause	**Modification for ATN Profile**
1.5, Table 1	replace the table “Profile supporting stack” with Table 6.4-1 in this document
5 (Conformance to AOM 12)	replace "and also in ISO/IEC ISP 11183-1" (which refers to ACSE, Presentation and Session layer requirements) with "and also in the ULCS profile"
5.1	delete "ISO/IEC ISP 11183-1 and".
5.3	delete Note 2, which refers to ISP 11183-1.
5.3	delete final paragraph.

ISP 11183-2 clause	**Modification for ATN Profile**
5.4	replace "the application context of conforming implementations shall support the mapping of ROSE APDUs only onto the P-DATA Presentation service" with "the application context of conforming implementations shall support the mapping of ROSE APDUs only onto the D-DATA Dialogue service".
A.1	This clause allows non-conformant implementations to list the non-supported mandatory capabilities. For the SM provisions specified here, non-compliance is not permitted. Therefore the following provision is required: "All mandatory capabilities of ISO/IEC ISP 11183-2 as modified here shall be implemented."
A.2.1	replace "association" with "dialogue" throughout this clause, as the CMISE services are mapped to the ULCS Dialogue service, and not directly to ACSE.
A.2.3, Table A.3	replace "(in AARQapdu)" with "(in D-START Request and Indication User-Data)".
A.2.3, Table A.4	replace "(in AAREapdu)" with "(in D-START Response and Confirmation User-Data)".
A.2.3, Table A.3 and A.4	redefine profile support for userInfo parameter in CMIPUserInfo as "out of scope".
Clause A.2.4, Table A.5	profile support for userInfo parameter in CMIPAbortInfo is changed to "out of scope".
Clause A.3.2, Table A.13a and A.13b, index A.13a.1, A.13a.2, A.13b.1, A.13b.2	replace "See ISP 11183-1, 8.3" with "(3)", and insert new note after table: (3) A sender shall not encode values of greater than 2**31-1 or less than -2**31. A receiver shall be able to decode at least values in the range -2**31 to 2**31-1.
Clause A.3.2, Table A.13a, index A.13a.10, A.13a.11, A.13a.12	profile support of the INTEGER form of actionType, attributeId and eventType is changed from "i" to "m".
Table A.123 and A.124	delete note referring to ISP 11183-1.

Note 1.— Access Control parameters are outside the scope of this profile.

Note 2.— The format of the information contained in the CMIP PDUs "userInfo" in CMIPUserInfo and CMIPAbortIInfo definitions is outside the scope of AOM 12.

6.4.4.6 Encoding Requirements

6.4.4.6.1 The abstract syntax of the management information conveyed in CMIP PDUs shall be as defined in the MIB specification using ASN.1.

6.4.4.6.2 The encoding of management information for interchange shall be realised using the basic, unaligned variant ASN.1 Packed Encoding Rules (PER).

6.4.4.6.3 Implementations shall support the transfer syntax derived from the encoding rules specified in ISO/IEC 8825-2 and named { joint-iso-itu-t asn1 (1) packed-encoding (3) basic (0) unaligned (1) } for the purpose of generating and interpreting CMIP PDUs as defined in ISO/IEC 9596-1 by the abstract syntax "CMIP-PCI".

Note.— The above requirement is equivalent to specifying that all CMISE and ROSE APDUs are encoded using the basic, unaligned variant ASN.1 Packed Encoding Rules. It replaces the requirement in clause 8.1 of ISO/IEC 9596-1 that "the implementation shall support the transfer syntax derived from the encoding rules specified in ISO/IEC 8825 and named { joint-iso-ccitt asn1(1) basic-encoding(1) } for the purpose of generating and interpreting CMIP PDUs as defined by the abstract syntax "CMIP-PCI".”

6.4.4.7 Mapping to Dialogue Service

6.4.4.7.1 ROSE service primitives shall map to the D-DATA request / indication primitives of the Dialogue Service defined in the ULCS Provisions.

Note.— The above requirement replaces the ISO 9072-2 mapping to P-DATA request / indication primitives.

6.4.4.7.2 When a CMISE-service-user requires to open an association for the exchange of CMISE / ROSE APDUs, the following sequence of events shall occur:

a) A connection is established using the D-START service (and not the A-ASSOCIATE service as specified in ISO/IEC 9596-1). The CMIPUserInfo maps to the D-START request User Data.
b) On receiving a D-START indication containing User Data, the peer CMIPM and CMISE-service-user analyse the CMIPUserInfo as specified in ISO/IEC 9596-1 A.2.2.
c) If the dialogue parameters are acceptable, the receiving CMISE-service-user and CMIPM construct the CMIPUserInfo required for the response and invoke a positive D-START response primitive, with the CMIPUserInfo as User-Data.
d) If the dialogue parameters are not acceptable, the receiving CMISE-service-user and/or CMIPM invoke a negative D-START response primitive, with the constructed CMIPUserInfo, if any, as User-Data.
e) If the initiating CMISE-service-user receives a negative D-START confirmation, no association has been established.
f) If the initiating CMISE-service-user receives a positive D-START confirmation, an association has been established and the peer CMISE-service-users can exchange management protocol data units.

6.4.4.7.3 When a CMISE-service-user requires the orderly termination of an association between peer application entities, the following sequence of events shall occur:

a) A D-END request primitive is invoked by the release initiator.
b) On receiving a D-END indication, the release responder invokes a positive D-END response, which will close the connection.
c) On receiving a positive D-END confirmation, the association ceases to exist.

6.4.4.7.4 When a CMISE-service-user requires the abrupt termination of the association between peer application entities, the following sequence of events shall occur:

a) A D-ABORT request primitive is invoked by the release initiator, with the Originator parameter set to “User” and no User Data parameter.
b) On receiving a D-ABORT indication, the Abort indication with Originator parameter is passed to the CMISE-User.
c) The association ceases to exist.

6.4.4.7.5 When the association between peer application entities is terminated by the loss of the underlying communications connection, the following sequence of events shall occur:

a) On receiving a D-P-ABORT indication, the Abort indication is passed to the CMISE-User.
b) The association ceases to exist.

6.4.4.8 Mapping to Dialogue Service Parameters

6.4.4.8.1 The D-START *Routing Class* QoS parameter shall be set as specified in Table 6.4-3.

Table 6.4-3

Abstract Class of Communication	Routing Class Value (Hex)
ATN Systems Management Communications	60

6.4.4.8.2 The D-START *Priority* QoS parameter shall be set as specified in Table 6.4-4.

Table 6.4-4

Abstract Priority Value	QoS Priority Value (Decimal)
Network / Systems Management	14

Editor's Note. — For further investigation - 14 is the highest priority available. Is this always appropriate, given that much of the management traffic will be non-urgent?

6.4.5 Common A-G and G-G Profile Requirements

6.4.5.1 Mapping to the ATN Transport Service

Note 3.— The protocol profile includes Transport and lower layers, and this is required to be ICS compatible. ATN-specific transport layer parameters are specified (traffic type, communications class, transport priority and integrity requirements).

6.4.5.2 The ATN systems management communication profiles specified above shall make use of the Connection Mode Transport Service as specified in 5.5.

6.4.5.3 The called and calling Transport Service Access Point (TSAP) address shall be provided to the TS-Provider on a per Transport Connection basis, using the called and calling Presentation Service Access Point (PSAP) addresses as provided to ACSE in the A-ASSOCIATE request, with null presentation and session selectors.

6.4.5.4 The TS-user shall indicate in all T-CONNECT requests that the transport expedited flow is not required.

6.4.5.5 Information on the use or non-use of the transport checksum shall be conveyed between the TS-User and TS-Provider via the "residual error rate" component of the T-CONNECT quality of service parameter.

Note 1. —5.5.1.2 requires that the TS-user specifies the required residual error rate to determine whether or not the transport checksum is required. In the ATN, the Quality of Service provided to applications is maintained using capacity planning techniques that are outside of the scope of this specification. Network administrators are responsible for designing and implementing a network that will meet the QOS requirements of the applications that use it.

Note 2.— If the TS-User requests the use of transport checksum the peer can only accept the use of checksum for this Transport Connection. If the TS-User proposes non-use of checksum the peer can either accept the non-use of checksum or force the use of checksum for this Transport Connection.

6.4.5.6 The use or non-use of the transport checksum shall be negotiated by the TS-Provider on a per Transport Connection basis, based on TS-User requests in the T-CONNECT request and response primitives, as follows:

a) If the required residual error rate in the T-CONNECT request has the abstract value "low", then the TS-provider uses best endeavours to obtain the lowest available residual error rate, including the use of the transport checksum in all Transport Protocol Data Units (TPDUs). The residual error rate in the T-CONNECT indication is set to the abstract value "low", and the responder can only accept this value in the T-CONNECT response.

b) If the required residual error rate in the T-CONNECT request has the abstract value "high", then the TS-provider proposes non-use of the transport checksum. The residual error rate in the T-CONNECT indication is set to the abstract value "high", and the responder can either accept this value, or request "low" in the T-

CONNECT response. In the former case, transport checksum is not used, and in the latter case the TS-provider uses the transport checksum for all TPDUs.

6.4.5.7 The Application Service Priority shall be provided to the TS-Provider for each Transport Connection, via the TC priority quality of service parameter, using the value for "Network / Systems Management" as specified in Table 1.3-2.

Note. — Although transport priority and network priority are semantically independent of each other, it is required (in 5.5.1.2), that the TS-user specifies the Application Service Priority, which in turn is mapped into the resulting CLNP PDUs according to Table 1.3-2, which defines the fixed relationship between transport priority and the network priority.

6.4.5.8 The ATN Security Label shall be provided to the TS-Provider per Transport Connection by local means, using the encoding specified in 5.6.2.2.2.

6.4.5.9 The value corresponding to a traffic type of "ATN Systems Management Communications" as specified in Table 5.6-1 shall be conveyed as the Security Tag field of the security tag set for Traffic Type and Associated Routing Policies within the ATN Security Label.

Note 1. —5.2.7.3.1 states: "The mechanism by which the [transport] connection initiator provides the appropriate ATN Security Label is a local matter. For example, it may be identified by an extension to the transport service interface, be implicit in the choice of a given TSAP, or be identified using a Systems Management function."

Note 2. —5.5.1.2 states that the TS-User provides the complete ATN Security Label, although only security tag value is of relevance.

6.4.5.10 No Transport Service quality of service parameters other than those specified in the preceding subsections shall be specified when establishing a transport connection.

6.5. MANAGEMENT INFORMATION

6.5.1 General Provisions

Editor's note.— The details of the format and content of the management information to be exchanged are not yet known, and in any case are likely to evolve over time. The requirement is therefore for a flexible, general-purpose interchange mechanism, which will allow manager applications to identify the information content and take appropriate action depending upon procedures which will be defined as required.

Note.— There is likely to be a requirement for a bulk transfer protocol, for example to transfer log files to a management application, or to download configuration files to a managed system. Such a protocol should be highly reliable, allow interruptions by users, and run in the background with priority such as not to interfere with other ATN usage (except in the case of management operations critical to the correct functioning of the ATN). AMHS might provide the only solution required. Alternatively, there are numerous standard bulk transfer mechanisms, including well-proven file transfer protocols such as FTAM and FTP. A profile to map one of these protocols to the ATN transport service could be developed. There are no plans to do this at present, and this is considered out of scope for the current specification.

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.

Note.— ATN Management Information is defined by specifying:

a) the managed object class definition of ATN MOs following the MO template;

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

6.5.1.1 All managed objects defined for use in ATN systems management, whether standardised or not, shall be defined in accordance with ISO/IEC 10165-1 (the Management Information Model), use the tools specified in ISO/IEC 10165-4 (Guidelines for the Definition of Managed Objects), and include Implementation Conformance Statements as required by ISO/IEC 10165-6 (Requirements and Guidelines for ICS Proformas related to OSI Management).

6.5.2 Systems Management Profiles For Management Functions

Note 1.— This section contains provisions for the Systems Management Application functionality in ATN systems (standard ISO 10164 or other) required to support Performance assessment, Accounting and Fault detection (with Configuration and Security support as needed) in ATN systems for Manager to Manager and Manager to Agent.

Editor's note.— International standardised profiles (ISPs) exist for OSI systems management functions. The AOM 2xx profiles should be analysed in the context of requirements (currently BIS/ES/Subnet). It is necessary to assess the suitability of these profiles to satisfy identified functional requirements for ATN systems management, and to select those profiles necessary to support such requirements.

Editor's note.— It is also required to develop Provisions for secure Systems Management application exchanges and access control to Systems Management resources (e.g. applicability of Access control 10164-9 Managed Objects for access control).

6.5.3 Global Containment Tree for One System

6.5.3.1 The upper part of the global containment tree (naming hierarchy) for one system shall be as illustrated in Figure 6.5-1.

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

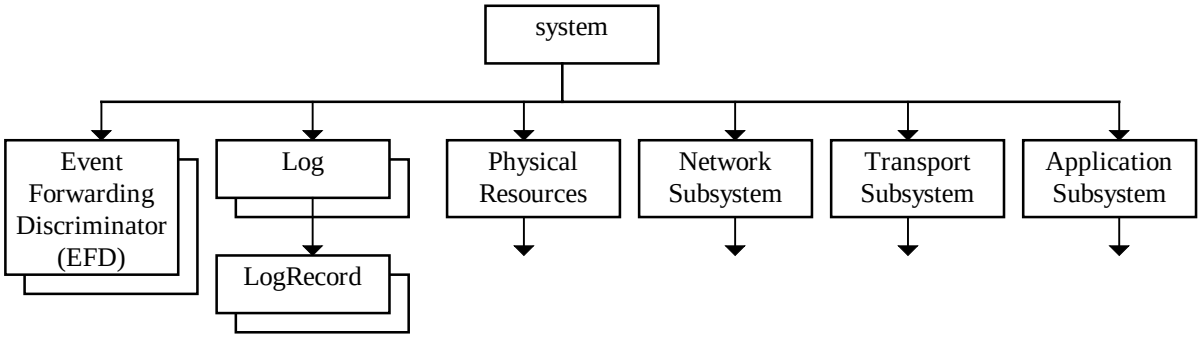

Figure 6.5-1. Global containment tree for one system

6.5.4 "System" MO Classes

Note.— 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.

6.5.4.1 System MO

6.5.4.1.1 MO Class Support

Index	**Property**	**Description**	**ISO Status**	**ATN Status**
1.	Managed Object Class	system **System** Class is ISO/IEC 10165-2 **system** class. There is only one such instance of this outmost external container of all MOs.	M	M
2.	Naming attribute	systemId	M	M
3.	Superior in Naming Tree	<none>		

6.5.4.1.2 Attributes

Index	**Attribute Name** **(Description)** **Syntax**	**Operations**	**ISO Status**	**ATN Status**
1.	administrativeState Indicates the permission to use the system, imposed through the management services. Can take following values: LOCKED, UNLOCKED.	GET, REPDEF	O	O
2.	operationalState Indicates whether the system is physically installed and working, if applicable.Can take following values: DISABLED, ENABLED.	GET	M	M
3.	supportedFeatures Identifies features within the system that are capable of being managed.	GET	O	O
4.	systemId Naming attribute. (GraphicString | INTEGER | NULL)	GET	M	M
5.	systemTitle Used by the Manager to uniquely identify the system (Object IDentifier).	GET	M	M
6.	usageState Indicates whether the system is actively in use, and if so, whether or not it has spare capacity for additional users. Can take one of the following values : IDLE, ACTIVE, BUSY.	GET	M	M

6.5.4.1.3 Actions

None.

6.5.4.1.4 Notifications

Index	Notification Name (Description) Syntax	ISO Status	ATN Status
1.	stateChangeAlarm This notification is sent upon start/stop of system	O	O

6.5.4.2 EventForwardingDiscriminator MO

Note.— This MO is exactly as defined in the ISO standards. It is included in the ATN MIB by the invocation of the ISP for AOM 221.

6.5.4.3 Log MO

Note.— This MO is exactly as defined in the ISO standards. It is included in the ATN MIB by the invocation of the ISP for AOM 231.

6.5.4.4 LogRecord MO

Note.— This MO is exactly as defined in the ISO standards. It is included in the ATN MIB by the invocation of the ISP for AOM 231.

6.5.4.5 AttributeValueChangeRecord MO

Editor's note.— This MO has not yet been considered in the ongoing MIB convergence process, and so is likely to change. Detailed technical discussions are needed on whether to include MOs such as this in the standardised ATN MIB.

6.5.4.6 CommunicationsInformationRecord MO

Editor's note.— This MO has not yet been considered in the ongoing MIB convergence process, and so is likely to change. Detailed technical discussions are needed on whether to include MOs such as this in the standardised ATN MIB.

6.5.4.7 ObjectCreationRecord MO

Editor's note.— This MO has not yet been considered in the ongoing MIB convergence process, and so is likely to change. Detailed technical discussions are needed on whether to include MOs such as this in the standardised ATN MIB.

6.5.4.8 ObjectDeletionRecord MO

Editor's note.— This MO has not yet been considered in the ongoing MIB convergence process, and so is likely to change. Detailed technical discussions are needed on whether to include MOs such as this in the standardised ATN MIB.

6.5.4.9 StateChangeRecord MO

Editor's note.— This MO has not yet been considered in the ongoing MIB convergence process, and so is likely to change. Detailed technical discussions are needed on whether to include MOs such as this in the standardised ATN MIB.

6.6. Issues / Work In Progress

1. To what extent should MOs be standardised? It may be desirable to adopt a common framework in order to reduce procurement and deployment costs, but should States be mandated to build the specified GDMO MIB? The only MOs essential to standardise are those used in management exchanges between administrative domains.

2. Statistical / aggregate MOs for Manager - Manager communication need to be defined (the so-called "Summary MIB", Inter-Domain MIB or Cross-Domain MIB (X-MIB)) Dependency on the immature CONOPS work. WG1/SG3/WP6-4 "Operational Concepts on Systems Management for the European ATN" by S.Tamalet makes a start on this topic at a high level.

3. 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.

4. There may be significant bandwidth savings in the air-ground "FastMIP" profile 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. Coding examples of CMIP / ROSE / PER to be developed for a typical CMIP exchange, for Guidance Material.

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

6. What does the distinguished name of "system" look like?

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

8. 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.

9. For further investigation - 14 is the highest priority available. Is this always appropriate, given that much of the management traffic will be non-urgent?

10. Should the AOM 12 requirements be reproduced here, especially as Table 6.4-2 contains detailed changes to the AOM 12 document. The general Doc 9705 approach has been to include ISPs by reference only as far as possible.