ATNP/WG3/WP 15-11

ATNP/WG1/JSG-SM/_____

Version DRAFT 1.2 (MS Word 6/7)
17 December 1998

AERONAUTICAL TELECOMMUNICATION NETWORK PANEL

WORKING GROUP 1 (System Planning and Concepts)

Joint Sub Group on System Management

ATN Systems Management

Sub-Volume 6 of ATNP Manual

Editor: A. J. Kerr

SUMMARY

This is the current draft of the ATN Systems Management technical provisions for inclusion as 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 of ATNP Manual

Version : DRAFT 1.2 (MS Word 6/7)

Date: 17 December 1998

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

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 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 SARPs 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 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

6.1. INTRODUCTION 4

6.1.1 Scope and Objectives 4
6.1.2 Structure of ATN Systems Management Specification 4
6.1.3 Symbols, abbreviations and terms 4
6.1.4 Systems Management Functionality 5
6.1.5 The “Lightweight CMIP” Application Model 5

6.2. NAMING AND ADDRESSING PROVISIONS 7

6.2.1 Assignment of Object Identifiers 7

6.3. ATN SYSTEMS MANAGEMENT COMMUNICATION PROFILES 8

6.3.1 General Provisions 8
6.3.2 Inter-domain Management Communication 8
6.3.3 Lightweight CMIP Profile 9
6.3.4 Full CMIP Profile 12

6.4. ATN SYSTEM MANAGEMENT FUNCTIONS 14

6.4.1 General Provisions 14

6.5. MANAGEMENT INFORMATION 15

6.5.1 General Provisions 15
6.5.2 Systems Management Profiles For Management Functions 15
6.5.3 Global Containment Tree for One System 15
6.5.4 “System” MO Classes 16

6.6. Issues / Work In Progress 29

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.

6.1.2 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 Communication Profiles (6.3) specifies provisions for data communications subsystems to support general ATN systems management activities. The scope includes secure systems management application exchanges and access control to systems management resources.

d) Management Information (6.4) specifies common provisions for systems management information which is made available by ATN entities.

Note.— 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 MIB structure and composition for local management within a domain is given in the Guidance Material associated with these technical provisions.

6.1.3 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.

6.1.4 Systems Management Functionality

6.1.4.1 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.

6.1.5 The "Lightweight CMIP" Application Model

6.1.5.1 Most of the existing ATN applications were 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.

6.1.5.2 The architecture, as applied to ATN systems management, is illustrated in Figure 6.1-1.

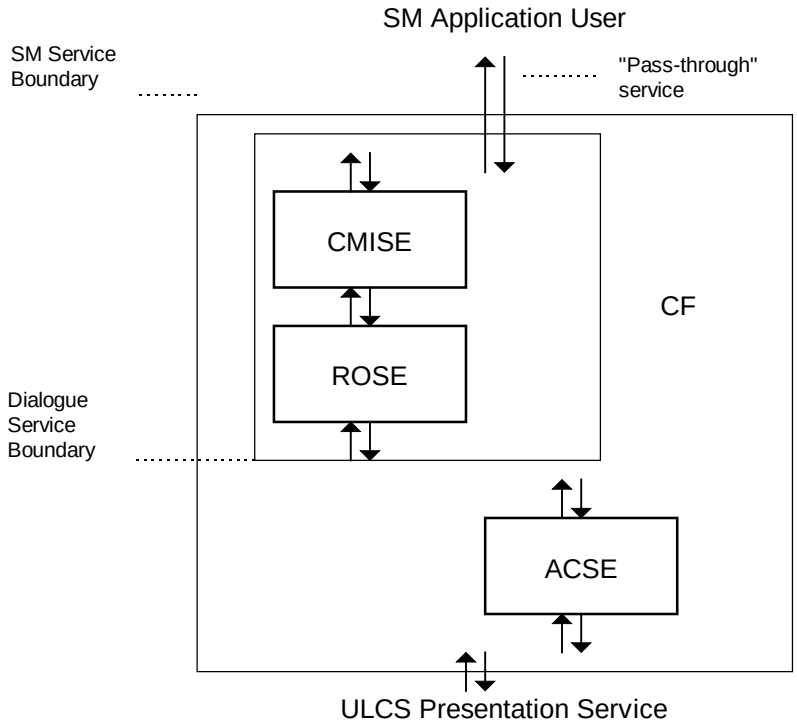

Figure 6.1-1. Use of the CNS/ATM-1 Dialogue Service

6.1.5.3 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.

6.1.5.4 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 (SAME) 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.

6.1.5.5 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.

6.1.5.6 The actions of the "conceptual SM ASO" are specified in this Sub-Volume, 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.

6.1.5.7 In particular, the specification 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.

6.1.5.8 The provisions in section 6.3.1 equate to the specification of the "conceptual SM ASO".

6.1.5.9 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.— The main problem of the ULCS architecture when used for the ATN air-ground application specifications 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 is therefore not encountered for the specification of the SM application.

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 COMMUNICATION PROFILES

6.3.1 General Provisions

6.3.1.1 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.

6.3.1.2 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.

6.3.1.3 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.

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

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

6.3.1.6 The CMIP implementation shall be capable of being configured to establish an association for the purposes of ATN system 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.

6.3.1.7 Peer entity authentication at time of association establishment

6.3.1.7.1 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.

6.3.1.8 Systems management functional unit negotiation

6.3.1.8.1 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.

6.3.2 Inter-domain Management Communication

Editor's note.— Discussions to date suggest that there are no special profile requirements for Manager to Manager communications. The lightweight profile defined in 6.3 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 System Management.

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

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

6.3.3 Lightweight CMIP Profile

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.

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).

6.3.3.1 The complete communication requirements between Manager and Agent for ATN systems management 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.

6.3.3.2 The complementary communications interactions between CMISE-service-users within two end Management Information systems, with scope as shown in Figure 6.3-1, shall comply with the provisions specified here.

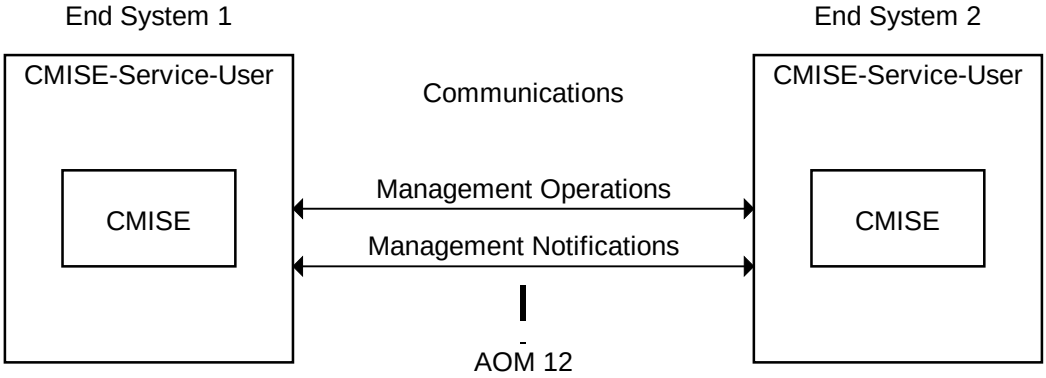

Figure 6.3-1. Scope of the SM Communications Profile

6.3.3.3 The supporting stack shall be as specified in the international standards indicated in Table 6.3-1, subject to the constraints and options specified in this profile.

Table 6.3-1. 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)

6.3.3.4 The communication profile for ATN system management shall be as specified in ISO/IEC ISP 11183-2, with modifications as specified in Table 6.3-2.

Table 6.3-2 - Modifications to ISP 11183-2

ISP 11183-2 clause	**Modification for ATN Profile**
1.5, Table 1	replace the table with Table 6.3-1 in this document
5 (Conformance to AOM 12)	replace "and also in ISO/IEC ISP 11183-1" with "and also in the ULCS profile"
5.1	delete "ISO/IEC ISP 11183-1 and".
5.3	delete Note 2.
5.3	delete final paragraph.
5.4	replace "shall support the mapping of ROSE APDUs only onto the P-DATA Presentation service" with "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.

6.3.3.5 Encoding Requirements

6.3.3.5.1 The abstract syntax of the management information conveyed in CMIP PDUs shall be as defined in the ATN MIB specification.

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

6.3.3.5.3 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".”

6.3.3.6 Mapping to Dialogue Service

6.3.3.6.1 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.

6.3.3.6.2 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.

6.3.3.6.3 When a CMISE-service-user requires the orderly termination of an association betwewen 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.

6.3.3.6.4 When a CMISE-service-user requires the abrupt termination of the association betwewen 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.

6.3.3.6.5 When the association betwewen 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.

6.3.3.7 Mapping to Dialogue Service Parameters

6.3.3.7.1 The D-START *Routing Class* QoS parameter shall be set as specified in Table 6.3-3.

Table 6.3-3

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

6.3.3.7.2 The D-START *Priority* QoS parameter shall be set as specified in Table 6.3-4.

Table 6.3-4

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

6.3.4 Full CMIP Profile

Note.— In addition to the "efficient" CMIP stack profile specified in the preceding section, there are requirements for a conventional "full stack" CMIP profile, to allow the use of existing products and management of full stack ATN applications, such as ATSMHS. ATSMHS make use of ISO standards and profiles. 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.

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

6.3.4.2 Mapping to the ATN Transport Service

6.3.4.3 The use of the connection-oriented transport service provided by the ATN Internet shall be as specified in Clause 6 of ISO/IEC 8327-1, except as stated in this section.

6.3.4.4 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.

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

6.3.4.6 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.

6.3.4.7 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.

6.3.4.8 The Application Service Priority shall be provided to the TS-Provider on a per Transport Connection basis, via the TC priority quality of service parameter, using the values for Transport Layer Priority 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.

6.3.4.9 The ATN Security Label shall be provided to the TS-Provider on a per Transport Connection basis.

6.3.4.10 The required ATN Security Label shall be conveyed by local means, using the encoding specified in 5.6.2.2.2.

6.3.4.11 The QOS parameter "Routing Class" shall take the value beconveyed 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."

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

6.4. ATN SYSTEM MANAGEMENT FUNCTIONS

6.4.1 General Provisions

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. The Security requirements come from WG3/SG.

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

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

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

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 System Management.

6.5.1.1 All managed objects defined for use in ATN system 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.

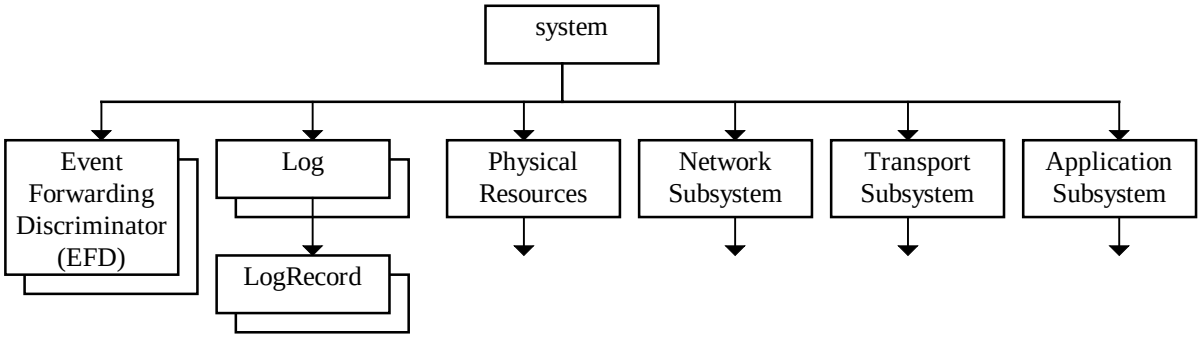

Figure 6.5-1. Global containment tree for one system

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 *<syntax ???>*	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	X
2.	operationalState Indicates whether the system is physically installed and working, if applicable.Can take following values: DISABLED, ENABLED.	GET	M	X
3.	supportedFeatures Identifies features within the system that are capable of being managed.	GET	O	X
4.	systemId Naming attribute.	GET	M	X
5.	systemTitle Used by the Manager to uniquely identify the system (Object IDentifier).	GET	M	X
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	X

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	X

6.5.4.2 EventForwardingDiscriminator MO

Note.— This MO is exactly as defined in the ISO standards

6.5.4.2.1 MO Class Support

Index	Property	Description	ISO Status	ATN Status
1.	Managed Object Class	EventForwardingDiscriminator This object class allows to filter the events generated , and to decide whether they should be sent by the Agent to the Manager. [CREATE/DELETE] operations supported on the MO. There are different instances for this MO.	O	M
2.	Naming attribute	discriminatorId	M	M
3.	Superior in Naming Tree	system	O	M

6.5.4.2.2 Attributes

Index	Attribute Name (Description) Syntax	Operations	ISO Status	ATN Status
1.	activeDestination An Application Entity Title (AET) which identifies the Application Entity (AE) to which events are currently forwarded by the discriminator.	GET	O	O
2.	administrativeState Indicates the permission to use the log, imposed through the management services. Can take following values: LOCKED, UNLOCKED.	GET SET	M	M
3.	availabilityStatus Can take the zero value or any of the following values: IN TEST, FAILED, POWER OFF, OFF LINE, OFF DUTY, DEPENDENCY, DEGRADED, NOT INSTALLED, LOG FULL.	GET	O	O
4.	backUpDestinationList An ordered list of AETs identifying AEs to be used as destinations if the destination specified in the destination attribute fails. This attribute is not used when the destination attribute has multiple values.	GET SET	O	O
5.	destination Identifies the destination(s) to which the discriminator forwards event reports. May be a single AET or multiple AETs.	GET SET	O	O

6.	discriminatorConstruct Specifies tests on the information that is sent to the manager. The discriminator construct may operate on any parameter of the information that is bound to be sent to the manager. Different profiles shall be built: • no information to be sent to Manager, except Alarms, • all information to be sent to Manager, • authorized events for Network LME plus Alarms, • authorized events for Transport LME plus Alarms, • authorized events for Application LME plus Alarms, • authorized events for System LME plus Alarms.	GET SET REPDEF	M	M
7.	discriminatorId Naming attribute.	GET	M	M
8.	intervalsOfDay Defines the list of time intervals for which the log will exhibit the logging-on condition. During excluded intervals, the log exhibits the logging-off condition. If not specified at creation time, its value defaults to a single interval encompassing the entire 24 hour period of a day.	GET SET REPDEF ADD REMOVE	O	O
9.	operationalState Operational state of the eventForwardingDiscriminator, telling whether EFD is able to operate. Can only take following value: DISABLED, ENABLED.	GET	M	M
10.	schedulerName Specifies the name of the external scheduler MO that is related to the logs.	GET	O	O
11.	startTime Defines date and time at which an unlocked and enabled log starts functioning. If not specified at creation time, its value defaults to the time of creation, thus causing the log to function immediately.	GET SET	O	O
12.	stopTime Defines the date and time at which the log stops functioning. If not specified at creation time, its value defaults to 'continuous operation', which is represented by a null value.	GET SET REPDEF	O	O
13.	weekMask This structured attribute defines a set of mask components, each specifying a 24-hour time-of-day clock, pertaining to the selected days of the week. Defaults to a set of scheduling criteria of 'ALWAYS ON' at creation time.	GET SET REPDEF ADD REMOVE	O	O

6.5.4.2.3 Actions

None.

6.5.4.2.4 Notifications

Index	**Notification Name** **(Description)** **Syntax**	**ISO Status**	**ATN Status**
1.	attributeValueChange Used to report change of value of one of the EFD attributes (except state attributes).	M	M
2.	objectCreation Used to report the EFD instance creation. Contains initial attribute values.	M	M
3.	objectDeletion Used to report the EFD instance deletion. Contains last known attribute values.	M	M
4.	stateChange Used to report the change in the value of one or more of the state attributes of the MO.	M	M

6.5.4.3 Log MO

Note.— This MO is exactly as defined in the ISO standards

6.5.4.3.1 MO Class Support

Index	**Property**	**Description**	**ISO Status**	**ATN Status**

1.	Managed Object Class	log This object class allows to filter events and to store events as log records. There are different instances for this MO. [CREATE/DELETE] operations supported on the MO.	O	M
2.	Naming attribute	logId		
3.	Superior in Naming Tree	system		

6.5.4.3.2 Attributes

Index	**Attribute Name** **(Description)** **Syntax**	**Operations**	**ISO Status**	**ATN Status**
1.	administrativeState Indicates the permission to use the log, imposed through the management services. Can take following values: LOCKED, UNLOCKED.	GET SET	M	M
2.	availabilityStatus Can take the zero value or any of following values: IN TEST, FAILED, POWER OFF, OFF LINE, OFF DUTY, DEPENDENCY, DEGRADED, NOT INSTALLED, LOG FULL.	GET	M	M
3.	capacityAlarmThreshold Specifies, as a percentage of maxLogSize, the point at which an event will be generated to indicate that a log full or log wrap condition is approaching. Support is mandatory for the halt behaviour is specified by the logFullAction attribute.	GET SET	O	O
4.	currentLogSize Current size of the log measured in octets.	GET	O	O
5.	discriminatorConstruct Specifies tests on the information that is to be logged, and thus decides whether events are suitable or not for storage. The discriminator construct may operate on any of the parameters of the information to be logged. A limited number of log profiles should be defined.	GET SET	M	M
6.	intervalsOfDay Defines the list of time intervals for which the log will exhibit the logging-on condition. During excluded intervals, the log exhibits the logging-off condition. If not specified at creation time, its value defaults to a single interval encompassing the entire 24 h period of a day.	GET SET REPDEF ADD REMOVE	O	O
7.	logFullAction Specifies the action to be taken when the maximum size of the log has been reached. Options are: wrap and halt.	GET SET	M	M
8.	logId Naming attribute.	GET	M	M
9.	maxLogSize Specifies the maximum size of the log measured in octets. A log may have an indetermined size. A maxLogSize of zero shall be used to specify that the log size has no predefined limit.	GET SET	O	O
10.	numberOfRecords Current number of records contained in the log.	GET	O	O
11.	operationalState Indicates whether the system is physically installed and working. Can take following values: DISABLED, ENABLED.	GET	M	M
12.	schedulerName Specifies the name of the external scheduler MO that is related to the logs.	GET	O	O
13.	startTime Defines date and time at which an unlocked and enabled log starts functioning. If not specified at creation time, its value defaults to the time of creation, thus causing the log to function immediately.	GET SET	O	O
14.	stopTime Defines the date and time at which the log stops functioning. If not specified at creation time, its value defaults to ‘continuous operation’, which is represented by a null value.	GET SETd	O	O

15.	weekMask This structured attribute defines a set of mask components, each specifying a 24-hour time-of-day clock, pertaining to the selected days of the week. Defaults to a set of scheduling criteria of 'ALWAYS ON' at creation time.	GET SET REPDEF ADD REMOVE	O	O

6.5.4.3.3 Actions

None.

6.5.4.3.4 Notifications

Index	**Notification Name** **(Description)** **Syntax**	**ISO Status**	**ATN Status**
1.	attributeValueChange Used to report change of value of non-state attributes.	M	M
2.	objectCreation Used to report the log instance creation. Contains initial attribute values.	M	M
3.	objectDeletion Used to report the log instance deletion. Contains last known attribute values.	M	M
4.	processingErrorAlarm Used to report a software or processing fault. Here it is used to report that the capacity alarm threshold has been reached or exceeded (see ISO 10164-6).	M	M
5.	stateChange Used to report the change in the value of one or more of the state attributes of the MO.	M	M

6.5.4.4 LogRecord MO

Note.— This MO is exactly as defined in the ISO standards

6.5.4.4.1 MO Class Support

Index	**Property**	**Description**	**ISO Status**	**ATN Status**
1.	Managed Object Class	logRecord This MO is a generic type for the logging of any type of event or alarm record; thus there are different instances for this MO.	O	M
2.	Naming attribute	logRecordId		
3.	Superior in Naming Tree	log		

6.5.4.5 AlarmRecord 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.

6.5.4.5.1 MO Class Support

Index	**Property**	**Description**	**ISO Status**	**ATN Status**

1.	Managed Object Class	alarmRecord This object class allows to log alarm notifications. [DELETE] supported on the MO. There are diferent instances for this MO (in accordance with 10164-4), such as: **communicationsAlarm** (many Mos are concerned), **processingErrorAlarm** (log is concerned), **qualityofServiceAlarm** (Operating System is concerned), **stateChangeAlarm** (System is concerned). There are different instances for this MO.		
2.	Naming attribute	logRecordId		
3.	Superior in Naming Tree	log		

6.5.4.5.2 Attributes

Index	**Attribute Name** **(Description)** **Syntax**	**Operations**	**ISO Status**	**ATN Status**
1.	additionalInformation When present, allows the inclusion of a set of additional information in the event report. It is a series of data structures, each of which contains three items: an identifier, a significance indicator, and the problem information. The information subparameter carries information about the event. This information can be parsed if the identifier is understood.	GET	O	O
2.	additionalText When present, allows a free form text description to be reported.	GET	O	O
3.	backedUpStatus When present, specifies whether the MO emitting the alarm has been backed-up, and services provided to the user have, therefore, not been disrupted. The use of this field in conjunction of the severity field forms an independent form to qualify the seriousness of the alarm and the ability of the system as a whole to continue to provide services. If TRUE, the MO emitting the alarm has been backed-up; if FALSE, it has not, which shall be a usual case.	GET	O	O
4.	backUpObject Present when the backedUpStatus attribute is present and has the value TRUE. Specifies the MO instance that is providing back-up services for the MO about which the notification pertains.	GET	O	O
5.	correlatedNotifications When present, contains the set of notification identifiers of all notifications to which this notification is considered to be correlated.	GET	O	O
6.	eventTime Event generation time (i.e. present in the event if available).	GET	O	O
7.	eventType Specifies the type of event being reported.	GET	M	M
8.	loggingTime The time at which the record was entered into the log.	GET	M	M
9.	logRecordId Naming attribute.	GET	M	M
10.	managedObjectClass The class of the MO in which the event occurred.	GET	M	M
11.	managedObjectInstance The instance (DN) of the MO in which the event occurred.	GET	M	M
12.	monitoredAttributes When present, defines one or more attributes of the MO and their corresponding values at the time of the alarm.	GET	O	O

13.	notificationIdentifier Contains a unique identifier for the notification, which may be present in the correlatedNotifications attribute of other notifications.	GET	O	O
14.	perceivedSeverity Defines six severity levels indicating how it is perceived that the capability of the MO has been affected: CLEARED, INDETERMINATE, CRITICAL, MAJOR, MINOR, WARNING .	GET	O	O
15.	probableCause Defines further qualification as to the probable cause of the alarm.	GET	O	O
16.	proposedRepairActions When present, used if the cause is known an the system being managed can suggest one or more solutions.	GET	O	O
17.	specificProblems When present, identifies further refinements to the probable cause of the alarm.	GET	O	O
18.	stateChangeDefinition When present, used to indicate a state transition associated with the alarm	GET	O	O
19.	thresholdInfo Shall be present when the alarm is a result of crossing a threshold. It includes the identifier of the triggered threshold, the threshold level, the observed value and the alarm time.	GET	O	O
20.	trendIndication When present, specifies the current severity trend of the MO. If present, it indicates that there is one or more outstanding alarms which have not been cleared, and belong to the same MO as the current alarm. Can take one of the following values: MORE SEVERE, NO CHANGE, LESS SEVERE.	GET	O	O

6.5.4.5.3 Actions

None.

6.5.4.5.4 Notifications

None.

6.5.4.6 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.

6.5.4.6.1 MO Class Support

Index	**Property**	**Description**	**ISO Status**	**ATN Status**
1.	Managed Object Class	AttributeValueChangeRecord This managed object class allows to log attributeValueChange notifications. [DELETE] operation supported on the MO. There are different instances for this MO.		
2.	Naming attribute	logRecordId		
3.	Superior in Naming Tree	log		

6.5.4.6.2 Attributes

Index	**Attribute Name** **(Description)** **Syntax**	**Operations**	**ISO Status**	**ATN Status**

1.	additionalInformation When present, allows the inclusion of a set of additional information in the event report. It is a series of data structures, each of which contains three items: an identifier, a significance indicator, and the problem information. The information subparameter carries information about the event. This information can be parsed if the identifier is understood.	GET	O	O
2.	additionalText When present, allows a free form text description to be reported.	GET	O	O
3.	attributeIdentifierList Identifies the set of attributes whose value change is being reported	GET	O	O
4.	attributeValueChange Definition Consists of a set of sequences of the three parameters: attribute identifier, old attribute value, new attribute value.	GET	M	M
5.	correlatedNotifications When present, contains the set of notification identifiers of all notifications to which this notification is considered to be correlated.	GET	O	O
6.	eventTime Event generation time (i.e. present in the event if available).	GET	O	O
7.	eventType Specifies the type of event being reported.	GET	M	M
8.	loggingTime The time at which the record was entered into the log.	GET	M	M
9.	logRecordId Naming attribute.	GET	M	M
10.	managedObjectClass The class of the MO in which the event occurred.	GET	M	M
11.	managedObjectInstance The instance (DN) of the MO in which the event occurred.	GET	M	M
12.	notificationIdentifier Contains a unique identifier for the notification, which may be present in the correlatedNotifications attribute of other notifications.	GET	O	O
13.	sourceIndicator When present, indicates the source of operation that led to the generation of this notification. Can take one of the following values: RESOURCE OPERATION, MANAGEMENT OPERATION, UNKNOWN.	GET	O	O

6.5.4.6.3 Actions

None.

6.5.4.6.4 Notifications

None.

6.5.4.7 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.

6.5.4.7.1 MO Class Support

Index	**Property**	**Description**	**ISO Status**	**ATN Status**
1.	Managed Object Class	CommunicationsInformationRecord This managed object class allows to log communicationsInformation notifications. [DELETE] operation supported on the MO. There are different instances for this MO.		
2.	Naming attribute	logRecordId		

3.	Superior in Naming Tree	log		

6.5.4.7.2 Attributes

Index	**Attribute Name** **(Description)** **Syntax**	**Operations**	**ISO Status**	**ATN Status**
1.	additionalInformation When present, allows the inclusion of a set of additional information in the event report. It is a series of data structures, each of which contains three items: an identifier, a significance indicator, and the problem information. The information subparameter carries information about the event. This information can be parsed if the identifier is understood.	GET	O	O
2.	additionalText When present, allows a free form text description to be reported.	GET	O	O
3.	correlatedNotifications When present, contains the set of notification identifiers of all notifications to which this notification is considered to be correlated.	GET	O	O
4.	eventTime Event generation time (i.e. present in the event if available).	GET	O	O
5.	eventType Specifies the type of event being reported.	GET	M	M
6.	informationData Generic structure of information carried by the communicationsInformation notification.	GET	O	O
7.	informationType The type of information held in the informationData attribute	GET	M	M
8.	loggingTime The time at which the record was entered into the log.	GET	M	M
9.	logRecordId Naming attribute.	GET	M	M
10.	managedObjectClass The class of the MO in which the event occurred.	GET	M	M
11.	managedObjectInstance The instance (DN) of the MO in which the event occurred.	GET	M	M
12.	notificationIdentifier Contains a unique identifier for the notification, which may be present in the correlatedNotifications attribute of other notifications.	GET	O	O

6.5.4.7.3 Actions

None.

6.5.4.7.4 Notifications

None.

6.5.4.8 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.

6.5.4.8.1 MO Class Support

Index	**Property**	**Description**	**ISO Status**	**ATN Status**

1.	Managed Object Class	ObjectCreationRecord This managed object class allows to log objectCreation notifications. [DELETE] operation supported on the MO. There are different instances for this MO.		
2.	Naming attribute	logRecordId		
3.	Superior in Naming Tree	log		

6.5.4.8.2 Attributes

Index	**Attribute Name** **(Description)** **Syntax**	**Operations**	**ISO Status**	**ATN Status**
1.	additionalInformation When present, allows the inclusion of a set of additional information in the event report. It is a series of data structures, each of which contains three items: an identifier, a significance indicator, and the problem information. The information subparameter carries information about the event. This information can be parsed if the identifier is understood.	GET	O	O
2.	additionalText When present, allows a free form text description to be reported.	GET	O	O
3.	attributeList When present, contains a list of attributes and their values at the time the MO was created.	GET	O	O
4.	correlatedNotifications When present, contains the set of notification identifiers of all notifications to which this notification is considered to be correlated.	GET	O	O
5.	eventTime Event generation time (i.e. present in the event if available).	GET	O	O
6.	eventType Specifies the type of event being reported.	GET	M	M
7.	loggingTime The time at which the record was entered into the log.	GET	M	M
8.	logRecordId Naming attribute.	GET	M	M
9.	managedObjectClass The class of the MO in which the event occurred.	GET	M	M
10.	managedObjectInstance The instance (DN) of the MO in which the event occurred.	GET	M	M
11.	notificationIdentifier Contains a unique identifier for the notification, which may be present in the correlatedNotifications attribute of other notifications.	GET	O	O
12.	sourceIndicator When present, indicates the source of the operation that led to the generation of this notification type. It can have one of the following values: RESOURCE OPERATION, MANAGEMENT OPERATION, UNKNOWN.	GET	O	O

6.5.4.8.3 Actions

None.

6.5.4.8.4 Notifications

None.

6.5.4.9 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.

6.5.4.9.1 MO Class Support

Index	**Property**	**Description**	**ISO Status**	**ATN Status**
1.	Managed Object Class	**6.5.4.9.1.1 ObjectDeletionRecord** This managed object class allows to log objectDeletion notifications. [DELETE] operation supported on the MO. There are different instances for this MO.		
2.	Naming attribute	logRecordId		
3.	Superior in Naming Tree	log		

6.5.4.9.2 Attributes

Index	**Attribute Name** **(Description)** **Syntax**	**Operations**	**ISO Status**	**ATN Status**
1.	additionalInformation When present, allows the inclusion of a set of additional information in the event report. It is a series of data structures, each of which contains three items: an identifier, a significance indicator, and the problem information. The information subparameter carries information about the event. This information can be parsed if the identifier is understood.	GET	O	O
2.	additionalText When present, allows a free form text description to be reported.	GET	O	O
3.	attributeList When present, contains a list of attributes and their values just before the MO was deleted.	GET	O	O
4.	correlatedNotifications When present, contains the set of notification identifiers of all notifications to which this notification is considered to be correlated.	GET	O	O
5.	eventTime Event generation time (i.e. present in the event if available).	GET	O	O
6.	eventType Specifies the type of event being reported.	GET	M	M
7.	loggingTime The time at which the record was entered into the log.	GET	M	M
8.	logRecordId Naming attribute.	GET	M	M
9.	managedObjectClass The class of the MO in which the event occurred.	GET	M	M
10.	managedObjectInstance The instance (DN) of the MO in which the event occurred.	GET	M	M
11.	notificationIdentifier Contains a unique identifier for the notification, which may be present in the «correlatedNotifications» attribute of other notifications.	GET	O	O
12.	sourceIndicator When present, indicates the source of the operation that led to the generation of this notification type. It can have one of the following values: RESOURCE OPERATION, MANAGEMENT OPERATION, UNKNOWN.	GET	O	O

6.5.4.9.3 Actions

None.

6.5.4.9.4 Notifications

None.

6.5.4.10 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.

6.5.4.10.1 MO Class Support

Index	Property	Description	ISO Status	ATN Status
1.	Managed Object Class	**6.5.4.10.1.1 StateChangeRecord** This managed object class allows to log stateChange notifications. [DELETE] operation supported on the MO. There are different instances for this MO.		
2.	Naming attribute	logRecordId		
3.	Superior in Naming Tree	log		

6.5.4.10.2 Attributes

Index	Attribute Name (Description) Syntax	Operations	ISO Status	ATN Status
1.	additionalInformation When present, allows the inclusion of a set of additional information in the event report. It is a series of data structures, each of which contains three items: an identifier, a significance indicator, and the problem information. The information subparameter carries information about the event. This information can be parsed if the identifier is understood.	GET	O	O
2.	additionalText When present, allows a free form text description to be reported.	GET	O	O
3.	attributeIdentifierList Identifies the set of attributes whose value change is being reported.	GET	O	O
4.	correlatedNotifications When present, contains the set of notification identifiers of all notifications to which this notification is considered to be correlated.	GET	O	O
5.	eventTime Event generation time (i.e. present in the event if available).	GET	O	O
6.	eventType Specifies the type of event being reported.	GET	M	M
7.	loggingTime The time at which the record was entered into the log.	GET	M	M
8.	logRecordId Naming attribute.	GET	M	M
9.	managedObjectClass The class of the MO in which the event occurred.	GET	M	M
10.	managedObjectInstance The instance (DN) of the MO in which the event occurred.	GET	M	M
11.	notificationIdentifier Contains a unique identifier for the notification, which may be present in the correlatedNotifications attribute of other notifications.	GET	O	O

12.	sourceIndicator When present, indicates the source of the operation that led to the generation of this notification type. It can have one of the following values: RESOURCE OPERATION, MANAGEMENT OPERATION, UNKNOWN.	GET	O	O
13.	stateChangeDefinition Consists of a set of sequences of the three parameters : attribute identifier, old attribute value, new attribute value.	GET	O	O

6.5.4.10.3 Actions

None.

6.5.4.10.4 Notifications

None.

6.6. Issues / Work In Progress

1. Is it really necessary to standardise MOs at the level given in this working draft? 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. Such communication is likely to be "manager-to-manager".

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 System 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 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.