ATNP/WG3/WP 17-15

ATNP/WG2/WP _____

ATNP/WG1/WP _____

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

Version: DRAFT 1.6 (MS Word 97)

15 September 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).

It should be noted that the whole area of MIB standardisation is under review, and the provisions in this draft may change fundamentally. 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 ATN Technical Provisions

Version : DRAFT 1.6 (MS Word 97)

Date: 15 September 1999

Contact: Sub-Volume editor: tony.kerr@ecsoft.co.uk
JSG chairman: moulton@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
1.4	Post Palo Alto and Naples meetings. General recommendations from Fault, Performance, Accounting and Security analysis WPs. Naming from JSG WP12-05 (F Picard). Cross-domain MIB from JSG WP12-04 (S Tamalet).	All	July 1999
1.5	Post Toulouse meeting July 99. 6.4 split into two – 6.4 now is only comms profile, new 6.5 is AOM 2x (management functions). Security MOs removed. Application recommendations from WP13-06rev (P Tupitza). AMHS MOs from WP13-10rev (J-M Vacher). XMIB structure revised.	All	August 1999

Version	Description	Affected Parts	Date
1.6	Post Toulouse meeting September 99. XMIB structure re-thought. Access control removed from scope. Various updates after JSG review. Profiles renamed. D-START mappings clarified.	Fig 6.1-1, 6.1.5.8, 6.1.5.9, 6.1.6, 6.3.1, 6.3.2, 6.4.1, 6.4.2, 6.4.3, 6.5.1.7, 6.6.1.1, 6.6.2.1, 6.6.3-7, 6.7	September 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 still change fundamentally.

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.

Cross-references:

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

[2] ATN Systems Management – Concept of Operations (CONOPS) V1.1

[3] Draft ACI/ProATN Convergent MIB

TABLE OF CONTENTS

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 ATN systems themselves (e.g. use of Echo within CLNP, 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. The technical provisions specified in this Sub-Volume support such operations between different administrations. Within a domain, general recommendations for ATN management are made, but the details of intra-domain systems management are a local matter.

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”.

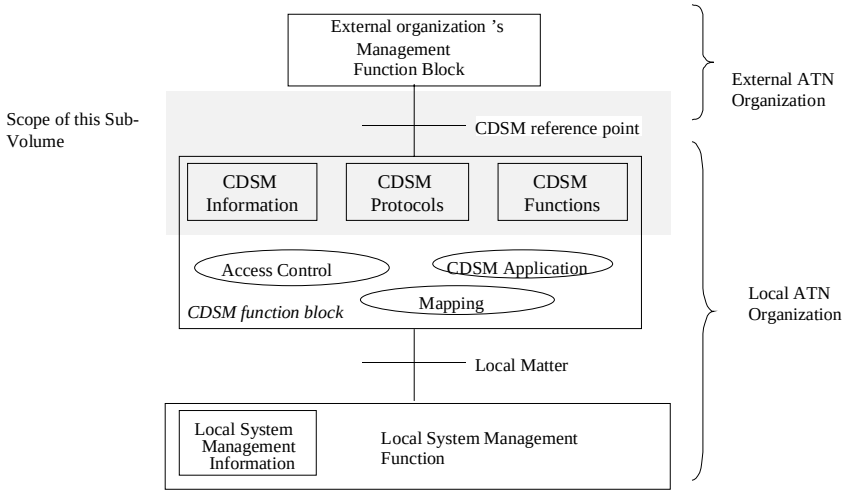

Figure 6.1-1. Functional Architecture of Cross-Domain Systems Management (CDSM)

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.

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) ATN Systems Management Function Profiles (6.5) specifies profile requirements for some common areas of systems management functionality, such as support for event reporting by means of the Event Forwarding Discriminator (EFD).

f) Cross-Domain Management Information Base (XMIB) (6.6) contains formal definitions of the 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 require 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 centre.

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.

6.1.4.4 The efficient ATN-specific CMIP profile for air-ground communications described in 6.1.5 may alternatively be used for ground-ground management communications.

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 Like the ATN air-ground applications in Sub-Volume 2, protocol overheads are minimised by application of the Packed Encoding Rules (PER) of ASN.1, and 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.

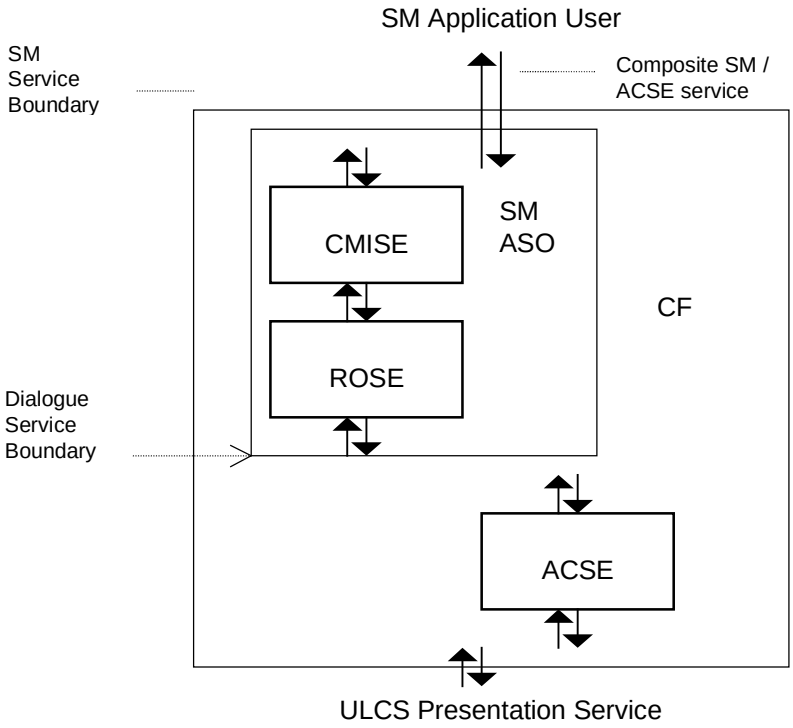

Figure 6.1-2. Use of the Dialogue Service

6.1.5.4 The CF provides a composite 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 composite service consisting of all the CMIS service primitives, plus 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 6.4.3, 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 6.4.3 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.

6.2 NAMING AND ADDRESSING PROVISIONS

Note.— This section specifies Managed Object addressing and registration requirements 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

Note 1.— ISO/IEC and ITU-T have standardised a scheme for the assignment of systems management object identifiers under the arc ***{joint-iso-ccitt ms(9) }.*** *The ISO registration scheme does not apply for non-ISO objects. It is necessary for ICAO and organisations that require to allocate object identifier values in the course of the development of management standards and development of systems management products to establish their own allocation schemes under an appropriate registration authority.*

Note 2.— The appropriate registration authority for objects defined in ICAO SARPs is ICAO. A specific arc for ATN systems management has been defined in [4]: ***{ iso (1) identified-organisation (3) icao (27) atn-sm (4) }***

Editor's Note.— This arc needs to be added in Sub-Volume 4 for Package 2.

Note 3.— The provisions defined here mirror the OSI Systems Management naming structure, to provide placeholders where additional objects specific to the ATN systems management will be identified.

6.2.1.1 ATN object identifiers for systems management shall be defined under one of the arcs defined in Table 6.2-1, which in turn are immediately subordinate to: { iso (1) identified-organisation (3) icao (27) atn-sm (4) }

Table 6.2-1. Registered Object Identifier arcs.

Registered Arc	Purpose
smo (0)	Identifies generic objects supporting the management of ATN systems.
cmip (1)	The optimised protocol option used for air-ground SM communications may require the definition of additional CMIP-related objects or the modification of existing OSI CMIP-related objects.
function (2)	Identifies objects related to additional systems management functions to support the ATN inter-domain administration, for instance the Trouble Ticket System (TTS)
smi (3)	Identifies inter-domain MIB MO Classes and MOCs needed to administer the efficiency enhanced protocol.
validation (4)	Identifies project-specific or vendor-specific entities for validation purposes.

6.2.1.2 Subordinate to { iso (1) identified-organisation (3) icao (27) atn-sm (4) validation (4) }, arcs shall be allocated to identify private organisations needing temporarily resources for object allocation.

Note.— Regional or bilateral inter-domain MIBs as well as intra-domain MIBs are not subject to standardisation by ICAO. Within a management domain, the detailed specification of systems management information is a local matter. This information contained in these MIBs will be defined either by the administration authority (e.g. CAAs) which wants to administer the ATN systems located in its domain or by the vendors of the operated ATN systems which provide a specific administration interface to its systems. The form and the location of the ATN registration tree for these MIBs cannot be pre-defined, since:

- *the form will depend of the type of Systems Management communication protocols in place between agent and manager (e.g. CMIP or SNMP). For instance, if CMIP is used as intra-domain SM communication protocol, the OSI registration tree can be used to identify MOC in use in ATN and already defined by ISO. The ATN registration tree will contain arcs for non-ISO objects.*
- *the location will depend of the level of visibility on the management information required: the registration tree could be inserted in a public arc under the responsibility of OSI, IETF or ICAO or under a private arc.*

– *the location will depend on the pre-existence of an arc assigned to the administration authority or vendor. If an arc already exists, it will be more convenient to use it rather than obtaining a new one from a registration body.*

As a consequence, there is no arc defined under the responsibility of ICAO for registering non-standardised objects. However, an arc is defined here for use by those ATN users or providers which do not have a private arc or which want to define temporarily MOC, for example for trials or the development of ATN SM products. This implies the existence of an ATN Registration Authority to which these authorities or vendors will be able to apply to assign them an arc value.

6.2.1.3 Further arcs of the ATN Systems Management global naming tree shall be allocated as shown in Table 6.2-2.

Table 6.2-2. Part of ATN Registration Tree

Object Identifier arcs							Description
1	2	3	4	5	6	7	
iso (1)	identified-organisation (3)	icao (27)	atn-sm (4)				
				smo (0)			ATN System Management Overview
				cmip (1)			Common Management Information Protocol – Fast MIP option
				function (2)			ATN Systems Management Functions
				smi (3)			ATN Structure of Management Information defined in ICAO Standards
					mibX (X)		Objects defined in ATN SARPs
						asn1Module (2)	ASN.1 Module Identifiers
						managedObjectClass (3)	Managed Object Class Identifiers
						package (4)	Package Identifiers
						parameters (5)	Parameter Identifiers
						nameBinding (6)	Name Binding Identifiers
						attribute (7)	Attribute Identifiers
						attributeGroup (8)	Attribute Group Identifiers
						action (9)	Action Types
						notification (10)	Notification Types
				validation (4)			Vendor-specific Identifiers
					ABCD (n)		Examples: projectX, CAA_Y, vendor_Z (n)
						asn1Module (2)	ASN.1 Module Identifiers
						managedObjectClass (3)	Managed Object Class Identifiers
						package (4)	Package Identifiers
						parameters (5)	Parameter Identifiers
						nameBinding (6)	Name Binding Identifiers
						attribute (7)	Attribute Identifiers
						attributeGroup (8)	Attribute Group Identifiers
						action (9)	Action Types

Object Identifier arcs							Description
1	2	3	4	5	6	7	
						notification (10)	Notification Types

Note.- The Naming Tree defined here allows for two extensibility mechanisms:

a) addition of new standard objects through the definitions of new versions of the ICAO inter-domain MIB, and

b) addition of widely-available, but non-standard, objects through the validation subtree.

6.3 ATN SYSTEMS MANAGEMENT GENERAL REQUIREMENTS

Editor's note.— The requirements in this chapter are derived from an analysis of the Working Papers "Fault Management Requirements Analysis," issue 1.1, "Performance Management Requirements Analysis," issue 1.2, "ATN Accounting Management Requirements," Draft 2.0 and "Security Management Aspect of ATN Systems Management" Also WP13-06 "Proposed Application Management BMIB". For traceability, the requirements references from these documents are given in [hidden text].

Note.— Since the ATN is dependent upon systems management procedures to monitor and maintain the provided quality of service, there is a minimum set of systems management requirements which applies to each type of ATN system (ES, BIS, IS, etc.). The general provisions in this section apply to all ATN systems, not just boundary management systems. They apply to intra-domain systems management as well as inter-domain, though details of the mechanisms used to satisfy the requirements within a given management domain are a local matter.

6.3.1 General Provisions

Note.— ATN systems are expected to support the general systems management capabilities specified in this and the following subsections as the minimum functionality available to a suitably authorised and authenticated local systems manager.

6.3.1.1 In general, for airborne systems, systems management events shall be logged locally for subsequent offline processing.

Note.— This does not preclude the implementation of a local airborne systems management Manager application, nor does it require such a Manager application.

6.3.1.2 Ground systems shall have the capability of notifying relevant events to the local systems management subsystem.

Note 1.— Such events may then be forwarded to a suitably authorised and authenticated local systems manager, depending upon factors such as the current Event Forwarding Discriminator (EFD) attribute values.

Note 2.— Other strategies such as a polling mechanism could alternatively be used.

6.3.1.3 **Recommendation.—** *It should be possible to selectively enable and disable event logging where a requirement to log an event is identified.*

6.3.1.4 **Recommendation.—** *It should be possible to selectively enable and disable event forwarding where a requirement to notify an event to a system manager is identified.*

6.3.1.5 **Recommendation.—** *ATN systems should provide for remote restart on command from a suitably authenticated and authorised Network Manager.*

6.3.1.6 **Recommendation.—** *ATN Routers should provide for remote isolation, i.e. graceful termination of the operational state and entry into a state where the router only responds to Systems Management requests.*

6.3.1.7 **Recommendation.—** *All ATN systems should keep local event logs for the recording of designated systems management events. Some mechanism should also be provided to transfer these logs to an offline processor.*

6.3.1.8 **Recommendation.—** *The MTBF and MTTR metrics of all ATN systems and subnetworks should be actively monitored to ensure that they match theoretical expectations.*

6.3.1.9 **Recommendation.—** *ATN Routers should maintain synchronised clocks for event logging purposes.*

6.3.1.10 **Recommendation.—** *System specific parameters that affect forwarding performance (e.g. memory utilisation) should be logged.*

6.3.1.11 A Network Management Station (NMS) shall support the basic functions of handling Notifications (e.g. by display to a human user) and supporting operations on Managed Objects (e.g. by means of a graphical user interface).

6.3.1.12 A Network Management Agent (NMA) shall support the basic functions of emitting Notifications and providing access to Managed Objects.

6.3.1.13 ATN systems shall support a general capability to allow them to be configured by a local systems manager, and for configuration parameters to be accessible by a local systems manager.

6.3.1.14 Manager-Agent operations shall be authenticated by the Agent.

Note.— Since SM Managers can access SM Agents to retrieve and modify (where applicable) managed objects in the agent's management domain, authentication must be performed to protect against potential masquerade. An SM Manager can also access another SM Manager's managed objects, therefore Manager-Manager authentication is also required.

6.3.1.15 Agent-Manager operations shall be authenticated by the Manager.

Note.— An SM Manager needs to authenticate an SM Agent to provide the protection that a third party may not masquerade as a legitimate SM Agent and provide false management information. This requirement also applies in Manager-Manager communication where one SM Manager acts as an SM Agent.

6.3.1.16 **Recommendation.—** *Only security alarm notifications and audit trail notifications should be included in security related notifications to a manager.*

6.3.1.17 **Recommendation.—** *Local access control policy should define the SM Manager(s) that are authorised to receive notifications.*

6.3.1.18 **Recommendation.—** *Local mechanisms should be provided to report physical access and application access control violations.*

6.3.1.19 A security alarm report shall be sent when there is a security violation such as failed authentication.

6.3.1.20 The following security events, as a minimum, shall be logged:

a) Authentication failures at ATS applications or at the boundary intermediate systems

b) Unauthorised accesses to management information and ATN resources

c) Detection of replayed ATS application messages or router IDRP PDUs

Note 1.— Encryption related integrity is not within the scope of ATN security although it may be used by other aeronautical organisations, such as airlines.

Note 2.— Denial of service is reported via security audit trail reporting.

6.3.1.21 **Recommendation.—** *Air-ground ATN implementations should report only critical and major severity levels of security alarm event; ground-ground ATN implementations may choose to report more levels of severity if necessary.*

6.3.1.22 **Recommendation.—** *ATN systems should maintain at least the following ATN security audit trail reports/logs:*

a) Requests (both successful and failed) of cryptographic key certificates (where applicable)

b) Attempts (both successful and failed) to create, delete, revoke, and modify cryptographic key certificates (where applicable)

c) Denial of data link service or ATS application service

6.3.1.23 **Recommendation.—** *In the ATN environment, the following service requests of event type serviceReport should be recorded: key creation, deletion, revocation, modification of key certificates, and X.500 service requests.*

6.3.2 General Management Provisions for ATN Upper Layers and Applications

6.3.2.1 **Recommendation.—** *Applications that implement compliancy checks on the operation of the Transport Service should generate a systems management event upon incorrect operation of the Transport Service.*

Note.— Mis-sequencing, corruption and loss and/or mis-delivery of user messages may occur due to incorrect operation of the transport layer software. This could be due to incorrect assignment of TPDU sequence numbers, packet re-ordering errors by the receiving transport entity, or failure to detect and handle network errors. ATN Applications require a high availability, reliable transport service, and this can only be provided if the transport layer software can be relied upon. High quality design and implementation of the transport layer software and extensive testing are required. This type of fault is not an ATN Internet error but a software error in the End System. Such problems should be logged locally, if detected by an application, as well as reported to the End User if there are implications for the correct operation of the application.

6.3.2.2 **Recommendation.—** *In order to allow percentage availability to be determined, the end-user application should record, in a local log, each successful attempt and each failed attempt to use the service provided by the communications subsystem, including, for example, each unsuccessful attempt to establish an end-to-end connection.*

6.3.2.3 **Recommendation**.— *To allow the percentage availability of applications to be determined, ATN end systems should record, in a local log, each time a 'service unavailable' application message is received.*

6.3.2.4 **Recommendation.—** *When authentication is implemented by means of some transformation of the user data being appended to the user data itself, this should be used to verify data integrity, by logging all authentication failures, as well as numbers of messages successfully received.*

Note.— Where a checksum or hash function is used as part of the authentication mechanism, reported authentication failures may in fact be the result of loss of data integrity e.g. through undetected network errors.

6.3.2.5 **Recommendation.—** *Authentication or data integrity failure events should result in a systems management notification being generated.*

Note.— Other strategies such as a polling mechanism could alternatively be used.

6.3.2.6 **Recommendation.—** *To enable connection establishment delay metrics to be measured, the ACSE or Dialogue Service should record, in a local log, each connect request, and the time at which the connect request was issued, as well as the time of each successful connection establishment.*

6.3.2.7 **Recommendation.—** *To allow transit times and reliability metrics to be deduced, ATN systems should have the capability to log an event when a user message crosses the notional ASE service boundary, i.e. when a message is submitted to or received from the communications subsystem.*

Note.— Such capability would not necessarily be utilised for every ASE service invocation; a sampling approach could be adopted for example.

6.3.2.8 **Recommendation.—** *Use should be made of application time-stamps, where available, to log the end to end transfer delays of user messages.*

6.3.2.9 **Recommendation.—** *For each confirmed application service, the round trip delay between request and confirmation messages should be logged, and used to provide an estimate of the end-to-end transfer delay in one direction.*

6.3.2.10 **Recommendation**.— *The mean and maximum values of the measured time interval between request and confirmation primitives should be recorded, in a local log, for each confirmed applications service.*

Note.— Measurements need to include transmission time of the request message, the message computation time by the remote system, the human response time and the transmission time of the corresponding response message. If no dialogue was in place, the delay includes the connection establishment delay and the transfer delay for the two messages. Otherwise, the delay includes the data transfer delay for the two messages only.

6.3.2.11 **Recommendation.—** A*pplications should generate a systems management event when the measured or deduced end-to-end transfer delay exceeds a specified threshold (typically application specific - e.g. based on ATSC Class). An unacceptably long transit delay should be reported both to the service user and (for Ground Systems) a Network Manager.*

6.3.2.12 The addressing and version information exchanged by the CM application shall be provided to any ATN system manager, on request.

6.3.2.13 **Recommendation.—** *ATN end systems should record, in a local log, protocol errors by reason.*

6.3.2.14 **Recommendation.—** *ATN end systems should have the ability to signal an event when version negotiation fails between peer systems.*

6.3.2.15 **Recommendation.—** *ATN end systems should have the ability to signal an event when an unrecoverable error exception leads to the shutdown of the application ASE.*

6.3.2.16 **Recommendation**.— *ATN systems should record, in a local log, each ASE provider abort by abort reason.*

6.3.2.17 **Recommendation.—** *ATN systems should signal an event when an ASE technical timer expires and results in the termination of the application.*

6.3.3 General Provisions for ATN Transport Layer

6.3.3.1 **Recommendation.—** *To enable connection establishment delay metrics to be measured, the transport layer should record, in a local log, each connect request, and the time at which the connect request was issued.*

6.3.3.2 **Recommendation.—** *To enable connection establishment delay metrics to be measured, the transport layer should record, in a local log, the time of each successful connection establishment.*

6.3.3.3 **Recommendation.—** *The Transport Provider should generate a systems management event when a Transport Connection fails to be established.*

6.3.3.4 **Recommendation.—** *The Transport Provider should generate a systems management event when an established Transport Connection is lost.*

6.3.3.5 **Recommendation.—** *To enable continuity to be measured, the transport layer should record, in a local log, each uncommanded transport connection loss and each corresponding resumption of service.*

6.3.3.6 **Recommendation.—** *To allow transit delay metrics to be calculated, the transport layer should record, on a per transport connection basis, the measured round trip delay between transmission of a TPDU and its acknowledgement, together with an indication of whether the TPDU marks the end of a TSDU.*

6.3.3.7 **Recommendation.—** *The CO Transport Layer should generate a systems management event when the end-to-end transit delay as measured by the transport provider and derived from the round trip delay, exceeds a specified threshold (typically application specific - e.g. based on ATSC Class). An unacceptably long transit delay should be reported both to the service user and (for Ground Systems) a Network Manager.*

6.3.3.8 **Recommendation.—** *The Transport Layer should generate a systems management event when the number of TPDU discards due to checksum validation failure exceeds a Network Manager specified threshold during a given reporting period.*

6.3.3.9 **Recommendation.—** *The transport entity should record and log the number of TPDUs and TPDU octets sent and received over each transport connection.*

6.3.3.10 **Recommendation.—** *To allow reliability and throughput metrics to be calculated, the transport layer should record, in a local log, the number and total size of user messages sent on each transport connection.*

6.3.3.11 **Recommendation.—** *To allow reliability and throughput metrics to be calculated, the transport layer should record, in a local log, the number and total size of user messages received, both with and without error, on each transport connection in a given time period, analysed by sender.*

6.3.4 General Provisions for ATN Lower Layers

6.3.4.1 **Recommendation.—** *The connectionless network service provider should support the remote invocation of the Echo Request function and option selection.*

6.3.4.2 **Recommendation.—** *ATN systems should have the ability to emit a systems management notification when an ECHO Request (ERQ) NPDU is delivered to that system, and that system is the final destination of the NPDU. The notification should include information contained in the ERQ NPDU.*

6.3.4.3 **Recommendation.—** *ATN systems should have the ability to emit a systems management notification when an ECHO Response (ERP) or Error NPDU is delivered to that system, and that system is the final destination of the NPDU. The notification should include information contained in the ERQ or Error NPDU.*

Note 1.— The above three Recommendations are of major importance for fault and performance investigation by systems managers. However, it is possible that not all ATN participants will allow a manager in another domain to initiate ERQs. This would be analogous to Internet systems that do not answer "ping" requests.

Note 2.— This is an important requirement for Fault Management, both intra- and inter-domain. For maximum utility, the above recommendations need to be supported in each and every ATN Router for any Network Manager Station. Safeguards would be required for local Agents to validate and/or prohibit access from external users (i.e. need to be able to monitor and identify the source of ECHO Requests in locally managed Routers, and be able to discard them if appropriate). A Network Manager could then be provided with tools to generate ECHO PDUs from any point in the ATN Internet, and to correlate the notifications of ECHO responses and Error Responses with ECHO requests. The generation and use of Test Data patterns as the payload of ECHO Request PDUs, including monitoring for inconsistencies between responses and requests, would also be useful.

6.3.4.4 **Recommendation.—** *CLNP Header checksums should be used in all CLNP packets.*

6.3.4.5 **Recommendation.—** *All ATN Systems should keep a count of the number of packets received with a CLNP header checksum failure.*

Note.— The detection of CLNP Header checksum failures supports the measurement of subnetwork integrity metrics, and facilitates detection of subnetwork problems at source.

6.3.4.6 **Recommendation.—** *ATN systems should log CLNP packet discards by discard reason.*

6.3.4.7 **Recommendation.—** *The connectionless network service provider should generate a systems management event when the number of CLNP PDU discards for Header Checksum verification, lifetime expiry or routing problems exceeds a specified threshold. Such thresholds should be specified by discard reason.*

6.3.4.8 **Recommendation.—** *When the number of packet discards due to congestion exceeds a defined threshold during a given reporting period, then a notification should be sent to a network manager.*

6.3.4.9 **Recommendation.—** *A CLNP Error Report should be requested (by means of the CLNP Header "error" bit) for all Data PDUs addressed to airborne destinations.*

6.3.4.10 **Recommendation.—** *The number, average and maximum size of CLNP packets sent and received during a reporting period should be logged. These should be analysed by ATSC Class and priority, and by each data link.*

6.3.4.11 **Recommendation.—** *For capacity planning, ATN Routers should keep counts of packets forwarded and data volumes, analysed by priority and ATSC Class.*

6.3.4.12 **Recommendation.—** *The connectionless network service provider should provide read-only remote access to its Forwarding Information Base (FIB).*

6.3.4.13 **Recommendation.—** *The IS-SME should report when the number of "Failure to complete the Route Initiation procedures" events exceeds a Network Manager specified threshold during a given reporting period.*

6.3.4.14 **Recommendation.—** *The ISSME or the ES-IS entity should record and log the number of ES-IS PDUs and ES-IS PDU octets exchanged with each adjacent system over each mobile subnetwork.*

6.3.4.15 **Recommendation.—** *The IDRP entity should record and log the number of IDRP PDUs and of IDRP PDU octets sent and received over each BIS-BIS adjacency.*

6.3.4.16 **Recommendation.—** *IDRP should provide read-only remote access to its Routing Information Base (RIB), permitting the download of the complete RIB by a Network Manager.*

6.3.4.17 **Recommendation.—** *IDRP should generate a systems management event upon loss of an adjacency.*

6.3.4.18 **Recommendation.—** *IDRP should support remote start up and shutdown of Ground/Ground adjacencies with other Routers (for fault isolation).*

6.3.4.19 **Recommendation.—** *IDRP should support remote invocation of the RIB Refresh procedure, where this is available in ground Routers.*

6.3.4.20 **Recommendation.—** *When the IS-IS protocol is used, then read-only remote access should be provided to its Routing Information Base (RIB), permitting the download of the complete RIB by a Network Manager.*

6.3.4.21 **Recommendation.—** *When the IS-IS protocol is used, then the protocol entity should generate a systems management event upon loss of an adjacency.*

6.3.4.22 **Recommendation.—** *When ES-IS protocol is used (i.e. for all airborne and air-ground systems, and optionally for ground systems), then read-only remote access should be provided to its Routing Information Base (RIB), permitting the download of the complete RIB by a Network Manager.*

6.3.4.23 **Recommendation.—** *If available, the Deflate compression algorithm should be invoked on all air/ground data links.*

Note.— The detection of Deflate checksum errors will facilitate early detection of ground station problems, and supports the measurement of subnetwork integrity metrics.

6.3.4.24 **Recommendation.—** *The Mobile SNDCF should generate a systems management event upon detecting packet level Deflate checksum failures (Air/Ground Routers only).*

6.3.4.25 **Recommendation.—** *When Deflate is implemented, ATN Systems should keep a count of the number of packets received with a Deflate checksum failure.*

6.3.4.26 **Recommendation.—** *Connection Mode SNDCFs should report unexpected subnetwork connection loss and subnetwork reset.*

6.3.4.27 **Recommendation.—** *To allow subnetwork service continuity metrics to be monitored, all ATN Systems should log the time of uncommanded loss of a subnetwork connection.*

6.3.4.28 **Recommendation.—** *SNDCFs should support remote start up and shutdown of data links.*

6.3.4.29 **Recommendation.—** *When subnetworks or subnetwork connections can be dynamically managed, Systems Management actions should be available to activate and deactivate them.*

6.3.4.30 **Recommendation.—** *To allow subnetwork service availability metrics to be monitored, all ATN Systems should log each successful and each unsuccessful attempt to use the subnetwork service, i.e. to establish a connection over a connection mode subnetwork, or to send a packet over a connectionless subnetwork.*

6.3.4.31 **Recommendation.—** *ATN Air/Ground Routers should log the establishment and termination of subnetwork connections with Airborne Routers, together with time stamps to allow the duration of each mobile subnetwork connection to be obtained.*

6.3.4.32 **Recommendation.—** *To allow subnetwork service connection establishment delay metrics to be monitored, on each connection mode subnetwork, an ATN system should log the time at which each connect request is sent and the time at which the connection is successfully established.*

6.3.4.33 **Recommendation.—** *To allow subnetwork service continuity metrics to be monitored, when possible, ATN systems should log the time of each failure to transmit a packet over a connectionless subnetwork, and time of the next successful transmission attempt.*

6.3.4.34 **Recommendation.—** *All ATN Systems should log the number of packets sent and received over each subnetwork or subnetwork connection, and count the volume of data sent and received, analysed by priority and ATSC Class.*

Note.— Implementing the above recommendation will allow the determination of subnetwork service Reliability (the probability that a packet is delivered without errors) and Throughput metrics. It will also be important for trend analysis and capacity planning..

6.3.4.35 **Recommendation.—** *The mobile SNDCF entity should record, both before and after compression, the number of PDU octets sent and received over each mobile connection.*

6.3.4.36 **Recommendation.—** *To enable detection of capacity overloads, all ATN Systems should monitor average queue length analysed by priority during each sampling period, and generate a notification when the average queue length exceeds a set threshold (high watermark) or drops below another set threshold (low watermark).*

6.3.4.37 **Recommendation.—** *Changes to the number of entries in a Router's FIB should be logged.*

6.3.4.38 **Recommendation.—** *ATN Routers should log each route received and each route advertised to another router, recording the time received/advertised.*

6.3.4.39 **Recommendation.—** *ATN Air/Ground Routers should log the establishment and termination of adjacencies with Airborne Routers.*

6.3.4.40 **Recommendation.—** *If the performance assessment mechanism adopted requires that data flows are individually monitored ("microscopic" view), ATN Routers should meter each data flow, counting number of packets and data volumes for each identified data stream, where a data stream is identified by a unique combination of source, destination, priority and ATSC Class.*

6.3.4.41 **Recommendation.—** *If the performance assessment mechanism adopted requires only that the total data flow at each entry and exit point is monitored ("macroscopic" view), ATN Routers should meter, for each ATSC Class and priority, the number of packets and data volume received from each identified source and the number and volume sent to each identified destination, i.e. metering of aggregate values, rather than individual flows.*

6.3.5 General Provisions for ATN Subnetworks

6.3.5.1 **Recommendation.—** *Subnetworks should keep counts of packets sent and received, and of error counts where applicable, and provide remote access to such statistics.*

6.3.5.2 **Recommendation.—** *Subnetworks should report error counts that exceed a specified threshold during a set reporting period.*

6.3.5.3 **Recommendation.—** *Subnetworks should provide subnetwork specific diagnostics and test procedures, as appropriate for the subnetwork type, and support their remote use by a Network Manager.*

6.3.5.4 **Recommendation.—** *Subnetworks should report the set of existing subnetwork connections and the operational parameters for each such connection.*

6.3.5.5 **Recommendation.—** *Mobile Subnetworks should report when the number of "Failure to join a mobile subnetwork" events exceeds a Network Manager specified threshold during a given reporting period.*

6.3.5.6 **Recommendation.—** *Ground Systems should generate a systems management event on failure to establish a subnetwork connection. This notification may be subject to threshold counts by diagnostic reason. Airborne systems should log such events.*

6.3.6 Accounting Meter Provisions

6.3.6.1 **Recommendation.—** *If the adopted charging model is based on usage-sensitive charging policies, ATN systems should implement a metering function that allows measurement of individual flows, which are distinguished in the ICS traffic as a function of the value of certain parameters. The local charging policy determines the distinguishing parameters (e.g. traffic type, source/destination address).*

6.3.6.2 **Recommendation.—** *For usage-sensitive charging policies, the metering function should be configurable and provide for the following capabilities:*

a) Filtering: to select based on certain criteria the subset of traffic for which accounting has to be performed

b) Segregation: to segregate the accountable traffic into individual flows that have to be accounted separately

c) Recording: to log for each of the individual flows the distinguishing parameters of the flows and the associated accounting data.

6.3.6.3 **Recommendation.—** *For usage-sensitive charging policies, the metering function should support the selection of zero, one or several of the following filters :*

a) Select for accounting, the packets exchanged over a particular subnetwork interface of the ATN system

b) Select for accounting, the packets exchanged with a particular adjacent system (i.e. packets received/sent from/to a particular remote SNPA address

c) Select for accounting, the packets whose source address in packets received and destination address in packets sent matches one particular NSAP address prefix

d) Select for accounting, the packets whose destination address in packets received and source address in packets sent matches one particular NSAP address prefix

e) Select for accounting, the packets whose source address in packets received and destination address in packets sent does not match one particular NSAP address prefix

f) Select for accounting, the packets whose destination address in packets received and source address in packets sent does not match one particular NSAP address prefix

g) Select for accounting, the packets exchanged between two particular zones of the ATN (i.e. whose source and destination NSAP addresses match a particular pair of NSAP address prefixes)

h) Select for accounting the packets that have a particular traffic type

i) Select for accounting the packets that have a particular priority.

6.3.6.4 **Recommendation.—** *For usage-sensitive charging policies, the metering function should be able to segregate the traffic into individual flows, on the basis of:*

a) The subnetwork interface over which the packets are exchanged (i.e. packets exchanged over different subnetwork interfaces, are considered to belong to different flows)

b) The remote SNPA address of the adjacent system with which the packets are exchanged (i.e. packets exchanged with different adjacent systems, are considered to belong to different flows)

c) The prefix of the source NSAP address in packets received and the destination NSAP address in packets sent (i.e. packets received from/sent to different zones of the ATN are considered to belong to different flows)

d) The prefix of the destination NSAP address in packets received and the source NSAP address in packets sent (i.e. packets received from/sent to different zones of the ATN are considered to belong to different flows)

e) The source and destination NSAP address prefixes (i.e. packets exchanged between two different zones of the ATN are considered to belong to different flows)

f) the traffic type (i.e. packets with different traffic types are considered to belong to different flows)

g) the priority (i.e. packets with different priority are considered to belong to different flows).

6.3.6.5 **Recommendation.—** *For usage-sensitive charging policies, the metering function should be able to record the following information:*

a) The start and stop time

b) The number of packets sent and received

c) The number of octets sent and received

d) The filters that were applied

e) The value of the distinguishing parameters of the flow.

6.4 ATN SYSTEMS MANAGEMENT COMMUNICATION PROFILES

6.4.1 General Provisions

Note 1.— Two distinct profiles for ATN inter-domain SM communications are defined in this chapter. The general requirements for SM communication are specified by reference to internationally standardised profiles (ISPs) to the extent possible. The communications functionality for both ATN profiles is defined in the ISP for the Enhanced Management Communications profile identified as AOM 12.

Note 2.— The provisions in this chapter are solely to facilitate the use of Cross-Domain Systems Management (CDSM) and the Cross-Domain management information base (XMIB). Requirements on Managers are therefore only applicable to boundary management systems, i.e. those that will communicate with Agents in other management domains. Requirements on Agents are only applicable to Agents that will communicate with Managers in other management domains, and that provide access to the cross-domain MIB specified in 6.6.

Note 3.— There may also be requirements 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.

6.4.1.1 ATN Systems Management communication between administrative domains shall use the ISO/IEC 9595 and 9596-1 Common Management Information Service and Protocol (CMIS/CMIP), as profiled in this chapter.

6.4.1.2 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 CMIP standards do not mandate the responsibility of establishing communication to either the manager role system or the agent role system but leave the particular style of management to be determined by the implementer or user. It is therefore necessary to ensure that all implementations are capable of establishing communications.

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

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

6.4.1.5 Inter-domain Communication between Manager Applications

Note.— Information exchanged between Managers is likely to be limited to cross-domain statistical or aggregate information e.g. for accounting purposes. No special profile requirements for Manager to Manager communications are specified. The Cross-Domain CMIP profiles defined here 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.

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

6.4.1.5.2 Thus Manager implementations with Cross-Domain responsibilities, i.e. those supporting a Cross-Domain MIB, shall support both Manager and Agent roles.

6.4.2 ATN Management Communications Profile using Full OSI Stack

Note.— The "full CMIP" profile referenced in this section is suitable for ground-ground management communications between management domains. It may also be used ground-ground within a local management domain if CMIP-based management is chosen, but this is a local matter.

6.4.2.1 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 6.4.2.2.

6.4.2.2 Mapping to the ATN Transport Service

Note.— 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).

6.4.2.2.1 The ATN systems management communication profile specified above shall make use of the connection mode ATN Transport Service as specified in 5.5.

6.4.2.2.2 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.

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

6.4.2.2.4 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.

6.4.2.2.5 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.

6.4.2.2.6 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.

6.4.2.2.7 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.

6.4.2.2.8 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.— The TS-User provides the complete ATN Security Label, although only security tag value is of relevance. 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.

6.4.3 ATN Management Communications Profile using ULCS

Note 1.— The ATN-specific "efficiency-enhanced CMIP" profile defined in this section is suitable for air-ground management communications. It may also be used for ground-ground management communications, by bilateral agreement between communicating parties.

Note 2.— This section specifies requirements for an ATN-specific 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 3.— For efficient use of air-ground data links, and to avoid multiple protocol stacks in ATN systems, the "efficient" 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.

6.4.3.1 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 efficiency options), then the communication profile shall be as specified in this subsection.

6.4.3.2 The complementary communications interactions between CMISE-service-users within two end Management Information systems shall comply with the provisions specified here, with scope as specified in International Standardised Profile AOM 12 and illustrated in Figure 6.4-1.

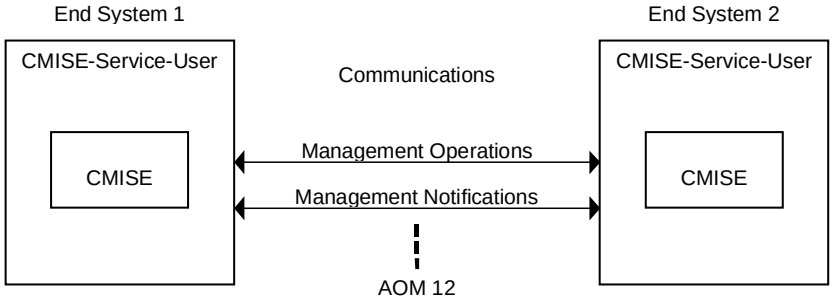

Figure 6.4-1. Scope of the SM Communications Profile

6.4.3.3 The supporting protocols for the efficient management communications profile shall be as specified in the 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)

Note.— Table 6.4-1 supersedes Table 1 of ISO/IEC ISP 11183-2 for the purposes of the ATN-specific efficient CMIP profile.

6.4.3.4 The profile requirements shall be as specified for profile AOM 12 in ISO/IEC ISP 11183-2, except that the functions required from the supporting protocol stack of ACSE, Presentation and Session layers are specified in Sub-Volume 4, and not in part 1 of the multipart ISP AOM 1n.

Note.— The differences between the "efficient" ATN management communications profile and the standard AOM 12 profile are listed in Table 6.4-2.

Table 6.4-2 – Divergence from 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 above.
1.5	Replace reference to part 1 of AOM 1n with reference to the Dialogue Service in Sub-Volume 4.
5 (Conformance to AOM 12)	Replace reference to ISO/IEC ISP 11183-1 (which refers to ACSE, Presentation and Session layer requirements) with reference to the ULCS profile in Sub-Volume 4.
5.1	Delete reference to ISO/IEC ISP 11183-1.
5.3	Delete Note 2, "The complete association requirements are specified in ISO/IEC ISP 11183-1."
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.

ISP 11183-2 clause	Modification for ATN Profile
A.2.3, Table A.3 caption	Replace "(in AARQapdu)" with "(in D-START Request and Indication User-Data)".
A.2.3, Table A.4 caption	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.

6.4.3.5 The CMIPUserInfo parameter shall be conveyed as the User-data of D-START primitives (rather than directly in AARQ and AARE apdus, as specified in ISP 11183-2).

6.4.3.6 Support for the CMIPUserInfo parameter shall be as specified in Tables 6.4-3 and 6.4-4 (which replace ISP 11183-2 Tables A.3 and A.4, respectively).

Table 6.4-3. CMIPUserInfo parameter support (in D-START Request and Indication User-data)

		D-START req			D-START ind		
Index	Parameter name	AOM 12	ATN	Type, value(s) & range(s)	AOM 12	ATN	Type, value(s) & range(s)
A.3.1	CMIPUserInfo	mm	mm		mm	mm	
A.3.1.1	protocolVersion	mm	mm	version 2	mm	mm	version 2
A.3.1.2	functionalUnits	mo	mo	(1)	mo	mo	(1)
A.3.1.3	accessControl	mo	mo	(2)	mo	mo	(2)
A.3.1.4	userInfo	mo	i	(2)	mo	i	(2)

(1) The Initiator (combination of CMISE user and CMISE provider) must be capable of proposing functional units value “11101”B, given that the CMISE user requires them. The CMIP provider must be capable of supporting all functional units, except for “extended service”.

(2) In order to parse or process this, there must be an agreement as to what abstract syntax will be used in the EXTERNAL type. If this parameter is present in a user request, the CMIP machine shall include it in the CMIP PDU sent. If this parameter is present on a received CMIP PDU, the CMIP machine shall pass the parameter to the CMISE user. The CMIP machine does not interpret this parameter.

Table 6.4-4. CMIPUserInfo parameter support (in D-START Response and Confirmation User-data)

		D-START rsp			D-START cnf		
Index	Parameter name	AOM 12	ATN	Type, value(s) & range(s)	AOM 12	ATN	Type, value(s) & range(s)
A.4.1	CMIPUserInfo	mm	mm		mm	mm	
A.4.1.1	protocolVersion	mm	mm	version 2 (3)	mm	mm	version 2 (3)

A.4.1.2	functionalUnits	mo	mo	(1)	mo	mo	(1)
A.4.1.3	accessControl	mo	mo	(2)	mo	mo	(2)
A.4.1.4	userInfo	mo	io	(2)	mo	i	(2)

(1) The Responding CMISE provider may negotiate down from proposed functional units value "11111"B to "11101"B. The CMIP provider must be capable of supporting all functional units, except for "extended service".

(2) In order to parse or process this, there must be an agreement as to what abstract syntax will be used in the EXTERNAL type. If this parameter is present in a user request, the CMIP machine shall include it in the CMIP PDU sent. If this parameter is present on a received CMIP PDU, the CMIP machine shall pass the parameter to the CMISE user. The CMIP machine does not interpret this parameter.

(3) The system may negotiate away Version 1.

6.4.3.7 Support for the CMIPAbortInfo parameter shall be as specified in Table 6.4-5 (which replaces ISP 11183-2 Table A.5).

Table 6.4-5. CMIPAbortInfo parameter support

		Sender			Receiver		
Index	Parameter name	AOM 12	ATN	Type, value(s) & range(s)	AOM 12	ATN	Type, value(s) & range(s)
A.5.1	CMIPUserInfo	mm	mm		mm	mm	
A.5.1.1	abortSource	mm	mm		mm	mm	
A.5.1.2	userInfo	mo	i	(1)	mo	i	(1)

(1) In order to parse or process this, there must be an agreement as to what abstract syntax will be used in the EXTERNAL type. If this parameter is present in a user request, the CMIP machine shall include it in the CMIP PDU sent. The CMIP machine does not interpret this parameter. If this parameter is present on a received CMIP PDU, the CMIP machine shall pass the parameter to the CMISE user. The CMIP machine does not interpret this parameter.

6.4.3.8 Static support for common protocol parameters shall be as specified in Table 6.4-6 (which replaces Tables A.13a and A.13b in ISP 11183-2).

Table 6.4-6. Common CMIP APDU parameter support.

Index	Parameter name	Syntax	Sending		Receiving		Type, value(s) & range(s)
			AOM12	ATN	AOM12	ATN	
A.13.1	invokeID	INTEGER	m	m	m	m	(3)
A.13.2	linked-ID	INTEGER	m	m	m	m	(3)
A.13.3	baseManagedObjectClass	OBJECT IDENTIFIER INTEGER	m i	m i	m m	m m	
A.13.4	baseManagedObjectInstance	DistinguishedName OCTET STRING RDNSequence	m i m	m i m	m m m	m m m	
A.13.5	accessControl	EXTERNAL	m	m	m	m	(2)
A.13.6	synchronization	ENUMERATED	m	m	m	m	0 to 1
A.13.7	managedObjectClass	OBJECT IDENTIFIER INTEGER	m	m	m	m	
A.13.8	managedObjectInstance	DistinguishedName OCTET STRING RDNSequence	m i m	m i m	m m m	m m m	
A.13.9	currentTime	GeneralizedTime	m	m	m	m	
A.13.10	actionType	OBJECT IDENTIFIER INTEGER	m i	m m	m m	m m	

A.13.11	attributeId	OBJECT IDENTIFIER INTEGER	m i	m m	m m	m m	
A.13.12	eventType	OBJECT IDENTIFIER INTEGER	m i	m m	m m	m m	

(1) The values for the Sending and receiving columns in this table apply consistently across all PDU parameter tables in AOM 12, which use the corresponding common parameter.

(2) In order to parse or process this, there must be an agreement as to what abstract syntax will be used in the EXTERNAL type. If this parameter is present in a user request, the CMIP machine shall include it in the CMIP PDU sent. If this parameter is present on a received CMIP PDU, the CMIP machine shall pass the parameter to the CMISE user. The CMIP machine does not interpret this parameter

(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.

6.4.3.9 Presentation and Session layer functional unit support shall be as specified in Sub-Volume 4, and not as specified in ISP 11183-2 Tables A.123 and A.124.

6.4.3.10 Encoding Requirements for the “efficient” ATN management profile

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

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

6.4.3.10.3 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".”

6.4.3.11 Mapping to Dialogue Service for the “efficient” ATN management profile

6.4.3.11.1 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.

6.4.3.11.2 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.

6.4.3.11.3 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.

6.4.3.11.4 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.

6.4.3.11.5 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.

6.4.3.12 Mapping to Dialogue Service Parameters

6.4.3.12.1 When a CMISE-service-user requires to open an association for the exchange of CMISE / ROSE APDUs, this shall be mapped to the D-START request primitive defined in [ULCS] 4.2.3.2 with parameter values as indicated in Table 6.4-7.

Table 6.4-7

D-START Request parameter	**Value**
Called Peer ID	(Optional) Location of peer SMAE (24-bit aircraft identifier or ground Facility Designator)
Called Sys-ID	(Optional) System identifier (LOC+SYS) from address to distinguish between multiple peer SMAEs at the given location, if required.
Called Presentation Address	(Optional) PSAP address of peer SMAE. Must be supplied if, and only if, Called Peer ID is not specified)
Calling Peer ID	Not used
Calling Sys-ID	Not used
Calling Presentation Address	Not used

D-START Request parameter	Value
DS-User Version Number	1
Security Requirements	For further study
Quality of Service: Routing Class	"ATN Systems Management Communications" (Value 60 Hex)
Quality of Service: Priority	"Network / Systems Management" (Value 14 Decimal)
Quality of Service: Residual Error Rate	"low"
User Data	CMIPUserInfo (see Table 6.4-3)

6.4.3.12.2 When a CMISE-service-user requires to respond to a request from a peer to open an association for the exchange of CMISE / ROSE APDUs, this shall be mapped to the D-START response primitive defined in [ULCS] 4.2.3.2 with parameter values as indicated in Table 6.4-8.

Table 6.4-8

D-START Response parameter	Value
DS-User Version Number	1
Security Requirements	For further study
Quality of Service: Routing Class	"ATN Systems Management Communications" (Value 60 Hex)
Quality of Service: Priority	"Network / Systems Management" (Value 14 Decimal)
Quality of Service: Residual Error Rate	"low"
Result	"accepted" or "rejected (transient)" or "rejected (permanent)" as selected by the CMISE-service-user.
User Data	CMIPUserInfo (see Table 6.4-4), if any.

6.4.3.13 Mapping to the ATN Transport Service

Note.— For the "efficient" ATN Management Communications profile, the use of the ATN connection-oriented Transport Service is specified in Sub-Volume 4.

6.5 ATN SYSTEMS MANAGEMENT FUNCTION PROFILE

Note 1.— In addition to the SM communication capabilities specified in 6.4, the basic level of SM functionality specified in the ISPs for profiles AOM211, AOM 221 and AOM 231 is required. These profiles in turn refer to AOM 12, so their specification automatically invokes the relevant parts of AOM 12.

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 (alarm reporting and state management capabilities) and/or AOM 213(alarm reporting capabilities) 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.

Note 5.— The provisions in this chapter are solely to facilitate the use of Cross-Domain Systems Management (CDSM) and the Cross-Domain management information base (XMIB). Requirements on Managers are therefore only applicable to boundary management systems, i.e. those that will communicate with Agents in other management domains. Requirements on Agents are only applicable to Agents that will communicate with Managers in other management domains, and that provide access to the cross-domain MIB specified in 6.6.

6.5.1.1 For inter-domain communication, Manager implementations shall satisfy 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 6.5.

6.5.1.2 For inter-domain communication, 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 6.5.

6.5.1.3 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 12060-5, except as explicitly stated otherwise in 6.5.

6.5.1.4 In all cases where reference is made to a management function profile specified by a part of the multi-part standard ISO/IEC ISP 12060, the supporting communications profile for ATN Upper Layers (Session, Presentation, ACSE and CMISE/ROSE) shall be as specified in 6.4, rather than as defined in the referenced ISP.

6.5.1.5 Peer entity authentication at time of association establishment

6.5.1.5.1 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.

6.5.1.6 Systems Management functional unit negotiation

6.5.1.6.1 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.

6.5.1.7 Access Control

6.5.1.7.1 Implementations shall support appropriate access control to Management Information at the level of granularity of individual attributes.

Note 1.— An example of an appropriate access control profile is AOM 24322 as specified by ISO/IEC ISP 12060-9. This profile specifies a combination of OSI standards, which collectively provide capabilities to apply an Access Control List scheme to initiators attempting to access a specific set of targets. Access is granted or denied based on initiator identity and constraints applicable to the operations and the targets in the request.

Note 2.— Details of Access Control mechanisms to be applied are currently left as a local issue, to be determined by the Access Control Policy of an ATN Management Domain and agreed bilaterally with adjacent domain Managers.

6.6 CROSS-DOMAIN MANAGEMENT INFORMATION BASE (XMIB)

6.6.1 General Provisions

Editor's note.— The details of the format and content of the management information to be exchanged are not yet stable, and in any case are likely to evolve over time. The requirement is therefore for a flexible, general-purpose information structure and 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.

Editor's note.— The final version of Chapter 6.6 will specify the relevant MOs using the formal GDMO notation (ISO/IEC 10165-4) only. Tabular descriptions, including rationale, will be included in the SV6 Guidance Material.

Note.— ATN Management Information is defined by specifying:

a) the managed object class (MOC) definition of ATN MOs, using the formal notation specified in ISO/IEC 10165-4 Guidelines for the Definition of Managed Objects (GDMO);

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

6.6.1.1 **Recommendation**.— *All Managed Objects defined for use in ATN systems management, whether standardised or not, should 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).*

6.6.1.2 The cross-domain MIB shall support the capability to query the current operational status of the ATN systems (ES or IS) operated by other organisations, that directly provide an ATN ICS or application service to the local organisation (i.e. the failure of which would inevitably affect the provided service).

6.6.1.3 The cross-domain MIB shall support the capability to allow a Manager to be warned (via a notification) as soon as an error occurs in an adjacent domain that affects the ATN service provision.

6.6.1.4 The cross-domain MIB shall include the ISO/IEC 10165-2 **log** managed object class for the support of the standard ISO/IEC 10164-6 log control function across administrative boundaries.

6.6.1.5 The cross-domain MIB shall include the ISO/IEC 10165-2 **eventForwardingDiscriminator** managed object class for the support of the standard ISO/IEC 10164-5 event report management function across administrative boundaries.

6.6.2 Summary of requirements for cross-domain exchange of management information

6.6.2.1 Management Information available between ATN Management Domains shall include:

a) Subnetwork send, receive and error counts in Boundary Routers;

b) Routing Information Base /Forwarding Information Base (RIB/FIB) information in Boundary Routers.

6.6.2.2 The following Notifications shall be capable of being sent between ATN Management Domains, subject to discriminator settings:

a) CLNP ECHO Request Received Notification issued by the ATN ES or IS which was the target for the ERQ NPDU;

b) CLNP Error Report Received Notification issued by the ATN ES or IS which was the target for the Error NPDU.

c) CLNP ECHO Response Received Notification issued by the ATN ES or IS which was the target for the ERP NPDU.

6.6.2.3 ATN systems shall support the generation of a CLNP ECHO request as the result of a Systems Management action available between ATN Management Domains.

Note.— Analysis of Performance Management requirements has identified a potential requirement for the exchange of performance statistics between ISPs, on the overall service provided to ATN end users. However, the analysis assumed that this will be co-ordinated through industry forums. This is therefore perceived as an off-line requirement that will be satisfied by the exchange of periodic (e.g. monthly) reports on ISPs network performance. Hence, this requirement is assumed to have no consequence for the XMIB specification.

6.6.2.4 The SM agent on the aircraft shall maintain two managed objects, discriminator and eventForwardingDiscriminator as defined in ISO 10165-2, in order to filter out unnecessary information.

Note.— These two managed objects also determine the interval at which reports are sent to SM managers.

6.6.2.5 **Recommendation.—** *The discriminator should comply with the minimum mandatory ATN security alarm reports and audit trail reports.*

6.6.2.6 Information required for cross-domain management of the AMHS

6.6.2.6.1 The MOs contained in the XMIB in support of cross-domain management of AMHS Message Servers and Gateways shall be as follows:

a) AMHS Summary MTA (derived from standard),

b) AMHS Summary Adjacent MTA (derived from standard),

c) association (standard),

d) AMHS Gateway (specific),

e) MTCU (specific).

Note.— These MOs are, for one part, derived from the standard ISO/IEC 11588-8 MOs, and, for another part, specifically defined for the AMHS and the ATN.

6.6.3 Management Information Containment Structure

Editor's Note.— The management information structure is still the subject of active development. The suggested hierarchy presented here is based on the latest ATNP SM subgroup discussions. Pervious versions were based on the Customer Network Management concepts in ITU-T Recommendation X.162. This is no longer thought to be appropriate due to the peer to peer nature of ATN CDSM interactions..

6.6.3.1 Management Information Structure for General CDSM Services

Note 1.— Cross-domain management information is defined based on XMIB users' concerns and XMIB access providers' security. Information elements provided to XMIB users may be limited due to security reasons.

Note 2.— The XMIB MOs are defined as generic MO classes and they may be refined by adding specific features to extend services by each XMIB access provider.

Note 3.— Which MOs may be accessed by an XMIB user, and which conditional packages are offered, is based on agreements between the XMIB access provider and the user.

6.6.3.1.1 The XMIB containment tree for general CDSM Services shall be as illustrated in Figure 6.6-1, where shadowed boxes represent Managed Object Classes which can have multiple instances.

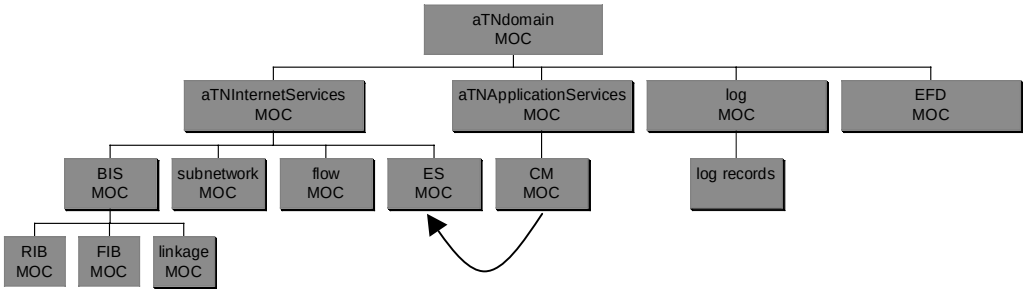

Figure 6.6-1. Naming hierarchy for General CDSM Services

6.6.3.2 Management Information Structure for AMHS Management

6.6.3.2.1 The XMIB containment tree for AMHS MO Classes shall be as illustrated in Figure 6.6-2, where shadowed boxes represent Managed Object Classes that can have multiple instances.

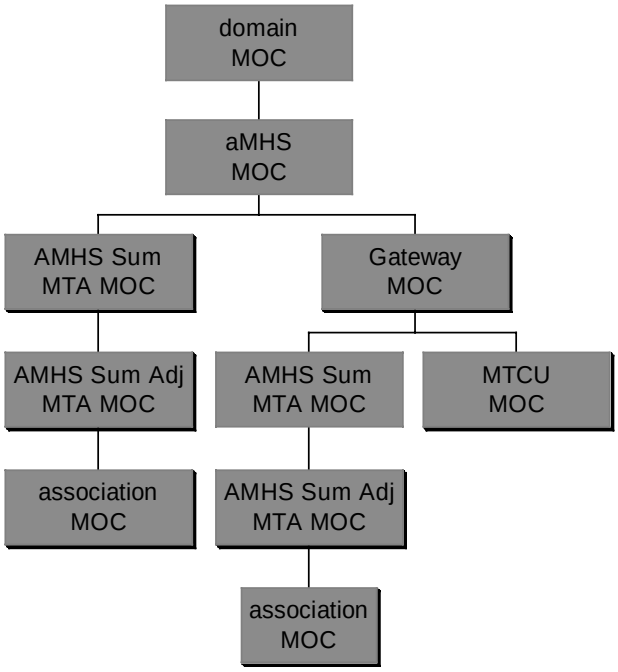

Figure 6.6-2. Naming hierarchy for AMHS Management Services

6.6.4 Managed Object Class Definitions

6.6.4.1 Referenced Managed Objects

6.6.4.1.1 The following “support” MO classes, for which the abstract syntax is specified in ISO/IEC 10165-2, shall be supported:

a) top,

b) log,

c) eventLogRecord

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.

6.6.4.1.2 System MO

Note.— This MO is exactly as defined in ISO/IEC 10165-2 (DMI). It is a superclass of the ATN-specific BIS and ES MO classes.

6.6.4.1.3 EventForwardingDiscriminator MO

Note.— This MO is exactly as defined in ISO/IEC 10165-2 (DMI). It is included in the ATN MIB by the invocation of the ISP for AOM 221.

6.6.4.1.4 Log MO

Note.— This MO is exactly as defined in ISO/IEC 10165-2 (DMI). It is included in the ATN MIB by the invocation of the ISP for AOM 231.

6.6.4.1.5 LogRecord MO

Note.— This MO is exactly as defined in ISO/IEC 10165-2 (DMI). It is included in the ATN MIB by the invocation of the ISP for AOM 231.

6.6.4.2 Defined Managed Objects

Editor's Note.— All of the MO definitions in this section will be updated in the next version of this document. For an example of the Work In Progress, refer to the GDMO definition of the BIS subtree in JSG-SM/WP14-07, by S. Tamalet.

6.6.4.2.1 The domain MO Class

6.6.4.2.1.1 The domain MO class shall be used to represent an entire ATN management domain.

6.6.4.2.1.2 At the top level of the containment hierarchy, a single instance of this MOC shall be used to identify the management domain itself.

6.6.4.2.1.3 Implementations of this MOC shall conform to the following formal definition:

aTNdomain MANAGED OBJECT CLASS

(to be defined)

6.6.4.2.2 The local MO Class

Editor's Note.— There may be no need for this MOC. It was intended to be a container for domain-wide parameters accessible to all external manager applications.

6.6.4.2.2.1 The local MO class shall be used as a container of all MOs representing the externally visible ATN systems in a domain, and aggregate management information offered by the local organisation.

6.6.4.2.2.2 Implementations of this MOC shall conform to the following formal definition:

aTNlocal MANAGED OBJECT CLASS

(to be defined)

6.6.4.2.3 The aTNsystems MO Class

Note.— This MOC is a container for those ESs and BISs that are visible to partner domains.

(To be defined)

6.6.4.2.4 The subnetwork MO Class

Note.— This MOC is a container for those ATN subnetworks that are visible to partner domains.

(To be defined)

6.6.4.2.5 The flow MO Class

Note.— This MOC is proposed to represent data flows through a domain, or starting or terminating within a domain. A data flow is a logical path between two ATN systems.

(To be defined)

6.6.4.2.6 The BIS MO Class

6.6.4.2.6.1 The BIS MO class shall be used to represent one Boundary Router of the local organisation.

6.6.4.2.6.2 The XMIB shall support multiple MO instances of this class.

6.6.4.2.6.3 Implementations of this MOC shall confirm to the following formal definition:
bIS MANAGED OBJECT CLASS

(to be defined)

6.6.4.2.7 The linkage MO Class

6.6.4.2.7.1 The linkage MO class shall be used to represent the attachment of the ATN system to a subnetwork.

6.6.4.2.7.2 The XMIB shall support multiple MO instances of this class.

6.6.4.2.7.3 Implementations of this MOC shall conform to the following formal definition:
linkage MANAGED OBJECT CLASS

(to be defined)

6.6.4.2.8 The rIB MO Class

6.6.4.2.8.1 The rIB MO class shall be used to represent the Routing Information Base (RIB) of a Boundary Router, frozen at an instant in time.

6.6.4.2.8.2 Implementations of this MOC shall conform to the following formal definition:
rIB MANAGED OBJECT CLASS

(to be defined)

6.6.4.2.9 The fIB MO Class

6.6.4.2.9.1 The fIB MO class shall be used to represent the Forwarding Information Base (FIB) of a Boundary Router, frozen at an instant in time.

6.6.4.2.9.2 Implementations of this MOC shall conform to the following formal definition:
fIB MANAGED OBJECT CLASS

(to be defined)

6.6.4.2.10 The eS MO Class

6.6.4.2.10.1 The eS MO class shall be used to represent one ATN End System of the local organisation.

6.6.4.2.10.2 The XMIB shall support multiple MO instances of this class.

6.6.4.2.10.3 Implementations of this MOC shall conform to the following formal definition:
eS MANAGED OBJECT CLASS

(to be defined)

6.6.4.2.11 The CM MO Class

Note.— There may be a cross-domain requirement to communicate CM addresses (not air-ground). The cM MOC supports this requirement.

(To be defined)

6.6.4.2.12 The gateway MO Class

6.6.4.2.12.1 The gateway MO Class shall be used to represent one (AFTN or CIDIN) AMHS Gateway; within an XMIB local MO there may be multiple MO instances of this class.

Editor's Note.— To be defined. Possible attributes of this class are:

a) Administrative State,

b) Operational State,

c) more generally the attributes and packages specified in M.3100 for state change notification,

d) the number of MTCUs included in the Gateway,

e) the "covered areas" to which the gateway provides connectivity (tbc).

6.6.4.2.13 The mTCU MO Class

6.6.4.2.13.1 The mTCU MO Class shall be used to represent the AFTN and/or CIDIN MTCUs of an AMHS Gateway; within an XMIB Gateway MO there may be multiple MO instances of this class.
Editor's Note.— To be defined. Possible attributes of this class are:

a) the MTCU type (Basic AFTN/AMHS MTCU, Extended AFTN/AMHS MTCU, CIDIN/AMHS MTCU with different MCFs),

b) the maximum convertible message size,

c) the maximum convertible recipient number,

d) the supported character sets,

e) Administrative State,

f) Operational State,

g) more generally the attributes and packages specified in M.3100 for state change notification.

6.6.4.2.14 The aMHSSumAdjMTA MOC

6.6.4.2.14.1 The aMHSSumAdjMTA MO Class shall be used to represent the MTAs adjacent to the MTA represented by the higher level instance of aMHSSumMTA MO. Within that portion of the tree, multiple MO instances of this class under one aMHSSumMTA MO instance shall be supported.

6.6.4.2.14.2 Implementations of this MOC shall conform to the following formal definition:

aMHSSumAdjMTA MANAGED OBJECT CLASS

DERIVED FROM (***tbd***);

CHARACTERISED BY

aMHSSumAdjMTAPackage,

"Rec. M.3100":createDeleteNotificationsPackage,

"Rec. M.3100":stateChangeNotificationPackage,

"Rec. M.3100":attributeValueChangeNotificationPackage;

CONDITIONAL PACKAGES

dirServiceReferencePackage PRESENT IF “Directory is used for MHS and an mhs-message-transfer-agent directory object instance is present for the adjacent MTA”;

REGISTERED AS **{ *tbd*};**

-- (derived from reference ISO/IEC 11588-8 Section 9.1)

6.6.4.2.15 The association MOC

6.6.4.2.15.1 The association MO Class shall be used to represent the associations between an adjacent MTA and the MTA represented by the higher level instance of aMHSSumMTA MO. Within that portion of the tree, multiple association MO instances of this class under one aMHSSumAdjMTA MO instance shall be supported.

6.6.4.2.15.2 Implementations of this MOC shall conform to the following formal definition:

association MANAGED OBJECT CLASS

DERIVED FROM “Rec. X.721 | ISO/IEC 10165-2”:top;

CHARACTERISED BY

associationPackage,

“Rec. M.3100”:createDeleteNotificationsPackage,

“Rec. M.3100”:stateChangeNotificationPackage;

CONDITIONAL PACKAGES

simpleCredentialsPackage PRESENT IF “Simple credentials are used for the current association”;

REGISTERED AS { MhsMgntMTAObjectIdentifiers.id-moc-association};

-- (in compliance with ISO/IEC 11588-8 Section 9.2)

6.6.4.2.16 The aMHSSumMTA MOC

6.6.4.2.16.1 Implementations of this MOC shall conform to the following formal definition:

aMHSSumMTA MANAGED OBJECT CLASS

DERIVED FROM (***tbd)***;

CHARACTERISED BY

aMHSSumMTAPackage,

“Rec. M.3100”:createDeleteNotificationsPackage,

“Rec. M.3100”:administrativeOperationalStatesPackage,

“Rec. M.3100”:stateChangeNotificationPackage,

“Rec. M.3100”:equipmentsEquipmentAlarmPackage;

CONDITIONAL PACKAGES

dirServiceReferencePackage PRESENT IF “Directory is used for MHS and an mhs-message-transfer-agent directory object instance is present for the adjacent MTA”;

REGISTERED AS { ***tbd***};

-- (derived from reference ISO/IEC 11588-8 Section 9.7)

6.6.5 GDMO Package Definitions

aMHSSumAdjMTAPackage PACKAGE

BEHAVIOUR aMHSSumAdjMTABehaviour,

creationAndDeletionNotificationBehaviour,

administrativeStateChangeNotificationBehaviour,

attributeValueChangeNotificationBehaviour;

ATTRIBUTES

"Rec X.721 | ISO/IEC 10165-2":administrativeStateGET,

adjMTAAccessPointAddressGET,

adjMTAGlobalDomainIdGET,

adjMTAMaxMessageSizeGET,

adjMtaName GET,

adjMTASupportedApplicationContextsGET,

localMTAMaxMessageSizeGET,

waitTimeToRelease GET;

REGISTERED AS { ***tbd***};

aMHSSumAdjMTABehaviour BEHAVIOUR

DEFINED AS

"The aMHSSumAdjMTA Managed Object Class describes the summary information related to the establishment of associations and to the exchange of MPR between the managed MTA and an adjacent MTA. For each adjacent MTA of the managed MTA, an instance of this class shall be created. An aMHSSumAdjMTA object instance is named by the adjMtaName attribute.";

creationAndDeletionNotificationBehaviour BEHAVIOUR

DEFINED AS

"An object creation or object deletion notification shall be generated at the creation and deletion of the object instance.";

administrativeStateChangeNotificationBehaviour BEHAVIOUR

DEFINED AS

"A state change notification is emitted when the administrative state attribute changes in value.";

attributeValueChangeNotificationBehaviour BEHAVIOUR

DEFINED AS

"An attribute change notification is emitted when any of the attributes change in value.";

-- (derived from reference ISO/IEC 11588-8 Section 10.1)

associationPackage PACKAGE

BEHAVIOUR associationBehaviour,

associationCreationDeletionBehaviour,

creationAndDeletionNotificationBehaviour,

operationalStateChangeNotificationBehaviour,

usageStateChangeNotificationBehaviour;

ATTRIBUTES

"Rec X.721 | ISO/IEC 10165-2":operationalStateGET,

“Rec X.721 | ISO/IEC 10165-2”:usageStateGET,
applicationContext GET,
associationInitiator GET,
associationObjectInstanceIdGET,
creationTime GET,
initiatorAccessPointAddressGET,
responderAccessPointAddressGET;
REGISTERED AS { MhsMgntMTAObjectIdentifiers.id-package-associationPackage};

associationBehaviour BEHAVIOUR
DEFINED AS
“The association managed object maintains dynamic information on an association established with the managed MTA. As several associations can be established at the same time between the managed MTA and an MtsUser, several association object instance can exist at the same time. An association object instance is named by the associationObjectInstanceId attribute.”;

associationCreationDeletionNotificationBehaviour BEHAVIOUR
DEFINED AS
“An association object instance is created each time an association is established with the managed MTA. An association object instance may also be created for a rejected attempt to establish an association. An association object instance need not to be deleted when the corresponding association is released.

The operational state attribute is set to enable if the association request was accepted. The operational state attribute is set to disable if the association request was rejected.

The usage state attribute is set to active at the creation of an association object instance. The usage state attribute is set to idle when the association is normally released.

The usage state attribute is set to idle and the operational state attribute is set to disable when the association is abnormally released.”;

operationalStateChangeNotificationBehaviour BEHAVIOUR
DEFINED AS
“A state change notification is emitted when the operational state attribute changes in value.”;

usageStateChangeNotificationBehaviour BEHAVIOUR
DEFINED AS
“A state change notification is emitted when the usage state attribute changes in value.”;
-- (identical to reference ISO/IEC 11588-8 Section 10.2)

aMHSSumMTAPackage PACKAGE
BEHAVIOUR aMHSSumMTABehaviour,
creationAndDeletionNotificationBehaviour,
operationalStateChangeNotificationBehaviour,
usageStateChangeNotificationBehaviour,

equipmentsEquipmentAlarmBehaviour;

ATTRIBUTES

defaultNonUrgentMprExpiryDurationGET,

defaultNormalMprExpiryDurationGET,

defaultUrgentMprExpiryDurationGET,

globalDomainId GET,

maxAdjMTAInboundAssocsGET,

maxAdjMTAOutboundAssocsGET,

mtaName GET,

supportedApplicationContextsGET;

REGISTERED AS { ***tbd*** };

aMHSSumMTABehaviour BEHAVIOUR

DEFINED AS

"The AMHSSumMTA Managed Object Class describes summary MTA management information in order to provide the cross-domain management of the MTA a view on the MTA overall capability and availability. This information is not changed except under specific management actions of the MHS system manager in charge of local management of the managed MTA (i.e. different from the cross-domain system manager). One instance of this object class shall be created for each monitored MTA. The AMHSSumMTA Managed Object Class is inherited from the Managed Object Class equipment which is defined in Rec. M.3100 (*tbc*). The following packages of the equipment object class shall be provided:

- createDeleteNotificationPackage
- stateChangeNotificationPackage
- administrativeOperationalStatePackage
- equipmentsEquipmentAlarmPackage

The equipmentId attribute is used to name an aMHSSumMTA object instance.";

equipmentsEquipmentAlarmBehaviour BEHAVIOUR

DEFINED AS

"A processing error alarm notification shall be emitted when the entity experiences any of the processing alarms conditions defined in Rec. X.733 | ISO/IEC 10164-4 (e.g. storage capacity problem, version mismatch, corrupt data, software error, underlying resources unavailable.";

-- (reference ISO/IEC 11588-8 Section 10.12)

6.7 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. **Resolution**: Only the cross-domain MIB will be in SARPs.

2. 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. Provisions for encoding MO attributes in PER also need to be considered. Potentially all MOs need to be augmented with PER-visible constraints and extensibility markers.

3. Does there need to be a separate containment tree per class of Router? **Resolution**: No longer relevant to the cross-domain MIB.

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

5. 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. What countermeasures should be specified if performance falls below acceptable thresholds? (e.g. switch off AOC if ATSC performance degrades).

7. It is a requirement that instances of the Cross-Domain MIB in different systems have similar accuracy and timeliness, therefore they must be updated consistently. This cannot be left as a local issue. "Virtual MOCs" (like OSIMIS – see P Tupitza WP in Rio) may be a possible approach to this. This is a service level agreement issue, to be raised with WG1.

8. The XMIB concepts need to be stabilised, and MOs defined.

9. In 6.2, values need to be assigned to Name Bindings.

10. All MOs need to be specified using GDMO notation.

11. Access control is left as a local policy issue, requiring bilateral agreements between domains.

12. The use of the D-START security parameter is for further study.