APPENDIX C

ATN SYSTEMS MANAGEMENT CONCEPT OF OPERATIONS
Version 2.0

ENGLISH ONLY

Page left intentionally blank

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose and Scope

1.1.1 The purpose of this document is to provide a basic understanding of how systems management will be needed in the distributed ATN environment.

1.1.2 This document describes the overall ATN systems management concepts.

1.2 Structure of the Document

1.2.1 The CONOPs is divided into sections. Section 2 presents a high-level overview of ATN Systems Management; section 3 defines the ATN environment for Systems Management including the description of terms used; section 4 presents the concept of systems management operations; section 5 describes the systems management co-ordination needed across ATN administrative boundaries; and Section 6 provides guidelines for the coexistence of the ATN Systems Management mechanisms with other Systems Management mechanisms potentially used within an ATN administrative management domain.

2. OVERVIEW OF ATN SYSTEMS MANAGEMENT

2.1 Systems Management provides mechanisms to monitor, control and co-ordinate communications, applications, and other (as required) resources with the goal of achieving a seamless communications service in support of real world air traffic operations. To achieve this goal, it is required that specific management information, functions and protocols be designed and built into any supporting communications network to provide deterministic and controllable network behaviour.

2.2 Systems Management is needed to provide deterministic and controllable behaviour in support of required service levels as the communications infrastructure evolves from simple point to point technology towards increasingly complex inter-networks used for program to program application services.

2.3 Systems Management may be distributed, centralized or local and can be achieved by a variety of mechanisms. The total systems management solution will involve a combination of the following approaches:

a) the appropriate design of the communications infrastructure and components to anticipate and provide sufficient capacity;

b) the implementation of local automated or operator controlled management functions in communications systems; and

c) the implementation of management functions in ATN systems that allow the exchange of systems management information based on a standardized systems management model and using a standardized protocol or method (e.g. using CMIP/CMIS from the

OSI world, SNMP from the TCP/IP world, file transfer mechanisms, messaging services etc.).

2.4 The real word situation is complex and will require a practical solution comprised of many building blocks organized into a coherent whole.

3. ATN ENVIRONMENT

3.1 Introduction

3.1.1 The ATN, as defined by ICAO, consists of a set of computer applications that exchange ATM-related information. This information is ultimately used by humans in support of air traffic control and airline operations. To support those applications, the ATN comprises a set of supporting communication services that create an internetwork. The internetwork is supported by communication sub-networks that have been standardized by ICAO.

3.1.2 The ATN is designed to consist of a (potentially large) set of autonomously owned, operated, and administered networks that are interconnected to form an internet. The networks are either directly interconnected or connected through a backbone arrangement.

3.1.3 The remainder of this section describes how the owners and operators of ATN equipment are organized from the perspective of administration and management.

3.2 Definitions

3.2.1 The following sub-sections provide definitions of terms used within this document. For clarity, the terms are not presented in alphabetical order but in a conceptual order.

3.2.2 Domains

3.2.2.1 A *Domain* is a generic term that is used to define a set of resources under the control of a single entity.

3.2.2.2 A <*name*> *Domain* defines the particular set of resources characterized by the value of <*name*>.For example, administrative domain, management domain, address domain.

3.2.3 ATN Organizations

3.2.3.1 What distinguishes an organization as an ATN organization is that it administratively controls a set of ATN resources. For example, an organization that controls the assignment of NSAP addresses for a portion of the ATN can be considered an ATN organization. ATN organizations consist of, for example, CAAs, IATA aircraft operating agencies, or ATN service providers.

3.2.3.2 To facilitate the discussion of the management of the ATN, the concept of *Domain* is introduced.

3.2.4 Administrative and Regional Domains

3.2.4.1 The owner and/or operator of an ATN network is defined by the term *Administrative Domain*. An *Administrative Domain* is the set of resources under the administrative control of a single authority.

3.2.4.2 In some instances, a group of Administrative Domains, e.g., all the CAAs within an ICAO Region, may join together into a *Regional Domain*.

3.2.5 Administrative and Regional Management Domains

3.2.5.1 ATN management may be primarily described in terms of the management information available and the use of that information by some organization. This leads to the definition of a management domain hierarchy that is used to classify information exchange requirements and associated responsibilities.

3.2.5.2 The hierarchy is defined so that the "lowest" level represents the most detailed information and typically represents the smallest organization.

3.2.5.3 The lowest level of the hierarchy is the Local Management Domain. This consists of the management of a portion of an Administrative Domain. Examples of a Local Management Domain are: a LAN, a portion of a CAA's ATN environment, or a portion of an airline's ATN environment. A Local Management Domain is entirely contained in a single Administrative Management Domain.

3.2.5.4 The next level of the hierarchy is the *Administrative Management Domain*. This consists of the management of an entire Administrative Domain. The Administrative Management Domain is the central building block for ATN Systems Management. It is within this domain that management information is gathered, reduced, and analysed to determine the operational state of that portion of the ATN. Most importantly, this is the central source of management information shared with other domains.

3.2.5.5 For the efficient management of the ATN, the operators of groups of Administrative Management Domains may agree to consolidate some aspects of management thereby forming a *Regional Management Domain*.

3.2.5.6 An Administrative Management Domain may be contained in one or more Regional Management Domains.

3.3 Large Scale Structure of the ATN

3.3.1 There are many possible ways for the ATN to be globally implemented. Figure 3.3-1 illustrates one possible large-scale structure of an example subset of the ATN environment that can be used for discussion purposes.

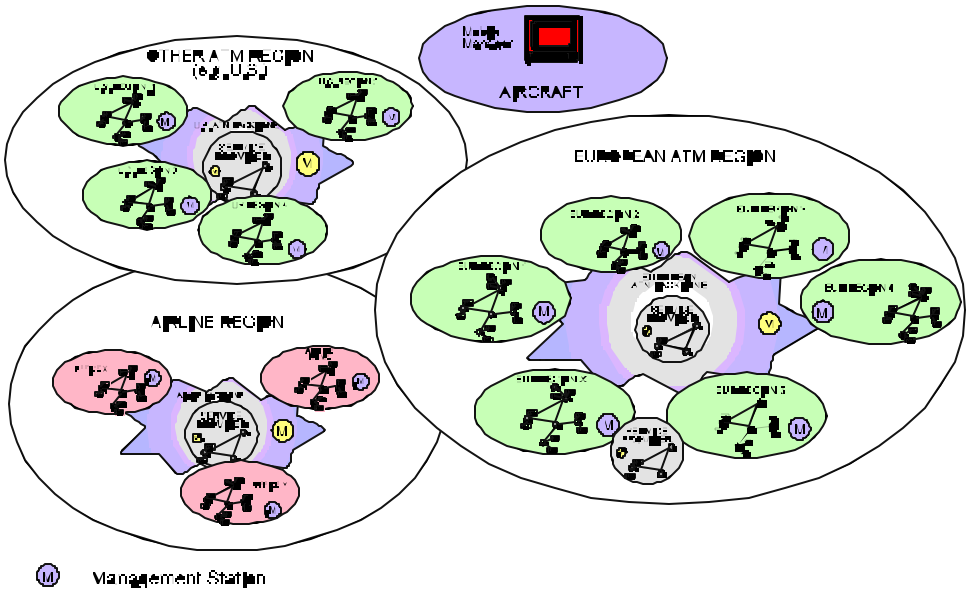

Figure 3.3-1. Large Scale ATN Structure

3.3.2 The large scale structure of the ATN will consist of the following:

a) administrative (CAA, airline, aircraft, and service provider) management domains; and

b) regional (CAA, airline, and service provider) management domains.

Note.— Aircraft are considered in a manner indistinguishable from any other administrative management domain.

3.3.3 Each domain is a logically separate network that is expected to exchange management information and traffic with other domains according to policy.

3.3.4 On the ground, within each regional management domain are 2 basic kinds of ATN administrative management domain, end users (e.g. CAAs or Airlines) and ATN communication (network) providers (i.e., the ATN backbone) which provides connectivity between end users.

3.3.5 The backbone may consist of a combination of nationally owned facilities and commercially owned facilities (service providers).

3.4 The Structure of Managers, Administrators and Institutions

3.4.1 There are several different structures of Managers, Administrators, and Institutions as they apply to managing the global ATN.

3.4.2 A possible end-state structure is represented in Figure 3.4-1 and described in the following sections.

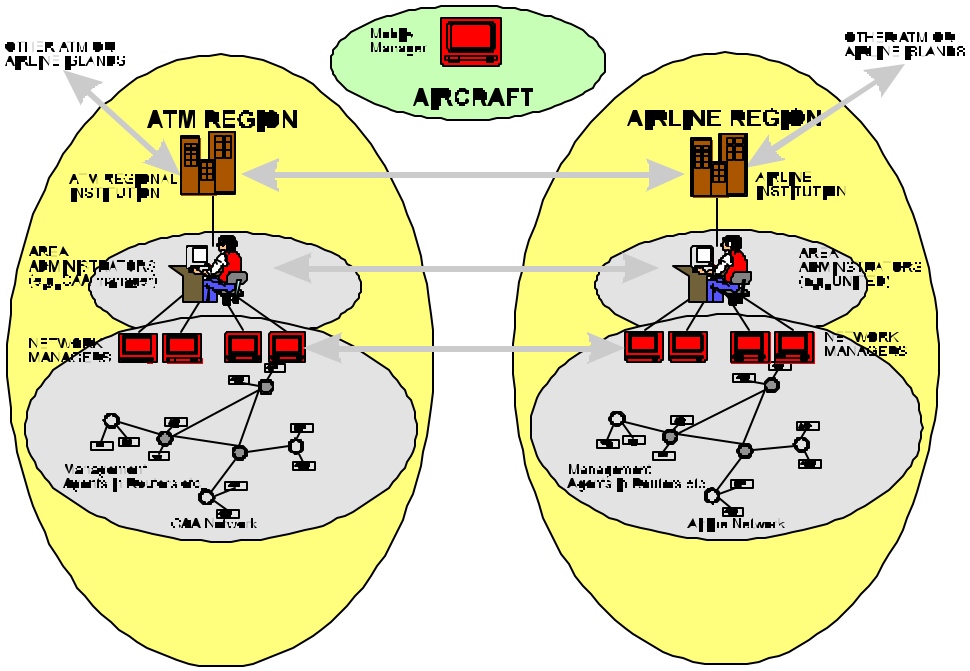

Figure 3.4-1. Structure of ATN Authorities

3.4.3 **Management on the Ground**

3.4.3.1 ***Regional***

3.4.3.1.1 As defined earlier a Regional Management Domain consists of a set of Administrative Management Domains that have agreed to consolidate its management functions into a single domain (The establishment of a regional management domain does not invalidate the existence of the component administrative management domains).

3.4.3.1.2 Every Regional Management Domain will have a single Regional Institution which has ultimate responsibility for the operation of the Region. These Institutions may delegate, by agreement, responsibility for actual administration to managers at their disposal (e.g. those in the CAA domains of responsibility).

Note.— The above does not imply that Regional Institutions are managers of a further hierarchy of managers.

3.4.3.1.3 Regional Institutions are the responsible authority for:

C Establishing contracts, agreements and polices regarding the structure, integrity and internal administration of the Region as a whole. This will involve co-ordinating

communication policies participants that form the Region (e.g., between CAA(s), Airlines and Service Provider(s).

- Negotiating policies for communicating with other Regions external to itself.

3.4.3.1.4 These agreements and policies will not be implemented or checked automatically by managers, responsibility for their active implementation is passed to the Area Administrators.

3.4.3.1.5 Regional institutions may provide support facilities to enable the implementation of agreements and policies (e.g. provide an address registration and allocation database accessible to administrators).

3.4.3.2 ***Administrative Management Domains***

3.4.3.2.1 Every Administrative Management Domain will have a two level hierarchy of active managers, Area Administrators and Network Managers which operate according to contracts, agreements and policies made by Management Domains.

3.4.3.2.2 **Area Administrators**

3.4.3.2.2.1 An area consists of a subset of either an administrative or regional management domain.

3.4.3.2.2.2 For those management domains that choose to define areas, every area will have an Administrator which has responsibility for its own area. These Managers may use subordinate managers/agents at their disposal (e.g. managers of networks) involving the collection and organization of data concerning operations of the network.

3.4.3.2.2.3 The Administrator who operates a management station will for example:

- administer costs;
- present performance assessment;
- take action in response to the analysis of data, events and fault reports collected from the network;
- take action to enforce agreements and policy statements made by the appropriate management domain;
- be responsible for address administration (including establishing and maintaining the routing structure of the network);
- administer and maintain Quality of Service (QoS), secure interaction and other policies common to domains; and
- switch Service Providers according to operational circumstances (fault reports etc.).

Note.— An agreement with service providers may oblige them to "present" accessible summary information on their services.

- present an overall picture of network operational status in centres; and

- implement access control between administrators in different areas.

Note.— When organizations exchange management information, specific administrative managed objects presenting a limited "view" of an organization may provide a sufficient means for access control.

3.4.3.2.3 **Network Managers**

3.4.3.2.3.1 Within some management domains, the operators may delegate responsibility for detailed management to others based on the component networks.

3.4.3.2.3.2 Every network will have a Network Manager which has responsibility for the detailed operation of the equipment in the network.

3.4.3.2.3.3 The Network Manager has access to the many pieces of distributed physical equipment. It collects data and administers the Management Information Base for groups of Host Computers, Routers and Subnetwork Components via "Management Agents" resident in those systems.

3.4.3.2.3.4 Network Managers relieve Administrators of the need to consider the details of the normal operation of network equipment.

3.4.3.2.3.5 Distributed systems management of ATN equipment within organizations will be required. It will obviously be impractical to have operations staff manning each piece of ATN equipment, operating it from a local interface. It would also be infeasible to guarantee equipment configuration and operation without such facilities.

Note.— The implementation of standard management solutions in ATN equipment may be required by regional certification authorities (and will help manufacturers develop and sell standard certified equipment in the world-wide ATN market).

Note.— The Administrator and Network Manager are defined above in functional terms. It is possible that these functions could be co-located in a single management station, this will depend on local design issues (e.g. physical topology, network size and complexity).

3.4.3.3 ***Regional Systems Management co-ordination models***

3.4.3.3.1 Within a Regional Management Domain, the systems management activities of the multiple component Administrative Management Domains must be co-ordinated on various aspects so as to ensure the overall availability, quality and performance of the ATN service in the Region.

3.4.3.3.2 The way the multiple component Administrative Management Domains collaborate to form the Regional Management domain depends on the model upon which the regional coordination is organized.

3.4.3.3.3 Regional coordination can be organized upon one of the three following models:

a) Distributed:

The principle of the distributed coordination model is to form global management coordination via the chain of bilateral service level agreements between pairs of Administrative Management Domains. Each pair of organizations engaged in communication exchanges establishes a Service Level Agreement between them and explicitly states their expectation for the common endeavour. The agreement is enforced by both organizations. In such a distributed environment, each Administrative Management Domain is responsible for the coordination of systems management issues with its partner Administrative Management Domains; the management of the regional ATN relies on individual organizations;

b) Centralized with a central management centre:

This organizational modelis based on the centralization of the systems management coordination activities, with the creation of a central body responsible for the overall coordination of the cross domain systems management activities in the region. The central body is logically separated from the Administrative Management Domains; and

c) Centralized with a co-ordinator organization:

In this model, one of the Administrative Management Domains is elected as responsible for the overall coordination of the cross domain systems management activities in the region

3.4.3.3.4 The Figure 3.4-2 illustrates these different organizational models

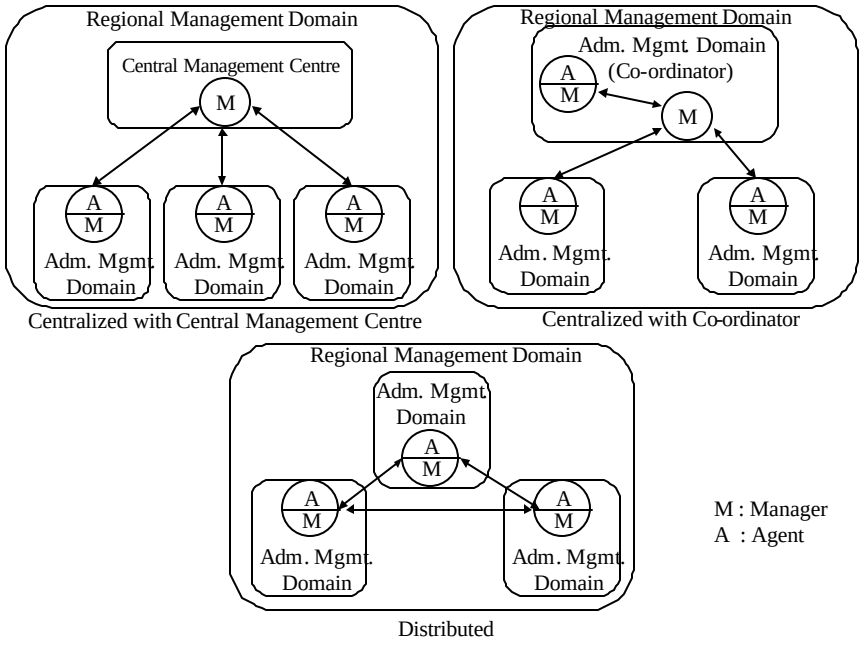

Figure 3.4-2. Organizational models for regional coordination

3.4.4 **Management of airborne systems**

3.4.4.1 Each aircraft has its own administrative management domain based upon its need to manage the ATN end-systems and communication facilities.

3.4.4.2 It is assumed that Systems Management traffic will flow over the air-ground link, if not in the short term then at some time in the future. The exchange of management information over the air-ground link is subject to the same procedures as for the exchange on the ground.

3.4.4.3 The ATN Systems Management procedures must therefore not preclude air-ground Systems Management traffic; a flexible, extensible ATN Systems Management architecture is needed, as it is not possible to predict all future Systems Management scenarios.

3.4.4.4 Every aircraft will have an airborne manager with responsibility for the detailed operation of the ATN equipment on board.

Note.— The concept of airborne manager is an ultimate concept. In the initial ATN operation, Airlines may only implement an agent for their own purpose or may not implement any on board systems management application.

3.4.4.5 In the flight deck environment, mobile managers will need to be autonomous applications requiring a minimal level of human intervention. There are particular requirements that initial avionics systems not to be adversely affected by ATN Systems Management operations.

3.4.4.6 Airborne systems may be managed by Airline Managers from the ground. The Airline Manager may provide ATC managers with data concerning the aircraft by ground-ground data exchanges. Systems Management exchanges between ATC authorities and Airborne systems may consist of event reports initiated by the Aircraft. Ground-based managers may also request specific data from airborne managers. Airborne systems may need to access ground-based management information. Operational parameters to be used in flight may be uploaded at the gate for use by mobile managers. Summaries of flight operation (e.g. engine performance) collected by mobile managers or other operational systems may be downloaded at the gate for analysis by Airline ground based managers.

3.4.4.7 Any defined mechanisms for real-time operational fault and event reporting to ATC authorities over the air-ground link must be standardized (e.g. as ATN application exchanges or as Systems Management application exchanges using specifically designed protocols (e.g. CMIP)). The reports themselves must also be standardized.

4. ATN SYSTEMS MANAGEMENT CONCEPT OF OPERATION

4.1 System Management Overview

4.1.1 The basic management configuration has a managing system that communicates with a managed system in order to manage a resource that is contained in or controlled by the managed system. On managing systems (or management stations), reside applications called “managers”. On managed systems (or network elements being managed), reside applications called “agents”. The terms “manager” and “agent” are also used in a loose and popular sense to refer to the managing and managed system, respectively.

4.1.2 Figure 4.1-1 depicts the relationship between a management station, the management application(s), agents and the managed resources.

4.1.3 Network management occurs when managers and agents cooperate (via protocols and a shared conceptual schema) to exchange monitoring and control information useful to the management of a network and its components.

4.1.4 The shared conceptual schema mentioned above is a priori knowledge about "managed objects" concerning which information is exchanged. Managed objects are abstractions of system and networking resources (e.g., a modem, a protocol entity, a routing table, a transport connection) that are subject to management. Management activities are effected through the manipulation of managed objects in the managed systems. Using the management services and protocol, the manager can direct the agent to perform an operation on a managed object for which it is responsible. Such operations might be to return certain values associated with a managed object (read a variable), or perform an action (such as self-test) on the managed object. In addition, the agent may also forward notifications generated asynchronously by managed objects to the manager.

4.1.5 The terms "manager" and "agent" are used to denote the asymmetric relationship between management application processes in which the manager plays the superior role and the agent plays the

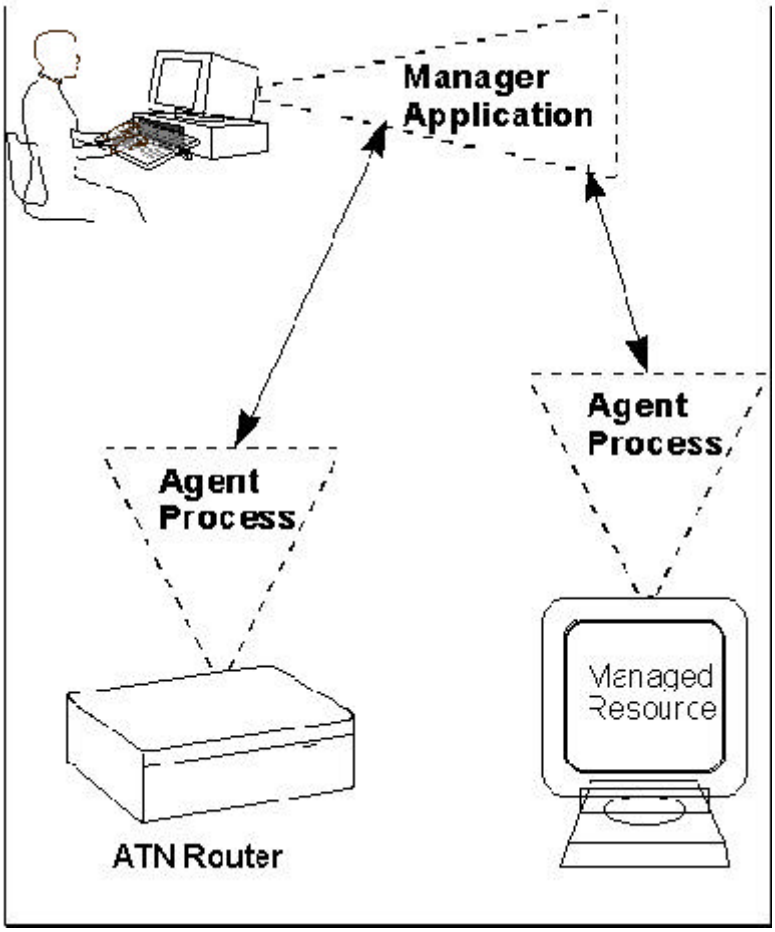

Figure 4.1-1. Primary elements of the Systems Management Model

subordinate.

4.1.6 Figure 4.1-2 presents a systems management scenario. Achieving an integrated systems management, the ATN applications, as well as many other aviation systems stand to benefit from an integrated network and systems management approach. As a general example, consider the fact that a significant amount of data is collected which relates to the operational status and maintenance of various ATN components on aircraft. Collecting this data by using integrated network and systems management provides the opportunity for immediate correlation of the data, thereby improving efficiency and enhancing fault and performance management capabilities.

4.2 Introduction to OSI System Management

4.2.1 ATNP has the task of defining a model for network and systems management that provides a common world view of the ATN network. The ISO standards for open system interconnection (OSI) have been officially adopted by the ATNP to facilitate the interoperability of ATN systems and systems management. The OSI model for the definition of network management is an object-oriented model. This is a departure from the standards developed for other areas of the communication standard. This follows the needs of today's systems to perform remote configuration of network elements, assess and optimize the performance of other elements, and offer intelligent reasoning capabilities for diagnosing network faults.

4.2.2 The OSI Management Framework

4.2.2.1 The OSI Management architecture provides a means by which control and monitoring information can be exchanged between a "manager" and a remote network element.

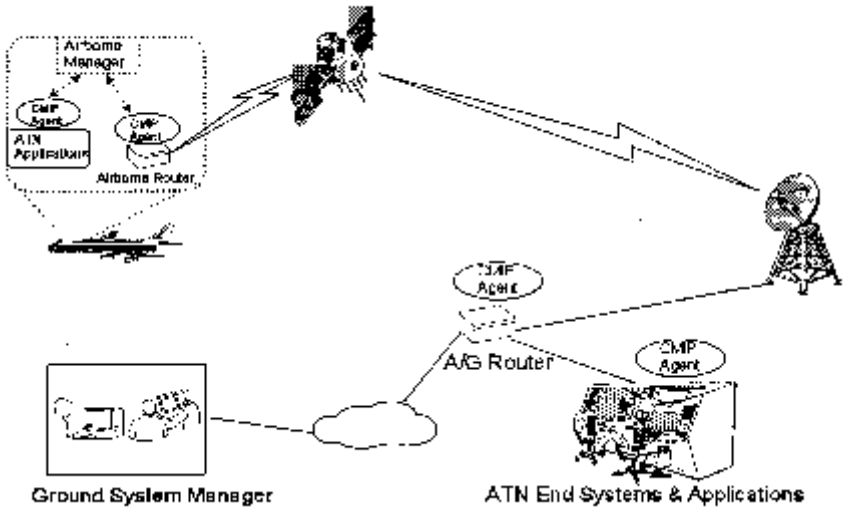

Figure 4.1-2. Integrated Systems Management Scenario

4.2.2.2 This architecture is defined in two documents:

- ISO/IEC 10040 (X.701) Systems Management Overview (SMO); and
- ISO/IEC 7498-4 (X.700) Management Framework for OSI.

4.2.3 **Overview of OSI System Management Architecture**

4.2.3.1 Three models are typically used to describe OSI information management. An organizational model describes ways in which management can be administratively distributed. The functional model describes the management functions and their relationships. The information model provides guidelines for describing managed objects and their associated management information.

4.2.3.2 OSI Management specifies a set of management services, defined in Common Management Information Service Definition (CMIS [ITU-T X.710].These services are provided by a network management protocol, defined in the standard Common Management Information Protocol (CMIP [ITU-T X.711]).OSI provides CMIP/CMIS as a consistent method to access the information stored by the management models about the network devices and system communications.

4.2.3.3 ***The Organizational Model***

4.2.3.3.1 The organizational model introduces the concept of a management “domain”. A domain is an administrative partition of a network or internet for the purpose of network management. Domains may be useful for reasons of scale, security, or administrative autonomy. Each domain may have one or more managers monitoring and controlling agents in that domain.In addition, both managers and agents may belong to more than one management domain. Domains allow the construction of both strict hierarchical and fully cooperative and distributed network management systems.

4.2.3.4 ***The Functional Model***

4.2.3.4.1 The OSI Management Framework defines five facilities or functional areas to meet specific management needs. This has proved to be a helpful way of partitioning the network management problem from an application point of view. These facilities have come to be known as the Specific Management Functional Areas (SMFAs): fault management, configuration management, performance management, accounting management, and security management.

4.2.3.4.2 Fault management provides the ability to detect, isolate, and correct network problems.

4.2.3.4.3 Configuration management enables network managers to change the configuration of remote network elements.

4.2.3.4.4 Performance management provides the facilities to monitor and evaluate the performance of the network.

4.2.3.4.5 Accounting management makes it possible to monitor users for use of network resources and to limit the use of those resources.

4.2.3.4.6 Finally, security management is concerned with managing access control, authentication, encryption, and so on.

4.2.3.5 ***The Information Model***

4.2.3.5.1 The OSI Management Framework considers all information relevant to network management to reside in a Management Information Base (MIB),which is a "conceptual repository of management information".

4.2.3.5.2 Information within a system that can be referenced by the management protocol is considered to be part of the MIB. Conventions for describing and uniquely identifying the MIB information allow specific MIB information to be referenced and operated on by the management protocol. These conventions are called the Structure of Management Information (SMI).

4.2.3.5.3 The information model is described more fully in section 4.2.5.

4.2.4 **Management Protocol and Service**

4.2.4.1 OSI has defined the 'Common Management Information Service (CMIS) as the preferred service for the exchange of management information (although the use of other exchange services, for instance a file transfer service, is still allowed). CMIS' role is restricted to the transfer of management information; actual control of systems is left to the Management Information Service (MIS) users which are located on top of CMIS (see Figure 4.2-1).

4.2.4.2 CMIS provides both confirmed and unconfirmed services for reporting events and retrieving and manipulating management data. These services are used by manager and agent application entities to exchange management information.

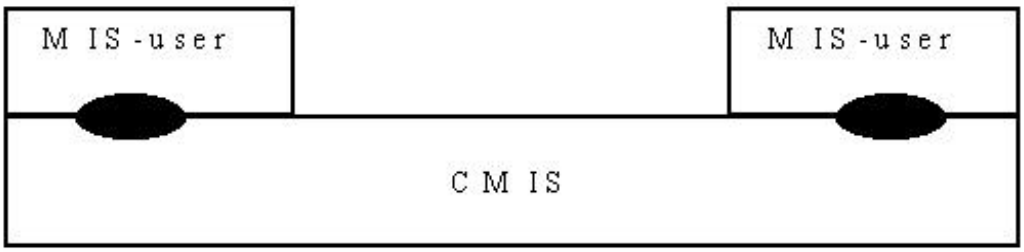

Figure 4.2-2. MIS-users on top of CMIS

4.2.4.3 The different service primitives provided by CMIS are listed below:

M-GET:	To retrieve management information from a remote MIS-user;
M-CANCEL-GET:	To cancel a previously invoked M-GET. It is helpful in those case where the M-GET delivers too much information;
M-SET:	To modify the attributes of a Managed Object;
M-ACTION:	To perform some action on a Managed Object;
M-CREATE:	To create a new instance of a Managed Object;
M-DELETE	To delete an existing instance of a Managed Object; and
M - E V E N T - REPORT:	To report the occurrence of some kind of event.

4.2.4.4 CMIS is provided by the Common Management Information Service Element (CMISE). The interaction between CMISE entities is defined by the 'Common Management Information Protocol' (CMIP).

4.2.5 **The Structure of Management Information**

4.2.5.1 Management information is defined by the OSI "Structure of Management Information' (SMI).It is a standard management object model, which has three parts. The Management Information Model [ITU-T X.720] defines the modeling concepts underlying the OSI SMI. The Definition of Management Information (DMI [ITU-T X.721]) defines basic management objects commonly used in an OSI MIB; and the Guidelines for the Definition of Managed Objects (GDMO) [ITU-T X.722] defines a special-purpose notation using its own templates.The OSI SMI uses object-oriented structuring principles for defining its managed objects.

4.2.5.2 ***Object Oriented Principles***

4.2.5.2.1 Management Information is modeled using object-oriented techniques.An object model describes the structure of objects in a system.The idea is to capture those concepts from the real world network that are important to the system.The object model is graphically represented with object diagrams containing object classes.Classes are arranged into hierarchies, inheritance and containment, sharing common structure and behaviour.

4.2.5.2.2 The object model describes the network as a collection of discrete objects that incorporate both data structure and behavior. These objects represent real resources in the network and are termed "managed objects". A "managed object" is an abstraction of the real work resource for the purpose of network management.

4.2.5.2.3 Each managed object belongs to an object class which describing a set of individual objects.The managed objects are abstracted into a class by generalizing common attributes and behavior. A particular managed object existing in a particular network is defined as an “object instance” of the object class to which it belongs.

4.2.5.2.4 Managed objects contain properties that are referred to as attributes. Attributes are atomic items of information that can only be manipulated as a whole. An example of an attribute is a counter providing a specific piece of information, such as the number of packets retransmitted.

4.2.5.2.5 Managed objects in OSI are fully defined using a set of templates and a special purpose notation. These guidelines are defined in GDMO (Guidelines for the Definition of Managed Objects).

4.2.5.3 ***GDMO - Guidelines for the Definition of Managed Objects***

4.2.5.3.1 GDMO is a managed object definition language providing a method of writing correct, complete and consistent specifications. Structural and behavioral characteristics important to network management are modeled in a set of templates.

4.2.5.3.2 The Managed Object Class Template is the base template for the definition of managed objects.It specifies the position of the class in the inheritance tree by defining the superclasses from which it has been derived.It includes additional templates including mandatory packages, conditional packages and notifications. It also provides a class name and registration scheme (i.e. registration of object identifier value) which may be used to identify the class in management protocol.

4.2.5.3.3 The PACKAGE template is a collection of properties such as behavior, operations, attributes and notifications. Packages included in a class extend the inherited behavior and properties of the superclass. There are both mandatory and conditional packages.Packages that are mandatory occur with every instance of the class.

4.2.5.3.4 This ATTRIBUTE template specifies attributes to be defined in the package. The property list that is associated with the attribute defines the allowable operations that may be performed on it. Default values, and permitted values for the attribute may be specified.

4.2.5.3.5 The NOTIFICATIONS template defines the notifications the managed object can issue to the management system. It identifies the event reports which a managed object can emit using the CMIS M-EVENT-REPORT service.Each NOTIFICATIONS template specifies the syntax of the information associated with the notification the syntax of the reply associated with it, and indicates whether or not it is confirmed.

4.2.5.3.6 The ACTION template specifies the actions which the management system may wish to perform using the CMIS M-ACTION service. Each ACTION templage specifies the syntax of the information associated with the action request, the syntax of the reply associated with it, and indicateswhether or not it is a confirmed action.

4.2.5.3.7 The BEHAVIOR template is used to provide behavioral information from the management perspective. It is specified in natural language.

4.2.5.3.8 The NAME BINDING template specifies a 'contained' object class.

4.2.5.4 ***Management Information Hierarchies***

4.2.5.4.1 Managed objects participate in relationships with each other.There are two relationships that are of particular importance for management information: the containment relationship and the inheritance relationship.These relationships can be used to construct hierarchies of managed objects.In addition, there is another hierarchy defined by the registration process for registering identifiers for object classes and attributes.

4.2.5.4.2 **The Inheritance Hierarchy**

4.2.5.4.2.1 Inheritance is a tool in object-oriented methodologies used to classify data. If there are two similar object classes sharing a subset of their properties, their common properties can be abstracted into a superclass or parent. They are called superclasses because they are higher-order abstractions than their subclasses.A continuance of the abstraction of the properties of superclasses result in the construction of an inheritance hierarchy (or object class hierarchy).The inheritance hierarchy provides a second order abstraction, in which common properties and behavior of classes can be isolated in yet other classes.It is a structuring principle allowing the second-order manipulation of entire classes via their superclasses, complementing the first-order manipulation of individual objects by their classes.This second-order abstraction is the defining characteristic of object-oriented modeling paradigms.When the inheritance hierarchy is constructed to the point where no further levels of abstraction arepossible, we have arrived at its root.For a given application domain, there is only one root of the inheritance hierarchy.The class inheritance hierarchy of the OSI SMI is rooted at an artificial object class called top.

4.2.5.4.2.2 The power of the inheritance hierarchy is as a specification tool and best utilized in a top-down fashion.Each class in the hierarchy is considered to implicitly possess all the properties abstracted in its superclass.

4.2.5.4.3 **The Containment Hierarchy**

4.2.5.4.3.1 The containment hierarchy is similar to the aggregation hierarchy of object oriented methodologies.Containment specifies which managed object classes may be contained in other MO classes and is defined using a construct known as a name binding.The NAME BINDING template specifies a subordinate, or contained, object class which is part of a superior, or containing, object class.

4.2.5.4.3.2 The containment hierarchy is also used to create names of object instances. In OSI SMI containment is also used as a naming mechanism, that is the addressing scheme for managed objects arises out of their logical containment in other objects. Each managed object can be addressed using its distinguished name, which is a sequence of MO names starting from the highest object in the containment hierarchy. The attribute used to name the MO could be unique. Therefore the name binding specifies the attribute used by the superior MO to name the subordinate MO. The containment hierarchy describes the subordinate managed object instances contained within superior managed object instances. By following the naming attributes from

the root of this hierarchy to any managed object within it, the complete distinguished name of the object can be constructed.

4.2.6 The Management Information Base

4.2.6.1 The Management Information Base (MIB) is a "conceptual repository of management information." It is an abstract view of all the objects that can be managed in a resource.

4.2.6.2 Note that the MIB is conceptual in that it does not carry any implications whatsoever about the physical storage (main memory, files, databases, etc.) of management information. A MIB can be viewed as a collection of access points at the agent, for the manager.

4.2.6.3 Within the agent, the MIB is a data structure providing access to specific resources in the form of variables or objects. Managers must share the same view of the MIBs as the agents with whom they need to communicate. Figure 4.2-2 illustrates the concept of a MIB.

4.2.7 Management Functions

4.2.7.1 Management information is used by the system manager to assist in making management decisions and to communicate those decisions to the system resources. Functionality required for each of the five systems management functional areas (fault, accounting, configuration, performance and security)

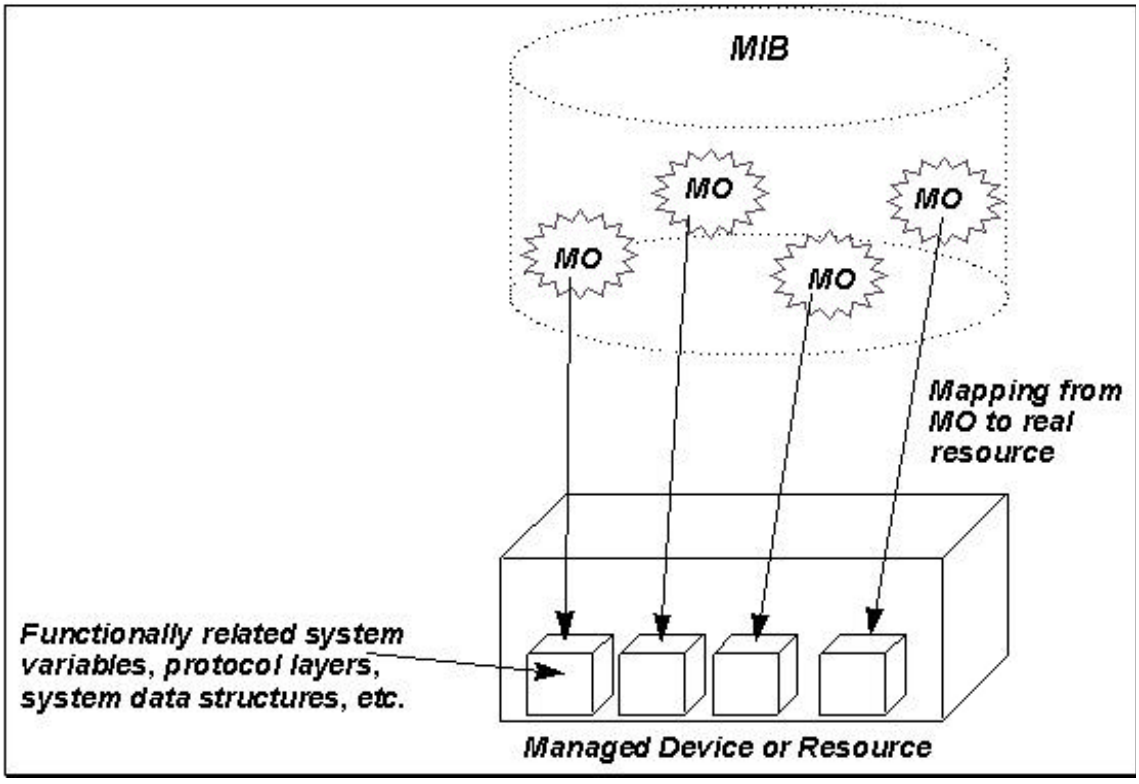

Figure 4.2-3. Concept of Management Information Base

consists of sets of elementary *Systems Management Functions*.

4.2.7.2 Systems Management Functions are specified in a sequence of ISO/IEC/ITU-T standards. These standards define a number of common ways in which agent systems and managed objects can operate.

4.2.7.3 Some specify general-purpose agent *support functions* that support management communications, of which the two most important control the forwarding and logging of event reports. These functions allow managers to control which event reports are sent where, and which are logged locally for subsequent retrieval. Others support access control, accounting, testing, and the creation and scheduling of statistical or summary reports. The standards for these functions define *support managed objects*, and in this way they specify both how the support functions work and how they can be managed.

4.2.7.4 Other systems management functions are intended to create consistency between different managed objects that have properties in common, such as state attributes or the need to generate alarm notifications. They do this by defining *generic management information*, usually attributes and notifications, that can be imported into any managed object definitions where they might be appropriate. Other examples are relationship attributes and accounting information.

4.2.7.5 Some systems management functions, such as test management, accounting and summarization, define support functions as well as generic management information.

4.3 Application of Systems Management Concepts to ATN

4.3.1 General

4.3.1.1 As described previously, the ATN consists of a set of autonomous administrative management domains. Each domain would be managed locally.

4.3.1.2 The core concept underlying the ATN Systems Management concept of operations is that there is a need to standardize the exchange of management information across administrative and management domain boundaries.

4.3.1.3 Systems Management can be viewed as a multi-part problem:

a) definition of management information;

b) exchange of management information; and

c) use of management information.

4.3.1.4 While everyone can agree that management of the systems comprising the ATN is necessary, agreement is not as easy on the exchange of information across administrative and management domain boundaries.

4.3.1.5 The concept of operations addresses the issue of management information exchanges by defining an interface between Management Domains as the point where information standardization is required.

4.3.2 Architecture for Cross-Domain Systems Management

4.3.2.1 *Overview of the Cross-Domain Systems Management Service*

4.3.2.1.1 The Cross-Domain Systems Management (CDSM) services provide ATN organizations with the ability to access management information relating to the services provided by another ATN organization. For example, an ATN organization may notify an ATN service provider of a fault affecting the service and the ATN service provider may keep the customer organization informed of progress on repairing the fault, ultimately sending Systems Management notifications when the fault is cleared. The Cross-Domain Systems Management (CDSM) services also include the capability for an organization to control the amount and type of cross-domain management information that is reported or must be logged by another ATN organization.

4.3.2.1.2 The cross-domain management information provided by an ATN organization to external ATN organizations is generally different from that used internally within an administrative management domain to manage the local ATN infrastructure. It is less detailed since the external organizations are only concerned with management information relating to provision of its own ATN service and are not concerned with the precise details of how the ATN service is provided.

4.3.2.1.3 The CDSM services provided by an ATN organization may only be accessed by authorized external ATN organizations. An ATN organization providing CDSM services will take all necessary steps to ensure that an agreed level of security is maintained.

4.3.2.1.4 By accessing cross-domain management information, an authorized ATN organization will be able to indirectly monitor the resources involved in the provisioning of an ATN service.

4.3.2.2 *Overview of the Cross-Domain Systems Management Functional Architecture*

4.3.2.2.1 The CDSM Functional Architecture is based on several function blocks. These blocks provide general functions needed for the provision of CDSM services.

4.3.2.2.2 The CDSM function block of the local ATN organization and the management function block of the external ATN organization which exchange management information are separated by the CDSM reference point. The CDSM function block may be further refined in terms of the functional components that comprise it.

4.3.2.2.3 The CDSM reference point is the logical point in the architecture at which conformance may be tested for a particular protocol realization of an interface that supports CDSM services.

4.3.2.2.4 The CDSM Functional Architecture is shown in Figure 4.3-1.

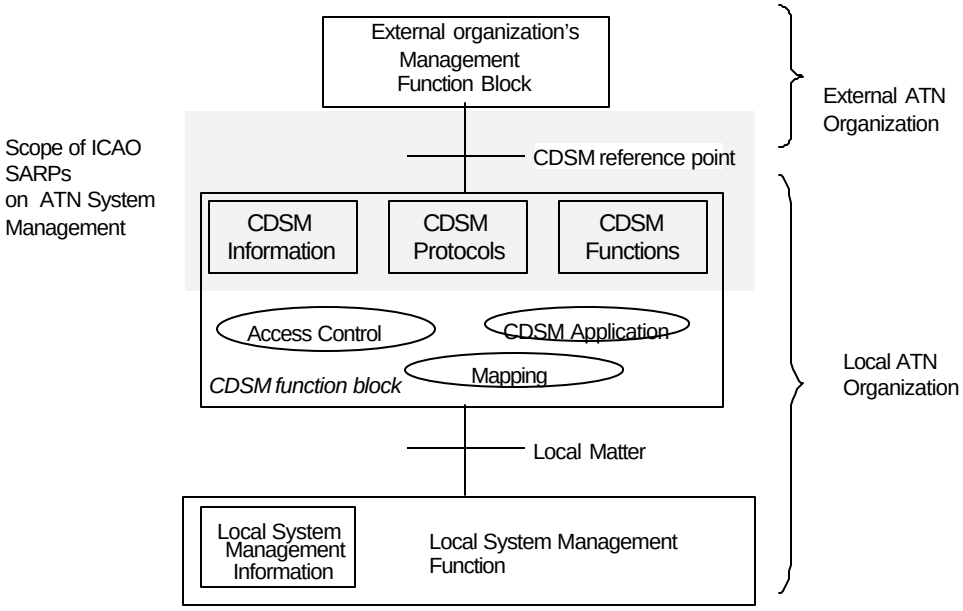

Figure 4.3-1. Functional Architecture of Cross-Domain Systems Management

4.3.2.2.5 The CDSM function block may include the following functional components:

- CDSM information;
- CDSM protocols;
- CDSM functions;
- access control;
- CDSM application; and
- mapping.

4.3.2.2.6 The CDSM information component contains an external view of local ATN services management related information.

4.3.2.2.7 The CDSM protocols component includes the protocols used to transfer the CDSM information across management domain boundaries.

4.3.2.2.8 The CDSM functions component includes a set of standard systems management functions addressing particular common requirements identified in the CDSM context.

4.3.2.2.9 The CDSM application functional component will actually implement the CDSM services. The CDSM application functional component acts always in the agent role. This functional component is not subject to standardization.

4.3.2.2.10 The access control functional component includes mechanisms allowing to restrict access to authorized external ATN organizations. The standardization of this component is out of the scope of ATN Systems Management.

4.3.2.2.11 The mapping functional component may be required in order to provide the external ATN organization oriented view of the local systems management information. The local systems management information and the details of the mapping are not subject to standardization. However, bilateral agreements must be established on aspects such as the currency of the information which is made available.

4.3.2.3 *Overview of the Cross-Domain Systems Management Physical Architecture*

4.3.2.3.1 The CDSM reference point is the only point in the functional and physical architectures for CDSM at which protocol verification / conformance testing applies. Currently, CDSM services may be provided across one type of CDSM interface: the CMIP CDSM interface. This interface is described in section 4.4. Other types of interfaces may be defined in the future, including interfaces which use EDI with AMHS as the supporting protocol.

4.4 Provision of Cross Domain Systems Management Services across the CMIP CDSM interface

4.4.1 General

4.4.1.1 The CMIP CDSM interface is applicable for the provision of a large range of Cross Domain Systems Management services. In particular, it is used where the supporting protocols must be interactive (with response time constraints), for meeting fault management and real time monitoring requirements.

4.4.1.2 The CMIP CDSM interface uses the CMIP protocol and provides/allows:

- real time/asynchronous notification;
- object oriented mechanism; and
- re-use of OSI Systems Management software.

Note.— When the supporting protocols need not be interactive/real time or the CDSM service requires a contractual interaction between the ATN organizations, another CDSM interface type (e.g. an EDI/AMHS based CDSM interface) may be more appropriate.

4.4.2 **Principle**

4.4.2.1 The provision of CDSM services across the CMIP interface relies on the implementation, by the ATN organizations, of a Cross-Domain MIB (XMIB), that is a special MIB dedicated to support the exchange of management information with other ATN organizations.

4.4.2.2 The Cross-Domain MIB is a MIB in which are gathered the elements of management information on the local ATN management domain that are shared with external ATN organizations. The Cross-Domain MIB consists of a summary and/or extracts of the local systems management information that are made accessible to other organizations via CMISE-based procedures.

4.4.2.3 An ATN organization providing CDSM services across the CMIP interface, achieves this by providing other ATN organizations with access to its Cross-Domain MIB. This organization is assumed to update the content of its Cross-Domain MIB according to the agreements on the required accuracy and timeliness of the information.

4.4.2.4 External ATN Organizations that have been granted access permission are allowed to read, periodically or on specific need occurrence basis, the content of the Cross-Domain MIB. Possibly, these organizations may register themselves to receive notifications of particular events.

4.4.3 **Functional architecture**

4.4.3.1 The functional architecture of the CMIP CDSM interface is based on several function blocks implemented either by the ATN organization providing access to its XMIB or by the organizations retrieving information from this XMIB. This is depicted in Figure 4.4-1.

4.4.3.2 The interface is based on the classic agent/manager model.For use between two management systems that are maintaining Cross-Domain MIBs, a request for information from one management system to another is a request from a manager to an agent.That means that each management system maintains its Cross-Domain MIB information acting as an agent; and that it fulfils requests for that information just like any other agent.

4.4.3.3 The following definitions apply:

XMIB User: This function block is a Management application operating in the manager role and to be implemented by organizations wishing to retrieve information from the XMIB maintained by other organizations;

XMIB Agent: This Function block is a Management application operating in the Agent role which performs the CMISE operations on the local XMIB. The XMIB Agent handles

information retrieval requests from XMIB Users. This system is implemented by the organization providing XMIB access services; and

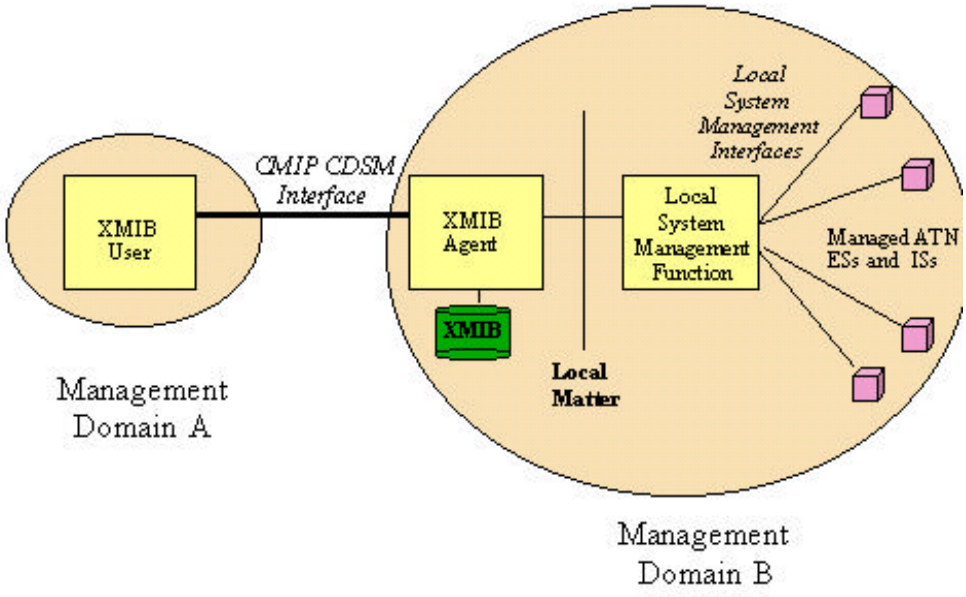

Figure 4.4-1. Functional Architecture for the provision of CDSM services via a CMIP interface

Local Systems Management Function: The functional model assumes that the local ATN organization operates a Systems Management Application that has the capability to collect, via local Systems Management procedures, management information from the individual pieces of ATN equipment distributed in the local domain. and to filter and process the gathered information in support of the provision of XMIB access services. This functional block is responsible for maintaining the accuracy and the timeliness of the management information made available to external organizations via the CMIP CDSM interface.

4.4.4 Characteristics of the CMIP CDSM interface

4.4.4.1 The CMIP CDSM interface relies on a direct CMIP-based manager-agent association between the XMIB User and the XMIB Agent. A XMIB User wishing to retrieve information from XMIBs of different organizations will have to establish one management association with each of the associated XMIB Agents.

4.4.4.2 Between a XMIB User and a XMIB Agent, the information will generally be exchanged on a demand basis: the XMIB User starts the management information retrieval through a CMIP operation sent to the XMIB Agent. The procedure is as follows:

a) First, the XMIB User sets up an association with the XMIB Agent. The association may be permanently set based on the agreement of both organizations or on a demand basis; and

b) The XMIB User may then send either a CMIP M_GET or a CMIP M_CANCEL_GET operation to the XMIB Agent. Having received the CMIP Protocol Data Unit (PDU), the XMIB Agent interprets what kind of requirement it has received and performs a management operation such as retrieval of an element of management information in the XMIB. The result is returned to the XMIB User in the form of a CMIP result PDU.

4.4.4.3 The management information can additionally be exchanged on an event occurrence basis: in such a case, the XMIB Agent takes the initiative and issues a notification to the XMIB Users that have registered themselves to receive notification of the event. The procedure is as follows:

a) First, the XMIB Agent sets up an association with the XMIB User. The association may be permanently set based on the agreement of both organizations or on an event occurrence basis; and

b) The XMIB Agent sends a CMIP M_EVENT_REPORT to the XMIB User.

4.4.5 Connectivities between XMIB Users and agents

4.4.5.1 A single XMIB user may communicate across the CMIP CDSM interface to one or more XMIB Agents using at least one association for each XMIB Agent.

4.4.5.2 A single XMIB Agent may support simultaneous associations with several XMIB Users.

4.4.6 Authentication control for the service

4.4.6.1 A XMIB Agent may authenticate the identity of the requesting XMIB User for the purpose of security. Access of the XMIB User to the management information is allowed when conditions of authentication and qualification defined by the ATN organization providing XMIB access services are satisfied. If access is not permitted, the XMIB agent may notify the XMIB user that the access has been refused. Details of security mechanisms are out of scope of this document.

4.4.7 **Role of the local Systems Management Function**

4.4.7.1 The local Systems Management Function is in charge of maintaining up to date information in the XMIB.

4.4.7.2 The method of collecting and maintaining the XMIB information is a local implementation choice for the administrative Management Domains as long as they meet the timeliness and accuracy of the management information.

4.4.7.3 Data fusion, or the process of collecting and utilizing data from several sources, is an important aspect of this function.The local Systems Management Function is required to take multiple separate data sources and combine those sources into a coherent view of the overall ATN.

4.4.7.4 The first source of systems management information is the local ATN management domain.The local Systems Management Function must be able to receive information from the agents in its domain and create the required Cross-Domain MIB information.(Of course, it may also be required to collect and locally display other information relevant to the operation of the local domain).

4.4.7.5 The management of the local domain, the types of information maintained, and the protocols used to collect that information are a local choice.It is the responsibility of the local Systems Management Function to take the information and convert it from the local form into the form needed by the Cross-Domain MIB.(This means that it is entirely satisfactory to maintain the local domain using SNMP for example and have a local Systems Management Function that collects the appropriate SNMP information, and translates it into the appropriate CMIP-based form when updating the Cross-Domain MIB).

4.4.7.6 The second source of information to a local Systems Management Function is data coming from other ATN Management Domains.This information may be the result of either requests or unsolicited.It will be necessary for each local Systems Management Function to analyze the received information in order to decide whether to include the information in its Cross-Domain MIB or to take corrective local actions based on changing conditions within the ATN.

4.4.7.7 The possible methods for maintaining the Cross-Domain MIB can be categorized as follows:

a) update on a periodical basis:management information is periodically transferred from the ATN equipment to the local Systems Management Function, which then filters/summarizes the information and updates the XMIB;

b) update on an event occurrence basis: any events (notifications) issued by an ATN equipment and in relation to management information present in the XMIB can be processedby the local Systems Management Function, and results in an update of the XMIB; and

c) update on a demand basis: the Local Systems Management Function starts the action of updating the XMIB when a management information retrieval request is received by the XMIB Agent.

4.4.7.8 Which method is used for updating the XMIB is a local issue.Any one or a combination of the three methods can be used, provided that requirements on the accuracy and timeliness of the Cross-Domain Management Information are met.

Note.— Depending on the type of the Cross-Domain Management Information element to be updated, one method may be more appropriate than the others. For instance, the status of an ATN system or link could be updated on an event occurrence basis, whereas configuration information could be updated on demand basis, and performance statistics could be updated on a periodical basis.

4.5 Management Information Standardization

4.5.1 Introduction

4.5.1.1 Systems Management information must be shared between different management domains either off-line or on-line depending upon the type of information.

4.5.1.2 The basic problem in defining systems management and the concept of operations is in defining the type of information that must be shared across domain boundaries.The reason that this is so difficult is that much of the management information can be viewed as proprietary information or may be considered sensitive from a national administration stand-point.

4.5.1.3 As defined in the previous section, the ATN Systems Management Concept of Operations is built on the definition of the “interface” between two management domains and the required information flow between those domains.

4.5.1.4 It is recognized that some information must to shared and that some of that information is required to be shared in an on-line mannerFurther, the information that needs to be shared on-line must be available from every ATN Management Domain when requested.

4.5.1.5 The systems management information that must be exchanged on-line across management domains is defined within the Cross-Domain MIB.

4.5.1.6 To ensure consistency of the Cross-Domain MIB information, a GDMO description of the information is required so that the semantics and accuracy requirements of the information is assured across domains.

4.5.1.7 Other information may be shared in an off-line, less timely manner.

4.5.2 Basic concept of cross-domain management information

4.5.2.1 An ATN organization will likely operate a complex infrastructure consisting of multiple components such as subnetworks, intra and inter domain routers, End Systems, the whole being architectured to meet local and external requirements, and taking into account constraints of various types, including

economical, geographical, and technical considerations. In order to maintain the service provided by its ATN infrastructure, this ATN organization will have to process the associated available management information. The amount and complexity of this management information will likely be proportional to the size and the architectural complexity of the local ATN infrastructure.

4.5.2.2 On the other hand, the management information to be provided to external ATN organizations is generally different from that used locally to manage the ATN infrastructure. It is less detailed since the external organizations are only concerned with management information relating to provision of their own ATN services, with little concern on the way the services are effectively provided.

4.5.2.3 The local management information shared with external ATN organization must be defined based on the external organizations concerns and on local security and non-disclosure concerns.

4.5.2.4 The XMIB Managed Objects are standardized as generic MO classes. They may be refined by each organization by adding specific features to extend its CDSM services.

4.5.2.5 Which object may be accessed by an XMIB user or which conditional packages should be offered is based on the agreement between the user organization and the provider organization of the CDSM services. An access control function must ensure that the initiating XMIB user has the proper right to access the requested XMIB information. Access control utilizes the authentication pattern (e.g. digital signature) in combination with locally defined access right associated with each user that is authorized to access the XMIB.

4.5.3 **Cross-domain management information structure**

4.5.3.1 The top level structure of the XMIB containment tree is represented on Figure 4.5-1.

4.5.3.2 In the figure, the shadowed boxes represent Managed Object Classes that can have multiple instances.

4.5.3.3 The Domain MO serves as the starting point of the naming. The Domain MO is a placeholder for general information on the ATN organization providing the CDSM services. Within an XMIB there is only one single MO instance of this class.

4.5.3.4 The atnInternetServices, atnApplicationServices and atnMHSServices MO classes are used as containers of all MOs representing the systems management information on, respectively, the local ATN Internet Services, the local ATN Application Services and the local AMHS services. For instance, MOs representing the local ATN routers can be defined as subordinate MOs of the atnInternetServices MO; MOs representing the local AMHS Message Transfer Agent (MTA) can be defined as subordinate MOs of the atnMHSServices.

4.5.3.5 The log MOs are repositories for log records. Each log MO contains a discriminator that specifies which information is to be logged.

4.5.3.6 The EFD (or Event Forwarding Discriminator) MOs allow specification of conditions to be satisfied by potential event reports related to managed objects before the event report is forwarded to a particular destination (for instance, to a particular XMIB User).

4.5.4 **Access Control**

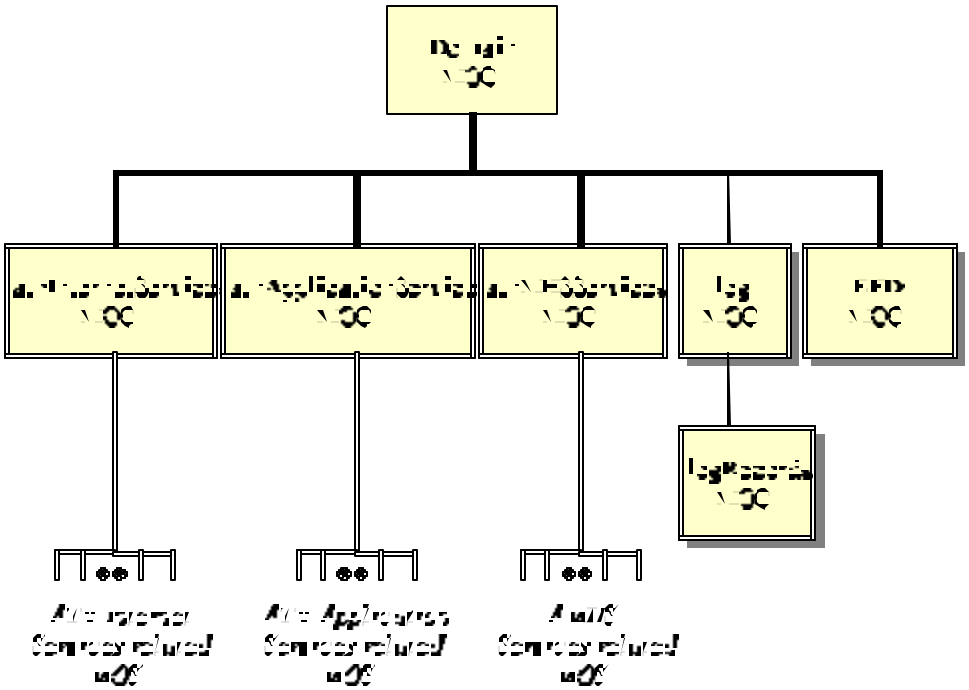

Figure 4.5-1. Top level structure of the XMIB containment tree

4.5.4.1 To prevent unauthorised access to the Cross-Domain Systems Management Information, an access control function must be supported by the organizations providing CDSM services.

4.5.4.2 The access control function must ensure that the initiating XMIB user has the proper right to perform the intended operations on the XMIB information. Access control must be applied at association time, when accessing objects and when generating notifications. In this way, unauthorized or unintended disclosure of management data are prevented.

4.5.4.3 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 on initiator identity and constraints applicable to the operations and targets in the request.

4.5.4.4 The access control function is determined by whatever access control policy is in force. The access control policy is peculiar to each specific ATN organization and so outside the scope of ATN SARPs. Details of access control mechanisms to be applied are therefore 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.

4.5.4.5 Whilst the standard does not make any access control policy and mechanisms mandatory, standard authentication mechanisms must be defined to allow for interoperability between Cross-Domain Management Systems. The definition of authentication mechanisms is however outside the scope of ATN Systems Management. These are defined in the scope of the ATN Security framework and specified in the Sub-Volume of ATN SARPs on ATN Security (Sub-Volume 8).

4.6 Overview of Cross-Domain Systems Management Protocol Profiles

4.6.1 Assuming that Cross-Domain MIB information is available across management domains, it remains that the method of accessing that information must be standardized. To access Cross-Domain MIB information, a standard protocol suite must be used. The protocol suite selected for the cross-domain exchange of management information in the ATN is based on the OSI defined Common Management Information Protocol (CMIP).Other protocols are possible for local Systems Management within an Administrative Domain.

4.6.2 However, the use of CMIP is only one part of the overall communication infrastructure that is required to support Cross Domain Systems Management through a CMIP interface. The other part of the problem is the selection of the underlying communication protocols.

4.6.3 The decision on what communication protocols to use is based on a set of well-defined criteria:

a) for ground-based management systems, the communication protocols selected must be compatible with standard management platforms; and

b) for air-based management systems, the communication protocols selected must be compatible with those already defined for the airborne system in Doc. 9705.

4.6.4 This leads to the following decision:

a) for ground-based cross domain management systems , a standard CMIP profile based on a full session and presentation layer is used. This profile should be supported by commercial CMIP-capable management systems;

b) for air-based cross domain management systems, a “Fast-MIP” profile should used that is both compatible with the existing Fast Byte communication profile and acceptable for use with CMIP; and

c) for the conversion between communication profiles, the conversion function should be placed in such a way to have minimal impact on COTS products.

5. SYSTEMS MANAGEMENT COORDINATION

5.1 Introduction

5.1.1 This section describes the systems management coordination needed across ATN administrative boundaries. These coordination needs were derived by developing ATN scenarios, then analyzing the scenarios for the characteristics of the inter-domain interactions that would require coordination. The scenario analysis identifies management functions for ATN and the responsible roles. The minimum needs for exchange of management data and functions across administrative domains are also identified.

5.1.2 The result of this analysis is discussed under the headings of the five standard OSI management functional areas, which are: Fault, Performance, Accounting, Configuration and Security Management

5.2 Fault Management

5.2.1 Introduction

5.2.1.1 Fault management is the set of facilities which enables the detection, isolation and correction of abnormal operation. Fault management includes functions to:

- report troubles;
- accept and act upon error notifications;
- maintain and examine error logs;

- trace and identify faults;
- carry out diagnostic tests; and
- correct faults.

5.2.1.2 Fault Management deals most commonly with alarm notifications emitted by network elements and with complaints (or trouble reports) from the network users.

5.2.1.3 To detect and mitigate faults quickly and before they affect other services, fault management relies heavily on actions taken by individual organizations. Network fault management at the level of an administrative domain is a common practice. Data network elements are generally equipped with management agents that automatically emit fault notifications to the managing system. Network Operations Centres are generally equipped with a Help Desk that users may contact in case of problems and with some kind of problem tracking system that helps the operator all along the different steps required to correct the problem associated with the alarm or symptom (fault analysis, alarm correlation, etc...).

5.2.1.4 However, fault management can also be a multi-organization problem: in one informal study of routing stability in the internet, it was found that while the majority of catastrophic routing problems could be identified as local software and configuration errors, about 10% of the problems could only be classified as " somebody else's problem ", since all parties questioned pointed to another party as the cause. Such problems are the most difficult to resolve, and underscore the need for inter-domain coordination, so that the true causes of problems may be identified and such circular referrals detected and resolved.

5.2.1.5 A second important point is that the true cause of a problem may be distant from its effect. For instance the failure of an A/G communication may be the result of a problem located anywhere between the ground ES and the airborne ES. Contacting one's local help desk is unlikely to be of much benefit in this case.

5.2.1.6 The demand for the ATN to be highly available and reliable makes necessary proactive maintenance and quick isolation of problems in the network. It is thus beneficial and necessary for organizations to cooperate in fault management to ensure high availability and reliability.

5.2.1.7 This section investigates the problem of such inter-domain coordination of troubleshooting and repair efforts, and addresses more specifically issues such as:

- reporting network outages and other problems across administrative boundaries;
- acquiring feedback on the problems across administrative domains;
- inter-administration negotiation of solutions; and
- pre-notification, or notifying organizations of downtime scheduled in the future.

5.2.2 **Characteristics of Fault Management**

5.2.2.1 This section highlights the characteristics of fault management coordination in the ATN environment.

a) Each organization is expected to design its portion of the ATN network to avoid single points of failure. This includes the design of points of attachment between the ATN elements of two organizations;

b) In the ATN environment, each organization is expected to isolate and mitigate faults quickly and to prevent faults from spreading and affecting other areas;

c) Fault mitigation is to be handled without noticeably affecting other ATM services;

d) When source of a detected fault is outside an organization, the source organization needs to be notified quickly so that they can isolate and mitigate the problem;

e) Due to limited A/G bandwidth, real-time A/G systems management exchanges must be minimized. This does not preclude other findings of a need for real-time A/G fault management exchanges. For example, IATA airlines intend to provide for the dynamic uplink and downlink of some systems management information to and from their ground based manager host systems;

f) ATN airborne equipment is expected to be maintained according to prevailing avionics standards and certification requirements. Real-time operational control of airborne avionics from the ground is not identified currently beyond that which is included in AOC applications. This does not preclude organizations that have the need and capability to provide support for systems management exchanges. For example, IATA airlines intend to provide for the dynamic uplink and downlink of some systems management information to and from their ground based manager host systems;

g) The most direct and immediate way for detecting failures in an application process (for instance, CPDLC) is through detection of a time-out or the loss of connectivity in the network elements or by means built-into the application processes. The display of detected failures immediately to the aircrew or controllers allows them to start alternative procedures, such as switching to voice communication. The end system where the application process resides may also notify the network manager to start fault mitigation procedures;

h) Remote testing and activation of diagnostic programs are desirable to enable timely verification of faults and to isolate faults before problems propagate throughout the ATN network;

i) To satisfy requirements for national security and for safety reasons, each organization is responsible and accountable for its network elements. Cross-domain interaction between the network manager of an organization and the agent in the ATN equipment of another organization is undesirable. This does not preclude cross-domain XMIB user to XMIB agent interaction; and

j) Cross-organization communication of faults should be management system to management system through the standard means of trouble ticket information exchange.

5.2.3 **Proactive Maintenance**

5.2.3.1 Proactive maintenance relies on regular monitoring and tracking of the ATN. By establishing the network trends, any deviation or anomaly can be detected and corrective action taken before failure occurs in the ATN.

5.2.3.2 Proactive maintenance involves performance management functions such as data collection, performance analysis, and threshold-crossing event monitoring. With the results of these functions, systems management operators can then choose preventive actions to avoid the symptoms and indications from developing into a fault. Further discussion of the performance management functions is provided in section 5.3, Performance Management.

5.2.3.3 Another aspect of preventive maintenance is to design each portion of the ATN to be without a single point of failure. Individual organizations are to protect their assets by minimizing single points of failure. This could be achieved by various means such as redundant connectivity, standby systems, and self-healing topologies.

5.2.3.4 Proactive maintenance is the responsibility of all participating organizations. However, it is especially necessary for the organizations that play a major role in forming the ATN backbone.

5.2.3.5 Avionics needs to be maintained according to certification and maintenance regulations, including pre-flight and post-flight examinations. These are the responsibilities of both the Airline and the end user (that is, the pilot).

5.2.3.6 Regional proactive maintenance activities may potentially provide operation optimization for the region. However, these activities are an addition to the responsibilities of individual organizations. Regional performance analysis should not be used as a replacement for the responsibilities of any individual organizations.

5.2.4 **Fault Detection and Mitigation**

5.2.4.1 Prevention helps to reduce but not to eliminate faults. Network faults are detected by four general sources:

C Alarm notifications generated by network elements;

- Customer complaints;
- Reports from adjacent networks; and
- Manager performing routine tests.

5.2.4.2 Typically, faults are tracked by way of trouble tickets. When a detected fault is verified, a trouble ticket is generated to track the mitigation process. Trouble tickets provide a means to ensure that all faults are resolved in an acceptable time. They are closed when the fault is resolved.

5.2.4.3 Fixing a root cause is the responsibility of individual organizations. In handling a fault, individual organizations are responsible for:

- Verifying that the fault is as reported;
- Finding the source of the fault;
- Isolating the source of the fault;
- Scheduling the repair;
- Repairing the fault;
- Verifying that the fault is resolved; and
- Returning the isolated element to operation.

5.2.4.4 Scheduled repair may require taking the elements out of service. This should be performed during low-peak hours to minimize service interruption. For example, the scheduled downtime cannot introduce unpredictable traffic congestion nor increase message delays in significant manner.

5.2.4.5 In the case where failure of a router requires reconfiguration within each organization, it is expected that configuration information is readily available to recover from the failure without delay.

5.2.4.6 In addition, each organization is expected to provide ATN network fault or down time information to its accounting process, if such interruptions have affected services or it is otherwise required by the billing policy.

5.2.4.7 Cross-organization coordination in fault handling is necessary for:

- Faults that originate from outside the organization;
- Faults that have impacts on neighbouring organizations; and

- Scheduled maintenance that has an impact on neighbouring organizations.

5.2.4.8 Examples of specific faults that need cross organization coordination are:

- Unexpected increases in data traffic at the point of attachment;
- Repeated transmission of errored data across the point of attachment; and
- Failure of elements at the point of attachment.

5.2.4.9 Fault detection and mitigation are the responsibility of all involved organizations in all segments of the ATN.

5.2.5 Fault Management Coordination Process

5.2.5.1 *General*

5.2.5.1.1 Trouble tickets is the general mechanism used for fault coordination between organizations. When an organization detects a fault where the source of the problem is in another organization, the detecting organization opens a trouble ticket and forwards it to the source organization.

5.2.5.1.2 The source organization verifies that the fault exists and goes on to identify the source of the problem. If the source is within the organization, a fault mitigation process is initiated. The organization that originates the trouble ticket is informed of the schedule for mitigating the fault.

5.2.5.1.3 When a fault is resolved, the trouble ticket is closed by the organization that was the source of the fault. The closed trouble ticket is forwarded to the original organization to complete the coordination process.

5.2.5.1.4 Trouble ticketing is used as a means to track faults and not the means for assigning responsibility. Organizations should work together to identify the source of the problem.

5.2.5.1.5 The priority for trouble tickets, based on the type of fault is standardized. Each organization is expected to take appropriate actions to resolve the trouble in an acceptable time. For example, high priority faults should be handled immediately. This is to localize problems quickly and to reduce the impact on the quality of the overall ATN network.

5.2.5.1.6 Common operational procedures should be defined and specify:

- in which cases an inter-domain trouble ticket is to be issued;
- to which organization(s) the trouble ticket should be delivered;

- which reporting actions have to be taken by an organization on receipt of a trouble ticket; and

- which reporting actions have to be taken by an organization on failure of one of its equipment, vis a vis the other organizations.

5.2.5.2 ***Cross-Domain Fault Management Services***

5.2.5.2.1 **Introduction**

5.2.5.2.1.1 In the ATN, the general Fault Management coordination process introduced above will rely on the following basic Cross-Domain Fault Management Services:

- The ATN Cross Domain Alarm Notification service;

- The ATN Cross Domain Fault History service; and

- The ATN Cross Domain Trouble Report service.

5.2.5.2.1.2 These services will be provided between ATN management domains across the CMIP CDSM interface introduced in section 4.4(i.e. across the Cross-Domain MIB access interface).

5.2.5.2.1.3 These services are described in the next sections. In all these sections, the term 'external ATN organization' is used to reference the user of the Cross-Domain Fault Management service; the term 'local ATN organization' is used to reference the provider of the Cross-Domain Fault Management service.

5.2.5.2.2 **Cross-Domain Alarm Notification Service**

5.2.5.2.2.1 **Service definition**

5.2.5.2.2.1.1 The ATN Cross-Domain Alarm Notification Service provides an external ATN organization with the capability to be notified when a failure or event occurs which affects the normal operation of a resource of the local ATN organization and upon which the external ATN organization depends for the provision of an ATN service.

5.2.5.2.2.2 **Functional Description**

5.2.5.2.2.2.1 The following functions are associated with the alarm notification service:

a) Report alarm function:

This function sends relevant alarms to an external ATN organization. Alarms may include communication faults, degradation of QoS, processing error of the network, equipment faults and abnormality of communication environment;

b) Report state change function:

This function sends event reports to an external ATN organization relating to state changes of local resources which are relevant to that organization;

c) Inhibit/Allow alarm and state change reporting function:

This function allows an external ATN organization to control the flow of alarm and state change reports to that organization.

d) Condition alarm and state change reporting function:

This function allows an external organization to modify criteria for reporting events (alarms or state change reports). Criteria may include the time of events, the type of events, the resource name from which alarms are emitted, the type of problem or cause, and severity of the fault; and

e) Request alarm and state change reporting conditions function:

This function allows the external organization to request the local Cross-Domain Management System to send the current assignment of the filtering criteria it specifies.

5.2.5.2.3 **Cross-Domain Fault History Service**

5.2.5.2.3.1 **Service Definition**

5.2.5.2.3.1.1 The ATN Cross-Domain Fault History service provides an external organization with the capability to retrieve fault history log records, stored at the local ATN organization side, and related to a local resource upon which the external ATN organization is dependent. The report contains information related to failure or event occurrence which affect the normal operation of the local resource upon which the external organization depends.

5.2.5.2.3.1.2 This service may be used, for example for particular events with low severity which have been recorded or logged within the fault history log but which have not been sent to the external organization.

5.2.5.2.3.2 **Functional Description**

5.2.5.2.3.2.1 The following functions are associated with the Cross-Domain Fault History Service:

a) Retrieve fault history log records function: This function accumulates alarms related to an external organization in the forms of a fault log record. Log records include communications faults, degradation of QoS, processing error of the network, equipment faults, abnormality of communication environment, creation/deletion of

the resources and change of their states. These records are accessed by the external organization;

b) Selection of specific fault log records function: This function selects specific fault log records based on the requested filtering condition; and

c) Modify the criteria for logging fault log records function: this function modifies criteria for logging fault log records.

5.2.5.2.4 **Cross Domain Trouble Report Service**

5.2.5.2.4.1 **Service Definition**

5.2.5.2.4.1.1 The Trouble Report service is the automated trouble ticketing function. This service provides an external ATN organization with the capability to report trouble on services or resources that affect the ATN communication of the external organization, track the progress of trouble to resolution, and identify the clearing and closure of trouble.

5.2.5.2.4.1.2 When an external ATN organization detects communication problems, it may issue a Telecommunication Trouble Report containing information about the problem. The external ATN organization can retrieve the format provided by the local ATN organization by electronic means. Several formats may be defined using standard attributes. Repair activities can be retrieved from historical records of activities performed to resolve the trouble, such as activity information and responsible person.

5.2.5.2.4.1.3 When the local ATN organization finds the occurrence of trouble in the communication of an external ATN organization, the local ATN organization creates a Telecommunication Trouble Report and notifies the external ATN organization of the trouble.

5.2.5.2.4.1.4 Also, this function allows the local ATN organization to report the trouble report progress information to the external organization, or log the information at the external organization side.

5.2.5.2.4.1.5 Through this service, an external organization is also given information about a plan or schedule for maintenance action which affects the external organization ATN communication.

5.2.5.2.4.1.6 An external organization may also retrieve past trouble reports that have been reported.

5.2.5.2.4.2 **Functional Description**

5.2.5.2.4.2.1 The following functions are associated with the Cross Domain Trouble Report service:

a) Control Basic Trouble Report function:

This function controls basic trouble report handling. Capabilities include:

- giving notice to the local/external ATN organization that an ATN service is in need of repair;
- allowing external organization to ask for status information on a previously entered trouble report;
- providing a template for a trouble report for a particular service or class of services (to show what attributes of a trouble report are considered mandatory or optional);
- notifying the external organization that the trouble report has been closed, or keeping the closure information in an internal log;
- allowing the external organization to ask for information about past troubles that have been reported;
- adding information to a trouble report already existing;
- notifying the external organization that the status of that trouble report has changed;
- notifying the external organization that the commitment time for that trouble report has changed;
- notifying the external organization that other attributes of interest for that trouble report have changed;
- notifying the external organization that a trouble report has been created, either as the result of a request or as a result of an internal action of the local ATN organization;
- notifying the external organization that a trouble report has been deleted, either as the result of a request or as a result of an internal action of the local ATN organization;
- notifying the external organization on a periodic basis about the status of any trouble that occurred during a defined period (this would be by prior agreement between the local ATN organization and the external organization);
- allowing the external organization to verify that the repair has been completed to its satisfaction before the trouble report is closed out in the local ATN organization;

- notifying the external organization that a Trouble Report Format Definition has been created;
- notifying the external organization that a Trouble Report Format Definition has been deleted;
- notifying the external organization that a Trouble Report Format Definition attribute of interest has changed;
- notifying the external organization about progress on resolving the trouble;
- allowing the external organization to notify a previously reported trouble is no longer of interest;
- providing information that may be use for trouble report correlation; and
- notifying a external organization of a plan or schedule for maintenance action which affects the external organization's communication such as file update, a kind of test;

b) Planned maintenance reporting function;

This function notifies the external organization that planned maintenance or preventive maintenance action is scheduled, to prevent future trouble; and

c) Report Trouble History function:

This function allows the local ATN organization to report the trouble report closure information to the external organization.

5.3 Performance Management

5.3.1 Introduction

5.3.1.1 Every organization participating in ATN communication and operating ATN equipment is responsible for collecting and archiving locally management information that indicates network utilization, growth, reliability, etc.. The primary goals of this activity are to facilitate real-time problem detection, near-term problem isolation and longer-term network planning within the organization.

5.3.1.2 In the broader context of ATN inter-domain communications, the goal of co-operative problem isolation and network planning among ATN organizations is likely to be similarly and increasingly important particularly as the ATN grows and the number of involved organizations expands, while the overall quality of service remains more of a concern.

5.3.1.3 In most cases, the requirement for the cross-domain exchange of performance management information will exist for the purpose of off-line network planning activities within a Region or between Regions (e.g. Improvements in network performance from re-configuring interconnected elements based on shared data). It is assumed that the ATN organizations will satisfy this requirement with multi-lateral agreements on the regular exchange of analysis reports on the performance of their own respective ATN domain. This area of cross-domain systems management coordination is out of the scope of ICAO SARPs.

5.3.1.4 However, there are also potential requirements for the real time sharing of performance data across organizations. These include:

a) detection of network degradation due to adverse effects from interconnected elements;

b) awareness of performance degradation detected from outside the management domain;

c) centralized monitoring of the overall ATN performance within a region in support of the regional coordination of systems management activities; and

d) availability of performance data for billing verification purposes.

5.3.2 **Characteristics of Performance Management**

5.3.2.1 This section highlights the characteristics of performance management coordination in the ATN environment.

a) Performance analysis is a way to achieve proactive maintenance of the ATN;

b) Cross-domain interaction between the network manager of an organization and the agent in the ATN equipment of another organization is undesirable. This does not preclude cross-domain XMIB user to XMIB agent interaction;

c) If sharing of performance data is agreed upon between organizations, only general performance data or data pertaining to those organizations should be shared and not third party data. For example, if raw ATN traffic data is to be exchanged between two organizations, the collected traffic data needs to be processed to eliminate traffic information concerning other organizations. This is to protect and honor organizational privacy and to avoid national security implications; and

d) Each organization is expected to provide performance analysis results and recommendations to its configuration management process to refine or maintain ATN network performance at an acceptable level. Impacts on the overall regional ATN network must be considered.

5.3.3 Data Collection

5.3.3.1 Each organization is responsible for collecting and storing performance information from its own portion of the network. Most data network elements are capable of providing performance data to a management system on a scheduled basis. Typically, performance data is collected and stored for future analysis and is not handled in real-time. Short-term performance degradation may need proactive handling, e.g. activation of backup systems. Thresholds may be pre-set such that, when performance is degraded beyond a threshold for a given time, the network element reports the situation as an alarm notification of a set severity. The notification is then handled in real-time by the fault management process. The mechanisms for setting up the thresholds, schedules, and selecting relevant performance data for collection are employed in commercial data network elements.

5.3.3.2 The set of performance data defined for collection in an organization depends on the operational purpose and the usage of the data. Some of this performance data could also be used for billing. In that case, relevant performance data is forwarded to the accounting process.

5.3.4 Performance Analysis

5.3.4.1 Regular performance analysis of the ATN is a method to achieve proactive maintenance. By understanding the ATN network performance patterns under normal operation, degradation can be quickly identified from any performance anomalies.

5.3.4.2 Various analyses can be done on the ATN. The basic need is to establish the operational trends of the ATN. Each organization, as a minimum, needs to know the normal traffic pattern of its portion of the ATN, the peak hour traffic for that portion of the ATN, the typical error rate in normal operation, and the maximum traffic load the ATN has been capable of handling with an acceptable error rate.

5.3.4.3 The analysis should be performed at various subnetworks within an organization. By knowing the trends of different portions of its ATN, the organization has better control of its ATN segment. In the case when re-routing is necessary, the organization can confidently load-balance its ATN segment while maintaining the required quality.

5.3.4.4 Besides establishing operational trends for the ATN, each organization is expected to analyse its ATN network performance data on a regular basis. They are expected to take appropriate action to mitigate degradation and to ensure ATN service quality.

5.3.5 Performance Management Coordination Process

5.3.5.1 *General*

5.3.5.1.1 The following minimum performance management exchanges across organizations are necessary to maintain the quality of the global ATN:

a) Each organization is to inform adjacent organization of an ATN performance degradation that affects that organization. The potential problem, the planned actions, and the schedule for mitigation are shared across organizations;

b) ATN performance degradation detected by adjacent organizations is to be communicated to the suspected source organization for necessary actions in correcting the cause;

c) If a change in ATN network traffic patterns across organizational boundaries is expected, the affected organizations need to be informed.

Note.— The above performance management exchanges can be through trouble tickets just as in exchanges for fault coordination described in section 5.2.5.Different priorities are used to differentiate the types of trouble tickets; and

d) Each organization is to provide other external organization with real time visibility on the local value of standardized shared performance data.

5.3.5.1.2 The provision of real-time cross-domain access to local performance data will be achieved across the CMIP CDSM interface introduced in section 4.4. Standardized shared performance data will be implemented in the Cross-Domain MIBs. ATN organizations which need a real-time view on the overall performances of another ATN domain, will monitor the relevant performance data in the associated Cross-Domain MIB.

5.3.5.1.3 The potential difficulty in the use of the performance data exchanged across domain boundaries is that every organization may use different systems management tools for the collection and presentation of performance management metrics, with different kinds of measurement and presentation techniques. To allow for the exchange of meaningful performance management data, there must be a general agreement on the exact definition of every shared performance metric.

5.3.5.2 ***Cross-Domain Performance Management Services***

5.3.5.2.1 **Introduction**

5.3.5.2.1.1 In the ATN, the general Performance Management coordination process introduced above will rely on the following basic Cross-Domain Management Services.

- The ATN Cross Domain Alarm Notification service, as defined in section 5.2.5.2.2;
- The ATN Cross Domain Fault History service, as defined in section 5.2.5.2.3;
- The ATN Cross Domain Trouble Report service, as defined in section 5.2.5.2.4; and
- The ATN Cross Domain Performance Information service.

5.3.5.2.2 **Cross-Domain Performance Information Service**

5.3.5.2.2.1 **Service Definition**

5.3.5.2.2.1.1 The ATN Cross-Domain Performance Information Service provides an external ATN organization with the capability to retrieve performance information.

5.3.5.2.2.1.2 This service will be provided between ATN management domains across the CMIP CDSM interface introduced in section 4.4(i.e. across the Cross-Domain MIB access interface).

5.3.5.2.2.2 **Functional Description**

5.3.5.2.2.2.1 Performance data collection refers to the ability for the local organization to collect the various performance data relating to the operation of the ATN communication services.

5.3.5.2.2.2.2 The following specific functions are associated with the Cross Domain Performance Information Service:

a) Retrieve performance data collection interval function:

This function retrieves the interval of the performance data collection;

b) Retrieve history duration function:

This function retrieves the duration during which specific record of performance historical data are maintained; and

c) Retrieve traffic data function:

By this function current or historical performance data is retrieved.

5.4 **Accounting Management**

5.4.1 **Introduction**

5.4.1.1 Accounting issues can be considered for the following 2 different aspects:

a) institutional issues on cost recovery: this addresses the construction of tariff (who gets billed, how much, for which things, based on what information, etc...). Tariff issues include fairness, predictability (how well can subscribers forecast their network charges), practicality (of gathering the data and administering the tariff), incentives (e.g. encouraging off-peak use), and cost recovery goals (100% recovery, subsidization, profit making). Issues such as these are out of the scope of Systems Management and are not covered here; and

b) technical issues on the possible ATN usage measurement and reporting architectures that permit the ATN organizations to perform accounting in a private or co-operative way and according to a personal or a commonly agreed accounting policy.

5.4.1.2 Accounting management only deals with the technical aspects.

5.4.1.3 Requirements for the exchange of accounting management data across domains may exist in the following cases:

a) between an ATN service provider and its customers, electronic cross-domain accounting management service may be implemented for the provision of invoicing information, for the provision/request of detailed accounting records, etc.; and

b) between a group of ATN service providers which enter into partnership so as to share the accounting management structure, combine the accounting post-processing tasks of maintaining the accounting database, generating reports, distributing bills, collecting revenue, etc .., .minimize the billing interactions with common external users or service providers and simplify the internal redistribution of costs and benefits between partner organizations. In this case, electronic cross-domain accounting management services may be implemented, for instance, for the periodical exchange of accounting usage records.

5.4.1.4 The general case is however that the ATN organizations will perform the usage data collection and analysis activities on their own and interactions with other organizations will be limited to the exchange of bills between finance departments. Accounting management is therefore considered as a private process, and which is likely to vary among organizations based on their billing practices and on private policies.

5.4.1.5 It results from these considerations that there no need to standardize accounting management across organizations.

5.4.2 **Characteristics of Accounting Management**

5.4.2.1 This section highlights the characteristics of accounting management coordination in the ATN environment.

a) Exchange of accounting data is based on a bilateral agreement between organizations;

b) Exchange of raw usage counts is not necessary unless agreed upon by the organizations;

c) There is no identified need for real-time exchange of data for ATN network accounting management;

d) There is no identified requirement for cross-organizational manager to agent collection of accounting information;

e) If the exchange of raw data becomes necessary across organizations, data regarding other (third party) organizations must be extracted before forwarding;

f) Accounting typically involves additional processing besides the collection of metering data and thus raw data sharing at the boundary is not always reflected in the bills;

g) Data collected for accounting may be used for other purposes such as for performance analysis. In these cases, the data should be processed to protect an organization's privacy and security, and forwarded to the appropriate processes for analysis. Each organization is expected to protect information pertaining to other organizations; and

h) Due to the sensitivity of the data for accounting, exchange of raw data at this level is kept to a minimum and typically non-real time.

5.4.3 Accounting Management Coordination

5.4.3.1 As mentioned above, there is no identified need for a uniform accounting management exchange across all organizations participating in the ATN. However, this does not preclude any agreement formed among organizations to exchange for accounting management information. Typically, the agreement is specific to a region and selective organizations.

5.5 Configuration Management

5.5.1 Introduction

5.5.1.1 For a globally distributed ATN environment, certain configuration information in an ATN element can affect ATN elements in other organizations. This dependency of configuration information requires coordination among the participating organizations.

5.5.2 Characteristics of Configuration Management Coordination

5.5.2.1 This section highlights the characteristics of configuration management coordination in the ATN environment. These characteristics affect the timing for coordination, the types of information to be exchanged among organizations, and the design of the exchange mechanisms.

a) Configuration changes in the ATN ground network are time sensitive and need to be in effect by a stipulated deadline. Interactions among organizations are mostly non real-time. No need for immediate action or direct flow of changes from cross-domain network manager to agents has been identified;

b) Configuration changes typically affect services and are performed at low-peak hours within a domain. For the global ATN network, low-peak hours will differ from region to region. In co-ordinating configuration changes, sufficient time is needed to allow the affected organizations to implement the changes;

c) Configuration changes are likely to affect more than one ATN system. To avoid long down times for upgrading the configuration and for reducing errors in propagating the changes, automation for configuration changes within a domain is desirable; and

d) Configuration responsibilities are often shared between network administrators and network management operators. Within a domain, it is expected that coordination between the different functional groups will be encouraged to ensure continued ATN network operability.

5.5.3 Configuration Management Coordination Process

5.5.3.1 *General*

5.5.3.1.1 In the ATN, most of the management responsibilities are delegated to individual participating organizations. Each organization that owns and operates ATN equipment is held accountable for some minimum configuration management functions. Because configuration information for an ATN element can affect adjacent ATN elements, participating organizations are also expected to cooperate in co-ordinating certain aspects of configuration changes. These are discussed below.

5.5.3.1.2 Coordination for configuration of the ATN systems will be required on the following aspects:

a) The attribution of values to the ATN systems configuration parameters;

b) The modification to the current configurations; and

c) The exchange of information on the current configuration of ATN systems.

5.5.3.2 *Coordination for the attribution of values to ATN systems configuration parameters*

5.5.3.2.1 The attribution of values to certain ATN system configuration parameters may be dependent on or impact the configuration of ATN systems of other organizations. In certain cases, coordination will therefore be required among groups of organizations for reaching agreements on values of interdependent configuration parameters. This is an off-line activity which will likely be performed by the network administrators. The coordination should simply result in the production of documents recording the agreements.

5.5.3.3 ***Coordination for the modification to the current configurations***

5.5.3.3.1 **General**

5.5.3.3.1.1 Changes in the configuration of the ground ATN infrastructure occur for the following scenarios:

a) evolution/extension/enhancement of the ATN network;

b) network reconfiguration in case of problem; and

c) new aircraft are equipped with ATN systems and need to be recognized by the ground and air/ground systems.

5.5.3.3.1.2 The third scenario is considered to be a security management problem

5.5.3.3.2 **Changes in the configuration due to expansion and improvement of the network**

5.5.3.3.2.1 Changes in the configuration due to expansion and improvement of the network is an activity which will mainly involve network administrators. Changes that have cross-domain repercussions will necessitate coordination between the network administrators. Coordination will mainly consist in the analysis, agreement, and planning of the proposed changes. It should simply result in the production of documents recording the agreements on the changes, and describing the schedule and the procedures for the modifications.

5.5.3.3.3 **Reconfiguration in case of problem**

5.5.3.3.3.1 When a problem occurs in the network (e.g. failure of a router) it may sometimes be necessary for the network operators to switch from the current configuration to another backup one. Changes that have cross-domain repercussions will necessitate coordination between the network operators and possibly the regional supervisor, if any. Coordination will consist in the spontaneous set-up of a dialogue for discussion of the problem, agreement on a correction, and synchronization of recovery actions. The phone, the electronic mail, and the trouble tickets will be the tools used all along the reconfiguration process.

5.5.3.4 ***Exchange of information on the current configuration of ATN systems***

5.5.3.4.1 It is commonly observed that the sharing between organizations of information on the current configuration of their ATN infrastructure facilitates a number of network operation and planning activities: information on the configuration of a partner organization is typically useful for the control of coherence of configurations, for the analysis of the behavior of the network, for the understanding of problems, etc...

5.5.3.4.2 This is why it is assumed that the organizations participating into the ATN will be ready to share configuration information with other organizations.

5.5.3.4.3 In the ATN, the shared configuration information will be exchanged across the CMIP CDSM interface by retrieving the information from the Cross-Domain MIBs of the partner organizations.

5.5.3.5 ***Cross-Domain Configuration Management Services***

5.5.3.5.1 **Introduction**

5.5.3.5.1.1 In the ATN, the exchange of information on the current configuration of ATN systems will rely on the following basic Cross-Domain Management Service:

- The ATN Cross Domain Configuration Inquiry service

5.5.3.5.2 **Cross-Domain Configuration Inquiry Service**

5.5.3.5.2.1 **Service Definition**

5.5.3.5.2.1.1 The ATN CNM Configuration Inquiry service provides an ATN organization with the capability to acquire and maintain certain information elements about the network and systems configuration of another ATN organization.

5.5.3.5.2.2 **Functional Description**

5.5.3.5.2.2.1 The following functions are associated with the configuration inquiry service:

a) Retrieve configuration information function:

This function allows an external ATN organization to acquire selectively (a) part(s) of the shared configuration information made accessible in the Cross-Domain MIB of the local ATN organization; and

b) Update configuration update function:

The function allows the local ATN organization to inform automatically other ATN organizations of a spontaneous change in the local configuration.

5.6 **Security Management**

5.6.1 **Introduction**

5.6.1.1 In the area of security management, the responsibility of the network managers is to coordinate and control the security mechanisms built into the configuration of ATN networks and systems under their management control.

5.6.1.2 In this area, it is important to distinguish between the ‘management of the security’ and the ‘security of the management’.

5.6.1.3 With regard to the former, management is required to maintain a secure environment though management services of themselves do not confer security. Management's task is to support the environment which can provide the security services effectively. Therefore security management may be concerned to provide the tools which can, for example, provide the safe distribution of authentication keys, but it is not concerned with the application of those keys in authentication algorithms. Security management also provides mechanisms to respond to alarms which may be generated whenever security is being compromised. It helps to maintain historic records of security related events which take place in the network so that independent audits of security can be carried out.

5.6.1.4 The 'security of management' is concerned with the protection and security of the network management processes themselves. If the network management system becomes compromised, it can have grave consequences for the health and security of the network generally. In addition, the network management processes may be conveying information that is confidential or proprietary to a particular management domain. The security of management addresses the control of access to system resources through physical security procedures, authentication techniques, and access authorization policies.

5.6.2 **Characteristics of Security Management**

5.6.2.1 This section highlights the characteristics of security management coordination in the ATN environment:

a) Systems Management protocols are not used in the ATN, for the cross-domain exchange of security keys. In the ATN, the exchange of authentication information is achieved using mechanisms (e.g. directory services) that are outside the scope of ATN systems management;

b) Due to the sensitivity of the data, exchange of access right information and operating parameters of security services and mechanisms is considered as a non real-time activity, which is achieved using mechanisms that are outside the scope of ATN systems management;

c) Due to the sensitivity of the data, exchange of security audit record or security alarms is considered as a non real-time activity, which is achieved using mechanisms that are outside the scope of ATN systems management standardization;

d) However, this does not preclude any agreement formed among organizations to exchange for security management information in real time, using locally defined Cross-Domain System Management services. Typically, the agreement is specific to a region and selective organizations; and

e) Security of management is achieved through the combination of authentication mechanisms and access control mechanisms. The specification of these mechanisms is outside the scope of ATN systems management.

5.6.3 Security Management Coordination

5.6.3.1 Security management is considered to be an individual process performed locally by each ATN organization with no general requirement or desire for the real-time exchange of security management information. In the general case, the cross-domain exchange of security management information is therefore an off line activity involving the network administrators or the security managers. However, this does not preclude any agreement formed among organizations to exchange for security management information. Typically, the agreement is specific to a region and selective organizations.

5.6.3.2 Locally within each ATN organization, security management must keep account of activity, or attempted activity, and detect and recover from attempted or successful security attacks. This includes the following local functions related to the maintenance of security information:

- event logging;
- monitoring security audit trails;
- monitoring usage and the users of security-related resources;
- reporting security violations;
- receiving notification of security violations;
- maintaining and examining security logs;
- maintaining backup copies for all or part of the security-related files; and
- managing the ATN Systems MIB access control service by maintaining general user profile and usage profiles for specific resources.

6. COEXISTENCE WITH LOCAL SYSTEMS MANAGEMENTS

6.1 Introduction

6.1.1 This section provides guidelines for the coexistence of the ATN Cross-Domain Systems Management mechanisms with local Systems Management mechanisms potentially used within an ATN administrative management domain.

6.2 Guidelines on technical accommodation of SNMP-based systems

6.2.1 Problem Statement

6.2.1.1 CMIP is the standard protocol adopted by ICAO for the exchange of management information across ATN management domain. However, this does not preclude the use of other protocols for the management of individual pieces of equipment within an ATN management domain. The Simple

Network Management Protocol (SNMP), or one of its successors, developed by the Internet Community is an example of an alternative protocol likely to be used "locally" within an ATN management domain.

6.2.1.2 Figure 6-2.1 illustrates possible configurations within a Management Domain where SNMP is used for intra-domain management and CMIP is used for inter-domain management. With such types of configuration, two main issues have to be considered:

a) The Boundary Management System has to handle two management protocols: SNMP for communicating with the local SNMP Agents or the local SNMP-based Manager and CMIP for accessing the Cross-Domain MIB of adjacent Management Domains and for communicating with aircraft CMIP-based management systems. The Boundary Management System needs, for consolidating the Cross-Domain MIB, to collect periodically local management information either directly from the equipment distributed in the domain or indirectly from the local SNMP-based Manager; and

b) Translation between the SNMP-compliant and the CMIP-compliant MIB formats may have to be performed on the management information.

6.2.1.3 It must be noted that these issues may have to be considered also when CMIP is internally used for managing local ATN equipment. This is because the local ATN infrastructure may include off-the-shelf pieces of equipment (e.g. intra-domain routers) that only support SNMP. This particular case is illustrated in the figure with the example of the Boundary Management System #2.

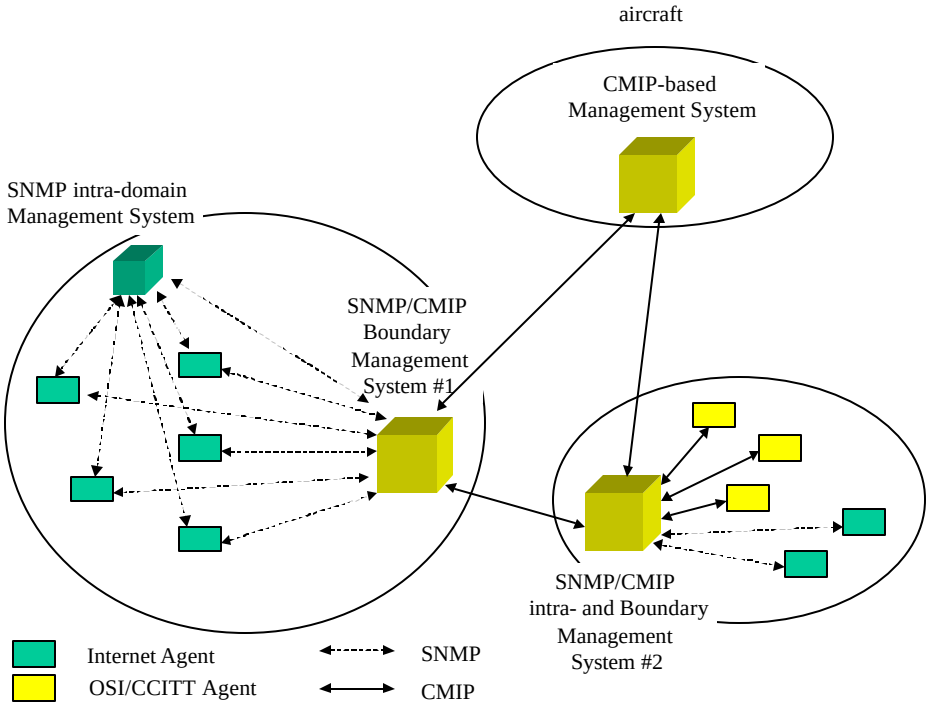

Figure 6.2-1. Possible ATN Systems Management Environments

6.2.2 ISO/CCITT – Internet Management Coexistence Strategy

6.2.2.1 *Introduction*

6.2.2.1.1 The Telemanagement Forum and ISO/CCITT have specified an approach and tools for SNMP/CMIP accommodation. It is based on the one hand on algorithms that ease automatic translation of MIBs between the two environments and on the other hand on mechanisms for implementing CMIP/SNMP protocol conversion in a "proxy" component. The proxy based on the dual knowledge of the MIB as formatted in the SNMP Agents and as formatted in the CMIP Manager emulates CMIP features missing in SNMP, such as the creation and deletion of MO instances, the notification of events, the invocation of actions as well as the scoping and filtering functions.

6.2.2.2 *MIB Translation Procedures*

6.2.2.2.1 **Overview**

6.2.2.2.1.1 The foundation of ISO/CCITT-Internet Management coexistence strategy is provided by the following two sets of Management Information Base (MIB) translation procedures:

- a set of translation procedures for converting MIBs from Internet MIB macro format into ISO/CCITT GDMO template format. These procedures could be used to translate existing proprietary Internet MIBs description into GDMO MIBs; and

- a set of translation procedures for converting MIBs from ISO/CCITT GDMO template format into Internet MIB macro format. These procedures could be used to translate GDMO MIBs into Internet MIBs.

6.2.2.2.1.2 This is illustrated by Figure 6.2-2.

6.2.2.2.2 **Translation of GDMO MIBs to SNMP MIBs**

6.2.2.2.2.1 It is possible that ATN organizations already operating the Internet management protocol for managing their existing communication infrastructure will choose to keep SNMP to manage the ATN components within their Management Domain. SNMP Agents will be installed in ATN Routers and End Systems providing SNMP Managers with a means of controlling remotely the operation of the ATN components.

6.2.2.2.2.2 In this context, a translation of GDMO MIBs to SNMP MIBs may be required.

6.2.2.2.2.3 The NMF CS341 specifies a method for translating ISO/CCITT GDMO MIB specifications to SNMPv1 and SNMPv2 MIB macro specifications. The translation rules specify the following steps:

a) Object registration and naming conventions;

b) Managed Object Class and Attributes template translation;

c) Specification of ACTIONS and NOTIFICATIONS in the Internet MIB; and

d) Support of CMISE DELETE and CREATE operations in the Internet MIB, etc.

6.2.2.2.2.4 The TeleManagement Forum CS341 provides core methodology such that a GDMO template specification can be translated to Internet MIB macro notation. While entirely mechanized translation from an ISO/CCITT GDMO MIB to an SNMP MIB is not always possible, the intent is to mechanize the process as much as possible and supply reasonable defaults that may be tempered by human judgement.

6.2.2.2.3 **Translation of Internet MIBs to ISO/CCITT MIBs**

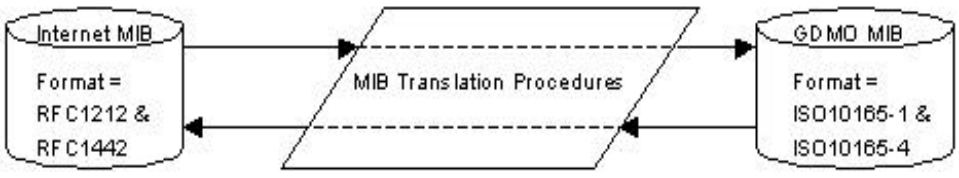

Figure 6.2-2. MIB translation procedures

6.2.2.2.3.1 ATN Management Administrations will have to integrate within their Management Domain the management of many different devices providing different management interfaces such as CMIP, SNMP or proprietary protocols. Some devices provide by default an SNMP agent and do not have the capability to integrate other management protocols.

6.2.2.2.3.2 ATN organizations using CMIP internally as the systems management protocol are facing the problem of interfacing their CMIP Manager with those SNMP-managed devices. The ISO/CCITT to Internet Proxy solution is an appropriate technical solution to address this problem. It is however necessary to provide the proxy with a description of the MIB supported by the devices in the GDMO format.

6.2.2.2.3.3 Procedures are defined in the TeleManagement Forum Component Set 341 to translate almost automatically SNMP MIBs into GDMO MIBs. The Internet MIB-II translated in GDMO format is provided as part of the TeleManagement Forum Component Set 341.

6.2.2.2.3.4 The translation rules specify the following steps:

a) Object registration and naming conventions;

b) Internet Groups, Object Class and Attributes translation using GDMO template;

c) Translation of Traps/Notifications;

d) Creation of a Containment Tree;

e) Internet Name binding specification; and

f) Cross-references to ASN.1 documents, etc.

6.2.2.3 ***The OSI/CCITT to Internet Proxy solution***

6.2.2.3.1 **Overview**

6.2.2.3.1.1 In the situations described 6.2.1, ATN systems management may require an integrated and unified view of the ATN network, despite differences in management protocol and information structure of CMIP and SNMP.

6.2.2.3.1.2 Integrated management can be facilitated by the development of “proxy” mechanisms which translate between functionally equivalent service, protocol, and SMI differences to create this unified view.

6.2.2.3.1.3 MIB translation procedures can be used to support proxy management, as well as to take advantage of existing MIB definition. If SNMP is used to manage ATN routers and End Systems for which a GDMO-based MIB has been defined (see the SNMP Management System in Figure 6.2-1), theMIB translation procedures will be used to convert the MIBs into an Internet MIB as input to the SNMP Agents.

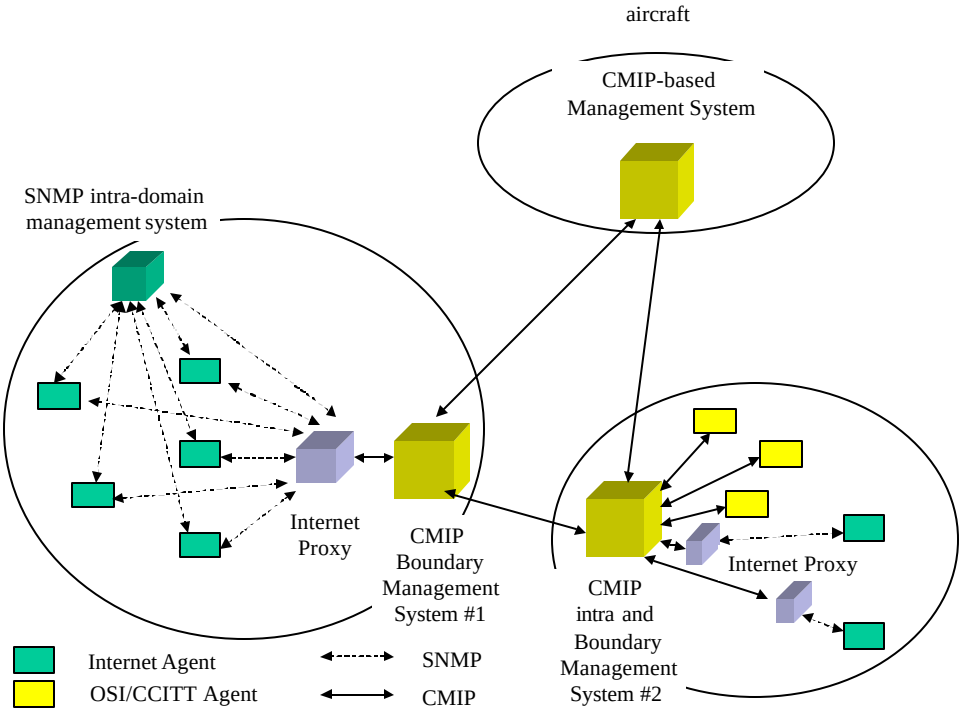

Figure 6.2-3. Use of the OSI/CCITT to Internet Proxy

6.2.2.3.1.4 Figure 6.2-3 illustrates how Internet proxies can be configured as front systems interfacing CMIP Managers to SNMP Agents.

6.2.2.3.2 **Proxy Management Model**

6.2.2.3.2.1 The basic model for ISO/CCITT to Internet proxy management is illustrated in Figure 6.2-4.

6.2.2.3.2.2 This ISO/CCITT to Internet proxy provides emulation of CMIS services by mapping to the corresponding SNMP message(s) necessary to carry out the service request. The service emulation allows management of Internet objects by an ISO/CCITT manager. The left hand side of the proxy behaves like an ISO/CCITT agent, communicating with the ISO/CCITT manager using CMIP protocols. The right hand side of the proxy behaves like an Internet manager, communicating with the Internet agent using SNMP protocols.

6.2.2.3.2.3 The proxy relies on the existence of a pair of directly-related MIB definitions (Internet MIB and ISO/CCITT GDMO MIB). The proxy uses these MIB definitions and rules to provide run-time translation of management information carried in service requests and responses.

6.2.2.3.2.4 The proxy is designed with a specified interface between the proxy and the underlying protocol stacks, and so deals primarily in terms of CMIS services and SNMP “services”. The proxy emulates

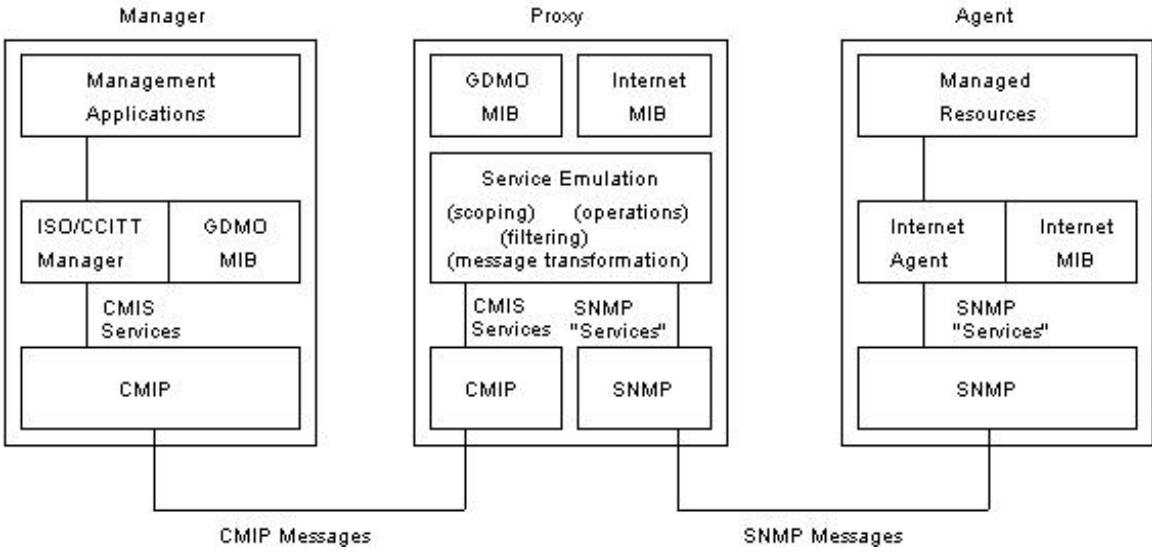

Figure 6.2-4. Proxy management model

CMIS services by performing a mapping process which must be tailored for each protocol (for example, SNMPv1 and SNMPv2 are variants of the same protocol mapping process).

6.2.2.3.2.5 The proxy performs the following functions:

- application-association handling;
- scoping and filtering;
- verification of the existence of MO instances;
- processing CMISE operations;
- incoming trap/notifications translations;
- derivation of SNMP Request parameters;
- derivation of CMIS parameters;
- error message translation;
- event forwarding discriminators (EFD) management on behalf of the agent; and
- log management, etc.

6.2.2.3.2.6 As shown in Figure 6.2-3, the proxy may be integrated as front system of the CMIP manager or as front system of the SNMP agent. In the former case, the proxy polls locally the SNMP devices.

6.2.2.3.2.7 An ISO/CCITT to Internet Proxy implementation can support different levels of CMIS service emulation:

- a basic proxy emulates CMIS kernel services, plus supports for scoped CMIS Get and single-assertion filtered CMIS M-GET on the objectClass attribute. This level of service might be sufficient for a proxy used to consolidate the Cross-Domain MIB; and

- an enhanced proxy which emulates all CMIS services, including scoping and filtering on all applicable CMIS services. This level of service is required for a proxy used to control in an ATN Management Domain both SNMP and CMIP managed systems.

6.2.2.3.2.8 The Proxy-based approach is proposed by the TeleManagement Forum and ISO/CCITT to accommodate SNMP in a CMIP environment. It is documented in the TeleManagement Forum standards and referenced as the TeleManagement Forum Component Set 341.

6.2.2.3.2.9 Many commercial Systems Management products claiming the support of both SNMP and CMIP have implemented the TeleManagement Forum Component Set to allow CMIP-based managers to manage SNMP-based components.

— — — — — — — —