)WG2 WP-478

ATNP/JWG/WP 9-4
September 24, 1998

AERONAUTICAL TELECOMMUNICATION NETWORK PANEL

JOINT SUB- GROUP ON SYSTEM MANAGEMENT

Toulouse, France, 06 October 1998

PRELIMINARY DRAFT VERSION 1.0 ATN SYSTEM MANAGEMENT -- CONCEPT OF OPERATIONS

Agenda Item: 6.3

Prepared by: James Moulton

Presented by: James Moulton

SUMMARY

This latest draft of the CONOPs is based on the previous draft and the results of the meeting in Toulouse. Experts are requested to review this document for approval as Version 1.0 at the meeting in Bordeaux

Guidance Material for Core/SV 1

Concept of Operations

DRAFT 1.0p

1 Introduction

1.1 Purpose and Scope

The purpose of this document is to provide a basic understanding of how system management will be needed in the distributed ATN environment. In providing that understanding, this document addresses the concepts of ATN management operation in a way that will guide future SARPs development.

This document describes the overall system management concepts. The need to definition functions based on the concepts may be either SARPs material or Guidance Material. This document does not distinguish between those items that should be in SARPs and those items that should be in Guidance Material. Since this document is meant to become part of the consolidated ATN Guidance Material, the separation of functions as to whether they belong in SARPs of Guidance Material will be included in a later version.

1.2 Structure of Document

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 system management operations; section 5 presents the System Management model based on the ISO model; section 6 presents examples of ATN management information; and Section 7 presents the conclusions.

1.3 Definitions

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

1.3.1 Domains

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

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

1.4 Model

2 Overview ATN Systems Management

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.

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.

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

1. The appropriate design of the communications infrastructure and components to anticipate and provide sufficient capacity.
2. The implementation of operational procedures to control resource allocation not requiring specific management functions or networking technology.
3. The implementation of local automated or operator controlled management functions in communications systems.
4. The implementation of management functions in ATN systems that allow the exchange of systems management information based on a standardised 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.).

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

3 ATN Environment

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

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.

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

3.1 ATN Organizations

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, commercial airlines, or ATN service providers.

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

3.1.1 Administrative and Regional Domains

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. In the case of the ATN, an Administrative Domain can be defined in terms of the authority responsible for assigning NSAP addresses at the CAA or airline level.

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

3.1.2 Management Domains

3.1.2.1 Basic Concept

A *Management Domain* is comprised of a portion of the ATN that is managed by a single entity.

3.1.2.2 Management Domain Hierarchy

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.

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

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.

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 System Management. It is within this domain that management information is gathered, reduced, and analyzed to determine the operational readiness of that portion of the ATN. Most importantly, this is the central source of management information shared with other domains. An Administrative Domain may be contained in one or more Regional Management Domains.

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 Large Scale Structure of the ATN

There are many possible ways for the ATN to be globally implemented. Figure 3-1 illustrates one possible large-scale structure of an example subset of the ATN environment that can be used for discussion purposes.

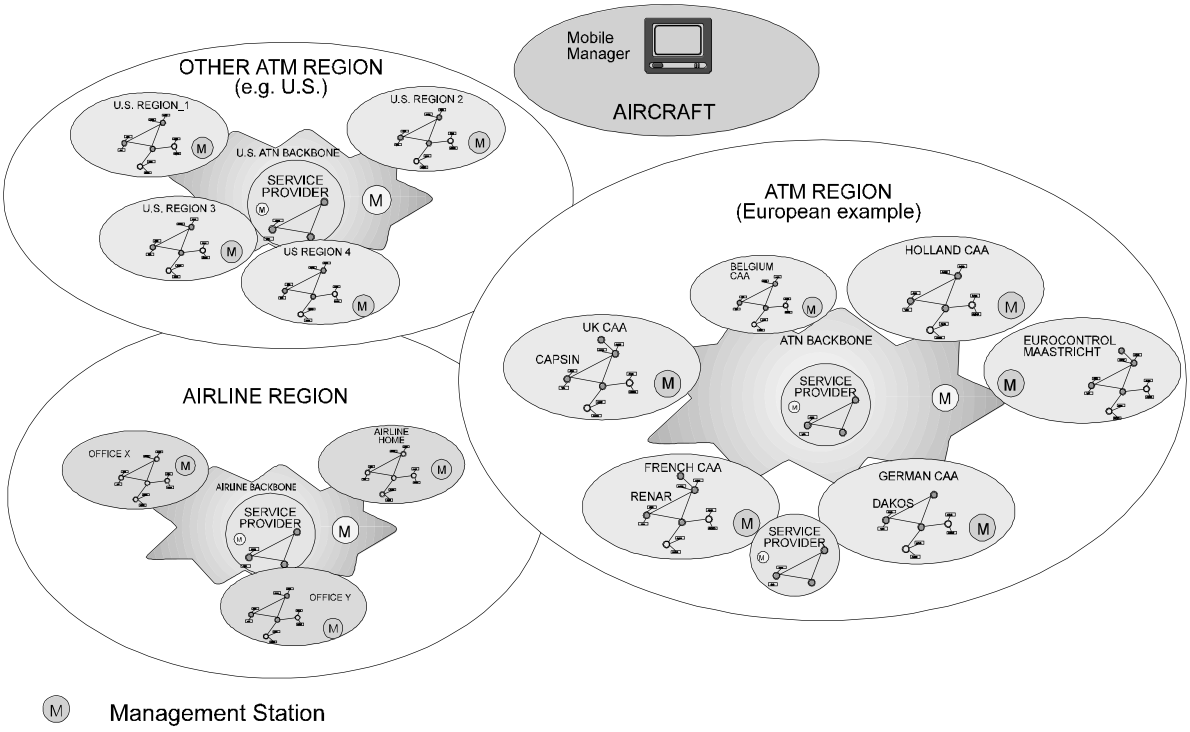


Figure 3-1 - Large scale ATN structure

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

- indivdual (CAA, airline, aircraft, and service provider) management domains, and
- regional (CAA, airline, and service provider) management domains.

Note: Aircraft are considered in a manner indistinguishable from any other individual management domain.

> *Note: An individual management domain may belong to one (or more) regional management domains.*

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

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

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

3.3 The Structure of Managers, Administrators and Institutions

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

Figure 3-2 presents a possible hierarchy of Managers, Administrators and Institutions.

There is a 2 level hierarchy of active managers; Area Administrators and Network Managers which operate according to contracts, agreements and policies made by Management Domains.

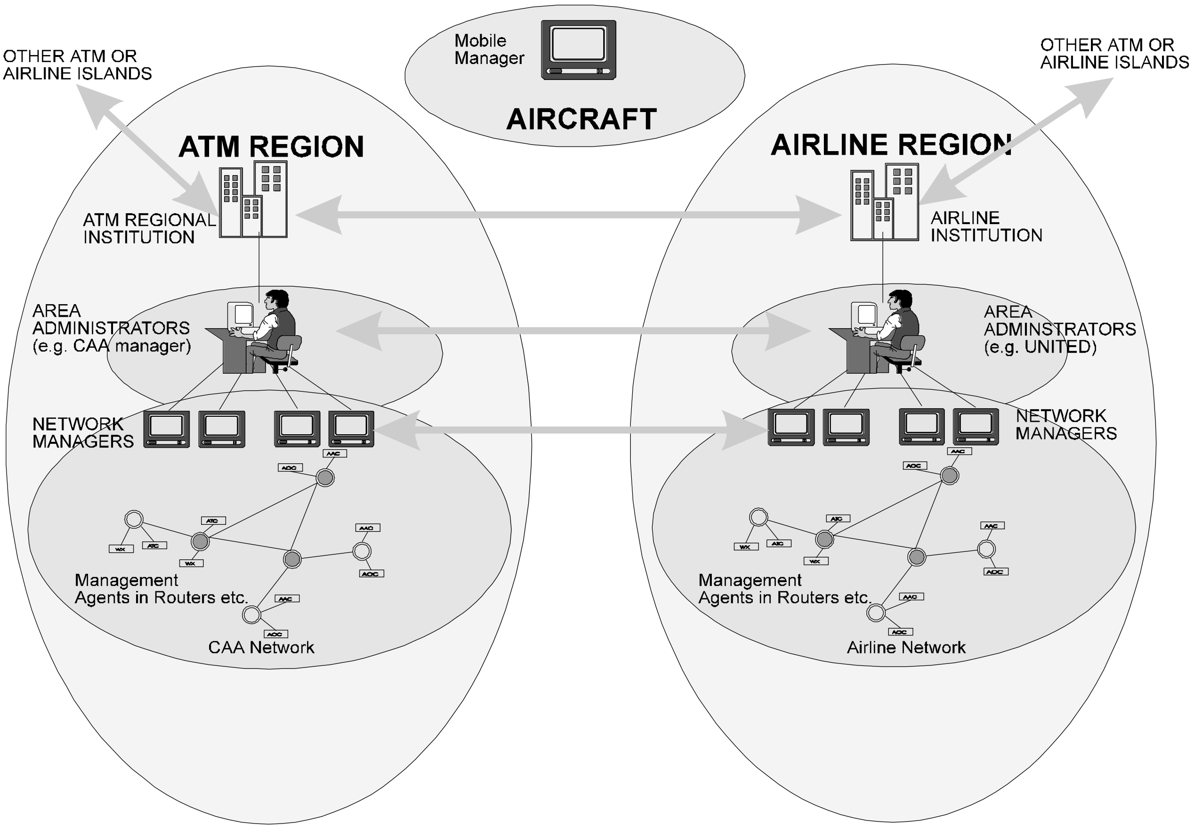

OTHER ATM OR AIRLINE ISLANDS
Mobile Manager
AIRCRAFT
OTHER ATM OR AIRLINE ISLANDS
ATM REGION
AIRLINE REGION
ATM REGIONAL INSTITUTION
AIRLINE INSTITUTION
AREA ADMINISTRATORS (e.g. CAA manager)
AREA ADMINSTRATORS (e.g. UNITED)
NETWORK MANAGERS
NETWORK MANAGERS
Management Agents in Routers etc.
CAA Network
Management Agents in Routers etc.
Airline Network

Figure 3-2 - Structure of ATN Authorities

3.3.1 Management on the Ground

3.3.1.1 Regional

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

Every Regional Management Domain will have a single REGIONAL MANAGER which has ultimate responsibility for the operation of the entities under its control.

For Regional Management Domains, a single REGIONAL INSTITUTION will have the ultimate responsibility for the operation of the REGION. These Institutions may delegate, by agreement, responsibility for active 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 active managers of a further hierarchy of managers.*

REGIONAL MANAGERS (or INSTITUTIONS) are the responsible authority for:

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

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

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).

3.3.1.2 Individual Management Domains

Every Individual Management Domain will have a single Manager which has ultimate responsibility for the operation of the entities within its domain. The designated Manager will set policy and exchange management information with other Management Domains.

3.3.1.2.1 Area Administrators

An area consists of a subset of (either an individual or regional) management domain.

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

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 QOS, secure interaction and other policies common to domains,
- 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,
- implement access control between administrators in different areas.

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

3.3.1.2.2 Network Managers

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

Every NETWORK will have a NETWORK MANAGER which has responsibility for the detailed operation of the equipment in the network.

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.

NETWORK MANAGERs hide the details of the normal operation of network equipment from ADMINISTRATORs.

Distributed systems management of ATN equipment within organisations 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).*

3.3.2 Management in the Air

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

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

The exchange of management information over the air-ground link is subject to the same procedures as for the exchange on the ground. However, ground-based managers should limit requests of airborne managers to specific data requests.

For non-commercial, the mechanisms for real-time operational fault and event reporting to ATC authorities over the air-ground link must be standardised (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 standardised.

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 commercial aircraft and ATC authorities and Airborne systems are limited to event reports initiated by the Aircraft.

In the flight deck environment, mobile managers will need to be autonomous applications requiring a minimal level of human intervention.

Airborne systems will not manage ground systems (although fault reports may be exchanged). Airborne systems may need to access ground-based management information.

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.

Operational parameters to be used in flight may be uploaded at the gate for use by mobile managers.

3.3.3 Management of the Air Ground Link

4 ATN System Management Concept of Operation

4.1 System Management Concepts

From the previous section, the ATN consists of a set of autonomous networks. Each network would be managed locally.

The core concept underlying the ATN System Management concept of operations is that there is a need to standardise and exchange management information.

System Management can be viewed as a multi-part problem:

- definition of management information,
- exchange of management information, and
- use of management information.

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.

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

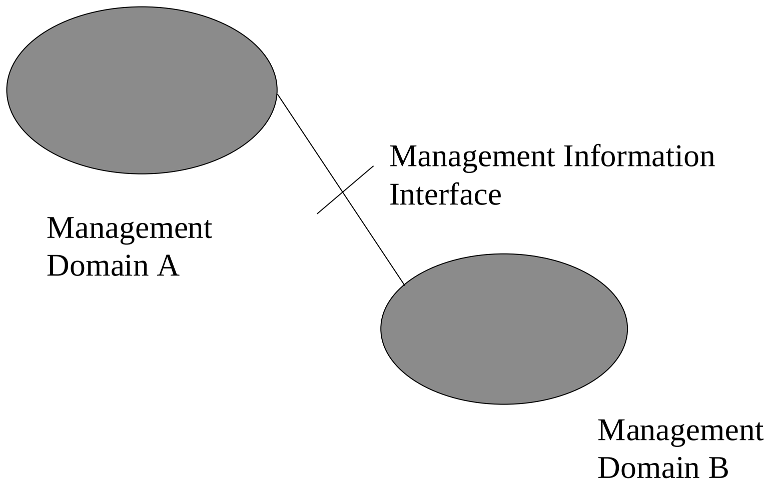


Figure 4-1 Management Information Interface

A basic principle underlying the structure of ATN systems management is the distinction between the two groups of functions designated as "off-line" and "on-line" management functions.

On-line management refers to functions that shall be executed in a short time period in order to maintain the level of service required from the ATN. This necessitates the rapid exchange of management information between ATN Network Managers.

Off-line functions do not need to be executed in a short time period. These relate to medium and long-term requirements and include, e.g., collection and processing of information from ATN Management Centres (statistics, inventory, etc.), preparation of configuration proposals (capacity and routing) and provision of technical support (certification, consultancy, etc.).

The detailed definition of the interface information and how that information is exchanged is given in Section xx.

4.2 The ATN Systems Management Model

4.2.1 Principles

The ATN Systems Management Model is based on the OSI Model described in ISO/IEC 10040, Systems Management Overview. Where management information exchange is required in an on-line (or “real-time) environment, CMIS/CMIP is used. Network management is accomplished through a system which is made up of at least these five components:

- The *Managed Resources*, which can include network devices such as ATN routers, as well as other equipment and applications (software) which requires management.
- A set of *Managed Objects* (MO). MOs are abstractions of the actual managed resources. These software abstractions provide the management interface to the real resources being managed. For example, a set of MOs have been defined for the management of ATN routers. Each ATN router MO represents specific data associated with the router “managed resource”.
- A management database in the form of a *Management Information Base* (MIB). The MIB is composed of the MOs, organised in an efficient manner to allow ease of retrieval of the data contained in each object.
- A management *Agent,* which is a software entity, residing in the device to be managed. The agent accesses management data from the managed device and converts this raw data into a MIB-compatible format. Agents respond to queries (from managers) regarding management data. Agents also notify managers when significant events take place.
- A *Manager* application, which resides on a *Management Workstation,* located at an organization’s (e.g. airline, civil aviation authority) operations control center. The manager is responsible for receiving and responding to fault notifications, initiating queries to accomplish the retrieval of management data, and providing an interface (usually a graphical interface) to the personnel in the operations control center.

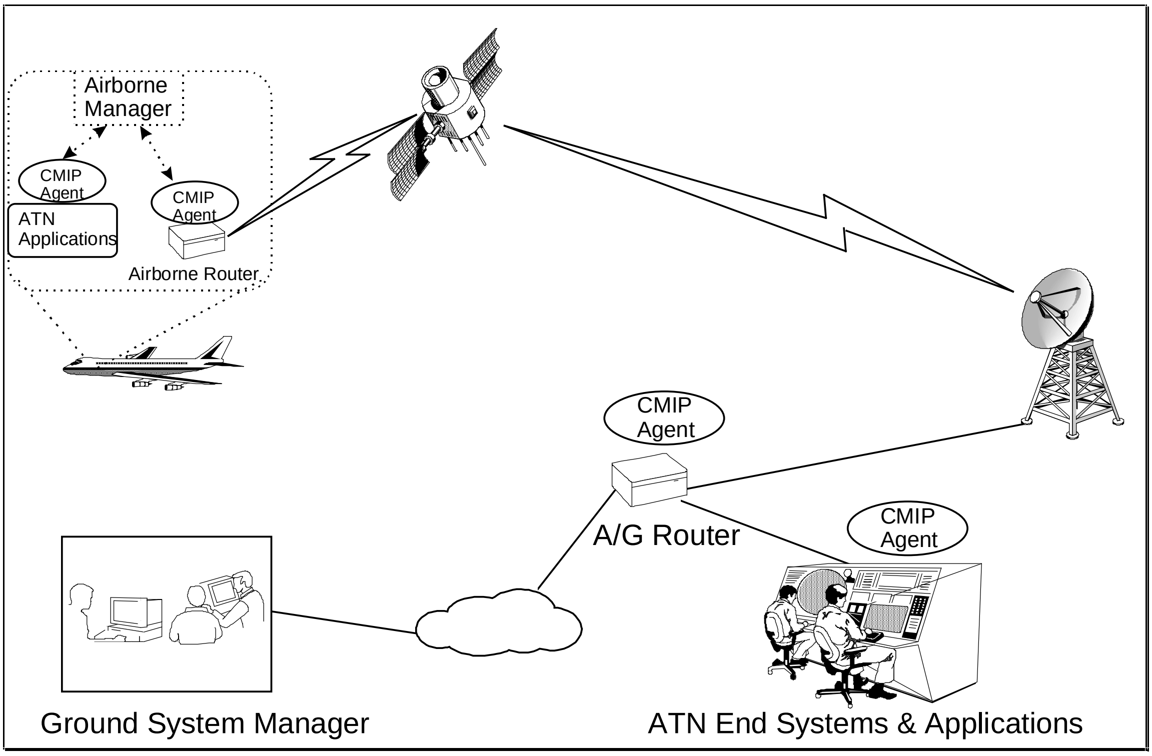


Figure 4-2

Figure 1-1 presents a systems management scenario. *Systems management* refers to the management of equipment resources that include but are not limited to network devices. Systems management also refers to the management of applications. Achieving an integrated *systems* management approach is an important goal. Just as ATN will benefit from NM, the ATN applications, as well as many other aviation systems stand to benefit from an integrated network and systems management (NSM) 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 avionics on aircraft. Collecting this data by using integrated NSM provides the opportunity for immediate correlation of the data, thereby improving efficiency and enhancing fault and performance capabilities.

4.2.2 ISO Standards Overview

There are four main groupings within the set of management standards. They are:

- a set of ISO standards relating to the framework for Systems Management;
- a set of ISO standards relating to the specification of managed objects;
- a set of ISO standards specifying systems management functions;
- a set of application layer service and protocol standards for communicating information relating to management functions.

An overview of the ISO standards for OSI Systems Management is illustrated in Figure 12.1.

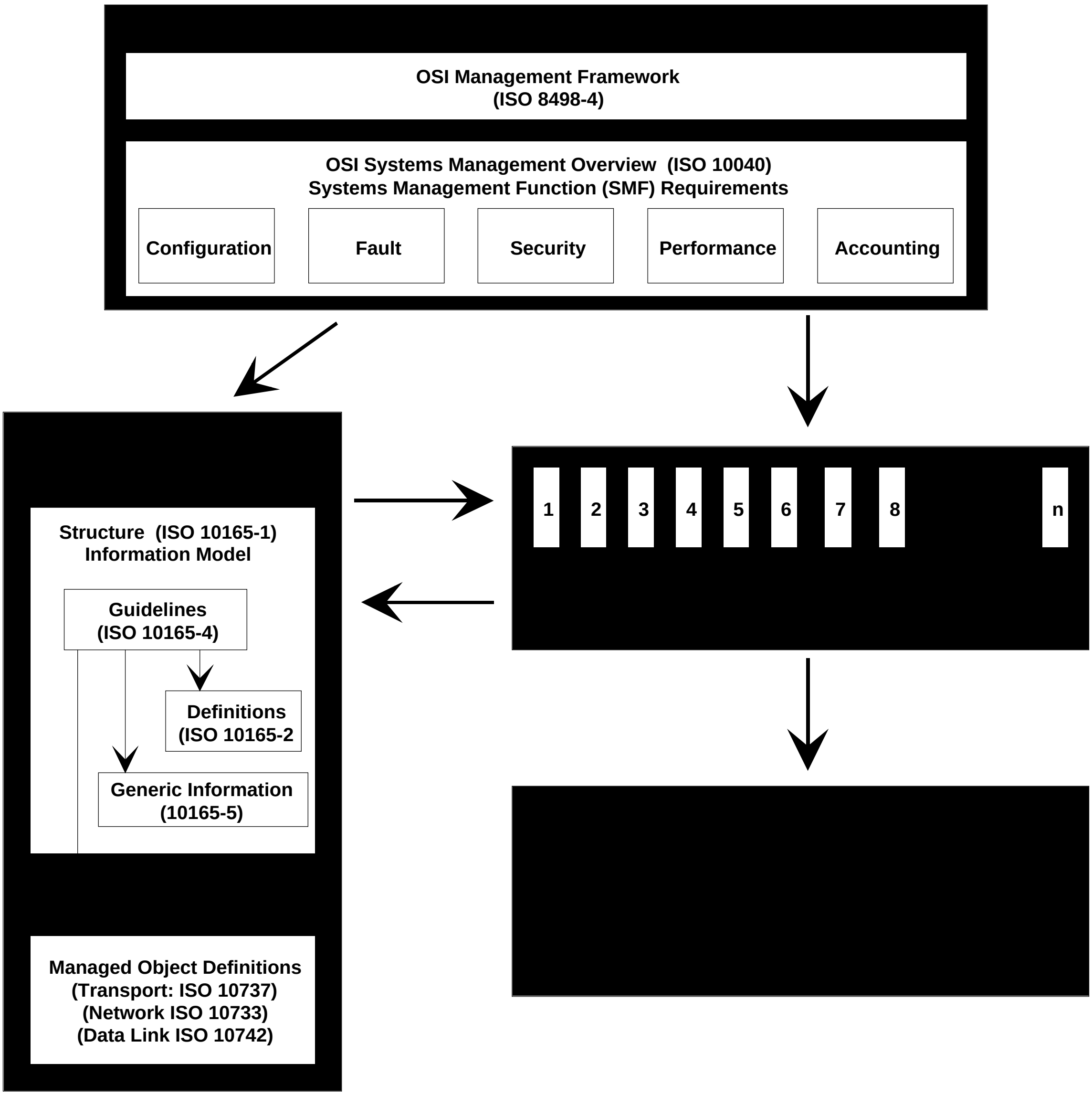


Figure 431: System Management Standards

4.2.3 Model Overview

This section presents a brief description of the basic elements of a network management system. The primary elements of any network management system include:

- Manager Station
- Management Agent

- Managed Resources
- Management Information Base
- Management Protocol

The following sections contain a brief summary of the important aspects of each of the primary elements listed above.

4.2.3.1 Management Station

A network manager workstation hosts one or more management applications. The application(s) provide the required set of management functions. The most significant functions of a management workstation are:

- Data collection
- Fault diagnosis and recovery
- Resource configuration
- Performance analysis
- Trend analysis and forecasting
- Graphical display of managed resources
- Integration of multiple data sources
- Automated correlation of data
- Integration of management applications

4.2.3.2 Management Agent

A management agent is usually co-located with the managed resource. The primary elements of a management agent include:

- MIB data structures
- Data retrieval module
- Management communications protocol module
- event-based or polling-based monitoring module
- Management Protocol: SNMP, CMIP, Proxy, Log readers, CORBA, Web Protocols, etc.

Figure 4-4 depicts the relationship between a management workstation, the management application(s), agents and the managed resources.

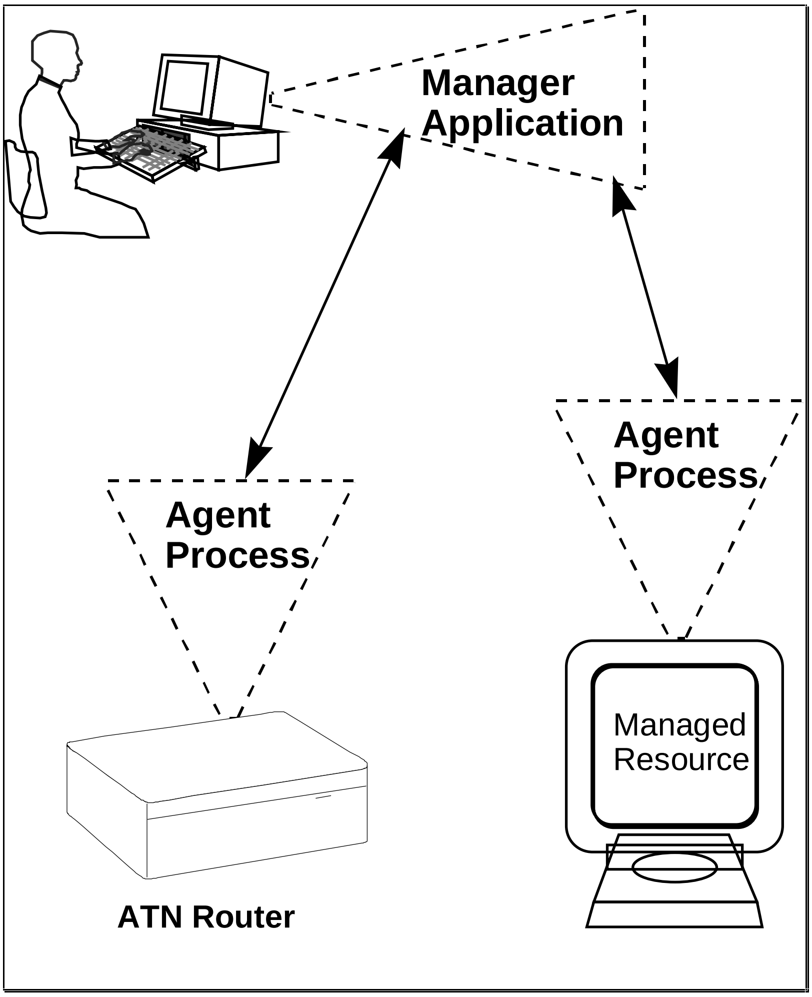


Figure 4-4

4.2.3.3 Managed Resources

Examples of managed resources:

- Host Computers
- Network devices like routers, switches, hubs
- System resources like memory, disk space, software licenses
- Applications
- Distributed Applications (e.g., ATN apps.)

4.2.3.4 Management Information Base

The Management Information Base (MIB), is a standardized, structured abstraction of the managed resources of interest. MIBs function as collections of access points at the agent, for the manager.

Within the agent, the MIB is a data structure providing access to specific resources in the form of variables or objects. Managers must implement the same MIBs as the agents with whom they need to communicate. Figure 4-5 illustrates the concept of a MIB.

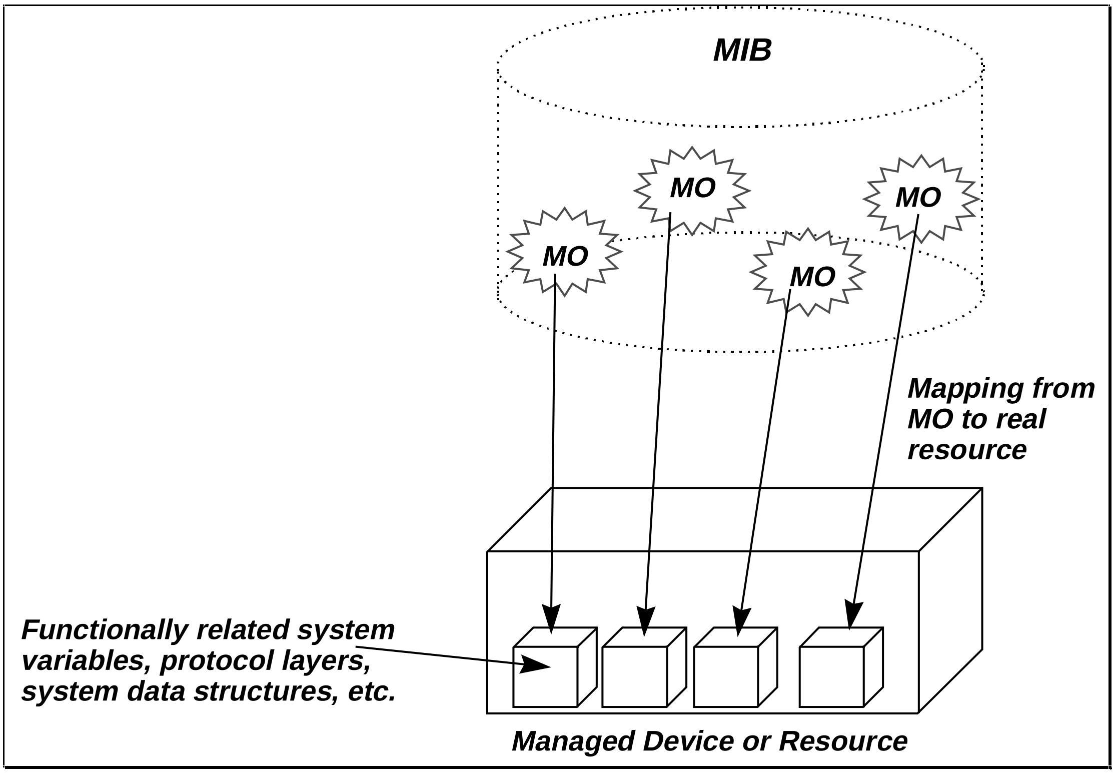

MIB
MO
MO
MO
MO
Mapping from MO to real resource
Functionally related system variables, protocol layers, system data structures, etc.
Managed Device or Resource

Figure 4-5

Given the Managed Object (MO) concept, several primitive types of MO have been identified:

OSI specific MOs: those defined in international standards to represent OSI protocol and system resources;

OSI generic MOs: those defined in OSI Systems Management standards for use in defining specific protocol and system MOs;

ATN MOs: MOs defined in ATN standards to represent ATN-specific protocol and system resources;

Administrative MOs: MOs defined to represent a selection or summary of information or a modification of the behaviour available in one or more other MOs, so as to meet a specific requirement for systems management.

4.2.3.5 Management Protocol

The management protocol provides the communication mechanism for the network manager and agent, by specifying the message format, command set and flow of control. Examples of current network management protocols include:

- Common Information Management Protocol (chosen for the ATN), and
- Simple Network Management Protocol (SNMP).

4.2.4 Management Functions

The user requirements for systems management must be satisfied by systems management functions. These functions may be used by an application in a centralized or distributed management environment to interact for the purposes of system management.

Management information is used by the system manager to assist in making management decisions and to communicate those decisions to the system resources. Functionality is required in the following areas:

- fault management,
- accounting management,
- configuration management,
- performance management,
- security management.

4.3 General Framework for the exchange of Management Information with a summary MIB

4.3.1 Principle of the approach

The Summary MIB concept assumes that every organization will operate, in its Network Operation Centre, a central Network Management Station that has the capability to collect, via local System Management procedure, management information from the ATN equipment distributed in the local domain.

It is then assumed that the information gathered from the individual pieces of equipment, can be filtered, and processed for updating one global MIB providing an aggregated summary of the management information.

The principle for the exchange of management information across domain assumes then each organisation would provide other organisations with access to such a summary MIB modelling the overall characteristics of its ATN domain. The summary MIBs would be periodically updated by the local organisation. Organisations that have been granted permission to access the Summary MIB of another organization, would then be allowed to read, periodically or on specific need occurrence basis, the content of the Summary MIB (SMIB).

4.3.2 Functional architecture

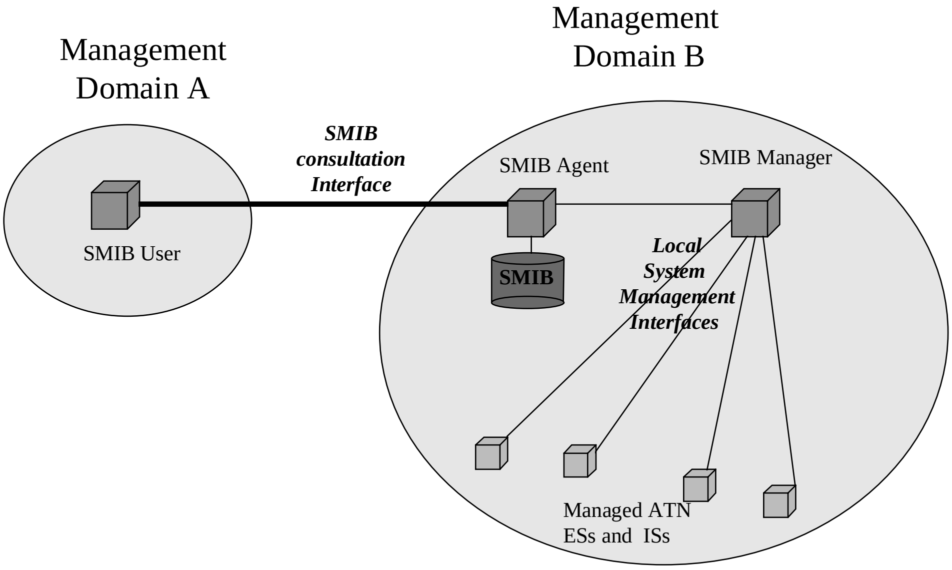
The functional architecture for the SMIB-based cross-domain exchange of management information is based on several function blocks implemented either by the organisation providing access to its SMIB or by the organisations retrieving information from this SMIB. This is depicted in figure 1.

In this document, the following definitions apply:

> **SMIB User**: This function block is a Management System operating in the manager role and to be implemented by organisations willing to retrieve information from the SMIB maintained by other organisations
>
> **SMIB Agent**: This Function block is a Management System operating in the Agent role which performs the CMISE operations on the local SMIB. The SMIB Agent handles information retrieval requests from SMIB Users and information Update Requests from the SMIB Manager. This system is implemented by the organisation providing SMIB services.
>
> **SMIB Manager**: This Function block is a Management System operating in the Manager role which is implemented by the organisation providing SMIB services. It retrieves necessary management information from the managed ATN equipment in the local domain, processes it, and generates information update requests to the SMIB agent.

The SMIB Agent and the SMIB Manager can be collocated on the same system. However, implementing these 2 functional blocks on 2 separate systems may present the following 2 advantages:

1. A separate SMIB Agent will constitute a security firewall for the local organisation. This eliminates the potential risk of an external user succeeding in taking some level of control and command on the SMIB Manager and hence on the local ATN network. This also eliminates the risk of an invalid external operation causing the failure of the local Manager.
2. The Network Management protocol used within the domain for the management of individual pieces of equipment may be different from the one that has been agreed for the exchange of management information across domain boundaries. As an example, SNMP may be the local protocol in use, whereas CMIP has been agreed at international level. In such a case, the system implementing the MIB will have to support both protocols, one being used for the MIB update and the other one being used for the MIB consultation. And it seems better, from a safety point of view, to have this double-stack configuration implemented outside the local Manager.



4.3.3 Characteristics of a SMIB consultation interface

The SMIB consultation interface relies on a direct CMIB-based manager-agent association between the SMIB User and the SMIB Agent. An SMIB User willing to retrieve information from SMIBs of different organisations will have to establish one management association with each of the associated SMIB Agents. The model does not include any notion of cascade relationships (such as in ITU-T TD1079) where a SMIB agent could potentially provide access to the summary management information of a third party organisation by relaying the information retrieval requests received from a SMIB User to another SMIB Agent.

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

First, the SMIB User sets up an association with the SMIB Agent. The association may be permanently set based on the agreement of both organisations or on a demand basis. The application context to be used and the functional unit negotiation rules are to be specified.

Then SMIB User may then send either a CMIP M_GET or a CMIP M_CANCEL_GET PDU to the SMIB Agent. Having received the CMIP PDU, the SMIB Agent interprets what kind of requirement it has received and perform a management operation such as retrieval of an element of management information in the SMIB. The result is returned to the SMIB User in the form of a CMIP result PDU.

4.3.4 Connectivities between SMIB Users and agents

A single SMIB user may communicate across the SMIB consultation interface to one or more SMIB Agents using at least one association for each SMIB Agent.

A single SMIB Agent may support simultaneous associations with several SMIB Users.

4.3.5 Authentication control for the service

The SMIB Service provider may authenticate the identity of the requesting SMIB User for the purpose of security. Access of the SMIB User to the management information is allowed when conditions of authentication and qualification defined by the SMIB service provider are satisfied. If access is not permitted, the SMIB agent may notify the SMIB user that the access has been refused. Details on security mechanisms are out of scope of this document.

4.3.6 Role of the SMIB Manager

The SMIB Manager in in charge of maintaining up to date information in the SMIB. This could be done in several manners:

1. On a periodical basis: Management Information is periodically transferred from the ATN equipment in the local domain to the SMIB Manager, which then filters/summarizes the information and updates the SMIB.
2. event occurrence basis: any events (notifications) in relation to management information presents in the SMIB can be catched by the SMIB Manager. The SMIB manager may then update the SMIB information accordingly.
3. On demand basis: The SMIB Manager starts the action of updating the SMIB when a management information retrieval request is received by the SMIB Agent

Which type of technics is used for updating the SMIB may be considered as a local issue to the organizations, or may be a topic which requires standardization (considering that different methods may not provide the same insurance on the “ freshness ” of the information in the SMIB). This has to be discussed by the JSG.

Note: A combination of the 3 methods could be envisaged, with a different method being used for a differnt type of data. For instance, status of ATN systems or links could be updated on en event occurrence basis, configuration information could be updated on demand basis, and performance statistics could be updated on a periodical basis.

4.4 Management Information Standardization

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

The basic problem in defining system 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 government stand-point.

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

It is recognized that some information must to be shared and that some of that information is required to be shared in an on-line manner. Other information may be shared in an off-line, less timely manner. Further, the information that needs to be shared on-line must be available from every ATN Management Domain when requested.

The system management information that is available cross management domains is defined as the “summary MIB”. The summary MIB may be a subset of the information maintained by individual domains. The method of collecting and maintaining the summary MIB information is a local implementation choice for the individual Management Domains as long as they meet the timeliness and accuracy of the management information.

To ensure consistency of the summary MIB information, a GDMO description of the information is required so that the semantics and accuracy of the information is assured across domains.

4.4.1 Summary MIB Structure and Content

4.4.1.1 Introduction

The purpose of this section is to discuss possible ways to structure an SMIB and to identify an initial first set of SMIB Managed Objects and attributes.

4.4.1.2 SMIB Services

4.4.1.2.1 General

Before investigating the structure and content of a summary MIB, it is important to define precisely the services that are expected to be provided with the implementation of a Summary MIB.

As identified in the ATN SM CONOPs, the main purpose of the implementation of a Summary MIB is twofold:

1. To allow for the real time exchange of operational performance statistics between organisations
2. Possibly, to allow for the exchange of configuration information between organisations

More specifically, and with reference to ITU-T Recommendation X.161, the implementation of a summary MIB is aimed at providing the following services:

- Traffic Information Service

- QoS Information Service
- Network statistics service
- Configuration Inquiry Service

4.4.1.3 Assumed Requirements

The assumed requirements that could be met with the implementation of SMIB services are the following ones:

1. **Monitoring the status of the systems providing an ATN service**: In order to speed up trouble diagnosis activities, there might be some benefits for an organisation to have a real time view on the operational, administrative and performance (e.g. congestion) status of ATN ES and ISs in another organisation and via which the local organisation gets access to a given ATN service.
2. **Monitoring the performance of the ATN service that is provided**: In order to speed up trouble diagnosis activities, there might be some benefits for an organisation to have a real time view on the global quality and performance of the services provided by another organisation. The services for which there might be a requirement to monitor the quality and the performance can be classified as follows:
   - ATN Internetworking service: it consists in the forwarding of CLNP packets from an input node of the organisation providing the service to the destination system or to the input node of another organization on the path to the destination system.
   - ATN Application services: there are potentially as many different application services as there are different ATN applications (e.g. CPDLC service, FIS, etc..)

System Management of Subnetwork services is out of scope of ATN System Management.

3. **Regional supervision**: For trend analysis, capacity planning and trouble shooting co-ordination in a region, there might be the requirement in a region that every organisation that participates in ATN service provision provides another organisation in charge of the overall supervision of the regional ATN with additional statistics on the performance and Quality of Service information on inter-organisation links or data-flows (e.g. status of inter-domain links, internet or application (e.g. AMHS) inter-domain traffic information, etc...)
4. **Configuration information exchange**: For configuration management and trouble diagnosis activities, there might be some benefits for an organisation which uses a service to have a real time access to (part of) the configuration information of the organisation providing the service.

4.4.2 Discussion

In this document, it is considered that there are potential requirements (as listed above) for having the ATN service providers (application and/or internetwork service providers) implementing a Summary MIB.

On the other hand, at this time, there are no identified requirements for having simple ATN Service Users providing local Summary management information to other organisations. This can be explained by the nature of user-provider relationships: in general, users are affected by a failure of their providers and hence may have a requirement for real time monitoring of the activity and performance of their service providers. On the other hand, a service provider should never be affected by a failure on the service users side, and hence has generally no particular requirements for service users management information.

It results from these considerations that a Summary MIB may have to be implemented by any organisations providing an ATN services (namely, the ATSOs, the International Aeronautical Communications Service Providers (ARINC, SITA, etc...), and possibly the meteorological and military organisations and the airport operators). On the other hand, no clear requirements have been yet identified for ATN service Users such as the Airlines operation centres and the Aircraft, to implement a Summary MIB.

4.4.2.1 A draft proposal for the SMIB information to be provided by an ATN internetwork Service provider

4.4.2.1.1 Introduction

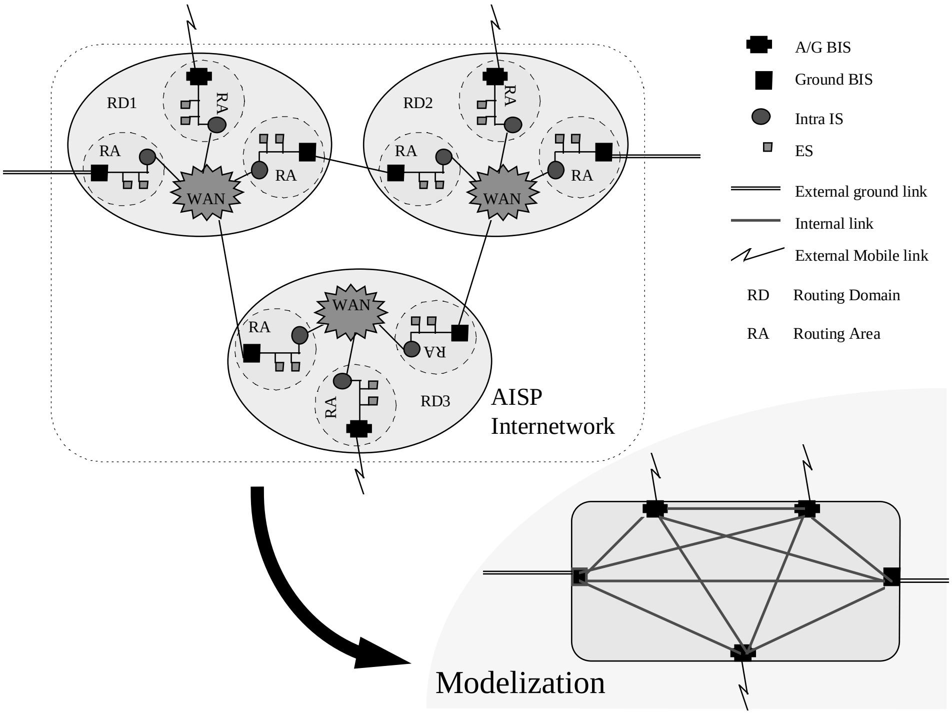
The objective of this section is to develop an initial proposal for the SMIB information that could be required to be made available by an ATN organisation providing an ATN internetwork service. This section does not consider SMIB information germane to the provision of ATN application services.

4.4.2.1.2 Approach

A simple model is defined for modelling the ATN infrastructure of an ATN organization providing ATN internetwork service. The model makes use of the following definition:

- AISP: ATN Internet Service Provider
- AISP cloud: the ATN internetwork of the AISP . An AISP cloud consists of one or several interconnected ATN Routing Domains or Routing Domain Confederations
- Egress Router: An ATN Ground or A/G BIS located at the boundary or the AISP Cloud
- internal linkage: the logical representation of a virtual direct link between 2 egress routers. An internal link may be physically supported by an internal subnetwork (e.g. a leased line, an X.25 WAN, etc.) or an internal ATN internetwork (e.g. a group of subnetworks interconnected by non-egress AISP ATN routers).
- external ground linkage: a link connecting an AISP cloud to another AISP cloud or to the ATN system of an ATN Internetwork service user.
- external mobile linkage: a mobile subnetwork to which one the AISP egress router is attached

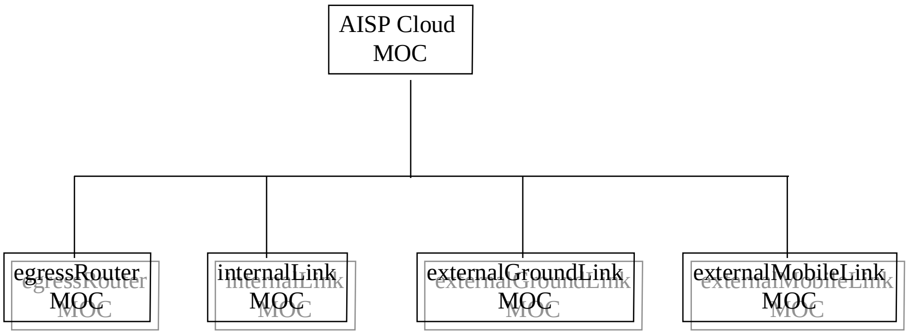
The approach proposed for summarizing the management information pertaining to the ATN infrastructure of an AISP, begins then by modelling the whole AISP internetwork as a single "AISP cloud" with egress routers, internal linkages, and external ground and mobile linkages, as illustrated by figure 2. The model hides the details of the internal architecture of AISP internetwork (e.g. internal routing architectures, internal routers, and subnetworks, etc....) but is believed sufficient for supporting the identified requirements on the exchange of operational statistics and configuration information.



The model can be recursively applied to a group of AISP internetworks, and can hence allow the summarization of multi-organisations internetworks such as an ATN backbone or an ATN Island.

4.4.2.2 SMIB Containment tree

As a draft proposal the following containment tree is proposed for the SMIB of an ATN Internet Service Provider.



This containment tree has simply been derived from the model of AISP internetwork described in the previous section, by considering each element of the model as a separate object.

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

4.4.2.2.1 The AISPCloud MO Class

The AISPCloud MO class is used to represent the whole ATN Internet Infrastructure of an AISP. Within a SMIB there should only one single MO instance of this class.

Possible attributes of this class are:

AISP Name	Name of the organization providing the ATN Internet Service
AISP Type	Type of the organization: ATSO, AICSP, Airport Operator, etc...
AISP Cloud Type	e.g. Routing Domain, Routing Domain Confederation, ATN Backbone RDC, ATN Island
AISP NSAP address prefixes	List of all prefixes of the AISP NSAP addresses

4.4.2.3 The egressRouter MO ClassMO Class

The egressRouter MO class is used to represent one egress Router of the AISP. Within a SMIB there may be multiple MO instances of this class.

Possible attributes of this class are:

Router type	A/G BIS, Ground BIS (and possibly L1 and L2 Intra-Domain IS)
Router NET	Router Network Entity Title
RDI	Routing Domain Identifier
OperationalState	Operational Status of the Router
AdministrativeState	Administrative Status of the Router
CongestionState	Congestion Status of the Router
ForwardedCLNPPackets	Number of CLNP Packets forwarded by the Router
DiscardedPackets	Number of CLNP Packets discarded by the Routers
configuration information	a selection of the configuration attributes of the router (e.g. IDRP Timers, SNPA addresses)
	to be defined

4.4.2.4 The internalLinkage MO class

The internalLinkage MO class is used to represent one internal linkage of the AISP. Within a SMIB there may be multiple MO instances of this class.

Possible attributes of this class are:

router1NET	Network Entity Title of the egress router at the first end of the internal linkage
router2NET	Network Entity Title of the egress router at the other end of the internal linkage
permitted traffic	ATSC Only, non-ATSC only, or both ATSC and non-ATSC
operationalState	Operational Status of the link (possibly for each direction of transfer)
administrativeState	Administrative Status of the link (possibly for each direction of transfer)
congestionState	Congestion Status of the link (possibly for each direction of transfer)
transitDelay	Delay of transit of the link (possibly for each direction of transfer)
capacity	Capacity (i.e. throughput) of the link (possibly for each direction of transfer)
ATSCtraffic	number of ATSC CLNP packets and PDU octets having transited over the link (possibly for each direction of transfer)
AOCtraffic	number of AOC CLNP packets and PDU octets having transited

	over the link
ADMtraffic	number of ADM CLNP packets and PDU octets having transited over the link
SMtraffic	number of SM CLNP packets and PDU octets having transited over the link
genTraffic	number of general communication packets and PDU octets having transited over the link
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair

4.4.2.5 The externalGroundLinkage MO Class

The externalGroundLinkage MO class is used to represent one external ground linkage of the AISP. Within a SMIB there may be multiple MO instances of this class.

Possible attributes of this class are:

localRouterNET	Network Entity Title of the egress router at the local end of the external linkage
externalSystemNET	Network Entity Title of the system at the other end of the linkage
permitted traffic	ATSC Only, non-ATSC only, or both ATSC and non-ATSC
operationalState	Operational Status of the link (possibly for each direction of transfer)
administrativeState	Administrative Status of the link (possibly for each direction of transfer)
congestionState	Congestion Status of the link (possibly for each direction of transfer)
transitDelay	Delay of transit of the link (possibly for each direction of transfer)
capacity	Capacity (i.e. throughput) of the link (possibly for each direction of transfer)
ATSCtraffic	number of ATSC CLNP packets and PDU octets having transited over the link (possibly for each direction of transfer)
AOCtraffic	number of AOC CLNP packets and PDU octets having transited over the link
ADMtraffic	number of ADM CLNP packets and PDU octets having transited over the link
SMtraffic	number of SM CLNP packets and PDU octets having transited over the link
genTraffic	number of general communication packets and PDU octets

	having transited over the link
UpdateIn	number of IDRP UPDATE PDU received on this link by the local router
UpdateOut	number of IDRP UPDATE PDU sent on this link by the local router
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair

4.4.2.6 The externalMobileLinkage MO Class

The externaMobileLinkage MO class is used to represent one external Mobile linkage of the AISP. Within a SMIB there may be multiple MO instances of this class.

Possible attributes of this class are:

localRouterNET	Network Entity Title of the egress router at the local end of the external mobile linkage
mobileSNtype	Satellite or VDL or Mode S of HF or Gatelink
permitted traffic	type of traffic permitted over the mobile subnetwork (e.g. bit map indicating permission for ATSC, AOC, SM, ADM, and general communication traffics)
operationalState	Operational Status of the link
administrativeState	Administrative Status of the link
congestionState	Congestion Status of the link
transitDelay	Delay of transit of the link (possibly for each direction of transfer)
capacity	Capacity (i.e. throughput) of the link (possibly for each direction of transfer)
ATSCtraffic	number of ATSC CLNP packets and PDU octets having transited over the link (possibly for each direction of transfer)
AOCtraffic	number of AOC CLNP PDU packets and octets having transited over the link
ADMtraffic	number of ADM CLNP PDU packets and octets having transited over the link
SMtraffic	number of SM CLNP PDU packets and octets having transited over the link
genTraffic	number of general communication packets and PDU octets having transited over the link
octetSent	number of octets sent over the link (after compression)
octetReceived	number of octets received over the link (before decompression)

aircraftContactNumber	the total number of aircraft having been in contact over the link
aircraftDiscontactNumber	the total number of aircraft having closed the contact over the link
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair

4.5 Protocol Overview

Assuming that summary MIB information is available across management domains, it remains that the method of accessing that information must be standardized. To access summary MIB information, a standard protocol suite must be used. The protocol suite selected for the ATN is based on the OSI defined Common Management Information Protocol (CMIP).

The CMIP is based on the classic agent/manager model. For use between two managers that are maintaining summary MIBS, a request for information from one manager to another is a request from a manager to an agent. That means that each manager maintains its summary MIB information acting as an agent; and that it fulfills requests for that information just like any other agent.

The use of CMIP is only one part of the overall communication infrastructure that is required to support system management. The other part of the problem is the selection of the underlying communication protocols.

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

1. For ground-based system managers, the communication protocols selected should be compatible with standard management platforms,
2. For air-based system managers, the communication protocols selected should be compatible with those already defined for the airborne system.

This leads to the following decision:

1. For ground-based system managers, a standard CMIP profile based on a full session and presentation layer should be used. This profile should be supported by commercial CMIP-capable managers.
2. For air-based system managers, a “Fast-MIP” profile should used that is both compatible with the existing Fast Byte communication profile and acceptable for use with CMIP.
3. For the conversion between communication profiles, it should be placed in such a way to have minimal impact on standard implementations.

4.6 Data Fusion

Data fusion, or the function of collecting and utilizing data from several sources, is an important aspect of ATN System Management. Each system manager is required to take two separate data sources and combine those sources into a coherent view of the overall ATN.

The first source of system management information is the local management domain. The manager must be able to receive information from the agents in its domain and create the required summary MIB information. (Of course, it may also be required to collect and locally display other information relevant to the operation of the local domain.)

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 system manager to take the information and convert it into the local form into the form needed by the summary MIB. (This means that it is entirely satisfactory to maintain the local domain using SNMP and have a system manager that supports both CMIP and SNMP maintain the summary MIB using CMIP. The system manager would need to be able to collect the appropriate SNMP information, translate it into a CMIP MIB and make that MIB available to other ATN system managers.)

The second source of information to a system manager is data coming from other system managers. This information may be the result of either requests or unsolicited. It will be necessary for each system manager to analyze the received information in order to decide whether to include the information in its summary MIB or to take corrective local actions based on changing conditions within the ATN.

5 System Management co-ordination scenarios

5.1 Introduction

This chapter examines possible overall System Management co-ordination scenarios. The objective is to identify the system management functional areas that require cross-administrative domain interactions, the categories of information that need to be exchanged, and the possible solutions for the exchange of information.

The system management functional areas for which there is a potential requirement for co-ordination, are the five standards OSI ones: performance, configuration, fault, security and accounting management.

5.2 Performance management in a multi-organisation context

5.2.1 Introduction

Every organisation participating in the ATN communication and operating ATN equipment will collect and archive network management metrics that indicate network utilisation, 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 organisation.

However, the broader goal of co-operative problem isolation and network planning among ATN organisations is likely to become increasingly important as the ATN grows, particularly as the number of involved organisations expands, while the overall quality of service remains more of a concern.

Therefore, there is a requirement for the exchange of common operational statistics between organisations that follow the agreed principles for system management co-ordination. This requirement is furthermore assumed to exist both for real-time supervision, and for off-line network planning activities. For real time supervision, information on the current overall performance on the ATN domain(s) of an organisation will have to be made dynamically accessible to one (central) or several external network managers. For off-line network planning activities, every network manager will have to gather raw performance data on the historical overall performance of its ATN network, and share these raw data with other managers or administrators. It is from this raw data , that network administrator can perform current operation and trend analysis and produce the various types of reports.

A potential difficulty for co-ordination, when the responsibilities for system management are distributed among all the involved organisation, is that every organisation may use different network management tools for the collection and presentation of network management metrics, with different kinds of measurement and presentation techniques. Such a diversity could make impossible the comparison of system management data among organisations.

As mention earlier, to allow for the exchange of meaningful performance management data, there must be a general agreement on what metrics should be regularly collected and on how their values must be presented and exchanged. More specifically, there needs to be an agreed-upon model for:

1. A minimal set of common network management metrics to satisfy the goal of co-operative problem isolation and network planning among ATN organisations,
2. a common interchange format and mechanism to facilitate the usage of these data by common presentation tools, and that will allow the real time monitoring of the metric value across domain boundaries.
3. a format for archiving the collected data, (Note: this may be necessary only in a distributed co-ordination context, to avoid that every organisation records the performance data of each other organisations; it is indeed better to have each organisation recording its own performance data, and providing a copy of the stored data collection, on request by other organisations)
4. the metric values refreshment, storing period and retention periods.

5.2.2 Guidelines for defining a common set of network performance management metrics

5.2.2.1 Introduction

The definition of a common set of overall network performance management metrics is out of the scope of this study. This set should be specified in the ATN SARPs. However, since nothing has yet been done at ATNP on the subject, this section is proposed to be used for providing initial guidelines for the identification of the common management information elements of interest.

The intent is to identify the categories of performance management information elements that would be require to exchange across organisation boundaries to facilitate real-time problem detection, near-term problem isolation and longer-term network planning.

Management information elements are generally structured in Managed Objects, which in turn are hierarchically organised to form a Management Information Base (MIB). A MIB is usually specified for an equipment (e.g. an ATN ES or IS) and provides access to performance, configuration, fault, accounting and security information that characterises this equipment.

The basic principle for providing access to performance and other types of information that characterise the ATN domain administered by an organisation, would be consider the ATN domain as one "equipment" of the regional ATN and to define a MIB that models the characteristics of this "equipment", i.e. that models the characteristics of the whole ATN domain. This MIB would hide the details on the performance of the individual components that constitute the domain (i.e. the subnetworks, the ESs, the routers), and would instead provide an aggregated summary of the overall performance of the ATN domain.

The objective of this section is to identify a first set of attributes in this MIB that would characterises the overall performance of an ATN domain.

5.2.2.2 Overall view of an ATN domain

An ATN domain is a collection of ATN ESs and ISs, interconnected via subnetworks. When an ATN domain is interconnected to other ATN domains, this is because this domain either provides or uses services to/from the other ATN domains. The services used and/or provided by an ATN domain can be classified in 2 main categories:

- The internetworking services
- The application services

The ATN domains that provide internetwork service are transit domains which accept to forward CLNP packets received from one adjacent ATN domain to another adjacent domain. To some extent, such ATN domains can therefore be viewed from outside as a "big ATN Intermediate System".

The ATN domains that provide or use application services are domain in which run ATN applications. When such domains do not provide internetworking services to the adjacent domains, they are generally classified as "End" domains. To some extent, such ATN domains can be viewed, from outside as a "big ATN End System", supporting all the international ATN applications that run in the domain.

By extension, ATN domains that are both End and Transit domains could be viewed as "big combined End plus Intermediate ATN System".

The only interest of these analogies is to identify the fact that the multi layers protocol nature of the ATN systems has to be reflected when modelling an ATN domain: there will be a need to consider the performance of an ATN domain, at subnetwork layers level, at CLNP protocol level, at IDRP level and possibly also at transport and upper layer levels.

The above analogies have limits and it is not proposed to model an ATN system exactly like an ATN systems. This is because they are other aspects of an ATN domain that would not be reflected if an ATN domain was simply modelled as an ATN End or Intermediate systems. Such other aspects are for instance topological information on the location, number and status of boundary nodes, the individual performance, utilisation and availability of the ATN BISs or of ATN ESs within the domain, etc.

5.2.2.3 Performance metrics for an ATN domain

The objective of this section is to identify a first minimum set of attributes that would characterises the overall performance of an ATN domain. This initial set could be used as a starting basis and refined in further studies on the subject.

The following set of metrics are identified:

- For each Intermediate System at the boundary of the ATN domain:
- the status of the system
- the level of congestion: this metric should be computed from internal (hidden) attributes implemented in the router (e.g. it may be the ratio of the number of packets dropped due to congestion on the total number of packets received by the IS (including packet received from an internal system and packets received from external systems)).
- the ratio of packets discarded on entry in the ATN domain
- the ratio of packets discarded on exit from the ATN domain
- For each of its external adjacent ground or A/G BISs:
- the status of the BIS-BIS connection
- the number of CLNP packets (possibly in separate counters per traffic types) sent and received to/from this adjacent BIS
- the number of octets sent and received to/from this adjacent BIS
- the number of UPDATE IDRP PDU sent and received to/from this adjacent BIS (to compute the incoming and outgoing update rate)

- the current, average and maximum transit delays of CLNP packets exchanged with the external adjacent BIS
- the number and waiting delays of outstanding IDRP update PDUs
- If the IS is an A/G BIS, the following attributes should also be provided:
- The current number of adjacent mobile BIS
- The total number of adjacent mobile BISs having been in contact with that A/G BIS
- The total number of CLNP packet sent and received to/from a mobile BIS
- for each subnetwork used for communication with external adjacent fixed or mobile BIS:
- the total number of octets sent/and received over this subnetwork
- the total number of packets dropped due to congestion on the subnetwork
- the congestion level of the subnetwork
- the current, maximum, and total number of Virtual circuit opened over the subnetwork
- For each of the other "internal" Intermediate Systems at the boundary of the ATN domain
- the current, average and maximum transit delays of CLNP packets exchanged with this internal IS
- the current, average and maximum route update propagation delay toward this internal IS

At the moment, no metrics associated with the performance of End Systems have been identified.

5.2.3 General principles for the real-time exchange of operational statistics

5.2.3.1 Introduction

The purpose of this section is to define mechanisms by which the Network Operation Centre of each organisation could share most effectively their operational statistics in real-time with one (central) or several other organisations. The purpose of such mechanisms would be to facilitate on-line ATN performance problem detection and resolution at a multi-organisation scale.

It is assumed that every Network Operation Centre will operate a central Network Management Stations from which it will be possible to collect periodically the operational statistics from the equipment distributed in the domain.

It is then assumed that the information gathered from the individual equipment, can be filtered, and processed for updating the summary ’ATN domain’ MIB introduced in section 5.2.2.1.

The general principle for the exchange of operational statistics is therefore that each organisation would provide other organisations with access to a summary MIB on the characteristics of its ATN domain. This MIB would be periodically updated by the local organisation. Others organisations that have been granted permission to access this MIB, and which need a real-time view on the overall performance of the ATN domain, would then be allowed to poll, periodically, the value of the performance metrics.

5.2.3.2 Location of the 'ATN domain summary' MIB

The 'ATN domain summary' MIB could be implemented either on:

- The Network Management Station (i.e. the manager) of the Network Operation Centre, or
- A separate dedicated system, receiving MIB update requests from the Network Management Station on one hand, and receiving poll request from external managers on the other hand..

Implementing the MIB on a separate dedicated system presents the following 2 advantages:

1. A separate dedicated system will constitute a security firewall for the local organisation. This eliminates the potential risk of an external user succeeding in taking some level of control and command on the local ATN network. This also eliminates the risk of an invalid external operation causing the failure of the Network Management Stations
2. The Network Management protocol used within the domain for the management of individual pieces of equipment may be different from the one that has been agreed for the exchange of management information across domain boundaries. As an example, SNMP may be the local protocol in use, whereas CMIP has been agreed at international level. In such a case, the system implementing the MIB will have to support both protocols, one being used for the MIB update and the other one being used for the MIB consultation. And it seems better, from a safety point of view, to have this double-stack configuration implemented outside the Network Management Station.

5.2.3.3 MIB Update and Polling frequencies

To serve as a basis for real-time problem detection, or near-term problem isolation, the performance statistics will have to be updated periodically by the local organisation and consulted regularly by the external organisation(s).

The "summary" MIB Update and Polling frequencies, is therefore a topic that will have to be discussed between organisations and standardised.

It may be noted that all performance metrics will certainly not need the same updating and polling period. There may be variables needing high resolution polling (and consequently high update frequency) and variables not needing high resolution polling (and consequently low update frequency).

5.2.4 Principles for the exchange of operational statistics to serve as a basis for trend and capacity planning

5.2.4.1 Introduction

The previous section focused on the mechanisms needed for the real-time exchange of operational statistics, for on-line performance problem detection, or near-term problem isolation.

Another objective of performance management is the use of the collected statistics for off-line longer term network trend analysis and capacity planning.

For off-line network planning activities, the value of the performance metrics that are periodically collected needs to be recorded for future use as historical raw data. It is from this raw data , that network administrator can perform current operation and trend analysis and produce the various types of reports.

When real-time access to current performance statistics is provided by an organisation according to the principles introduced in the previous section, other organisations can periodically poll the values of these statistics, record them locally and then constitute the raw data files that will later be used for network planning activities. For the following 2 reasons, this scenario is not however very satisfactory:

1. The partner organisations needing the data for network planning activities only (and not for real-time supervision) are compelled to perform the on-line periodical polling of the performance metrics, so as to have these data collected.
2. When the data are of interest for multiple partner organisations, the same data will be collected and recorded several times. This is a waste of efforts and resources, since the data could instead be collected and recorded once for all in a unique reference archive, that could then be shared among the partner organisations as necessary.

A better approach would then be to have each organisation responsible for the recording of the performance statistics on its own ATN domain, and sharing the resulting raw data file with other partner organisations.

This approach necessitates the definition of a common format for archiving the collected data, and of common mechanisms for sharing the content of the archive.

5.2.4.2 Elements for the definition of operational statistics archive

5.2.4.2.1 Introduction

The specification of a common archive format and sharing mechanism is out of the scope of this document. This section will be used to provide informative elements on the subject.

The exchange of common operational statistics is an issue that has been studied by the internet community. Two RFCs address the subject:

- RFC 1857: A Model for Common Operational Statistics
- RFC 1856: The Opstat Client-Server Model for Statistics Retrieval

The 2 following sections provide a summary of the ideas brought in these papers.

5.2.4.2.2 Definition of an interchange file format

RFC 1857 defines an interchange file format. The model is not necessarily intended to be used for the actual data storage of operational statistics. Its goal is to provide complete, self-contained, portable files rather than to describe a full database for storing the data.

The proposed format is the one of a plain text, human readable file, with well specified labels to mark the beginning and end of the multiple sections and records. The file can be transferred from one Network Operation Centre to another one using conventional file transfer or message transfer mechanisms.

The specification of the interchange file format, comprises the following aspects:

- the syntax used to describe the recorded data
- the definition of the recorded data
- the specification of the storing period of each data (within the same set of logged data, different data can be logged at different frequencies)
- the definition of aggregation rules: to avoid storing redundant data, some levels of pre-processing and aggregation of the raw data may be required. The volume of data that may be generated by short statistics collection period (e.g. every minutes) makes indeed aggregation of the stored data desirable if not necessary. Aggregation refers to the replacement of data values on a number of time intervals by some function of the values over the union of the intervals.
- the specification of aggregation periods: e.g. over a 24 hour period, aggregate to 15 minutes, over a 1 month period, aggregate to 1 hour, over a 1 year period, aggregate to 1 day, etc.
- the specification of retention periods (i.e. how long will the data be archived)

5.2.4.2.3 use of a client/server based statistical exchange system

A client/server approach is proposed in RFC 1857 for the exchange of operational statistics. Such an architecture envisions that each Network Operation Centre should install a server which provides locally collected statistics for clients. Using a query language the client should be able to define the network object of interest, the metrics and the time period to be examined. The server would then transmit the requested data.

5.2.4.3 Elements for the exchange of performance reports

The raw data files will be used by network administrators to generate reports on the current network operations and trends. Another area of co-operation and co-ordination between organisations is therefore the exchange of such reports. Effort and resources could indeed also be saved if some basic classes of network performance reports were standardised: every organisation could produce periodically such standard reports on the performance of its own ATN domain and could share the document with the partner organisations.

The idea would then be to define at international level the structure and contents of basic classes of reports to be produced by the area administrators according to a well specified schedule.

As an example scenario, there could be:

- short-term weekly reports giving information about medium-term changes in network behaviour which could serve as input to the medium term engineering activities
- monthly and yearly reports showing long-term tendencies in the network

The content of these reports could be bar-charts giving a total value, for the period, of some major performance metrics, such as:

- the number of CLNP packets exchanged at the boundary nodes of the ATN domain
- the number of UPDATE PDU exchanged at the boundary nodes of the ATN domain
- the number of aircraft having been in contact with the ATN domain.

5.3 Fault management in a multi-organisation context

5.3.1 Introduction

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

- Maintain and examine error logs
- Accept and act upon error notifications
- Trace and identify faults
- Carry out diagnostic tests
- Correct faults

Fault Management deals most commonly with alarm notifications emitted by network elements and with complaints from the network users.

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...)

However, work to date in the area of fault management has concentrated on effectively managing the resolution of problems within an Administrative domain. To our knowledge, little has been done to address the problem of co-ordinated fault management across administrative domains, although the need for such a global co-ordination system is not specific to the ATN: in one recent informal study of routing stability in the internet, it was found that while the majority of catastrophic routing problems could be identified as 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 co-ordination, so that the true causes of problems may be identified and such circular referrals detected and resolved.

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.

This section investigates the problem of such inter-domain co-ordination 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
- pre-notification, or notifying organisations of downtime scheduled in the future

5.3.2 Fault management within administrative domain

5.3.2.1 Introduction

The definition of possible inter-domain troubleshooting co-ordination scenario requires to make some assumption on the way fault management will be performed within each organisation.

We will make the assumption that every organisation will use some kind of central problem tracking system as this is generally required for professional quality handling of computing problems. Such central system is referred hereafter as a “ trouble ticket ” system.

This section gives an overview of the general functions of a trouble ticket system.

5.3.2.2 What is a trouble ticket system ?

5.3.2.2.1 General

Problem reporting and resolution is a multi-phase procedure. In the first phase, an error is reported and a first hypothesis on the cause of the problem is submitted to an expert whose area of expertise includes the network element which is experiencing problems. The expert next attempts to verify the existence of the reported problem. If the problem is confirmed, the expert then generates additional hypotheses about potential causes, which are in turn submitted to appropriate experts. This process continues until one or more problems are confirmed which have no causes. Repairs are then requested for these problems. If repairs can not be immediately initiated, repairs are then attempted at their immediate effects, and soon back down the cause tree.

A basic trouble ticket system co-ordinates the work of multiple people who may need to work on a problem.

5.3.2.2.2 Purposes of a trouble ticketing system

A good description of the desirable features of a trouble ticketing system is found in RFC 1297: a trouble ticketing system may serve many purposes:

1) SHORT-TERM MEMORY AND COMMUNICATION ("Hospital Chart"). The primary purpose of the trouble ticket system is to act as short-term memory about specific problems for the Network Operation Centre (NOC) as a whole. In a multi-operator or multi-shift NOC, calls and problem updates come in without regard to who worked last on a particular problem. Problems extend over shifts, and problems may be addressed by several different operators on the same shift. The trouble ticket (like a hospital chart) provides a complete history of the problem, so that any operator can come up to speed

on a problem and take the next appropriate step without having to consult with other operators who are working on something else, or have gone home, or are on vacation. In single-room NOCs, an operator may ask out loud if someone else knows about or is working on a problem, but a trouble ticket system allows for more formal communication.

2) SCHEDULING and WORK ASSIGNMENT. NOCs typically work with many simultaneous problems with different priorities. An on-line trouble ticket system can provide real time (or even constantly displayed and updated) lists of open problems, sorted by priority. This allows operators to sort their work at the beginning of a shift, and to pick their next task during the shift. It also allows supervisors and operators to keep track of the current NOC workload, and to call in and assign additional staff as appropriate.

3) REFERRALS AND DISPATCHING. If the trouble ticket system is thoroughly enough integrated with a mail system, or if the system is used by Network Engineers as well as Network Operators, then some problems can be dispatched simply by placing the appropriate Engineer or Operator name in an "assigned to" field of the trouble ticket.

4) ALARM CLOCK. Typically, most of the time a trouble ticket is open, it is waiting for something to happen. A timer is then generally associated with every wait. If a ticket is referred to a public network operator providing subnetwork service, there will be an escalation time before which the public network operator is supposed to call back with an update on the problem. For tickets referred to remote site personnel, there may be other more arbitrary time-outs. Tickets referred to local engineers or programmers may also have time-outs ("Check in a couple of days if you don't hear back from me"). A good trouble ticket system allows a time-out to be set for each ticket. This alarm generates an alert for that ticket at the appropriate time. Preferably, the system allows text to be attached to that timer with a shorthand message about what the alert involves (The full history of the problem can always be found by checking the trouble ticket).

5) OVERSIGHT BY ENGINEERS AND CUSTOMER/SITE REPRESENTATIVES. NOCs frequently operate more than one network, or at least have people (engineers, customer representatives, etc.) who are responsible for subsets of the total network. For these individual representatives, summaries of trouble tickets can be filtered by network or by node, and delivered electronically to the various engineers or site representatives. Each of these reports includes a summary of the previous day's trouble tickets for those sites, a listing of older trouble tickets still open, and a section listing recurrent problems. These reports allow the site representatives to keep aware the current outages and trends for their particular sites. The trouble ticket system also allows network access to the details of individual trouble tickets, so those receiving the general reports can get more detail on any of their problems by referencing the trouble ticket number.

6) STATISTICAL ANALYSIS. The fixed-form fields of trouble tickets allow categorisations of tickets, which are useful for analysing equipment and NOC performance. These include, Mean Time Between Failure and Mean Time to Repair reports for specific equipment. The fields may also be of use for generating statistical quality control reports, which allow deteriorating equipment to be detected and serviced before it fails completely. Ticket breakdowns by network allow NOC costs to be apportioned appropriately, and help in developing staffing and funding models. Data such as the number of specific models of hard drives that have been repaired or replaced over the last month, quarter or year, allow the administrator to weed out those devices that cost too much to repair. Analysis of this sort typically drive the cost of maintenance down.

7) ACCOUNTABILITY, FACILITATING CUSTOMER FOLLOW-THROUGH, AND NOC IMAGE. Keeping user-complaint tickets facilitates the kind of follow through with end-users that generates happy clients (and good NOC image) for normal trouble-fixing situations. But also, by their nature, NOCs deal with crises; they occasionally find themselves with major outages, and angry users or administrators. The trouble ticket system documents the NOC's (and the rest of the organisation’s) efforts to solve problems in case of complaints.

5.3.2.3 What is a trouble ticket ?

A trouble ticket is simply a well defined form with fixed and/or free fields, and which is used as the representation of an event for problem report. A ticket is opened when a problem is raised; it is then held by the right responsible of the problem; and finally closed when the problem has been solved.

A trouble ticket consists generally of the following 3 parts:

1) HEADERS. Inevitably, a trouble ticket begins with a number of fixed fields. These generally include:

- Time and Date of problem start.
- Initials or signon of the operator opening the ticket.
- The unique trouble ticket number
- Severity of the problem (possibly separating the "customer severity" and the "NOC priority", since these could be different).
- A one-line description of the problem for use in reports.
- A status (e.g. OPENED, HELD or CLOSED)

There can be many other fixed fields for specific purposes. There may also be different kinds of tickets for different problems, where the ticket format differs mainly in fixed fields. These include:

- Who reported the problem? (Name, organisation, phone, e-mail address)
- Machine(s) involved.
- Network involved (for multi-network NOCs).
- User’s machine address.
- Destination machine address.
- Next Action.
- Time and date for alarm on this ticket.
- Who should the ticket be dispatched to?
- Ticket "owner" (one person designated to be responsible overall).

2) INCIDENT UPDATES. The main body of trouble tickets is usually a series of freeform text fields recording the incident updates, and the date and time of these updates. The first incident update usually is a description of the problem. Since the exact nature of the problem is usually not known when the ticket is first opened, this description may be complex and imprecise. (e.g. it may include traces of PDUs exchanged, the dump of a Forwarding Information base, a copy of the original message for problems that are reported by electronic mail, etc...) . Generally, this section also includes an indication of what the next action for this ticket ought to be

3) RESOLUTION DATA. Once a problem is resolved, it is useful to summarise the problem for future statistical analysis. The following fields are generally found to be useful:

- Time and Date of resolution
- Outage duration
- Resolution (description of what happened and on how the problem was fixed).
- Key component affected (for MTBF and similar reports).
- Checked By -- a field for supervisors to sign off on ticket review.

5.3.2.4 Trouble tickets and incident reports

A single network failure might well produce a large number of individual user phone calls and hence " user complaint " tickets. In the same way, a failure may result in several " error notifications " received on the alert system.

As multiple events occur for the same problem, it is often most efficient to record only a single trouble ticket. However, it is still important to track all the individual incidents related to the trouble ticket to more accurately respond to the problem and to measure the total performance of the problem correction. NOC generally wants to use " special forms " to track each one of the user complaints (e.g. to make sure each user is informed and satisfied about the eventual resolution of problem) and error notifications. Such special forms are called " incident reports ": incident reports can be used to store the user view of a problem or to capture duplicate (correlated) error notifications received on the alert system.

An incident report is a well defined form which typically includes the following fields:

- the incident report unique number,
- the date and time when the incident report was opened
- the number of the associated trouble ticket
- the origin of the incident report: this field may contain information on the person who reported the problem or information received on the alert system
- A description of the place which are affected by the problem
- A title summarising the problem
- A description of the problem
- The time when the problem was detected
- The time when the problem was corrected

5.3.3 Inter-domain troubleshooting co-ordination

5.3.3.1 Introduction

From the previous description on the general fault management process within administrative domain, it follows that inter-domain troubleshooting co-ordination should be based on the exchange of trouble tickets and incident reports across domains.

The basic scenario is the following:

- a fault occurs within a domains that impacts other ATN domains (e.g. a BIS or an ES failure). This error is likely to result first in error notifications or user complaints received by the Network Operation Centres of each organisation impacted by the problem (including the NOC of the organisation where the fault has effectively occurred).

- In a first phase, each of those organisations is assumed to open a trouble ticket for the problem, and to investigate the causes. All but one organisations should then conclude that the origin of the problem is external to their domain (those are referred hereafter as the impacted organisations). One organisation should conclude that it is responsible for the resolution of the problem (it is referred hereafter as the faulty organisation).
- The impacted organisations may then be willing to report the problems. If they have identified the faulty organisation, the following 2 scenarios are conceivable:
    1. The impacted organisations report the incident to the faulty organisation, and need feedback on the resolution of the problem (e.g. time to repair, notification of the resolution of the problem, etc...)
    2. The impacted organisations report the incident to the faulty organisation, and do not need feedback on the resolution of the problem. This may occur when the organisations have detected a problem that has no real impact on their own domain (e.g. the failure of the ATN equipment on board of an aircraft for an ATSO). In these cases the organisations are simply willing to help other organisations in the process of identification and resolution of their problem.

If the impacted organisations do not know which organisation is at the origin of the problem, the following co-ordination scenarios could be envisaged:

3. If there is a central co-ordination entity within the ATN region, the impacted organisations report the incident to this entity, which is then in turn assumed to investigate the problem, and co-ordinate its resolution.
4. If there is no central co-ordination entity, the impacted organisations report the incident to one or several of its immediate partner organisations which are then assumed to investigate the cause of the problem and either deny it, or accept to participate in its resolution. In the latter case, the partner organisations may have to propagate the incident report to other organisations, and this process may continue until the true responsible is identified.

- The faulty organisation may be willing to:
    5. Warn every partner organisation about the problem.
    6. Acknowledge the receipt of incident reports from those of the partner organisations that have detected and reported the problem.
    7. Inform the partner organisation on the status of the problem resolution

Inter-domain troubleshooting co-ordination addresses therefore issues such as:

- The definition of common inter-domain trouble tickets and incident reports.
- The definition of common mechanisms for the exchange of trouble tickets and incident reports
- The definition of common operational procedures governing the exchange of the trouble tickets and incident reports.

5.3.3.2 Definition of common inter-domain trouble tickets and incident reports

All ATN organisations should agree on a common specification of the content and the structure of ATN trouble tickets and incident reports. The specification on the content should include:

- **a common definition of the severity of a problem** (e.g. ‘critical’ when the problem causes widespread interruption in the ATN communication service, ‘Major’ when a work-around can be applied to the problem and the service can continue in a degraded mode, ‘Minor’ for problems that should be fixed in the normal course of business and for which the change can wait until the future for correction)
- **a common definition of the status of a problem**. For instance:
  - Unconfirmed: A test is in progress to confirm that the problem exists.
  - Diagnosis-Deferred: The test for the existence of the problem has been deferred until a later time.
  - Rejected: The test failed, indicating that the problem does not exist, and the problem state will shortly go away.
  - Indeterminate: Either no test is known, or the test was inconclusive, and the problem state will shortly go away.
  - Confirmed: Existence of the problem is acknowledged, and causes are currently being investigated.
  - Covered: Another problem is known to be causing the current problem, and hence the expert is waiting for the cause to be repaired.
  - CantRepair: No repair is possible for the problem.
  - Isolated: A repair and retest are in progress.
  - Repair-Deferred: The repair has been deferred until a later time.
  - Repaired: The problem was successfully repaired, and the problem state will shortly go away.

  - WentAway: The problem disappeared, and hence the problem state will shortly go away.
  - Retesting: All previously-confirmed causes are gone, and a retest is in progress.
  - Deleted: No state for the problem exists.

- **a common definition of the types of problems:** this may be a catalogue of well identified error cases to which an organisation may refer when reporting an problem or the diagnostic of a problem.
- **the list of all other information elements to be provided** (e.g. time when the problem was detected/corrected, who reported the problem, who is responsible for the problem, expected repair time, etc...)

The specification on the structure of the trouble ticket and incident report should describe how the information is encoded. Possible structures are:

- a plain text form that can be exchanged in the body of an electronic mail
- an EDI/EDIFACT document
- CMIP notifications
- others....

5.3.3.3 Definition of common mechanisms for the exchange of trouble tickets and incident reports

The ATN organisations should agree on common mechanisms for:

1. the exchange of trouble tickets and incident reports,
2. and possibly for the real time monitoring of the status of trouble tickets

Possible mechanisms for the exchange of trouble tickets and incident reports are:

- AMHS
- CMIP (there are apparently TMN standards, addressing the issue of inter-domain trouble-ticketing, and based on the use of CMIP)
- others ?

Real-time monitoring of the status of trouble tickets would require the implementation in the Network Operations Centres of an information server accessible by remote clients. Possible architectures for such services are:

- the use of a data base manager (with SQL interactions between the clients and the server)
- the use of http-based servers and browsers (e.g. Netscape)

5.3.3.4 Definition of common operational procedures governing the exchange of the trouble tickets and incident reports

Common operational procedures should be defined and specify:

- in which cases an inter-domain incident report is to be issued,
- to which organisation(s) the incident report should be delivered,
- which reporting actions have to be taken by an organisation on receipt of an incident report (acknowledgement of the report, acceptance or denial of the problem, notification on the opening of a trouble ticket, possible reports on the change of status of the trouble ticket,....
- Which reporting actions have to be taken by an organisation on failure of one of its equipment, vis a vis the other organisations
- etc...

These operational procedures will certainly depend on the organisational principles (centralised or distributed). adopted in the ATN region to achieve overall co-ordination among the ATN organisations. In ATN regions where a centralised co-ordination entity is in place it may be assumed that this central entity will take a preponderant role in the handling and redistribution of incident reports and trouble tickets.

5.3.3.5 Recommendation

The specification and implementation of an overall trouble ticketing architecture is a complex problem. However, trouble ticketing is a domain which has long been considered by the industry and there are today numerous COTS products and solutions that answer most of the requirements.

It is therefore recommended that the ATN community builds and specifies a trouble ticketing architecture that can be based on and integrate COTS trouble ticket systems. The ATN inter-domain troubleshooting co-ordination requirements should be specified by the ATN community by making in parallel a survey of the current trouble ticketing systems available on the market, and of those currently used by ATSOs, Airlines and IACSPs, and by analysing how these COTS tools could be interfaced with the ATN.

5.3.4 Off-line fault management

ATN organisation will normally mitigate the effects of faults, by taking preventive actions that are planned as part of the network/application design and that consider the cost and the criticality of the services. Preventive actions may include built-in redundancy such as automatic switch to backup system, or a complete change in application such as switching from data exchange to voice exchange of pertinent information.

The prevention of fault is a domain which may require co-ordination among the different ATN organisation. This domain may comprise the following aspects:

- Establishment of bilateral or multilateral procedures to be performed on the occurrence of well-identified error cases (e.g. switch from one subnetwork service provider to another one).
- Bi-lateral or multi-lateral agreement on normative time for, the detection and report of problem by an ATN organisation (mean time to detection), the recovery of problem with backup or redundant components (mean time to recover), and the restoration to original configuration (mean time to restoration)
- The co-ordination and planning of downtime for routine maintenance
- Liability issues

5.4 Accounting management

5.4.1 Introduction

Accounting is a complex problem. The ATN will consist of networks of varying sizes and capacities, operated both by administrations and commercial organisations. Subsidies and funding mechanisms appropriate to non-profit organisations often restrict commercial use or require that "for profit" use be identified and billed separately from the non-profit use. Tax regulations may require verification of network usage. Some portions of the ATN will be distinctly "private", whereas other ATN segments will be treated as public, shared infrastructure. Each of the administrations may have different policies and by-laws about who may use an individual network, who pays for it, and how the payment is determined. Also, each administration will balance the OVERHEAD costs of accounting (metering, reporting, billing, collecting) against the benefits of identifying usage and allocating costs.

Different billing schemes may be employed. In certain cases a flat-fee, usage-insensitive model, similar to the monthly unlimited local service phone bill, could be sufficient and could be preferable for financial, technical, or other reasons. In other cases, usage-sensitive charges may be preferred or required by a local administration’s policy. The wishes of ATN users with low or intermittent traffic patterns may force the issue (note: flat fees are beneficial for heavy network users. Usage-sensitive charges generally benefit the low-volume user).

The exact requirements for ATN usage accounting will therefore vary from one network administration to the next and will depend on policies and cost trade-offs.

Accounting issues have normally to be considered on the following 2 different aspects:

1. 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, subsidisation, profit making). Issues such as these are out of the scope of System Management and are not covered here.
2. technical issues on the possible ATN usage measurement and reporting architectures that will permit the ATN organisations to perform accounting in a private or co-operative way and according to a personal or a commonly agreed accounting policy . This technical aspect of the accounting is considered in this section.

Accounting management only deals with the technical aspects. This section will therefore be used to provide background and tutorial information on accounting management architecture that may have to be implemented within organisations and addresses the issues of the possible accounting co-ordination requirements between organisations.

5.4.2 Accounting Architectures

5.4.2.1 Introduction

The accounting management process is likely to vary among organisations based on billing practices. However, in order to identify the areas where accounting management co-ordination across organisations may be required, we will describe a general accounting management model and assume that this model will not be very different from the accounting management process performed within the organisations participating in the ATN.

The following sections outline the model for traffic flow measurement that has been developed by the Internet community and which is currently proposed in RFC 2063. This accounting architecture has been derived and developed from the working drafts of the OSI accounting model (ISO 7498-4 OSI Reference Model Part 4: Management Framework).

The architecture is based on the definition of the following basic entities:

1) the METER, which examines streams of packets on a communications medium or between a pair of media and aggregates the results of those measurements. Meters count certain attributes (such as numbers of packets and bytes) and classify them as belonging to ACCOUNTABLE ENTITIES using other attributes (such as source and destination addresses). An accountable entity is someone who (or something which) is responsible for some activity on the network. It may be a user, a host system, a network, a group of networks, etc., depending on the granularity specified by the meter's configuration. Meters are placed at measurement points determined by network Operations personnel (e.g. in Routers or dedicated traffic monitors). Each meter selectively records network activity as directed by its configuration settings. It can also aggregate, transform and further process the recorded activity before the data is stored. The processed and stored results are called the 'usage data.'

2) the COLLECTOR, or METER READER, which is responsible for the integrity and security of METER data in short-term storage and transit. A meter reader reliably transports usage data from meters so that it is available to analysis applications.

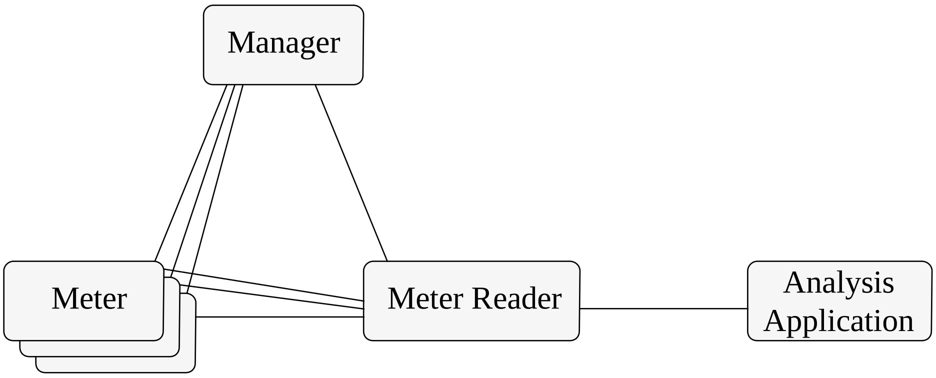
3) the ANALYSIS APPLICATION which processes the usage data so as to provide information and reports which are useful for network engineering and management purposes. Examples include:

- TRAFFIC FLOW MATRICES, showing the total flow rates for many of the possible paths within the managed portion of the ATN.
- FLOW RATE FREQUENCY DISTRIBUTIONS, indicating how flow rates vary with time.
- USAGE DATA showing the total traffic volumes sent and received by particular systems.

4) The traffic measurement MANAGER: it is an application which configures 'meter' entities and controls 'meter reader' entities. It uses the data requirements of analysis

applications to determine the appropriate configurations for each meter, and the proper operation of each meter reader. The meter reader and the manager may be combined within a single network entity.

The relationships between these 4 entities are shown in the following figure:



5.4.2.2 Interaction Between METER and METER READER

The information which travels along this path is the usage data itself. A meter holds usage data in an array of flow data records known as the FLOW TABLE. A meter reader may collect the data in any suitable manner. For example it might upload a copy of the whole flow table using a file transfer protocol, or read the records in the current flow set one at a time using a suitable data transfer protocol.

A meter reader may collect usage data from one or more meters. Data may be collected from the meters at any time. There is no requirement for collections to be synchronised in any way.

5.4.2.3 Interaction Between MANAGER and METER

A manager is responsible for configuring and controlling one or more meters. Each meter's configuration includes information such as:

- Flow specifications, e.g. which traffic flows are to be measured, how they are to be aggregated, and any data the meter is required to compute for each flow being measured.

- Meter control parameters, e.g. the maximum size of its flow table, the 'inactivity' time for flows (if no packets belonging to a flow are seen for this time the flow is considered to have ended, i.e. to have become idle).
- Sampling rate (when the local accounting policy does not require the observation of every packets)

5.4.2.4 Interaction Between MANAGER and METER READER

A manager is responsible for configuring and controlling one or more meter readers. A meter reader needs to know at least the following for every meter it is collecting usage data from:

- The meter's unique identity, i.e. its network name or address.
- How often usage data is to be collected from the meter.
- Which flow records are to be collected (e.g. all active flows, the whole flow table, flows seen since a given time, etc.).
- Which attribute values are to be collected for the required flow records (e.g. all attributes, or a small subset of them)

5.4.2.5 METER READERs and APPLICATIONs

Once a collection of usage data has been assembled by a meter reader it can be processed by an analysis application. A possible application may be the automatic generation of bills. Other applications may be dedicated to the generation of network usage reports for network planning activities.

5.4.3 Accounting management co-ordination

5.4.3.1 Introduction

For a number of organisations participating in the ATN, accounting management will be considered as a private process which does not require any technical co-ordination with other organisations. These organisations will perform the usage data collection and analysis activities on their own and interactions with other organisations will be limited to the exchange of bills between finance departments. Upon occasion, requests for verification of bills will arise; but this is typically handled through the finance process rather than the network management process.

On the other hand, other organisations may be willing to enter into partnership so as to share the accounting management structure, minimise the billing interactions with common external users or service providers and simplify the internal redistribution of costs and benefits between partner organisations. This may typically be the case of European ATSOs, which could be willing to combine and centralise the accounting post-processing tasks of maintaining the accounting database, generating reports, distributing bills, collecting revenue, etc ...

For those organisations accounting management co-ordination will be required. This section analyses possible co-operation scenarios with the intent to identify the possible requirements for specification of common standard accounting information exchange procedures.

5.4.3.2 Accounting Management co-ordination scenarios

5.4.3.2.1 General

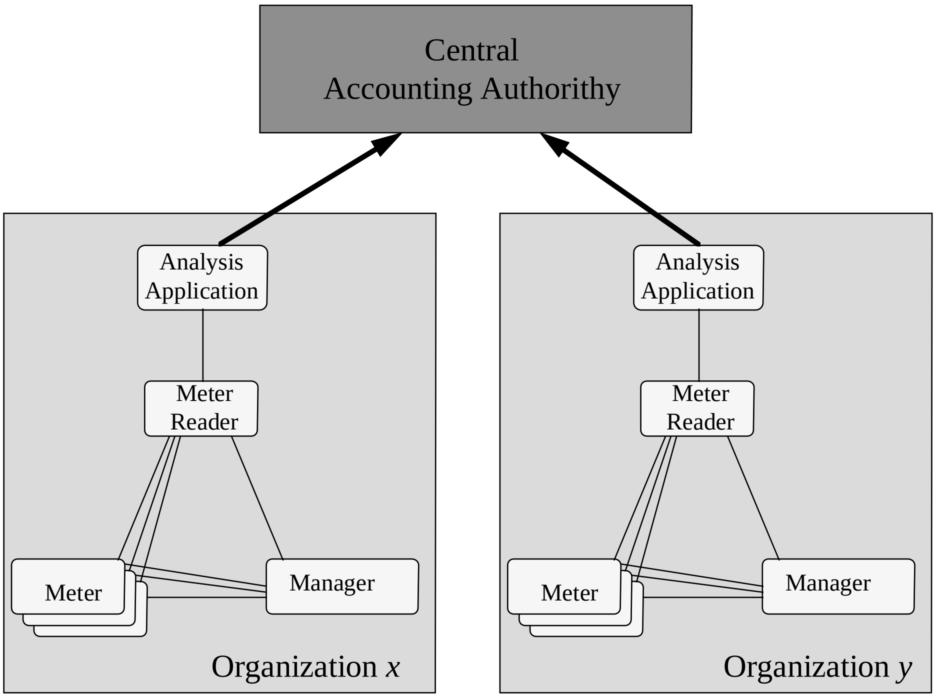
Each scenario considered in this section presents the following common characteristics:

- It is assumed that there is a central accounting authority, the ultimate goal of which is to perform the post processing billing and revenue collection activities on behalf of all partner organisations.
- The overall accounting management architecture is based on the implementation of meters, meter readers, traffic measurement manager and analysis applications as introduced in the previous section

The variations between the different scenarios arise from the difference of location of the meter readers, traffic measurement managers and analysis applications. Depending on the scenario, these entities are either assumed to be centralised and under the responsibility of the central accounting authority or distributed within organisations and under the responsibility of each of those organisations. The meters are distributed by nature, and are assumed to be under the responsibility of entity which is responsible of the traffic measurement manager.

5.4.3.2.2 Scenario 1: maximum distribution of the accounting management activities

This first scenario assumes that meters, meter readers, traffic measurement managers, and analysis applications remain under the responsibility of every partner organisation. The central accounting authority is then assumed to perform its billing and revenue collection activities on the basis of information elements resulting from the analysis applications operated by the individual organisations. This scenario is depicted in the figure below:



The implication of this scenario is that accounting analysis reports will need to be exchanged between the organisations and the central accounting authority. This will require the specification of common standards for:

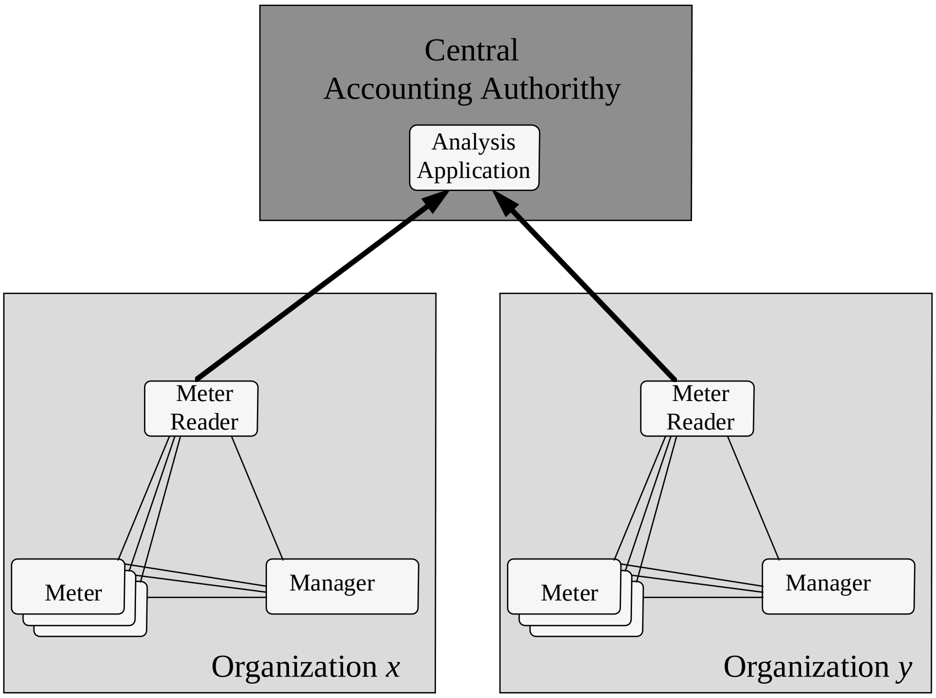
1. The content and forms of these reports;
2. The mechanisms of exchange of these reports (e.g. fax, mail, electronic mail, file transfer programs, etc...);
3. The issuing periods of these reports

This scenario is very simple with regard to the interactions involved at the boundary of administrative domains. On the other hand, this simple scenario presents the following drawbacks:

1. The accounting data collection, collection management and analysis processes need to be performed within each organisation.
2. The analysis reports processed by the central accounting may hide details that would be required for an accurate and truly equitable accounting.

5.4.3.2.3 Scenario 2: centralisation of the analysis applications

This second scenario assumes that meters, meter readers, traffic measurement managers remain under the responsibility of every partner organisation, while the analysis application is in the hands of the central accounting authority. This scenario is depicted in the figure below:



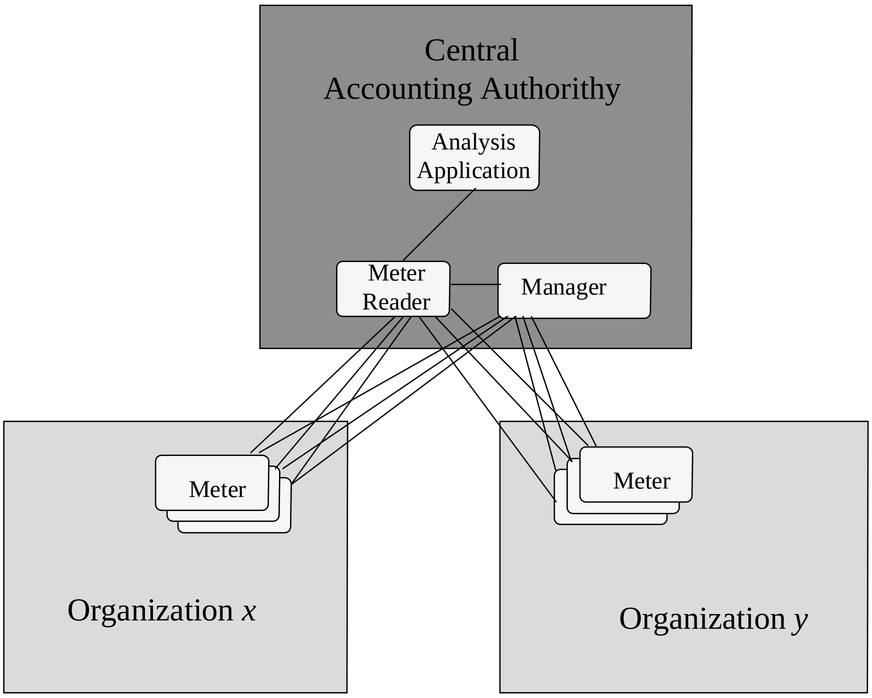
With this scenario, the collected usage data, that is assumed to be stored periodically in flow data files on the meter reader, will be exchanged between the organisations and the central accounting authority. This will require the specification of common standards for:

1. The content and forms of the flow data files;
2. The mechanisms of exchange of these files (e.g. file transfer programs, etc...);
3. The interval of times at which the meter readers must collect usage data accumulated by the meters.
4. Usage data retention periods
5. Access control functions for protecting data integrity and confidentiality

This scenario is more complex than the first one with regard to the interactions involved at the boundary of administrative domains. On the other hand, it allows to alleviate the individual organisations from their independent accounting data analysis activities and makes possible the global automation of the accounting process.

5.4.3.2.4 Scenario 3: maximum centralisation of the accounting management activities

This third scenario assumes that meter readers, traffic measurement managers and analysis applications are operated by the central accounting authority. This scenario is depicted in the figure below:



This scenario requires the specification of standard mechanisms for the management of meters and for the collection/reporting of usage data. This assume the definition of a common Network Management Protocols (e.g. CMIP, SNMP) and of common accounting metering functions and managed object (e.g. ISO/IEC 10164-10, RFC 2064).

This scenario allows to alleviate the individual organisations from all accounting management activities. Its main drawback is to force the implementation of a specific network management protocol within the systems supporting the meters. This approach may therefore remove the freedom that organisations have on the choice of the technology used internally for Network Management. The solution to overcome this problem would be to agree on a set of several possible metering management and collection interfaces (e.g. CMIP with ISO/IEC 10164-10, and SNMP with RFC 2064) and to ask each partner organisations to select one of the possible alternatives. The Central Accounting Authority would then have to support each of these multiple possible interface but this seems preferable to constraining the partner organisation in their choice for a network management technology

5.5 Configuration Management

5.5.1 Introduction

Configuration Management is certainly a domain which will require co-ordination between the different organisations involved in the ATN. This is because certain aspects of the configuration of an ATN system within an organisation will often impact or depend on the configuration of other ATN systems in other organisations; then, if we assume, as it is likely, that the responsibility for the setting and update of the configuration of the individual ATN systems will be distributed among different and multiple organisations, the requirement for co-ordination of the configuration management activities becomes obvious.

Co-ordination for configuration of the ATN systems will be required on the following aspects:

1. The attribution of values to the ATN systems configuration parameters
2. The exchange of information on the current configuration of ATN systems
3. The modification to the current configurations

5.5.2 Co-ordination for the attribution of values to ATN systems configuration parameters

The attribution of value to certain ATN system configuration parameters may be dependent on or impact the configuration of ATN systems of other organisations. In certain cases, co-ordination will therefore be required among group of organisations 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 co-ordination should simply result in the production of documents recording the agreements.

5.5.3 Exchange of information on the current configuration of ATN systems

With the exception of some parameters, such as the addresses of the systems, the requirements for the exchange of configuration information between organisations are difficult to identify.

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

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

There are several possible scenarios for the exchange of the configuration information, ranging from the exchange of questions/answers by mail between the network administrators, to inter-domain manager-agent interactions for dynamic consultation of the content of the MIB of the ATN systems.

Between European ATSOs, the most likely scenario for the exchange of configuration information is the one which is currently proposed for the management of the CIDIN: each European ATSO would provide the configuration data on a regular schedule to the regional administrator, and these data would then be entered into a central database which would then serve for the production of reports on the overall European ATN network configuration.

This approach would require the specification of common standard for:

1. the identification and definition of the configuration parameters which value has to be provided by each organisation
2. the format used for the configuration data exchange (e.g. plain text forms)
3. the mechanisms for the exchange of the configuration data (e.g. electronic mail)
4. the issuing periods

A possible alternative to this scenario could be to follow, for the exchange of configuration information, the same approach as the one identified for the exchange of operational statistics (see section 5.2.3): the configuration information would be provided as part of the 'ATN domain summary MIB' maintained by every organisation. Other organisation could access this information by browsing the summary MIB content. This approach would require the specification of common standard for:

1. The Managed Object Classes used to hold the configuration information
2. The Management Information exchange protocol (e.g. CMIP, SNMP)
3. The information update period

5.5.4 co-ordination for the modification to the current configurations

5.5.4.1 General

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

1. Evolution/extention/enhancement of the ATN network
2. Network reconfiguration in case of problem
3. New aircraft are equipped with ATN systems and need to be recognised by the ground and air/ground systems

The third scenario is considered to be a security management problem. It is analysed in section 5.6.

5.5.4.2 Changes in the configuration due to expansion and improvement of the network

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 co-ordination between the network administrators. Co-ordination 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.

5.5.4.3 Reconfiguration in case of problem

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 co-ordination between the network operators and possibly the regional supervisor, if any. Co-ordination will consist in the spontaneous set-up of a dialogue for discussion of the problem, agreement on a correction, and synchronisation of recovery actions. The phone, the electronic mail, and the trouble ticket systems will be the tools used all along the reconfiguration process.

5.6 Security Management

5.6.1 Introduction

The purpose of security management is to support the application of security policies by means of functions which include:

1. the creation, deletion and control of security services and mechanisms,
2. the distribution of security-relevant information; and
3. the reporting of security-relevant events

Security management assumes that security mechanisms are implemented. At the time this report is produced the security mechanisms for the ATN are still under definition. It would therefore be premature to try develop scenarios on security management issues, while the ATN security mechanisms, that will be standardised in the Package 2 ATN SARPs, are not developed further by the ICAO technical committees.

There might however be security management issues to be considered in the context of the management of an ATN Network consisting of Package 1 ATN systems. Indeed, although the Package 1 ATN SARPs do not specify any overall security mechanism for the ATN, they include at least one basic function that will provide some levels of security in the initial stage of the ATN implementation. This function concerns the validation of aiborne routers address by Air/Ground router. Security management issues pertaining to this function are discussed in the next section.

5.6.2 Management of authorised airborne routers addresses

The “ NET validation function ” implemented within ATN A/G BIS allows the A/G routers to validate the acceptability of the connection with an airborne router. If an A/G router does not validate the airborne router address, it must terminate the connection.

The ATN SARPs do not specify exactly how the NET validation function must determine the acceptability of the airborne routers addresses, but the most likely procedure will be the comparison of the address received from the airborne router with a list of authorised addresses configured at the level of each ATN A/G Router.

This pauses the problem of the maintenance of this list of authorised airborne addresses in the A/G routers. A likely scenario is simply that network administrators will receive regularly announcements on the existence of a new ATN-equipped aircraft, with information on their configuration (addresses, support or non support of IDRP, etc..). The network administrators will then plan the reconfiguration of the A/G BISs, and the network operators will later on perform this reconfiguration using their local ATN system configuration mechanisms.

This scenario would require the definition of standard procedures and forms for the announcement of new airborne router addresses. In Europe, it is assumed that the regional administrator could be in charge of collecting these announcements from the airlines, and of publishing regularly the new list of addresses.

6 Conclusions

The ATN System Management Concept of Operations identifies the need for the standardization of the information exchange between Management Domains. The information fits into two categories:

that which needs to be exchanged off-line, and

that which needs to be exchanged on-line.

For the information that will be exchanged off-line, SARPs must be developed that define the information, define how the information may be exchanged, and define what the responsibilities of the organizations receiving that information.

For the information that will exchanged on-line, SARPs must be developed. This document recongnizes that for the exchange of management information, CMIP is the appropriate protocol for the exchange. SARPs are required to specify the subset and use of CMIP in the ATN environment. It is also concluded that all management information that may be exchanged across domains must be specified to a level of detail that ensures interoperability. This would mean that a GDMO description of all information is required.