CHAPTER 12 SYSTEMS MANAGEMENT GUIDANCE

12.1 Introduction

The System Management material presented within this Manual is intended to support management of the Network and Transport Layer entities in ATN intermediate-systems and end-systems in general, and ATN Boundary Intermediate Systems in particular. This material has been developed based on the recognition that in order for a diverse networking environment such as the ATN to function successfully, certain layer management capabilities must be an integrated part of these ESs and ISs. As such, this material constitutes the baseline level of System Management functionality necessary to ensure the reliable operation of the ATN.

While it is expected that these management provisions will be implemented in many end-systems and intermediate-systems in both fixed and mobile installations, this does not imply or mandate the exchange of management information over limited-throughput mobile subnetworks where no operational requirement for such exchanges exists.

12.1.1 Overview

Systems management provides mechanisms for the monitoring, control and co-ordination of resources and uses OSI protocols for communicating information pertinent to those resources. In order to describe management operations on resources, the resources are viewed as managed objects with defined properties. Information required for systems management purposes in any open system may be provided through local input, may result from communication with other open systems or may be a result of lower layer protocol exchanges.

Systems Management may be distributed, centralized or local, these considerations are not subject to ISO standardization.

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.

12.1.2 General Considerations

Systems Management Applications (SMAs) are Management Information Service Users (MIS-Users) operating in either the manager (SMA-Manager) or agent role (SMA-Agent) as described in ISO/IEC 10040. SMA-Agents manage the local system and perform operations on managed objects in response to communications from an MIS-User taking the Manager role, they also emit notifications. SMA-Managers are part of the distributed management application which has the responsibility for one or more management activities, they issue management operations and receive notifications but may themselves be managed.

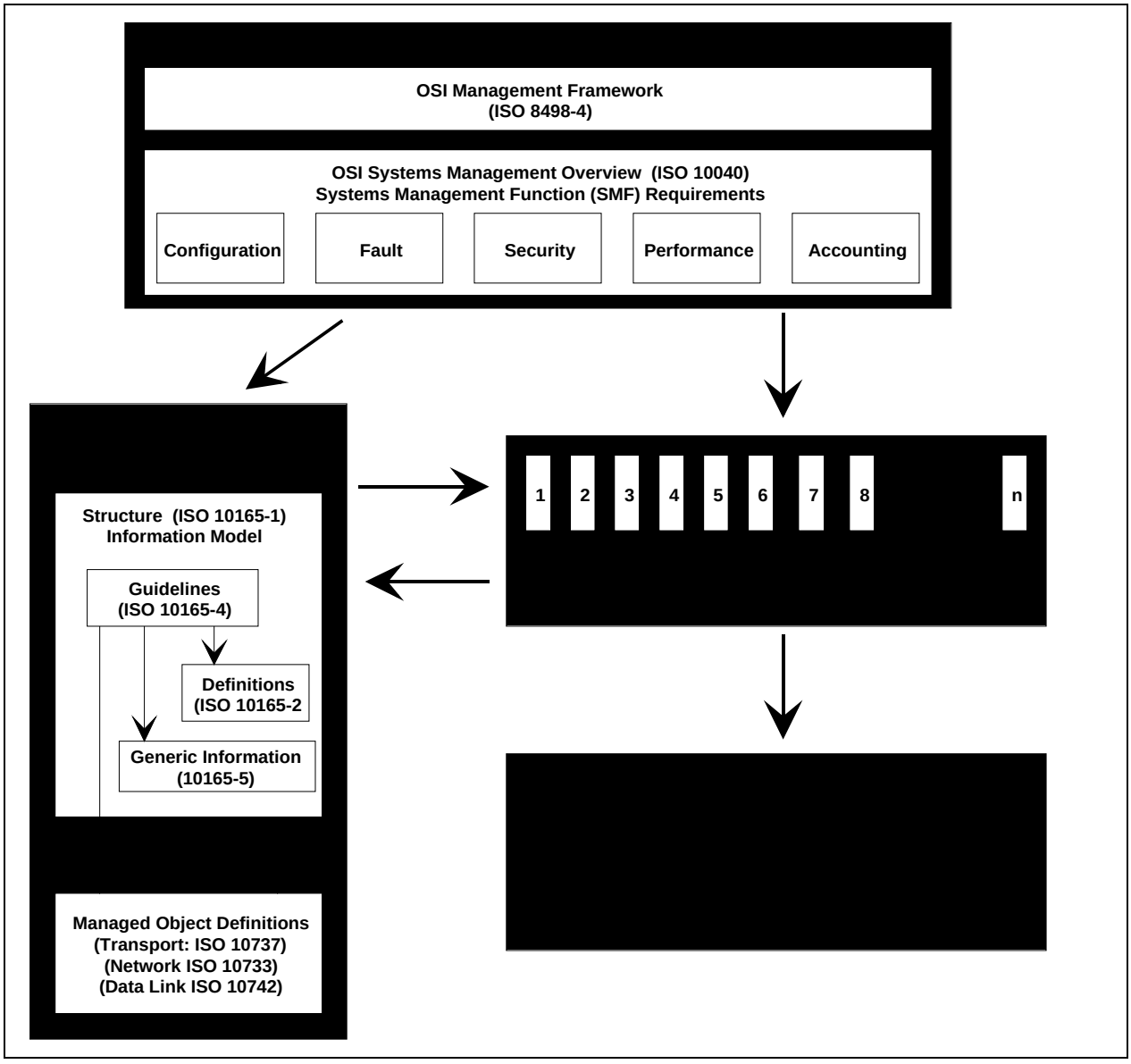

Figure 12.1: System Management Standards

In the ATN, Systems Management Functions (SMFs) are made available to SMAs via the Systems Management Application Entity (SMAE) in the application layer.

Managed objects may be specific to a layer in which case they are known as (N)-Layer Managed Objects. Those managed objects that are relevant to more than one layer, to a specific system management function (management support) or to the system as a whole are known as System Managed Objects. The set of objects in a system, together with their attributes constitutes that system's Management Information Base (MIB). The MIB is available to applications via the SMAE.

The ATN Systems Management Profile includes the Application Layer, Presentation Layer and Session Layer specifications and is further described in sections 12.3 and 12.4. Management information is exchanged between SMAs using the ATN Systems Management Profile defined in Sections 12.3 and 12.4 of this document.

SMAs use management communication services resident in the Application Layer. These services are contained within the Systems Management Application Entity (SMAE). Some of the key services include::

- the Common Management Information Service Element (CMISE) defined in ISO/IEC 9595,
- the Remote Operations Service Elementdefined in ISO/IEC 9072-1,
- the Association Control Service Element defined in ISO 8649.

CMIS defines the Common Management Information Service Element that will be used to exchange information in management operations and notifications for the purposes of systems management. The Common Management Information Protocol specifies a protocol to support CMIS; it is used by SMAEs to exchange management information.

ROSE defined in ISO/IEC 9072-1 is required by CMISE and it in turn assumes the use of ACSE and the presentation service P-Data service element defined in ISO 8822.

ACSE is required to manage associations between Systems Management Applications (SMAs). The service provided by the ACSE is defined in ISO 8649. The ACSE and the ACSE protocol are defined in ISO 8650.

Together CMISE, ROSE and ACSE provide the services of the SMAE in the application layer.

The ATN Systems Management Profile uses the ATN Internet to relay management communications. Management systems incorporate the ATN Internet Profile as defined and described in this manual. The term 'ATN Internet Profile' is used to encompass the definitions of the Transport and Network layers in this document and is a multi-part profile.

12.2 Systems 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.

A systems management function may satisfy more than one requirement and to satisfy some requirements, more than one function may be applicable (e.g. several functions described below are applicable to security). The specification of a systems management function defines the management activities and information that are necessary to meet the requirements.

The functional model introduces the concept of Specific Management Functional Areas (SMFAs). A SMFA comprises all management activities which are directed to a common network aspect, e.g. network security, network configuration, etc.

Systems Management function definitions consist of:

- generic definitions to be made available for general use (e.g. a common set of alarm types);
- services for management purposes (e.g. the alarm reporting service allows one user to notify another user of an alarm detected in a managed object);

- functional units, a named set of systems management services defined for the purpose of identifying sets of functionality, the use of which may be established between end systems. The sets may also be defined so that they may be referenced by other ISO standards. A functional unit definition may be null.

It should be noted that the definitions of functions has been carried out such that they are independent of the underlying communication service.

Standardization has been directed to define classes of Systems Management Objects (ISO/IEC 10165-2) and Systems Management Functions (ISO/IEC 10164 all parts) that use those generic object classes. These definitions will be of general use in open systems.

The general requirements for Systems Management Functions are briefly described below.

12.2.1 Object Management Function (ISO/IEC 10164-1)

The management user must be able to create, delete, examine and change the set of Managed Objects that forms part of the OSI environment. The user also needs the ability to examine and modify individual items of information about parts of the OSI environment, such as the operational parameters affecting the operation of each part. All changes in the configuration must be notified.

Included in this function is the definition of a service (defined as a functional unit) that maps functionality onto the communications infrastructure using CMIS.

12.2.2 State Management Function (ISO/IEC 10164-2)

The management user must be able to examine and be notified of changes in state, to monitor overall operability and usage of resources in a consistent manner, and to control the general availability of specific resources.

12.2.3 Attributes for Representing Relationships (ISO/IEC 10164-3)

The management user must be able to examine the relationship among various parts of the system, to see how the operation of one part of the system depends on, or is dependent on other parts. The user also needs the ability to change relationships and to be notified of such changes when they occur due to other causes.

12.2.4 Alarm Reporting Function (ISO/IEC 10164-4)

The function defines the reporting of alarms,errors and related information in a standard fashion.

12.2.5 Event Report Management Function (ISO/IEC 10164-5)

The function defines:

- a flexible event report control service which will allow systems to select which event reports are to be sent to particular managing systems;
- a specification for destinations for event reports (including the local system);
- a specification of the mechanism to control the forwarding of event reports by suspending or resuming them;
- a user capability to modify the conditions under which reports are sent;
- a user capability to designate a backup location to which event reports should be sent if the primary location is not available.

12.2.6 Log Control Function (ISO/IEC 10164-6)

Many management functions need to preserve information about events that have occurred or operations that may have been performed on various objects. In a real open system resources will be allocated to store such information, these will be logs containing log records.

The above requires the following:

- the definition of a flexible log control service that allows the selection of the information to be logged and to change that selection in a managed system;
- the ability to modify the criteria for logging information;
- the ability to determine whether log characteristics have changed or logs have been lost;
- the specification of a mechanism to control log timing and on/off switch;
- the ability to retrieve and delete log records;
- the ability to create and delete logs.

12.2.7 Security Alarm Reporting Function (ISO/IEC 10164-7)

The security management user must:

- receive notifications of security related events and must be made aware of any malfunctioning of security services and mechanisms;
- be made aware of attacks and breaches of system security;
- be informed of the perceived severity of any failed operation, attack or breach of security;

12.2.8 Security Audit Trail Function (ISO/IEC 10164-8)

The security management user must be able to record in a security audit trail log, security related events that occur in the management domain. The security policy of an open system may require that particular security-related events be sent to a security audit trail log in the same or in a different open system.

12.2.9 Access Control Function (ISO/IEC 10164-9)

The OSI management user requires that unauthorized access to OSI management applications and management applications be prevented by the use of one or more access control mechanisms. Control of access management is required in each of the following areas.

- to prevent unauthorized establishment of OSI Management associations;
- to protect management information from unauthorized creation, deletion, modification or disclosure by means of OSI management operations;
- to prevent unauthorized initiators from using management operations;
- to prevent management information from being transmitted to unauthorized recipients by means of confirmed and non-confirmed event reports.

Various levels of access control may be required (e.g. read only access as opposed to read/write). Some users may be granted access control to some managed objects but not to others.

12.2.10 Accounting Meter Function (ISO/IEC 10164-10)

Users of an OSI service need management information advising them of the use of resources. Accounting records derived from data supplied by accounting meters are required to provide an historical record of the usage of resources.

12.2.11 Workload Monitoring Function (ISO/IEC 10164-11)

The following requirements are identified:

- the definition of statistical monitoring tools to derive metrics to characterize performance;
- the definition of a monitoring function which provides metrics of the workload, workload rejected and the resources used;

- the specification of mechanisms to obtain these metrics;
- the specification of notifications to be generated when these metrics exceed threshold values, and the ability to include additional performance information in those notifications;
- the specification of mechanisms to control the operation of this function, for example to initiate and terminate monitoring;
- the ability for an external managing system to modify parameters defined and used in this monitoring system;
- the ability to model either physical capacity limitations or those limitations imposed by administrative decisions;
- the ability for a metric object to observe a managed object that is in the same system;
- the scheduling of metric monitoring over a specified period of time.

12.2.12 Test Management Function (ISO/IEC 10164-12)

The specification is intended to satisfy requirements for the remote control of tests involving real open systems and the specification of tests which exercise OSI resources.

A test is the operation and monitoring of open systems, or parts thereof, within an environment designed to elicit information regarding the functionality and/or performance of the subject systems. It will involve the creation of a test environment and subsequent restoration of the operational environment after the test.

Tests will need to be scheduled. It should be possible to create complex tests from simpler ones. Some example tests might be loop back tests, fault injection tests, self tests, saturation tests.

12.2.13 Summarization Function (ISO/IEC 10164-13)

Performance monitoring aspects of performance management imply requirements to measure throughput, response times, availability, and other measures of congestion and resource utilization. This will require the acquisition of attribute(s) from managed object(s) throughout a period of time and the analysis of this information according to algorithms in order to present a summary.

12.2.14 Confidence and Diagnostic Tests (ISO/IEC 10164-14)

Confidence and diagnostic tests are required in order to investigate:

- the ability of a resource to perform its allotted function;
- the ability of any part of the communications system to establish a connection between a number of open systems and to transfer data without alteration between a number of systems;
- the integrity of a protocol;
- the effect of increased utilization of a resource;
- the ability to set up the necessary actions in order to identify the cause of a failure.

12.2.15 Scheduling Function (ISO/IEC 10164-15)

Many management functions will require scheduling at predefined times or intervals.

12.2.16 Performance Management Function (ISO/IEC 10164-B)

Performance management enables the behavior of resources in the OSIE and the effectiveness of communication resources to be evaluated. Performance management includes functions to:

- gather statistical data;
- maintain and examine logs of system state histories;

- determine system performance under natural and artificial conditions;
- alter system modes of operation for the purpose of conducting performance management activities.

12.2.17 Management Knowledge Management Function (ISO/IEC 10164-16)

Open systems participating in OSI Systems Management associations may need specific knowledge in order to determine the peer open systems with which to associate, to enable an association and to fulfil the functions of distributed OSI Systems Management.

The types of knowledge needed by managing systems will be:

- Managed Object Class knowledge e.g. which MO classes are made available by a given system;
- Managed Object Instance knowledge e.g. which MO instances exist in a given system;
- Naming schema knowledge e.g. name bindings and hierarchies;
- Relationship knowledge e.g. which relationship types are known;
- Relationship instance knowledge e.g. which relationships exist in a system;
- MIS-user knowledge, (there is a need to determine the AE titles of the systems with which management associations can be established, the presentation addresses of those systems, the application contexts supported and associated syntaxes and which functional units for SMF, CMISE, ACSE, presentation, session are supported);
- The formal definitions of management information;
- Domains and Policy knowledge e.g. which domains a managed object instance is a member of, which policies a managed object is subject to.

12.2.18 Management Domain Management Function

Managed objects may be grouped into management domains for logistic or other management reasons. Managed objects may be associated with more than one Management Domain and therefore subject to more than one policy. It is the objective that polices will be consistent from the design stage, but inconsistencies may arise during operations, these must be reported and appropriate action taken.

Functional requirements are summarized below:

- All members of a management domain may be members of other management domains;
- Management Domain MOs, management policy MOs, the relationship between a management domain and its members, the relationship between a policy and a domain and the MO providing conflict detection to be provided;
- A mechanism to manage the change of systems management policies;
- A mechanism for managing the membership of a domain;
- A mechanism for manipulating other domain specific characteristics;
- A mechanism for discovering and managing the relationships among management domains.

12.2.19 Change Over Function

This function provides specifications for the identification, choice, management and termination of a back up service for those managed objects which participate in a fallback or a backup relationship.

Backup services consist of a service that causes a managed object to backup of another managed object and a service that terminates this backup. By sending a change over action to a managed object of backup control

function the backup is made while the backup is released by sending a change back action to the managed object. Functions supporting the backup services are called “Change Over Function”.

12.2.20 Software Management Function

Software Management must be able to satisfy the following requirements, subject to possible imposed controls and conditions:

- be able to request delivery of software to a specific managed system
- be able to control the installation of software on a managed system, including the installation of patches (e.g. upgrades) and to revert back to a previous version of the software
- be able to initiate the execution of a software program
- be able to inquire as to the attributes of all software held on a managed system
- be able to create and delete the management view of software resources held on a managed system
- be able to validate software held on a managed system in order to check its integrity and to terminate validation
- be able to use of software resources on a managed system for administrative purposes
- be able to back up a software item and to restore a previously backed up software item

12.3 Systems Management Services

Note.— This section describes those services which are expected for the use of management applications, i.e., CMIS and ACSE services.

12.3.1 Management Communication Services

The ability is required to exchange and/or modify management information between the elements in a management domain. This will require supporting communication services. Shared management information manifests itself in terms of distributed management applications.

Management knowledge can be established at any time, specifically:

- prior to any communication taking place (e.g., system build, start-up)
- during an application association establishment phase (ISO 8649)
- subsequently, during the lifetime of the association.

Having set up an association for the purposes of system management, a mechanism may be used to modify or acquire management knowledge. This mechanism will involve the use of communication services such as the OSI Common Management Information Service (CMIS), which defines a set of communication service primitives (they constitute an application service element); these services use the Common Management Information Protocol (CMIP) for information exchange. CMIS has been standardized in ISO 9595 and CMIP in ISO 9596. The CMIS services are provided in the application layer by the CMIS Service Element (CMISE).

Note.— Other application service elements may also be used for management communication. For example OSI File Transfer, Access and Management (FTAM, ISO 8571) may be used for the bulk transfer of files of management information.

Management information services are used by applications in peer open systems to exchange information and commands for the purposes of system management.

12.3.2 Association Services

Systems Management is based on a connection-oriented information exchange mode. Therefore, an association with a peer user is required before any of the CMIS services can be used. In contrast to earlier draft versions, the international CMIS standard ISO 9595 does not provide any services for the establishment and release of management application associations. Management application processes have to utilize the services of the Association Control Service Element (ACSE, ISO 8649), which is another ASE, for the control of application-associations.

ACSE is used to establish, terminate, or abort an association between cooperating application entities. During the association establishment phase, various ASEs may exchange initialization information to establish an association using ACSE. The application context specifies the rules required for coordinating the information belonging to different ASEs, embedded in the ACSE user information service parameters.

The A-ASSOCIATE service of ISO 8649 is invoked by a CMISE-service user to establish an association with a peer CMISE-service user. Association establishment is the first phase of any instance of management information service activity. The application context, presentation and session requirements are conveyed using parameters of the A-ASSOCIATE service.

The A-RELEASE and A-ABORT services of ISO 8649 are used for the termination of an association. They may be invoked by either of the peer CMISE-service users.

Note.— The authentification functional unit is not described since it is not contained in the profile described in this chapter.

12.3.3 The Common Management Information Service (CMIS)

This section gives a brief overview of CMIS.

There are two types of information transfer service:

a) a management notification service

b) a management operation service

The definition of the operation/notification and the consequent behavior of the communicating entities is dependent on the managed object at which the operation is directed, or which generated the notification. It is outside the scope of CMIS. However, certain operations and notifications are used frequently within the scope of systems management and CMIS provides the following definitions of the common services that may be used to convey management information applicable to the operations/notifications.

The CMISE-services will relate to identified managed objects. The services are parameterized to allow the selection of one or many objects and attributes from the managed object hierarchy, this is termed scoping and filtering. When multiple objects are selected, the operations may be synchronized using the synchronization parameter.

12.3.3.1 Management Notification Services

The M-EVENT-REPORT service is invoked by a CMISE-service user to report an event about a managed object to a peer CMISE-service-user. The service may be requested in a confirmed or a non-confirmed mode. In the confirmed mode a reply is expected.

12.3.3.2 Management Operation Services

The M-GET service is invoked by a CMISE-service user to request the retrieval of information from a peer CMISE-service-user. The service may only be requested in a confirmed mode. In the confirmed mode, a reply is expected.

The M-SET service is invoked by a CMISE-service user to request modification of management information from a peer CMISE-service-user. The service may be requested in a confirmed or a non-confirmed mode. In the confirmed mode a reply is expected.

The M-ACTION service is invoked by a CMISE-service user to request a peer CMISE-service-user to perform an action. The service may be requested in a confirmed or a non-confirmed mode. In the confirmed mode a reply is expected.

The M-CREATE service is invoked by a CMISE-service user to request a peer CMISE-service-user to create an instance of a managed object. The service may only be requested in a confirmed mode. In the confirmed mode, a reply is expected.

The M-DELETE service is invoked by a CMISE-service user to request a peer CMISE-service-user to delete an instance of a managed object. The service may only be requested in a confirmed mode. In the confirmed mode, a reply is expected.

The M-CANCEL-GET service is invoked by a CMISE-service user to request a peer CMISE-service-user to cancel a previously requested and currently outstanding invocation of the M-GET service. The service may only be requested in a confirmed mode. In the confirmed mode, a reply is expected.

12.3.3.3 CMIS Functional Units

The CMIS general service capabilities are classified into functional units which correspond to the support of service primitives or parameters. Only the Kernel functional unit is mandatory in implementations of CMIP which conform to ISO 9596-1. The functional units defined in ISO 9595 are:

a) The *Kernel* functional unit includes all the CMIS services listed above except for M-CANCEL-GET. Scoping and filtering for managed object selection are not supported and neither is the CMIS synchronization service.

b) The *Cancel-Get* functional unit makes available the use of the M-CANCEL-GET service.

c) The *Multiple Object Selection* functional unit makes available the use of the scope and synchronization parameters in the services provided by the Kernel functional unit. The scope parameter allows one or more managed objects to be selected based on a sub-tree within the managed object containment hierarchy. The synchronization parameter indicates how the invoking CMISE-service-user requires the requested operation synchronized across the selected object instances. If the Multiple Object Selection functional unit is proposed for use on a given association, then the Multiple Reply functional unit must also be proposed.

d) The *Multiple Reply* functional unit makes available the use of the 'linked identification' parameter in the services provided by the Kernel functional unit, and allows for more than one response to be generated for a given management operation if the invoking CMISE-service-user selects multiple managed objects or requests an M-ACTION operation for a single managed object in which the action is defined to produce multiple responses.

e) The *Filter* functional unit makes available the use of the filter parameter in the services provided by the Kernel functional unit. This parameter is concerned with the selection of one or more managed objects which satisfy defined criteria.

f) The *Extended Service* functional unit makes available presentation services in addition to the P-DATA service.

12.4 ATN Systems Management Protocols

The Common Management Information Protocol (CMIP) is a standardized procedure (ISO 9596) which specifies protocol elements that may be used to provide the operation and notification services required by CMIS. It supports a request/response service between peer users in OSI open systems.

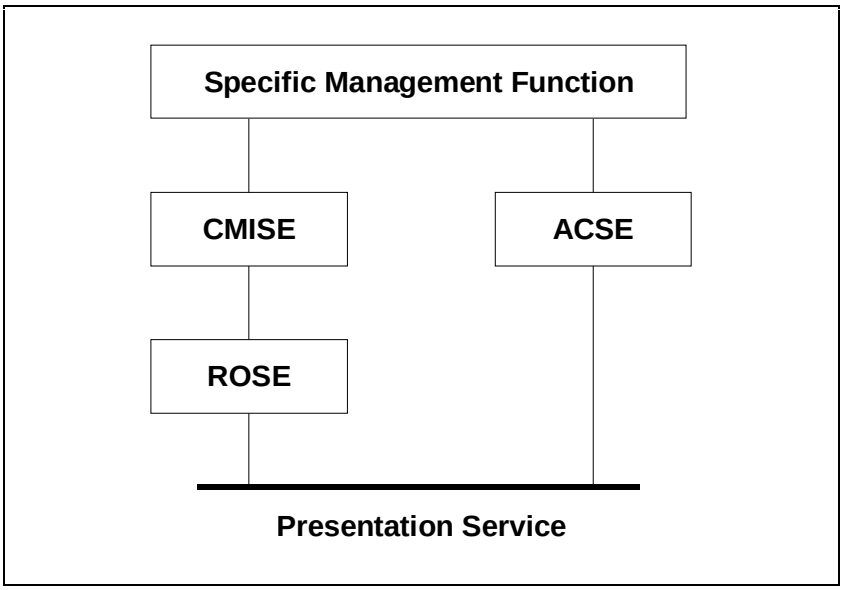

Figure 12.2: OSI Protocol Stack for Management Communications

The CMIP specification provides:

- procedures for the transmission of management information between application entities residing in end systems
- the abstract syntax and, by application of associated encoding rules, the transfer syntax
- procedures for the correct interpretation of protocol control information
- a written procedure for each CMIS primitive
- conformance requirements for systems claiming to implement the CMIP procedures.

12.4.1 Profiles for Management Communication

In the ATN environment, profiles for system management are needed, describing the Application Layer protocols and the supporting services needed (if appropriate) from the Presentation and Session Layers. The Application Layer protocols supporting the control of managed objects are CMIP (ISO 9596-1), Remote Operation Service Element (ROSE) protocol specification (ISO 9072-2) and ACSE protocol specification (ISO 8650). This protocol stack is illustrated in Figure 12.2.

Note.— System management may also require a bulk data transfer protocol.

Standardized profiles for OSI systems management are classified hierarchically in the Taxonomy of International Standardized Profiles (ISO TR 10000) as connection-oriented application profiles (A-profiles) identified by the prefix 'AOM', as follows:

AOM nn OSI Management

1n Management Communications

11 Basic Management Communications

12 Enhanced Management Communications

2n Management Functions

21 Management Capability

211 General management capabilities

212 Alarm Reporting and State management capabilities

213 Alarm Reporting capability

22 Event Report Management

221 General Event Report Management

23 Log Control

231 General log control

Management communication profiles are thus classified under the 'AOM 1x' arc.

AOM 11 (standardized as ISO/IEC 11183-3) specifies support for the CMIS Kernel functional unit that allows simple management operations and notification. (It excludes the Multiple Object Selection, Cancel Get, Extended Service and Multiple Reply functional units).

AOM 12 (standardized as ISO/IEC 11183-2) specifies support for the following CMIS functional units:

- Kernel
- Multiple Object Selection (scoping)
- Filter
- Cancel Get
- Multiple Reply

Scoping and filtering, although requiring greater processing and memory capabilities at the Manager and Agent processes, serve to reduce the communications traffic by pre-selecting only those managed objects which satisfy certain criteria.

An end system which operates profile AOM 11 can interwork with an end system implementing profile AOM 12 in the mode of operation specified by AOM 11 as long as the end system implementing AOM 12 is prepared to negotiate downwards to the level of service provided by AOM 11.

The ATN Manual identifies a number of specific management functions which will be applied to the managed objects defined for the ATN, namely:

- Object management (ISO/IEC 10164-1)
- State management (ISO/IEC 10164-2)
- Alarm reporting (ISO/IEC 10164-4)
- Event reporting (ISO/IEC 10164-5)
- Log Control (ISO/IEC 10164-6)
- Security alarm reporting (ISO/IEC 10164-7)
- Objects and attributes for access control (ISO/IEC 10164-9)

ISPs for these functional areas are currently under development. The relevant ISPs are:

ISP 12059 OSI Management - Common Information for Management Functions

Part 0: Common definitions for Management Function profiles

Part 1: Object Management functions

Part 2: State Management function

Part 3: Attributes for representing relationships

Part 4: Alarm reporting function

Part 5: Event report Management function

Part 6: Log control function

ISP 12060 AOM 2n - OSI Management - Management Functions

Part 1: AOM 211 - General management capabilities

Part 2: AOM 212 - Alarm Reporting and State management capabilities

Part 3: AOM 213 - Alarm Reporting capability

Part 4: AOM 221 - General Event Report Management

Part 5: AOM 231 - General log control

AOM 212 and AOM 213 require a subset of AOM 11 for their communications capabilities.

AOM 211, AOM 221 and AOM 231 require a subset of AOM 12 for their communications capabilities.

12.4.2 ATN CMIP Profile

CMIP profiles for ATN refer to the developing International Standardized Profile (ISP) (ISO/IEC 11183) for OSI Management, which consists of the following parts:

- Part 1: Specification for ACSE, Presentation and Session Protocols for use by ROSE and CMISE
- Part 2: AOM 12 : Enhanced management communications
- Part 3: AOM 11 : Basic Management communications

ATN Applications may have their own requirements in addition to these standardized profiles. As well as defining their own Managed Objects, it is possible that ATN Applications could use CMIP for generalized object manipulation.

The ATN CMIP profile will be based on AOM 12, since:

a) this is the most general profile

b) it supports scoping and filtering

c) it is required for certain management functions.

The ISP and its supporting IPRL will be cited wherever possible for the specification of ATN management communications.

12.4.3 Supporting Communication Protocols

AOM 11 and AOM 12 specify the use of ROSE and of CMIP; they also specify requirements for the use of ACSE, Presentation and Session. The profiles specify required functions from the supporting protocol stack shown below.

Application Layer	
CMIP	ISO/IEC 9595, 9596-1
ROSE	ISO 9072-1, 9072-2
ACSE	ISO 8650
Presentation Layer	ISO 8823
	Kernel Functional Unit only
	Basic encoding rules (BER) only

Session Layer	ISO 8327
	Kernel and Duplex Functional Units only

They require use of the Connection Mode Transport Service.

The standard profiles require the use of BER, which means that the length of the CMIP protocol data units as transferred over the communications link is not optimized.

Note.— Packed encoding rules (PER) ISO/IEC 8825-2 may be considered in the future for support of ATN systems management information transfer.

12.5 Systems Management Information

OSI management information is described using object oriented design techniques. For a full description of the OSI view of management information see ISO/IEC 10165-1, this refines the concept of management objects introduced in the OSI Management Framework (ISO 7498-4). It deals with object attributes, the management operations that may be performed on them and the notifications they emit. Instances of managed object classes are arranged hierarchically in an information tree.

A managed object is the OSI Management view of a resource that is subject to management, such as a layer entity or a connection. A managed object is the abstraction of such a resource that represents its properties as seen by management. An essential part of the definition of a management object is the relationship between these properties and the behavior of the resource.

Attributes are properties of managed objects, they have either simple or complex values.

Part of the specification of a managed object is the specification of the set of management operations that may be performed upon it and the effect that these operations may have.

Managed objects may emit notifications, which contain information concerning the occurrence of an event associated with it.

The set of management objects in a system together with their attributes constitutes that system's Management Information Base.

Managed objects may be specific to a layer in which case they are known as (N)-Layer Managed Objects. Those managed objects that are relevant to more than one layer, to a specific system management function (management support) or to the system as a whole are known as System Managed Objects.

In addition to the use of the object modelling techniques described above, OSI systems management also defines a General Relationship Model (ISO 10165-7). Relationships between resources are modelled in terms of *managed relationships*, i.e. relationships between the managed objects that represent the relevant resources. Managed relationships are new concepts within the Structure of Management Information yet they are represented and managed by using the existing in the management information model (ISO 10165-1).

Managed relationships that share the same definition are grouped into *managed relationship classes*.

The model recognises that the same managed relationship class may be represented in different ways within the management information model. A *role binding* describes a particular representation.

12.5.1 ATN Managed Object Containment Hierarchy

A managed object of one class can contain other managed objects of the same or different classes. This relationship is called containment. This containment relationship is a relationship between managed objects instances, not classes. A managed object is contained within one and only one containing managed object. Containing managed objects may themselves be contained in another managed object. Containment does not necessarily represent the physical containment of one resource within another. The containment relationship does not show an inheritance hierarchy.

The containment relationship can be used to model real-world hierarchies.

The specification of a particular containment relationship can be used to define static behavior (e.g., constrain the number and class of managed objects that can be contained in managed objects).

The specification of a particular containment relationship can be used to define dynamic behavior (e.g., the availability of contained and containing managed objects).

The containment relationship is used for naming managed objects. Names are designed to be unambiguous in a specified context determined by the containing object. Objects that are named in terms of another object are termed subordinate objects of that object. The object that establishes the naming context for other objects is called the superior object of these subordinate objects.

A subordinate object is named by the combination of:

- the name of its superior object
- information uniquely identifying this object within the scope of its superior object.

The name of an object that is unambiguous in a local context may not be so in the larger context (e.g., all Routers in a Routing Domain will contain a Network Layer Subsystem). The local name is made unambiguous by its naming context and this naming context can be recursively qualified by another naming context. Superior objects form the naming contexts for their subordinate objects so that their names need only be unambiguous within the context of its superior object, within a wider context its name is always qualified by the names of its superior objects.

Containment, naming and the existence of managed objects are closely related as follows:

- A managed object can exist only if its superior object exists (and has therefore been created and not deleted)
- Every managed object has a name, which is derived from the related containment.

The top level of the naming tree is referred to as "root" which is a null object (i.e. an object without properties) that always exists. For each object class defined, the attributes and the superior object classes whose instances may be used in constructing the name of the object must be identified. The relationship that identifies the possible superior object class that can be used in its naming is known as a "name binding". Additional name bindings for a particular object may be specified at any time, i.e., not all name bindings need be specified when the object class is first defined. Supported name bindings are not a property of the object class as whole and individual instances of the same object may use different name bindings.

In the ATN, the resources and protocols used in the Network and Transport Layers should be managed. The following standards provide standard definitions for the management information representing these resources and protocols:

- ISO 10733: Elements of Management Information Related to OSI Network Layer Standards
- ISO 10747: IDRP
- ISO 10737: Specification of the Elements of Management Information Relating to OSI Transport Layer Standards

~~The minimum containment hierarchy for ATN Systems has been defined in Appendix 12.5. This hierarchy will need expansion when particular local or regional Systems Management implementations include more than the minimum subset of management functions as defined in Appendix 12.2.~~

The ATN will need a global Systems Management strategy identifying both the large and small scale structure of the ATN with managed object containment hierarchies representing differing organizational and operational viewpoints and responsibilities grouped into management domains. ~~The definition of the containment hierarchy in~~

Appendix 12.5 is limited to that needed to allow individual ATN Systems to be managed, further considerations are outside the scope of this document.

12.5.2 ATN Managed Object Instances

As stated above further instances of different managed objects will be required if ATN Systems implement more than the minimum subset of management functions as defined in Appendix 12.

12.6 Transport Layer Managed Objects

Systems/Layer management will result in both procedural and interface requirements for the Transport Layer.

The Transport Layer resources and processes will need to be managed. To enable this, resources and processes will be grouped into managed objects according to the OSI principles defined in ISO 7498-4. Management will operate on these objects via a service interface using a protocol. The manager may be local and/or remote.

12.6.1 The Transport Subsystem Managed Object (TSMO) Class

The TSMO exists to provide a container for the transport layer entity MOs, it can not be created or deleted explicitly by management operation. It exists inherently in a system. It is created and deleted as part of system operation.

12.6.2 The Transport Entity Managed Object (TEMO) Class

There may be multiple instances of these MOs within a system. These managed objects can not be created or deleted explicitly by management operation. They exist inherently in a system, and are created and deleted as part of system operation.

12.6.3 The Connection-Oriented Transport Protocol Managed Object (CO TPM MO) Class

The definition of this MO permits it to be created and deleted explicitly by management operation, but in some systems it may exist inherently with neither creation nor deletion by management operation possible. Name binding will operate differently in these two cases, it will either be created explicitly by management or automatically by the system.

A CO-TPM-MO may be created in the 'enabled' Operational State.

The Administrative State of the object may be 'locked', 'unlocked' or 'shutting down'. For this object the following meanings apply (see ISO/IEC 10164-2 for a state transition diagram):

- 'locked' - the resources associated with the object are unavailable,
- 'unlocked' - the resources associated with the object are available,
- 'shutting down' - the resources have been 'unlocked' at some time and are in transition to the 'locked' state.

12.6.4 The TSAP Managed Object (TSAP MO) Class

Some implementations may require TSAP MOs to be created explicitly through management before they can be used. Others may create them automatically when a user entity attaches itself to them (in some implementation-dependent fashion). Name binding will operate differently in these two cases, it will either be created explicitly by management or automatically by the system.

12.6.5 The Transport Connection Managed Object (TCMO) Class

There may be multiple instances of these MOs within a connection mode protocol machine. Each corresponds to a transport connection. It is created and deleted by the operation of the protocol machine.

A TCMO may also exist prior to the transmission of a CR TPDU, corresponding to interactions across the service interface. Synchronisation of creation and deletion of these objects with protocol changes is implementation-dependent. For example, there may be a visible delay after transmission or reception of a CR TPDU or interaction at the service interface before the MO is created and becomes visible to management.

A TCMO is not required for terminated connections whose references have been placed in the frozen state.

12.6.6 The Transport Connection Initial Value Managed Object (TC IVMO) Classes

An object of this class represents a collection of attribute values used to supply default values when a transport connection is established. A TC IVMO may be used to supply initial values for the attributes of automatically created TCMOs.

A TC IVMO may be created or deleted explicitly by management and there may be multiple instances of these objects.

The values supplied in an IVMO may be overridden by values supplied in an implementation-specific manner across the service interface.

12.6.7 The Connectionless-Mode Transport Protocol Managed Object (CL TPM MO)

Instances of the object class may be created or deleted explicitly by management operation, but in some systems they will exist inherently and neither creation nor deletion by management operation will be possible. Name binding will operate differently in these two cases; it will either be created explicitly by management or automatically by the system.

A CO-TPM-MO may be created in the 'enabled' Operational State.

The Administrative State of the object may be 'locked', 'unlocked' or 'shutting down'. For this object the following meanings apply (see ISO/IEC 10164-2 for a state transition diagram):

'locked' - the resources associated with the object are unavailable,

'unlocked' - the resources associated with the object are available,

'shutting down' - the resources have been 'unlocked' at some time and are in transition to the 'locked' state.

12.6.8 The ATN Transport Layer Superset MO Classes

Note.— These are objects and events identified for use specifically in the ATN environment. They have not been standardized by ISO but they are still contained in the Transport Subsystem managed object hierarchy.

12.6.8.1 The Transport Connection QOS Initial Value Managed Object (TCQ-IVMO)

An object of this class represents a collection of attribute values used to supply default QOS values (when not supplied by the Transport user) when a transport connection is established. A TCQ IVMO may be used to supply initial QOS values for the attributes of automatically created TC MOs.

A TCQ IVMO may be created or deleted explicitly by management and there may be multiple instances of these objects. The values supplied in a TCQ IVMO may be overridden by values supplied across the service interface.

12.6.8.2 Network Layer QOS and Ranking

The ATN Network Layer QOS parameters include the relative ranking of cost, transit delay and error. Cost is not one of the QOS parameters available at the Transport Service user interface. The Transport user, therefore, has no direct control over the Network Layer QOS ranking. The NLRANK attribute (described in Table 12-1) provides a mechanism accessible to management to correct this deficiency.

Chapter 8 describes an alternative dynamic means for management to rank network layer QOS based on certain assumptions and the Transport Layer QOS, Transit Delay and Residual Error Rate. Use of either ranking method is valid but exclusive. Use of the management method involves the addition of the NLRANK attribute to the TC-

MO, TC-IVMO and CL-TPMO attributes since it applies to both connection oriented and connectionless Transport Protocol machines. In ISO GDMO terminology, it will be defined in a CONDITIONAL PACKAGE, included in object class instantiation when required.

Default values for Network Layer QOS may also be supplied as attributes to the TC-MO, TC-IVMO and CL-TPMO (except priority; NSDU priority is always mapped from TS-User priority). In ISO GDMO terminology, this group of attributes will be defined in a CONDITIONAL PACKAGE, included in object class instantiation when required. The NLQOS attribute is described in Table 12-2.

Table 12-1: NLRANK Conditional Package

Index	**Object Class Attributes**	**Ref.**	**Type**	**Operation**
TE.33.1	NLRANK - Expense, Transit delay, Residual error rate combination		R/W	DEFAULT, REPLACE, GET

Table 12-2: NLQOS Conditional Package

Index	**Object Class Attributes**	**Ref.**	**Type**	**Operation**
TE.34.1	Transit delay		R/W	DEFAULT, REPLACE,GET
TE.34.2	Protection from unauthorised access		R/W	DEFAULT, REPLACE,GET
TE.34.3	Expense		R/W	DEFAULT, REPLACE,GET
TE.34.4	Priority		R	GET

CHAPTER 12 SYSTEMS MANAGEMENT GUIDANCE 1

12.1 INTRODUCTION 1
12.1.1 Overview 1
12.1.2 General Considerations 1
12.2 SYSTEMS MANAGEMENT FUNCTIONS 3
12.2.1 Object Management Function (ISO/IEC 10164-1) 4
12.2.2 State Management Function (ISO/IEC 10164-2) 4
12.2.3 Attributes for Representing Relationships (ISO/IEC 10164-3) 4
12.2.4 Alarm Reporting Function (ISO/IEC 10164-4) 4
12.2.5 Event Report Management Function (ISO/IEC 10164-5) 4
12.2.6 Log Control Function (ISO/IEC 10164-6) ..... 5~~4~~
12.2.7 Security Alarm Reporting Function (ISO/IEC 10164-7) 5
12.2.8 Security Audit Trail Function (ISO/IEC 10164-8) 5
12.2.9 Access Control Function (ISO/IEC 10164-9) 5
12.2.10 Accounting Meter Function (ISO/IEC 10164-10) ..... 6~~5~~
12.2.11 Workload Monitoring Function (ISO/IEC 10164-11) ..... 6~~5~~
12.2.12 Test Management Function (ISO/IEC 10164-12) 6
12.2.13 Summarization Function (ISO/IEC 10164-13) 6
12.2.14 Confidence and Diagnostic Tests (ISO/IEC 10164-14) ..... 7~~6~~
12.2.15 Scheduling Function (ISO/IEC 10164-15) ..... 7~~6~~
12.2.16 Performance Management Function (ISO/IEC 10164-B) ..... 7~~6~~
12.2.17 Management Knowledge Management Function (ISO/IEC 10164-16) 7
12.2.18 Management Domain Management Function ..... 8~~7~~
12.2.19 Change Over Function ..... 8~~7~~
12.2.20 Software Management Function 8
12.3 SYSTEMS MANAGEMENT SERVICES ..... 9~~8~~
12.3.1 Management Communication Services ..... 9~~8~~
12.3.2 Association Services ..... 9~~8~~
12.3.3 The Common Management Information Service (CMIS) ..... 10~~9~~
12.4 ATN SYSTEMS MANAGEMENT PROTOCOLS ..... 11~~10~~
12.4.1 Profiles for Management Communication ..... 12~~11~~
12.4.2 ATN CMIP Profile ..... 14~~13~~
12.4.3 Supporting Communication Protocols ..... 14~~13~~
12.5 SYSTEMS MANAGEMENT INFORMATION ..... 15~~14~~
12.5.1 ATN Managed Object Containment Hierarchy ..... 15~~14~~

CHAPTER 12 SYSTEMS MANAGEMENT GUIDANCE 1

12.1 INTRODUCTION 1
12.1.1 Overview 1
12.1.2 General Considerations 1
12.2 SYSTEMS MANAGEMENT FUNCTIONS 3
12.2.1 Object Management Function (ISO/IEC 10164-1) 4
12.2.2 State Management Function (ISO/IEC 10164-2) 4
12.2.3 Attributes for Representing Relationships (ISO/IEC 10164-3) 4
12.2.4 Alarm Reporting Function (ISO/IEC 10164-4) 4
12.2.5 Event Report Management Function (ISO/IEC 10164-5) 4
12.2.6 Log Control Function (ISO/IEC 10164-6) 4
12.2.7 Security Alarm Reporting Function (ISO/IEC 10164-7) 5
12.2.8 Security Audit Trail Function (ISO/IEC 10164-8) 5

12.2.9 Access Control Function (ISO/IEC 10164-9) 5
12.2.10 Accounting Meter Function (ISO/IEC 10164-10) 5
12.2.11 Workload Monitoring Function (ISO/IEC 10164-11) 5
12.2.12 Test Management Function (ISO/IEC 10164-12) 6
12.2.13 Summarization Function (ISO/IEC 10164-13) 6
12.2.14 Confidence and Diagnostic Tests (ISO/IEC 10164-14) 6
12.2.15 Scheduling Function (ISO/IEC 10164-15) 6
12.2.16 Performance Management Function (ISO/IEC 10164-B) 6
12.2.17 Management Knowledge Management Function (ISO/IEC 10164-16) 7
12.2.18 Management Domain Management Function 7
12.2.19 Change Over Function 7
12.2.20 Software Management Function 8
12.3 SYSTEMS MANAGEMENT SERVICES 8
12.3.1 Management Communication Services 8
12.3.2 Association Services 8
12.3.3 The Common Management Information Service (CMIS) 9
12.3.3.1 Management Notification Services 9
12.3.3.2 Management Operation Services 9
12.3.3.3 CMIS Functional Units 10
12.4 ATN SYSTEMS MANAGEMENT PROTOCOLS 10
12.4.1 Profiles for Management Communication 11
12.4.2 ATN CMIP Profile 13
12.4.3 Supporting Communication Protocols 13
12.5 SYSTEMS MANAGEMENT INFORMATION 14
12.5.1 ATN Managed Object Containment Hierarchy 14

~~CHAPTER 12 SYSTEMS MANAGEMENT GUIDANCE 1~~

~~12.1 INTRODUCTION 1~~
~~*12.1.1 Overview* 1~~
~~*12.1.2 General Considerations* 1~~
~~12.2 SYSTEMS MANAGEMENT FUNCTIONS 3~~
~~*12.2.1 Object Management Function (ISO/IEC 10164-1)* 4~~
~~*12.2.2 State Management Function (ISO/IEC 10164-2)* 4~~
~~*12.2.3 Attributes for Representing Relationships (ISO/IEC 10164-3)* 4~~
~~*12.2.4 Alarm Reporting Function (ISO/IEC 10164-4)* 4~~
~~*12.2.5 Event Report Management Function (ISO/IEC 10164-5)* 4~~
~~*12.2.6 Log Control Function (ISO/IEC 10164-6)* 4~~
~~*12.2.7 Security Alarm Reporting Function (ISO/IEC 10164-7)* 5~~
~~*12.2.8 Security Audit Trail Function (ISO/IEC 10164-8)* 5~~
~~*12.2.9 Access Control Function (ISO/IEC 10164-9)* 5~~
~~*12.2.10 Accounting Meter Function (ISO/IEC 10164-10)* 5~~
~~*12.2.11 Workload Monitoring Function (ISO/IEC 10164-11)* 5~~
~~*12.2.12 Test Management Function (ISO/IEC 10164-12)* 6~~
~~*12.2.13 Summarization Function (ISO/IEC 10164-13)* 6~~
~~*12.2.14 Confidence and Diagnostic Tests (ISO/IEC 10164-14)* 6~~
~~*12.2.15 Scheduling Function (ISO/IEC 10164-15)* 6~~
~~*12.2.16 Performance Management Function (ISO/IEC 10164-B)* 6~~
~~*12.2.17 Management Knowledge Management Function* 6~~
~~*12.2.18 Management Domain Management Function* 7~~
~~12.3 SYSTEMS MANAGEMENT SERVICES 7~~
~~*12.3.1 Management Communication Services* 7~~
~~*12.3.2 Association Services* 8~~

12.3.3 The Common Management Information Service (CMIS) *8*
12.3.3.1 Management Notification Services 9
12.3.3.2 Management Operation Services 9
12.3.3.3 CMIS Functional Units 9
12.4 ATN SYSTEMS MANAGEMENT PROTOCOLS 10
12.4.1 Profiles for Management Communication *10*
12.4.2 ATN CMIP Profile *12*
12.4.3 Supporting Communication Protocols *12*
12.5 SYSTEMS MANAGEMENT INFORMATION 13
12.5.1 ATN Managed Object Containment Hierarchy *13*
12.5.2 ATN Managed Object Instances *14*
12.6 TRANSPORT LAYER MANAGED OBJECTS 14
12.6.1 The Transport Subsystem Managed Object (TSMO) Class *15*
12.6.2 The Transport Entity Managed Object (TEMO) Class *15*
12.6.3 The Connection-Oriented Transport Protocol Managed Object (CO TPM MO) Class *15*
12.6.4 The TSAP Managed Object (TSAP MO) Class *15*
12.6.5 The Transport Connection Managed Object (TCMO) Class *15*
12.6.6 The Transport Connection Initial Value Managed Object (TC IVMO) Classes *15*
12.6.7 The Connectionless-Mode Transport Protocol Managed Object (CL TPM MO) *16*
12.6.8 The ATN Transport Layer Superset MO Classes *16*
12.6.8.1 The Transport Connection QOS Initial Value Managed Object (TCQ-IVMO) 16
12.6.8.2 Network Layer QOS and Ranking 16