ETSI TECHNICAL REPORT

ETR 269

April 1996

Source: ETSI TC-TM

Reference: DTR/TM-02212

ICS: 33.040.20

Key words: transmission, network, information model

Transmission and Multiplexing (TM); Network level information modelling

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

*

Contents

Foreword

This ETSI Technical Report (ETR) was produced by the Transmission and Multiplexing (TM) Technical Committee of the European Telecommunications Standards Institute (ETSI).

ETRs are informative documents resulting from ETSI studies which are not appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status. An ETR may be used to publish material which is either of an informative nature, relating to the use or the application of ETSs or I-ETSs, or which is immature and not yet suitable for formal adoption as an ETS or an I-ETS.

Blank page

1 Scope

This ETR describes some of the issues, related to the modelling process which should be completed in order to model the network layer of a transmission network, in particular those issues related to the production of interface specifications described in terms of Guidelines for the Definition of Managed Objects (GDMO) templates using the ensemble technique. It describes the principles to be used when developing ensembles in terms of the use of ITU-T Recommendation G.803 [1], the use of ITU-T Recommendation M.3010 [6], the functional management architecture, the use of a standard class library, the modelling methodology to be used, the need to support multiple managers and the management capabilities to be supported. It also describes the structure required in the ensemble which conforms to the Network Management Forum (NMF) Ensemble specification technique.

2 References

This ETR incorporates by dated and undated reference, provisions from other publications. These references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETR only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ITU-T Recommendation G.803: "Architectures of transport networks based on the synchronous digital hierarchy (SDH)".

[2] prI-ETS 300 653: "Telecommunications Management Network (TMN); Generic managed object class library for the network level view".

[3] ITU-T Recommendation M.3100: Generic network information model".

prI-ETS 300 293: "Telecommunications Management Network (TMN); Generic managed objects".

[4] ITU-T Recommendation G.774: "Synchronous digital hierarchy (SDH) management information model for the network element view".

[5] ETS 300 304 (1994): "Transmission and Multiplexing (TM); Synchronous Digital Hierarchy (SDH) information model for the Network Element (NE) view".

[6] ITU-T Recommendation M.3010: "Principles for a telecommunications management network".

[7] Network Management Forum: "The "Ensemble" Concept and Format", Issue 1.0 (1992), Forum 025.

[8] Network Management Forum: "Ensemble example Reconfigurable Circuit Service: Configuration Management Ensemble", Issue 1.0, Forum 017.

[9] ITU-T Recommendation X.700 Series: "OSI Management" (see annex C, Bibliography).

[10] ETR 037: "Network Aspects (NA); Telecommunications Management Network (TMN); Objectives, principles, concepts and reference configurations".

3 Abbreviations

For the purposes of this ETR, the following abbreviations apply:

CCITT	International Telephone and Telegraph Consultative Committee
CMIP	Common Management Information Protocol
CMISE	Common Management Information SErvice
Conf	Confirm
ETSI	European Telecommunications Standards Institute
ETR	ETSI Technical Report
ETS	European Telecommunications Standard
f	f type reference point
GDMO	Guidelines for the Definition of Managed Objects
I-ETS	Interim ETS
Ind	Indication
ISO	International Organisation for Standardisation
MO	Managed Object
MOCS	Managed Object Conformance Statement
NE	Network Element
NEF	Network Element Function
NMF	Network Management Forum
OS	Operations System (physical implementation)
OSF	Operations System Function
OSFB	Business Management Layer OSF
OSFE	Element Management Layer OSF
OSFN	Network Management Layer OSF
$OSFN_{SP}$	Service Provider OSF within the network management layer
$OSFN_{User}$	User OSF within the network management layer
OSFS	Service Management Layer OSF
$OSFS_{SP}$	Service Provider OSF within the service management layer
$OSFS_{User}$	User OSF within the service management layer
OSF_{SP}	Service Provider OSF
OSF_{User}	User OSF
OSI	Open Systems Interconnection
q	q type reference point
$Q3_{nn}$	Interface between one network management layer OS and another network management layer OS
$Q3_{sn}$	Interface between a service management layer OS and a network management layer OS
QoS	Quality of Service
Req	Request
Rsp	Response
SDH	Synchronous Digital Hierarchy
SP	Service Provider
TM	Transmission and Multiplexing
TMN	Telecommunications Management Network
TP	Termination Point
x	x type reference point

4 The Modelling process

The modelling process takes a number of management capabilities and produces one, or more, ensembles (as defined in the NMF "The Ensemble Concept and Format" [7]) which will support such capabilities. A number of ensembles may be used in order to define one interface, in order to provide a combination of the management capabilities from different ensembles at that interface. However, different managers may be given different views of the managed objects at that interface, depending on the desired level of access given to individual managers. For instance, a configuration ensemble and a fault ensemble may be combined at one interface. This implies that the managed object model chosen to implement a particular set of management capabilities in an ensemble should be compatible with that of other ensembles, if combination of the ensembles is to be allowed.

A number of constraints have been placed on the development of these ensembles (see figure 1):

1) only an identified transport network architecture will be managed;

2) management capabilities should be described in terms of their influence on ITU T Recommendation G.803 [1] entities. These ITU-T Recommendation G.803 [1] entities describe the underlying transport network resources to be managed;

3) the functional and information architecture should be described in terms of the Telecommunications Management Network (TMN) concept as defined in ITU-T Recommendation M.3010 [6];

4) a fixed functional architecture will be used to manage the transport network, although different ensembles may specify different functional architectures;

5) the information model of the ensemble should be based on object classes from a standard class library;

6) the production of the ensemble should use a clearly defined methodology;

7) ensembles shall support multiple managers, including where several managers wish to use the same management capabilities;

8) only a limited set of management capabilities will be supported by any one ensemble.

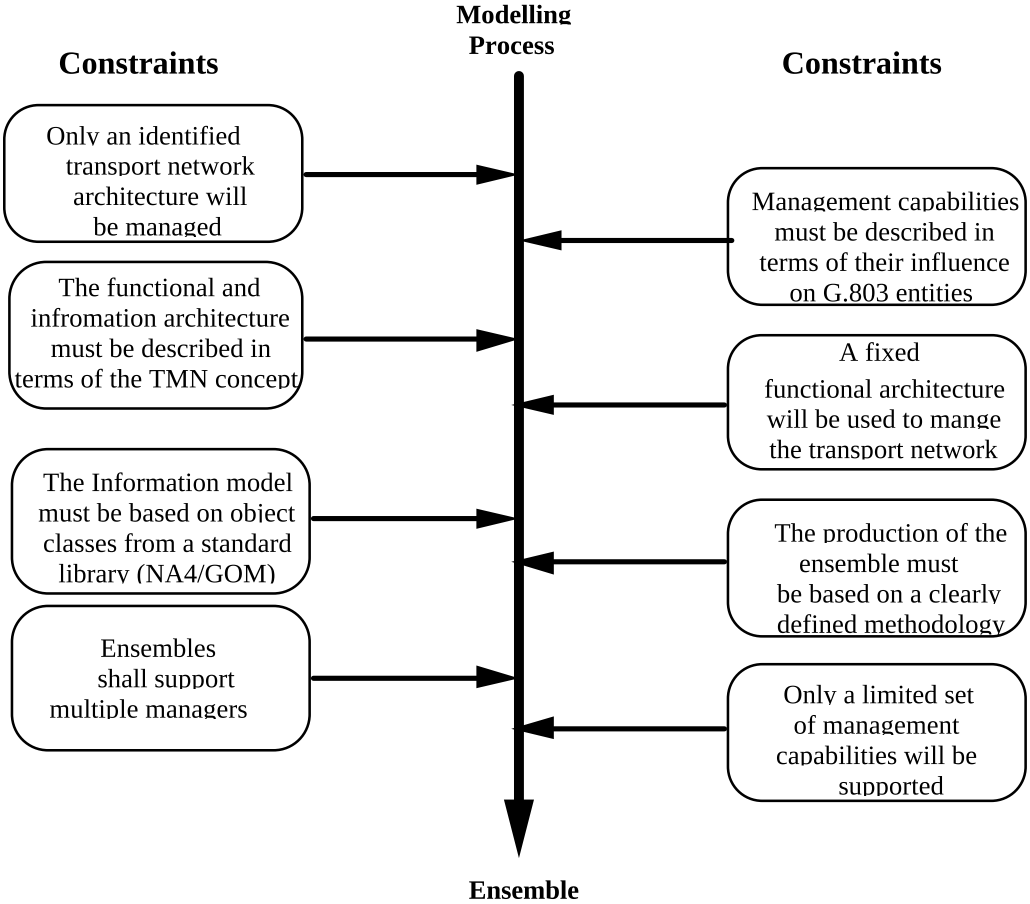


Figure 1: The constraints placed upon the network level modelling process

The following describes these constraints in more detail.

4.1 The transport network architecture to be managed

In order to simplify the required management capabilities to be supported only the management of identified transport network architectures will be considered (e.g. a ring of Synchronous Digital Hierarchy (SDH) multiplexers).

4.2 The use of ITU-T Recommendation G.803 to describe the transport network resources to be managed

The resources to be managed are described below. These resources are based on entities and concepts defined within ITU-T Recommendation G.803 [1]. However ITU-T Recommendation G.803 [1] is highly complex and in places inconsistent. Therefore a sub-set of ITU-T Recommendation G.803 [1] has been taken and used to describe the resources. The definitions of the resources below shall be used within the modelling process. These are the base resources - these may be extended or built upon within an ensemble.

Taken together these resources make up a part of a layer network, a complete layer network or a number of layer networks. A layer network is itself a resource composed of several distinct types of resource, along with certain functions associated with these resources. Therefore the resources to be managed are:

- access groups;
- access points;
- adaptation functions;
- characteristic information;
- connection points;
- layer network;
- links;
- link connections;

- matrices;
- sub-networks;
- sub-network connections;
- tandem connections;
- tandem connection bundles;
- termination connection points;
- trails;
- trail termination functions.

Figure 2 is an Entity-Relationship (E-R) diagram for the resources and figure 3 shows a single ring represented with those resources. Detailed descriptions of the resources are given below.

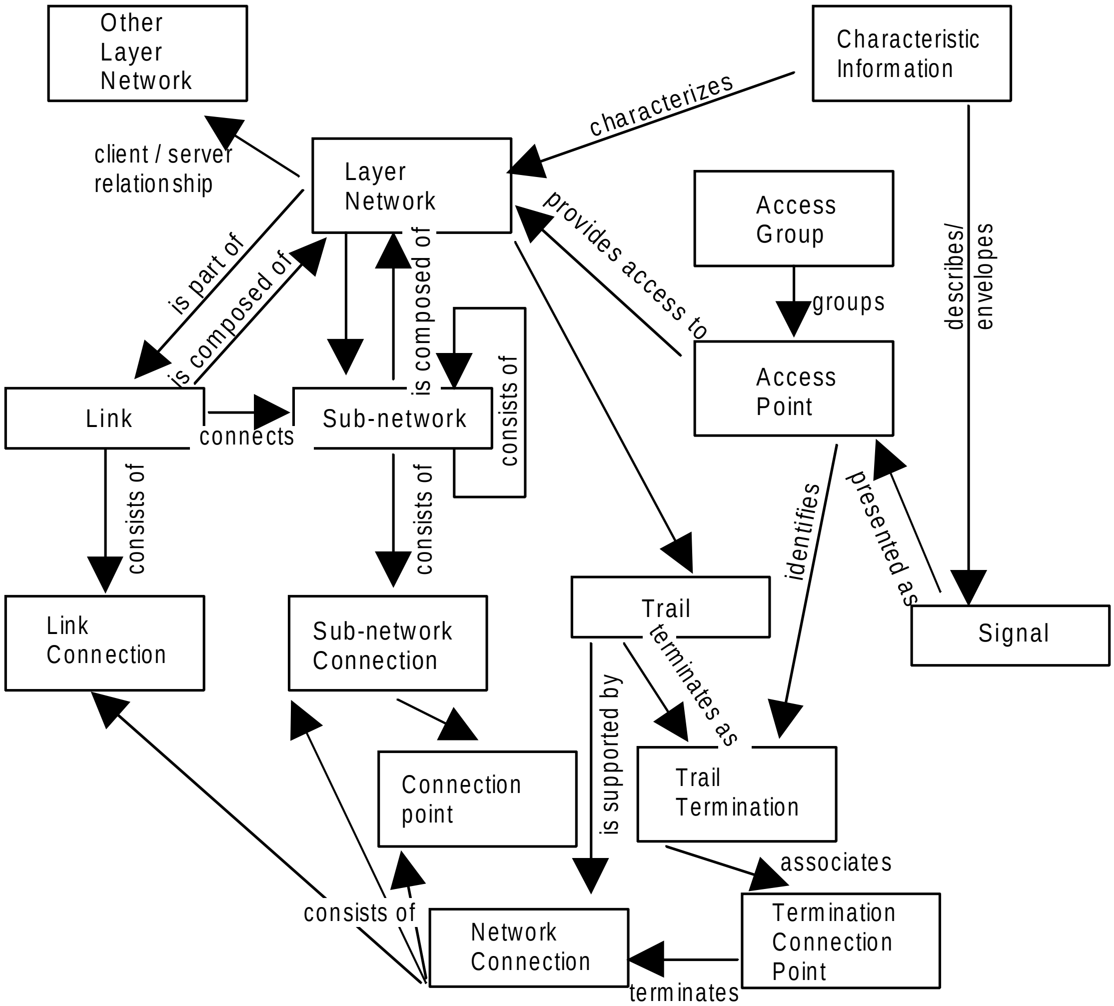


Figure 2: Managed resources E-R diagram

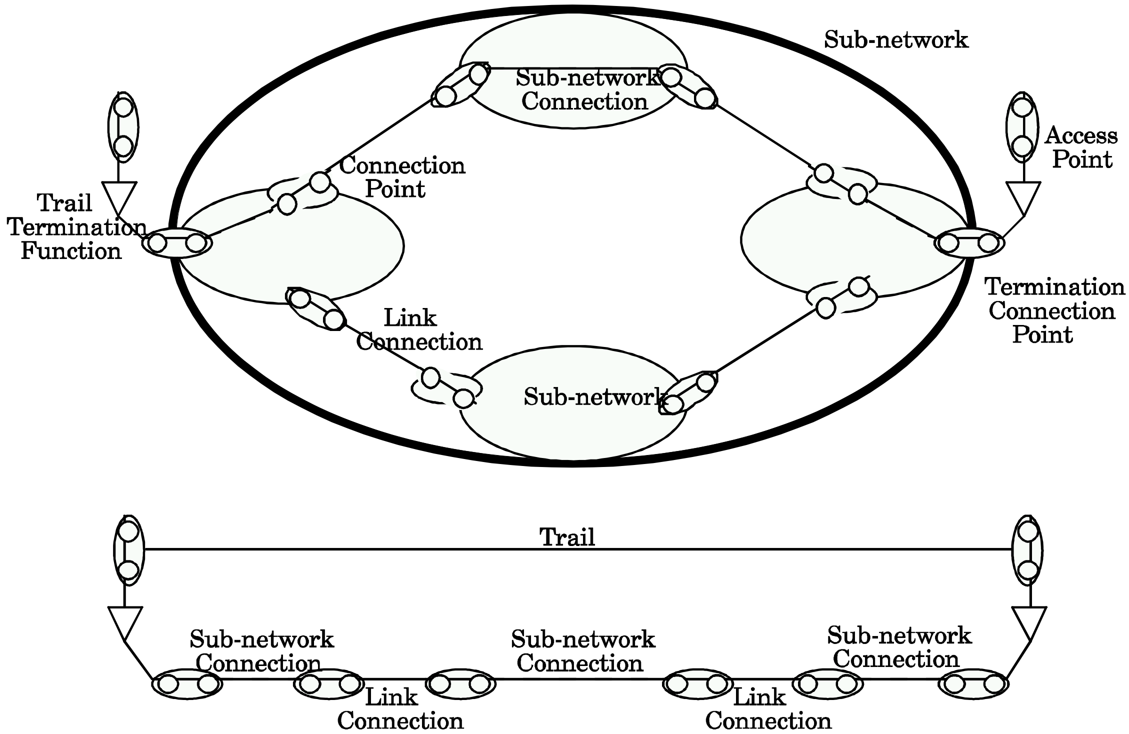


Figure 3: Single ring described in terms of ITU-T Recommendation G.803 [1] resources

The following describes the layer network and the resources that make it up in a technology independent way (terms in *italics* refer to entities described between subclause 4.2.1 and subclause 4.2.17 in ITU-T Recommendation G.803 [1]).

4.2.1 Access group

An access group is a group of co-located access points together with their associated trail termination functions. (Trail termination generates the characteristic information of a layer network and ensures integrity of transport of that characteristic information.).

NOTE: An *access point* does not have to belong to an access group.

The *access points* within an access group may be within a single Network Element (NE) or within a limited geographical region (e.g. a building).

4.2.2 Access point

An access *point* is where the adapted characteristic information from a client *layer network* enters the server *layer network*. It is the point where the adapted *characteristic information* is bound to a trail termination function, and thus the point where the adapted *characteristic information* enters the *trail*. (Trail termination generates the *characteristic information* of a *layer network* and ensures integrity of transport of that *characteristic information*.)

4.2.3 Adaptation function

The adaptation function is a "transport processing function" which adapts a server layer to the needs of a client layer. The adaptation function defines the server/client association between the *connection point* and *access point* and these points therefore delimit the adaptation function. Adaptation functions have been defined for many client/server interactions.

4.2.4 Characteristic information

Characteristic information is a signal of characteristic rate and format which is transferred within and between *sub-networks* and presented via an adaptation function to an *access point* for transport by a server *layer network*. (The adaptation function adapts the signal so that it may be transported by the server *layer network,* e.g. by multiplexing several client layer signals together.)

4.2.5 Connection point

A connection point is where:

1) *a link connection may be bound to another link connection;*

2) *a link connection may be bound to a sub-network connection;*

3) *a link connection may be bound to a trail termination function (associated with an access point) forming the end of a trail;*

4) *a sub-network connection may be bound to a trail termination function (associated with an access point) forming the end of a trail.*

4.2.6 Layer network

A layer network is defined by the complete set of like *access points* which may be associated for the purpose of transferring information. The information transferred is characteristic of the layer and is termed *characteristic information*. *Access point* associations may be made and broken by a layer management process thus changing its connectivity (i.e. the establishment or clearing down of *trails*). A separate, logically distinct layer network exists for each *access point* type. A layer network is made up of *sub-networks* and *links* between them. A layer network may serve a client layer network by transporting the *characteristic information* of the client layer within a signal of *characteristic information* of its own layer.

4.2.7 Link

A link describes the fixed relationship between a *sub-network* and another *sub-network* or *access group*. It is defined by the sub-set of *connection points* on one *sub-network* which are associated with a sub-set of *connection points* or *access points* on another *sub-network* or *access group* for the purpose of transferring *characteristic information*. The set of *connection point* associations which define the link are represented by *link connections*. The link represents the topological relationship between a pair of *sub-networks* or a *sub-network* and an *access group*.

4.2.8 Link connection

A link connection is supported by a *trail* in the server *layer network*. It is capable of transferring information transparently across a *link* between two *sub-networks,* or across a *link* between an *access group* and a *sub-network*. It is delimited by *connection* and represents the association between those *connection points.* Link connections are configured by the *trail* management process of the server *layer network* (i.e. the establishment of a *trail* in a server *layer network* results in the establishment of *link connections* in one or more client *layer networks*).

4.2.9 Matrix

A matrix is a special case of a *sub-network* and represents the limit to the recursive partitioning of *a sub-network*.

4.2.10 Sub-network

A sub-network describes the potential for *sub-network connections* across the sub-network. It can be partitioned into interconnected sub-networks and *links*. Each sub-network in turn can be partitioned into smaller sub-networks and links and so on. It is defined by the complete set of like *connection points* which may be associated for the purpose of transferring *characteristic information*. The *connection point* associations in a sub-network may be made and broken by a layer management process thus changing its connectivity (i.e. the establishment or clearing down of *sub-network connections*).

4.2.11 Sub-network connection

A sub-network connection is capable of transferring *characteristic information* across a *sub-network* transparently. It is delimited by *connection points* at the boundary of the *sub-network* and represents the association between *connection points* within the same *sub-network*. Sub-network connections are in general made up of a series of adjacent lower level sub-network connections and *link connections* and can be viewed as an abstraction of this more detailed view.

NOTE: Sub-network connections, trails, link connections and tandem connections may take the form of point to multi-point connectivity entities. This is not explicitly covered by ITU-T Recommendation G.803 [1] but is provided for here to allow the description of such connectivity configurations.

4.2.12 Tandem connection

A tandem connection is an arbitrary series of adjacent *link connections* and *sub-network connections*.

4.2.13 Tandem connection bundle

A parallel set of *tandem connections*. This entity is not described in ITU-T Recommendation G.803 [1], and is provided here as a likely additional entity required to fully describe resources.

4.2.14 Termination connection point

A Termination connection point is a special case of a *connection point* where a *trail termination function* is bound to an *adaptation function* or a *matrix*.

4.2.15 Trail

A trail in a server *layer network* is responsible for the integrity of transfer of *characteristic information* from one or more client *layer networks* between the server layer *access points*, utilising the *characteristic information* of its own layer. It defines the association between *access points* in the same *layer network*. Trail termination functions at either end of the trail monitor the integrity of transfer by adding incremental information to the adapted *characteristic information* from the client *layer networks.* These trail termination functions are thought of as being part of the *trail*.

4.2.16 Trail termination function

The Trail termination function is a transport processing function which generates *the characteristic information* of a *layer network* and ensures integrity of that *characteristic information*. The trail termination function defines the association between the *access point* and *termination connection point* and these points therefore delimit the trail termination function.

The Trail termination source is a transport processing function which accepts adapted client layer network *characteristic information*, adds *trail* overhead and assigns it to an associated network connection in the same transport network layer.

The Trail termination sink is a transport processing function which terminates a *trail*, extracts the *trail* overhead information, checks validity and passes the adapted client layer network *characteristic information* to the *adaptation function*.

4.2.17 Configuration examples

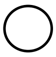
The following presents a number of configuration examples. These examples are not intended to be exhaustive, but are intended to give an appreciation of the range of complexity that may be covered.

In figures 4 to 10 the following symbols are used:

 access point

 access group

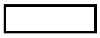
 trail

 sub-network

 link connection

 sub-network connection

 connection point

 link

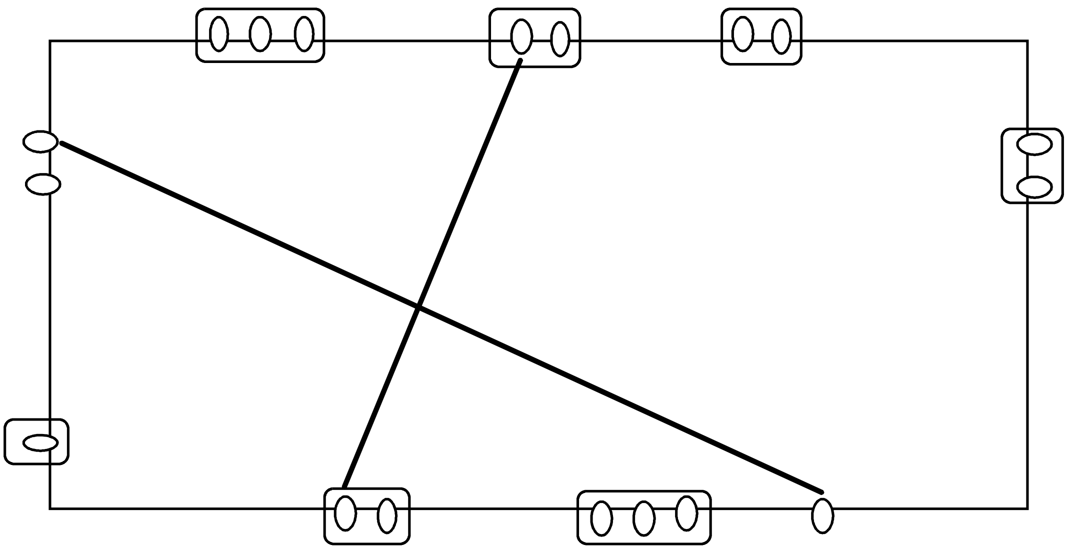


Figure 4: Trails

Figure 4 shows two point to point trails across a layer network. They are supporting link connections outside the domain of the agent.

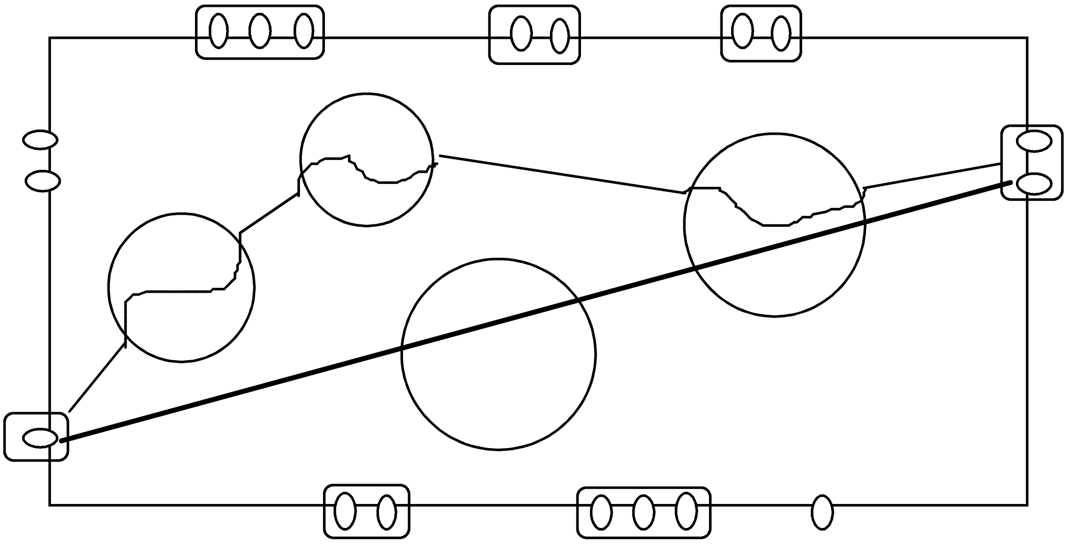


Figure 5: Trail with link connections and sub-network connections made visible

Figure 5 shows a point to point trail across a layer network. The routing here is shown in terms of the link connections between sub-networks. It could be shown in terms of the links between sub-networks.

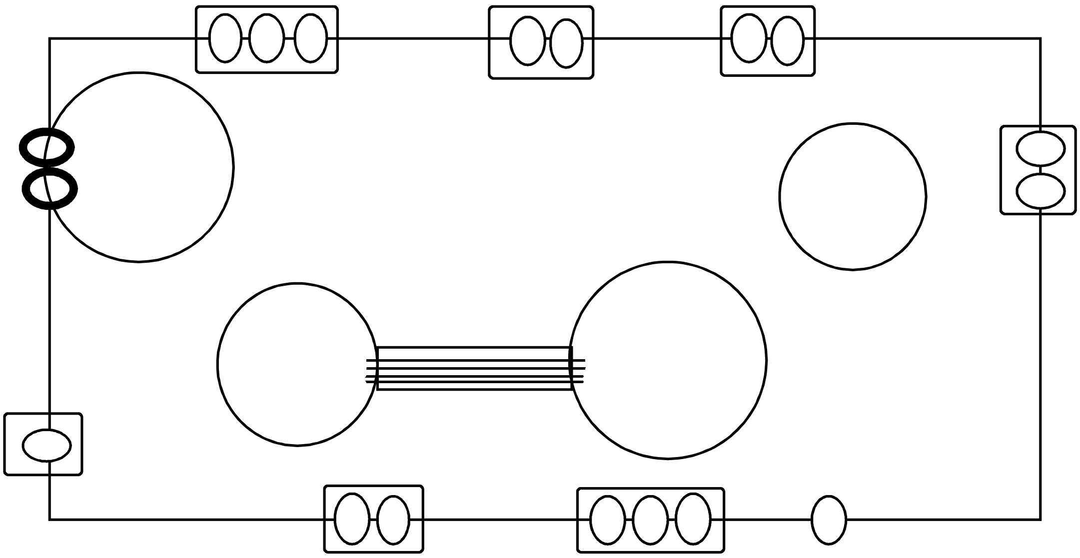


Figure 6: Capacity on a link

Figure 6 shows a link between two sub-networks. This example also shows how access points (shown in bold) may in fact be at the edge of a sub-network (there would also be a trail termination function and termination connection point associated with the access point at the edge of the sub-network - these are not shown), as well as being at the edge of the layer network. Thus these access points can effectively be flexibly cross-connected (from the termination connection point) via sub-network connections to connection points within the sub-network.

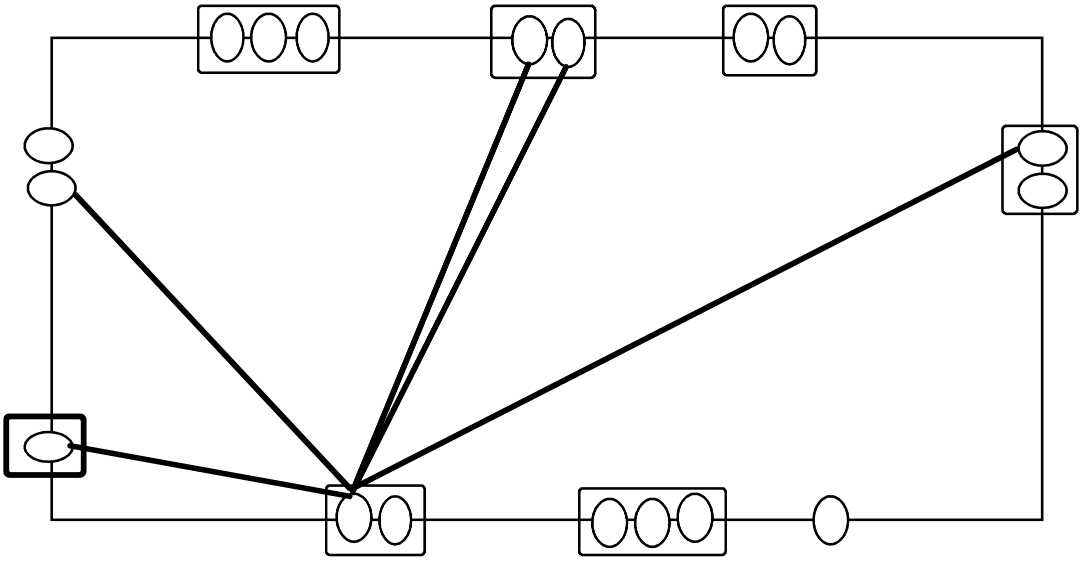


Figure 7: Point to multi-point trail

Figure 7 shows a point to multi-point trail. This trail will support one or more point to multi-point link connections in its client layer.

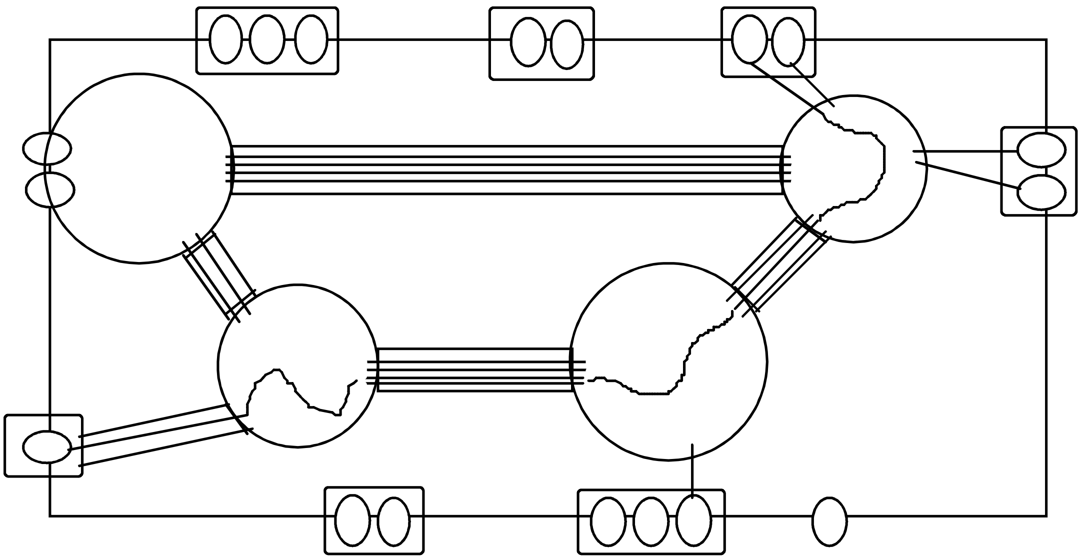


Figure 8: Sub-network connections

Figure 8 illustrates sub-network connections configured within sub-networks.

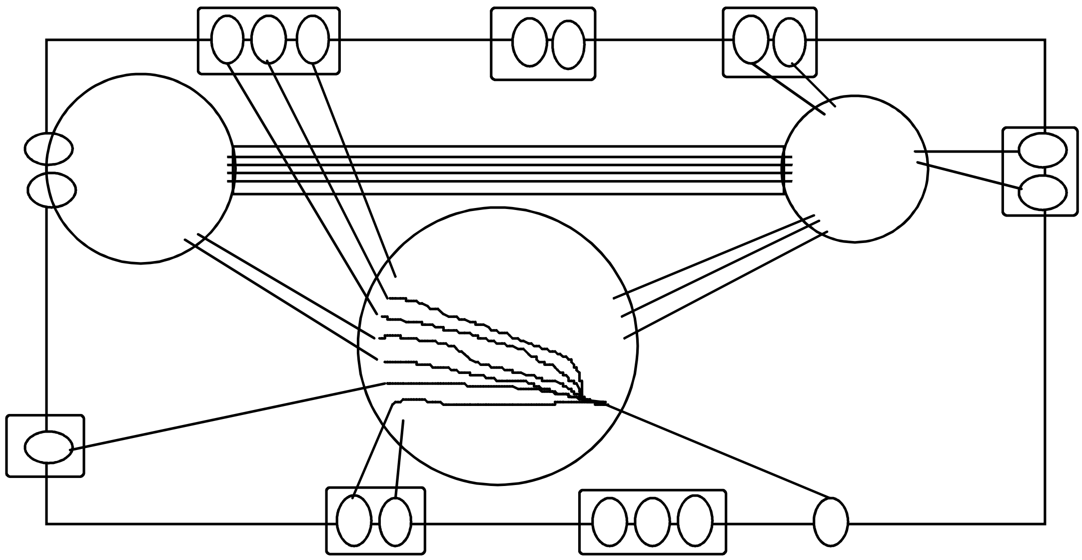


Figure 9: Point to multi-point sub-network connection

Figure 9 illustrates a point to multi-point sub-network connection, which could be used as the basis for creating a point to multi-point trail.

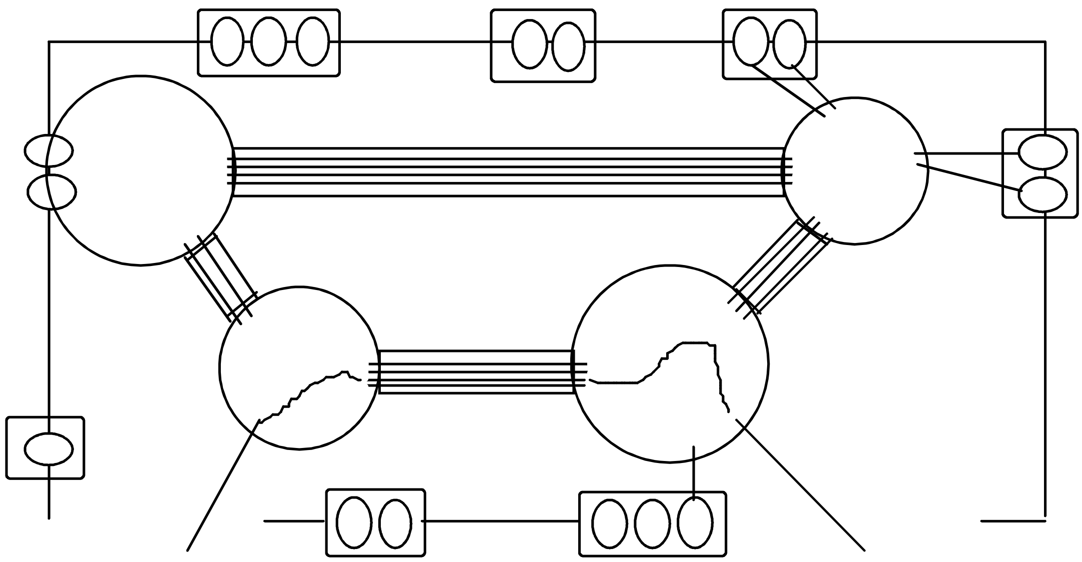


Figure 10: Tandem connection

Figure 10 illustrates a tandem connection, where the end points are outside the domain of the agent.

4.3 The use of ITU-T Recommendation M.3010's TMN concept

4.3.1 The layering concept

For operational purpose, management functionality may be considered to be divided into layers. Each layer restricts management activities within the boundaries of each layer to a clearly defined rank that is concerned with a subset of the total management activity. This is illustrated in figure 11 which is based on annex B, clause B.3 of ETR 037 [10].

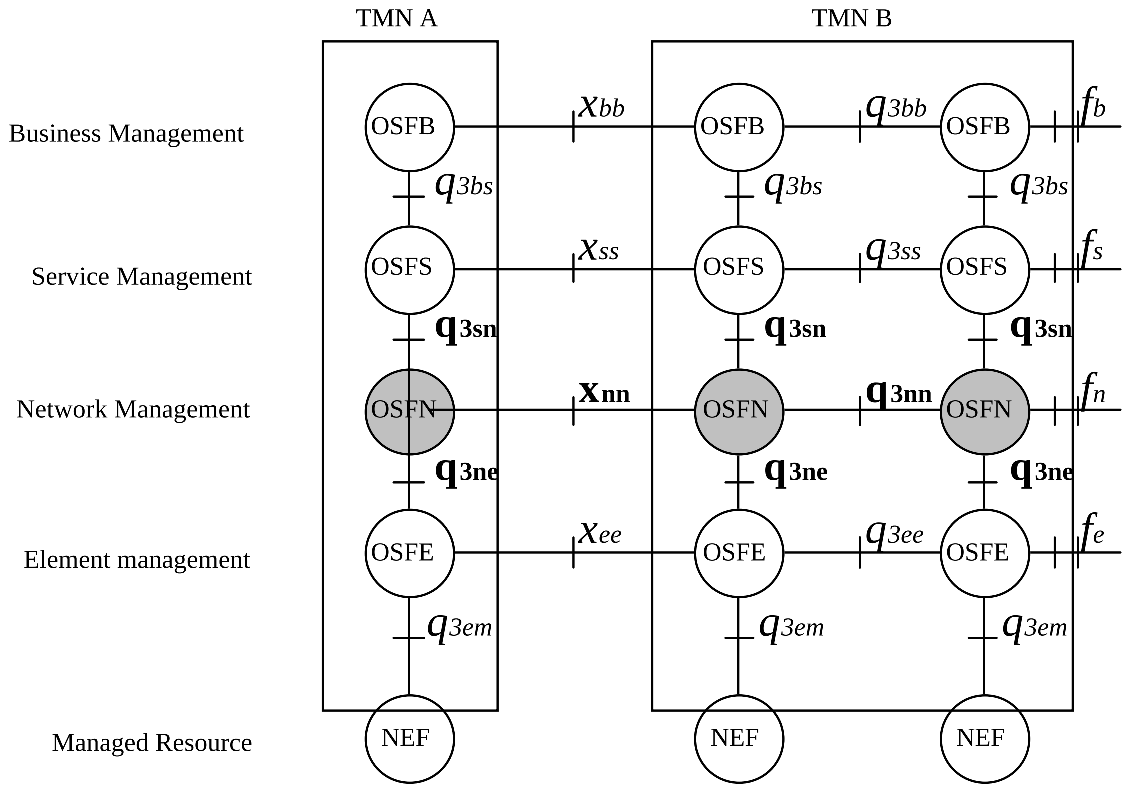


Figure 11: The reference point within the TMN reference architecture (on annex B, clause B.3 of ETR 037 [10])

Each of these layers has the following characteristics:

1) a layer may be divided into sub-layers (in this ETR, except where stated, all statements made concerning "layers" are also relevant for "sub-layers");

2) it presents an abstraction of its "object space" to its adjacent higher layer;

3) it sees an abstraction of the "object space" of its adjacent lower layer;

4) these abstractions may contain information regarding the "object space" of the layer to which the abstraction is being presented, or of the layer from which the abstraction is being viewed;

5) the management capabilities of a layer are implemented within one or more Operations System Function (OSF) within that layer. Where a management capability is implemented in more than one OSF, the different OSFs may belong to different sub-layers.

In point 2 and 3 above the abstraction represents the information which is used to map between the two "object spaces" of adjacent management layers. This abstraction may contain information from both layers (for example, an abstraction may contain the mapping between a service {belonging to the service management layer} and the supporting network layer trail) or may contain information from one of the layers only (for example, the service management layer may use network layer "Quality of Service (QoS) parameters" to determine the QoS that will be experienced by a customer at the service management layer).

4.3.2 The nature of the network layer

The network layer which has a set of network managers has the responsibility for the management of all network elements, as presented by the element management layer, both individually and as a set. It is not concerned with how a particular element provides services internally.

At this layer, functions addressing the management of a wide geographical area are located. Complete visibility of the whole network is typical and a vendor independent view will need to be maintained.

The network management layer has three principle roles:

1) the control and coordination of the network view of all network elements within its scope or domain;

2) the provision, cessation or modification of network capabilities for the support of services to customers;

3) to interact with the service management layer on performance, usage, availability, etc..

Thus the network management layer provides the functionality to manage a network by coordinating activity across the network and supports the "network" demands made by the service management layer.

4.4 The functional architecture used to manage the transport network

The following functional architecture will be used to manage the transport network (figure 12):

1) the service provider is represented by the OSF (OSF_{SP}):

   - $OSFN_{SP}$, within the network management layer;

2) the service user is represented by one of two OSFs (OSF_{User}):

   - $OSFS_{User}$, when the OSF is within the service management layer; and

   - $OSFN_{User}$, when the OSF is within the network management layer;

3) in order to provide a service either for the service or network user, the service provider OSF communicates with one or more element manager OSFs (the OSFEs), (within the element management layer) which are responsible for the network elements.

   NOTE 1: In this ETR the term "service" is normally used to describe a feature offered by one entity to another entity within a relationship (either client/server or peer-to-peer). Where "service" is used to refer to the service management layer as described in ITU-T Recommendation M.3010 [6], appendix B, the full term, "service management layer", will be used.

   NOTE 2: In addition it should be noted that any two OSFs, OSF-A and OSF-B, may have a number of client/server relationships and that the role of each OSF as a service user or as a service provider is defined independently for each relationship. That is in one relationship OSF-A may take on the service user role, with OSF-B representing the service provider, whilst in another relationship OSF-B assumes the service user role with OSF-A as the service provider.

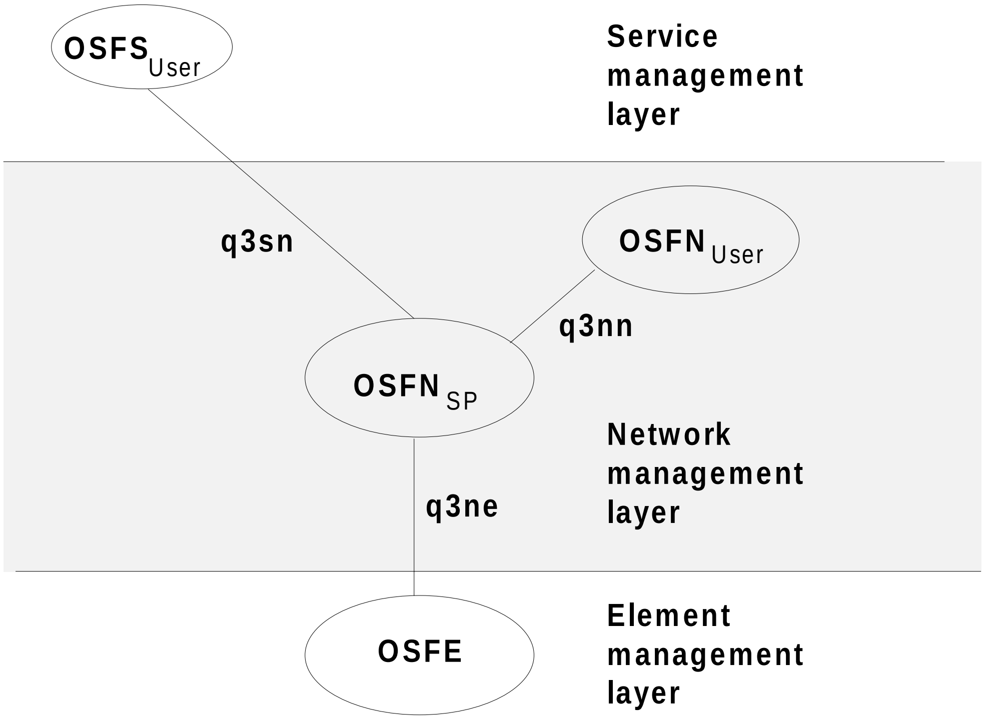


Figure 12: The TMN (management layer) view

The element managers (OSFEs) simultaneously control a number of different NEs, NE-1..NE-n. However, each NE is controlled independently.

The (service management layer or network management layer) user OSF has the responsibility for a "larger" part of the network, which it undertakes by coordinating the activities of a number of service provider OSFs each of which has responsibility for a smaller part of the network.

The (service management layer or network management layer) user OSF requests the service provider OSF to provide a service and the service provider OSF performs the service inter-working, where necessary, with the element manager OSFs.

An Operations System (OS) is a physical implementation of an OSF.

The (service management layer or network management layer) user OS plays the OSI manager role and the service provider OS plays the agent role for the interface between the (service management layer or network management layer) user OS and the service provider OS. For the interface between the service provider OS and the element manager OSs the service provider OS plays the Open Systems Interconnection (OSI) manager role and the element manager OSs plays the agent role (see figure 13).

An ensemble should state which of the above interfaces it is applicable to.

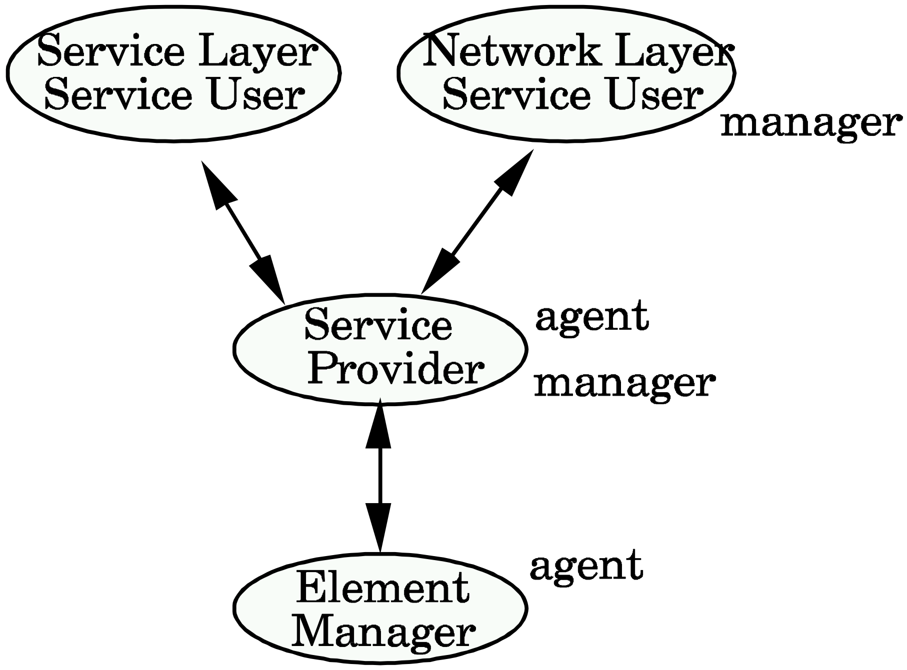


Figure 13: The OSI (manager - agent) view

4.5 The use of a standard class library

Depending upon the management application and the network level interface under consideration, managed objects from the following sources may be used. Wherever possible existing object classes should be used to fulfil the ensemble requirements.

1) I-ETS 300 653 [2]: Managed Object Class Definitions for the Network Level Viewpoint.

2) ITU-T Recommendation M.3100 [3]: Generic Network Information Model.

3) ITU-T Recommendation G.774 [4]: Synchronous Digital Hierarchy (SDH) Management Information Model for the Network Element View.

4) ETS 300 304 [5]: Transmission and Multiplexing SDH Information Model for the Network Element View.

5) ITU-T Recommendation X.700 Series [10]: OSI Management (see annex C, Bibliography).

4.6 The modelling methodology

As already stated the purpose of the modelling process is the description of a number of management capabilities and the production of one, or more, ensembles which will support such management capabilities. A number of ensembles may be combined at an interface. This implies that the following should be supported by a modelling methodology:

1) the description of management capabilities;

2) the mapping of the management capabilities to an information model and the description of that information model (including a Managed Object Conformance Statement (MOCS)).

4.6.1 The description of management capabilities

4.6.1.1 Introduction

An important issue when describing management capabilities is the granularity of management capabilities to be described. This granularity ranges from the broad level, for example, "it shall be possible to configure the network", down to the finest level where, for example, individual result codes may be specified.

It is assumed that the management capabilities described will in general map to a single interaction across the Q3nn or Q3sn interface, described using a template (see below). Where a dialogue is required, several templates should be used.

Management capabilities related to SDH may be grouped together into an ensemble. Ensembles, in general, have the following characteristics:

1) an ensemble may be applicable at more than one interface (e.g. the Q3nn and Q3sn). The service user is located on one side of the interface and the service provider on the other side;

2) an ensemble represents a "contractible" entity. To be compliant with an ensemble, an interface should support the mandated management capabilities specified in the specific conformance requirements of the ensemble;

3) an ensemble may contain a number of individual management capabilities. Management capabilities are associated together for "contracting" purposes, that is, when "contracting" for one service, it would be usual to also "contract" to the associated services.

   The following general management capabilities may be identified:

   a) The management capability itself;

   b) the aborting of the management capability;

   c) the viewing of information related to the management capability.

   NOTE: This list of general services is only given as an example.

4) different ensembles may contain the same management capability;

5) if functional optionality is desired, such optionality should be regarded as a different management capability, and should be described within a separate ensemble. This characteristic should be considered on a case by case basis and is included here as an initial guide;

6) ensembles are described in terms of a list of included management capabilities;

7) a management capability might use other management capabilities at other interfaces in order to fulfil its own function. These should not be mandated by the ensemble.

4.6.1.2 Management capability template

A management capability should be described using the template shown in table 1:

Table 1: Management capability template

Template entry	Entry description
Management capability description	A management capability description describes the purpose and/or scope of the management capabilities as seen by a service user.
Functional requirements	This is a numbered list of functional requirements supported by the management capability.
The input data	This is the data which a service user should supply to a service provider in order for the service provider to provide the service. Some of the data may be optional.
The output data	This is the data which a service provider returns to the service user after having completed the management capability. An important output datum is the "result code" which indicates the success or failure of a request, and, in the case of failure, the reason for the failure. Although result codes should be identified for each service, table 2 identifies a number of general result codes.
Pre-conditions	Pre-conditions express constraints placed on the state of the system for a service to be performed in terms of the resources being managed. Typically, a pre-condition will be checked by a service provider before attempting to perform a service. If one of the pre-conditions associated with the service is not met, then the service can not be performed. As it may not be possible for a service user to know all of the pre-conditions, these are described from the service provider's perspective.
Post-conditions	Post-conditions express the state of the system following successful completion of a management capability in terms of the resources being managed. If a post-condition cannot be fulfilled by the service provider, then the service has failed. A statement should be made as to whether a service is atomic, i.e. will leave the system in its previous state if it fails. Some services, for example, a viewing service, may not change the state of the system, that is, pre- and post-conditions are the same. As it may not be possible for a service user to know all of the post-conditions, these are described from the service provider's perspective.

Table 2: General fault types

Fault type	Description
Parameter value error	A sent parameter value is not supported. A sent parameter value is out of range. A sent parameter value is not recognised.
Pre-conditions not met	A pre-condition can not be met.
Service could not be provided	Post-conditions can not be met e.g. because communication to a network element has been lost.
Access restriction	The service user does not have the authority for the service.
Insufficient management resources	The service provider is not able to process the request due to insufficient management resources.

4.6.2 The mapping of the management capabilities to the information model

The information model which supports the identified management capabilities is described in terms of similar concepts as those used to describe a management capability (see subclause 4.6.1.2), namely:

a) **pre-conditions**, describing the state that the information model should be in prior to the invocation of the first Common Management Information Service (CMISE) service in order for the service to be performed successfully;

b) **CMISE service(s)** requested by the manager and the resulting actions performed by the agent in order to fulfil the requested CMISE service;

c) **Common Management Information Protocol (CMIP) parameters** sent with a CMISE service request and returned to the manager;

d) **potential fault cases** which may be indicated within the CMISE service responses;

e) **post-conditions**, describing the state of the information model at the conclusion of the final CMISE service.

Mapping is performed at the service level. The components of each management capability template are mapped to the information model:

- the resources concerned are mapped to the Managed Object (MO) classes (including any required new classes) in the ensemble, in terms of the pre- and post-conditions;

- the input/output data is mapped to MO attributes, action information syntax and the CMISE error parameter (i.e. to CMISE service parameters);

- the functional requirements are mapped to MO actions.

Table 3 describes the form of the mapping. For each management capability template, several mappings to the information model may be required, e.g. if there are several functional requirements relating to one management capability.

Table 3: Service level mappings

Management capability template component	Requirement (service) description	Implementation (information fragment) description
Functional requirements	Messages	Normally described in terms of a single CMISE service and the resulting actions performed by the agent. The following CMISE services may be required: CMISE management notification service, that is, * M-EVENT-REPORT (used by one CMISE-service-user to report an event about a managed object to a peer CMISE-service-user), and CMISE management operation services, that is, * M-GET (used by one CMISE-service-user to request the retrieval of management information from a peer CMISE-service-user) * M-SET (used by one CMISE-service-user to request the modification of management information by a peer CMISE-service-user) * M-ACTION (used by one CMISE-service-user to request a peer CMISE-service-user to perform an action) * M-CREATE (used by one CMISE-service-user to request a peer CMISE-service-user to create an instance of a managed object) * M-DELETE (used by one CMISE-service-user to request a peer CMISE-service-user to delete an instance of a managed object) Each CMISE service is described in terms of the following primitives: * A Service Request (Req) and a Service Indication (Ind) * A Service Confirm (Conf) and a Service Response (Rsp) A brief introduction to the use of CMISE/CMIP is given in annex B. The description of the resulting actions performed by the agent describes those actions performed by the agent in order to fulfil a CMISE Req. These actions are described by MO behaviour which is written in an implementation independent manner.

(continued)

Table 3 (concluded): Service level mappings

Management capability template component	Requirement (service) description	Implementation (information fragment) description
		This implies that such descriptions should not mandate the interface across which any consequential agent actions are performed nor the form of those actions.
Input data	Message parameters	CMISE service parameters.
Output data	Message parameters	CMISE service parameters.
Output data - Potential fault cases	Informal description according the management capability template output data result codes	Specific value of a CMISE service parameter or the CMISE error parameter.
Pre-conditions	The status of ITU-T Recommendation G.803 [1] entities as perceived by the agent prior to the invocation of the service	The status of the information fragment prior to the first CMISE Service Request (Req) being sent by the manager is described in terms of: * Pre-existing object instances; * Object instances' attribute values, in particular: state attribute values; pointer attribute values.
Post-conditions	The status of ITU-T Recommendation G.803 [1] entities as perceived by the agent at the completion of the service	The status of the information fragment after the final CMISE Service Response (Rsp) has been received by the manager is described in terms of: * Object status (which instances exist); * Attribute values (in particular state attribute and pointer values) within object instances.
NOTE: The term "action" (lower-case) is used in its normal sense (feat or deed).		

A MOCS proforma should be provided in an ensemble. These are described in section 4 of The "Ensemble" Concept and Format [7], and an example can be found in annex B of Reconfigurable Circuit Service: Configuration Management Ensemble [8].

4.7 The support of multiple managers

All network level interfaces should support multiple managers. This means that the CMISE services should allow different managers to interact with the same managed object tree. This can be achieved by allowing each manager its own view of that tree (which may be more or less restrictive than another manager's view). This has implications for the security and control of access and for the naming of managed objects in the tree.

4.8 The management capabilities to be supported

Initially only a limited set of management capabilities will be considered. These functions will be taken from the functional area "Configuration management" which is described in annex A.

The following is a list of functional areas which may have to be considered for the development of ensembles:

- configuration management;
- scheduling;
- event (including fault) management;
- performance monitoring;
- restoration/protection;
- accounting management / charging / usage control;
- lifecycle provisioning / inventory handling;
- synchronisation;
- security;
- conformance and testing.

NOTE 1: It is not possible to assign a priority regarding the order in which each functional area should be considered.

NOTE 2: It is possible to consider management capabilities and derive CMISE service descriptions and the corresponding information fragment in an isolated fashion. However, if ensembles are to be combined at an interface, then those ensembles should use a compatible managed object model. For instance, one ensemble might use sub-classes of the objects used in the first, or might specify additional object classes and name bindings, thus adding to the originals by containment. Either of these techniques would allow the requirements of the first ensemble to be met and additionally meet the requirements of the second. The use of containment would probably be the most flexible method, as the use of sub-classing could lead to conflicts where more than two ensembles were being combined.

5 The structure of an ensemble

The format of an ensemble is given in The "Ensemble" Concept and Format [7] and guidance is given in the Reconfigurable Circuit Service: Configuration Management Ensemble [8] on the content of the various sections. The principles described in the preceding subclauses are applied to the format given in The "Ensemble" Concept and Format [7] resulting in an ensemble with the following structure:

1 Introduction

Text is taken from the Reconfigurable Circuit Service: Configuration Management Ensemble [8].

1.1 Unique identity

The unique identity is a registered object identifier used to identify the ensemble.

1.2 General description of the ensemble

1.3 Scope and purpose

including - *Statement of the management capabilities to be covered by the ensemble (see subclause 4.8);*

Statement of the transport network architecture that the ensemble is intended for (see subclause 4.1).

1.4 Relationships with other ensembles

2 Management context

2.1 General introduction

2.2 Management view and level of abstraction

including - *Statement of the functional management architecture that is to be used and which interfaces the ensemble is applicable to (see subclause 4.4).*

2.3 Resources

Description of the resources that are to be managed in terms of ITU-T Recommendation G.803 [1] entities (see subclause 4.2).

2.4 Functions

A detailed description of the management capabilities (using the template defined in subclause 4.6.1).

3 Management information model

3.1 General introduction

including - *Statement of which standard library or libraries are to be used (see subclause 4.5), whether extensions are required and where those extensions are defined (e.g. in an appendix of the ensemble);*

General mapping of resource entities to managed object classes.

3.2 Relationships

3.3 Scenarios

The mapping of the management capabilities to the information model (using the template defined in subclause 4.6.2).

3.4 Management information references

A formal reference list of all the definitions of management information relevant to the ensemble (this will repeat some of the information in subclause 3.1).

4 Ensemble conformance requirements

4.1 General conformance requirements

4.2 Specific conformance requirements

Annex A Glossary

Annex B MOCS proformas (see subclause 4.6.2)

Annex C References list

Annex D Additional managed object definitions if required

Annex A: Configuration management

Configuration management includes the following functions:

Table A.1: Configuration management functions

	Functions
1	The provisioning of a layer network and characteristic information
2	The provisioning of access points
3	The provisioning of access groups
4	The configuration of access groups
5	The provisioning of connection points
6	The configuration of connection point groups
7	The provisioning of sub-networks
8	The configuration of sub-networks
9	The setting-up of trails
10	The release of trails
11	The setting-up of tandem connections
12	The release of tandem connections
13	The setting-up of sub-network connections
14	The release of sub-network connections
15	The provisioning of links
16	The configuration of links
17	The provisioning of link connections
18	The release of link connections
19	Viewing functions

A.1 The provisioning of a layer network and characteristic information

The mechanism for the establishment of a layer network is outside the scope of this ETR.

Characteristic information is a signal generated at a trail termination function for transport across a layer network, and presented to serving layer networks via an adaptation function. Thus the characteristic information itself is not directly managed, only the access points, trails, adaptation functions etc. involved in its transport.

A.2 The provisioning of access points

A manager is allowed to request the creation or deletion of an access point.

A.3 The provisioning of access groups

A manager will have the ability to request the creation or deletion of access groups. An initial view of access points in access groups may be provided, which may be fixed. Access groups may also be formed into a hierarchy, with an access point being a member of all the superior access groups which contain the lowest access group of which it is a member.

Where multiple managers may be accessing the same agent, the access groups will be part of a particular manager's "view". This will be a case where the agent either restricts the view of the access group to the manager which created it, or prevents the other managers from deleting it.

A.4 The configuration of access groups

A manager will have the ability to add and remove access points to/from an access group. Where the access groups form a hierarchy, the access points should be added to/removed from an access group at the lowest level of the hierarchy.

A.5 The provisioning of connection points

A manager is allowed to request the creation or deletion of one or more connection points.

A.6 The Configuration of connection point groups

A manager will have the ability to group connection points together. These groups may be associated with particular links leaving a sub-network. This allows an association between connection points and links to be established before the link connections bundled by the links have been established.

A.7 The provisioning of sub-networks

A manager will have the ability to request the creation or deletion of sub-networks. The manager will be presented with a "view" of sub-networks provided by the agent, which will reflect the cross-connectability of the connection points. This view will not necessarily be of the lowest possible level of partitioning, but will be appropriate for the task to be performed by the manager. The manager can create and delete sub-networks as it wishes, specifying whether a new sub-network is to be a super- or sub- partition of existing sub-networks. Normally a manager is not allowed to delete the initial sub-network view.

A.8 The configuration of sub-networks

A manager will have the ability to add and remove connection points and access points to/from a sub-network. An access point will be visible from all the levels of sub-network partitioning in which it is contained. A connection point will be visible from a particular level of sub-network partitioning if it provides access to that sub-network (i.e. it will not be visible if it is internal to the sub-network).

A manager may require more than one view of the resources. Therefore the manager will have the ability to add and remove access and connection points to/from multiple sub-networks taking part in separate partitioning structures. Normally a manager is not allowed to delete connection points within the initial sub-network view.

A.9 The setting-up of trails

A manager will have the ability to request that a trail be set up between two access points. The manager may specify the routing in terms of the sub-networks or links to be used, or in terms of particular link connections to be used, or may not specify a routing. The manager may also specify that the trail is to be separate at some level from another configuration, may specify a particular QoS or a particular method of protection.

A.10 The release of trails

A manager will be able to request the release of a previously set-up trail.

A.11 The setting-up of tandem connections

A manager will have the ability to request that a tandem connection be set up between two connection points. The manager may specify the routing in terms of the sub-networks or links to be used, or in terms of particular link connections to be used, or may not specify a routing.

A.12 The release of tandem connections

A manager will be able to request the release of a previously set-up tandem connection.

A.13 The setting-up of sub-network connections

A manager will have the ability to request a sub-network connection between two connection points, or groups of connection points, in the same sub-network. The manager may request the sub-network connection by specifying the links and sub-networks at lower levels of partitioning to be used, or specify individual connection points within sub-networks at lower levels of partitioning.

A.14 The release of sub-network connections

Will be able to request the release of a previously set-up sub-network connection.

A.15 The provisioning of links

Initially, the manager may be presented with a "view" of links provided by the agent between sub-networks, which will reflect provisioned link connections. This view will not necessarily be of the lowest possible level of partitioning, but will be appropriate for the task to be performed by the manager.

A manager will have the ability to request that a link be instantiated between two sub-networks. These links may be empty (i.e. not have any link connections). A manager will in general be required to create multiple links which share some mutual disjointedness to support diverse routing for protected sub-network connections and trails. This implies that the manager will be able to read some disjointedness information in the network topology on which to base its routing choices.

A.16 The configuration of links

A manager will have the ability to add and remove link connections to/from a particular link, according to its topological needs, or to request more link connections for the link.

A.17 The provisioning of link connections

A manager will have the ability to request that a link connection be set up between two connection points. It has been recognised that there may be a need to allow the construction of "composite" link connections between sub-networks, delimited by "elementary" (i.e. normal) link connections, consisting of a series of transit sub-network connections and link connections. These then hide the detail of the intermediate sub-networks, and may be mixed in links with elementary link connections provided they share the same topological properties.

A.18 The release of link connections

A manager will be able to request the release of a previously set-up link connection.

A.19 Viewing functions

The following is an initial list of viewing functions:

1) viewing of provisioning state;

2) viewing of network topology;

3) viewing of network connectivity.

Annex B: Introduction to CMISE/CMIP

The following annex provides an introduction to Common Management Information Service (CMISE) and Common Management Information Protocol (CMIP).

This introduction is not meant to supersede ITU-T Recommendations X.710 or X.711 but intended to aid readers in their understanding of CMISE/CMIP descriptions.

The following issues should be covered in section 3.3 of the ensemble:

- use of Req, Ind, Conf, Rsp;

- which service parameters will be used and their meaning:

  - base object class / instance;
  - managed object class / instance.

- the class to which an action is sent (where ACTION is defined or sub-class which uses ACTION);

- policy concerning which state change notifications will be described in the case of object creation and deletion;

  no EVENT-REPORTS, except those which explicitly indicate the creation / deletion of an object instance will be sent in the case of the creation / deletion (that is, EVENT-REPORTS indicating a attribute value change of a state change in the case of and attribute or state being initially set or removed due to the creation or deletion of the containing object instance will not be sent);

- information sent back by the agent in the case of creation of a new object (all attribute values or just those set by the agent);

- description of error cases ("normal" + "pre-conditions" not met);

- which fault cases "caught" by the CMIP protocol (e.g. parameter faults).

The following tables summarise CMISE message parameters:

Table B.1: Summary of CMISE message parameters

Service	M-GET		M-SET		M-ACTION		M-CREATE		M-DELETE		M-EVENT-REPORT	
Parameter name	**Req/ Ind**	**Rsp/ Conf**	**Req/ Ind**	**Rsp/ Conf**	**Req/ Ind**	**Rsp/ Conf**	**Req/ Ind**	**Rsp/ Conf**	**Req/ Ind**	**Rsp/ Conf**	**Req/ Ind**	**Rsp/ Conf**
Invoke identifier	M	M	M	M	M	M	M	M(=)	M	M	M	M(=)
Mode	ND	ND	M	-	M	-	ND	ND	ND	ND	M	-
Linked identifier	-	C	-	C	-	C	ND	ND	-	C	ND	ND
Base object class	M	-	M	-	M	-	ND	ND	M	-	ND	ND
Base object instance	M	-	M	-	M	-	ND	ND	M	-	ND	ND
Scope	U	-	U	-	U	-	ND	ND	U	-	ND	ND
Filter	U	-	U	-	U	-	ND	ND	U	-	ND	ND
Access control	U	-	U	-	U	-	U	-	U	-	ND	ND
Synchronisation	U	-	U	-	U	-	ND	ND	U	-	ND	ND
Attribute identifier list	U	-	ND	ND	ND	ND	ND	ND	ND	ND	ND	ND
Managed object class	-	C	-	C	-	C	M	C	-	C	M	U
Managed object instance	-	C	-	C	-	C	U	C	-	C	M	U
Superior object instance	ND	ND	ND	ND	ND	ND	U	-	ND	ND	ND	ND
Reference object instance	ND	ND	ND	ND	ND	ND	U	-	ND	ND	ND	ND
Current time	-	U	-	U	-	U	-	U	-	U	-	U
Attribute list	-	C	M	C	ND	ND	U	C	ND	ND	ND	ND
Event reply	ND	ND	ND	ND	ND	ND	ND	ND	ND	ND	-	C
Action type	ND	ND	ND	ND	M	C(=)	ND	ND	ND	ND	ND	ND
Action information	ND	ND	ND	ND	U	-	ND	ND	ND	ND	ND	ND
Action reply	ND	ND	ND	ND	-	C	ND	ND	ND	ND	ND	ND
Errors	-	C	-	C	-	C	-	C	-	C	-	C

Key:

M: The parameter is mandatory.

(=): The value of the parameter is equal to the value of the parameter in the column to the left.

U: The use of this parameter is a service-user option.

-: The parameter is not present in the interaction described by the primitive concerned.

C: The parameter is conditional. The condition(s) are defined in the text which describes the parameter.

ND: The parameter is not defined for the service concerned.

Table B.2: CMISE message parameter descriptions

Parameter name	Parameter description
Invoke identifier	This parameter specifies the identifier assigned to the operation. It can be used to distinguish this operation from other notifications or operations that the CMISE-service-provider may have in progress.
Mode	This parameter specifies the mode requested for the operation. The possible values are: - confirmed; - not-confirmed.
Linked identifier	If multiple replies are to be sent for this operation, then this parameter specifies the identification that is provided by the CMISE-service-user when those replies are returned. The linked identifier shall have the same value as that of the invoke identifier provided in the indication primitive.
Base object class	This parameter specifies the class of the managed object that is to be used as the starting point for the selection of managed objects on which the filter (when supplied) is to be applied.
Base object instance	This parameter specifies the instance of the managed object that is to be used as the starting point for the selection of managed objects on which the filter (when supplied) is to be applied.
Scope	This parameter indicates the sub-tree, rooted at the base managed object, which is to be searched. The levels of search that may be performed are: * the base object alone; * the n^{th} level subordinates of the base object; * the base object and all of its subordinates down to and including the n^{th} level; * the base object and all of its subordinates. The default scope is the base object alone.
Filter	This parameter specifies the set of assertions that defines the filter test to be applied to the scoped managed object(s). Multiple assertions may be grouped using the logical operations AND, OR and NOT. Each assertion may be a test for equality, ordering, presence, or set comparison. Assertions about the value of an attribute are evaluated according to the matching rules associated with the attribute syntax. If an attribute assertion is present in the filter and that attribute is not present in the managed object, then the result of the test for that attribute assertion shall be evaluated as FALSE. The managed object(s) for which the filter test evaluates to TRUE are selected for the application of the operation. If the filter is not specified, all of the managed objects included in the scope are selected.
Access control	This parameter is information of unspecified form to be used as input to the access control functions.
Synchronisation	This parameter indicates how the invoking CMISE-service-user wants information retrievals synchronised across the selected object instances. Two ways of synchronising a series of retrievals are defined: - Atomic: All retrievals are checked to see whether they can be performed. If an retrieval cannot be performed, then none is performed, otherwise all retrievals are performed; - Best effort: All retrievals are attempted. If an unsuccessful retrieval occurs, the remaining retrievals are still attempted. If this parameter is not supplied, best effort synchronisation is performed. When the synchronisation parameter is used and a single managed object is specified, then the value of this parameter has no effect on the retrieval.
Attribute identifier list	This parameter contains the set of attribute identifiers for which the attribute values are to be returned by the performing CMISE-service-user. If this parameter is omitted, all attribute identifiers are assumed. The definitions of the attributes are found in the specification of the managed object class.

(continued)

Table B.2 (concluded): CMISE message parameter descriptions

Parameter name	Parameter description
Managed object class	If the base object alone is specified, then this parameter is optional, otherwise it shall specify the class of managed object whose attribute values are returned. It may be included in any confirmation.
Managed object instance	If the base object alone is specified, then this parameter is optional, otherwise it shall specify the instance of managed object whose attribute values are returned. It may be included in any confirmation.
Superior object instance	This parameter identifies the existing managed object instance which is to be the superior of the new managed object instance. If this parameter is supplied by the invoking CMISE-service-user, then the managed object instance parameter shall not be supplied.
Reference object instance	When this parameter is supplied by the invoking CMISE-service-user, it should specify an existing instance of a managed object, called the reference object, of the same class as the managed object to be created. Attribute values associated with the reference object instance become the default values for those not specified by the attribute list parameter.
Current time	This parameter indicates the time at which the response was generated. It may be included in the success confirmation.
Attribute list	This parameter contains the set of attribute identifiers and values that are returned by the performing CMISE-service-user. It shall be included in the success confirmation.
Event reply	This parameter contains the reply to the event report. It may be included in the success confirmation.
Action type	This parameter specifies a particular action that is to be performed. It may be included in the success confirmation and shall be included if the action reply parameter is included.
Action information	This parameter specifies extra information when necessary to further define the nature, variations or operands of the action to be performed. The syntax and semantics of the parameter depend upon the action requested.
Action reply	This parameter contains the reply to the action. It may be included in the success confirmation.
Errors	Possible error values are listed in table B.3 below.

Table B.3: CMISE service - errors

CMISE service parameter name		M-GET	M-SET	M-ACTION	M-CREATE	M-DELETE	M-EVENT REPORT
Not related to a particular CMISE service parameter	* Processing failure: A general failure in processing the notification was encountered;	G	S	A	C	D	ER
	* Resource limitation: The notification was not processed due to resource limitation;	G	S	A	C	D	ER
	* Unrecognised operation: The operation is not one of those agreed between the CMISE service-users;	G	S	A	C	D	D
	* Complexity limitation: The requested operation was not performed because a parameter was too complex;	G	S	A		D	
	* Mistyped argument: One of the parameters supplied has not been agreed for use on the association between the CMISE-service users.		S	A	C		
Invoke identifier	* Duplicate invocation: The invoke identifier specified was allocated to another notification or operation.	G	S	A	C	D	ER
Access control	* Access denied: The requested operation was not performed for reasons pertinent to the security of the open system.	G	S	A	C	D	
Action information	* Invalid argument value: The action information value specified was out of range or otherwise inappropriate;			A			
	* No such argument: The action information specified was not supported.			A			
Action reply	No directly related error.						
Action type	* No such action: The action type specified was not supported.	A		A			
Attribute identifier list	No directly related error.						
Attribute list	No directly related error.						
Base object class	* No such object class: The class of the specified managed object was not recognised.	G	S	A		D	ER
Base object instance	* No such object instance: The instance of the specified managed object was not recognised;						
	* Class instance conflict: The specified managed object instance is not a member of the specified class;						
	* Duplicate managed object instance: The new managed object instance value supplied by the invoking CMISE-service-user was already registered for a managed object of the specified class.						

(continued)

Table B.3 (concluded): CMISE service - errors

CMISE service parameter name		M-GET	M-SET	M-ACTION	M-CREATE	M-DELETE	M-EVENT REPORT
Current time	No directly related error.						
Event information	* Invalid argument value: The event information value specified was out of range or otherwise inappropriate; * Invalid argument value: The event information specified was not recognised.	G	S	A		D	ER ER
Event reply	No directly related error.						
Event time	No directly related error.						
Event type	* No such event type: The event type specified was not recognised.						ER
Filter	* Invalid filter: The filter parameter contains an invalid assertion or an unrecognised logical operator.	G	S	A		D	
Linked identifier	No directly related error.						
Managed object class	* No such object class: The class of the specified managed object was not recognised.				C		
Managed object instance	* Invalid object instance: The object instance name specified implied a violation of the naming rules.				C		
Mode	No directly related error.						
Reference object instance	* No such reference object: The reference object instance parameter was not recognised.				C		
Scope	* Invalid scope: The value of the scope parameter is invalid.	G	S	A		D	
Superior object instance	* No such object instance: The instance of the specified superior managed object was not recognised.				C		
Synchronisation	* Synchronisation not supported: The type of synchronisation specified is not supported.	G	S	A		D	
Errors	No directly related error.						

Annex C: Bibliography

- ITU-T Recommendation X.700: "Management framework for Open Systems Interconnection (OSI) for CCITT applications".

- ITU-T Recommendation X.701: "Information technology - Open Systems Interconnection - Systems management overview".

- CCITT Recommendation X.710: "Common Management Information Service definition for CCITT applications".

- CCITT Recommendation X.711: "Common management information protocol specification for CCITT applications".

- ITU-T Recommendation X.712: "Information technology - Open Systems Interconnection - Common management information protocol: Protocol implementation conformance statement proforma".

- ITU-T Recommendation X.720: "Information technology - Open Systems Interconnection - Structure of Management Information: Management information model".

- ITU-T Recommendation X.721: "Information technology - Open Systems Interconnection - Structure of Management Information: Definition of management information".

- ITU-T Recommendation X.722: "Information technology - Open Systems Interconnection - Structure of Management Information: Guidelines for the definition of managed objects".

- ITU-T Recommendation X.723: "Information technology - Open Systems Interconnection - Structure of management information: Generic management information".

- ITU-T Recommendation X.724: "Information technology - Open Systems Interconnection - Structure of management information: Requirements and guidelines for implementation conformance statement proformas associated with OSI management".

- ITU-T Recommendation X.730: "Information technology - Open Systems Interconnection - Systems Management: Object management function".

- ITU-T Recommendation X.731: "Information technology - Open Systems Interconnection - Systems Management: State management function".

- ITU-T Recommendation X.732: "Information technology - Open Systems Interconnection - Systems Management: Attributes for representing relationships".

- ITU-T Recommendation X.733: "Information technology - Open Systems Interconnection - Systems Management: Alarm reporting function".

- ITU-T Recommendation X.734: "Information technology - Open Systems Interconnection - Systems Management: Event report management function".

- ITU-T Recommendation X.735: "Information technology - Open Systems Interconnection - Systems Management: Log control function".

- ITU-T Recommendation X.736: "Information technology - Open Systems Interconnection - Systems Management: Security alarm reporting function".

- ITU-T Recommendation X.738: "Information technology - Open Systems Interconnection - Systems management: Summarization function".

- ITU-T Recommendation X.739: "Information technology - Open Systems Interconnection - Systems Management: Metric objects and attributes".

- ITU-T Recommendation X.740: "Information technology - Open Systems Interconnection - Systems Management: Security audit trail function".

- ITU-T Recommendation X.745: "Information technology - Open Systems Interconnection - Systems Management: Test management function".

- ITU-T Recommendation M.60: "Maintenance terminology and definitions".

History

Document history	
April 1996	First Edition

ISBN 2-7437-0650-3
Dépôt légal : Avril 1996