ETSI TS 101 892 V1.1.1 (2001-01)
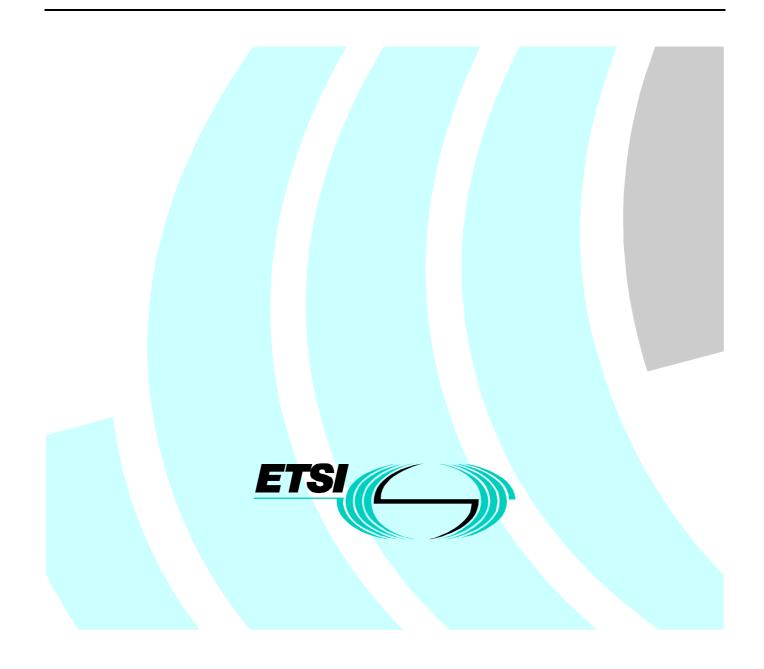
Technical Specification

**Telecommunications Management Network (TMN);
Protocol and interface service requirements**

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or
perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF).
In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive
within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at http://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

ETSI

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Telecommunications Management Network (TMN).

Introduction

The telecommunications industry has developed management architectures and interfaces that are scalable and have the capability to manage large complex networks. With the convergence of telecommunications and computing the telecommunications infrastructure technology is changing. New approaches to management are being introduced and additional interface protocols are being proposed. Therefore, there is a requirement to assist the industry with the selection of interface protocols that are suitable for the management of large telecommunications networks.

1 Scope

The present document specifies key application level protocol and message service requirements to support TMN management interfaces. It includes a general set of requirements together with requirements based on the traditional FCAPS functional breakdown for management.

The present document is applicable to the selection of interface technology for the TMN architecture defined in ITU-T Recommendation M.3010 [1]. The primary requirements that should be supported across an interface at any particular management layer will be dependent on the functionality to be managed across that interface.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies.

[1] ITU-T Recommendation M.3010: "Principles for a Telecommunications Management Network".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

action: action operation requests an object to perform a specified task and to indicate the result of that task. The action and optional associated information are a part of the definition of the object class.

attribute: element of management information.

3.2 Abbreviations

For the purposes of the present document, the following abbreviation applies:

TMN Telecommunications Management Network

4 Protocol and Interface Service Requirements

4.1 All-purpose Requirements

The following is a list of general requirements to support management:

session control: with the increasing use of a connectionless approach, a managing system needs to be informed if/when a TMN session is broken.

knowledge management: unless everybody does the same thing and it never changes, there is always the need to know the capabilities of the system at the other end of the TMN interface. It is necessary to have some method to discover what that is (without going through trial and error on a per instance basis). There is also a requirement to discover what management information is at the other end of a TMN interface (some sort of bulk upload).

multiple responses: for example, a test action request that is to be performed every 10 minutes on some remote object will generate a test result response every 10 minutes until told to stop. The managing system should not have to request the action each time.

support for multiple simultaneous managing systems: it is common in telecommunications management that the same entity is managed by different applications from different operations support systems. For example, it should be possible for multiple managing systems to receive notifications.

containment relationship: in telecommunication equipment the name of an entity often reflects the containment relation. For example, the name of a circuit pack is defined in terms of the shelf and slot it is plugged into (contained). This is a very specific type of relationship that is used to carry information about equipment hierarchy in many products. Therefore, there is a requirement to support containment relationships.

support for multiple objects manipulation: it should be possible to efficiently search the containment tree (or subtree) for objects with attributes meeting specific criteria and then to set the values of a specified set of attributes.

length of messages: for all practical purposes there should be no limit on the length of messages or data exchanged.

segmentation of message: to avoid long messages blocking communication, it should be possible to segment messages. To support this requirement, mechanisms such as sequence numbers should be used to maintain transmission sequence.

communication: both asynchronous and synchronous operations and communication should be supported.

synchronous operations: to maintain data integrity the manager may want operations to be synchronized across selected object instances. Two ways of synchronising a series of operations are:

- Atomic: all objects that are selected for an operation are checked to ascertain if they are able to successfully perform the operation. If one or more is not able to successfully perform the operation, then none perform it, otherwise all perform it;

- Best effort: all objects selected for the operation are requested to perform it.

multi-Tasking: the interface should permit multiple message requests to be outstanding at a time, therefore, the interface should not limit the managing system to one process at a time.

support for attribute locking: for example, the interface should support read only attributes.

identification of objects: the use of unique names to identify objects is required.

operation acknowledgement: this is necessary to ensure that critical management operations have been carried out.

4.2 Fault Management Requirements

The following lists additional requirements to support fault management:

handle unsolicited fault messages in (near) real-time: cable cuts, for example, may cause many fault notifications from many network elements and these need to be handled in (near) real-time.

enable targeted control: to control alarm distribution and ensure fault messages contain identities.

autonomous notifications with the managing system able to select the received notifications: a managed entity should be able to send notifications corresponding to events such as change of state. The managing system should be able to control which events should be reported to it.

definition of notifications: there should be a facility to define the structure for the information in the notification as well as describe the behavioural aspects such as the impact on state information.

provide auditability and traceability: provide interface services to enable tracking of alarm handling. (e.g., support for logging of alarms and sequencing of information).

4.3   Configuration Management Requirements

The following lists additional requirements to support configuration management:

support for various levels of granularity: it should be possible to manipulate objects at different levels of granularity, i.e., to be able to manipulate at an attribute, at a single managed entity (object) or multiple managed entities (objects) with a single operation. (E.g., get, set or list default value of a counter attribute).

support for query capabilities: it should be possible to efficiently read multiple attributes values as well as all object attributes with a single request.

support for modification capabilities: it should be possible to efficiently construct modification for an arbitrary set of attributes thus offering an efficient mechanism to update multiple attributes values in one operation.

support to add and remove attributes in set valued attributes: it should be possible to efficiently add and remove attributes for set valued attributes.

support for selective access to attributes: it should be possible to selectively perform operations on single and set valued attributes. For example, it should be possible for an attribute with a set of values to be tested for superset/subset or set intersection of a given set of values. Single valued attributes should be testable for equality, ordering, and substring (beginning, end, anywhere).

support for multiple object query: it should be possible to efficiently search the containment tree (or subtree) for objects with attributes meeting specified criteria (including the set valued attribute matching criteria specified above) and to then return selected attribute values as discussed above.

support for deletion semantics: information models should be defined to include semantics when deleting an object. It should be possible to delete an object and specify all the containing objects that are also to be deleted. This has two advantages - 1) maintaining referential integrity among the objects and 2) efficient operation to delete a collection of objects in a co-ordinated manner.

support for creation semantics: there is a need to clearly specify how objects are created either by management operations or automatically created.

support for actions: this is to enable a manger to requests a managed entity (object) to perform a specified task and to respond with the results of that task. For example, setting up a connection across a cross connect would require multiple transactions across the wire without the support of an action.

4.4   Accounting and Performance Management Requirements

This requires efficient handling of large amounts of data. The following lists additional requirements to support accounting and performance management:

- to be able to collect large amounts of information into a file or other structure;

- to be able to process files, which contain many records or on just one record, as a single unit;

- transfer of bulk data;

- transfer of single records;

- transaction control - it must be possible to guarantee records arrive at their destination.

4.5 Security Management Requirements

The following lists additional requirements to support security management:

- authentication: it is important to guarantee that the two ends of a TMN conversation are genuine entities. It should be possible to enable authentication on a session basis, rather than repeat it for each individual message ("who are you" and "can you prove it");

- for connectionless communications it may be necessary to provide a more secure mechanism to avoid sending security information on a per message basis;

- provide support for access control at various levels;

- support non-repudiation (data integrity/control and repeatability);

- be able to guarantee receipt of specific messages. This is essential for security alarms;

- support should also be provided for encryption.

History

Document history		
V1.1.1	January 2001	Publication