Technical Specification Group Services and System Aspects
Meeting #7, Madrid, Spain, 15-17 March 2000

TSGS#7(00)0012

Source: **WG SA5 (Telecom Management)**

Title: **32.106 v.2.0.0 (3G Configuration Management)**

Document for: **Approval**

Agenda Item: **5.5.3**

Ty	Number	Title	WG	editor	version
TS	32.106	3G Configuration Management	S5	Thomas Tovinger	2.0.0

Based on:

S5-000169	3G TS 32.106 v1.4.0 (3G Configuration Management)	CM rapporteur (Thomas Tovinger)

Open issues for R99:

……

CM rapporteur (Thomas Tovinger)

Thomas Tovinger (ERV) [Thomas.Tovinger@erv.ericsson.se]

Telecom Management
System Design and Standardization
ERICSSON MOBILE DATA DESIGN AB
Box 333
SE-431 24 Mölndal, Sweden
Tel.: +46 31 747 3010

Mobile: +46 31 747 3010

Fax: +46 31 747 2942

E-mail: Thomas.Tovinger@erv.ericsson.se

Technical Specification Group Services and System Aspects *TSGS#7(00)0012 annex*
Meeting #7, Madrid, Spain, 15-17 March 2000
3GPP TSG-SA5 (Network Management) POST-meeting #10, Luleå, Sweden, 29 Feb – 3 Mar 2000 ***Tdoc S5-000169***

3G TS 32.106 V2.0.0 (2000-03)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Configuration Management (3G TS 32.106 version 2.0.0 Release 1999)

Reference
3TS/TSGS-0532106U

Keywords
Configuration Management

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3GPP.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 Indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the specification;

Introduction

Configuration Management (CM), in general, provides the operator with the ability to assure correct and effective operation of the 3G network as it evolves. CM actions have the objective to control and monitor the actual configuration on the NEs and NRs, and they may be initiated by the operator or functions in the OSs or NEs.

CM actions may be requested as part of an implementation programme (e.g. additions and deletions), as part of an optimisation programme (e.g. modifications), and to maintain the overall Quality of Service. The CM actions are initiated either as a single action on a network element of the 3G network or as part of a complex procedure involving actions on many network elements.

In this document, Clauses 4 through 6 are here provided to give an introduction and description of the main concepts of configuration management, which is not mandatory for the compliance to this specification in this release. Clause 7 contains the specific definitions for the standardised N-interface, which are necessary to follow for compliance.

Clause 4 provides a brief background of CM while Clause 5 explains CM services available to the operator. Clause 6 breaks these services down into individual CM functions, which support the defined services. Clause 7 defines the N-interface to be used for 3G CM.

1 Scope

This Technical Specification (TS) describes the Configuration Management (CM) aspects of managing a 3G network. This is described from the management perspective outlined in the two 3GPP specifications 32.101 [1] and 32.102 [2].

This TS defines a set of controls to be employed to effect set-up and changes to a 3G network in such a way that operational capability and quality of service, network integrity and system inter working are ensured. In this way, this TS describes the interface definition and behaviour for the management of relevant 3G network NEs in the context of the described management environment. The context is described for both the management systems (OS) and NE functionality.

Clause 7 contains the specific definitions for the standardised N-interface, which are necessary to follow for compliance to this specification.

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, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an TS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative references

[1] 3GPP 32.101 - 3G Telecom Management principles and high level requirements

[2] 3GPP 32.102 - 3G Telecom Management architecture

3 Definitions and Abbreviations

3.1 Definitions

For the purposes of this TS the following definitions apply.

Data: is any information or set of information required to give software or equipment or combinations thereof a specific state of functionality.

Element Manager (EM): provides a package of end-user functions for management of a set of closely related types of network elements. These functions can be divided into two main categories:

- *Element Management Functions* for management of network elements on an individual basis. These are basically the same functions as supported by the corresponding local terminals.

- *Sub-Network Management Functions* that are related to a network model for a set of network elements constituting a clearly defined sub-network, which may include relations between the network elements. This model enables additional functions on the sub-network level (typically in the areas of network topology presentation, alarm correlation, service impact analysis and circuit provisioning).

Equipment: is one or more hardware items which correspond to a manageable or supervisable unit or is described in an equipment model.

Firmware: is a term used in contrast to software to identify the hard-coded program, which is not downloadable on the system.

Hardware: is each and every tangible item.

IRP Information Model: See [1].

IRP Information Service: See [1].

IRP Solution Set: See [1].

Managed Object (MO): an abstract entity which may be accessed through an open interface between two or more systems, and representing a Network Resource for the purpose of management. The MO is an instance of a Managed Object Class (MOC) as defined in a Management Information Model (MIM). The MIM does not define how the MO or NR is implemented; only what can seen in the interface.

Managed Object Class (MOC): a description of all the common characteristics for a number of MOs, such as their attributes, operations, notifications and behaviour.

Managed Object Instance (MOI): an instance of a MOC, which is the same as an MO as described above.

Management Information Base (MIB): the set of existing managed objects in a management domain, together with their attributes, constitutes that management domain's MIB. The MIB may be distributed over several OS/NEs.

Management Information Model (MIM): Also referred to as NRM – see the definition below. There is a slight difference between the meaning of MIM and NRM – the term MIM is generic and can be used to denote any type of management model, while NRM denotes the model of the actual managed telecommunications network resources.

Network Element: is a discrete telecommunications entity, which can be, managed over a specific interface e.g. the RNC.

Network Manager (NM) : provides a package of end-user functions with the responsibility for the management of a network, mainly as supported by the EM(s) but it may also involve direct access to the network elements. All communication with the network is based on open and well-standardized interfaces supporting management of multi-vendor and multi-technology network elements.

Network Resource: is a component of a Network Element which can be identified as a discrete separate entity and is in an object oriented environment for the purpose of management represented by an abstract entity called Managed Object.

Network Resource Model (NRM): A model representing the actual managed telecommunications network resources that a System is providing through the subject IRP. An NRM describes managed object classes, their associations, attributes and operations. The NRM is also referred to as “MIM” (see above) which originates from the ITU-T TMN.

Object Management Group (OMG): see http://www.omg.org

Operations System (OS): indicates a generic management system, independent of its location level within the management hierarchy.

Operator: is either

- a human being controlling and managing the network; or,
- a company running a network (the 3G network operator)

Optimisation: of the network is each up-date or modification to improve the network handling and/or to enhance subscriber satisfaction. The aim is to maximise the performance of the system.

Re-configuration: is the re-arrangement of the parts, hardware and/or software that make up the 3G network. A re-configuration can be of the parts of a single NE or can be the re-arrangement of the NEs themselves, as the parts of the 3G network. A re-configuration may be triggered by a human operator or by the system itself.

Reversion: is a procedure by which a configuration, which existed before changes were made, is restored.

Software: is a term used in contrast to firmware to refer to all programs which can be loaded to and used in a particular system.

Up-Dates: generally consist of software, firmware, equipment and hardware, designed only to consolidate one or more modifications to counter-act errors. As such, they do not offer new facilities or features and only apply to existing NEs.

Up-Grades: can be of the following types:

- enhancement - the addition of new features or facilities to the 3G network;
- extension - the addition of replicas of existing entities.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CM	Configuration Management
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
EM	Element Manager
FM	Fault Management
FW	Firmware
HW	Hardware
MIB	Management Information Base
MIM	Management Information Model
MOC	Managed Object Class
MOI	Managed Object Instance
NE	Network Element
NM	Network Manager
NR	Network Resource
NRM	Network Resource Model
OMG	Object Management Group
OS	Operations System
OSF	Operations System Function
SW	Software
TRX	Transceiver
TS	Technical Specification
UML	Unified Modelling Language (OMG)

4 Network configuration management

4.1 General

In the development of a 3G network, three general phases can be described which represent different degrees of stability. Once the first stage is over, the system will cycle between the second and the third phases. This is known as the network life-cycle and includes:

1) the 3G network is installed and put into service;

2) the 3G network reaches certain stability and is only modified (dynamically) to satisfy short-term requirements. E.g. by (dynamic) re-configuration of resources or parameter modification; this stable state of a 3G network cannot be regarded as the final one because each equipment or SW modification will let the 3G network progress to an unstable state and require optimisation actions again;

3) the 3G network is being adjusted to meet the long-term requirements of the network operator and the customer, e.g. with regard to performance, capacity and customer satisfaction through the enhancement of the network or equipment up-grade.

During these phases, the operators will require adequate management functions to perform the necessary tasks.

4.1.1 Installing a 3G network

When a 3G network is installed and initialised for the first time, all NEs need to be introduced to the NM, the data for initialisation and SW for proper functioning need to be provided. All these actions are carried out to create NEs and to initialise them.

4.1.2 Operating a 3G network

Whilst in service, the operator needs to react to short term incidents such as traffic load requirements which are different from the current network capabilities, NEs/NRs need to be re-configured and parameters need to be adapted to follow these day-to-day requirements.

4.1.3 Growing/pruning a 3G network

As the 3G network grows and matures new equipment is installed and understanding of system behaviour increases. Subscriber requirements/wishes may demand that operators modify their system. In addition manufacturers improve the infrastructure components and add features to their products hence the operator will start modifying the 3G network to profit from these changes and to improve subscriber satisfaction. Additionally, the 3G network configuration will be modified (i.e. it will be up-dated or up-graded) to cope with a need for increasing or decreasing network capacity. These actions are carried out for the long term strategy of the operators to optimise the network.

4.1.3.1 System up-date

Whenever the 3G network needs to be improved for reasons of reducing failures, the system will be up-dated. In this case SW or equipment will be replaced without adding new functionalities or resources to the network. The basic function required is:

the modification of existing SW/equipment; it may be necessary to introduce a different set of data to cope with the modified SW/equipment.

For system up-date the network shall not be disturbed in its function until the required modification is activated. This requires mechanisms to

- do SW/data downloading in parallel with on-going traffic;
- isolate the affected NEs/NRs from traffic before the actual modification is done;

– minimise system outage due to the activation of up-dated components.

4.1.3.2 System up-grade

System up-grade may affect all areas of 3G network activities and can be described as enhancements, whereby either new features or new facilities are implemented. Also extensions, reductions or further replications of existing facilities are covered by this CM aspect. The CM functions employed are:

– Creation of NEs and/or NRs;

– Deletion of NEs and/or NRs; and,

– Modification of NEs and/or NRs.

The following requirements are to apply:

– to support expeditious handling of SW and data while minimising impact on ongoing traffic;

– to follow a required sequence of up-grades: e.g. the new SW depends upon the availability of the new equipment functionality;

– to provide the capability to create an additional logical NE/NR without having installed the physical resource supporting it: for example it should be possible to create a cell in an RNC without the physical equipment present or connected. However, additional mechanisms should be in place to prevent any service connection to any physically non-existent NE/NR or reporting failures from non-existing NE/NR;

– to provide the capability to install an additional physical NE/NR without creation of the logical resource managing it (no management functionality) and without impact of the current functionality;

– to provide the capability to prevent the erroneous taking into service of a NE/NR which is not fully installed and initialised: whenever a NE/NR is modified (extension or reduction) it shall be taken out of service until the logical part of the procedure is finished. An extended NE/NR cannot be placed into service until all needed parameters and equipment are initialised. Likewise, a reduced NE/NR cannot be placed back into service until the applicable re-configuration is performed.

When the network is up-graded by the addition of NEs or NRs or a change in the configuration, it is essential that the NE/NR can be restored to the configuration, which existed before the changes were made. This procedure is called "reversion" and is useful in maintaining service if any difficulty should arise from a network up-grade.

4.2 Operational context for configuration management

The CM functions available to the operator need to address various aspects beyond that which might strictly be regarded as management of the network. These include:

– assisting the operator in making the most timely and accurate changes thus avoiding lengthy waiting periods or complex scenarios;

– ensuring that CM actions will not have any secondary effects on the network other than the specified ones;

– providing mechanisms to protect the telecommunication-related traffic from effects due to CM actions - it shall be possible to inhibit traffic if a traffic affecting CM action is expected and to gracefully release calls prior to the closure of the resource;

– providing mechanisms to overcome data inconsistency problems by logging the modifications for reversion reasons, or to recover through data update from a second source.

4.2.1 Administrative aspects of configuration management

When managing the network by creating, deleting or modifying NEs/NRs, the operator should ensure that there is no uncontrolled impact on the network. The network management system therefore needs to support the following set of management functionalities when addressing various administrative aspects:

- Security;
- Data Validity;
- Data Consistency; and,
- Resource Administration.

4.2.1.1 Security aspects

It is ultimately up to the operator to ensure the network security by employing the appropriate mechanisms for control of logical and physical access.

Changes of the network configuration shall be possible only for operators with appropriate authorisation profiles.

4.2.1.2 Data validity

It is the responsibility of all management systems and NEs that data input to and transferred between the systems is valid given the particular management context.

4.2.1.3 Data consistency and distribution of the MIB

The Network Manager (NM) and Element Manager (EM) use different object model abstractions of the network's (NEs') physical and logical resources to be managed by these systems. This is the agreed Network Resource Model (NRM) between the NM and EM/NEs to be used at the N-interface and EM-NE interface (see ref. [2] for the definition of these interfaces). The NRM of the N-interface is fully standardized (see Annex E) while the NRM for the EM-NE interface is product-specific and is not standardized in this or related TSs. The NE local representation of those physical and logical instantiated resources to be managed, as well as their accurate mapping onto the agreed object model abstraction, is also product-specific. Thus the consistency between the actual local representation of physical and logical resources to be managed within an NE, and the corresponding view of the OS, relies on:

- which information is exchanged between the NE and the management systems; For the EM-NE interface this is defined in a product-specific NRM, where the actual network infrastructure is modelled. This is internal to a specific development organisation and does not need to be open; thus it is not further discussed in the present document. In fact, by publishing the management information portion of these interfaces, too much of the internal design will be revealed and it may become impossible or at least very expensive and time-consuming to later enhance the systems using the interface. For the N-interface between NM and EM/NE, the NRM as mentioned above is defined in Annex E.
- how such information is exchanged between NE and management systems - this is for the N-interface fully standardized by this and related documents, while for the EM-NE interface only the protocol is standardized (cf. fig. 2 in [2]).
- how information is locally represented and treated by an NE and by its associated (OSs); this is a product-specific choice of the manufacturers of NEs and OSs.
- where this information is kept; whether it is kept only at the "origin NEs" where the Managed Object Instances representing the managed NRs are created (NE-local MIB), or if also a copy of that information is kept in one or several of the OSs ("mirrored MIB"). This is again a product-specific choice of the manufacturers of NEs and OSs. If the "NE-local MIB" approach is chosen, the consistency "only" has to be maintained between the NEs, while if the "mirrored MIB" approach is chosen, the consistency has to maintained between the NEs as well as the NM/EM and the NEs.

A peer-to-peer data consistency between NM-EM and EM-NE does not guarantee overall data consistency from a network point of view. It is however possible for the NM to maintain consistency on the network level, as far as the information in the MIB for the N-interface is concerned, by comparing related information (MOIs and attributes) in all connected systems (EMs and NEs) in the managed network.

In order to promote data consistency, the following operational procedures are recommended:

– Awareness of autonomous NE re-configuration:

  local NE re-configuration, for example partial or full reversion mechanisms (either triggered autonomously or by an operator), should always be reported;

– Define appropriate audit procedures on the N- and EM-NE- interface to support MIB re-synchronisation:

  A. In case the "mirrored MIB" approach is chosen, take the following actions:

  1. The NM shall be able to retrieve all management information from the EM and NE accessible via the N-interface by applying appropriate data retrieval methods (periodically or on request);

  2. The NM shall after the retrieval compare the retrieved information with its own data and if necessary also compare related information between connected NEs (if the MIB stored in the NM already has been checked and found consistent, the latter step is not necessary);

  3. The NM shall report any deviations between the NE's view and the NM's view, and related NEs' views, to the operator;

  4. The NM shall automatically, or on operator command, after the check in step 2 above correct the deviating information in either the NM or the NEs (depending on whether the NEs or NM are regarded as "master" for the information; this is manufacturer dependent);

B. In case the "NE-local MIB" approach is chosen, take the following actions:

  1. The NM shall be able to retrieve all management information from the EM and NE accessible via the N-interface by applying appropriate data retrieval methods (periodically or on request);

  2. The NM shall after the retrieval compare the retrieved information between connected NEs;

  3. The NM shall report any deviations between the related NEs' views to the operator;

  4. The NM shall automatically, or on operator command, after the check in step 2 above correct the deviating information in the NEs;

– If the "mirrored MIB" approach is chosen, maintain the NM/EM view: As far as possible, operational concepts for data manipulation should employ the NM/EM as the only managing system for an NE. If however access to local NE data is given to maintenance personnel, the following actions are recommended/necessary in order to enable the NM/EM to maintain data consistency:

  – applying a remote OS terminal for the local access to the NE under consideration rather than directly modifying NE data without any control of the OS;

  – changes made locally shall be notified to the managing OS(s).

5 Configuration management service components

While a 3G network is first installed and brought into service, and following installation the 3G network operator will enhance and adapt the network to short and long term requirements. In addition, it will be optimised to satisfy customer needs. To cover these aspects of CM, the system will provide the operator with the following capabilities:

- initial system installation to establish the network;
- system operation to adapt the system to short term requirements;
- system up-date whenever it is necessary to modify the system to overcome SW bugs or equipment faults;
- system up-grade to enhance or extend the network by features or equipment respectively.

These capabilities are provided by the management system through its service components:

- system modification to change the network to meet the operators requirements;
- system monitoring to gain an overview on the present SW, equipment and data situation of the network.

The service components will be explained in more detail in the following subclauses.

5.1 System modification service component

Whenever it is necessary to adapt the system data to a new requirement due to optimisation or new network configurations, it will require an operator action to introduce new or modified data into the system. The data will be distributed to:

- either one EM/NE when dealing with a locally limited modification; or,
- each EM/NE concerned when the change affects multiple EM/NEs; and,
- the other NMs in the case where multiple NMs exist in the same management domain.

This implies the necessity of mechanisms to ensure data integrity and to maintain system data consistency (cf. section 4.2.1.3).

The concept of system modification includes the following aspects:

- if subscriber traffic impacting data modifications are performed, the NEs/NRs concerned are first cleared from traffic in a controlled way;
- the necessary modification is performed by the EM/NE;
- only once all needed data is given to the system, are the concerned NEs/NRs put back into traffic again;
- safeguards shall be available within the NEs to prevent changes to configuration affecting service(s) in use. In emergencies, it shall be possible to override these safeguards.

On occasion, modifications may not be stable or not fulfil the operator intentions. In these cases, reversion to the previous stable configuration may be necessary. Occasionally there will be changes to the network that create a new configuration, which cannot revert to any previous network status for protection. Such changes may involve major equipment modification to the core elements of the network or re-distribution of traffic across interconnected nodes to other Operators. In these cases it is necessary to implement the changes and to manage the consequences of any problems or failures without the protection of 'reversion', as equipment may have been removed or the work programme may be complex, time limited and expensive.

Progress of these changes should be sequential through an agreed milestone plan which includes effective tests to prove network functionality with only one action, or a coherent series of actions, completed at a time. The decision points, beyond which there is no return, should be clearly identified.

"Automatic re-configuration" shall not be dealt with in this document as it is dependent on the implementation. However, if an automatic re-configuration occurs, the operator shall be informed of the result.

5.2 System monitoring service component

The system monitoring service component provides the operator with the ability to receive reports (on request or spontaneously) on the configuration of the entire network or parts of it from managed NEs. These consist of structure, states, versions employed and data settings. Spontaneous reports are sent by the NE if there was an autonomous change of, for example, the states or other values due to fault management actions. Also, the NM may ask the managed EM/NE to send the information required to the NM at any time.

The data that shall be possible to provide on request is a subset of, or the whole, MIB, which is an instantiation of the NRM, defined in Annex E.

Any inconsistencies found during system monitoring by the NM should be reported to the operator, and it is left to the operator or an OSF to take appropriate actions.

6 Configuration management functions

6.1 System modification functions

The requirements of CM and their usage lead to basic CM functions to be defined for the network. These describe the required actions on managed elements (NEs or NRs) and the expected reactions. The system modification functions identified are:

- Creation of Network Elements and Resources;
- Deletion of Network Elements and Resources;
- Conditioning of Network Elements and Resources.

For all identified functions, the following major requirements apply:

- minimum disturbance of the network by taking the affected resources out of service if needed;
- physical modifications should be independent of the related logical modifications;
- all the required actions to satisfy a defined task should be completed correctly before the resources can be brought into service;
- data consistency checks shall be performed as described in subclause 4.2.1.3.

There are three aspects of NE and NR management, which can be distinguished:

1) Management of the physical aspect (equipment);
2) Management of the executable aspect (SW and FW); and,
3) Management of the logical/functional aspect (data).

All three management aspects are addressed by this TS.

6.1.1 Creation of network elements and network resources

The creation of a NE or NR is used to initially set up a 3G network or to extend an already existing network. The action of creation is a combination of installation, initialisation and introduction of the newly installed equipment to the network and to the OS, which will control it. The creation can affect equipment, SW and data.

Whenever a 3G network or parts of it are installed, the created NEs/NRs requires to be:

- physically installed and tested and initialised with a possible default configuration;
- logically installed by means of introduction to the network, possibly involving changes to related existing NE/NR configurations;
- allowed to be put into service.

The sequence of physical and logical installation may vary depending on the specific 3G network operator strategy. In case the logical creation takes place before the physical creation no related alarms shall be reported to the operator.

6.1.2 Deletion of network elements and network resources

If a network is found to be over-equipped, the operator may wish to reduce the scale of the network or to re-use the spare equipment elsewhere. This can occur when an operator over-estimates the traffic in one area and, for example, under-estimates the load in a different one.

The deletion of a NE or NR requires:

- taking the affected NEs or NRs out of service;
- logical removal from the network (possibly involving changes to other NE or NR configurations, for example, neighbour cell description);
- if necessary, the physical dismantling of the equipment;
- return of other affected NEs or NRs to service.

The sequence of logical and physical removal will not matter if the affected NEs are taken out of service prior to their removal. This will help to protect the network from error situations.

6.1.3 Conditioning of network elements and network resources

There are three categories of modifications to be regarded with respect to NEs or NRs. It is possible to either modify SW, equipment or data or a certain combination of them. Which aspects are affected by any particular modification is implementation dependent.

When an MO/NR is to be modified the following actions shall be performed:

- Locking or logical removal of the MO/NR (including first clearing it from traffic if necessary);
- Required modification (physical and/or logical); and,
- Unlocking or logical re-installation of the MO/NR.

This sequence is recommended to provide protection to the network against fault situations, which may occur during the modification process. By default, locking/modification/unlocking shall be the procedure to follow, and if logical removal/re-installation is necessary for a certain MO/NR, this shall be described in the NRM.

The result of conditioning should be able to be determined by the operator by employing the appropriate mechanisms provided through the System Monitoring functions (see clause 6.2).

A modification to data, which has a controlling influence on some resources, could influence the resource throughput or its capability to originate new traffic during the modification time. This distinction is made because, for particular modifications, the capacity of the NR can be decreased without influencing the ongoing traffic. Before deciding to perform an action, the operator should consider the effects that a modification might have on capacity, throughput and current activity of a resource.

6.1.3.1 Considerations on conditioning mechanisms

The data, which characterise a 3G network, will not all be subject to the same rate of change or need to be modified using the same mechanism. Changes to the logical configuration may also need to be applied across multiple NEs. These aspects are described in the following subclauses.

Whenever the configuration of the network requires modification, the following questions will be important to the operator:

- What will be the influence on the ongoing traffic?
- What will be the impact on the capacity of the network?
- How difficult and time-consuming will the modification procedure be?

The answer to these questions will give an idea as to when the modification can be best performed with the aim to keep traffic disturbance as low as possible and to require the modification process itself to cause as little disturbance as possible. On the other hand, it does not seem to be reasonable to invent a "low disturbance" modification algorithm for each single parameter, especially those, which are only modified once or twice during the lifetime of the network. These rare modifications could be performed with an acceptable level of interruption to traffic. Therefore, the system data elements may be classified by:

- modification once or twice during the life time of the system (e.g. protocol supervision timers);

- modification required seldom;
- modification is expected frequently and/or for a short term (telecom parameters).

Depending on this rating the requirements on the modification mechanism for certain data elements should vary.

6.1.3.2 Network traffic considerations

As stated previously, different types of modification mechanisms can be distinguished with regard to their impact on traffic and their extent:

For the impact regarding traffic, the following types can be identified:

- no impact on the traffic at all:
  the modified data values have no relation to the traffic capability;
- impact on traffic:
  the data modification causes for example a change in the volume of allowable traffic without affecting existing traffic.

For the impact regarding extent, the following types can be identified:

- Impact on only the NR or NE
  The modification of SW, equipment or data is effective for a NR, or a complete NE.
- Impact on more than one NE or different NRs of one NE
  Certain modifications on SW, equipment or data will require changes to be performed upon more than one NR in one NE or more than one NE. Such changes require consideration of data consistency, data integrity and network integrity. E.g. it should be distinguished between the NR directly affected by a modification and other impacted NRs. The relationships and dependencies between data values should be described and a mechanism defined to protect the system against inconsistency.

6.2 System monitoring functions

A major aspect of CM is the ability of the operator to monitor the operation of the network. This monitoring capability is necessary for the operator to determine the current operational state of the network as well as to determine the consistency of information among various NEs. The monitoring capability requires three functions to support it: the information request function, the information report function and the response/report control function.

6.2.1 Information request function

In order to support the operator's need to monitor the network, the NM needs to be able to gather information on request from the various EMs and/or NEs. The EM may then act as a mediator for one or more NEs (how this is done is product specific and outside the scope of this TS). The information request function should support the capabilities of the NM to be able to request information for any single attribute defined in the management information base. In addition, the NM should be able to gather large amounts of information in a single request by providing appropriate scope and filtering constructs in the request.

On receipt of a valid request, the addressed EM/NE shall respond with the current values of the specified data elements. This response will be immediate if so requested by the NM. However, in cases where very large amounts of data are concerned and where the EM and the NE support the capabilities, the NM may request the EM/NE to store the information in a file and transfer it using a file transfer mechanism.

In case there is a communication failure when a response is to be sent, the response shall be safely stored and forwarded as soon as possible after re-establishment of communication. An exception that may inhibit this type of delayed response, is if the transaction has timed out in the requesting NM.

6.2.2 Information report function

In addition to being able to provide information on request, the NE is required to have the capability of reporting notifications about changed/removed information autonomously. Generally this will be performed when some information on the state or operation of the system has changed. The following shall be supported:

- The following type of events shall be notified to the NM, if enabled by the NM (these three notification types may be enabled/disabled separately by the NM):

  1. Object creation/deletion;
  2. Attribute value change;
  3. State change;

- Optionally: The above mentioned notifications may be logged locally at the EM/NE. Logged notifications may be requested by the NM to be transferred from the EM/NE. Transfer mechanisms may be by file transfer or using messages;
- In case there is a communication failure when one or more notifications are to be forwarded, the notification(s) shall be safely stored and forwarded as soon as possible after re-establishment of communication.

6.2.3 Response/report control function

For responses to information requests and for information reports, it should be possible for the operator to specify where and when the information should go. The NM, EM and NE shall provide a capability to configure the response/reporting capabilities such that the following requirements are met at the N-interface:

– information forwarding shall be possible to be enabled and disabled;

– information shall be possible to be forwarded to the NM as soon as it is available;

– information shall be possible to be directed to any of various NMs (one or several);

7 N Interface

7.1 Configuration Management (CM) principles

The N (Network) interface (Itf-N; see ref. [2]) is an object oriented interface, i.e. all resources of the 3G network (functional and physical resources) are represented as Managed Object Instances (MOI) of a Network Resource Model (NRM).

Taking into account the required multi-vendor capability of the Itf-N, the related Network Resource Model may contain only functional object classes, which should provide the means for an efficient management on the network management level to the operator. Nevertheless, for the practical management of the network, also some equipment information shall be presented to the NM operator (e.g. for the purpose of fault management), some of which may be manufacturer specific. To fulfil this requirement, some generic functional object classes (which model the network resources in a generic way) are needed, which provide, e.g. by means of dedicated attributes, the required manufacturer-specific information towards the superior NM. That is, some of the attributes are standardised while the values (e.g. "board name") are manufacturer-specific.

The definition of the Network Resource Model for the Itf-N (connecting the NM with a "subordinate entity", which may be an EM or a NE) is described in Annex E, which defines the Basic CM IRP Information Model including the NRM applicable to UMTS management.

This clause describes the specific functional requirements related to Configuration Management of network resources on the Itf-N, which may be classified in two main groups:

- *Passive* CM (configuration overview), which mainly provides to the NM current information about the current configuration changes and allows a retrieval and synchronisation of configuration-related data on NM request.

  The forwarding of these notifications over the Itf-N is controlled by means of configuring adequate filtering mechanisms within the subordinate entities. The N interface also provides the means for storage ("logging") and later retrieval of desired information within the subordinate entities.

- *Active* CM, which offers to the NM operator a real capability to change the current network configuration.

7.2 Overview of IRPs related to configuration management

The N interface for Configuration Management is built up by a number of Integration Reference Points (IRPs) and a related Name Convention, which realises the functional capabilities over this interface. The basic structure of the IRPs is defined in [1] and [2]. For CM a number of general IRPs (and the Name Convention) are defined herein, used by this as well as other technical specifications for telecom management produced by 3GPP. All these documents defined within the scope of this technical specification are included in annexes to this specification as follows:

Notification IRP Information Service: Annex B

Notification IRP CORBA Solution Set: Annex C

Notification IRP CMIP Solution Set: Annex D

Basic Configuration Management IRP Information Model (including NRM): Annex E

Basic Configuration Management IRP CORBA Solution Set: Annex F

Basic Configuration Management IRP CMIP Solution Set: Annex G

Name Convention for Managed Objects: Annex H

7.3 Passive Configuration Management

7.3.1 Real-time forwarding of CM-related event reports

During normal operation the NM is continuously informed by the managed subordinate entities about all network configuration changes, in accordance with the Network Resource Model applied on the N interface. For this purpose the following CM-related event reports with regard to the ITU-T X.721, X.730 and X.731 standards are forwarded to the NM:

- Object creation
- Object deletion
- Attribute value change
- State change.

The real-time forwarding of these event reports occurs via appropriate filtering mechanisms ("discriminators" on CMIP interfaces, “subscription” on CORBA interfaces) located in the subordinate entity in accordance with ITU-T X.734 or OMG event/notification service. These filters may be controlled (i.e. created, modified and eventually deleted) locally in the subordinate entities or remotely by the NM (via the N interface) in order to ensure that only the event reports which fulfil pre-defined criteria can reach the superior NM. In a multiple manager environment each NM may have its own filtering mechanism within every subordinate entity which is able to generate CM-related notifications.

It shall be possible to pack multiple events into one notification/event report. This provides more efficient use of data communication resources, and reduces the delay in notifying all NMs of a potentially large sequence of events. In order to pack multiple event information records into one notification, the System defines the maximum number of events in the notification. A system configurable parameter shall specify the maximum time delay for the events before they have to be sent.

Note: In this release the real-time forwarding of event reports may not be provided by all solution sets.

7.3.3 Retrieval/synchronisation of CM-related information on NM request

As long as the network is in operation and fault free, the update of the CM-related information on NM level is continuously ensured by the real-time forwarding of concerned reports as described in subclause 7.3.1. In case of faults (either on the NM or in a subordinate entity or on the communication link) it is possible that some CM-related event reports are lost. Therefore the CM-related information on the NM may become non-aligned with the real configuration of the network (depending on the strategy of the NM where to store network configuration information). In this case a synchronisation process may be necessary to align the CM-related information of the NM with the configuration information of the subordinate entities.

The retrieval or synchronisation ("alignment") of network configuration information between the NM and one or more of its subordinate entities can be triggered at any time by the NM.

There are two different alternatives for this synchronisation:

- via a read command with appropriate filtering
- as an ordered sequence of CM-related event reports

7.4 Active Configuration Management

In this release of the 3G-management standard, it is assumed that active configuration management is a task that can be performed only by the Element Managers and/or local maintenance terminal actions. Thus it is outside the scope of this specification.

Annex A (informative): Change history

Meet	TSG-SA document	TSG-SA5 document	CR	Rev	Rel	Cat	Subject	Resulting Version
			-		R99			

Annex B (normative): Notification Integration Reference Point: Information Service

B1 Introduction

B1.1 Background

The need to support and automate end-to-end processes clearly requires telecom management applications and systems to be interoperable. The technical enablers for achieving this interoperability are here referred to as Integration Reference Points (IRPs), reflecting their use for a Communications Provider in the following fields:

1. Accessing the network infrastructure
2. Achieving interoperability between internal management applications and systems (within and between application areas)
3. Achieving interoperability with external management systems, corresponding to business relations with other Communications Providers
4. Providing access to customers (end-users)

The IRPs are introduced to ensure interoperability between product-specific and generic applications. These IRPs are considered to cover the most basic needs of task automation.

Relating to the OSI management functional areas “FCAPS”, IRPs address parts of “FCPS” – Fault, Configuration, Performance, and Security management. Comparing with TMF TOM (Telecom Operations Map), the introduced IRPs address process interfaces at the EML-NML (Element Management Layer – Network Management Layer) boundary. In 3GPP/SA5 context, this can also be applied to the “Itf-N” between EM-NM and NE-NM.

The three cornerstones of the IRP concept are:

1. **Top-down, process-driven modelling approach**
   The purpose of each IRP is automation of one specific task, related to TMF TOM. This allows taking a "one step at a time" approach with a focus on the most important tasks.
2. **Protocol-independent modelling**
   Each IRP consists of a protocol-independent model (the IRP Information Model) and several protocol-dependent models (IRP Solution Sets).
3. **Standard-based, protocol-dependent models**
   Models in different IRP solution sets (CORBA, CMIP, SNMP,...) will be different as existing standard models of the corresponding protocol environment need to be considered. This means that solution sets largely need to be "hand crafted".

B1.2 Scope

This document defines the Notification IRP Information Model .

Network elements (NEs) under management generate events to inform event receivers about occurrences within the network that may be of interest to event receivers. There are a number of categories of events. Alarm, as specified in Alarm IRP: Information Model [2], is one member of this category.

The purpose of Notification IRP is to define an interface through which an Actor (typically a network management system) can subscribe to System (typically a NE manager (EM) or a NE) for receiving network events. It also specifies

attributes carried in the network events. These attributes are common among all event categories. Attributes that are specific to a particular event category are not part of this specification. For example, `perceivedSeverity` is an attribute specific for alarm event category. This attribute is not defined here but in Alarm IRP [2].

B1.3 Key Terms

This section lists key terms used in this document.

Actor: It models all kinds of objects outside the domain of the *System* and it interacts directly with the System using this IRP. Since Actors represent System users, they help delimit the System and give a clearer picture of what System is supposed to do.

Event: It is an occurrence that is of significance to network operators, the network elements under surveillance and network management applications. Events can indicate many types of network management information, such as network alarms, network configuration change information and network performance data.

Notification: It refers to the transport of events from event producer to consumer. In this IRP, Notification is used to carry network events from System to Actor. Producer sends Notifications to consumers as soon as there are new events occur. Consumer does not need to pull for events.

Notification Identifier: It provides an identifier for the notification, which may be carried in the Correlated Notifications parameter (see below) of future notifications. Notification identifiers shall be chosen to be unique across all notifications of a particular managed object throughout the time that correlation is significant. Notification carries this identifier in an optional parameter called `otificationId`.

It may be reused if there is no requirement that the previous notification using that Notification identifier be correlated with future notifications. Generally, System should choose it to ensure uniqueness over as long a time as is feasible for the managed system.

Correlated Notifications: It contains a set of Notification identifiers; the distinguished names of their associated managed object instances and the distinguished names of the Systems that emit the original Notifications. Notifications in this set are correlated to the subject Notification. Notification carries this in an optional parameter called `Correlated_Notifications`. The algorithm by which correlation is accomplished is outside the scope of this IRP.

System: It models the object that interacts with Actor using this IRP. For this document, System encapsulates network element functions regarding network event detection and reporting. From Actor's perspective, System behaviour is only visible via this IRP.

B1.4 Glossary

CORBA	Common Object Request Broker Architecture
IDL	Interface Definition Language
IRP	Integration Reference Point
NE	Network Element
NM	Network Manager
EM	Element Manager
ITU-T	International Telecommunication Union, Telecommunication Sector
OMG	Object Management Group
SNMP	Simple Network Management Protocol

B2 System Overview

B2.1 System context for Notification

The following figures identify system contexts of Notification IRP in terms of implementations called System and Actor.

"Actor" depicts a process that interacts with System for the purpose of receiving network Notifications via this IRP. System detects network events. System sends Actors Notifications carrying the events. Examples of Actors can be a network Notification logging device or network Notification viewing devices (such as a local craft terminal). System implements and supports this IRP. System can be one Network Element (NE) (see Figure 1) or it can be one NE Manager (EM) with one or more NEs (see Figure 2). In the latter case, the interfaces (represented by a thick dotted line) between the EM and the NEs are not subject of this IRP. Whether EM and NE share the same hardware system is not relevant to this IRP either. By observing the interaction across the IRP, one cannot deduce if EM and NE are integrated in a single system or if they run in separate systems.

For the case when Actor only interacts with the EM and not the NE, this IRP defines a third system context including a second interface (see Figure 3). In this interface the Actor interacts only with an EM. This can be used when the Actor is not allowed to interact with the NE, but only is allowed to access information from the NE. Actor could typically be an NM.

Figure 1: System Context A

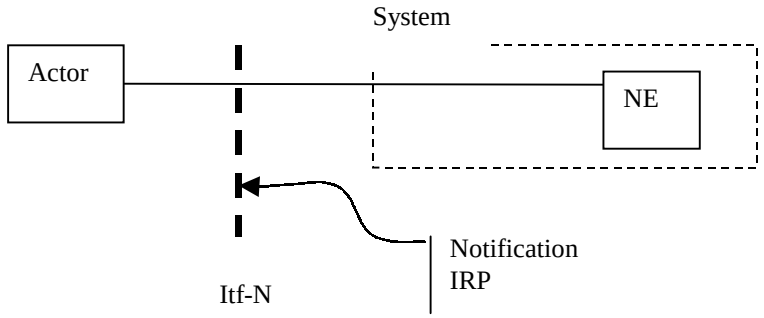


Figure 2: System Context B

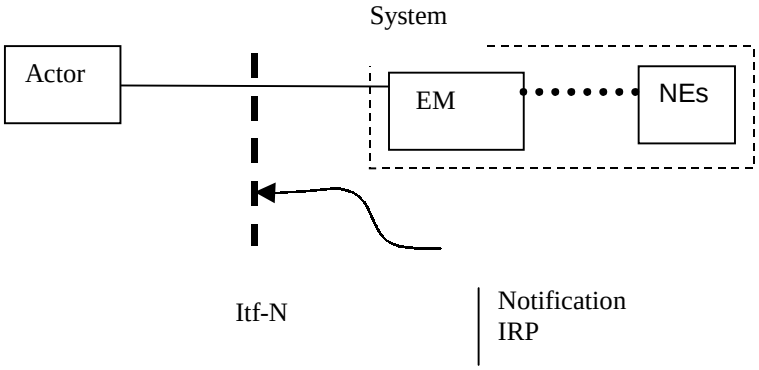
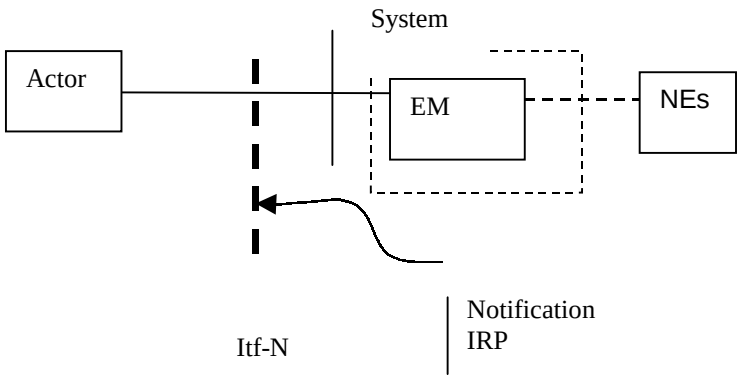


Figure 3: System Context C



This interface supports the following implementation strategies.

- One System supports emission of different categories of Notifications, such as alarms (as specified in [2]) and others.
- One Systems supports emission of one specific category of Notification. For example, one System implementation only emits alarms specified in [2]. Another System implementation emits configuration status change Notifications.
- Actor can specify the categories of Notifications it wants to receive using `subscribe`() operation. In the case Actor does not specify the Notification category in `subscribe`(), System will then emit all categories of Notifications that System handles. This implementation is solution set dependent.
- Actor can query the categories of Notification that System is emitting. This implementation is solution set dependent.

The Notification IRP defines attributes, carried in Notifications that are common in all categories of Notifications. Attributes specific to a particular category of Notification shall be specified in corresponding IRP (such as Alarm IRP). Those IRP also defines the protocol interaction via which Actor receives the Notifications.

B3 Modelling Approach

This section identifies the modelling approach adopted and used in this IRP.

This IRP bases its design on work captured in ITU-T Recommendation X.734 [4], OMG Notification Service [7] and IETF RFC-2573 [8]. The central design ideas are:

- Separation of Notification Consumers from producers;
- Notifications are forwarded from producers to consumers in a store and forward manner; and
- Notifications are pushed to consumers without the need for consumers to periodically pull for new Notifications.
- Common characteristics related to notifications in all other IRPs are gathered in one IRP (this document).

B4 IRP Information Model

This clause defines this IRP Information Model in the form of an Interface Model and a Dynamic Model.

B4.1 Interface Model

This section defines the interface model supporting this IRP. This model is protocol environment neutral.

Operations, *Notifications*, *parameters* (of operation and Notification) and *attributes* (of event record) defined in this section are qualified by *mandatory* (M) and *optional* (O).

The meaning of *mandatory* in IRP Information Model is that the subject shall be present in all solution sets as mandatory. The meaning of *optional* in IRP Information Model is that the subject shall be present in all solution sets if it is technically possible. When it is present, it shall be optional.

The following defines the meaning of mandatory and optional operations in solution sets.

- System shall implement all mandatory operations. System may implement optional operation. Actor may use any operation.
- Actor shall implement all mandatory and optional Notifications. System shall use all mandatory Notifications. System may use any optional Notification.

The following defines the meaning of mandatory and optional parameters of operation and Notification in solution sets.

- Method (operation and Notification) implementation shall support all mandatory parameters. They may support optional parameters. Method caller shall use mandatory parameters in calls. Method caller may use optional parameters in calls.

The following defines the meaning of mandatory and optional attributes in event record in solution sets.

- Actor shall support all mandatory and optional attributes. System shall support all mandatory attributes. It may support optional attribute.

The solution set may specify capability via which Actor can discover if System has implemented an optional operation or parameter.

This model does not specify if an operation or Notification is asynchronous or synchronous, blocked or unblocked, direct call or store-and-forward call-type. This type (and other types) of call semantics shall be defined in each solution set.

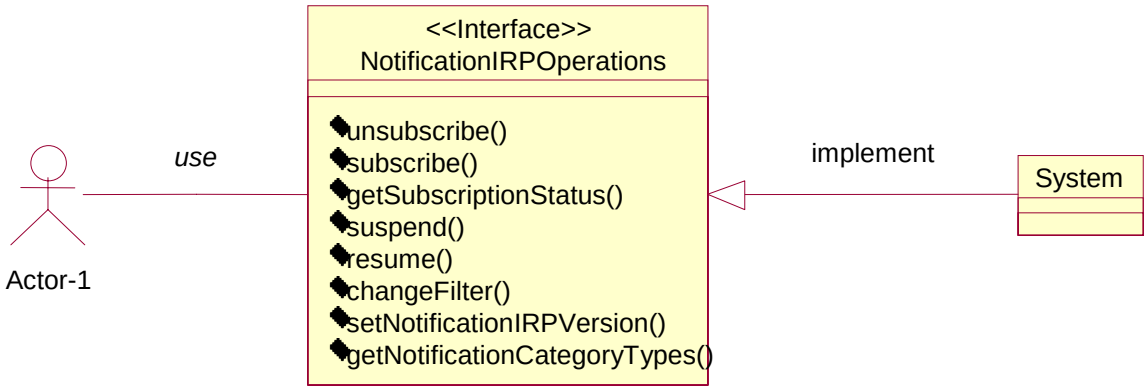
B4.1.1 Interface Class Diagram

The following figure illustrates the operations and Notifications defined as interfaces[1] implemented and used by System and Actor. Parameters and return status are not indicated.

One interface, called `NotificationIRPOperations`, is defined. This interface defines operations implemented by System and used (or called by) Actor.

Figure 4: Protocol Independent interface for Notification IRP

[1] Interface in IRP Information Model is identical to concepts conveyed by stereotype <<interface>> of Rational Rose Model.



B4.1.2 Interface Description

B4.1.2.1 Operations of `NotificationIRPOperations`

B4.1.2.1.1 Operation `subscribe (M)`

Actor invokes this operation to establish subscription to receive network events via Notifications. How Actor discovers the System's address or reference (so that Actor can invoke this operation) is outside the scope of this document. This operation is mandatory.

Table 1: Parameters of `subscribe`

Name	Qualifier	Purpose
`ActorReference`	Input, M	It specifies the address of `NotificationIRPNotifications` (0) against which System shall send events.
`Notification CategoryTypes`	Input, O	It identifies the kinds of Notifications wanted by Actor. Kinds of Notifications can be that defined by IRPs such as Alarm IRP [2], etc. Kinds of Notifications can be others, not defined by any IRPs, as well. Valid values for this parameter are solution set dependent. Each solution set shall define, at the minimum, legal values for all IRP Notification categories. Each solution set may specify values for Notifications not specified by IRP as well. If this parameter is absent or its value is NULL, then the meaning is that Actor wants all kinds of Notification emitted by System.
`Filter`	Input, O	It specifies a filter constraint that System shall use to filter network events of a particular Notification category. System shall notify Actors of an event only if the event satisfies the filter constraint. If this parameter is absent or its value is NULL, then it means that no filter constraint shall be applied. Valid filter constraint grammars are specified by individual Notification IRP solution set, e.g. Notification IRP: CORBA solution set.

SubscriptionId	Output, M	It holds a unique identity of the subscription managed by System.
SystemReference	Output, O	System can return this reference to Actor so that Actor can invoke operations against it to manage events. Operation examples are for Actor to request System to suspend and resume event Notification.
Status	Output, M	(a) Operation succeeded in that the requested subscription has been established successfully AND that System is emitting kinds of Notification specified by Actor via the NotificationCategoryTypes parameter AND that the filter, if present, contains a valid filter constraint including NULL or (b) Operation failed because of specified or unspecified reason.

B4.1.2.1.2 Operation unsubscribe (M)

Actor invokes this operation to cancel subscription. Actor shall supply the subscriptionId assigned by System in the corresponding operation subscribe. This operation is mandatory.

Table 2: Parameters for unsubscribe

Name	Qualifier	Purpose
SubscriptionId	Input, M	It carries the subscriptionId carried as the OUT parameter in the subscribe operation.
Status	Output, M	(a) Operation succeeded in that subscription is cancelled successfully or (b) Operation failed because of specified or unspecified reason.

B4.1.2.1.3 Operation setNotificationIRPVersion (M)

Actor wishes to communicate with System using a particular Notification IRP solution set version. System shall respond with operation unsuccessful in case System does not support the requested version. In this case, System shall return with a list of (one or more) version numbers currently supported by System. System shall respond with operation successful in case System supports the requested version. In this case, System shall not return to Actor with a list of version number currently supported by System. This operation is mandatory.

Table 3: Parameters for setNotificationIRPVersion

Name	Qualifier	Purpose
VersionNumber	Input, M	It indicates the Notification IRP solution set version number supported by Actor.
VersionNumberList	Output, M	It indicates one or more solution set version numbers supported by the System. This value should be NULL if status is successful, indicating that System is accepting the version number provided by Actor.

Status	Output, M	(a) Operation succeeded in that System is supporting the solution set version indicated in the input parameter. In this case, the output parameter versionNumberList shall be NULL. (b) Operation failed in that the System is not supporting the solution set version indicated in the input parameter. In this case, the output parameter versionNumberList shall contain one or more solution set version numbers currently supported by the System.

B4.1.2.1.4 Operation getSubscriptionStatus (M)

Actor invokes this operation to verify if System has lost the Actor's reference and as a consequence, the System is not able to send information specified under NotificationIRPNotifications to the Actor.

Table 4: Parameters for getSubscriptionStatus

Name	Qualifier	Purpose
SubscriptionId	Input, M	It carries the subscriptionId carried as the OUT parameter in the subscribe operation.
Notification CategoryTypes	Output, M	It identifies the kinds of Notifications emitted by System towards the subject Actor. If this parameter is absent or its value is NULL, then the meaning is that System is not emitting any Notification to the subject Actor.
FilterInEffect	Output, M	It contains the filter constraint currently active. If it contains a NULL string, it means that there is no filter constraint applied to Notification emitted towards the subject Actor.
Subscription Status	Output, M	(a) System has knowledge of the subscriptionId or (b) System has no knowledge of the subscriptionId.

B4.1.2.1.5 Operation changeFilter (O)

Actor invokes this operation to replace the present filter constraint with a new one.

Table 5: Parameters for changeFilter

Name	Qualifier	Purpose
SystemReference	Input, M	It carries the same value as the SystemReference in OUT parameter of subscribe().
Filter	Output, M	See description of Table 1: Parameters of subscribe.
Status	Output, M	(a) Operation succeeded in that System is now producing events based on the new filter constrain or (b) Operation failed in that, for unspecified reason, the new filter constraint cannot be installed. The old filter constraint, if present before this operation, is still in effect. An example of failure is that Actor uses subscribe() operation and not subscribe_b() operation.

B4.1.2.1.6 Operation suspend (0)

Actor invokes this operation to request System to stop emission of events.

Table 6: Parameters for `suspend`

Name	Qualifier	Purpose
`SystemReference`	Input, M	It carries the same value as the `SystemReference` in OUT parameter of `subscribe`().
`Status`	Output, M	(a) Operation succeeded in that System has suspended emission of events or (b) Operation failed in that, for unspecified reason, System has not suspended emission of events. An example of failure is that Actor uses `subscribe`() operation and not `subscribe_b`() operation.

B4.1.2.1.7 Operation resume (0)

Actor invokes this operation to request System to resume emission events.

Table 7: Parameters for `resume`

Name	Qualifier	Purpose
`SystemReference`	Input, M	It carries the same value as the `SystemReference` in OUT parameter of `subscribe`().
`Status`	Output, M	(a) Operation succeeded in that System is has resumed emission of events or (b) Operation failed in that, for unspecified reason, System cannot resume emission of events. An example of failure is that Actor uses `subscribe`() operation and not `subscribe_b`() operation.

B4.1.2.1.8 Operation getNotificationCategoryTypes (0)

Actor invokes this operation to query the categories of Notification emitted by System.

Table 8: Parameters for `getNotificationCategoryTypes`

Name	Qualifier	Purpose
`Notification CategoryTypes`	Output, M	It identifies the kinds of Notifications emitted by System. Kinds of Notifications can be that defined by IRPs such as Alarm IRP [2], etc. Kinds of Notifications can be others, not defined by any IRPs, as well. Valid values for this parameter are solution set dependent. Each solution set shall define, at the minimum, legal values for all IRP Notification categories. Each solution set may specify values for Notifications not specified by IRP as well. If this parameter is absent or its value is NULL, then the meaning is that System is not emitter of any kind of Notification at the moment.

Status	Output, M	(a) Operation succeeded in that the output parameter contains valid information or (b) Operation failed in that the output parameter does not contain valid information.

B4.1.3 Behaviour

B4.1.3.1 System Supports Multiple Subscriptions from Actor

An Actor can invoke multiple subscriptions (i.e., invoke subscribe() operation using different references). As far as System is concerned, the System is sending alarms to multiple "places".

If Actor invokes multiple subscriptions with identical reference, all but the first subscription shall fail with exception indicating that the Actor is already in subscription.

System may return a reference (the optional OUT parameter called systemReference in subscribe()). If so, Actor can invoke operations such as changeFilter(), suspend() against this reference. If System does not return the systemReference, then Actor cannot suspend System from sending Notifications. Actor cannot change filter as well. In such case, if the filter requirement changes, Actor shall invoke unsubscribe() and then subscribe() with a new filter constraint reflecting the new filter requirement.

Actor does not have the concept of filter object. Actor controls the filter constraint via subscribe() operations. Actor cannot know if System has created one or multiple filter objects (linked in series) to satisfy the filter constraint expressed in the subscribe() operation.

B4.1.3.2 System Supports Emission of Multiple Types of Notifications

System of this IRP may emit multiple categories of Notifications. For example, it may emit Notification defined in Alarm IRP [2]. System supports mechanism that Actor can use to determine the types of Notifications emitted by System. System also supports mechanism that Actor can use to specify the categories of Notifications System should emit to Actor during subscription.

B4.1.3.3 Event Attributes

Network events are carried in EventRecord that contains multiple attributes. This IRP specifies attributes that will appear in all EventRecord in all IRPs. They are mandatory. Other attributes are specified in IRPs such as Alarm IRP [2], etc. Whether they are mandatory or not are also specified in those IRPs.

B4.1.3.3.1 NotificationId (M)

This parameter, when present, provides an identifier for the notification, which may be carried in the correlated_notifications parameter (see below) of future notifications. NotificationId shall be chosen to be unique across all notifications of a particular managed object throughout the time that correlation is significant.

A NotificationId may be reused if there is no requirement that the previous notification using that NotificationId be correlated with future notifications. Generally, NotificationIds should be chosen to ensure uniqueness over as long a time as is feasible for the managed system.

It uniquely identifies this Notification from other Notifications emitted from the System. System emitting the Notification assigns its value.

If Actor receives Notifications from multiple Systems and needs to identify uniquely all Notifications received, then Actor shall use this identification, together with systemDN, for unique identification.

In case a network event is carried by multiple Notifications across multiple Notification IRPs arranged in tandem, the NotificationId appearing in all Notifications shall have identical values.

If and when the value of this can be re-used is specified in solution sets.

B4.1.3.3.2 Correlated_Notifications (O)

This parameter, when present, contains a set of the following set of information:

- Notification identifier;
- Distinguished name of the managed object instance associated with the Notification identified by the above identifier; and
- Distinguished name of the System that emits the Notification identified by the above identifier.

Notifications in this set are correlated to the subject Notification. The algorithm by which correlation is accomplished is outside the scope of this IRP.

B4.1.3.3.3 EventTime (M)

It indicates the event occurrence time. The time indication is UTC (Co-ordinated Universal Time). The Bureau Internationale De l'Heure (International Time Bureau) maintains UTC time scale and it forms the basis of a co-ordinated dissemination of standard frequencies and time signals. The source of this definition is Recommendation 460-2 of the Consultative Committee on International Radio (CCIR). CCIR has also defined the acronym for Co-ordinated Universal Time as UTC. UTC is also referred to as Greenwich Mean Time (GMT) and appropriate time signals are regularly broadcast.

The time indicates the year month, day, hour, minute and second.

B4.1.3.3.4 SystemDN (M)

SystemDN carries the Distinguished Name (DN) of System that detects the network event and generates the Notification. See [5] for name convention regarding DN.

If Notification IRP is arranged in tandem, the SystemDN appearing on the Notification across IRP reflects the system's DN of the first System that detects the network event and originates the Notification. Referring to the following figure, the SystemDN of the Notifications across NotificationIRP-1 and NotificationIRP-2 carry DN of Entity-C.

Figure 5: Use of systemDN

Entity-A < - - - - - - - **NotificationIRP-1** - - - - - **Entity-B** < - - - - - **NotificationIRP-2** - - - - **Entity-C**

B4.1.3.3.5 EventType (M)

It carries identification of event types carried in the Notification. Event types are specific to a particular Notification category. For example, for Notification category of Alarm IRP [2], the event types may be communication alarm, environmental alarm, equipment alarm, integrity violation, operational violation etc. See corresponding IRP document, such as Alarm IRP: Information Model [2], for a listing of possible event types for that Notification category.

The following values of EventType are currently reserved for different IRPs:

0..100: Reserved for Alarm IRP [2].

B4.1.3.4 Subscription list loss

System can lose the list of ActorReference that identifies current Actors under subscription. Under this condition, System is incapable of sending events to the affected subscriber(s).

This Notification IRP recommends that Actor should invoke the getSubscriptionStatus operation periodically to confirm that System still has the Actor's reference in its list. In case Actor does not obtain a positive confirmation, Actor should assume that System has lost the Actor's reference. In this case, Actor should invoke unsubscribe and then subscribe operation again.

This IRP does not recommend the frequency Actor should use to invoke `getSubscriptionStatus` operation.

B4.2 Dynamic Model

B4.2.1 Use Cases

B4.2.1.1 Actor subscribes to receive events

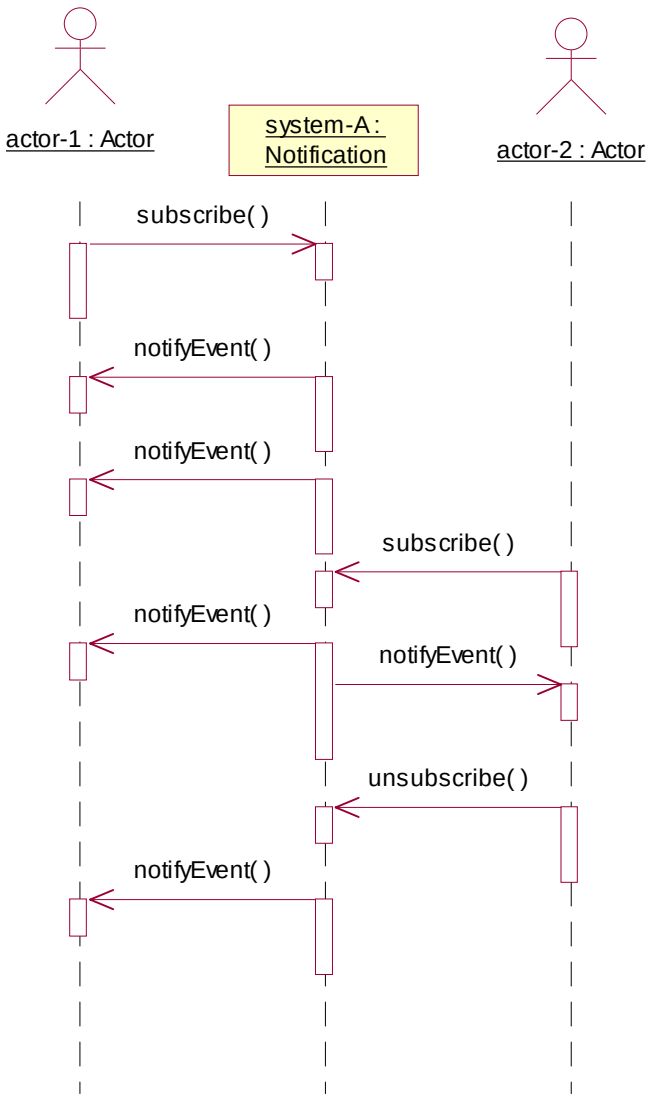
Name: Actor subscribes to receive events

Summary: This use case illustrates the interactions for actors to subscribe for events.

Pre-conditions: Actor knows the address of System.

Post-conditions: None.

Figure 6: Interaction diagram for Actor subscription to events



B4.2.1.2 Actor performs Heartbeat

Name: Actor performs heartbeat.

Summary: This use case allows Actor to confirm if System is functioning, regarding emission of events, or otherwise.

Pre-conditions: Actor knows the System's address.

Begins when: System issues `getSubscriptionStatus` operation.

Ends when: Operation completes.

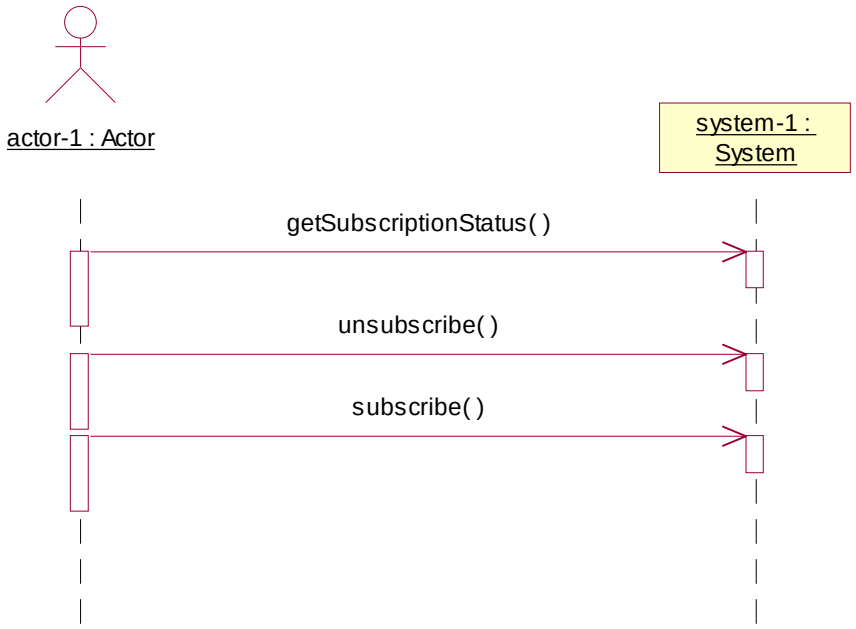
Post-conditions: None.

The following figure illustrates the scenario when System responds negatively to the operation, indicating that it is not functioning correctly as far as emitting events to the invoking Actor. Most probably, the System has lost the Actor's subscription reference. In such case, Actor is recommended to invoke `unsubscribe` and `subscribe` operations as illustrated.

In such a scenario, Actor shall assume that some events may have been lost. How Actor can recover the lost is outside the scope of this IRP. The recovery mechanism, if any, will be specified in IRPs (e.g., Alarm IRP) that refer to this IRP.

Actor should periodically invoke this operation to confirm if System is still functioning well.

Figure 7: Interaction diagram for Heartbeat



B5 Issues discussed & possible future enhancements

This section provides issues discussed and the resulting comments/recommendations.

- Via this IRP, Actor can request System to suspend and resume the emission of events. This is an optional capability. Offering of such capability in CORBA solution set may pose security problem.
- A System capability whereby Actor can create, delete and modify profiles that capture the requirement of Notification emission (in terms of categories of Notification requirements such as Alarm IRP, Performance IRP and

filter constraint requirements) has been considered but not included in this document. In the current document, System does not maintain profiles. Actor maintains its profiles. When Actor invokes `subscribe` operation, Actor provides System with the Notification category and the filter constraint applicable to the category. For example, Actor indicates that it wants Notification relevant to Alarm IRP and in addition, wants only Notification that carries alarm record whose `perceivedSeverity` is `CRITICAL`. System behaves accordingly.

Further enhancement to this IRP may be of interest in future versions. Enhancement can be realized in several forms, such as class inheritance or aggregation. The enhancements are not part of this IRP. They could be included in future versions of this IRP if there is a common interest.

The following are examples:

- Add capability for Actor to specify the QoS (e.g., guarantee reliability of delivery).
- Add capability for System to maintain subscription profiles (as mentioned above).
- The provisioning of a logging capability by System is not included in this document. OMG standardization on this capability took more time than anticipated. It is expected that by 4Q-99, the Telecommunication Log will become an OMG standard. There is also an IETF draft called “Notification Log MIB” for consideration. By 4Q-99, a log capability could be included in this IRP. Please note that this does not mean that this logging capability shall only be supported by a CORBA Solution Set, but it's an important cornerstone that should be considered.

B6 References

1. Intentionally left blank

2. Alarm IRP: Information Model[2]

3. Intentionally left blank

4. ITU-T Recommendation X.734 (09/92) - Information technology - Open Systems Interconnection - Systems management: Event report management function

5. Name Convention for Managed Objects[3]

6. Performance Data IRP: Information Model[4]

7. OMG Notification Service, Joint Revised Submission (state frozen - only fault corrections allowed).

8. RFC-2573, SNMP Applications

2 See Tdoc S5-99302

3 See Tdoc S5-99189

4 See Tdoc S5-99234

Annex C (normative):

Notification IRP: CORBA Solution Set

<To be provided>

Annex D (normative):

Notification IRP: CMIP Solution Set

<To be provided>

Annex E (normative):

Basic Configuration Management IRP: Information Model

<To be provided>

Annex F (normative):

Basic Configuration Management IRP: CORBA Solution Set

<To be provided>

Annex G (normative):

Basic Configuration Management IRP: CMIP Solution Set

<To be provided>

Annex H (normative): Name Convention for Managed Objects

H1 Introduction

H1.1 Background

The need to support and automate end-to-end processes clearly requires telecom management applications and systems to be interoperable. The technical enablers for achieving this interoperability are here referred to as Integration Reference Points (IRPs), reflecting their use for a Communications Provider in the following fields:

1. Accessing the network infrastructure
2. Achieving interoperability between internal management applications and systems (within and between application areas)
3. Achieving interoperability with external management systems, corresponding to business relations with other Communications Providers
4. Providing access to customers (end-users)

The IRPs are introduced to ensure interoperability between product-specific and generic applications. These IRPs are considered to cover the most basic needs of task automation.

The detailed IRP specifications are divided into two main parts, following to the directives from TMF's SMART TMN:

- The Management Information Service (MIS) for an Actor to access and/or manipulate information on Managed Objects maintained by a System, and a Base Management Information Model (MIM), specified with a protocol neutral modelling language. The Unified Modelling Language (UML) has been selected, as it is standardised (by the OMG), supported by most OO tools and used in several ongoing standardisation efforts (EEI, CIM, etc.).
- Solution Sets, i.e. mappings of the information models to one or several technologies (CORBA/IDL, SNMP/SMI, CMIP/GDMO, COM/IDL, etc.). Different technology selections may be done for different IRPs.

H1.2 Scope

To perform network management tasks, co-operating applications require identical interpretation of names assigned to network resources under management. Such names are required to be unambiguous as well. This document recommends one name convention for network resources under management in the IRP context.

We believe wide deployment of this name convention is necessary to facilitate interworking among distributive management applications. We strongly encourage developers of directory-enabled products, directory clients, network elements, network element managers and user interfaces, to assume that this naming convention will see widespread use and design their products accordingly.

IETF has specified a Distinguished Name string representation in RFC 2253 [7]. A Distinguished Name string representation using the subject name convention is also a valid Distinguished Name string according this RFC. The subject name convention imposes further restrictions as compared to the RFC. The most important restrictions are:

- Multi-valued RDN[1] is not supported in the subject name convention
- Character escape mechanism is not supported in the subject name convention

[1] RDN stands for Relative Distinguished Name (see 0). Multi-value RDN is a concept of X.500 (see reference [2]).

- Character star ('*', ASCII 42) is used to denote wildcard in the subject name convention.

H1.2.1 Current problems

At present, multiple name conventions are used by different vendors' network elements (NEs), or even within the same vendor, to name network resources. Following problems arise:

- Different classes of NE use different name conventions. Network Management applications, when interfacing with these NEs, are required to understand multiple name conventions to manage the NEs.
- Network management applications (e.g., fault management application), when interfacing with other applications (e.g., configuration management application, trouble ticket system) are required to understand multiple name conventions.
- When a customer purchases multiple classes of NEs from the same or different vendors, the customer is confronted with multiple name conventions.
- Without a name convention, it is difficult to integrate IRP conformant vendors' resource namespace [see section 0 for definition of namespace] into the customer's Enterprise namespace.

H1.2.2 Benefits

This section lists the benefits of using the subject name convention to name 3G network resources for network management purposes.

- It is obviously a large benefit to have one name convention that works for all the allowed protocols for 3G-network management.
- A resource name is guaranteed to be unambiguous in that it refers to, at most, one network resource.
- The resource name syntax is specified such that management applications can be designed with assurance that its name-parsing algorithm needs not be modified in the future. We can derive this benefit only if the subject name convention is widely accepted.
- The root and upper portions of the name hierarchy are based on name infrastructure of Domain Name System (DNS) [5]. The subject name convention can naturally fit in DNS and can integrate well with other hierarchical naming systems, such as X.500 [2].
- One name convention for a wide range of 3G network management products can improve 3G network management standards' image (compared to GSM) that the various next generation NEs' and network management systems' development are in synchrony.

H1.3 Document Structure

This document is structured following multiple sections.

Section 1 introduces the document.

Section 2 provides the system overview.

Section 3 specifies the string representation of Managed Object using the concept of ITU-T X.500 [2] Distinguished Name (DN).

Section 4 provides examples of DNs.

Section 5 provides a DN usage scenario illustrating how a NE designer should use the subject name convention.

Section 6 provides references.

Appendix A specifies the Relative Distinguished Name (RDN) `AttributeType` strings.

Appendix B provides a rule for MO designers to avoid ambiguity concerning the `AttributeType` of a Distinguished Name (DN) string.

Appendix C discusses the topics of DN prefix and Local Distinguished Name.

H1.4 Key Terms

This section defines terms essential for understanding of name convention in the IRP context.

H1.4.1 Managed Object and Network Resource

In the context of this document, a Managed Object (MO) is a software object that encapsulates the manageable characteristics and behaviour of a particular network resource. Examples of network resource are switch, scanner for monitoring performance data, cell, site, transmission links, satellite, operator profile, etc. In this document, MO sometimes is referred to as MO instance.

H1.4.2 Name

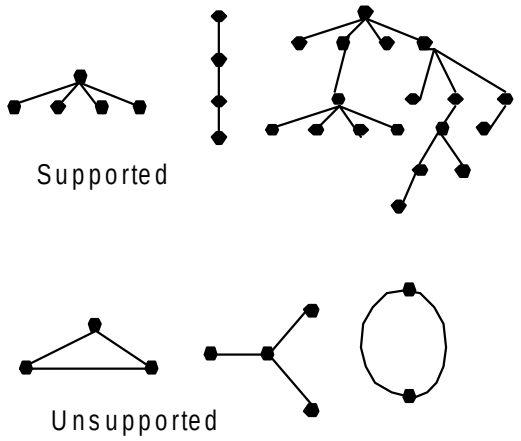
In the context of this document, a name is restricted to the identification of a Managed Object (MO), that is, a software object representing a real network resource.

H1.4.3 Namespace

A namespace is a collection of names. This name convention uses a hierarchical containment structure, including its simplest form - the one-level, flat namespace. This name convention does not support an arbitrarily connected namespace, or graph structure, in which a named object can be both child and parent of another named object. The following figure shows some examples of supported and unsupported namespaces[2].

[2] The figure is from Reference [3]. It provides useful information on namespace design.

Figure 3: Examples of supported and unsupported namespaces



H1.4.4 Global Root and Local Root

Names in namespace are organized in hierarchy. A MO instance that contains another is said to be the superior (parent); the contained MO instance is referred to as the subordinate (child).

In modern network management, it is expected that the Enterprise namespace be partitioned[3] for implementations in multiple managed system. The parent of all MO instances in a single managed system is called the Local Root. The ultimate parent of all MO instances of all managed systems is called the Global Root.

H1.4.5 Distinguished Name and Relative Distinguished Name

A Distinguished Name (DN) is used to uniquely identify a MO within a namespace. A DN is built from a series of "name components", referred to as Relative Distinguished Names (RDNs). ITU-T Recommendation X.500 [2] defines the concepts of DN and RDN in detail, using ASN.1, in the following way:

```
DistinguishedName ::= RDNSequence
RDNSequence ::= SEQUENCE OF RelativeDistinguishedName
RelativeDistinguishedName ::= SET SIZE (1..MAX) OF
      attributeTypeAndValue
AttributeTypeAndValue ::= SEQUENCE {
      type AttributeType, value AttributeValue}
```

This document references this ASN.1 structure but it only uses single-valued (not a set of) RDN.

From a DN of a MO, one can derive the DN of its containing MO, if any. This containment relation is the only relation carried by the DN. No other relation can be carried or implied by the DN.

See Appendix B for a rule for MO designers to avoid ambiguity concerning the `AttributeType` of a DN string.

See Appendix C for discussion of DN prefix and Local Distinguished Name (LDN).

H1.5 Glossary

Actor and System: These are terms used in all IRP contexts. Actor is used to model all kinds of objects outside the domain of the System and it interacts with System using the IRP. System models the object that interacts with Actor using IRP.

---

[3] See Appendix C for reasons of namespace partitioning.

ASN.1: Abstract Syntax Notation One
BNF: Backus-Naur Form
DC: Domain Component
DN: Distinguished Name
DNS: Domain Name Service
IETF: Internet Engineering Task Force
LDN: Local Distinguished Name
MIM: Management Information Model
MO: Managed Object
MOI: Managed Object Instance
NE: Network Element
NEM: Network Element Manager
RDN: Relative Distinguished Name
ITU-T: International Telecommunication Union, Telecommunication Standardization Sector

H2 System Overview

H2.1 System context

Following are situations under which MO (representing network resource) names will be used.

- MO names will cross various Integration Reference Points (IRPs).

  Example 1: In the context of Alarm IRP [8], System notifies Actor of the alarm condition of a network resource. The DN of the MO, representing alarmed network resource, encoded as specified in this document, is carried in the `Managed Object Instance` parameter of the notification.

  Example 2: In the context of Configuration Service IRP [9], System notifies Actor of the creation of new object. The DN of the newly created object, encoded as specified in this document, is carried in the notification.

  Example 3: In the context of Configuration Service IRP [9], Actor requests System to search for a particular object by specifying the start point of the search. The DN of the base object, upon which the search begins downward hierarchically, is carried in the request.

- Co-operating management applications need to exchange information that includes MO (representing network resource) names.

  Example 1: A fault management application may request a trouble ticket system to open a new trouble ticket reporting the alarmed condition of a network resource by specifying, among other things, the MO name representing the alarmed network resource. The DN of the MO, encoded as specified in this document, is included in the request.

  Example 2: A performance management system that produces reports on performance of network resources. The DNs of the MOs, representing the reported network resources, encoded as specified in this document, are printed on the report.

H3 String Representation of DN

DN can be encoded and represented in many ways. This document specifies one such encoding and representation, the string representation. String representation of DN shall be used in all IRP works. See section 0, H2.1 System context, for more information on when DNs are used.

This work is based on work published in RFC 2253 [7].

H3.1 Converting DN from ASN.1 to a String

H3.1.1 Converting `RDNSequence`

If the `RDNSequence` is an empty sequence, the result is the empty or zero length string.

Otherwise, the output consists of the string encoding of each `RDN` in the `RDNSequence` (according to 0), starting with the first element of the sequence and moving forward toward the last element.

The encoding of adjacent RDNs are separated by a comma character (",", ASCII 44), to be consistent with IETF RFC 2253 [7].

White spaces adjacent to the slash character shall be ignored.

H3.1.2 Converting `RelativeDistinguishedName`

When converting from an ASN.1 `RDN` to a string, the output consists of the string encoding of the singleton `AttributeTypeAndValue` (according to 0).

Although X.500 DN supports multi-valued RDN, this specification supports single-valued RDN only.

H3.1.3 Converting `AttributeTypeAndValue`

The `AttributeTypeAndValue` is encoded as the string representation of the `AttributeType`, followed by an equals character ('=', ASCII 61), followed by the string representation of the `AttributeValue`.

If the `AttributeType` is published in Table 9: RDN **`AttributeType`** Strings in Appendix A, then the type name string from that table is used. If the `AttributeType` is not in the published table, implementation is free to use any string as long as the string does not begin with "IRP".

Although X.500 ASN.1 `AttributeValue` and `AttributeType` support wide range of character representation, this specification supports a restrictive set of characters according to section 0.

String representation of `AttributeValue` and `AttributeType` do not allow (character) escape[4] mechanism such as the use of a backslash followed by two hex digits to replace a character in a string.

See Appendix B for a rule for MO designers to avoid ambiguity concerning the `AttributeType` of a DN string.

H3.2 Character Syntax

This section specifies the character syntax for `AttributeType` and `AttributeValue`.

They are:

[4] In the example, the backslash and the two hex digits form a single byte in the code of the escaped character. The backslash, followed by "0D", indicates a carriage return. Example: "`CN=Before\0DAfter,O=Test,C=GB`".

1. Any character except <special> where <special> is

   "," or "=" or <CR> or <LF> "+" or "<" or ">" or "#" or ";" or "\" or ""'

2. The dot character ('.', ASCII 46). This character shall only be used in the `AttributeValue` whose `AttributeType` is "`DC`". An example is "`DC=lme.ericsson.se`". This dot character shall not be used in `AttributeType`.

3. The star character ('*', ASCII 42) is reserved to denote wild card. Wild card character(s) can appear in `AttributeType` and `AttributeValue`.

H3.3 BNF of DN String Representation

The following is the BNF[5] for DN in string representation.

```
DistinguishedName := RDNSequence
<spaced-separator> ::= <optional-space> <separator> <optional-space>
<separator> ::=  ","
<optional-space> ::= ( <CR> ) *( " " )
RDNSequence := RDNSequence <spaced-separator>
    RDNSequence | RelativeDistinguishedName
RelativeDistinguishedName := AttributeTypeAndValue
AttributeTypeAndValue := AttributeType "=" AttributeValue
<special> ::= "," |"=" |<CR> |<LF> |"+" |"<" |">" |"#" |";" |"\" | """
AttributeType := <one or more StringChar>
AttributeValue := <one or more StringChar>
StringChar := any character except <special>
```

H3.4 Maximum size of DN string

The maximum length of a DN string, including RDN separators and including white spaces, shall not exceed 400 characters.

[5] Backus-Naur Form is popular in IETF specifications to define format syntax. See RFC733, "Standard for the Format of ARPA Network text messages" for more information.

H4 Examples

This section gives a few examples of DN written in the string representation specified in this document.

1. "`DC=com,DC=Teleglobe,DC=Marketing,System=ATMPVCBilling,Log=19990101131000,AccountingRecord=100098`". In this example, the namespace aligns with DNS. The `AttributeType` of the top three RDN are "`DC`". Concatenation of the corresponding `AttributeValues` produces the DNS registered name, i.e. "`marketing.teleglobe.com`". The top RDN is the Global Root because DNS defines "`DC=com`" as the root of its namespace. That top RDN is the Local Root as well.

2. "`DC=marketing.Teleglobe.com,System=ATMPVCBilling,Log=19990101131000,AccountingRecord=100098`". In this example, the namespace aligns with DNS as well. Instead of using three RDNs to represent the DNS registered name, this example chooses to use one RDN. The top RDN is the Global Root (and Local Root as well).

3. "`IRPNetwork=Telia,Subnet=TN2,BSS=B5C0100`". In this example, the namespace designer chooses not to name its objects under the DNS nor X.500 scheme. The namespace designer chooses to use "`IRPNetwork=Telia`" as the Local Root[6] of its namespace. DNs in this namespace will start with that string as their Local Root. One string ("`IRPNetwork`") for `AttributeType` (of the `AttributeTypeAndValue` of the RDN) starts with "IRP". This indicates that this string is mapped from the MO class names specified in Base MIM of [9]. Other strings do not start with "IRP", indicating that those strings are not mapped from MO class names specified in Base MIM of [9]. They are probably mapped from MO classes that are specific for a particular product line and thus specified in a product-specific MIM.

4. The following example illustrates the use of "," as separator for RDNs. It also illustrates the use of space and period as part of the legal character syntax for RDNs.

   ```
   CN=John T. Mills, O= Cyber System Consulting, L= Göteborg, C=SE
   ```

[6] By looking at the DN string, it is not possible to say if the Local Root is the Global Root.

H5 Usage Scenario

H5.1 DN prefix usage

This section presents recommended steps designer uses to partition the Enterprise name space while building an Alarm IRP compliant NE (the Alarm IRP System).

1. NE designer specifies the MIM[7] for the NE. Suppose the MIM is a two level hierarchy with 3 classes like

```
Node
  |----- Port
|----- CrossConnect
```

2. NE designer, based on the MIM and other design choices, decides that there are 7 instances within the NE that can report alarms, such as
`Port=1, Port=2, Port=3, Port=4, Port=5, CrossConnect=1, Node=1.`
3. NE designer decides on the DN prefix (see Appendix C) and configures its system accordingly. Since NE designer will not know the customer's namespace in advance, he would normally configure the DN prefix to reflect his test environment. The DN prefix can be configured to "`IRPNetwork=test`". The Global Root is "`IRPNetwork=test`". The Local Root is "`Node=1`". Note that NE should not hard code the DN prefix but should treat DN prefix as a system configuration parameter, settable, for example, at system start-up time.

4. When constructing the alarm record (in coding phase), NE designer shall concatenate the name of the alarmed instance with the DN prefix to form the DN of his test environment. The resultant DN (e.g., "`IRPNetwork=test,Node=1,Port=3`") will be placed in the `Managed Object Instance` (`MOI`) field of the alarm record.

5. The NE is sold to a customer. The customer administrator knows his Enterprise namespace, the topology of his network and where the NE will be deployed. Based on the information, he configures the DN prefix of the NE. For example, the customer administrator can configure it to:

   "`DC=Teleglobe.com,Net=DS3BackBone,Station=TMR`".

   The Global Root in this case is "`DC=Teleglobe.com`".

6. At run time, whenever NE is reporting an alarm on `Port=3` via the IRP, the following string will be in the `MOI` field of the alarm record.

   `"DC=Teleglobe.com,Net=DS3BackBone,Station=TMR,Node=1,Port=3".`

[7] MIM is Management Information Model. It is a collection of classes of network resources arranged in containment hierarchy. Instances of the classes encapsulate the behaviour of the real network resources under management.

H6 References

[1] Intentionally left blank.

[2] [X.500] ITU-T Recommendation X.500 (11/93) - Information technology - Open Systems Interconnection - The directory: Overview of concepts, models, and services

[3] Understanding and Deploying LDAP Directory Services, T.Howes, ISBN 1-57870-070-1.

[4] [RFC1737] Functional Requirements for Uniform Resource Names 1994.

[5] [RFC2247] Using Domains in LDAP Distinguished Names, January 1998.

[6] [RFC1035] Domain Name – Implementation and Specification, November 1987.

[7] [RFC2253] Lightweight Directory Access Protocol version 3: UTF-8 String Representation of Distinguished Name, December 1997.

[8] Alarm IRP: Management Information Service

[9] Configuration Service IRP: Management Information Service

Annex H Appendix A: Mapping of RDN AttributeType to Strings

AttributeType of RDN are mapped into strings for use in the DN string representation. This appendix specifies the mapping.

The AttributeType shall include all MO classes defined in Base Management Information Model (MIM) of [9].

There is one AttributeType that is not defined in Base MIM of [9]. This special AttributeType is used to denote the domain component of the DNS. The following partial DN string representations are examples to illustrate the valid use of "DC" strings for the three DNS domain components of "lme.ericsson.se".

- DC=se.ericsson.lme,..
- DC=se,DC=ericsson,DC=lme,..
- DC=se,DC=ericsson.lme,..
- DC=se.ericsson,DC=lme,..

Table 9: RDN AttributeType Strings

String	AttributeType
DC	Domain component of DNS
IRPEquipment	MO Class name irpEquipment defined in Base MIM of [9].
IRPNetwork	MO class name irpNetwork defined in Base MIM of [9].
IRPManagedElement	MO class name irpManagedElement defined in Base MIM of [9].
etc.	Other MO class names as defined in Base MIM or product-specific MIM (extension to Base MIM).

Annex H Appendix B: Rule for MO Designers regarding AttributeType interpretation

This appendix discusses the two possible interpretations for the AttributeType of the DN string and recommends a rule for MO designers to avoid ambiguity concerning its usage. It identifies the protocol environment(s) under which each interpretation functions. It then recommends a rule for designing MO classes such that one DN string, regardless of protocol environment (therefore, regardless of interpretation used), will result in the unique reference to the identical network resource.

First interpretation

ITU-T X.500 uses the AttributeType (defined for use as the first component of the AttributeTypeAndValue of a RDN, see section 0) to identify one attribute of the subject MO for naming purpose. This AttributeType is called the *naming attribute* to distinguish itself from other attributes that may be present in the MO.

Suppose the following is the MO class definition in pseudo notation and this MO class is inherited from root.

```
Class Bsc {
 Attribute id;
 Attribute ..}
```

Suppose further that the naming attribute is id.

If this (first) interpretation is used for constructing the DN string, then the DN will be "…,id=123". MO class name cannot be derived from the DN string. The value of the AttributeValue contains the value of the naming attribute.

Second interpretation

In CORBA protocol environment, it is preferable to use the following interpretation.

The AttributeType (defined for use as the first component of the AttributeTypeAndValue of a RDN) is used to identify the MO class.

If this interpretation is used for constructing the DN string, then the DN will be "…,Bsc=123". The name of the naming attribute cannot be derived from the DN string. The value of the AttributeValue contains the value of the naming attribute.

Rule

Given the two interpretations, a DN reader cannot know how to interpret the AttributeType. To avoid ambiguity, the following rules shall apply when specifying MO classes for the Base MIM in [9] and MO classes in product-specific specifications.

1. MO designer, when designing a MO class, shall include an attribute composed of the following two strings: name of the class and "Id". Identify this attribute as the name distinguishing attribute. For example, if Bsc is the name of a class, then it shall have an attribute named bscId as well. This attribute is considered the naming attribute. If IRPManagedElement is the MO class name, then this class shall have an attribute called irpManagedElementId as well.

2. If the class is abstract in that no object of this class can be instantiated, then it is not necessary to include a naming attribute in the class. For example, if IRPNetwork is an abstract class, it does not need to have a naming attribute called irpNetworkId. If IPBackBone inherits irpNetwork and the class IPBackBone is not abstract, then it shall contain a naming attribute called iPBackBoneId.

3. If the class is not abstract in that object of this class can be instantiated, then it is required to include a naming attribute in this class using the rule specified in this section. When another class inherits this class, the other class shall include a naming attribute as well. For example, if Circuit is not an abstract class, it shall have a naming attribute called circuitId. If DS3 inherits Circuit, DS3 class shall also have a naming attribute called dS3Id. When an instance of DS3 class is created, the dS3Id shall be used and other naming attribute (in this case, circuitId) shall be ignored.

Annex H Appendix C: DN Prefix and Local Distinguished Name (LDN)

A Distinguished Name (DN) is used to uniquely identify a MO within a namespace. A DN is built from a series of "name components", referred to as Relative Distinguished Names (RDNs).

DNs within a namespace are arranged in hierarchy similar to concepts of naming files in UNIX file system. A file name, in the context of a local subdirectory, contains the path (series of subdirectory names) of the file starting from the local subdirectory. The same file, in the global context, contains the path of the file starting from the root directory. Similar concept applies to naming MOs. From a particular (local) context, the name of a MO is the Local Distinguished Name (LDN). From a global context, the name of the same MO is the DN. LDN is a proper subset of DN. In the context of a particular local context, a DN prefix is defined such that all LDNs in that particular context, if attached behind the DN prefix of that context, will yield the DNs of the MOs.

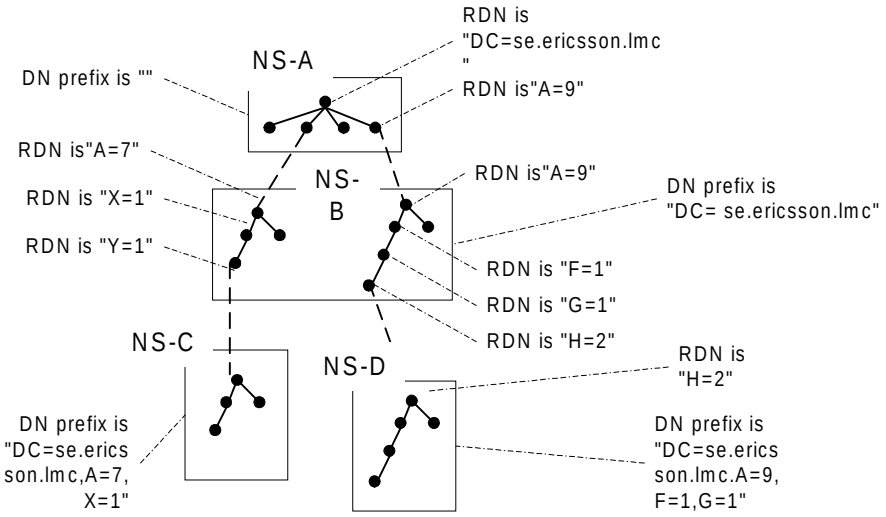
The concepts of DN Prefix and LDN support the partitioning of large namespace into smaller ones for efficient namespace implementation. DN design, the subject of this document, does not depend on these concepts. There exist other concepts that support partitioning of large namespace as well. Although these concepts are independent from DN design, their use is wide spread and this appendix illustrates their use in partitioning large namespace.

In modern network management, it is expected that the Enterprise namespace be partitioned for implementations in multiple hosts. The following are reasons for the partitioning.

- The Enterprise namespace can be large (e.g., containing millions of objects). Partition of a large namespace facilitates namespace management. For example, it may be easier to manage two name spaces of 1 million objects each than to manage one name space with two million objects.
- Separate Systems manage sub-set of the Enterprise namespace relevant to their own local environment. For example, one NE manages a namespace (subset of the Enterprise name space) containing names of its MOs representing its own network resources. Another NE manages another sub-set, etc.
- For reasons such as security, replication, back-up policy and performance, sub-sets of the Enterprise namespace are managed by separate systems. For example, Operation and Marketing departments may want to manage their namespaces using their respective management policies. Partitioning of Enterprise namespace according to departmental jurisdiction may facilitate deployment of independent management policies.

Suppose the Enterprise namespace is organized hierarchically and is partitioned into 4 sub-sets as shown in the following figure.

Figure 4: Namespace partitions



NS (namespace)-A contains 5 objects. DN prefix is NULL. The Global Root and Local Root of NS-A is "`DC=se.ericsson.lmc`"[8]. DN of top object is "`DC=se.ericsson.lmc`". RDNs of the other four objects are, from bottom left to bottom right, "`A=1`", "`A=7`", " `A=3`" and "`A=9`". DNs of the same four objects are "`DC=se.ericsson.lmc,A=1`", "`DC=se.ericsson.lmc,A=7`", "`DC=se.ericsson.lmc,A=3`" and "`DC=se.ericsson.lmc,A=9`". The second and fourth objects are reference objects to MOs in NS-B.

NS-B contains two branches. They have the same DN prefix that is "`DC=se.ericsson.lmc`". The Global Root is "`DC=se.ericsson.lmc`".

The Local Root and RDN of top object of the right branch is "`A=9`". Its DN is "`DC=se.ericsson.lmc,A=9`". RDNs of other objects are shown in the figure. DN of the bottom object is "`DC=se.ericsson.lmc,A=9,F=1,G=1,H=2`". This object refers to object of another namespace called NS-D.

The Local Root and RDN of the top object of the left branch is "`A=7`". Its DN is "`DC=se.ericsson.lmc,A=7`". RDNs of other objects are shown in the figure. DN of the bottom object is "`DC=se.ericsson.lmc,A=7,X=1,Y=1`". This object refers to object of another namespace called NS-C.

NS-C contains a branch of 4 objects. Its DN prefix is "`DC=se.ericsson.lmc,A=7,X=1`". The Local Root an RDN of the top object is "`Y=1`".

NS-D contains a branch of 5 objects. Its DN prefix is "`DC=se.ericsson.lmc,A=9,F=1,G=1`". The Local Root and RDN of the top object is "`H=2`".

In the above figure, the bottom object of NS-B right branch has the following names:

- DN is "`DC=se.ericsson.lmc,A=9,F=1,G=1,H=2`".
- LDN is "`A=9,F=1,G=1,H=2`".
- RDN is "`H=2`".

---

[8] Use of "`DC`" in "`DC=se.ericsson.lmc`" is an attempt to align the RDN with DNS name associated with the named organisation. The "`DC`" stands for domain component and is an attribute name defined by IETF for use in directory work. Appendix A specifies other valid ways to align RDN with DNS as well. Equally valid, the example can choose to align the RDN with the X.500 convention. In such case, the subject string can be "`C=se,O=Ericsson,L=lmc`" where C, O and L are X.500 standard attributes denoting country, organisation and location respectively. The alignment choice belongs to the namespace designer of the customer who purchases our products. The choice will be reflected in the value of the DN prefix, probably a product configuration parameter. See Section 0, H5 Usage Scenario, for more information.

With this example, we can see that DN of an object is a series of RDNs spanning the global namespace. LDN of an object is a series of RDNs spanning the local namespace where the subject MO resides.

The concatenation of the LDN with DN prefix of that (partitioned) namespace shall produce the DN of the global namespace.