ETSI
TECHNICAL
REPORT

ETR 224

August 1995

Source: ETSI TC-NA

Reference: DTR/NA-060804

ICS: 33.040

Key words: CS2, IN, management

Intelligent Network (IN);
Capability Set 2 (CS2);
IN intra domain management requirements for CS2

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

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

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

New presentation - see History box

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Foreword

This ETSI Technical Report (ETR) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI).

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

Introduction

The management aspects of Intelligent Network (IN) will be specified using Telecommunications Management Network (TMN) concepts following the approach of ETR 062 [1]. A suitable procedure resulting in the specification of IN management is needed. This specification should be defined by the use of managed objects (Guidelines for the Definition of Managed Objects (GDMO), ITU-T Recommendation X.722 [10]) and the General Relationship Model (GRM), ITU-T Recommendation X.725 [11]. The first step in such a procedure is the capture of the IN management requirements.

This ETR is restricted to the first step, the management requirements capture. It contains the IN management requirements concerning needs analysis, service creation (but not the requirements for the management of the service creation process), acceptance testing, service deployment, service operation and service removal of IN-provided services.

NOTE: The management requirements as such will not be subject to standardization. The list of management requirements will provide a check list to guide the standardization process of the functions, objects and messages, ensuring that it supplies all the functionality that is necessary to support the perceived usage of the management implementation.

In order to structure the process of identifying IN management requirements properly a suitable approach has been defined. This approach is presented in clause 5.

Clauses 5 and 6 list the IN functional management requirements identified for CS2. Clause 5 contains the management requirements between the actors involved in the service life cycle of IN-based services. Clause 6 lists the management requirements on the IN Functional Entities (FEs). The requirements in clause 6 are more detailed than those in clause 5.

The IN management requirements listed in these clauses imply the re-use of generic management functions, related to e.g. security, log control, scheduling and filtering. These generic management functions are not repeated in this ETR but are captured in the following ITU-T Recommendations:

ITU-T Recommendation X.731 [13]: "State management function".
ITU-T Recommendation X.733 [15]: "Alarm reporting function".
ITU-T Recommendation X.734 [16]: "Event report management function".
ITU-T Recommendation X.735 [17]: "Log control function".
ITU-T Recommendation X.736 [18]: "Security alarm reporting function".
ITU-T Recommendation X.738 [19]: "Summarization function".
ITU-T Recommendation X.739 [20]: "Metric objects and attributes".
ITU-T Recommendation X.740 [21]: "Security audit trail function".
ITU-T Recommendation X.741 [22]: "Objects and attributes for access control".
ITU-T Recommendation X.742 [23]: "Usage metering function".
ITU-T Recommendation X.744 [24]: "Software management function".
ITU-T Recommendation X.746 [25]: "Scheduling function".
ITU-T Recommendation M.3400 [4]: "TMN management functions".
ITU-T Recommendation Q.822 [8]: "Performance management".

Blank page

1 Scope

In the Intelligent Network (IN)-concept three kinds of processes are distinguished:

- service execution;
- service creation; and
- management.

The scope of this ETSI Technical Report (ETR) is the further development of the IN concept, and in particular of the management process of INs, i.e. the management of the IN resources and the IN services in the network.

Within the IN-concept, service execution has been separated from service creation and management for IN Capability Set 1 (CS1). IN CS1 has only focused on the service execution capabilities. However, the increasing complexity of IN-based services and features has led to a need to identify the IN management capabilities in CS2.

The aim of this deliverable is to provide a set of requirements on IN management, in the scope of CS2 (and, therefore, also supporting CS1). This set of IN management requirements should not be seen as exhaustive or necessarily mandatory, but will provide a basis for the development of IN standards with respect to the management of the IN. The management requirements identified in this ETR are described as the need for exchange of management information (functions and data) between the set of actors and entities in figure 1.

This ETR includes requirements:

- for management of one IN-structured network. These requirements, however, cover some non IN-specific aspects such as requirements related to customer contact;
- for management of the following IN Functional Elements (FEs): Service Switching Function (SSF), Specialised Resource Function (SRF), Service Control Function (SCF) and Service Data Function (SDF);
- related to the full service life cycle, see figure 2.

This ETR does not include requirements for:

- the management of the interworking between IN-structured networks; or
- the management aspects of the interworking between private networks (IN-structured and non-IN-structured) and public IN-structured networks;
- the management related to service interaction.

Clauses 1 through 4 deal with introductory remarks. Clause 5 describes the approach that is used to identify the IN management requirements. This approach is meant to apply to all current IN management requirements studies and will probably form the basis for all future IN management requirements studies. Clauses 5 and 6 of this ETR contain the results of the IN requirements capture for CS2. These IN management requirements may imply additional generic management requirements.

2 References

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

[1] ETR 062: "Network Aspects (NA); Baseline document on the integration of Intelligent Network (IN) and Telecommunication Management Network (TMN)".

[2] ITU-T Recommendation Q.1290: "Glossary of terms used in the definition of intelligent networks".

[3] ITU-T Recommendation M.3200: "TMN management services: overview".

[4] ITU-T Recommendation M.3400: "TMN management functions".

[5] ITU-T Recommendation Q.1211: "Introduction to intelligent network capability set 1".

[6] ITU-T Recommendation Q.1213: "Global functional plane for intelligent network CS-1".

[7] ITU-T Recommendation Q.1214: "Distributed functional plane for intelligent network CS-1".

[8] ITU-T Recommendation Q.822: "Stage 1, stage 2 and stage 3 description for the Q3 interface - Performance management".

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

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

[11] ITU-T Recommendation X.725: "Information technology - Open Systems Interconnection - Structure of management information: General relationship model".

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

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

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

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

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

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

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

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

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

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

[22] ITU-T Recommendation X.741: "Information technology - Open Systems Interconnection - Systems Management: Objects and attributes for access control".

[23] ITU-T Recommendation X.742: "Information technology - Open Systems Interconnection - Systems Management: Usage metering function".

[24] ITU-T Recommendation X.744: "Information technology - Open Systems Interconnection - Systems Management: Software management function".

[25] ITU-T Recommendation X.746: "Information technology - Open Systems Interconnection - Systems Management: Scheduling function".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this ETR, the following specific definitions apply:

(IN structured) domain: In this ETR the term (IN structured) domain is used to indicate a named set of (IN) resources (FEs) and their managers (SM and N/EM).

Network/Element Manager (N/EM): The N/EM is an actor who provides the basic switching and transmission capabilities as well as the service execution capabilities (offered by the Service Control Point (SCP), Service Data Point (SDP) and Intelligent Peripheral (IP)) to the SM. The N/EM is also responsible for the development and maintenance of the transmission, switching and service execution capabilities. To ease the identification of management requirements, in this ETR the N/EM encompasses both the Telecommunications Management Network (TMN) network management and network element management functionality.

NOTE: The future trend towards a more open competitive environment in Europe may mean that the functional entities of the service execution environment could be owned and operated by separate organisations. The implications for network/element management and the relationship between the N/EM and SM within this environment is for further study.

service management: Service management is concerned with and responsible for:

- subscriber facing;
- management of information relating to the contractual aspects of services that are being provided to subscribers or available to potential new subscribers, within the bounds specified by policies produced by the business management (layer);
- the proper operation of services;
- provisioning of information to the network management required for the proper planning, deployment, provisioning and operation of network resources necessary to support services;
- interaction with the business management (layer) for guidelines and policies, and;
- interaction with service providers Q.1290 [2].

Service Manager (SM): The SM is the actor who provides the IN-based services to its customers on a contractual basis, and who is responsible for the services offered. The SM uses the service execution, transmission and switching capabilities offered by the Network/Element Manager (N/EM) to offer the services to its customers.

Service Subscriber (SS): The SS is an “entity that contracts for services offered by service providers” (Q.1290 [2]).

In addition to this definition, for this ETR the following restriction applies:

The SS is the actor who has a contractual agreement with a SM regarding the use of a service (including possible customer control capabilities) offered by the SM. The SS is also responsible for fulfilling the contractual obligations (e.g. for paying the service usage) that result from service invocations by the SUs that he has authorised to use the service.

Service User (SU): The SU is an “entity external to the network that uses its service(s)” Q.1290 [2].

In addition to these definitions, the following remarks can be made:

- the SU is the actor who actually uses a service in order to fulfil his communications needs. The SU is not responsible for the subscription and for paying anything for using the service (at least not towards the SM);
- from the Q.1290 [2] definition of the SS and SU above, it could be deducted that only the Service User should be seen as an entity external to the IN-structured domain. At least in this ETR, this is not implied, both actors are seen as entities external to the IN-structured domain (see also figure 1);
- it should be noted that the SU and the SS can be the same physical entity. But it is important to differentiate between these two actors because they have different demands and requirements on the services;
- the terms subscriber, service subscriber and customer are used in this ETR with the same meaning.

3.2 Abbreviations

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

CPM	Customer Profile Management
CSx	Capability Set x
FE	Functional Entity
GDMO	Guidelines for the Definition of Managed Objects
GRM	General Relationship Model
IN	Intelligent Network
IP	Intelligent Peripheral
NE	Network Element
N/EM	Network/Element Manager
OSI	Open System Interconnection
QoS	Quality of Service
SCF	Service Control Function
SCP	Service Control Point
SDF	Service Data Function
SDP	Service Data Point
SLP	Service Logic Program
SM	Service Manager
SMFA	Systems Management Functional Area
SRF	Specialised Resource Function
SS	Service Subscriber
SSF	Service Switching Function
SU	Service User
TMN	Telecommunications Management Network

4 Guidelines for determination of IN management requirements

4.1 Introduction

This subclause is aiming at introducing a general approach for the description of IN management requirements. The current approach is aimed to capture the IN management requirements for CS2. Enhancements to the approach to capture management requirements for future CSs are possible.

In ITU-T Recommendation M.3200 [3] a TMN management services template tool is described. The use of this tool helps to ensure complete coverage of the functional requirements of a management service. It is a two-dimensional template, the first dimension being the logical representation of an administration management hierarchy (Business-, Service-, Network, and Network element management) and the second dimension being a list of those management functional areas (like configuration management, fault management, etc.) to be covered. All of the resultant intersections need to be addressed.

In this study a slightly adjusted approach was developed to ensure easier identification of IN management requirements and achieving the maximum coverage possible. As a first step in the approach, a detailed template is provided to identify IN management requirements.

4.2 The approach

The approach makes use of a number of dimensions from which IN management requirements can be identified. These dimensions are described in subclause 4.2.1. The requirements can then be structured according to the templates using these dimensions. The templates are described in subclause 4.2.2.

4.2.1 The dimensions

The various dimensions that have been considered, are:

- **Actors,** i.e.:
  - Service Manager (SM);
  - Network/Element Manager (N/EM);
  - Service Subscriber (SS); and
  - Service User (SU).

  The definitions of these actors are given in subclause 3.2. The various relationships between these actors involved in the management of one IN-structured domain are illustrated in figure 1.

- **IN Functional Entities:**
  - Service Switching Function (SSF);
  - Specialised Resource Function (SRF);
  - Service Control Function (SCF); and
  - Service Data Function (SDF).

  These functional entities are described in ITU-T Recommendation Q.1214 [7].

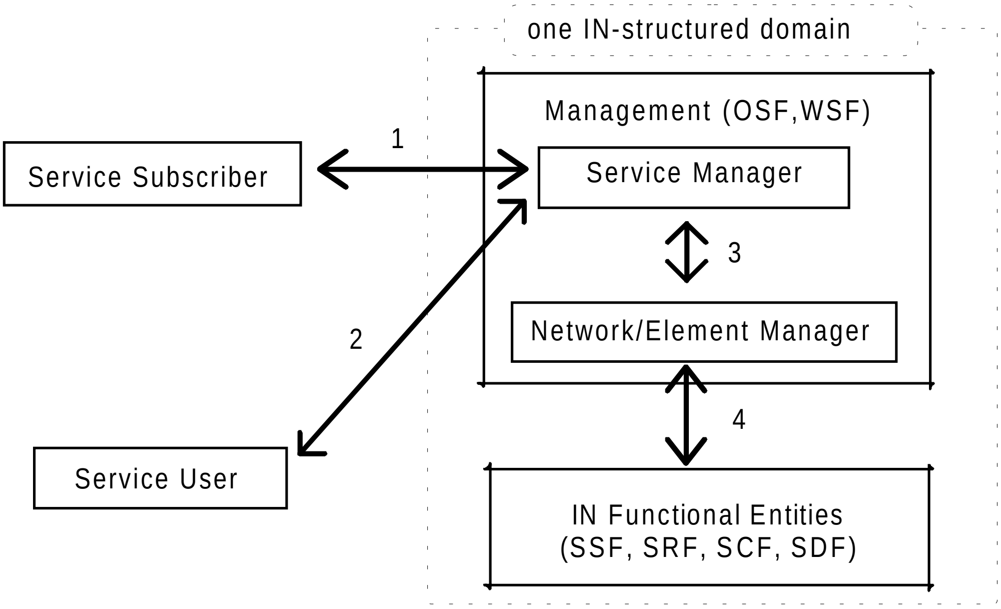

Figure 1: The relationships between the actors identified in this ETR

- **Service life cycle phases**
  For the ease of understanding the phases and activities of the Service Life Cycle for services supported by an IN are briefly summarised in figure 2.

<table>
<tr><th></th><th>Phases</th><th colspan="4">Activity Groups</th></tr>
<tr><td>customer or market need</td><td>Needs Analysis</td><td colspan="4">market needs analysis
customer needs analysis</td></tr>
<tr><td></td><td>Service Creation</td><td colspan="4">service specification
service validation
service type development and building block development
service verification</td></tr>
<tr><td></td><td>Service Acceptance Testing</td><td colspan="4">service acceptance test
service pilot (field trial), ...</td></tr>
<tr><td></td><td>Service Deployment</td><td colspan="4">downloading of service logic and service data into network elements
installation of management functions and management data associated with the service</td></tr>
<tr><td rowspan="3">Service type available</td><td rowspan="3">Service Provisioning and Operation</td><td rowspan="3">Service Type Control Activities</td><td colspan="3">Service Instance Provisioning</td></tr>
<tr><td>Service Instance Control Activities</td><td>Service Invocation Control Activities</td><td>Service Invocation Activities</td></tr>
<tr><td colspan="3">Service Instance Withdrawal</td></tr>
<tr><td>Service type removed</td><td>Service Removal</td><td colspan="4">removal of service logic and service data from network elements
removal of management functions and management data associated with the service</td></tr>
</table>

Figure 2: Phases and main activities of the service life cycle

- **Open System Interconnection (OSI) Systems Management Functional Areas (SMFAs), ITU-T Recommendation X.701 [9]:**

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

- **services, service features or SIBs, ITU-T Recommendations Q.1211 [5] and Q.1213 [6]**

- **TMN layering (hierarchy), ETR 062** [1]:

  the TMN layers are business management, service management, network management, and network element management. The business management layer, however, is out of the scope of this ETR. The exact definition of what constitutes service management (data and functions) and what constitutes network management (data and functions) has not been made within the TMN standards work yet. Such a definition will eventually impact the relationship between NE/network management and service management.

4.2.2 The templates

Based on the dimensions actors, IN functional entities, service life cycle and OSI SMFAs, two groups of IN management requirements have been identified. For each group a refined template is defined enabling a structural approach for the identification of IN management functional requirements. A pictorial representation of these two templates can be found in figures 3 and 4 respectively.

1) Management requirements between actors SS-SM, SU-SM and SM-N/EM.

These are the requirements between actors for relationships 1, 2 and 3 in figure 1. First the requirements are structured according to the actor who puts the requirement upon another actor. Structuring in a second dimension is done according to the phases of the service life cycle in which the requirements occur.

The requirements from this group are described in clause 5.

Management requirements between actors			
	SS - SM	SU - SM	SM - N/EM
Needs analysis			
Service creation			
Service Acceptance testing			
Service deployment			
Service provisioning and operation			
Service type control activities			
Service provisioning			
Service instance control activities			
Service invocation control activities			
Service invocation activities			
Service instance withdrawal			
Service removal			

Figure 3: The IN management functional requirements identification template for the requirements between actors

The following is a step-by-step procedure of the use of the template in figure 3:

- go through the phases/activities of the Service Life Cycle from the viewpoint of the actors SU, SS and SM;
- identify in each service life cycle phase/activity for each actor his/her management requirements upon another actor regarding a service;
- describe the management requirement (data and functions) identified following a notation that should:
  - support a uniform and brief notation;
  - make clear who puts a requirements upon who;

  The resulting notation to be used has the following format:

```
<actor XX>-<actor YY>

-       <requirement 1>

-       <requirement 2>

                :
                :

-       <requirement n>
```

where the actor "XX" puts the requirements 1 through n upon actor "YY" (to be read as: 'the "XX" requires "requirement" from the "YY"').

2) Management requirements from the N/EM on the FEs

These are the requirements for relationship 4 in figure 1. These requirements are first of all structured according to the FE to which they apply. Structuring in a second dimension is done according to OSI SMFAs.

The requirements from this group are described in clause 6.

Management requirements from the N/EM on the FEs				
	SSF	SRF	SCF	SDF
Fault management				
Configuration management				
Accounting management				
Performance management				
Security management				

Figure 4: The IN management functional requirements identification template for the requirements from the N/EM on the FEs

The use of the template in figure 4 is almost the same as for the template in figure 3. The main difference is that only one actor (the N/EM) is involved in managing the IN FE. The following steps should be made when using the template in figure 4:

- Identify for each OSI SMFA the management requirements that the N/EM puts upon each of the IN FE;
- Describe the management requirement identified following a notation that should:
  - support a uniform and brief notation (since only one actor is involved the notation of the requirements can be just a simple list);
  - be written as requirements from the N/EM on the IN FEs, e.g. the SSF should be able to receive trigger data.

5 IN functional management requirements between actors

This clause contains a description of all IN functional management requirements identified between the actors regarding IN-provided services in the scope of CS1 and CS2. The methodology and templates used are introduced in clause 5.

It is assumed that all management interactions between actors are secured by access control, authentication and security logging ITU-T Recommendations X.736 [18], X.740 [21] and X.7.41 [21]. Also, it should be possible to perform management interactions based on events ITU-T Recommendation X.734 [16] or based on a schedule ITU-T Recommendation X.746 [25].

5.1 Service subscriber - service manager

5.1.1 Needs analysis phase

No specific management requirements have been identified for the needs analysis phase. In this phase the service manager collects information from possible service subscribers in order to plan its services and to make an inventory of the (management) requirements that future subscribers have on the service. One of the results of the needs analysis phase will be a list of (service specific) management requirements that can be added to the generic management requirements that are already listed in this ETR.

5.1.2 Service creation phase

In the planning process all the subscriber requirements towards the service manager, resulting from the needs analysis phase as described in subclause 5.1.1, should be identified for impact on needed functionality.

5.1.3 Acceptance testing phase

In this phase a limited set of service subscribers will take part in a service pilot. For these subscribers, the service deployment and service utilisation phases are applied before the service acceptance phase is completed. Based on the acceptance test, a number of additional management requirements may arise.

5.1.4 Service provisioning and operation phase

Service type control activities.

SS-SM:

1) the SM should offer the SS one-stop-shopping, one-stop-billing and one-stop-complaining;
2) the SM should notify the SS of service changes;
3) the SM should notify the SS of an upcoming enabling/disabling of the service;
4) the SM should inform the SS on problems (foreseen) in the service.

Service provisioning.

SS-SM:

5) the SM should provide the SS with the capability to subscribe to a service;
6) the SM should inform the SS on the time the service will be / has been provided;
7) the SM should inform the SS on service usage details;
8) the SM should be able to receive (new or updated) subscriber data;
9) the SM should provide the SS with service configuration data;
10) the SM should provide the SS with service tariff data.

Service instance control activities.

SS-SM:

11) the SM should inform the SS on how to use the service;
12) the SM should provide the SS with the capability to (de)activate a service (e.g. for a specific user);
13) the SM should provide the SS with an overview of available services (functionality, price, etc.);
14) the SM should provide the SS with the capability to monitor and control his users specific data (e.g. limited control on user information and service profile);
15) the SM should provide the SS with the capability to restrict the use of a service to a specific charge, to specific users, etc.;
16) the SM should provide the SS with (customised) bills;
17) the SM should provide the SS with an indication of the cost of a particular call or a set of calls related to a service (before, during and/or after the call);
18) the SM should provide the SS with the capability to monitor the service performance (QoS, statistics).

Service instance withdrawal.

SS-SM:

19) the SM should provide the SS with the capability to unsubscribe from a service;
20) the SM should send the SS a final bill (accounts to be settled before service withdrawal);
21) the SM should inform the SS on the service removal;
22) the SM should inform the SS on alternative services.

5.2 Service user - service manager

5.2.1 Service provisioning and operation phase

Service invocation control activities.

SU-SM:

1) the SM should provide the SU with the capability to complain about a service (i.e. the SM should provide an access point to his service users for complaints);
2) the SM should provide the SU with the capability to monitor and control his specific data (e.g. limited control on his service profile);
3) the SM should provide the SU with the capability to monitor the service performance;
4) the SM should inform the SU on how to use the service;
5) the SM should provide the SS with the capability to change his user profile;
6) the SM should provide the SU with service tariffs and service usage metering data.

Service invocation activities.

The implementation to satisfy the management requirements for the service invocation activities can be made in service control systems or in the management systems.

SU-SM:

7) the SM should inform the SU on the service removal;
8) the SM should send the SU an indication of the cost of a particular call (before, during and/or after the call);
9) the SM should notify the SU of an upcoming enabling/disabling of the service;
10) the SM should notify the SU of problems in the service;
11) the SM should provide the SU with a forecast of possible problems in the service.

5.3 Service Manager (SM)- Network/Element Manager (N/EM)

In this subclause, the requirements between the SM and N/EM are indicated. In addition, resulting N/EM activities are mentioned. These activities are used as the basis to derive the requirements in clause 6.

5.3.1 Service creation phase

N/EM-SM:

1) the N/EM requests the SM to provide the following information:

    - expected service usage.

    On the basis of this, the N/EM will (be able to) configure and plan its network to support the expected service usage.

5.3.2 Acceptance testing phase

SM-N/EM:

1) the N/EM should provide the SM with the ability to test the service aspects of the created service in a non-operational environment.

5.3.3 Service deployment phase

SM-N/EM:

1) the N/EM should provide the SM with the ability to install and configure the service script (/software);
2) the N/EM should provide the SM with the ability to install and configure Service Management scripts (/software) (e.g. script for the introduction and allocation of subscriber specific data);
3) the N/EM should provide the SM with the ability to install and configure the service testing (for the provisioning of tests on line);
4) the N/EM should provide the SM with the ability to install and configure the service generic data;
5) the N/EM should provide the SM with the ability to install and configure specialised resource data;
6) the N/EM should provide the SM with the ability to set the target time and date the service should be enabled (service is pending);
7) the N/EM should send the SM reports on installation and configuration.

To meet these requirements the N/EM will:

- test the installed software;
- install and configure trigger data;
- install and configure signalling routing data;
- install and configure network elements;
- install and configure specialised resource data.

5.3.4 Service provisioning and operation phase

Service type control activities.

SM-N/EM:

1) the N/EM should notify the SM on faults in the network that may have impact on service availability;
2) the N/EM should provide the SM with a forecast on possible faults in the network that may have impact on service availability;
3) the N/EM should provide the SM with the ability to enable/disable (parts of) the service on a global (network wide) level;
4) the N/EM should provide the SM with information on network usage that may impact the service performance, such as traffic flow, performance, and throughput;
5) the N/EM should provide the SM with the ability to monitor and control (e.g. setting conditions on alarm reporting) service fault reporting;

6) the N/EM should provide the SM with the ability to perform customer oriented fault localisation and correction;
7) the N/EM should provide the SM with the ability to perform service oriented fault localisation and correction;
8) the N/EM should provide the SM with the ability to upgrade an existing service;
9) the N/EM should provide the SM with the ability to complain;
10) the N/EM should provide the SM with the ability to update service generic data;
11) the N/EM should provide the SM with the ability to update specialised resource data;
12) the N/EM should provide the SM with the ability to initialise and modify tariff information stored in the NEs;
13) the N/EM should provide the SM with the ability to perform a diagnostics service test.

To fulfil these requirements the N/EM will:

- monitor and control the performance/QoS of the NE and the whole network;
- enable/disable the use of the resources of the NE involved in the "service execution";
- re-allocate specialised resources (e.g. following QoS criteria);
- test the NE;
- update signalling routing data;
- update trigger data;
- update list of accountable events;
- generate, collect and store usage information (e.g. for accounting purposes).

Service provisioning.

SM-N/EM:

14) the N/EM should provide the SM with the ability to install and modify customer specific data in the network.

Service instance control activities & service invocation control activities.

SM-N/EM

15) the N/EM should be able to handle complaints from/via the SM on network/service malfunctioning;
16) the N/EM should be able to handle customer control requests (e.g. update customised announcements, change parameter settings, etc.) via the SM.

Service invocation activities.

SM-N/EM:

17) the N/EM should inform the SM on the usage of the service per SS and per service (feature) e.g. for billing (e.g. via usage records).

Service instance withdrawal.

SM-N/EM:

18) the N/EM should provide the SM with the ability to remove customer data from the network.

5.3.5 Service removal phase

SM-N/EM:

1) the N/EM should provide the SM with the ability to remove service management scripts (/software);
2) the N/EM should provide the SM with the ability to remove the service script (/software);
3) the N/EM should provide the SM with the ability to remove the service testing;
4) the N/EM should provide the SM with the ability to remove the service generic data;
5) the N/EM should provide the SM with the ability to remove specialised resource data;
6) the N/EM should provide the SM with reports on the removing actions;
7) the N/EM should provide the SM with the ability to set the target time and date the service should be disabled.

To fulfil these requirements the N/EM will:

- remove the installed software;
- remove trigger data;
- remove signalling routing data;
- remove network elements;
- remove specialised resource data.

6 IN functional management requirements from the Network/Element Manager (N/EM) on the Functional Entities (FEs)

This clause contains a description of all IN functional management requirements identified from the N/EM regarding the IN functional entities in the scope of CS1 and CS2. The methodology and templates (to be) used are introduced in clause 5.

6.1 General

1) It should be possible to schedule management activities according to the scheduling function, ITU-T Recommendation X.746 [25].
2) The FEs should have the capability of forwarding event notifications based on the crossing of thresholds, ITU-T Recommendation X.731 [13].
3) The FEs should support logging and filtering of events [ITU-T Recommendations X.734 [16] and X.735 [17].
4) It should be possible to perform management actions based on the exceeding of thresholds, ITU-T Recommendation X.734 [16].

6.1.1 Fault management

1) Send alarms in cases of malfunctioning, ITU-T Recommendation X.733 [15].
2) Support logging and filtering of alarms.

6.1.2 Configuration management

1) Support of the Software Management Function, ITU-T Recommendation X.744 [24] to install data/logic in the FEs.
2) The FE should support the reporting of creation and deletion of managed objects and the changing of attributes of managed objects (ITU-T Recommendations X.730 [12] and X.732 [14]).

6.1.3 Accounting management

1) Support Usage Metering Function for the collection of accounting information ITU-T Recommendation X.742 [23].

NOTE: No decision has been made on which FE will be responsible for generating (part of) the accounting information. Therefore, this requirement is listed in the general section and is meant to apply to any FE that generates accounting information.

6.1.4 Performance management

1) Monitor the load of FEs, ITU-T Recommendation X.739 [20].
2) Route the traffic towards an alternative FE in case of overload.
3) Display statistics:
   - use of service (e.g. number of calls per day);
   - processing load;
   - load of communication lines.
4) Support logging and filtering of performance events.

ITU-T Recommendation Q.822 [8] contains more information on this subject.

6.1.5 Security management

1) Support access control, authorisation, authentication, logging and non repudiation for management operations, ITU-T Recommendations X.736 [18], X.740 [21] and X.741 [22].

6.2 Service Switching Function (SSF)

6.2.1 General

ITU-T Recommendation Q.1214 [7] subclause 4.2 identifies entities/components and data related to the SSF which have to be managed.

6.2.2 Fault management

1) Report automatic restoration.

6.2.3 Configuration management

1) Download and remove trigger data.
2) Modify trigger data.
3) Trigger data to be set per trigger:
   - trigger type;
   - routing to SCF;
   - service key;
   - congestion control (what to do in case of SCF overload):
     - termination of call;
     - play announcement;
     - alternative routing.
4) Block/unblock trigger tables.

6.2.4 Accounting management

See note in subclause 6.1.3.

6.2.5 Performance management

1) Monitor call gapping, e.g.:
   - number of calls blocked per call gap;
   - number of calls blocked per call gap type.
2) Manage (get/set) parameters per call gap:
   - type of call gapping (e.g. manual, SCF overload, destination overload);
   - status of call gap (e.g. active, passive);
   - criteria for call gap (e.g. calling region, called region, calling party, called party);
   - gapping duration interval;
   - treatment given to gapped calls (e.g. play announcement, busy tone).
3) Traffic measurements (maybe per service), such as:
   - number of unsuccessful call attempts due to caller abandon, SCF failure or SSF failure;
   - number of successful calls;
   - number of queries sent to SCF;
   - average waiting time per call.

6.2.6 Security management

No specific requirements identified.

6.3 Specialised Resource Function (SRF)

6.3.1 General

ITU-T Recommendation Q.1214 [7] subclause 4.3 identifies entities/components and data related to the SRF which have to be managed.

6.3.2 Fault management

1) Report current alarm summary.
2) Route current alarm summary.

6.3.3 Configuration management

1) Store/retrieve/delete messages (all or a selected set).
2) Set/retrieve prompt and collect user information parameters.
3) Convert message to other media (speech, data, image) or language.
4) Set/retrieve internal SRF purging criteria.
5) Download and remove announcements.
6) Update announcement.
7) Activate/deactivate an announcement.
8) Specify whether an announcement may be interrupted or not by digit reception.
9) Overview of subscriber/user initiated activities (subscriber control) (audit trail), for example: number of discarded entries during digit collection, number of digit collection time outs.

6.3.4 Accounting management

See note in subclause 6.1.3.

6.3.5 Performance management

1) Generate statistics related to an announcement:
   - number of times an announcement is used;
   - number of times "prompt and collect user information" is used;
   - number of failures to get user information due to time-out.
2) Generate statistics on the usage of the SRF.

6.3.6 Security management

1) Set/retrieve access control parameters for user/subscriber access to SRF procedures.

6.4 Service Control Function (SCF)

6.4.1 General

ITU-T Recommendation Q.1214 [7] subclause 4.4 identifies entities/components and data related to the SCF which have to be managed.

6.4.2 Fault management

1) Report current alarm summary.
2) Route current alarm summary.

6.4.3 Configuration management

1) Perform version management for Service Logic Programs (SLP), ITU-T Recommendation X.744 [24].
2) Download and remove SLPs.

6.4.4 Accounting management

See note in subclause 6.1.3.

6.4.5 Performance management

1) Control (incl. enabling/disabling) over call gapping activities of the SCF.
2) Statistics on invocation of an SLP.
3) Traffic measurements, such as:
   - number of operations from SSF;
   - number of operations from SSF completed;
   - number of operations from SRF;
   - number of operations from SRF completed.

6.4.6 Security management

No specific requirements identified.

6.5 Service Data Function (SDF)

6.5.1 General

ITU-T Recommendation Q.1214 [7] subclause 4.5 identifies entities/components and data related to the SDF which have to be managed.

6.5.2 Fault management

1) Report current alarm summary.
2) Route current alarm summary.

6.5.3 Configuration management

1) Downloading and removal of service generic data.
2) Downloading and removal of subscriber/customer data.
3) Updating subscriber/customer data (changed through TMN).
4) Receive notification on updates of subscriber/customer data performed through IN (i.e. CPM).

6.5.4 Accounting management

See note in subclause 6.1.3.

6.5.5 Performance management

1) Statistics on access of service data.
2) Traffic measurements, such as:
   - number of "update date" received from SCF;
   - number of "update date" received from SCF and successfully completed;
   - number of queries received from SCF;
   - number of queries received from SCF and successfully completed.

6.5.6 Security management

No specific requirements identified.

History

Document history	
August 1995	First Edition
February 1996	Converted into Adobe Acrobat Portable Document Format (PDF)

ISBN 2-7437-0214-1
Dépôt légal : Août 1995