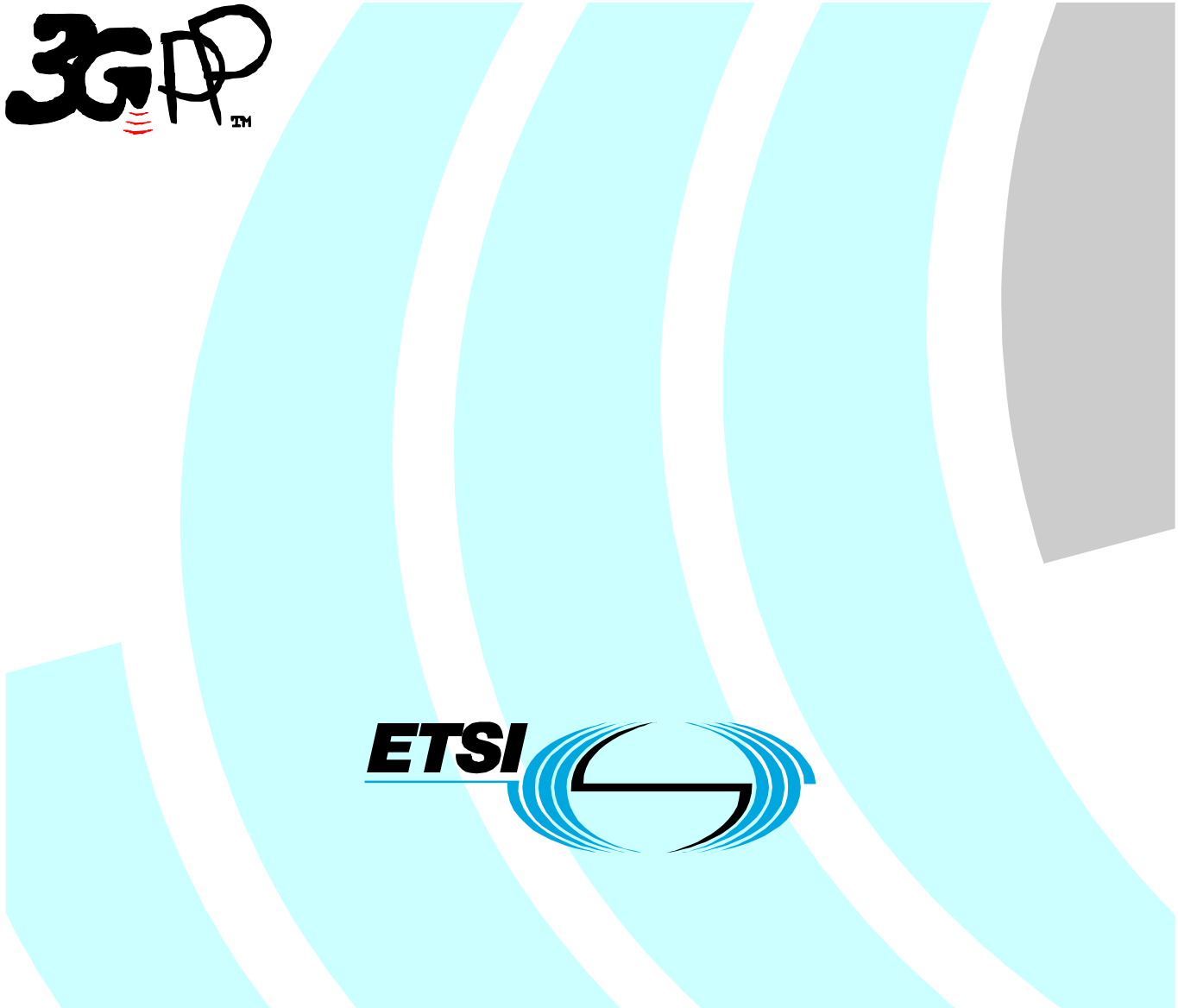
ETSI TS 132 101 V6.1.0 (2004-12)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
Telecommunication management;
Principles and high level requirements
(3GPP TS 32.101 version 6.1.0 Release 6)



Reference
RTS/TSGS-0532101v610

Keywords
UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

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

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

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

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp .

Contents

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (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 the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater 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 document.

1 Scope

The present document establishes and defines the management principles and high-level requirements for the management of PLMNs.

In particular, the present document identifies the requirements for:

- the upper level of a Management System;
- the reference model, showing the elements the Management System interacts with;
- the network operator processes needed to run, operate and maintain a network;
- the functional architecture of the Management System;
- the principles to be applied to Management Interfaces.

The requirements identified in the present document are directed to the further development of Management specifications as well as the development of Management products. The present document can be seen as guidance for the development of all other Technical Specification addressing the management of PLMNs.

The present document does not provide physical architectures of the Management System. These aspects are defined and discussed in more detail in TS 32.102 [101].

Verbal forms used to indicate requirements in the present document (e.g. "shall", "should", "may") are used in compliance with 3GPP specification Drafting Rules TR 21.801 [104].

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] ITU-T Recommendation M.3010 (2000): "Principles for a telecommunications management network".

[2] 3GPP TS 22.101: "Service aspects; Service Principles".

[3] 3GPP TS 32.111-1: "Telecommunication management; Fault Management; Part 1: 3G fault management requirements".

[4] IETF RFC 959: "File Transfer Protocol (FTP)"; October 1985, J. Postel, J. Reynolds, ISI. (Status: Standard).

[5] IETF RFC 783: "Trivial File Transfer Protocol (TFTP)"; rev. 2, June 1981, K.R. Sollins MIT. (Status: Unknown).

[6] IETF RFC 1157: "Simple Network Management Protocol (SNMP)": May 1990, J. Case, SNMP Research, M. Fedor, Performance Systems International, M. Schoffstall, Performance Systems International, J. Davin, MIT Laboratory for Computer Science. (Status: Standard).

[7] IETF RFC 2401: "Security Architecture for the Internet Protocol"; November 1998. (Status: Proposed Standard).

[8] The Object Management Group (OMG) "The Common Object Request Broker: Architecture and Specification", Revision 2.3, June 1999.
http://www.omg.org/technology/documents/vault.htm#CORBA_IIOP

[9] ITU-T Recommendation Q.811 (1997): "Lower Layer Protocol Profiles for the Q3 Interface and X interfaces".

[10] ITU-T Recommendation Q.812 (1997): "Upper Layer Protocol Profiles for the Q3 Interface and X interfaces".

[11] ITU-T Recommendation X.650 (1996): "Information Technology - Open Systems Interconnection - Basic Reference Model: Naming and Addressing".

[12] ITU-T Recommendation X.700 (1992): "Management Framework for Open Systems Interconnection (OSI) for CCITT applications".

[13] ISO 8571-1 (1988): "Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management - Part 1: General Introduction".

[14] ISO 8571-2 (1988): "Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management - Part 2: Virtual Filestore Definition".

[15] ISO 8571-3 (1988): "Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management - Part 3: File Service Definition".

[16] ISO 8571-4 (1988): "Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management - Part 4: File Protocol Specification".

[17] ISO/IEC ISP 10607-1 (1995): "Information technology - International Standardized Profiles AFTnn - File Transfer, Access and Management - Part 1: Specification of ACSE, Presentation and Session Protocols for the use by FTAM".

[18] ISO/IEC ISP 10607-2 (1995): "Information technology - International Standardized Profiles AFTnn - File Transfer, Access and Management - Part 2: Definition of Document Types, Constraint sets and Syntaxes".

[19] ISO/IEC ISP 10607-3 (1995): "Information technology - International Standardized Profiles AFTnn - File Transfer, Access and Management - Part 3: AFT 11 - Simple File Transfer Service (Unstructured)".

[20] ITU-T Recommendation X.710 (1997): "Information Technology - Open Systems Interconnection - Common Management Information Service".

[21] ITU-T Recommendation X.711 (1997): "Managed objects for diagnostic information of public switched telephone network connected V-series modem DCE's".

[22] ITU-T Recommendation X.25 (1996): "Interface between Data Terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE) for Terminals operating in the Packet Mode and connected to Public Data Networks by Dedicated Circuit".

[23] ISO/IEC ISP 11183-1 (1992): "Information technology - International Standardized Profiles AOM1n.OSI Management - Management Communications - Part 1: Specification of ACSE, presentation and session protocols for the use by ROSE and CMISE".

[24] ISO/IEC 9545:1994: "Information technology - Open Systems Interconnection - Application Layer Structure".

[25] ITU-T Recommendation X.200 (1994): "Information Technology - Open Systems Interconnection - Basic Reference Model: The Basic Model".

[26] ITU-T Recommendation X.208 (1988): "Specification of Abstract Syntax Notation One (ASN.1)".

[27] ITU-T Recommendation X.209 (1988): "Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)".

[28] ITU-T Recommendation X.210 (1993): "Information Technology - Open Systems Interconnection - Basic Reference Model: Conventions for the definition of OSI Services".

[29] ITU-T Recommendation X.211 (1995): "Information Technology - Open Systems Interconnection - Physical Service Definition".

[30] ITU-T Recommendation X.212 (1995): "Information Technology - Open Systems Interconnection - Data link Service Definition".

[31] ITU-T Recommendation X.213 (1995): "Information Technology - Open Systems Interconnection - Network Service Definition".

[32] ITU-T Recommendation X.223 (1993): "Use of X.25 to provide the OSI Connection-mode network service for ITU-T applications".

[33] ITU-T Recommendation X.214 (1995): "Information Technology - Open Systems Interconnection - Transport Service Definition".

[34] ITU-T Recommendation X.224 (1995): "Information Technology - Open Systems Interconnection - Protocol for providing the connection-mode transport service".

[35] ITU-T Recommendation X.215 (1995): "Information Technology - Open Systems Interconnection - Session Service Definition".

[36] ITU-T Recommendation X.225 (1995): "Information Technology - Open Systems Interconnection - Connection-oriented session protocol: Protocol specification".

[37] ITU-T Recommendation X.216 (1994): "Information Technology - Open Systems Interconnection - Presentation Service Definition".

[38] ITU-T Recommendation X.226 (1994): "Information Technology - Open Systems Interconnection - Connection-oriented presentation protocol: Protocol specification".

[39] ITU-T Recommendation X.217 (1995): "Information Technology - Open Systems Interconnection - Service definition for the association control service element".

[40] ITU-T Recommendation X.227 (1995): "Information Technology - Open Systems Interconnection - Connection-oriented protocol for the association control service element: Protocol specification".

[41] ITU-T Recommendation X.219 (1988): "Remote Operations: Model, Notation and Service Definition".

[42] ITU-T Recommendation X.229 (1988): "Remote Operations: Protocol Specification".

[43] ISO/IEC 7776 (1995): "Information technology - Telecommunications and information exchange between systems - High-level data link control procedures - Description of the X.25 LAPB-compatible DTE data link procedures".

[44] ISO/IEC 8208 (2000): "Information technology - Data communications - X.25 Packet Layer Protocol for Data Terminal Equipment".

[45] ISO/IEC 8878 (1992): "Information technology - Telecommunications and information exchange between systems - Use of X.25 to provide the OSI Connection-mode Network Service".

[46] IETF RFC 1006: "ISO Transport on top of the TCP", Marshall T. Rose, Dwight E. Cass, Northrop Research and Technology Center, May 1987. Status: Standard.

[47] IETF RFC 793: "Transmission Control Protocol (TCP)", September 1981. Status: Standard.

[48] IETF RFC 791: "Internet Protocol (IP)", September 1981. Status: Standard.

[49] ITU-T Recommendation X.680 (2002): "Information Technology-Abstract Syntax Notation One (ASN.1): Specification of Basic Notation".

[50] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[51] 3GPP TS 22.115: "Service aspects; Charging and Billing".

[52] The Object Management Group (OMG) "The Common Object Request Broker: Architecture and Specification", Revision 2.1, August 1997. http://www.omg.org/technology/documents/vault.htm#CORBA_IIOP

[53] 3GPP TS 32.400-series: "Telecommunication management; Performance Management (PM); Concept and requirements".

[54] 3GPP TS 32.600: "Telecommunication management; Configuration Management (CM); Concept and high-level requirements".

[55] 3GPP TS 32.200: "Telecommunication management; Charging management; Charging principles".

[56] 3GPP TR 22.121: "Service aspects; The Virtual Home Environment; Stage 1".

[57] 3GPP TS 32.140 : "Telecommunication management; Subscription Management (SuM) requirements".

[58] 3GPP TS 32.141: "Telecommunication management; Subscription Management (SuM) Architecture".

[59 to 99] Void

[100] TMF GB910: "Telecom Operations Map"; Approved Version 2.1 March 2000, (may be downloaded from http://www.tmforum.org.).

[101] 3GPP TS 32.102: "3G Telecom Management Architecture".

[102] ITU-T Recommendation M.3013 (2000): "Considerations for a telecommunications management network".

[103] Void.

[104] 3GPP TR 21.801: "Specification Drafting Rules".

[105] TMF GB910B: "Telecom Operations Map Application Note-Mobile Services: Performance Management and Mobile Network Fraud and Roaming Agreement Management"; Public Evaluation Version 1.1, September 2000. (May be downloaded free from http://www.tmforum.org.)

3 Definitions and abbreviations

3.1 Definitions

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

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 and Sub-Network Management Functions.

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.

Enterprise Systems: Information Systems that are used in the telecommunication organisation but are not directly or essentially related to the telecommunications aspects (Call Centre's, Fraud Detection and Prevention Systems, Invoicing etc).

Information Object: entity used to encapsulate information when modelling a network resource or a support object. The encapsulation has the form of "object classes". It is composed of a name, attributes, relationship and may support notifications and operations. Information Object Classes are independent from the specific implementation of the interface. Information objects are the only objects used to describe Information Services.

Information Service: describes the information related to the entities (either network resources or support objects) to be managed and the way that the information may be managed for a certain functional area (e.g. the Alarm IRP Information Service in the fault management area). Information Services can be defined for IRPs as well as for NRMs.

IRP (Integration Reference Point): an architectural concept that is described by a set of specifications for definition of a certain aspect of the Itf-N, comprising a **Requirements** specification, an **IRP Information Service** specification, and one or more **IRP Solution Set** specifications.

IRP Information Model: a **technology/protocol independent model** (information objects and/or interactions) of an IRP Information Service.

IRP Information Service (IS): an Information Service describes the information related to the entities (either network resources or support objects) to be managed and the way that the information may be managed for a certain functional area (e.g. the Alarm IRP Information Service in the fault management area). Information Services are defined for all IRPs.

IRP Solution Set (SS): contains a mapping of the IRP Information Service (IS) to one of several technologies. An IS can be mapped to several different Solution Sets. Different technology selections may be made for different IRP Information Services. The functionality and information specified in a Solution Set is constrained by the functionality and information specified in the associated Information Service.

Managed Object: entity used to represent information in a Solution Set. The Managed Objects (MO) are obtained as the result of a mapping exercise of Information Objects defined in IS, taking into account some engineering choices and technology specificity.

Management Infrastructure: the collection of systems (computers and telecommunications) a PLMN Organisation has in order to manage its network.

Network Element (NE): 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 Model (NRM): an Information Service describing Information Object Classes representing the manageable aspects of network resources, e.g. an RNC or NodeB.

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

Public Land Mobile Network (PLMN): see 3GPP TR 21.905 [50].

PLMN Organisation: legal entity that is involved in the management of a telecommunications network providing mobile cellular services.

Sub-Network Management Functions: functions 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).

Support object: object that represents a particular capability, introduced to model a service. As an example of support object, for the Alarm IRP Information Service there is the "alarm information" and "alarm list".

3.2 Abbreviations

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

API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
B2B	Business to Business
B-ISDN	Broadband ISDN

BOOTP	Boot protocol
CLI	Command Line Interface
CMIP	Common Management Information Protocol
CMIP/GDMO	Common Management Information Protocol/Guidelines for the Definition of Managed Objects
COPS	Common Open Policy Service
COPS-PR	COPS Usage for Policy Provisioning
CORBA IIOP	Common Object Request Broker Architecture Internet Inter-ORB Protocol
CORBA	Common Object Request Broker Architecture
CORBA/IDL	Common Object Request Broker Architecture/Interface Definition Language
DCN	Data Communications Network
DECT	Digital Enhanced Cordless Telecommunications
DHCP	Dynamic Host Configuration Protocol
DNS	Directory Name Service
DSS1	Digital Subscriber System 1
EM	Element Manager
EMS	Element Management System
FFS	For Further Study
FTAM	File Transfer Access and Management
FTP	File Transfer Protocol
ftp	FTP
GDMO	Guidelines for the Definition of Managed Objects
GGSN	Gateway GPRS Support Node
Go interface	The interface between the GGSN and the Policy Decision Function (PDF)
GSM	Global System for Mobile communications
HLR	Home Location Register
HSS	Home Subscriber Server
IDL	Interface Definition Language
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IN	Intelligent Network
INAP	Intelligent Network Application Part
IRP	Integration Reference Point
IS	Information Service
ISDN	Integrated Services Digital Network
LDAP	Lightweight Directory Access Protocol
LDUP	LDAP Duplication/Replication/Update Protocols
LLA	Logical Layered Architecture
MAP	Mobile Application Part
MExE	Mobile Execution Environment
MIB	Management Information Base
MMI	Man-Machine Interface
NM	Network Manager
NMS	Network Management System
NRM	Network Resource Model
OAM&P	Operations, Administration, Maintenance and Provisioning
OS	Operations System
OSI	Open Systems Interconnection
OSS	Operations Support System
PDF	Policy Decision Function
PDH	Plesiochronous Digital Hierarchy
PDP	Policy Decision Point
PIB	Policy Information Base
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RNC	Radio Network Controller
RSVP	Resource ReserVation Protocol
SDH	Synchronous Digital Hierarchy
sftp	secure ftp
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol (IETF)

SNMP/SMI	SNMP/Structure of Management Information
SOM	Service Operations Management
SS	Solution Set
SS7	Signalling System No. 7
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/ Internet Protocol
tftp	trivial ftp
TM	Telecom Management
TMF	TeleManagement Forum
TMN	Telecommunications Management Network (ITU-T)
TOM	Telecom Operations Map (TMF)
UML	Unified Modelling Language
UPT	Universal Personal Telecommunication
USIM	Universal Subscriber Identity Module
UTRA	Universal Terrestrial Radio Access
VHE	Virtual Home Environment

4 General

4.1 PLMN Telecom Management

4.1.1 Basic objectives for PLMN management

The requirements and decomposition of Telecom Management for 3G do not differ radically from that of 2G systems. The following basic objectives to be supported by the management specifications have been identified:

- to be capable of managing equipment supplied by different vendors including the management systems themselves.
- to minimise the complexity of PLMN management.
- to provide the communication between Network Elements (NEs) and Operations Systems (OS) or between OSs themselves via standardised interfaces (e.g. CMIP, CORBA, SNMP, etc.) as appropriate and necessary.
- to minimise the costs of managing a PLMN such that it is a small component of the overall operating cost.
- to provide configuration capabilities that are flexible enough to allow rapid deployment of services.
- to provide integrated Fault Management capabilities.
- to simplify maintenance interventions by supporting remote maintenance operations.
- to allow interoperability between Network Operators/Service Providers for the exchange of management/charging information. This includes interoperability with other networks and services (e.g. ISDN/B-ISDN, PSTN and UPT) as well as other PLMNs.
- to enable the support and control of a growing number of resources. This would allow the system to start from a small and simple configuration and grow as needed, both in size and complexity.
- to re-use existing relevant standards (e.g. GSM, IN, ISDN/B-ISDN, ITU-T, TMF etc.) where applicable.
- to support the security management of PLMNs (e.g. key management, access control management, operation and administration of security mechanisms) with particular emphasis on new features such as automatic roaming and packet switched services.
- to provide and support a flexible billing and accounting administration, to support charging across PLMNs.
- to address the management and assessment of system performance and operation through the use of common measurements, etc. This would enable a Network Operator/Service Provider to assess actual performance against planned targets.

- to expose any information only once.
  (Example: In case an operator would like to change one parameter in a cell: Then all occurrences of this parameter, e.g. transceiver frequency, hand-over relationships, performance measurements, frequency hopping control, etc., should be changed by one action only.)

- to support the restoration of an Operations System (e.g. resynchronisation and atomic transactions).

- to have one (1) name convention for network resources under management in the 3GPP context. 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.

It is acknowledged that the introduction of new architecture to support new services or the introduction of new services themselves may impact the detailed requirements of some or all of the above.

4.1.2 3GPP reference model

A 3GPP System is made of the following components:

- one or more Access Networks, using different types of access techniques (GSM, UTRA, DECT, PSTN, ISDN, ...) of which at least one is UTRA;

- one or more Core Networks;

- one or more Intelligent Node Networks service logic and mobility management, (IN, GSM ...);

- one or more transmission networks (PDH, SDH etc.) in various topologies (point-to-point, ring, and point-to-multi-point...) and physical means (radio, fibre and copper ...).

The 3GPP system components have signalling mechanisms among them (DSS1, INAP, MAP, SS7, RSVP,...).

From the service perspective, the 3GPP system is defined to offer:

- Service support transparent to the location, access technique and core network, within the bearer capabilities available in one particular case;

- User to terminal and user to network interface (MMI) irrespective of the entities supporting the services required (VHE);

- Multimedia capabilities.

4.1.3 3GPP provisioning entities

TS 22.101 "Services Principles" [2] identifies two major entities, which cover the set of 3GPP functionalities involved in the provision of the 3GPP services to the user. These are:

Home Environment: This entity holds the functionalities that enable a user to obtain 3GPP services in a consistent manner regardless of the user's location or the terminal used;

Serving Network: This entity provides the user with access to the services of the Home Environment.

4.1.4 Management infrastructure of the PLMN

Every PLMN Organisation has its own management infrastructure. Each management infrastructure contains different functionality depending on the role-played and the equipment used by that PLMN Entity.

However, the core management architecture of the PLMN Organisation is very similar. Every PLMN Organisation:

- provides services to its customers;

- needs an infrastructure to fulfil them (advertise, ordering, creation, provisioning ...);

- assures them (Operation, Quality of Service, Trouble Reporting and Fixing ...);

- bills them (Rating, Discounting ...).

Not every PLMN Organisation will implement the complete Management Architecture and related Processes. Some processes may be missing dependent on the role a particular Organisation is embodying. Processes not implemented by a particular Organisation are accessed via interconnections to other organisations, which have implemented these processes (called X-interfaces in the ITU-T TMN architecture).

The Management Architecture itself does not distinguish between external and internal interfaces.

4.2 ITU-T TMN

ITU-T TMN (Telecommunications Management Network standard from the ITU-T), as defined in ITU-T Recommendation M.3010 [1], provides:

- an architecture, made of OS (Operations Systems) and NEs (Network Elements), and the interfaces between them (Q, within one Operator Domain and X, between different Operators);
- the methodology to define those interfaces;
- other architectural tools such as LLA (Logical Layered Architecture) that help to further refine and define the Management Architecture of a given management area;
- a number of generic and/or common management functions to be specialised/applied to various and specific ITU-T TMN interfaces.

The PLMN Management Architecture is based on ITU-T TMN, and will reuse those functions, methods and interfaces already defined (or being defined) that are suitable to the management needs of a PLMN.

Another management approach that is employed is the Telecom Operations Map from TeleManagement Forum (TMF). The Telecom Operations Map, using the TMN model as a foundation, addresses operation support and management for any communications service from a top down customer oriented standpoint.

5 Architectural framework

5.1 Management Reference Model and Interfaces

5.1.1 Overview

Figure 1 illustrates the Management Reference Model. It shows the Operation System interfacing with other systems.

The present document (and the rest of the 3GPP Management detailed specifications) addresses the Operations System (function and architecture wise) and the interfaces to the other systems (information and protocol wise).

The present document does not address the definition of any of the systems, which the Operations System may interface to. The rest of the 3GPP specifications regarding Management will not cover them either.

It is not the approach (nor it is possible) to re-define the complete management of all the technologies that might be used in the provision of a PLMN. However, it is the intention to identify and define what will be needed from the perspective of management.

A number of management interfaces in a PLMN are identified in figure 1, namely:

1) between the Network Elements (NEs) and the Element Manager (EM) of a single PLMN Organisation;
2) between the Element Manager (EM) and the Network Manager (NM) of a single PLMN Organisation;

NOTE: In certain cases the Element Manager functionality may reside in the NE in which case this interface is directly from NE to Network Manager). These management interfaces are given the reference name Itf-N and are the primary target for standardization.

3) between the Network Managers and the Enterprise Systems of a single PLMN Organisation;
4) between the Network Managers (NMs) of a single PLMN Organisation;

5) between Enterprise Systems & Network Managers of different PLMN Organisations;

6) between Network Elements (NEs).

The present document focuses primarily on management interfaces of Type 2 and to a lesser extent on management interfaces of Type 1 from the above list, while interfaces of Types 3 & 5 will be identified in the present document. Detailed specification of these interfaces is For Further Study (FFS). Interfaces of type 4 & 6 are beyond the scope of standardisation.

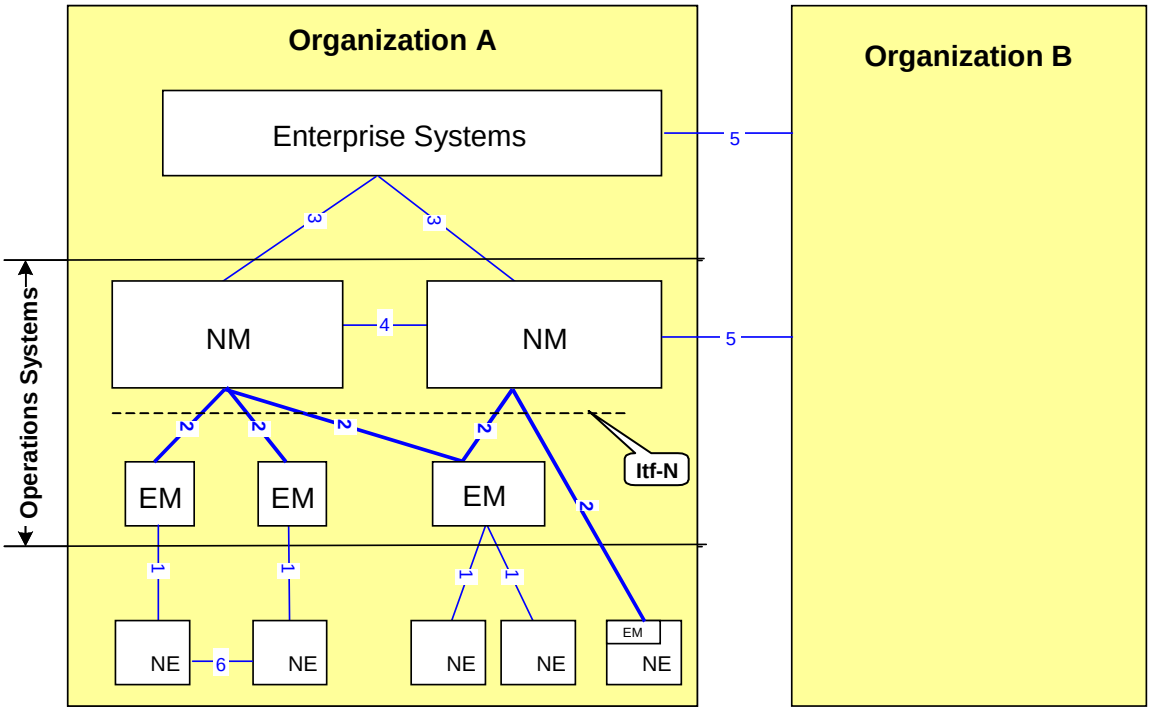


Figure 1: Management System Interactions

5.1.2 Interfaces from Operations Systems to NEs (Type 1 & 2)

In some cases, the management interfaces to NEs have been defined bottom-up, trying to standardise the complete OAM&P functionality of the various NEs.

For PLMN management, a top-down approach will be followed to streamline the requirements from the perspective of Operators top priority management processes.

It is assumed that this will not fully cover the OAM&P functionality of all NE types at once; therefore a part of the functionality will be phased for further work and consideration. Some proprietary solutions (local and/or remote) will be needed in the interim. The rationale of this approach is not only the best use of resources, but also to follow a pragmatic step-wise approach that takes into account the market forces (the manufacturers and operators capabilities). A further rationale is to define clear and easy-to-agree steps that allow Management functionality to be implemented in the same time frame as the telecom functionality in the network (i.e. to synchronise the management and network releases).

The approach for NE Management Interfaces will be to concentrate on protocol independent information models, allowing a mapping to several protocol suites. The rational is:

- due to the convergence of Information and Telecommunication technologies, it is required to work on a more open approach (acknowledging the market status and foreseen evolutions);
- the life cycle of information flows is 10 to 20 years, while that of protocols is 5 to 10 years;
- developments in automatic conversion from information models to various protocols/technologies will allow a more pragmatic and open approach (e.g. UML to GDMO, UML to IDL).

However, it is the intention to a least recommend one mapping for each interface.

5.1.2.1 Interfaces from EM Operations Systems to NEs (Type 1)

The approach for NE Management Interfaces of Type 1 will be to allow the use of certain Management Application Protocol Suites (see Annex A for a list of Management Protocol Suites).

5.1.2.2 Interfaces from NM Operations Systems to NEs (Type 2)

The approach for NE Management Interfaces of Type 2 will be to concentrate on protocol independent information models, allowing a mapping to several protocol suites. The rational is:

- due to the convergence of Information and Telecommunication technologies, it is required to work on a more open approach (acknowledging the market status and foreseen evolutions);
- the life cycle of information flows is 10 to 20 years, while that of protocols is 5 to 10 years;
- developments in automatic conversion from information models to various protocols/technologies will allow a more pragmatic and open approach (e.g. UML to GDMO, UML to IDL).

However, it is the intention to a least recommend one mapping for each interface.

Figure 2 shows the management interfaces of one part of the 3GPP System (the Radio Network), by way of illustration of interfaces of types 1 and 2.

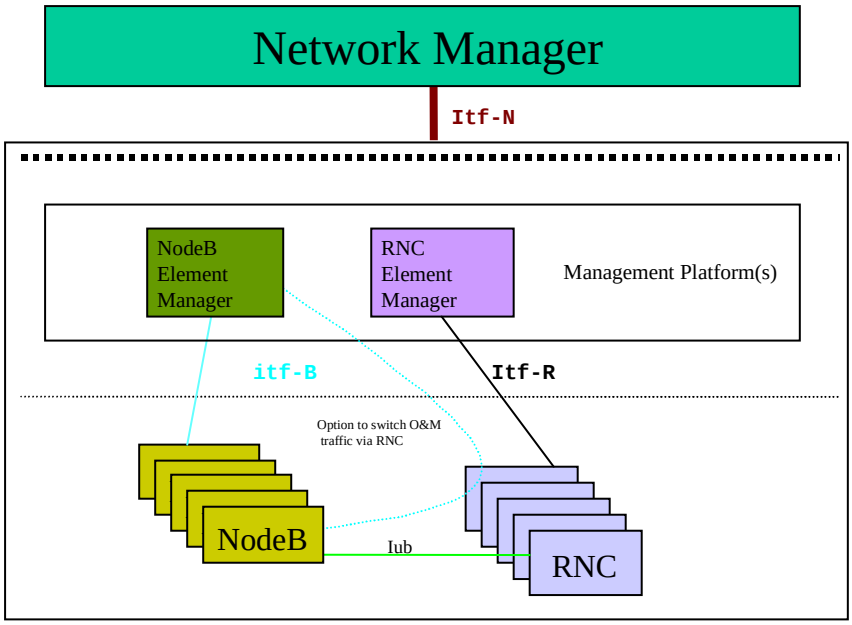


Figure 2: Radio Network Management Interfaces

Figure 2 identifies the following Management Interfaces:

- Itf-B - between Node B & its Manager (physically, this may be a direct connection or via the RNC) (type 1).
- Itf-R - between RNC & its Manager (type 1).
- Itf-N – between the Network (Element Manager or NEs with an embedded EM) & Network Manager (type 2).

5.1.3 Interfaces to Enterprise Systems (Type 3)

The approach is to define a Management structure that fully fits into the enterprise process needs of the PLMN Organisations. One of the essential issues of today's way of running telecommunications businesses is integral operation (e.g. customer care, from service subscription to billing, from order fulfilment to complaint management).

Enterprise Systems are those Information Systems that are used in the telecommunication organisation but are not directly or essentially related to the telecommunications aspects (Call Centres, Fraud Detection and Prevention Systems, Invoicing etc.).

Standardising Enterprise Systems is out of the scope of 3GPP work, since it involves many operator choices (organisational, etc.) and even regulatory. Also Enterprise Systems are often viewed as a competitive tool. However, it is essential that the requirements of such systems are taken into account and interfaces to the Operations Systems are defined, to allow for easy interconnection and functional support.

5.1.4 Interfaces to Operations Systems in other Organisations (Type 5)

PLMN Management considers integrally the interaction with the Operations Systems of other legal entities for the purpose of providing Mobile services.

There are two major types of interfaces to other management systems:

1) To the Operations Systems of another PLMN Organisation;

2) To the Operations Systems of a non-PLMN Organisation .

The first type deals with co-operation to provide Mobile services across a number of PLMN networks (e.g. roaming related interactions). The second type deals with client-server relationship to other operators (e.g. to leased lines providers, to added value service providers, etc.).

The approach that will be followed is to identify and define integral processes, not taking into account in the first step, how many operators or operations systems might be involved, but rather concentrating on the interactions between them (i.e. assuming an operator encompasses all functionalities). A further step will be to consider and define extra requirements (security, confidentiality etc.) when part of the process involves interactions with other operators Operations Systems (OSs).

5.1.5 Inter-NE Interfaces (Type 6)

Interfaces between Network Elements are sometimes used to carry management information even though this may not be the primary purpose of the interface. An example in a 3G network is the I_{ub} interface between Node-B and RNC (see figure 2 above). This type of interface is not within the scope of this specification, though potential impacts upon it should be considered.

5.2 Interface levels

5.2.1 Overview

The Management interfaces are studied here from five different perspectives or levels:

1) Logical (information model and flows used in the relationship manager-agent, or equivalent);

2) Solution Set (SS) Level;

3) Application protocol (end-to-end, upper layers protocol running between manager-agent, or equivalent);

4) Networking protocol (lower layer protocols carrying the information in/out the manager and agent, or equivalents);

5) Physical (mapping of the manager and agent, or equivalents, roles into physical entities).

5.2.2 Logical level

This level covers the mutual and conceptual knowledge of entities being connected by a given interface.

For type 2 interfaces (such as Itf-N in Figure 2 above) interactions at this level are fully standardised by 3GPP in terms of protocol independent Network Resource Models (static information definition) and IRP Information Services (information flows) where available. These protocol-independent Network Resource Models and IRP Information Services are hereafter referred to as IRP Information Models (Integration Reference Point Information Models).

5.2.3 Solution Set (SS) level

For an IRP Information Model at the logical level there will be at least one Solution Set defined. A Solution Set is a mapping of the Information Service to one of several technologies (for a full definition refer to subclause 3.1).

See annex C for the valid 3GPP Management IRP Solution Sets (see also ITU-T Recommendation M.3013-2000 [102]).

5.2.4 Application Protocol level

This level covers the set of primitives used to pass information across a given interface and the means to establish associations between the application entities (including the related addressing aspects) across a given interface.

Generally, the Application Protocol Suite used for the interaction between entities across a given interface is optional within the valid 3GPP Management Application Protocol Suites (see Annex A for a list of 3GPP Management Protocol Suites). However, in the case of interfaces of type 2 (such as Itf-N in figure 2 above) at least one of those protocol suites will be chosen as the standard protocol suite.

5.2.5 Networking Protocol level

Whatever standardised protocol suite at the networking level that is capable of meeting the functional and operational requirements (including the network addressing aspects) of the Logical and Application Protocol levels of a given management interface, is a valid Networking Protocol for that interface.

A number of requirements shall be met by the Networking Protocol, as follows:

- capability to run over all supported bearers (leased lines, X.25, ATM, Frame Relay, ...);
- support of existing transport protocols and their applications, such as OSI, TCP/IP family, etc.;
- widely available, cheap and reliable.

The Internet Protocol (IP) is a Networking Protocol that ideally supports these requirements. IP also adds flexibility to how management connectivity is achieved when networks are rolled out, by offering various implementation choices. For instance, these may take the form of:

- Dedicated management intranets.
- Separation from or integration into an operator's enterprise network.
- Utilisation, in one-way or another, of capacities of the public Internet and its applications or other resources.

5.2.6 Physical level

Though the interaction at the logical level takes place between the Management System and the NEs, it is left to the implementer's choice the possibility to use the Q-Adapter concept of ITU-T TMN Architecture as physical implementation (as defined in ITU-T Recommendation M.3010 [1]).

The present document does not preclude the usage of Q-Adapters at other PLMN Management interfaces.

5.3 3GPP Compliance conditions

For a 3GPP entity (Management System or NE) to be compliant to a given Management Interface, all the following conditions shall be satisfied:

- it implements the management functionality following the Information Model and flows specified by the relevant 3GPP Management Interface Specifications applicable to that interface;
- it provides at least one of the IRP Solution Sets (see Annex C) related to the valid Application Protocols specified by 3GPP Application Protocols for that interface (see annex A). For each interface at least one of the valid protocols will be recommended;
- it provides at least one standard networking protocol (see Annex B);
- in case the entity does not offer the management interface on its own, a Q-Adapter shall be provided. This Q adapter shall be provided independently of any other NE and/or Management System.

6 PLMN Management Processes

6.1 Process decomposition

The present document details the general aspects of PLMN Management . It describes primarily the management processes that collectively support Customer Care Service Development and Operations, and Network and Systems Management Processes.

These management processes are based on the widely accepted Telecom Operations Map from the TeleManagement Forum [100]. The Telecom Operations Map uses the TMN Model as a foundation as defined in the ITU-T Recommendation M.3010 [1].

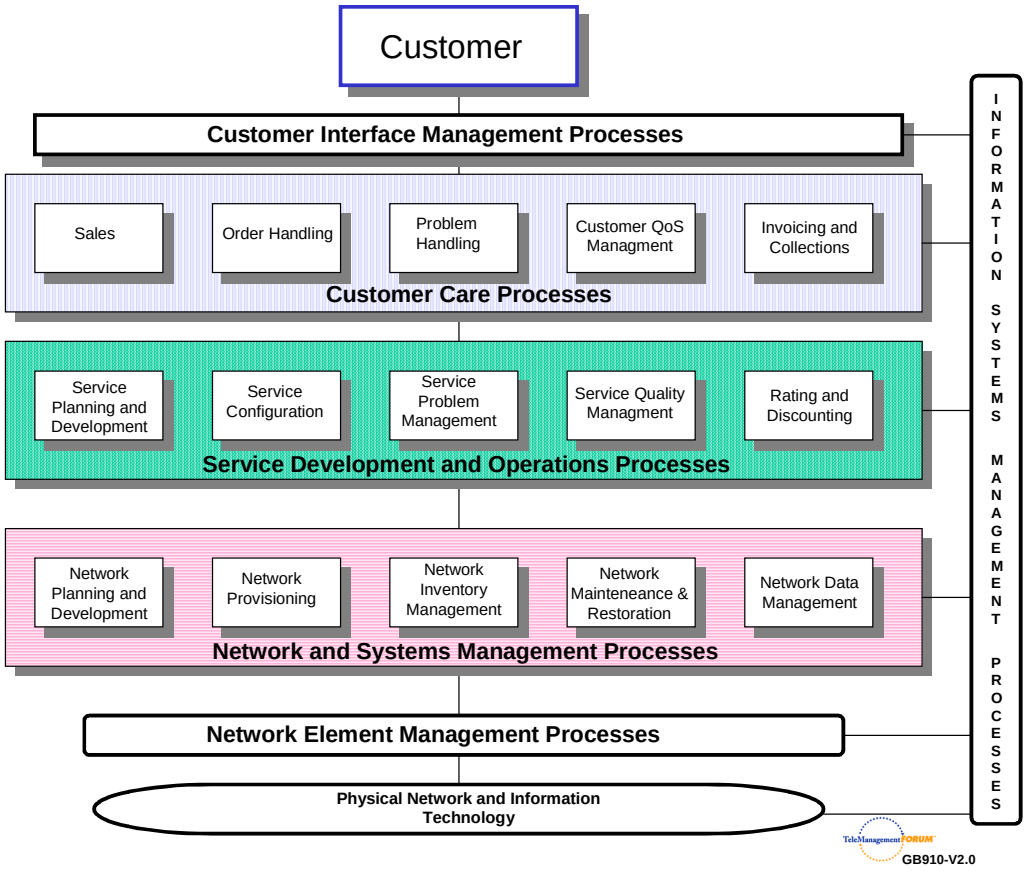


Figure 3: Telecom Operations Map Business Process Model (* imported from [100])

The following clauses give a short description of each of the management processes introduced in the "TMF Telecom Operations Map" [100]. To see a more detailed description and process spider diagram for each process, refer to "TMF Telecom Operations Map"[100].

6.2 Customer Care Processes

These processes involve direct interaction with a customer to provide, maintain, report on service, and bill for services. The customer is the ultimate buyer of a communications service with many end users in their organization that utilize the

Service Provider's services. The Service Provider **must** interact at many interfaces to support its customer and end users.

6.2.1 Customer Interface Management

The Customer Interface Management Process may be a distinct process, or may be performed as part of the individual Customer Care Processes on an individual service or cross-service basis. These are the processes of directly interacting with customers and translating customer requests and inquiries into appropriate "events" such as, the creation of an order or trouble ticket or the adjustment of a bill.

6.2.2 Sales

The Sales Process encompasses learning about the needs of each customer, and educating the customer about the communications services that are available to meet those needs.

6.2.3 Order Handling

The Order Handling Process includes all the functions of:

- Accepting a customer's order for service, whether directly from the customer, from the Sales process, from the customer's agent (e.g. Outsourcer, another service provider);
- Tracking the progress of the order and updating the customer;
- Notifying the customer when the order is complete.

6.2.4 Problem Handling

The Problem Handling Process is responsible to receive service complaints from customers, resolve them to the customer's satisfaction and provide meaningful status on repair or restoration activity.

6.2.5 Customer QoS Management

This process encompasses monitoring, managing and reporting of Quality of Service (QoS) as defined in Service Descriptions, Service Level Agreements (SLA), and other service-related documents.

6.2.6 Invoicing and Collection

This process encompasses sending invoices to customers, processing their payments and performing payment collections. In addition, this process handles customer inquiries about bills, provides billing inquiry status and is responsible for resolving billing problems to the customer's satisfaction.

6.3 Service Development and Operations Processes

These processes are generally "one step removed" from day-to-day direct customer interaction. Focus is on service delivery and management as opposed to the management of the underlying network and information technology. Some of these functions are done on a one-time basis, like designing and developing a new service or feature. Other functions involve service capacity planning, the application of a service design to specific customers or managing service improvement initiatives, and are closely connected with the day-to-day customer experience.

6.3.1 Service Planning and Development

This process encompasses:

- Designing technical capability to meet specified market need at desired cost;
- Negotiating joint service arrangements, e.g., SLAs with other providers, Mobile Services Roaming Agreements, Bilateral Agreements etc. Inter-Provider Agreements.
- Ensuring that the service (product) can be properly installed, monitored, controlled, and billed;
- Initiating appropriate process and methods modifications, as well as initiating changes to levels of operations personnel and training required;
- Initiating any modifications to the underlying network or information systems to support the requirements;
- Assuring that the technical capability works, that the operational support process, procedures, and systems function properly.
- Managing deployment and Controlled Introduction of a new service, feature, enhancement or other change to the service.
- Ensuring that sufficient capacity is available to meet forecasted sales.

6.3.2 Service Configuration

This process encompasses the installation and/or configuration of service for specific customers, including the installation/configuration of customer premises equipment.

6.3.3 Service Problem Management

This process encompasses reporting on service problems and trouble performance, isolating the root cause of service-affecting and non-service-affecting failures and acting to resolve them. Typically, failures reported to this process affect multiple customers.

6.3.4 Service Quality Management

This process supports monitoring service or product quality on a service class basis in order to determine:

- Whether service levels are being met consistently;
- Whether there are any problems with or improvements that can be made for the service or product;
- Whether the sale and use of the service is tracking to forecasts.

6.3.5 Rating and Discounting

This process encompasses:

- Applying the correct rating rules to usage data on a customer-by-customer basis, as required for a usage-based service;
- Applying any discounts agreed to as part of the Ordering Process;

- Applying promotional discounts and charges;
- Applying outage credits;
- Applying rebates or charges due because Service Level Agreements were not met or exceeded respectively;
- Resolving unidentified and zero billed usage cases.

6.4 Network and Systems Management Processes

These processes are responsible for ensuring that the network and information technologies infrastructure supports the end-to-end delivery of the required services.

The job of these processes is to implement the infrastructure required, ensure it runs smoothly, is accessible to services, is maintained and is responsive to the needs, whether directly or indirectly, of services and customers. Network and Systems Management is also the integration layer between the Element Management Layer and the Service Management Layer. Its basic function is to assemble information from the Element Management systems, and then integrate, correlate, and in many cases, summarize that data to pass on the relevant information to Service Management systems or to take action in the network.

6.4.1 Network Data Management

This process encompasses the collection of usage data and network and information technology events and data for the purpose of network performance and traffic analysis. This data may also be an input to Billing (Rating and Discounting) processes at the Service Management Layer, depending on the service and its architecture.

6.4.2 Network Maintenance and Restoration

This process encompasses maintaining the operational quality of the network, in accordance with required network performance goals.

6.4.3 Network Inventory Management

This process encompasses anything to do with physical network and information technology equipment and the administration of this equipment.

6.4.4 Network Provisioning

This process encompasses the configuration of the network, to ensure that network capacity is ready for provisioning and maintenance of services.

6.4.5 Network Planning and Development

This process encompasses:

- Development and acceptance of network and information technology infrastructure strategies.
- Description of standard network configurations primarily for operational use.
- Definition of rules for networks, e.g., planning, installation, usage recording and maintenance, etc.
- Designing the network capabilities to meet a specified service need at the desired cost, i.e. the introduction of new technologies to support new services, features or enhancements.
- Design, deployment and introduction of new technologies for network and information technology cost reductions or quality improvements.
- Ensuring that the network can be properly installed, monitored and controlled.

- Ensuring that enough network capacity will be available to meet the forecasted demand. Based on the required network capacity, orders are issued to suppliers or Other Network Operators (ONOs) and site preparation and installation orders are issued to Network Inventory Management or a third party network constructor (work orders). A design of the logical network configuration is provided to Network Provisioning.

Supporting cases of un-forecasted demand.

7 PLMN Management Functional Architecture

7.1 TM Architectural aspects

The basic aspects of a TM architecture, which can be, considered when planning and designing a TM are:

- the functional architecture;
- the information architecture;
- the physical architecture.

The management requirements from the business needs are the base for the functional architecture, which describe the functions that have to be achieved. The information architecture defines what information that has to be provided so the functions defined in the functional architecture can be achieved. The physical architecture has to meet both the functional architecture and the information architectures. These relationships are shown in figure 5.

The present document addresses the Functional Architecture, the Physical Architecture is addressed in TS 32.102 [101].

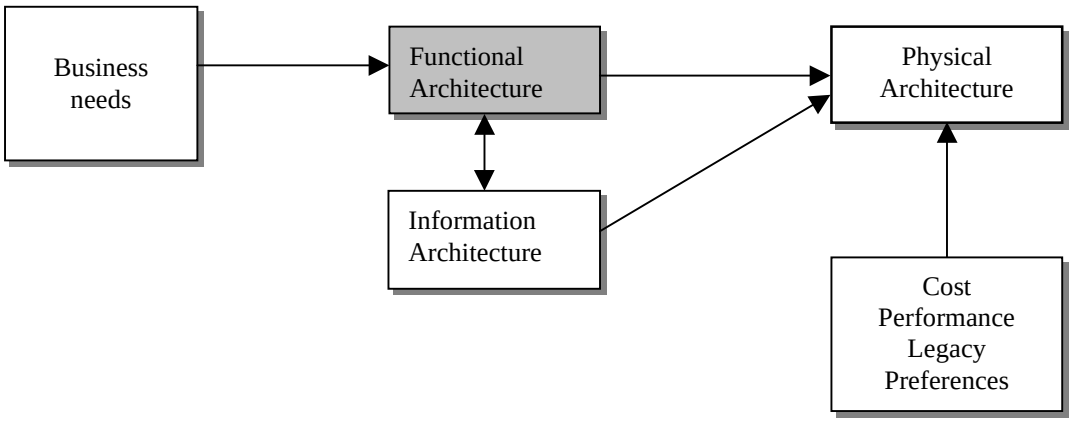


Figure 4: Architectural relationship

The present document details the PLMN Management Functional Architecture.

All management processes have functions in several management areas. By identifying only those processes and interfaces relating to a certain management function, for example performance management, it is possible to take a slice through the Telecom Operations Map that details the functional architecture for performance management, this will be the approach taken by the present document.

The management functions are:

- Performance management;
- Roaming management;
- Fraud management;
- Fault management;
- Security management;

- Software management
- Configuration management;
- Accounting management;
- Subscription management;
- Quality of Service (QoS) Management (see informative annex D);
- User equipment management.

7.2 Performance Management

7.2.1 Overview

An initial view of Performance Management is described in [105]. This shows an example decomposition of Performance Management processes to identify essential information flows. It shows a slice through the Telecom Operations Map from a Performance Management point of view. This slice is applicable to Mobile Networks and other networks. Although the "slice" or view is quite large, it does not contain all interfaces or process activities that are related to Performance Management. It does however show the main processes and interfaces involved in Performance Management. Please refer to [105] for further detail.

7.2.2 Standardisation Objectives

During the lifetime of a 3G network, its logical and physical configuration will undergo changes of varying degrees and frequencies in order to optimise the utilisation of the network resources. These changes will be executed through network configuration management activities and/or network engineering, see TS 32.600 [54].

Many of the activities involved in the daily operation and future network planning of a 3G network require data on which to base decisions. This data refers to the load carried by the network and the grade of service offered. In order to produce this data performance measurements are executed in the NEs, which comprise the network. The data can then be transferred to an external system, e.g. an Operations System (OS) in TMN terminology, for further evaluation. The purpose of the present document is to describe the mechanisms involved in the collection of the data and the definition of the data itself.

The Performance Management functional area concerns the management of performance measurements and the collection of performance measurement data across a 3G network. It defines the administration of measurement schedules by the Network Element Manager (EM), the generation of measurement results in the Network Elements (NEs) and the transfer of these results to one or more Operations Systems, i.e. EM(s) and/or Network Manager(s) (NM(s)).

The management requirements have been derived from existing telecommunications operations experience. The management definitions were then derived from other standardisation work so as to minimise the re-invention factor. References are given as appropriate.

The objectives of the present document are:

- To provide the descriptions for a standard set of measurements;
- To produce a common description of the management technique for measurement administration and result accumulation; and
- To define a method for the bulk transmission of measurement results across a management interface.

The definition of the standard measurements is intended to result in comparability of measurement data produced in a multi-vendor 3G network, for those measurement types that can be standardised across all vendors' implementations.

As far as possible, existing standardisation in the area of Performance Management is re-used and enhanced where particular requirements, peculiar to the mobile telephony environment, have been recognised.

Performance management is further specified in TS 32.400-series [53].

7.3 Roaming Management Overview

Roaming is a service provided by Mobile Service Providers. Customers of a Home Service Provider may use the infrastructure of another, a Serving Service Provider (see figure 5) to give its customer the ability to make calls when outside the home service provider' s territory. The goal is to have a customer receive the same service (or as close to the same service) when travelling in an area supported by another network as the customer receives when in their home service provider's area. Please refer to [105] to see an example implementation with more detail.

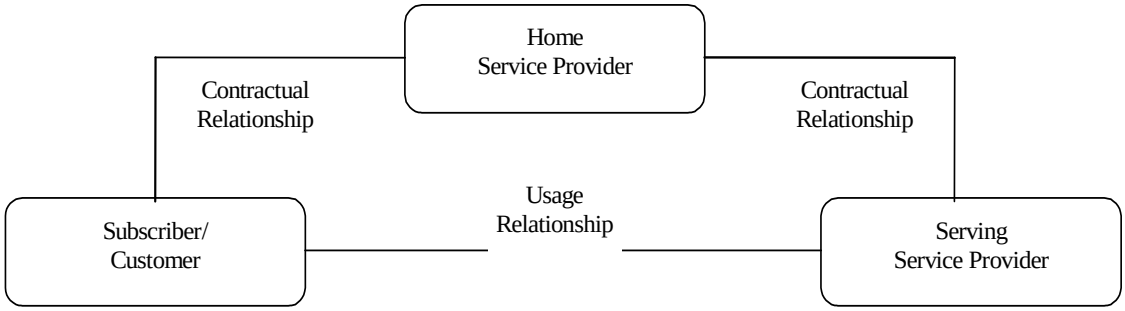


Figure 5: Relationships between Subscriber, Home and Serving Service Provider

7.4 Fraud Management Overview

Fraud and all the activities to detect and prevent fraud are quite common to any network. Nonetheless, mobility and roaming, two integral mobile services, make fraud detection and fraud prevention more complicated and more urgent. The mobile service provider does not know the location of the "end of the wire," which would lead to the home of a fraudulent customer. For roaming, the situation is demonstrably worse. For a roaming visitor the caller is not the service provider's customer and therefore, the service provider does not have complete information to assess fraud. In the reverse case, the service provider has little control when its customers are roaming, e.g., potentially going over credit limits or using service after being suspended. In this case, the fraudulent customer uses the network facilities of another provider (the serving service provider) meaning the home service provider has to rely on the serving service provider for some level of fraud protection support. This means to a large extent that fraud prevention is largely out of the control of the home service provider when one of its customers roams on another network and out of the control of a serving service provider when being visited by another provider's roamer. Please refer to [105] to see an example implementation with more detail.

7.5 Fault Management

7.5.1 Overview

Fault Management is accomplished by means of several Processes/Sub-processes like fault detection, fault localisation, fault reporting, fault correction, fault repair, etc. These Processes/Sub-processes are located over different management layers, however, most of them (like fault detection, fault correction, fault localisation and fault correction) are mainly located over the Network Element and Network Element Management layers, since this underlying network infrastructure has the 'self healing' capabilities.

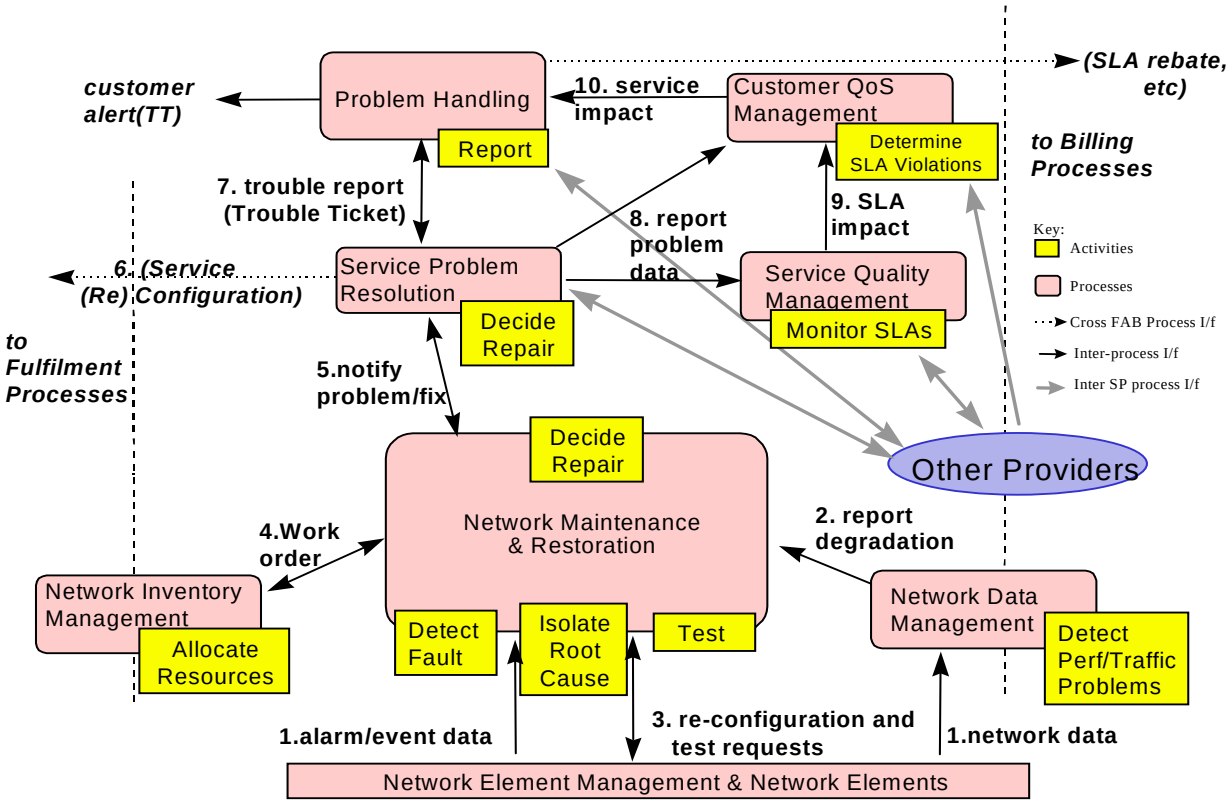
It is possible, however, that some faults/problems affecting the telecom services are detected within the "Network and Systems Management" layer, by correlating the alarm/events (originated by different Network Elements) and correlating network data, through network data management.

Network data management logically collects and processes both performance and traffic data as well as usage data.

While the Fault Management triggered within the Network Element and NE Management layers is primarily reactive, the Fault Management triggered within the Network and Systems Management layer is primarily proactive. Meaning triggered by automation rather than triggered by the customer; and this is important for improving service quality, customer perception of service and for lowering costs.

Focusing on the Network and Systems Management layer, when a fault/problem is detected, no matter where and how, several processes are implicated, as described in figure 6.

Figure 6 taken from the Telecom Operations Map [100] shows an example of how Fault Management data can be used to drive an operator's service assurance process. Service assurance then becomes primarily proactive, i.e. triggered by automation rather than triggered by the customer. It is argued that this approach is key to improving service quality, customer perception of service and for lowering costs.



NOTE: Flow "3." has been added in the present document.

Figure 6: Service Assurance Process Flow (* imported from [100])

TOM assurance activities (and their associated interfaces) shown in figure 6 can be associated with ITU-T TMN service components from TS 32.111-series "3G Fault Management" [3] according to Table 1 below:

Table 1

ITU-T TMN Service Component TS 32.111-x [3]	TOM Network Management Assurance Activities
Alarm Surveillance	Detect Fault
Fault Localisation	Isolate Root Cause
Fault Correction	Decide Repair / Allocate Resources
Testing	Test

The TOM assurance example shown in figure 6 also recognises that Performance Management data can also be used to detect network problems.

The TOM assurance example also adds some detail to the Service Management Layer by showing how activities such as determining and monitoring Service Level Agreements (SLAs) and trouble ticket reporting are interfaced to the Network Management layer.

7.5.2 Standardisation Objectives

A 3G system is composed of a multitude of Network Elements (NE) of various types and, typically, different vendors, which inter-operate in a co-ordinated manner in order to satisfy the network users' communication requirements. The occurrence of failures in a NE may cause a deterioration of this NE's function and/or service quality and will, in severe cases, lead to the complete unavailability of the respective NE. In order to minimise the effects of such failures on the Quality of Service (QOS) as perceived by the network users it is necessary to:

- detect failures in the network as soon as they occur and alert the operating personnel as fast as possible;
- isolate the failures (autonomously or through operator intervention), i.e. switch off faulty units and, if applicable, limit the effect of the failure as much as possible by reconfiguration of the faulty NE/adjacent NEs;
- if necessary, determine the cause of the failure using diagnosis and test routines; and
- repair/eliminate failures in due time through the application of maintenance procedures.

This aspect of the management environment is termed "Fault Management" (FM). The purpose of FM is to detect failures as soon as they occur and to limit their effects on the network Quality of Service (QOS) as far as possible. The latter is achieved by bringing additional/redundant equipment into operation, reconfiguring existing equipment/NEs, or by repairing/eliminating the cause of the failure.

Fault Management (FM) encompasses all of the above functionalities except commissioning/decommissioning of NEs and potential operator triggered reconfiguration (these are a matter of Configuration Management (CM), cf. TS 32.600 [54]).

FM also includes associated features in the Operations System (OS), such as the administration of a pending alarms list, the presentation of operational state information of physical and logical devices/resources/functions, and the provision and analysis of the alarm and state history of the network.

Fault management is further specified in TS 32.111-series [3].

7.6 Security Management

7.6.1 Overview

This clause describes an architecture for security management of the TMN that is divided into two layers, as shown in figure 7. No individual layer is dependent on any specific technology in the other one.

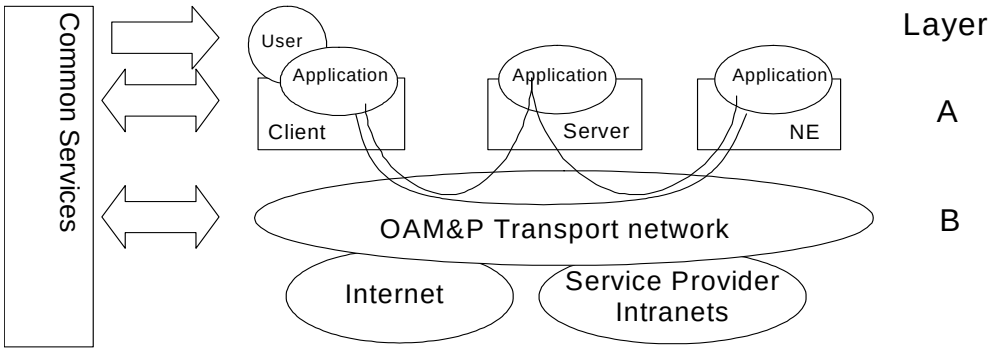


Figure 7: Security Management Architecture

7.6.1.1 Layer B - OAM&P Transport IP Network

Some Service Providers might build their OAM&P transport network as a completely private, trusted network. In the normal case though, the OAM&P transport network should be regarded as partly insecure due to its size, complexity, limited physical security and possible remote access from dial-up connections or from the Internet. The only security service provided then is that the OAM&P transport network when based on IP is logically separated from the Internet.

For IP based transports infrastructure aspects on security are handled to the extent possible utilizing IP classic features (addressing schemes, DNS, DHCP, BOOTP, protection with firewalls etc.).

Additionally, a trusted IP-environment to the application level might be provided, e.g. an environment with no masquerading IP-hosts and where potential intruders cannot communicate. One way to accomplish such a secure DCN is to use IP security mechanisms (IPSec; see IETF RFC 2401 [7]) to achieve authentication of IP hosts (servers, gateways, Network Elements) and optional encryption of OAM&P traffic. Note however that the secure DCN does not authenticate users.

7.6.1.2 Layer A - Application Layer

On this layer we find Telecom Management applications performing their tasks in the normal management functional areas. Managed objects residing in the network resources are often accessed or manipulated.

Layer A provides authentication of users ensuring that every party involved in OAM&P traffic is securely authenticated against every other party. The implementation of the authentication service supports "single log-on" (a user only has to log-on once to get access to all OAM&P applications in the network) and "single point of administration" (an administrator only needs to maintain a user and his/her profile in one place).

Layer A also provides authorization (access control) - to verify if a user is authorized to perform a certain operation upon a specified target object at a given time. In addition, it addresses the use of signing and logging of events. Logging of events here means "logging of actions" (not necessarily logging of ALL actions) to be able to check "who did what". At least all "critical" actions (configurations etc.) should be logged.

Interface definitions addressing authentication and authorization are needed. Also note that layer A requires confidentiality. Layer B may provide this service. If not, layer A instead has to provide it itself.

7.6.1.3 Common Services

In common services we find the security infrastructure components:

- Directory (for storage of user information, certificates, etc.);
- PKI (Certificate Authority, Registration Authority, Public Key Certificate, etc.).

Layer A relies on, and interacts with, the Common Services through distribution of certificates and keys, authentication of users, authorization, utilities for security administration (setting access rights), etc.

NOTE: Layer B does not necessarily interact with Common Services for security management purposes. The arrows in figure 7 simply indicate the possible use of common services for Configuration Management.

7.7 Software Management

7.7.1 Overview

This subclause describes the software management process for 3rd Generation networks. Two main scenarios are considered:

1) Main Software Management Process: It covers requesting, acceptance, installation, monitoring, documenting, database updating and feedback to the vendor for managing software. The sub-processes are valid for complete software releases and software patches for fault correction of the Network Elements and even element managers.

2) Software Fault Management: Its emphasis is on network monitoring and handling faults, which are caused by software malfunctions.

7.7.1.1 Main Software Management Process

The main focus is the management of new software releases and correction patches. Importance is placed integrating new software into a network with out causing unnecessary service disruptions and maintaining high levels of quality for the network. The main steps in the software management process are:

- Delivery of software from the vendor.
- Delivery of the software to local storage in the Network Elements and/or element managers.
- Validation of the software to ensure that the Software is not corrupt.
- Activation of the software to an executable state.
- Validation of the software to ensure that it runs correctly.
- Acceptance or rejection of the software, depending on the outcome of the validation. (A rejection of the software implies a reversion to a previous software version).

Figure 8 shows an example of how these steps may be realized in terms of activities involving the processes defined in the Telecom Operations Map. However, alternative sequences may exist. For example, increased automation may cause step 3 to be omitted. Instead, a vendor certification activity could be run for a series of software releases or patches.

The following list is an explanation to the steps in figure 8.

1) Based on inputs from customer care interactions and marketing research, a network operator will establish new feature requirements. These requirements are sent to the vendor in the form of a feature request.
2) The vendor delivers a new software release/correction with the corresponding documentation and installation procedure to the network operator. It should be noted that when a network operator utilises equipment from more than one vendor, this process runs as multiple parallel processes.
3) A service quality management department of the network operator receives and reviews the software. Upon approving the software for installation, the software is sent to the network-provisioning department.
4) Installation Task:
    a) The software is installed in the appropriate Network Elements and/or element managers by network provisioning.
    b) Installation information is sent to the network maintenance and restoration department to inform them of pending changes in the network.
    c) Installation information is sent to the customer care centre to inform them of pending changes in the network.
5) Installation Test and Validation:
    a) Once the software has been installed, network provisioning performs tests to check and ensure that the new software is working properly.
    b) In addition to the checks that are performed by network provisioning, network maintenance and restoration could also detect malfunctions within and outside the updated Network Element (NE).
    c) Should network maintenance and restoration detect a problem within the updated Network Element (NE), then network provisioning is informed to decide on further actions.
6) Successful Installation Result:
    a) Upon successful installation of the software, the service quality management department is informed.
    b) A report is sent to network maintenance and restoration to inform them that the software will remain implemented in the network. At this point the documentation library and software database is updated.
    c) The network data management department is informed over the changes in the network.

7) Negative Installation Result:

   a) If the installation fails, network provisioning performs a "fallback", i.e. remove the new software and insure that the Network Element (NE) is running properly on the old software.

   b) A report containing the negative results and findings will be sent to service quality management and at the same time to network maintenance and restoration.

8) Once the installation procedure has been ended, the network maintenance and restoration department closely monitors the affected Network Element (NE) to ensure proper performance.

9) Service quality management will send feedback to the vendor as to the positive or negative results of the installation.

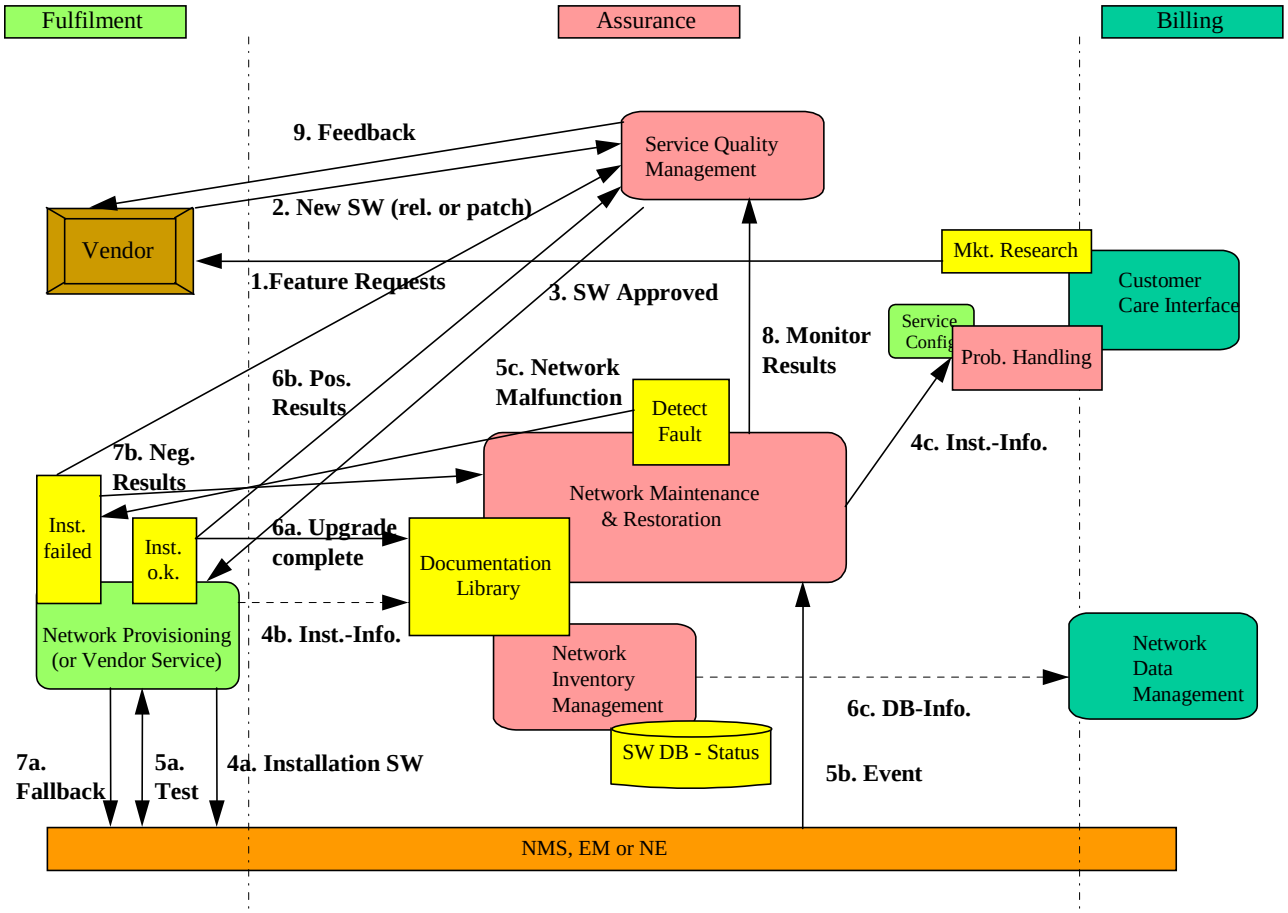


Figure 8: Main Software Management Process

7.7.1.2 Software Fault Management

Software Fault Management involves the following steps:

- Detection of Software malfunctions in the network.
- Problem resolution. The origin of the malfunction is determined and corrective action is decided. The corrective action can be one of the following:
  - Reversion to an earlier software version. This can imply both load and activation of the earlier software.
  - Load and activation of correction software, according to subclause 8.7.1.
  - Re-activation of current software.

Figure 9 shows an example of how these steps may be realized in terms of activities involving the processes defined in the Telecom Operations Map.

The following list is an explanation to the steps in figure 9.

1) The network maintenance and restoration department detects an event or an alarm/fault from the Network Element (NE).

2) Problem solving and informing customer care:

   a) The alarm is forwarded to the service problem resolution department for corrective actions and it is determined that the problem is caused by a software defect.

   b) In parallel the Customer Care Centre is informed, if the malfunction of the network may have impact on customers.

3) The service problem resolution department informs problem handling and subsequently the customer care centre over service impairments with in the network.

4) Problem handling reports to the service quality management department. The service disturbance is described within the report.

5) Service quality management checks the current software level of the affected Network Element with the network inventory management department.

6) If major network disturbances still appear the Service Quality management decides to fallback to a stable Software version (maybe some time after a new Software installation) and requests Network Provisioning.

7) a+b): Network Provisioning performs the fallback and informs Network Maintenance and Inventory.

8) Service quality management sends a request for a software correction to the vendor.

9) The vendor sends a new software release or correction to the network operator. The rest of the procedure can be followed in the main software management process.

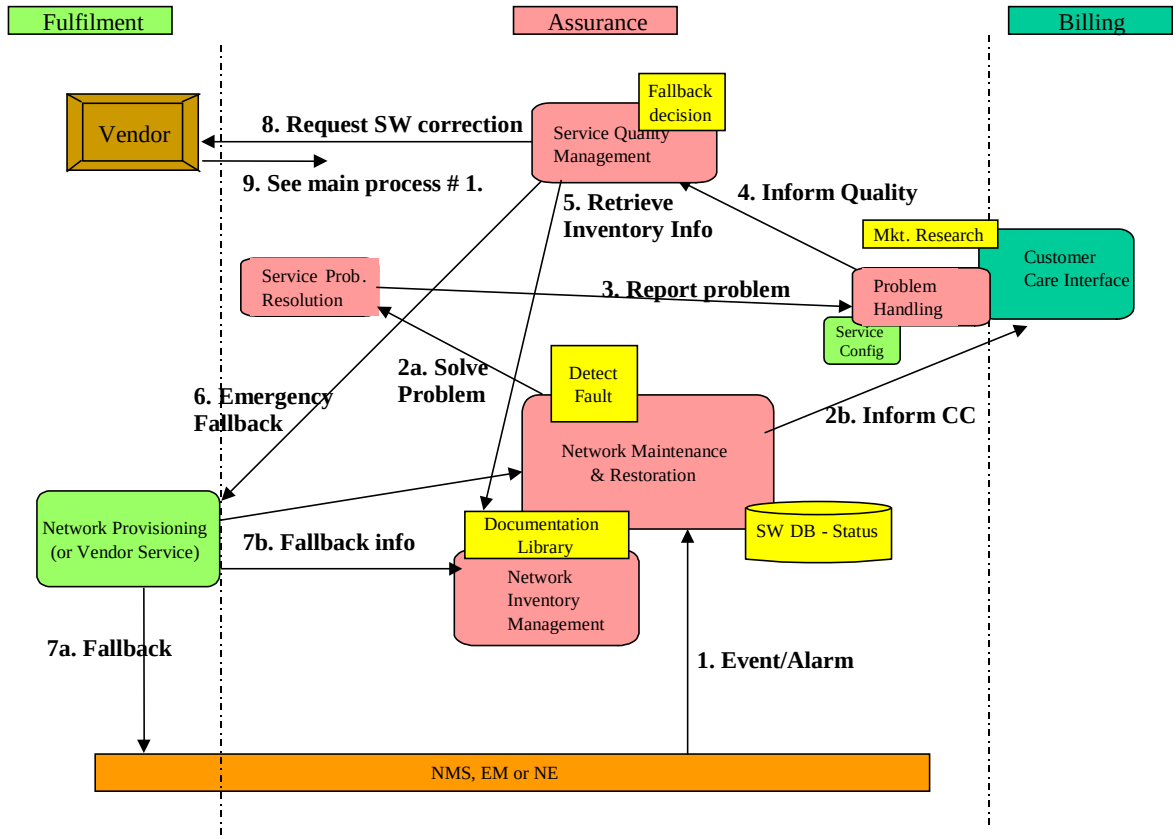


Figure 9: Software Fault Management

7.8 Configuration Management

A variety of components will make up an operator's actual implementation of a 3G network. Since it is an explicit goal of the standardisation effort within 3GPP to allow mix and match of equipment from different vendors, it is expected that many networks will indeed be composed of multiple vendors' equipment. For an operator to be able to properly manage this diverse network, in order to provide the quality of service expected by his customers, it is essential to standardise the Configuration Management for 3G systems at least to an extent that the operation of the multi-vendor network will be possible effectively and efficiently. Within the scope of Configuration Management, a distinction has to be made between those aspects targeting single Network Elements (NE management level) and those that are also, or exclusively, relevant for some part or the entire network (Network Management level).

Configuration Management is further specified in TS 32.600 [54].

7.9 Accounting Management

3G charging data descriptions will be based on the requirements specified in TS 22.115 "Service aspects; Charging and Billing" [51] and on the charging principles outlined in TS 32.200 "Charging management; Charging Principles" [55]. The main content of 3G charging data descriptions will be:

- Layout and formats of charging data records (CDRs) for the 3G core network nodes (circuit, packet switched and IP Multimedia) and service nodes (e.g. MMS);
- Data generation dependent on call states, chargeable events and TS 22.115 [51] service requirements;
- Formal description of the CDRs format in ASN.1 (ITU-T Recommendation X.680-1997 [49]) and definition of a file transfer mechanism (FTP).

7.10 Subscription Management

Subscription Management (SuM) is a feature that permits Service Providers, Value Added Service Providers and Mobile Operators to provision services for a specific subscriber. The feature is necessary to allow Service Providers and Operators to provision, control, monitor and bill the configuration of services that they offer to their subscribers. SuM focuses on the OAM processes to manage subscription information. These correspond to the 'Fulfillment' Process areas of the TeleManagement Forum Telecom Operations Map [100].

SuM is an area of service operation management that sets a complex challenge for Service Providers and Operators in their support of new or existing subscribers during their every day network operation.

In 2G solutions the main repository of the subscription information is in the Home Locations Register (HLR). However the management and administration interfaces for controlling this information is proprietary to each vendor. The use of proprietary interfaces is inconvenient for those Operators using multiple vendors' equipment since their provisioning systems have to accommodate multiple proprietary interfaces, which perform essentially identical functions. Moreover, it makes it more difficult to generate customer self care applications that allow subscribers to provision, and amend subscription data.

The 3G environment requires more complex service delivery mechanisms than in 2G and SuM is no longer simply an internal matter for a single operator but a capability that is achieved by linking together features across multiple Service Providers and Operators Operations Support Systems (OSS). Historically, the services provided by Operators have been defined within standards groups such as ETSI or 3GPP. With the advent of Open Services Access (OSA) being adopted by 3GPP the User Service Definitions will be replaced by Service Capabilities traded amongst Service Providers and Network Operators. This will allow Operators and Service Providers to define customized service environments that roam with users as they move amongst networks - this is the Virtual Home Environment (VHE) 3GPP TR 22.121 [56]. This customized service environment means that subscription information is held in a number of locations including the Home Network, the Visited Network, the User Equipment, Application VASP Equipment (e.g. servers accessed by the subscriber for content and information based services) and the Operations Systems of the Service Providers, and Operators supporting the subscriber's service subscription.

Service delivery and support across multiple vendors' solutions and organizations is a feature of other industries, and the solutions adopted are secure supply chain solutions based upon mainstream e-commerce principles, methods and technologies.

There is a relationship between this feature and the PS Domain, CS Domain, IP Multimedia Subsystem (IMS), Authentication Center (AuC), Open Services Access (OSA) and Generic User Profile (GUP) documented in other 3GPP specifications.

The conceptual model for SuM is illustrated in figure 10.

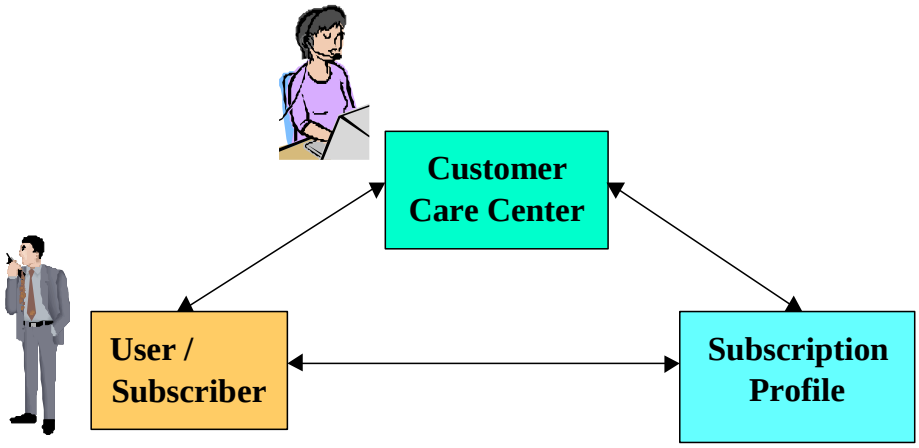


Figure 10: High level view of Subscription Management (SuM)

SuM is concerned with provisioning the subscription profile throughout all the systems and trading partners needed to realize the customer service, SuM provides specifications that define the interfaces and the procedures that interconnect the three points of the SuM triangle: Customer Care Center, the User and the network (s) where the Subscription profile resides (such as HSS, USIM, etc.).

The SuM requirements are described in more detail in 3GPP TS 32.140 [57], The SUM Architecture is described in 3GPP TS 32.141 [58].

7.11 Subscriber and Equipment Trace Management

Subscriber and Equipment Trace Management is a Feature that allows a Network Operator to activate/deactivate from the Network Management system the tracing of a particular subscriber within the network. Once activated the trace activity is reported back to the Network Management system. It will be possible to request activation of a trace from different Network Elements (via the appropriate Element Management Functionality) depending on the operator's requirements. The activation/deactivation and reporting interface for Trace Management between the Network Management and Element Management Systems will be standardised using new and existent IRP Interfaces.

7.12 OAM&P of the PLMN "Management Infrastructure"

As described earlier in the present document, each PLMN organisation has a management infrastructure consisting of a collection of systems (computers and telecommunications) - a TMN in ITU-T parlance - used to manage its network. Though this management network is logically distinct from the PLMN , the operations systems and supporting data communications network comprising it have the same management needs as described for network elements and where possible should be managed using the same principles and similar management processes and functionality.

Annex A (normative): 3GPP Management Application Layer Protocols

The valid Management Application Layer Protocols for 3GPP are:

- CMIP (see references [20], [21]);

NOTE: Normative references relating to running CMIP over OSI application, presentation and session layers are [9] - [12] and [23] - [42].

- SNMP (see reference [6]);

- CORBA IIOP (see references [8] and [52]).

The valid Application Layer Protocols for Bulk & File Transfer are:

- FTAM (see references [13] – [19]);

- ftp (see reference [4]);

- tftp (see reference [5]).

- sftp (secure ftp)

NOTE: sftp is an implementation of ftp that uses SSL (SSH-1 or SSH-2 transport protocol) to provide a secure ftp. There are many commercial and open source implementations available. An IETF Secure Shell working group exists, whose goal is 'to update and standardize the popular SSH protocol'. Currently no IETF RFCs are available, however a number of IETF drafts can be found at the working groups home web site: http://www.ietf.org/html.charters/secsh-charter.html.

Annex B (normative): 3GPP Management Network Layer Protocols

The valid Network Layer Protocols for the Management of 3GPP are:

- IP (see reference [48];
- X.25 (see reference [22]).

NOTE 1: IP is the recommended Networking Protocol.

NOTE 2: Normative references relating to ISO Transport over TCP-IP are [46] and [47] and ISO Transport over X.25 are [43] - [45].

Annex C (normative): 3GPP Management IRP Solution Sets

The valid IRP Solution Sets for the Management of 3GPP on the Itf-N interface are:

- GDMO (CMIP);
- CORBA (IDL).

Annex D (informative): QoS Management

D.1 Overview

QoS Management, from an OAM&P perspective, in 2.5G and 3G networks primarily consists of two functional areas: QoS policy provisioning and QoS monitoring. QoS Policy Provisioning is the process of configuring and maintaining selected Network Elements with QoS policies that are created based upon customer SLAs and observed network performance. QoS Monitoring is the process of collecting QoS performance statistics and alarms; this data is then used to generate analysis reports for making changes/upgrades to the network. The detailed relationship between SLA Management and QoS Provisioning and Monitoring is for future study. A conceptual breakdown of QoS Management is shown in figure D.1.

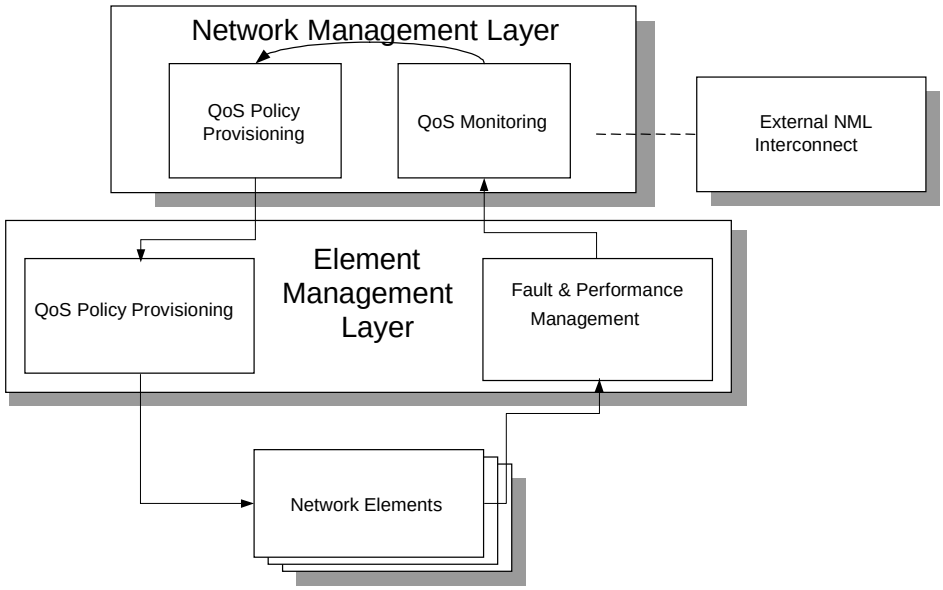


Figure D.1: QoS Management

The following subclauses provide descriptions of QoS Provisioning and Monitoring.

It should be noted that the same descriptions could apply to other Policy Management instantiations, e.g. Security and Service Provisioning.

D.2 QoS Provisioning

In the 2.5G and 3G networks, multiple network domains **must** inter-work in order to provide the end-to-end quality of service required by end-user applications. To add to this complexity, there are many classes of Network Elements from many network infrastructure suppliers, each of which require configuration in a consistent manner in order to the network operator's QoS objectives. Within each Network Element, there are many QoS functions (such as Admission Control, Policers, Shapers, Queue Manager and Scheduler), which **must** be configured.

In order to configure these heterogeneous networks so that they can deliver the desired QoS, the operator needs a management solution that meets the following high-level requirements:

- *Automation* of management tasks.
- *Centralized* management with fewer classes of management interface.
- *Abstracted* (or simplified) management data.

- *End-to-End* provisioning of the network.
- *Consistent and uniform* provisioning across all Network Elements.
- *Standards-based* solution in order to allow *inter-operability* at Network Element and OSS level.
- *Scalable* solution for large networks.

The IETF Policy Management Framework has been designed with these requirements in mind

The various standards that apply to QoS Policy Provisioning as described in the following subclauses are listed in D.4.1. At time of publication of the present document there are also a significant amount of IETF Drafts available on the subject at http://www.ietf.org,

D.2.1 Conceptual Architecture

The conceptual architecture for a policy-based QoS Management System is shown in figure D.2.

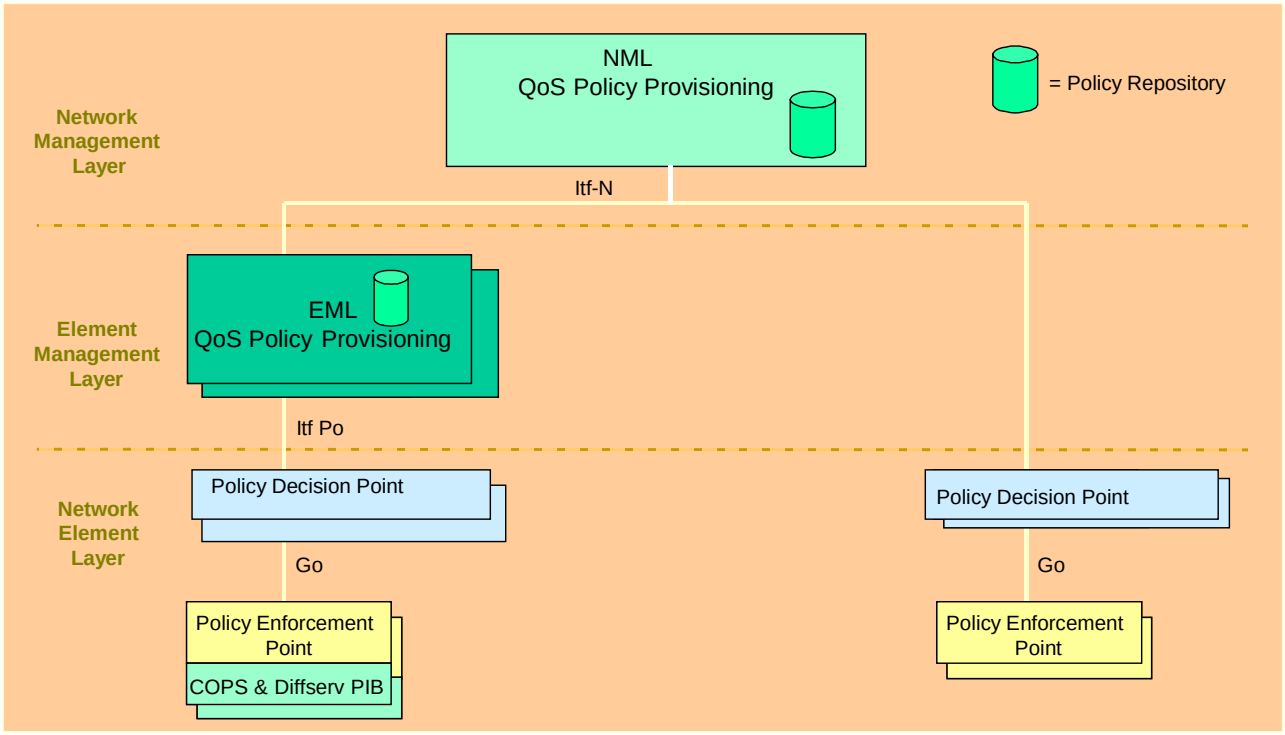


Figure D.2: QoS Provisioning

The architectural components identified in figure D.2 are described in the following subclauses.

NOTE: The Policy Repository and the Policy Decision Point can be implemented on the same node.

The Itf N interface is specified in the 32 series.

The Itf Po, between the Policy Repository and the Policy Decision Point is to be defined. The protocols under consideration includes: LDAP, LDUP, SNMP and COPS-PR.

The reference point Go is defined in TS 23.207 (see D.4 QoS Management Reference [22]) and the interface implementing the reference point is defined in TS 29.207 (see D.4 QoS Management Reference [23]).

D.2.2 NML QoS Policy Provisioning

This is a network-level operational support function that serves as the policy administration point for the entire network.

The NML QoS Policy Provisioning provides the following functions:

- Network policy administration user interface
- Master network policy repository for storage of all network policies for all domains
- Policy distribution capability to distribute policy data to the EML Policy servers.
- Global policy conflict detection

The policy repositories will use an LDAP-based directory to store the policy information.

D.2.3 EML QoS Policy Provisioning

This is an element management function that serves as the policy administration point for a network domain. A domain is an area of the network that contains equipment that performs a logically related function. Examples of network domains are: access network, core network and transport network, or supplier specific sub-networks within these networks.

The EML QoS Policy Provisioning provides the following functions:

- An optional EML-level policy administration user interface.
- EML-specific policy repository.
- Policy distribution capability to distribute policy data to the Policy Decision Points.
- Local policy conflict detection

It is envisioned that the optional EML-level policy administration user interface will be required in small networks that do not have a network-level policy provisioning OSS.

Note that EML-specific policy repositories contain policies that apply only to that domain as well as general network policies that apply across domains.

D.2.4 Policy Decision Point

The Policy Decision Point is the point in the network at which policy decisions are made for the Policy Enforcement Points under its scope of control. Whereas the Policy Enforcement Point is a function within a network node, the Policy Decision Point is separate functional entity that may reside within a separate Policy Server, for example, on an application server. The Policy Decision Point will make decisions based on the policy information held within the Policy Repository.

The Policy Decision Point provides the following functions:

- Retrieval of Policy Information from the policy repository
- Evaluates the policy information retrieved and decides what actions needs to taken.
- Distributes policy data to the Policy Enforcement Points. This distribution can either be sent to the PEP by the Policy Decision Point or the Policy Decision Point can wait for the PEP to request the information.
- Translation from QoS policy schema employed by the policy servers to Policy Information Base (PIB) format employed by the Policy Enforcement Points.
- Optional real-time policy decision-making function.
- Local policy conflict detection

The optional real-time policy decision-making function may be required when dynamic policy decisions **must** be made in response to current network conditions.

NOTE: The 3GPP Term Policy Decision Function (PDF) used in 23.207 and 29.207 is equivalent to the IETF Term Policy Decision Point.

TS 23.207 describes the End-to-end Quality of Service (QoS) concept and architecture, and TS 29.207 describes Policy control over Go interface (see D.4 QoS Management Reference [22]) and TS 29.207 (see D.4 QoS Management Reference [23]). If there are any inconsistencies then the definitions in 23.207 and 29.207 take precedence.

D.2.5 Policy Enforcement Point

The Policy Enforcement Point is a function that is part of a Network Element that **must** implement the policies defined by the policy administration system(s).

The Policy Enforcement Point provides the following functions:

- Storage of policy-related data locally.
- Execution of policies as network conditions dictate.
- Support for the Differentiated Services QoS mechanism (diffserv).

On initialization, the Policy Enforcement Point will contact its parent Policy Decision Point and request download of any policy data that it requires for operation. Note that information such as the address of the parent Policy Decision Point function **must** be provisioned in the Policy Enforcement Point MIB as part of normal network provisioning.

TS 23.207 describes the End-to-end Quality of Service (QoS) concept and architecture, and TS 29.207 describes Policy control over Go interface (see D.4 QoS Management Reference [22]) and TS 29.207 (see D.4 QoS Management Reference [23]). If there are any inconsistencies then the definitions in 23.207 and 29.207 take precedence.

D.3 QoS Monitoring

QoS Monitoring in 2.5G and 3G networks consists of collecting/processing performance statistics, usage data and QoS related faults. In order to obtain end-to-end quality of service monitoring, the Network Elements, the Element Management Layer and Network Management Layer **must** all be involved with the QoS Monitoring process. Alarm and performance collection is done at the Network Element layer and alarm/performance aggregation, report generation, and analysis is done at the Element Management and Network Management layers.

The following functions summarize the QoS Monitoring process:

- Manage QoS fault conditions received from Network Elements.
- Retrieve QoS Performance data from Network Elements.
- Collect and process usage data.
- Generate QoS Reports – trend analysis of key QoS parameters.
- Audit/Analyse collected QoS parameters against expected values.

References that apply to QoS Monitoring and the following subclauses are listed in subclause D.4.2.

D.3.1 QoS Monitoring Conceptual Architecture

The architecture of a QoS Monitoring system is shown in figure D.3.

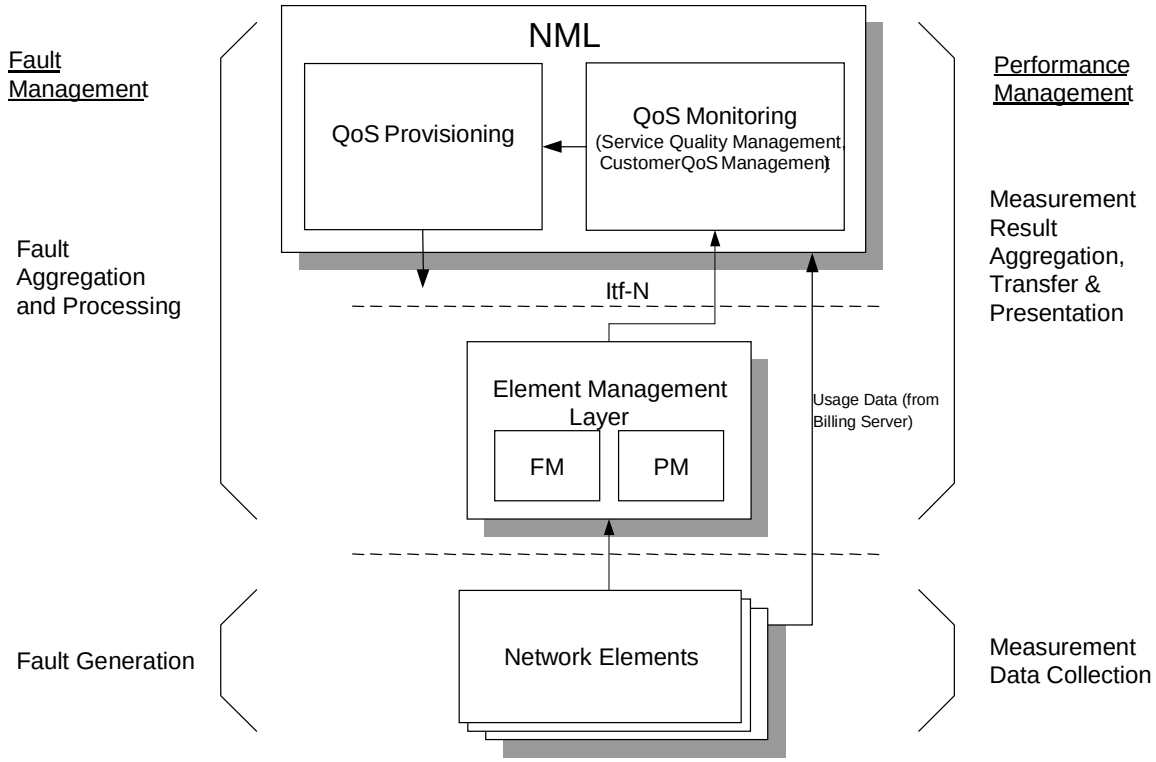


Figure D.3: QoS Monitoring

The architectural components identified in figure D.3 are described in the following subclauses.

D.3.2 Network Element

The Network Element component is responsible for collecting performance measurements, usage data and generating alarms. The Network Element component can contain the Policy Enforcement Point or the Policy Decision Point functions.

The Network Element component provides the following functions:

- Collect performance data according to the definition of the measurements and to return results to the EML.
- Collect usage data and forward the data to mediation
- Perform the following fault management functions: Fault detection, Generation of alarms, Clearing of alarms, Alarm forwarding and filtering, Storage and retrieval of alarms in/from the NE, Fault recovery, Configuration of alarms.

D.3.3 Element Management Layer

The Element Management Layer is responsible for aggregating and transferring the collected performance measurements and generated alarms/events.

The Element Management Layer provides the following functions:

Performance Management

- Measurement data collection
  - Measurement types. Corresponds to the measurements as defined in TS 52.402 (see D.4 QoS Management Reference [24]) and TS 32.403 (see D.4 QoS Management Reference [25]), i.e. measurement types specified in the present document, defined by other standards bodies, or manufacturer defined measurement types;

  - Measured network resources. The resource(s) to which the measurement types shall be applied have to be specified
  - Measurement recording, consisting of periods of time at which the NE is collecting (that is, making available in the NE) measurement data.
- Measurement reporting
  - Measurement Report File Format Definition
  - The measurement related information to be reported has to be specified as part of the measurement. The frequency at which scheduled result reports shall be generated has to be defined.
- Measurement result transfer
  - Measurement results can be transferred from the NE to the EM according to the measurement parameters, and/or they are stored locally in the NE and can be retrieved when required;
  - Measurement results can be stored in the network (NEs or EM) for retrieval by the NM when required.

Fault Management

- Management of alarm event reports
  - Mapping of alarm and related state change event reports
  - Real-time forwarding of event reports
  - Alarm clearing
- Retrieval of alarm information
  - Retrieval of current alarm information on NM request
  - Logging and retrieval of alarm history information on NM request

D.3.4 Network Management Layer

From a QoS Monitoring perspective, the NML is responsible for the collection and processing of performance, fault, and usage data.

The NML QoS Monitoring layer provides the following functions:

- **Service Quality Management** – responsible for the overall quality of a service as it interacts with other functional areas to access monitored information, process that information to determine quality metrics, and initiate corrective action when quality level is considered unsatisfactory. Inputs to SQM include both performance and fault data.
- **Customer QoS Management** – includes monitoring, managing, and reporting the Quality of Service customers receive against what has been promised to the customer in Service Level Agreements and any other service related documents. Inputs to CQM include data from SQM and usage data.

D.4 QoS Management References

D.4.1 Policy Based QoS Provisioning References

The following documents apply to policy-based QoS provisioning:

[1] IETF RFC 3060: "Policy Core Information Model – Version 1 Specification", Moore et al., February 2001. http://www.ietf.org/rfc/rfc3060.txt

[2] IETF RFC 2251: "Lightweight Directory Access Protocol (v3)", M. Wahl, T. Howes, S. Kille, December 1997. http://www.ietf.org/rfc/rfc2251.txt

[3] IETF RFC 2940: "Definitions of Managed Objects for Common Open Policy Service (COPS) Protocol Clients" ,. A. Smith, D. Partain, J. Seligson. October 2000. http://www.ietf.org/rfc/rfc2940.txt

[4] IETF RFC 3084: "COPS Usage for Policy Provisioning (COPS-PR)"; K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Yavatkar, A. Smith. March 2001. http://www.ietf.org/rfc/rfc3084.txt

[5] IETF RFC 2748: "The COPS (Common Open Policy Service) Protocol", J. Boyle, R.Cohen, D. Durham, S. Herzog, R. Rajan, A. Sastry. January 2000, http://www.ietf.org/rfc/rfc2748.txt

[6] IETF RFC 2753: "A Framework for Policy-based Admission Control", R. Yavatkar, D. Pendarakis, R. Guerin. January 2000. http://www.ietf.org/rfc/rfc2753.txt

D.4.2 Policy Based QoS Monitoring References

The following documents apply to QoS monitoring:

[7] 3GPP TS 32.101: "3G Telecom Management: Principles and high-level requirements".

[8] 3GPP TS 32.102: "3G Telecom Management Architecture".

[9] 3GPP TS 32.401: "Telecommunication Management; Performance Management (PM); Concept and requirements".

[10] 3GPP TS 32.200: "Telecommunication Management; Charging Management; Charging Principles".

[11] 3GPP TS 32.205: "Telecommunications Management; Charging management; 3G charging data description for the CS domain".

[12] 3GPP TS 32.215: "Telecommunication Management; Charging Management; Charging Data Description for the Packet Switched (PS) Domain".

[13] 3GPP TS 32.600: "Telecommunication Management; Configuration Management; 3G Configuration Management; Concepts and main requirements".

[14] 3GPP TS 32.111-1: "Telecommunication Management; Fault Management; Part 1: 3G fault management requirements".

[15] IETF RFC 959: "File Transfer Protocol", J. Postel, J.K. Reynolds. Oct-01-1985. http://www.ietf.org/rfc/rfc0959.txt?number=959

[16] IETF RFC 1901: "Simple Network Management Protocol, v2", J.Case, K. McCloghrie, M. Rose, S. Waldbusser. January 1996. http://www.ietf.org/rfc/rfc1901.txt?number=1901

[17] IETF RFC 2573: "SNMP Applications", D. Levi, P. Meyer, B. Stewart. April 1999. http://www.ietf.org/rfc/rfc2573.txt?number=2573

[18] IETF RFC 1907: "Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)", SNMPv2 Working Group, J. Case, K.McCloghrie, M. Rose, S. Waldbusser. January 1996. http://www.ietf.org/rfc/rfc1907.txt?number=1907

[19] TelemanagementForum (TMF) Telecom Operations Map (TOM), GB910, Approved Version 2.1, March 2000. http://www.tmforum.org/

[20] TelemanagementForum (TMF) TOM Application Note, Mobile Services: Performance Management and Mobile Network Fraud and Roaming Agreement Management, GB910B, Public Evaluation Version 1.1, September 2000. http://www.tmforum.org/

[21] TeleManagement Forum (TMF) NGOSS specifications http://www.tmforum.org/

[22] 3GPP TS 23.207: "End to End Quality of Service QoS Concept and Architecture".

[23] 3GPP TS 29.207: "Policy Control over Go interface".

[24] 3GPP TS 52.402: "Telecommunication management; Performance Management (PM); Performance measurements - GSM".

[25] 3GPP TS 32.403: "Telecommunication management; Performance Management (PM); Performance measurements - UMTS and combined UMTS/GSM".

Annex E (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
Dec 1999	S_06	SP-99577	--	--	Approved at TSG SA #6 and placed under Change Control	--	3.0.0
Mar 2000	S_07	SP-000014	001	--	Clarify use of X.25 as a Network Layer Protocol	3.0.0	3.1.0
Mar 2000	S_07	SP-000014	002	--	Correction of IRP-related terminology	3.0.0	3.1.0
Mar 2000	S_07	SP-000014	003	--	Clarification of Software Management	3.0.0	3.1.0
Mar 2000	--	--	--	--	Cosmetic	3.1.0	3.1.1
Jun 2000	S_08	SP-000225	004	--	Add and Update Correct Normative Reference List	3.1.1	3.2.0
Jun 2000	S_08	SP-000226	005	--	Terminology corrections	3.1.1	3.2.0
Dec 2000	S_10	SP-000522	006	--	Update references to allow both CORBA Versions 2.1 and 2.3	3.2.0	3.3.0
Mar 2001	S_11	SP-010022	007	--	Removal of Reference to 32.105 (not available for R99).	3.3.0	3.4.0
Mar 2001	S_11	--	--	--	Automatic upgrade to Rel-4	3.3.0	4.0.0
Apr 2001	--	--	--	--	Created Rel-4 from the latest R99 version (3.4.0 instead of 3.3.0)	3.4.0	4.0.1
Jun 2001	S_12	SP-010231	008	--	Scope update for Rel4	4.0.1	4.1.0
Jun 2001	S_12	SP-010231	009	--	Updates and Corrections for Rel4	4.0.1	4.1.0
Jun 2001	S_12	SP-010231	010	--	Alignment with TMF GB910 and associated Editorial improvements	4.0.1	4.1.0
Jun 2001	S_12	SP-010231	011	--	Update and re-organisation of clause 8 (Functional Architecture)	4.0.1	4.1.0
Jun 2001	S_12	SP-010231	012	--	Introduce Subscription Management	4.0.1	4.1.0
Jun 2001	S_12	SP-010231	013	--	Introduction of QoS Management Annex	4.0.1	4.1.0
Jun 2001	S_12	SP-010231	014	--	Update the definition of IRP terminology	4.0.1	4.1.0
Jun 2001	S_13	SP-010465	015	--	Reference Corrections	4.1.0	4.2.0
Mar 2002	--	--	--	--	Cosmetics	4.2.0	4.2.1
Mar 2002	S_15	SP-020013	016	--	Correction and update to QoS Management (alignment on Policy Management with S2, CN3 in 23.207, 29.207)	4.2.1	5.0.0
Mar 2002	S_15	SP-020013	017	--	Introduction of Subscriber and Equipment Trace Management	4.2.1	5.0.0
Mar 2002	S_15	SP-020013	018	--	Update of Accounting Management to cover the IMS (alignment with SA5's 32.200 Charging management; Charging Principles)	4.2.1	5.0.0
Sep 2002	S_17	SP-020449	019	--	Introduction of a new subcaluse (7.12) on O&M of the UMTS "Management Infrastructure"	5.0.0	5.1.0
Dec 2002	S_18	SP-020726	020	--	Aligning IRP related terminology with SA5's SWGC IRP specifications (32.6xy)	5.1.0	5.2.0
Mar 2003	S_19	SP-030043	021	--	Align QoS Terminology with SA2's 23.207 & CN3's 29.207	5.2.0	5.3.0
Jun 2003	S_20	SP-030266	022	--	Correction and update of Management System Interactions	5.3.0	5.4.0
Sep 2003	S_21	SP-030401	023	--	Removal/Replacement of the term UMTS - Alignment with SA1/2 specifications	5.4.0	5.5.0
Jun 2004	S_24	SP-040239	024	--	Subscription Management Corrections - Align with SA5's 32.140/1	5.5.0	6.0.0
Jun 2004	S_24	SP-040239	025	--	Align with SA5 SWGC WT01 Security terminology and architecture	5.5.0	6.0.0
Dec 2004	SA_26	SP-040768	026	--	Add sftp (secure ftp) as a valid File Transfer Protocol - Align with 32.341 File Transfer IRP Requirements	6.0.0	6.1.0

History

Document history		
V6.1.0	December 2004	Publication