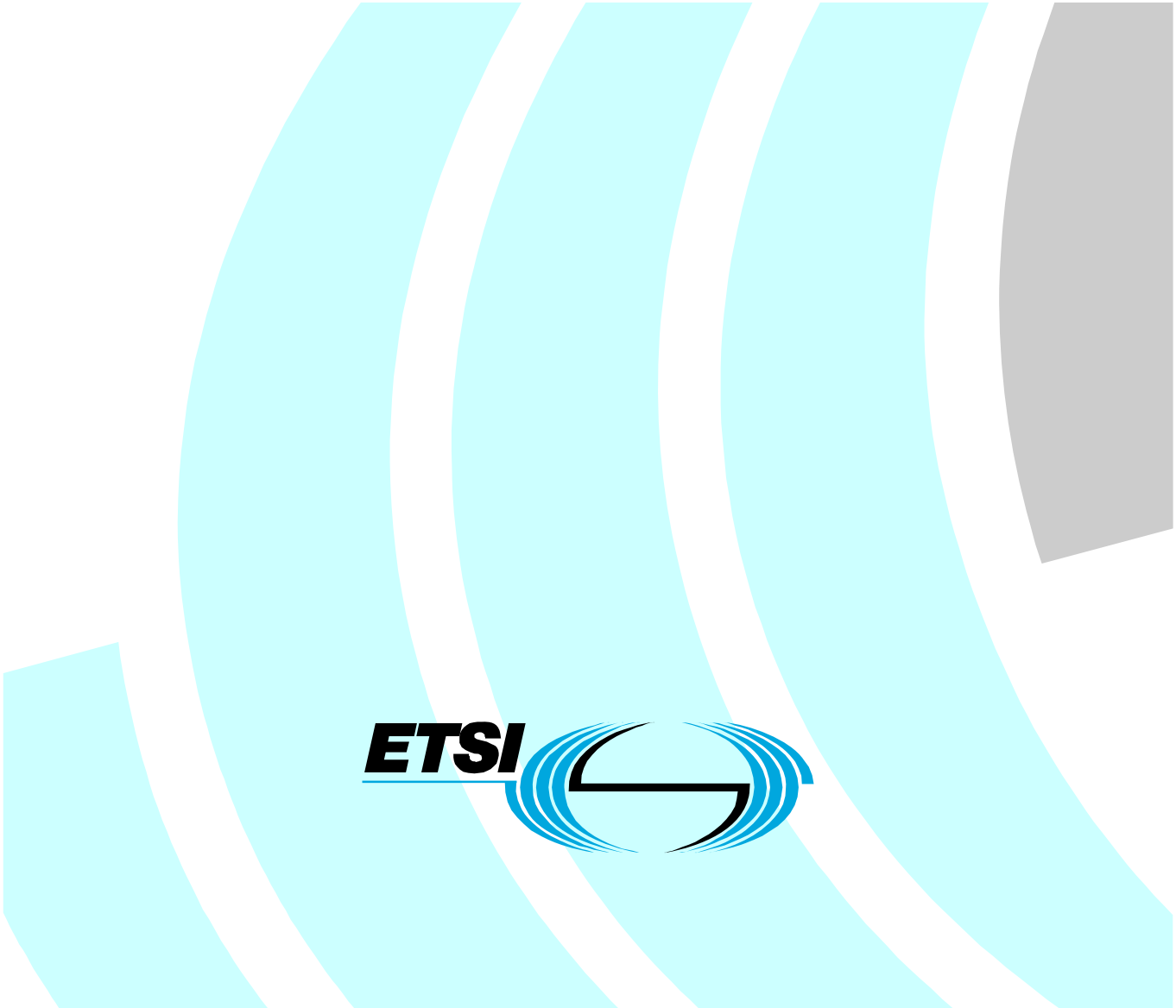
ETSI TS 102 672 V1.1.1 (2009-11)

Technical Specification

Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Management Functional Architecture



Reference
DTS/SES-00289

Keywords
architecture, broadband, management,
multimedia, satellite

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

Contents

Intellectual Property Rights

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

Introduction

The focus of the present document is on the functional architecture of network management for BSM systems, including the management of IP-based services.

Network Management of IP-based broadband satellite multimedia (BSM) systems may be chosen to be similar in many ways to that of terrestrial networks. However there are important differences in emphasis, for example in that the management traffic overhead across a satellite system should be minimised. Also the scalability of satellite networks interconnecting potential many terminals must be considered. Furthermore, integrated management of satellite and terrestrial IP networks has not been widely implemented and a standardised approach is considered desirable.

The BSM network management system (BNMS) should also be designed to cope with the latency and bandwidth asymmetry that are characteristic of satellite links. However the timescale of management operations is usually of an order that does not impose tight time constraints or high data rates.

1 Scope

The present document defines an open specification dealing with scenarios and functional network architectures for the management plane (M-plane) of Broadband Satellite Multimedia (BSM) systems, including any potential interfaces with external or higher level network management functions. The BSM management functions should include, for example, performance management, security management and QoS management, including the associated management functions of Service Level Agreements (SLAs) and Policies.

The BSM management functional architecture will take into account requirements for emerging IP-centric (Internet Protocol) broadband multi-service satellite-based networks, integrated with fixed and wireless (broadband) access networks on one side, and backbone networks on the other. This internetworking and service interoperability scenario is generally within the scope of Next Generation Networks.

The boundaries of the BNMS will be defined as well as the interfaces, protocols and message types on the internal and external interfaces. The specification will include, where appropriate, the BSM SI-SAP protocol stack interface including its interactions with higher and lower layers.

The architecture specified will be concerned mainly with the lower layers of the management functional layers, particularly the service management, network layer management and network element management, which will allow maximum flexibility for compatibility and mediation with OSS equipment as well as for Operators in building functionality as they see fit.

2 References

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

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] IETF RFC 1213: "Management Information Base for Network Management of TCP/IP-based internets: MIB-II".

[2] IETF RFC 1445: "Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)".

[3] IETF RFC 2578: "Structure of Management Information Version 2 (SMIv2)".

[4] IETF RFC 3411: "An Architecture for Describing SNMP Management Frameworks".

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

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

2.2 Informative references

The following referenced documents are not essential to the use of the ETSI deliverable but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI TR 101 984: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Services and architectures".

[i.2] ETSI TS 102 429-4: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Regenerative Satellite Mesh - B (RSM-B); DVB-S/DVB-RCS family for regenerative satellites; Part 4 : Specific Management Information Base".

[i.3] ETSI TS 188 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Management; Operations Support Systems Architecture".

[i.4] "Web-based Management of IP Networks and Systems". J-P Martin-Flatin, Wiley.

[i.5] "On the Evolution of Management Approaches, Frameworks and Protocols: A Historical Perspective". George Pavlou, J. Netw Syst Manage (2007) 15:425-445, Springer Science+Business Media, LLC 2007.

[i.6] IETF RFC 1155: "Structure and Identification of Management Information for TCP/IP-based internets".

[i.7] IETF RFC 1156: "Management information base for network management of TCP/IP-based internets".

[i.8] IETF RFC 1157: "Simple Network Management Protocol".

[i.9] IETF RFC 1451: "Manager-To-Manager MIB".

[i.10] IETF RFC 1901: "Introduction to Community-based SNMPv2".

[i.11] IETF RFC 1902: "Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)".

[i.12] IETF RFC 2741: "Agent Extensibility (AgentX) Protocol Version 1".

[i.13] IETF RFC 3415: "View-based Access Control Model".

[i.14] IETF RFC 3418: "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)".

[i.15] IETF RFC 3444: "On the Difference between Information Models and Data Models".

[i.16] IETF RFC 3584: "Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework".

[i.17] IETF RFC 4741: "NETCONF Configuration Protocol".

[i.18] ETSI TR 101 790: "Digital Video Broadcasting (DVB); Interaction channel for Satellite Distribution Systems; Guidelines for the use of EN 301 790".

[i.19] draft-combes-ipdvb-mib-rcs-05.txt: "DVB-RCS MIB".

[i.20] SatLabs System Recommendations Part 3:"Management & Control Planes Specifications v2".

[i.21] ITU-T Recommendation M.3000: "Overview of TMN Recommendations".

[i.22] ITU-T Recommendation M.3050.0: "Enhanced Telecom Operations Map - Introduction".

[i.23] ITU-T Recommendation M.3060: "Principles for the Management of the Next Generation Networks".

[i.24] ITU-T Recommendation X.901-X.904: "Reference Model of Open Distributed Processing: Overview".

[i.25] TeleManagement Forum TMF 053: "NGOSS Technology Neutral Architecture".

[i.26] Telemanagement Forum document number GB921: "eTOM, The Business Process Framework for the Information and Communications Services Industry".

[i.27] ISO/IEC 9595: "Information technology - Open Systems Interconnection - Common management information service definition".

[i.28] ISO/IEC 9596-1: "Information technology - Open Systems Interconnection - Common management information protocol".

[i.29] Distributed Management Task Force: "Common Information Model (CIM) Infrastructure Specification, DSP0004".

[i.30] The Object Management Group (OMG): "MDA Specifications".

NOTE: See http://www.omg.org/mda/specs.htm

[i.31] ITU-T Recommendation Y.2001: "General overview of NGN".

[i.32] IETF RFC 4022: "Management Information Base for the Transmission Control Protocol (TCP)".

[i.33] IETF RFC 4113: "Management Information Base for the User Datagram Protocol (UDP)".

[i.34] IETF RFC 4293: "Management Information Base for the Internet Protocol (IP)".

[i.35] IETF RFC 2863: "The Interfaces Group MIB".

[i.36] IETF RFC 4133: "Entity MIB (Version 3)".

[i.37] IETF RFC 4268: "Entity State MIB".

[i.38] IETF RFC 3877: "Alarm Management Information Base (MIB)".

[i.39] IETF RFC 1441: "Introduction to version 2 of the Internet-standard Network Management Framework".

[i.40] IETF RFC 1452: "Coexistence between version 1 and version 2 of the Internet-standard Network Management Framework".

3 Definitions and abbreviations

3.1 Definitions

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

agent: entity that acts in a managed role

architecture: abstract representation of a communications system

NOTE: Three complementary types of architecture are defined:

- **functional architecture:** discrete functional elements of the system and the associated logical interfaces
- **network architecture:** discrete physical (network) elements of the system and the associated physical interfaces
- **protocol architecture:** protocol stacks involved in the operation of the system and the associated peering relationships

control plane: layered structure that performs the call control and connection control functions; it deals with the signalling necessary to set up, supervise and release calls and connections

Customer Premise Network (CPN): customer's private network

NOTE: In the simplest case, the CPN is just a single end-host or TE.

data link layer: second layer of the OSI model it provides connectivity between segments of the network (bridging); in addition the data link may perform session control and some configuration

data model: description of a specific data structure, with the way the data elements (in the structure) are defined and the relationship to each other

NOTE: It is normally used in software engineering to describe how data is represented and accessed (see also RFC 3444 [i.15]).

eTOM: business process model or framework that has the objective of describing and classifying the business processes required for a Service Provider; it analyses the processes to different levels of detail according to their significance and priority for the business

NOTE: eTOM uses hierarchical decomposition to structure the business processes according to which all of the processes of the enterprise are successively decomposed. Process elements are formalized by means of a name, a description, inputs/outputs, etc.

flow: flow of packets is the traffic associated with a given connection or connectionless stream having the same source host, destination host, class of service, and session identification

information model: formal representation of real-world objects and concepts, with associated relationships, constraints, rules, and operations, used to specify semantics in a given domain

NOTE: It includes things of interest (entities), relationships between these entities (associations), and details/characteristics of these entities (attributes). An information model provides formalism to the description of a problem domain without constraining how that description is mapped to an actual implementation in software. The possible mappings of the information model are the data models (see also RFC 3444 [i.15]).

management plane: provides two types of functions, namely layer management and plane management functions:

- **plane management functions:** performs management functions related to a system as a whole and provides co-ordination between all the planes. Plane management has no layered structure.
- **layer management functions:** performs management functions (e.g. meta-signalling) relating to resources and parameters residing in its protocol entities. Layer Management handles the Operation And Maintenance (OAM) of information flows specific to the layer concerned.

Management Information Base (MIB): virtual information store containing managed objects

NOTE: Objects in the MIB (identified by their OIDs) are essentially variables, and are typically defined using Abstract Syntax Notation One format (ASN.1).

Manager: entity that acts in a managing role

Network Control Centre (NCC): equipment that controls the access of terminals at the lower protocol layers (OSI Layer 2 and below) to a BSM network

Network Management Centre (NMC: equipment that manages the lower protocol layers (OSI Layer 2 and below) of a BSM network

Network Management System (NMS): equipment that manages a network at several or all protocol layers

Next Generation Network (NGN): (from ITU-T Recommendation Y.2001 [i.31]) packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies

NOTE: It offers unrestricted access by users to different service providers. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

Next Generation Operations Support System (NGOSS): Telecommunications Management Forum's (TMF's) core framework for developing, procuring and deploying operational and business support systems and software

NOTE: The term is also used elsewhere e.g. as the basis for TISPAN OSS standards.

Operations Support System (OSS): generic term for a suite of management functions that enable an enterprise to monitor, analyse and manage systems, resources and services

Service Level Agreement (SLA) (SP and ANO): SLA between a Service Provider and an Access Network Operator is usually characterized by a forward link guaranteed capacity for SP aggregated traffic expressed in kb/s and a return link guaranteed capacity for SP aggregated traffic expressed in kb/s

NOTE: It can also include other elements related to traffic policy and availability.

Service Level Agreement (SLA) (Subscriber and Service Provider): SLA between a SP and its subscriber is characterised by the choice of one data transfer capability and the allocation attribute related to this transfer capability

NOTE: The SLA is agreed upon by the subscriber at the initiation of the contract with the SP and will remain the same for all the contract duration.

Service-Oriented Architecture (SOA): (ITU-T) Service-Oriented Architecture (SOA) is a software architecture of services, policies, practices and frameworks in which components can be reused and repurposed rapidly in order to achieve shared and new functionality

NOTE: This enables rapid and economical implementation in response to new requirements thus ensuring that services respond to perceived user needs. SOA uses the object-oriented principle of encapsulation in which entities are accessible only through interfaces and where those entities are connected by well-defined interface agreements or contracts.

user: entity that uses the network services requested by the subscriber

user plane: layered structure and provides user information transfer, along with associated controls (e.g. flow control, recovery from errors, etc.)

3.2 Abbreviations

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

3GPP	Third Generation Partnership Project
ANO	Access Network Operator
API	Application Program Interfaces
BNMS	BSM Network Management System
BSM	Broadband Satellite Multimedia
CIM	Common Information Model
CLI	Command Line Interface
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off The Shelf
CPE	Customer Premise Equipment
CPN	Customer Premise Network
DEN	Directory Enabled Networks
DMTF	Distributed Management Task Force
DTD	Document Type Definition
eTOM	enhanced Telecom Operations Map
FAB	Fulfilment, Assurance and Billing
FCAPS	Fault, Configuration, Accounting, Performance and Security
HTTP	HyperText Transfer Protocol
IDL	Interface Definition Language
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organisation for Standardization
ISP	Internet Service Provider
ITU	International Telecommunications Union
JRMI	Java Remote Method Invocation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLA	Logical Layered Architecture
MIB	Management Information Base
NAP	Network Access Providers
NCC	Network Control Centre
NGN	Next Generation Network
NGOSS	Next Generation Operations Support System
NM	Network Management
NMC	Network Management Centre
NMS	Network Management System
NNI	Network to Network Interface
NOC	Network Operations Centre
OAM	Operation And Maintenance
OBP	On Board Processing
OID	Object Identifier
OMA	Object Management Architecture
OMG	Object Management Group
OSI	Open Standards Interconnection
OSS	Operations Support System
OSS/J	OSS through Java initiative
QID	Queue IDentifier
QoS	Quality of Service
RFC	Request For Comments
RMI	Remote Method Invocation
RM-ODP	Reference Model of Open Distributed Processing
RMON	Remote Monitoring
RSVP	Resource ReserVation Protocol
SD	Satellite Dependent
SI	Satellite Independent

SI-SAP	Satellite Independent-Service Access Point
SLA	Service Level Agreement
SMI	Structure of Management Information
SMIv2	Structure of Management Information version 2
SNMP	Simple Network Management Protocol
SNO	Satellite Network Operators
SO	Satellite Operator
SOA	Service-Oriented Architecture
SP	Service Provider
ST	Satellite Terminal
TCP	Transmission Control Protocol
TMF	Telecommunications Management Forum
TMN	Telecommunications Management Network
TOM	Telecom Operations Map
TR	Technical Report
TS	Technical Specification
UDP	User Datagram Protocol
UML	Universal Modelling Language
WBEM	Web-Based Enterprise Management
XML	eXtensible Markup Language

4 Overview and Background

Network Management should be seen as a means of enabling operators to configure their networks easily, quickly and cost-effectively, in order to provide users with flexible and efficient services which can be adapted to their needs in the latest service environments (e.g. compatible with a Service-Oriented Architecture (SOA)). This should include fast addition and deletion of users, monitoring and management of QoS, network topology management, fault diagnosis and billing.

Network Management is taken to mean all layers of the management stack, from element layer at the bottom to business layer at the top, whether the network being managed is a sub network or a complete end-to-end network. This is distinct from the network layer protocol (in the user and control plane) which is concerned with end-to-end communications.

Operational Support Systems (OSS) is the term usually given to the suite of management application functions that provide the manager with high level support and control interface to lower level management data from network elements. In practice an OSS is often a complex and heterogeneous assembly of equipment and implementations due to the number of functions they must support, and due to their potential incremental historical implementation and organisation in hardware and software, owing to legacy and business constraints.

There is a range of alternative potential NM standards and solutions as described in annex B. The choice of approach depends on for example:

- cost -effectiveness;
- flexibility (scalability, ease of update, modularity for additional functions);
- reliability (redundancy, reconfigurability);
- security;
- transmission bandwidth;
- legacy entity compatibility.

The present document focuses on the network management system outside the OSS and is concerned with extraction and configuration of management data.

4.1 Existing Solutions and Standards

State There is a range of potential solutions for BSM network management architecture (e.g. centralised or distributed) which offer different advantages and disadvantages. In addition, the type of management information representation and communication protocol often dictates a type of architecture; SNMP is probably the best known of these protocols and it imposes a centralised architecture and certain other constraints such as the need for polling of MIBs, which results in repetition of retrieved data even if no changes in MIB data have occurred.

However Web-based network management is one alternative which is becoming more common as owing its lower cost and technical advantages. A common arrangement is to use SNMP for fault event management (such as alarms) and use XML for configuration, performance, security and accounting functions.

In the world of telecommunications networking there are currently several approaches to defining and standardising network management architectures.

The main technological approaches that have been, or are being, standardised are:

1) The SNMP architecture defined by the RFC 3411 [4].

2) The TMN (Telecommunications Management Network) [i.21] defined by the ITU and ISO, and based on the CMIP protocol and CMIS architecture.

3) The NGOSS (Next Generation Operations Support System) [i.24] OSS/J (OSS through Java Initiative) and enhanced Telecom Operations Map (eTOM) defined by the Telecommunications Management Forum (TMF).

4) The Object Management Architecture (OMA) based on CORBA from the Object Management Group (OMG).

5) COPS-PR (IETF) for configuration (e.g. as a complement to SNMP).

6) The Common Information Model (CIM) [i.29] and Web-Based Enterprise Management (WBEM) defined by the Distributed Management Task Force (DMTF).

7) The NGN Operations Support Systems Architecture defined by ETSI TISPAN [i.3].

Other initiatives include, for example, Java/RMI from Sun, the Model-Driven Architecture (MDA) as a development of the OMA [i.30], and several web-based designs using Java.

An overview of the main approaches is given in Annex A. In spite of the efforts over recent years in defining the above approaches, there is still no universally accepted solution for all aspects of network management, but typically a collection of separate complementary solutions are employed depending on their strengths (e.g. SNMP for network monitoring, NETCONF [i.17] for configuration, and vendor-specific solutions for large-scale network monitoring e.g. traffic engineering and data collection.

The approach to BSM management should take into account as many of the above approaches as possible, focussing on those in use today and on the most likely candidates for the future.

Of the above approaches, SNMP is widely adopted, but mainly for relatively simple tasks, like Fault Management and read-only type operations, e.g. to obtain the current configuration and to retrieve performance data. Although designed for IP networks, SNMP has many disadvantages in today's OSS environments, such as that it:

- does not scale well due to reliance on polling, which generates redundant traffic even in the absence of faults or alarms;
- has a limited instruction set and is not suited to management above element layer;
- is not object-orientated and does not suit distributed managers and agents;
- uses UDP, the unreliability of which is a factor especially for network configuration;
- has security mechanisms that are only available if SNMPv3 is implemented.

The TMN/CMIP manager-agent protocol paradigm has proven too complicated and expensive for most applications (even if the overall TMN requirements e.g. FCAPS are still valid).

The Web-Based Enterprise Management (WBEM) standard has not yet "taken off" even if the CIM is implemented on Windows platforms (amongst others). The enterprise management frameworks seem to be too expensive, complex to implement and the return-on-investment is not proven.

The TMF's efforts on NGOSS seem promising. The next steps are to agree on the "Shared Information Model" and to implement a process engine.

The trend today is towards use of http to allow OSS servers and clients to communicate in order to support distributed services that also use the Web. This represents convergence in that both the services and their OSS are tending to use distributed software components that communicate using the Web.

4.2 Availability of NMS/OSS solutions

There are commercial and freeware (including open source) network management systems (e.g. Xymon [previously hobbit], OpenNMS, zenoss, Nagios.) available which usually employ the term OSS for these products. However while vendors claim to offer complete OSS solutions, they are often adapted for a specific type of operator and aim at an off-the-shelf solution to suit a particular need. Therefore, such a readily available OSS may pose a number of disadvantages:

- Single-vendor OSS's often have unique implementations and do not perform all required tasks equally well.
- Multi-vendor support i.e. the freedom to select network equipment from other supplier may be restricted.
- Flexibility for future adaptation to services and networks is not always adequate.

A general definition of OSS requirements and architecture is considered necessary in order to provide a sound basis for a BSM operator to define his overall requirements.

5 BSM network management functional requirements

This clause clarifies the functions required for the overall management process.

The overall requirements of NMS's for terrestrial networks (see clause 5.2) are generally applicable to satellite networks.

However, satellite networks have some specific constraints compared with terrestrial networks, for example:

- the management traffic overhead across a satellite system should be minimised;
- the scalability of satellite networks interconnecting potentially many terminals must be considered;
- Latency and possible bandwidth asymmetry.

The first of these constraints is justified by the valuable satellite resources and thus the need to reduce management overhead. A protocol such as SNMP is not bandwidth-efficient since the manager relies on regular polling (pull model) of remote network elements (e.g. BSM STs) to obtain management status information, and this generates repeated data and redundant traffic. Also SNMP data is not compressed. Furthermore as the number of STs may become very large in a practical network, the SNMP polling of STs generates an increasing amount of traffic which has to be budgeted for in always-on satellite management channels.

Functions and protocols which generate management messages only when new data is present, and which can compress data, are therefore preferred. This requires agents to be more intelligent in order to react when necessary and to generate adapted messages (i.e. push model). SNMP Traps are an example of such messages.

5.1 Management Functions

The overall management requirements adopted by NMS's and OSS's today fall into the following main categories:

- FCAPS defined for the TMN by the ITU [6].
- The TOM from the TMF, which is a development of FCAPS.
- The eTOM from the TMF in which FCAPS has been re-classified as Operations Support, Fulfilment, Assurance and Billing.

Annex A describes these models in more detail.

The FCAPS Model has been defined for DVB-RCS systems by Satlabs in [i.20].

5.2 Management logical layered model

The concept of hierarchical 'horizontal' logical layers in TMN [5] is usually shown in the pyramid form of figure 1. The Logical Layered Architecture (LLA) structures the management functions and describes the relationships between layers. A logical layer reflects particular aspects of management arranged by different levels of abstraction.

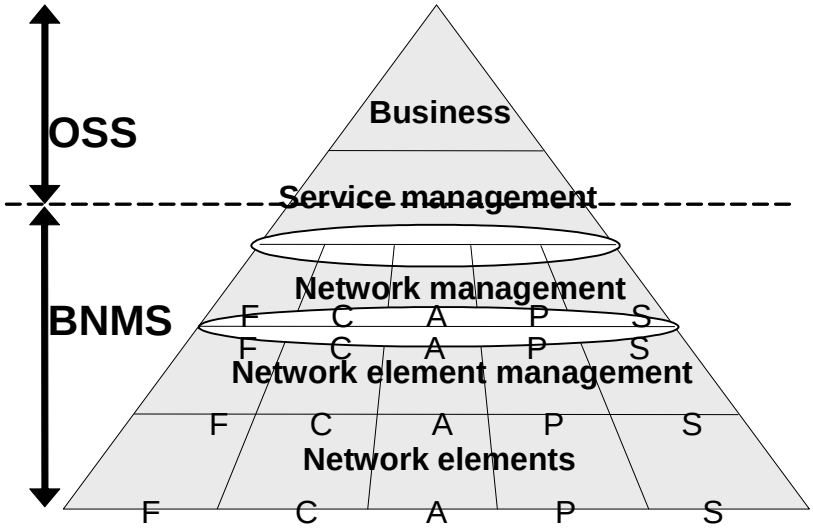


Figure 1: TMN NM Logical Layered Architecture (LLA) showing BSM-specific layers

The eTOM model retains this concept of layering and develops it further in [i.22].

As indicated in figure 1 the BSM Network Management System (BNMS) described herein is concerned with part of service management and the layers below. The service layer may be split into BSM-service-related functions and end-to-end network service functions. Higher layers are considered to be more generic and not specific to the BSM. These layers may be provided by readily available and configurable off-the-shelf software management systems (OSSs), as far as the BSM system is concerned.

In this model each layer is dependent on the services provided by the underlying layer.

At the lowest level, the BSM physical network is clearly a set of network elements (satellite terminals, hub stations, gateways, routers, servers, etc) as represented in the lowest level of figure 1, each of which should monitor its own fault status (F), be capable of reconfiguration (C), hold local user accounting data (ISP number, user account number) (A), report performance data (P) and possess password and link encryption data (S). Otherwise functions at this level have minimal management plane involvement in that they react to or control real time events, and are mainly involved in Control Plane or User Plane functions. For example, call management in a telecommunications switch would be performed at this level, where the switch would route a call in response to signalling.

Above this is the **Network Element Management** (device management) layer which manages the communications path. At this layer (containing the management functions required to operate single pieces of equipment), the BSM should be capable of autonomous reconfiguration in response to a number of fault states (F and C). It should be capable of responding to performance requirements, for example, uplink power control (P). In the case of Accounting, it should be capable of holding several user accounts per multi-user terminal.

The next higher layer is the **Network Management** layer, concerned predominantly with the management of element managers. Resource management is generally performed at this level, although resource allocation can also occur in all lower levels. In a heterogeneous network the NM layer may be partitioned between different subnetworks, each part being responsible for network layer (e.g. IP) aspects in that subnetwork.

NOTE: Network Management here is applies mainly to the Network Layer (L3) protocol, as a subset of the overall Network Management System (NMS).

The above model shows the FCAPS functions present at each of the three lower network layers. The intention is that, for example, the Fault function of a network element reports to the fault function in the element controller which in turn provides a summary report to the network management system. In theory, if a device at any layer is designed to support FCAPS, the appropriate functions can communicate with their equivalent on another layer. The aim is easy integration of a management system. The difficulty with this approach is that many network devices and element controllers do not implement the full FCAPS functionality, so integration into a complete network management system may become difficult.

The **Service Management** layer is concerned with functions such as quality of service monitoring, billing functions, and planning. It is concerned with end-to-end service management in a similar way to Network Management, but again in a heterogeneous network the SM layer may be partitioned between different subnetworks, each part being responsible for service resources in that subnetwork.

The **Business Management** layer is concerned with the customer and stakeholder facing aspects of the system, the details of which are out of scope here.

5.3 Management Plane

The management functions are considered to be implemented via communications protocols over the shared network, but in a plane independent from the control and user planes as shown in figure 2.

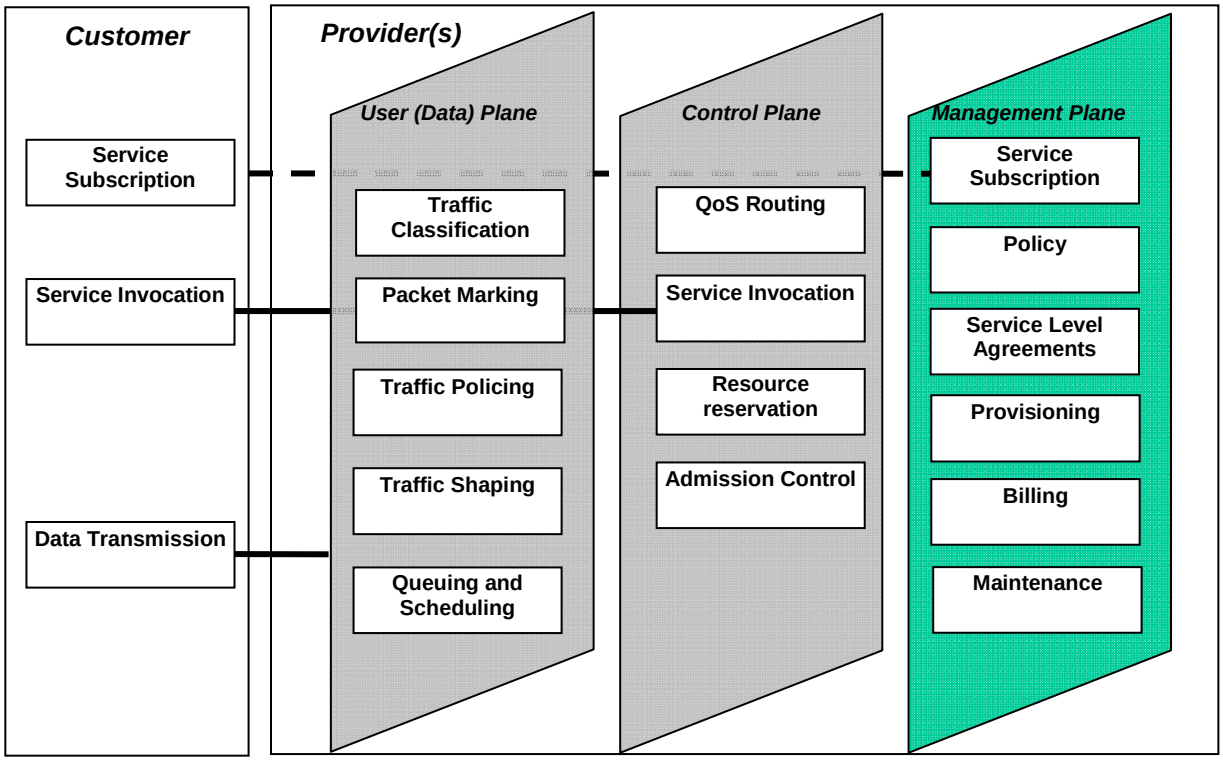


Figure 2: Management Plane relationships

Here the management functions shown are a representative sample of the FCAPS or eTOM sets. The interaction between the operators and the customer may begin from highest level with service subscription in the management plane. This would be followed by service invocation in the control plane, and subsequently with user plane transmission etc.

5.4 Security

Security for Management is clearly a requirement for the BMS, in the same way as for many other networks. Security can be achieved by encryption and authentication of management data at Link Layer for dedicated frames. Otherwise security is available at Layer 3 and above, for example through SNMP security or through secure http (https). Further security considerations are outside the scope of the present document.

5.5 BSM Recommendations

The BSM NMS shall adopt the following models as a basis for architectural definition:

1) The Logical Layered Architecture (see figure 1), in particular the lower layers as indicated.

2) The FCAPS functional model.

6 BSM Network Management Scenarios

This clause first describes scenarios involving relationships between BSM network actors including users, operators and providers of different types for the purpose of providing a managed service in clause 6.1. These relationships generally invoke, for example, SLA's (service level agreements) between the actors.

The actors have their own network management entities which may need to communicate with each other to provide end-to-end service management. Examples of the communication flows between these entities are then described in clause 6.2.

The scenarios lead to a global network management architecture description in clause 6.3.

6.1 Management Relationships between BSM Network Actors

The relationship and hierarchy between BSM network actors is shown in figure 3.

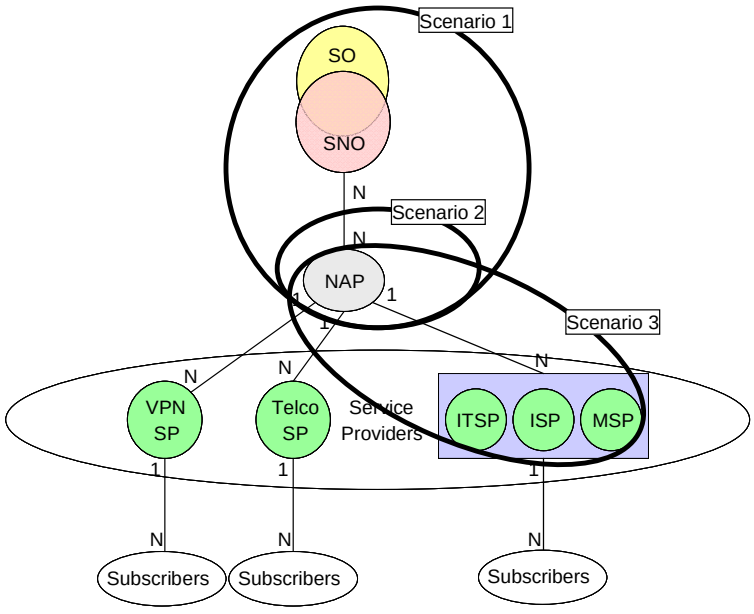


Figure 3: Relationships between BSM network actors

For a full description of these actors see [i.1]. An important concept embedded in figure 3 is that several NAPs can be present per SNO i.e. the NAPs can share the capacity of satellite payloads or transponders by means of layer 1 and 2 protocol techniques.

SO and SNO are always considered together because either they do not exchange NM data, or this exchange is invisible to the NAP (or BSM network operator), and any such exchange is out of scope of the present document.

NOTE: The role of the SO is out of scope in the present document.

The management entities associated with the relevant actors are as follows:

Table 1: BNMS actors and associated management entities

Actor	Management Entities
Satellite Operator (SO)	
Satellite Network Operators (SNO)	NOC (Network Operations Centre)
Network Access Providers (NAP) (also known as BSM Network Operator)	BNMS + BSM elements BNMS includes NMC (Network Management Centre) for layer 2 and private management
Service Providers (SP)	Service Manager
Subscribers	CPE network manager + CPE elements (Examples would be Access Gateway [e.g. residential gateway, or corporate gateway] for management of PEPs, SLAs, etc.) (no management of ST/NAP contract)
Users (or end-users)	Service Management client

The primary focus of the present document is on the NAP and its associated NMC and BNMS including interfaces to the SP.

Scenarios showing different groupings of BSM actors and different arrangements of the associated "ownership" of NMC/NCC are shown in clause 6.2.

6.2 Scenarios of relationships between network actors

The following scenarios illustrate options and business relationships between actors when the BSM network is considered as an access network.

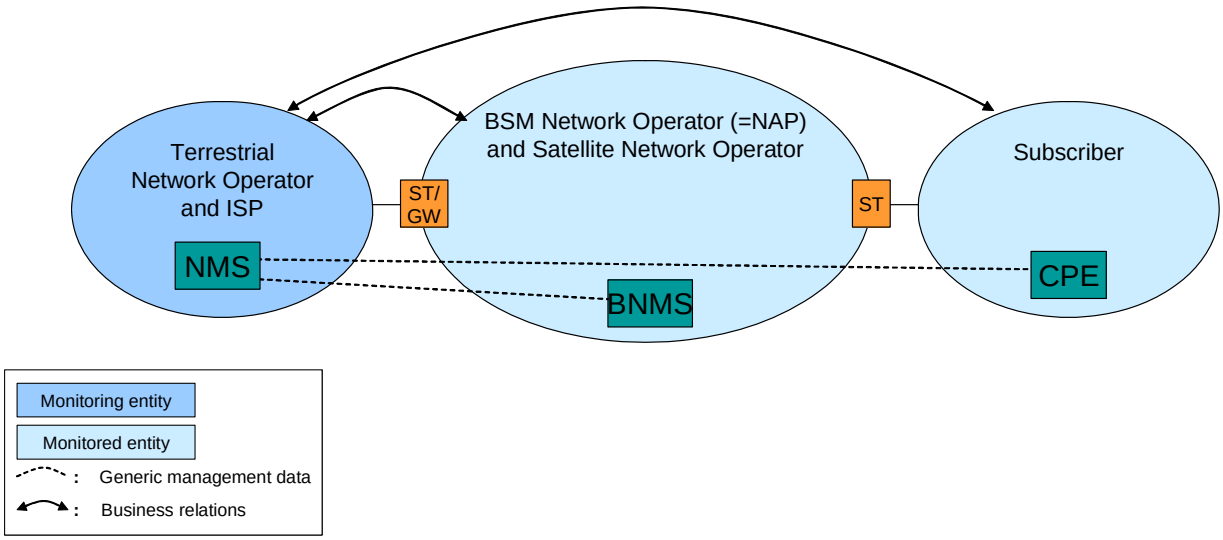


Figure 4: Scenario BSM Access 1

In this scenario the NMS needs to interrogate the BNMS about any remote networks (e.g. attached CPE's). Information can concern Faults, Accounting, Performance, and Security (but Configuration unlikely).

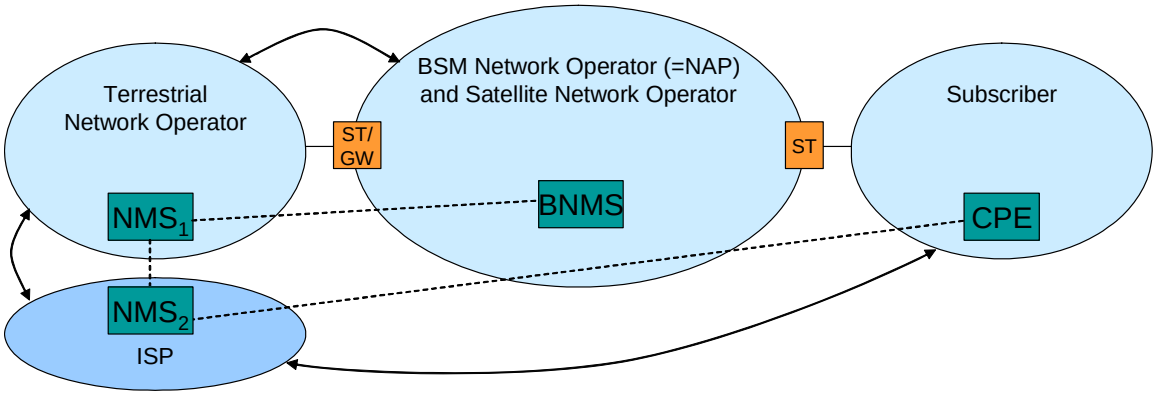


Figure 5: Scenario BSM Access 1a

This scenario is similar to Scenario 1 except NMS2 has the highest status (as far as user service subscription is concerned) and there is no business relationship between the ISP and the BSM NAP.

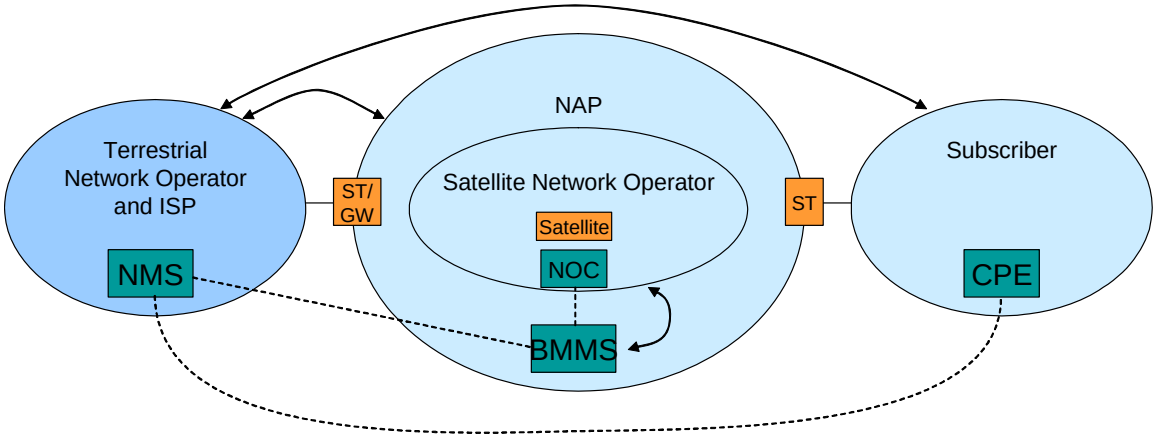


Figure 6: Scenario BSM Access 2

This scenario develops Scenario1 and shows the relationship between independent NAPs and SNOs.

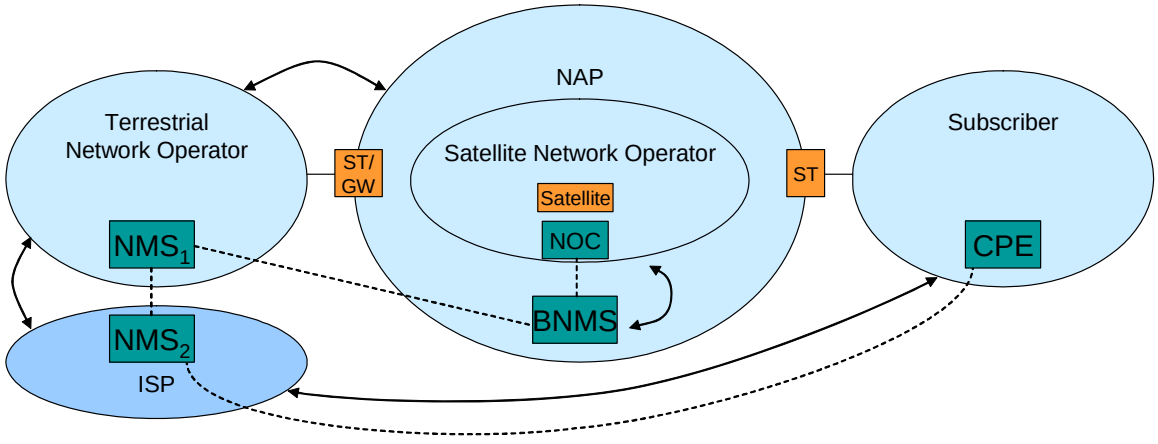


Figure 7: Scenario BSM Access 2a

This scenario develops Scenario 1a and shows the relationship between independent NAPs and SNOs.

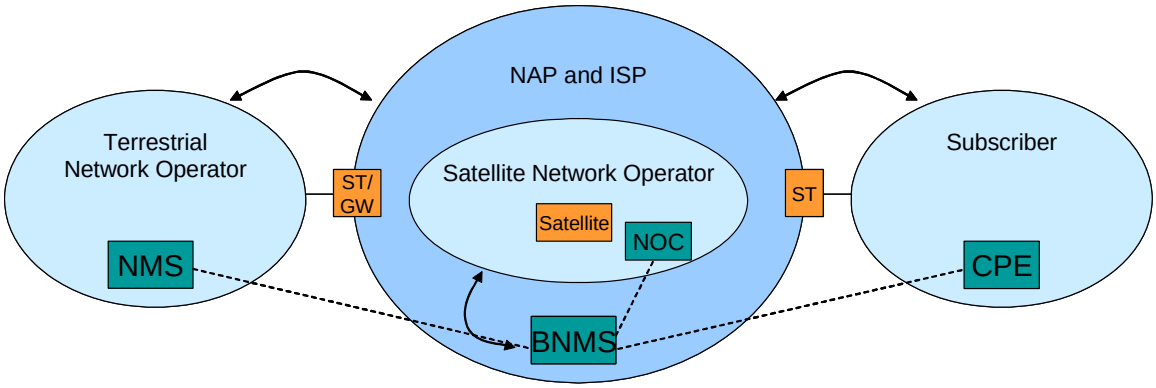


Figure 8: Scenario BSM Access 3

This scenario shows a variation of scenario 2a in the case where the NAP and ISP are the same and different business relationships exist.

6.3 Global Network Management Architecture

Figure 9 shows a general network management architecture for service provision. NMS messages flow generally vertically in the business model (shown with solid lines) while signalling functions (control plane) flow generally horizontally, i.e. the management plane and control plane are generally orthogonal to one another.

In general, SLAs should exist between all adjacent boxes in figure 9.

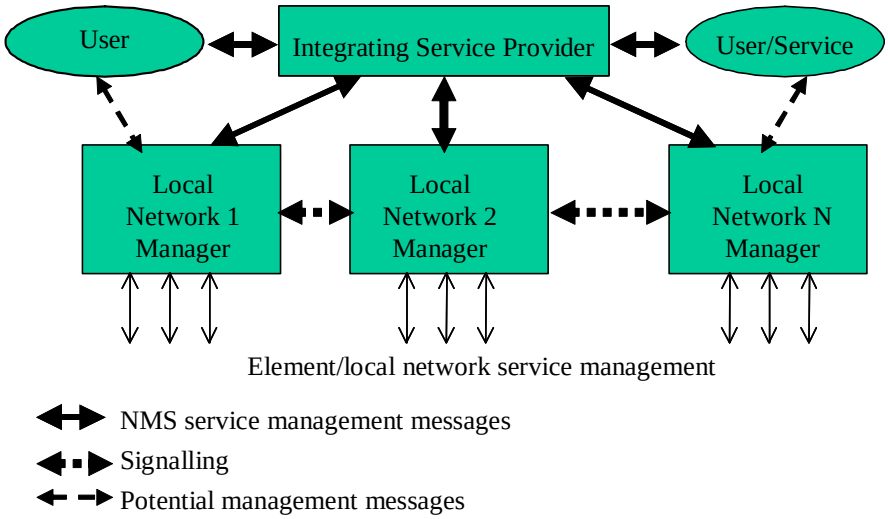


Figure 9 Generalised integrated OSS and Signalling paths

Negotiation for QoS parameters should be made in the control plane for a particular service. (Examples of inter-network signalling that carry QoS parameter requests are the IMS in mobile networks, the ATM-forum NNI, routing metrics in BGP4 and supplementary services in CCITT No 7). Then monitoring of performance parameters and management of the agreed SLA is done on the management plane. However, Network Operators are very reluctant to allow viewing, much less managing, of any NMS parameters, particularly those concerning performance measurements, in each other's networks. In practice therefore the global service management situation is fraught with political and commercial difficulties.

6.4 BSM Service Management Scenarios

The following BSM service scenarios illustrate the main examples to be considered in the definition of the BSM Management Architecture. These scenarios assume that services, including network bearer services and higher layer services (content, etc.), are to be provided across the end-to-end network managed by a hierarchy of network managers, and in these examples by a higher level Service Manager which has overall responsibility. Lower level subnetwork managers are under the responsibility of this manager.

It should be noted that the control plane actions are not shown, but these would be used in a subsequent phase to set up connections after the management plane has been used to configure services (including authorisation, policy, billing, etc.).

6.4.1 Residential Internet Access Scenario

An example of an operational scenario for Residential Internet Access is shown in figure 10, which illustrates the physical and functional architecture and the interfaces considered. In this case the remote attached users (or their LANs) are connected to the ISP's network by means of a BSM system. The different management message flows are indicated by the appropriate arrows.

The BSM provides the access network to the Internet.

Here the user subscribes to a service provided by a content service provider or to a network service (that is not provided by the ISP). In this case the Service Manager has a integrating role and is responsible for management of lower level sub-network services (via SLA's, etc.) by negotiating service policy and SLA's etc. with the ISP's local Network Manager (NM) and other NM's in the Internet of equal status in terms of management hierarchy. Service invocation is then permitted in the control plane.

If there is no high layer service management, but simply a network service provided by the ISP, it is assumed that the ISP's NM is responsible for overall service management with delegation to the BSM NMC (with policy, SLA, etc.). The BSM NAP may be the ISP in which case the NMC would manage overall services.

The BSM contains the BNMS which manages the BSM and includes the NMC (for SD layer management). The BNMS manages the BSM network elements such as STs, Hub and NCC/satellite.

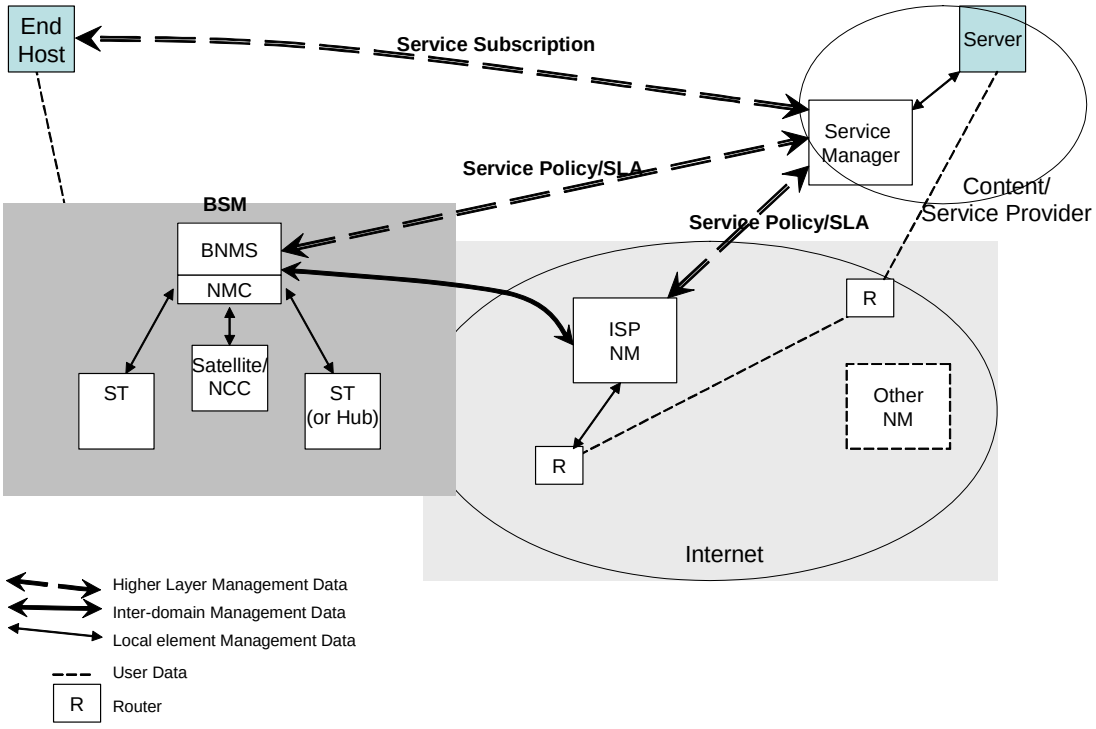


Figure 10: Residential Internet Access Scenario

6.4.2 Enterprise Office-LAN Interconnect Scenario A

An example of an operational scenario for a distributed enterprise office (or LAN interconnect) is shown in figure 11 In this case remote office LANs are integrated into the same enterprise network by means of a BSM system, using VPN links for example.

A high layer Service Manager may be invoked at some location in the integrated LAN, e.g. in the head office LAN. This Service Manager has a similar role to that in clause 6.4.1 and contains the higher layer manager for overall integrated LAN management. The LANs are assumed to have their own network managers (NM) responsible for their local network layer services. The Service Manager would normally include its own lower level NM for its own LAN.

The message flows are similar to figure 10, but the boundaries between management domains are different.

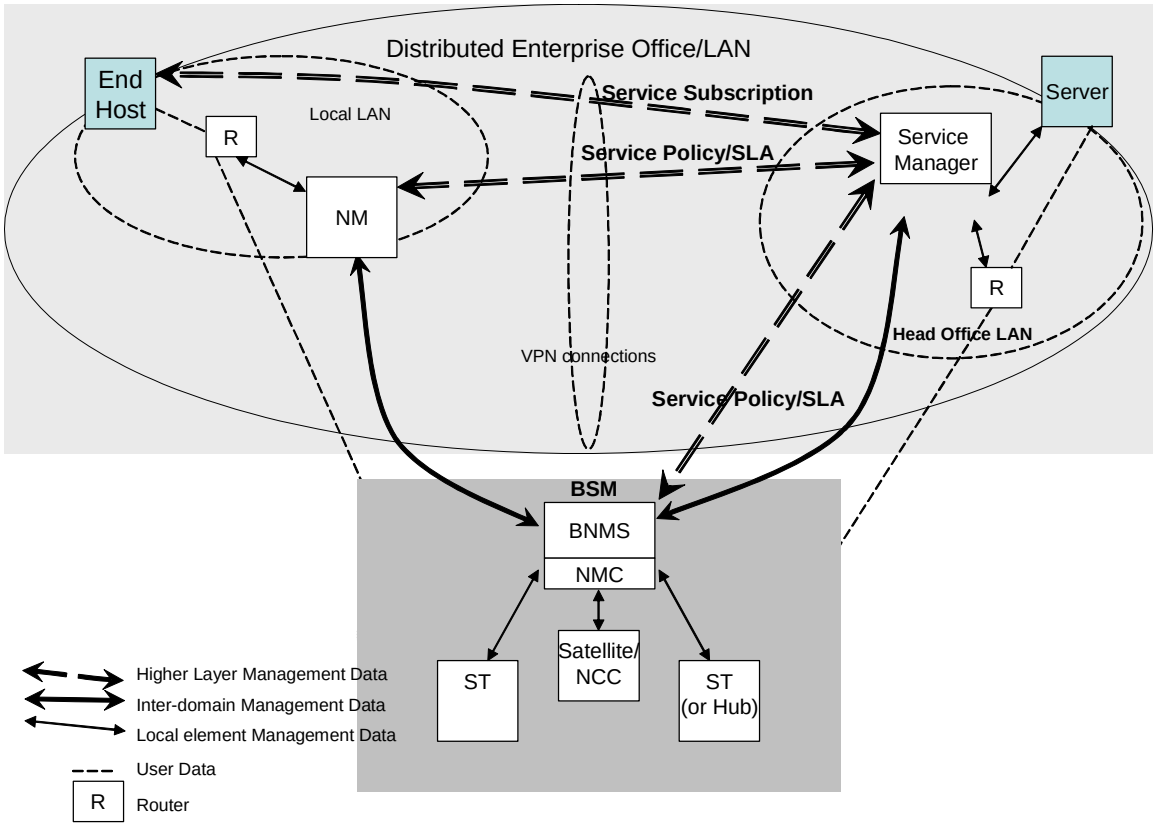


Figure 11: Enterprise Office-LAN Interconnect Scenario A

6.4.3 LAN Interconnect Scenario B

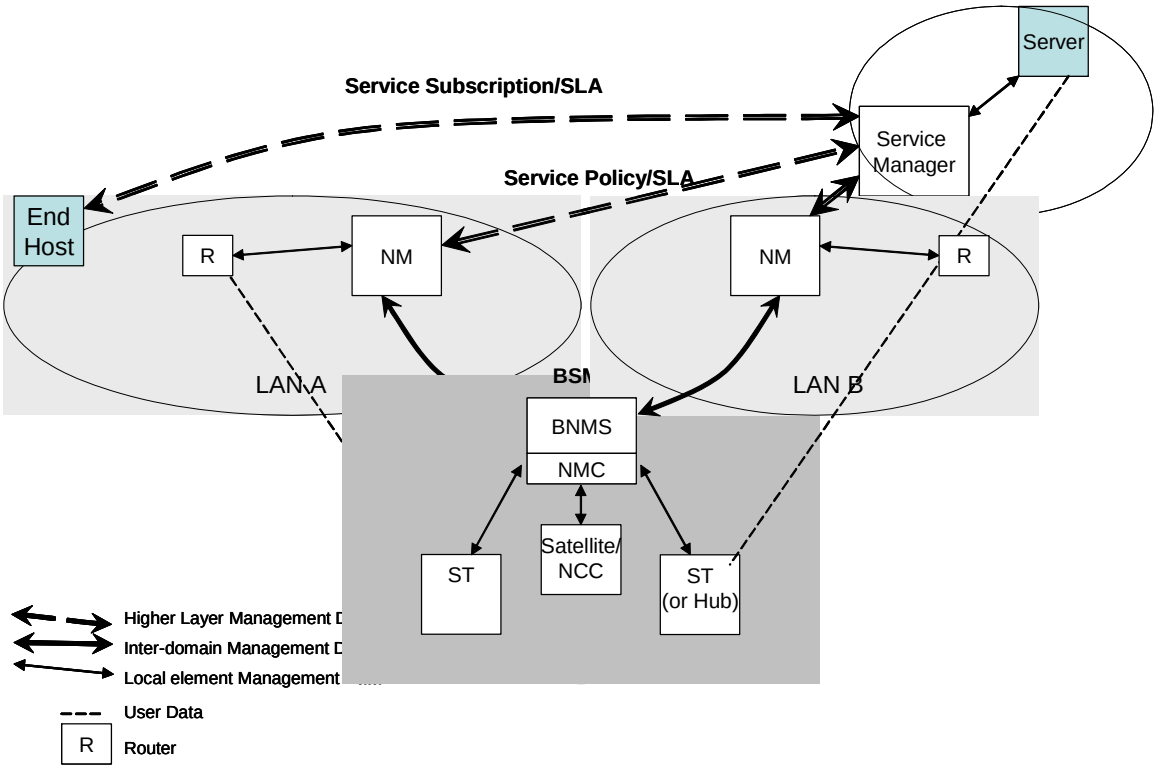


Figure 12: LAN Interconnect Scenario B

In this scenario there is no is no direct relationship between the Service Manager and the BNMS (i.e. this is a difference from Scenario A).

In this variation of the LAN interconnect scenario of clause 6.4.2, the remote LAN's are autonomous and of equal status in terms of management hierarchy. The service required by the end user is provided and managed externally to the LAN's by a content provider with higher layer Service management. The local network managers for each LAN could communicate at a peer level with the BSM NMC e.g. if SLA's are pre-established. If new network services need to be negotiated dynamically with the user, then one NM (or BNMS) needs to be nominated as highest level manager.

In this case, unlike LAN Interconnect scenario A, there is no direct relationship between service manager and BNMS.

7 BSM Management Architecture

7.1 BSM Management Architecture Fundamentals

A centralised management architecture will be adopted for the BSM, that is a centralised manager communicating with agents installed in network elements. This architecture is considered best suited to a satellite system which suits a star network configuration with associated centralised control and management.

The approaches adopted in current satellite systems are mainly based on SNMP architecture, MIBs and protocols. This is often used in parallel with:

- existing proprietary techniques including CLI/Telnet (e.g. for element configuration);
- basic IP functions (e.g. ICMP including "Ping") for monitoring;
- newer technologies e.g. http and Web browsers and use of XML for database management.

The BSM Management Functional Architecture will allow these protocols to be operated in parallel.

The main network elements subject to management in a BSM system are as shown in figure 15.

The BNMS includes the NMC (of the NAP), as well as any managers of the network (e.g. SLA) and services. The network elements include:

- Satellite Terminals.
- Gateway ST.
- The NCC which is closely connected to the satellite (though possibly for OBP satellites the satellite itself could be separately addressed as a network element).
- Possible Application Servers within the BSM network.
- Potentially elements of CPE's accessing BSM services (these are considered as external to the BSM, but in some case may be part of the same management domain).

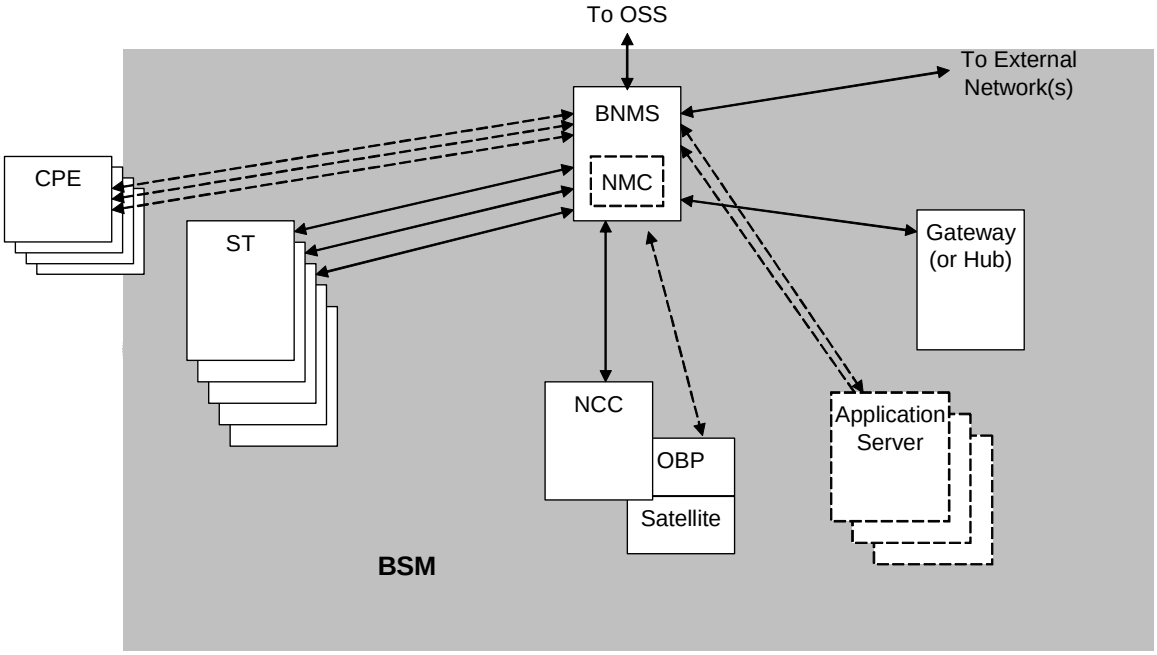


Figure 13: BNMS and managed elements

From a layered viewpoint the management functions may be depicted as follows, where an interface from the BNMS to a higher level OSS is available.

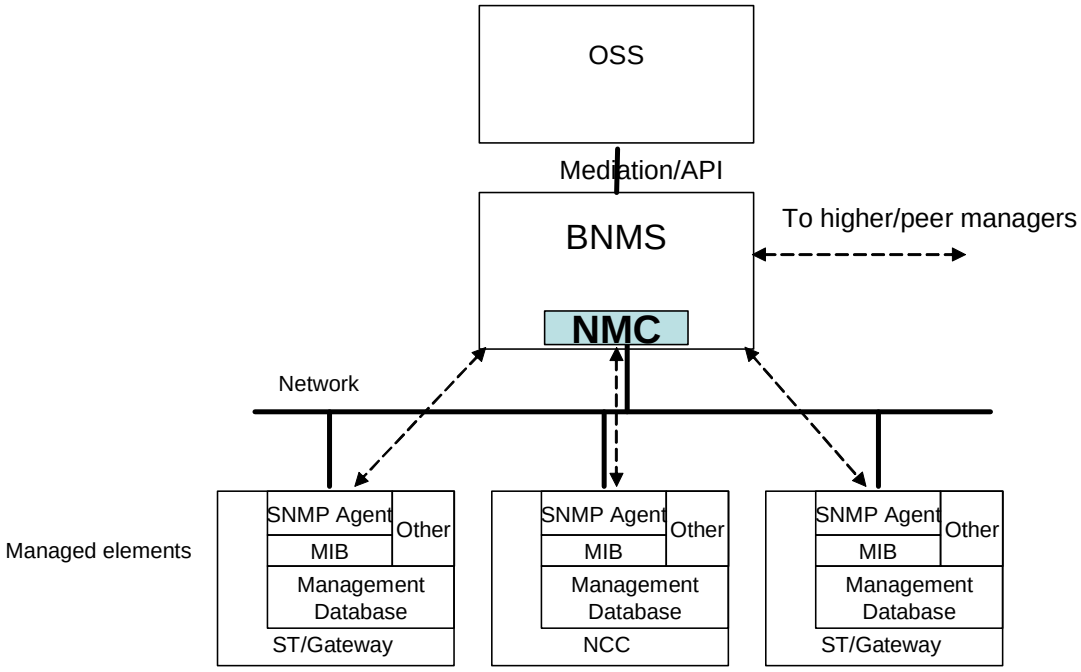


Figure 14: Management architecture showing database access and OSS relationship

7.2 BSM Management Functional Architecture

Taking into account the assumptions in clause 7.2 the core BSM Management Functional Architecture is shown in figure 15. This shows that the BNMS contains three main functional layers - Service, Network and Element Management.

SM is concerned with BSM services such as local SLAs. NM is concerned with aggregated IP layer service management, and EM is responsible for lowest level element management. At least part of the EM function is normally included in the NMC of the Satellite-Dependent functions.

Several protocols may be used to access data from network elements, including IP-based ICMP, Telnet, etc., SNMP, and http(s).

Configuration functions, starting from the service layer and going down to the network element layer, are critical functions which needs strong security. Hence these need to use a secure protocol (e.g. IPsec, https, SSL) and/or encrypted data. Other management data is not so critical but is nevertheless of more or less importance for overall integrity, and other protocols are suitable.

The BSM network elements contain a database for storage of management data which may be accessed by any suitable protocol (SNMP, http, etc.) and converted into a compatible data format (e.g. ASN.1).

Also the BNMS contains a database for storage of retrieved management data and for access to this data by higher level processes as well as external interfaces where necessary.

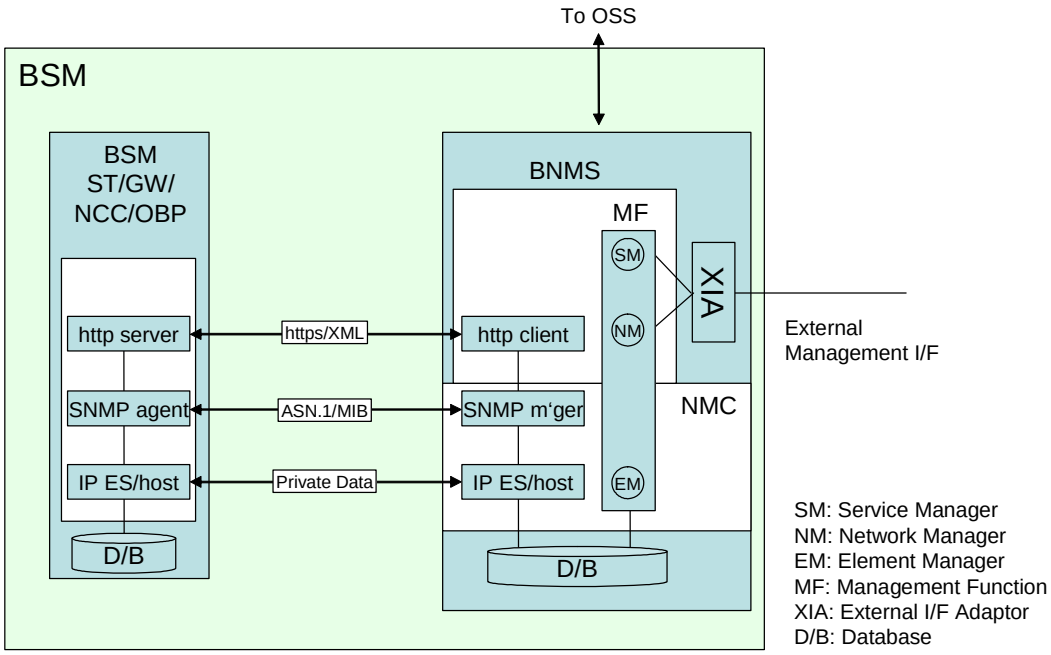


Figure 15: BSM Management Functional Architecture

The BSM Management "Physical" Architecture in figure 16 shows the types of physical network options which may be used to interconnect management entities. Routers in elements are able to select appropriate networks by configuration or other criteria.

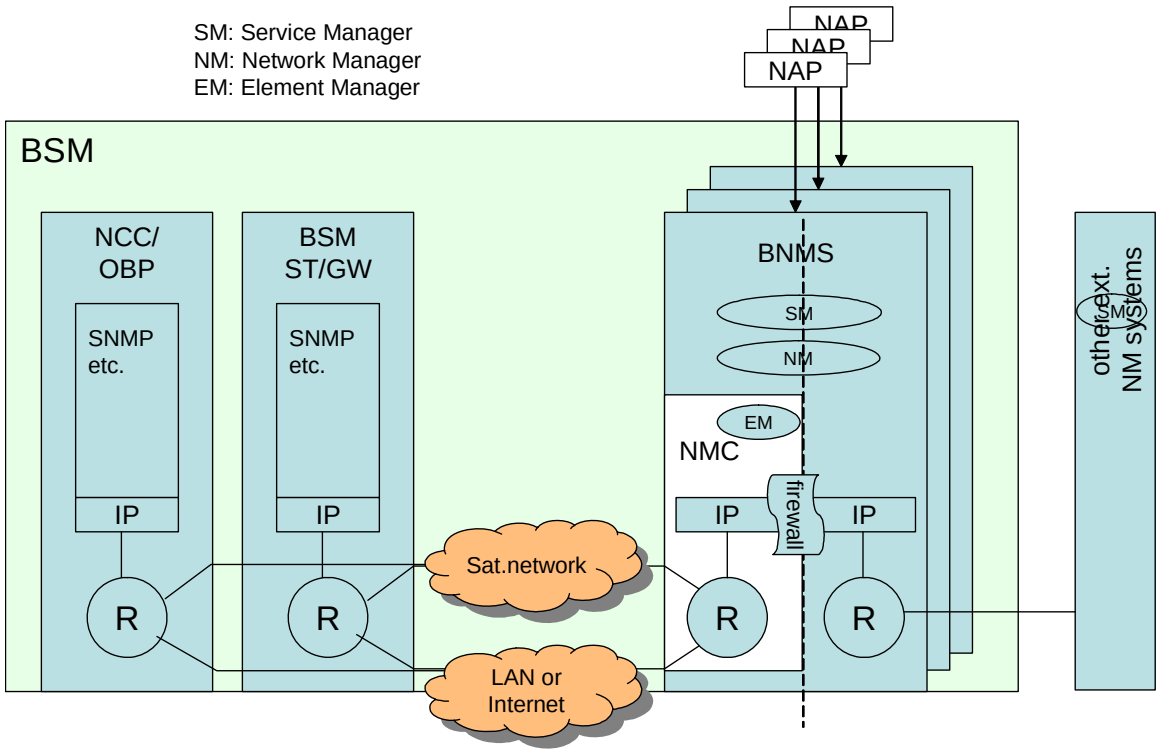


Figure 16: BSM Management "Physical" Architecture

In figure 16 multiple possible NAPs are indicated to show that several network operators may each have their own BNMS on the same BSM network.

7.2.1 Internal Interfaces

The underlying physical architecture, based on IP, allows network elements to be managed by the BNMS via either satellite links or terrestrial links where available. The choice between the type of access link allowed depends on equipment firewalls, access rights to MIBs, etc. The NCC and gateway ST are usually connected to the BNMS via a LAN or the internet.

The management protocols may be SNMP, IP (ICMP) or http. A DMM function allows managers to access databases via one or other of these protocols. These protocols are used to transfer different data structures from the elements.

7.2.2 External Interface

The external management interface to other network managers may support several options such as TMN X or SOAP etc.

An external BNMS interface may also be provided to an OSS, located within the BSM.

The BNMS maintains its own management database for external interactions. This database can be accessible by data transfer modules using alternative transfer formats such as XML, MIB, etc.

In addition external managers may potentially access directly the databases or MIBs of BSM network elements if access rights are granted.

7.2.3 Evolution to Web-based Network Management Architectures

Web browsers and protocols are increasingly attractive for providing visual tools (GUIs etc.) for management, and the trend today is towards use of http for communications at least between a browser-based management application and either the OSS server or directly with Agents, in order to support remote services. Network elements are also increasingly provided with web management interfaces. However there are legacy and other issues with existing systems which would benefit from an evolutionary approach to full web-based network management.

The examples below show such evolutionary architectures (and exclude considerations for higher level and external management).

7.2.3.1 Browser-Based Management of SNMP-based BSM

This solution involves no modification to SNMP-based network elements. Here operators use a Web browser as a single interface to all management tasks, and the SNMP-based management platform (e.g. NMC) is modified into an http-SNMP gateway (e.g. by addition of a BNMS). A common database in the BNMS is used to store BSM-wide management data in a convenient format which can be read or written by both SNMP Manager and http server, using appropriate format conversion.

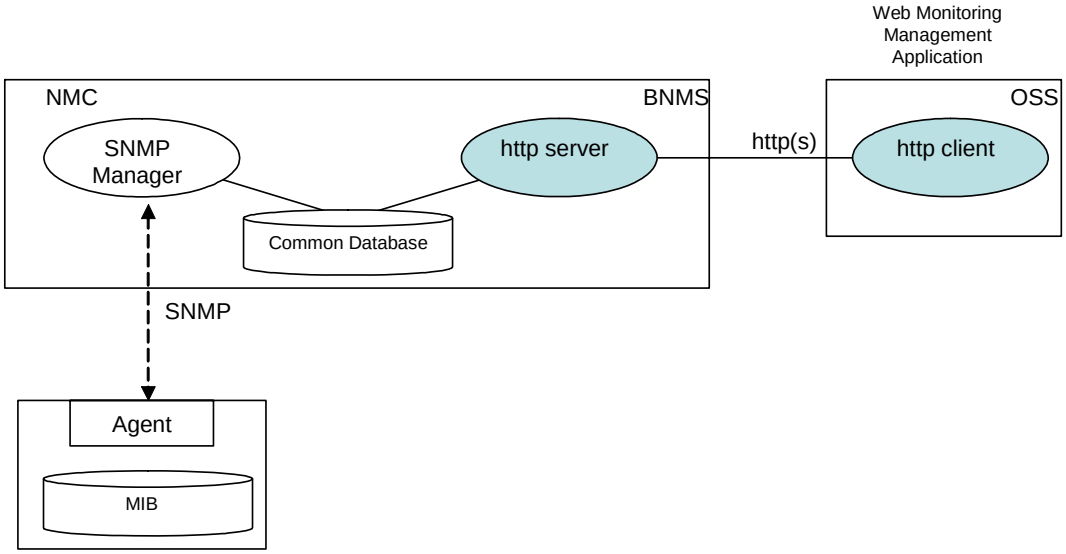


Figure 17 Browser-Based Management with SNMP elements

7.2.3.2 Browser-Based Management with modified SNMP Elements

In this case elements are modified to enable a fully web-based manager to be employed. Communication with elements is then only via http(s). The elements include http servers with SNMP, etc.

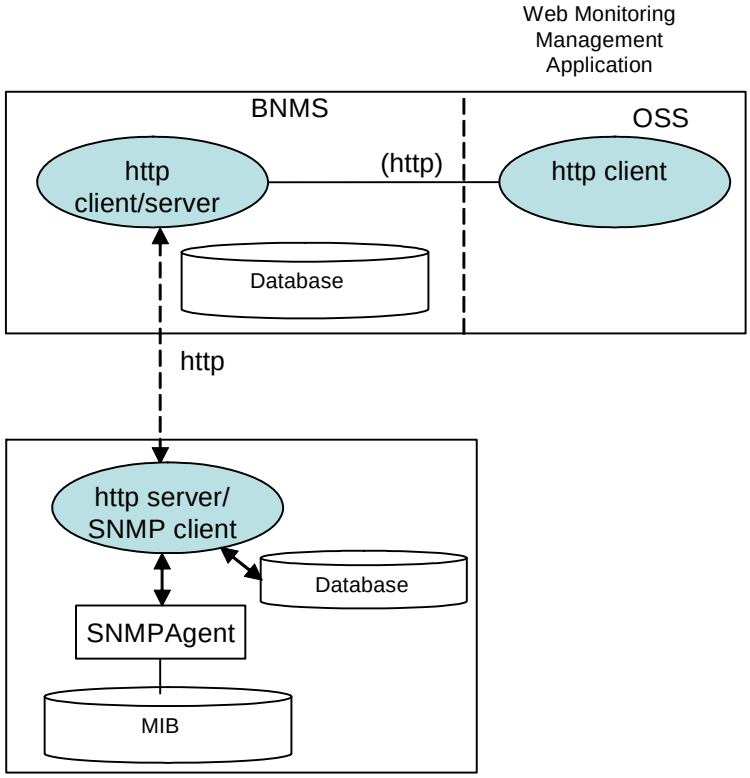


Figure 18 Web-based Management architecture with modified elements

7.2.3.3 Multiple http/IP/SNMP management protocols

In this case agents are modified with additional Web-based interfaces alongside existing IP (for ICMP, RSVP, telnet, etc.) and SNMP interfaces.

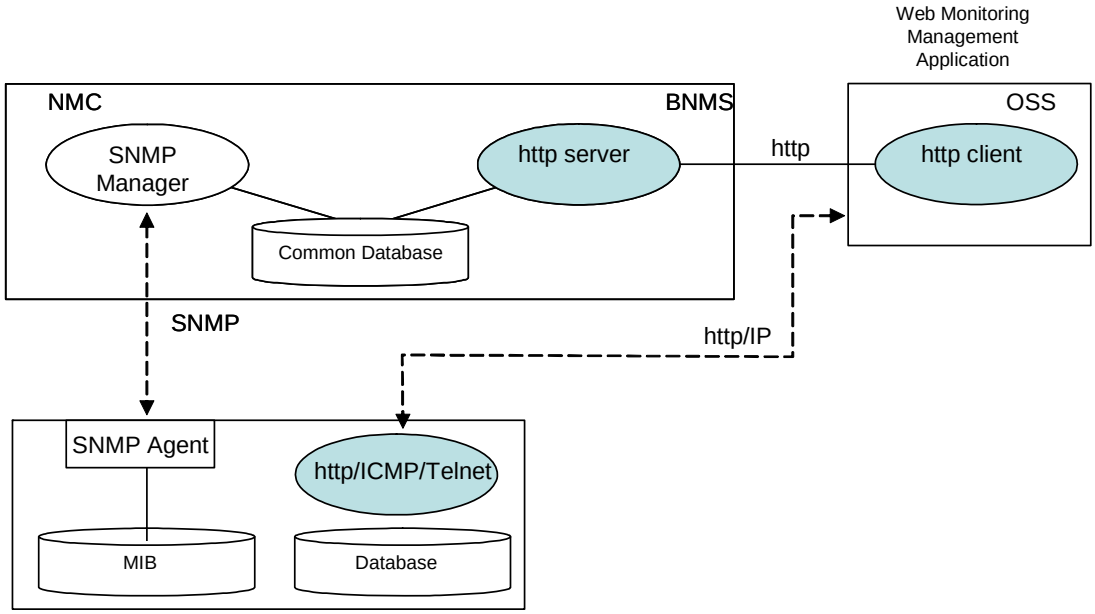


Figure 19 Multiple SNMP/http/IP management

7.3 BSM Management Data Models

In BSM we define a two-level data model:

- An element-level data model, corresponding to the interface between the element and the BNMS.
- A network-service data model, corresponding to the interface between the BNMS and the external management system.

7.3.1 Data Model Structure

MIBs are written using ASN.1 and are specific to the element being managed. They consist of a list of managed parameters and limits.

The access rights for particular OIDs within a MIB determine the "views" of management data in each network element available to different managers or network actors. A BSM MIB should allow parameters (e.g. for performance) to be viewed dependent on the network manager's access rights.

Other data models can use other formats e.g. object-oriented, based on XML format, etc.

Annex A (informative): Overview of Existing Network Management Architectures

A.1 Overview

For a further description and classification of NM approaches see also [i.5].

There is a range of alternative potential NM standards and solutions as described in clause 4. The choice of approach depends on for example:

- cost -effectiveness;
- flexibility (scalability, ease of update, modularity for additional functions);
- reliability (redundancy, reconfigurability);
- security;
- transmission bandwidth;
- legacy entity compatibility.

A.1.1 Network Management Architecture Classification

Network Management Architectures are sometimes broken down into four component models [i.4]:

a) A Data model e.g. SMI, CIM (the way in which information is represented; object-oriented etc.).

b) Communication model e.g. SNMP, CMIP, http (i.e. protocol).

c) Organisational model e.g. centralised, distributed, and the way in which agents and managers communicate.

d) Functional model e.g. the FCAPS functions or eTOM (which are almost universally accepted as models).

In practice it is possible to choose between these four models to some extent independently, even if some standardised architectures have a complete set of these models. A solution can be found for a different set of these models by using protocol gateways for example.

Items a), b) and c) can be considered as elements of an information model.

These features are described further below.

A.1.2 Data Model

The Data Model depends largely on the approach to abstraction of management data and of the management applications, particularly in terms of flexibility and reliability. These approaches can be split into four types:

- Managed Objects e.g. in MIBs (low abstraction level).
- Computational Objects (medium to high abstraction level).
- Goals (high abstraction level - this could include policies).
- Trends (highest abstraction level).

A.1.3 Organisational Model

In overall network management, scalability issues are typically solved by distributing management over several logical entities and autonomous domains.

The centralised management approach (e.g. a client-server model, typified by SNMP) is the simplest approach (at least conceptually) and is characterised by a central manager concentrating all management application processing, and collecting data from a number of relatively simple agents.

SNMP allows exchange of parameters across networks in principle (e.g. using RMON), but as SNMP is not object-based it does not easily lend itself to distributed managers and agents.

Distributed management systems were addressed for telecommunication networks, for example, in the TMN and the CMIS which employs object-based databases for easier exchange between networks.

A further step in distributed management is the "distributed object" approach typified by CORBA and Java/RMI, in which management functions (objects) can be flexibly implemented on different entities. Also a software infrastructure commonly called "middleware" provides consistent mechanisms for distributed software "components"as well as agents and managers based on existing architectures such as CMIP and SNMP, to communicate with each other across a network.

A.2 SNMP (IETF)

In general, although SNMP exists in several versions, the advantages of using SNMP are that it is:

- simple and widely implemented;
- light-weight requiring less memory and computing power than CMIP.

The disadvantages are that it:

- defines a specific non-object-oriented information model which is simple but cannot easily be abstracted and does not suit distributed managers and agents;
- has a limited instruction set;
- is not suited to management above network element layer, e.g. is not intended for inter-domain management, or network service management;
- generally uses UDP, the unreliability of which is a weakness especially for network configuration;
- is unsuitable for network configuration management because of the lack of transaction support and security;
- does not scale well due to reliance on polling;
- generates redundant traffic even in the absence of faults or alarms owing to the bandwidth-inefficient polling method.

Among the security implications of SNMP are:

- versions 1 and 2c are subject to packet sniffing of the clear text "community" string in network traffic;
- All versions of SNMP are subject to brute force and dictionary attacks for guessing the community strings/authentication strings/authentication keys/encryption strings/encryption keys, because they do not implement a challenge-response handshake;
- SNMP is most commonly used over UDP (although it works over TCP and other protocols), which is connectionless and vulnerable to IP spoofing attacks. Thus, all versions are subject to bypassing device access lists that might have been implemented to restrict SNMP access, though SNMPv3's other security mechanisms should prevent a successful attack;

- SNMP's configuration (write) capabilities can be misconfigured and used to cause severe damage. These 'write' capabilities are very rarely used in practice, partly due to lack of security in SNMP versions before SNMPv3 and partly due to the fact that many devices do not implement SNMP configuration interfaces.

The following clauses describe the status of SNMP, its architecture and the uses of MIBs.

A.2.1 SNMP Versions

The SNMP protocol exists in several versions including v1, v2 and v3 and sub-versions thereof:

- SNMPv3 [i.9] is the official IETF standard but is not widely implemented. SNMPv3 includes mechanisms (e.g. security) that can also be used with SNMPv1and SNMPv2c.
- SNMPv1 [i.8] is still used, but is largely superseded by SNMPv2 which, however, does not retain the simplicity of SNMPv1.

Of the several SNMPv2 [3] sub-versions, SNMPv2c [i.10] is classified as "experimental", but is widely accepted as the *de-facto* SNMPv2 standard.

SNMPv2 (RFC 1441 [i.39] and RFC 1452 [i.40]) revised v1 and included improvements to performance, security, confidentiality, and manager-to-manager communications. It introduced GETBULK, an alternative to iterative GETNEXTs for retrieving large amounts of management data in a single request. However, the new party-based security system in SNMP v2 was not widely accepted as being too complex.

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without its security using instead the simple community-based security scheme of SNMP v1. The security mechanism involves authentication of clients by a "community string", in effect a type of password, which is transmitted only in clear text, and is thus considered weak.

SNMPv2 is incompatible with SNMPv1 in two key areas: message formats and protocol operations. SNMPv2c messages use different header and protocol data unit (PDU) formats than SNMPv1 messages.

In practice, SNMP implementations often support multiple versions [i.16].

A.2.2 SNMP architecture

The SNMP standards define an architecture based on a manager-agent model.

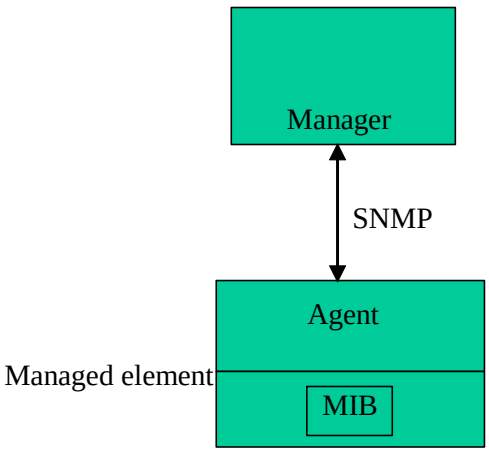


Figure A.1: Location of MIB and agent

Managed resources are modelled through managed objects (MOs), which represent the underlying resource and offer an abstract access interface. These managed objects are collected in a MIB. An agent located in a managed element is a software entity that administers these managed objects (e.g. configures parameters of the managed objects). The agent behaves as a server by responding to management requests across the interface, and also disseminates spontaneous events through the management protocol.

Manager applications use SNMP to access managed objects in the MIB for implementing management policies. The manager functions as the equivalent of a client in the client-server architecture for issuing requests for management operations, and it also receives traps from agents.

Options and variations on this architecture are also specified, for example higher layer, hierarchical SNMP management layers for complex network elements containing multiple MIBs [i.12], and Manager-to-Manager MIBs [i.9]. A management application in this case may act in both agent and manager roles, and this is the case for peer-to-peer management interactions or for hierarchical management environments. However these options are considered "historic" and are not normally implemented in SNMP.

A.2.3 MIBs

The Management Information Base (MIB) is a virtual information store, consisting of "Managed objects".

Objects in the MIB are defined using the mechanisms defined in the SMI [i.6].

MIB version 2 (MIB-II) is the most widely implemented MIB. RFC 1902 [i.11] discusses the MIB II structure (see figure A.2).

New MIB modules that extend the Internet-standard MIB are continually being defined by various IETF working groups. It is also common for enterprises or individuals to create or extend enterprise-specific or experimental MIBs. For example there are 318 RFCs defining MIBs in the first 5 000 RFCs from the IETF. Examples of MIBs are:

- SNMP - SMI:RFC 1155 [i.6] - Defines the Structure of Management Information (SMI).
- MIB-I: RFC 1156 [i.7] - Historically used with CMOT , not to be used with SNMP.
- SNMPv2-SMI: RFC 2578 [3] - Structure of Management Information Version 2 (SMIv2).
- MIB-II: RFC 1213 [1] - Management Information Base for Network Management of TCP/IP-based internets.
- SNMPv2-MIB: RFC 3418 [i.14] - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).
- TCP-MIB: RFC 4022 [i.32] - Management Information Base for the Transmission Control Protocol (TCP).
- UDP-MIB: RFC 4113 [i.33] - Management Information Base for the User Datagram Protocol (UDP).
- IP-MIB: RFC 4293 [i.34] - Management Information Base for the Internet Protocol (IP).
- IF-MIB: RFC 2863 [i.35] - The Interfaces Group MIB.
- ENTITY-MIB: RFC 4133 [i.36] - Entity MIB (Version 3).
- ENTITY-STATE-MIB: RFC 4268 [i.37] - Entity State MIB.
- ALARM-MIB: RFC 3877 [i.38] - Alarm Management Information Base (MIB).

IANA maintains a large MIB repository at ISI (ftp://ftp.isi.edu/mib/).

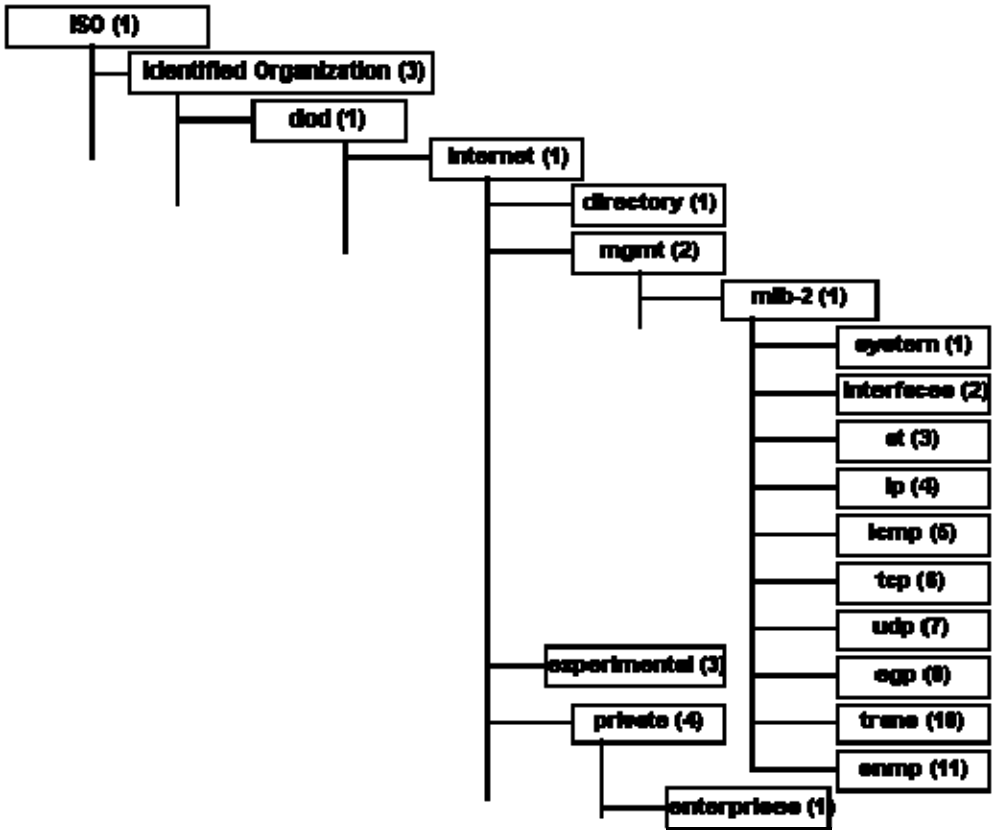


Figure A.2: MIB tree structure and MIB-II Object Groups

The above tree is a visual form of the OID structure. An OID is made up of a series of integers based on the nodes in the tree, separated by dots (.).

A.2.3.1 DVB-RCS

SNMP is optional for DVB-RCS. The DVB-RCS guidelines document [i.18] has defined a MIB for use with SNMPv2c. The private enterprise RCST MIB is defined under the private.enterprises.dvb MIB tree. IANA has allocated the number 2 696 to it.

DVB-RCS manufacturers have implemented their private MIB's as a complement to the standard MIB-II, taking typically a subset of the DVB-RCS MIB.

SatLabs has defined a common MIB for all manufacturers [i.20], as a substitute for the DVB-RCS MIB, which covers their additional features and functionality (e.g. QoS, PEP), see figure A.3.

A draft DVB-RCS MIB is being submitted to the IETF [i.19].

ETSI has defined a MIB for DVB-S/DVB-RCS regenerative mesh satellite systems [i.2] classified as RSM-B.

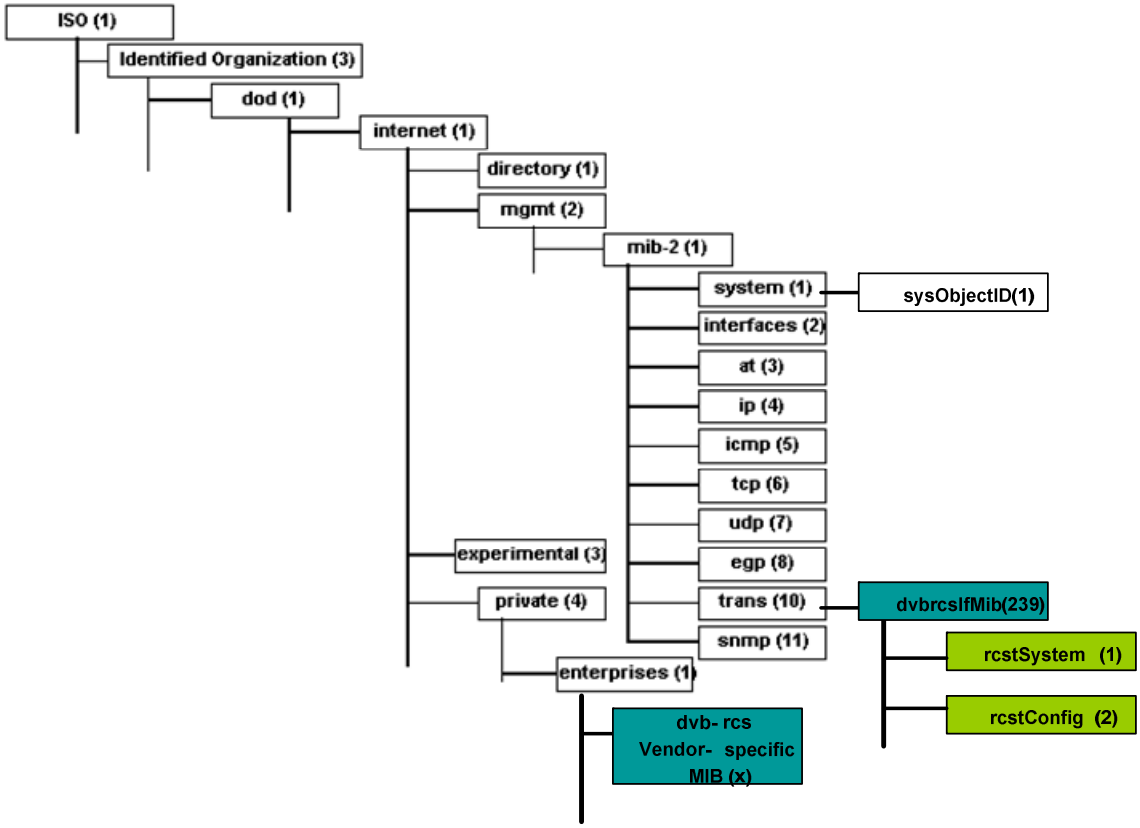


Figure A.3: Satlabs and DVB-RCS additions to the MIB II

A.2.3.2 MIB Views

A MIB view [2] is defined by a collection of view subtrees in a MIB II structure. A table locally maintained by each SNMPv2 entity defines the MIB view associated with each SNMPv2 context [i.13] that refers to local object resources.

A.2.3.3 SNMP Traps/Notifications

A "Trap" was originally an SNMPv1 unsolicited message sent from an agent to a manager in order to notify it that an event has taken place, typically a fault. However Traps are unacknowledged.

Trap-directed notification can result in substantial savings of network and agent resources by eliminating the need for frequent SNMP requests. However, it is not possible to totally eliminate SNMP polling as SNMP requests are required for discovery and topology changes. In addition an agent can not send a trap if the element has a catastrophic outage.

SNMPv2 PDUs introduced a "Notification" (sometimes Inform) message, as an "acknowledged Trap", so that it can be used reliably by network entities to signal abnormal conditions to management stations.

SNMPv3 mandates that the Trap or Notification message is rejected unless the SNMPv3 user sending the trap already exists in the user database.

A.2.3.4 RMON

Like SNMP, the RMON [i.15] implementation typically operates as a client/server model. Monitoring devices ("probes") contain RMON software agents that collect information and analyse packets. These probes act as servers and the Network Management applications that communicate with them act as clients. Although RMON agent configuration and data collection use SNMP, RMON is designed to operate differently than other SNMP-based systems:

- Probes have more responsibility for data collection and processing, which reduces SNMP traffic and the processing load of the clients.
- Information is only transmitted to the management application when required, instead of continuous polling.

RMON is designed for "flow-based" monitoring, while SNMP is often used for "device-based" management. One disadvantage of this system is that remote devices shoulder more of the management burden, and require more resources to do so. Some devices balance this trade-off by implementing only a subset of the RMON MIB groups (see below). A minimal RMON agent implementation could support only statistics, history, alarm, and event.

The RMON1 MIB consists of ten groups:

1) Statistics: real-time LAN statistics e.g. utilization, collisions, CRC errors.
2) History: history of selected statistics.
3) Alarm: definitions for RMON SNMP traps to be sent when statistics exceed defined thresholds.
4) Hosts: host specific LAN statistics e.g. bytes sent/received, frames sent/received.
5) Hosts top N: record of N most active connections over a given time period.
6) Matrix: the sent-received traffic matrix between systems.
7) Filter: defines packet data patterns of interest e.g. MAC address or TCP port.
8) Capture: collect and forward packets matching the Filter.
9) Event: send alerts (SNMP traps) for the Alarm group.
10) Token Ring: extensions specific to Token Ring.

The RMON2 MIB adds ten more groups:

1) Protocol Directory: list of protocols the probe can monitor.
2) Protocol Distribution: traffic statistics for each protocol.
3) Address Map: maps network-layer (IP) to MAC-layer addresses.
4) Network-Layer Host: layer 3 traffic statistics, per each host.
5) Network-Layer Matrix: layer 3 traffic statistics, per source/destination pairs of hosts.
6) Application-Layer Host: traffic statistics by application protocol, per host.
7) Application-Layer Matrix: traffic statistics by application protocol, per source/destination pairs of hosts.
8) User History: periodic samples of user-specified variables.
9) Probe Configuration: remote configuration of probes.
10) RMON Conformance: requirements for RMON2 MIB conformance.

A.3 TMN (ITU)

The Telecommunication Management Network (TMN) from the ITU is designed for networks involving concatenated sub-network domains and potentially organised into a management hierarchy, within which management entities can intercommunicate and be organised. The ITU adopted the ISO's management model for OSI systems (OSI-SM) for the TMN.

A.3.1 FCAPS Model

Network management functions are those that are responsible for extracting and configuring fundamental management information as required by the management user:

- Fault management.
- Configuration management.
- Accounting management.
- Performance management.
- Security management.

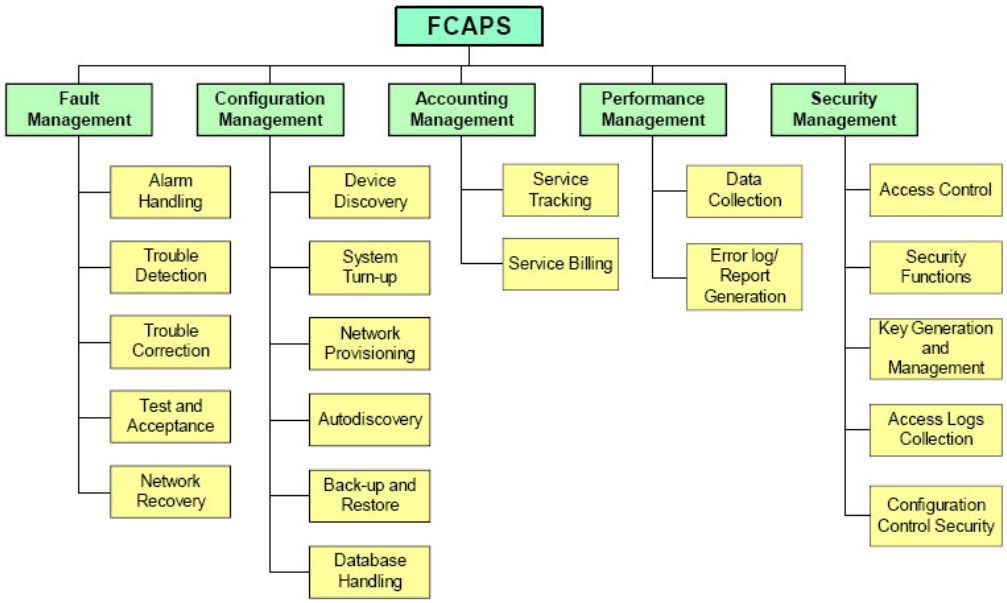


Figure A.4: TMN FCAPS Model

A.3.2 CMIP (ISO)

The ISO's OSI-SM (System Management) model provides a more powerful infrastructure than SNMP by adopting an object-oriented approach [i.27] and [i.28]. In this model, elements are represented through managed object abstractions that can be handled by agent applications and accessed by manager applications. Communications between these agents and managers is achieved through the OSI Common Management Information Service/Protocol (CMIS/P). CMIS provides the OSI management services to the management applications, and CMIP provides the information exchange capability to support CMIS.

Since CMIS is object-based, it can be used on distributed management systems using a suitable architecture. A software infrastructure commonly called "middleware" in the client/server distributed computing environment, provides consistent mechanisms for distributed software 'components' such as agents and managers, to communicate with each other across a network.

CMIP is also applicable to peer communications at the service management layer whereas SNMP is used almost exclusively for element management. CMIP is designed as an OSI-based protocol suitable for telecoms networks, but CMIP can also run over TCP, which increases its usability and also its reliability over wide-area networks.

However this complex approach to open platforms for network management based on TMN/CMIP never became widely accepted, since in reality, network management is not that different from any other type of application. These complex platforms are used today mainly for fault management, to display alarms and to provide topology maps.

A.3.3 NGN Network Management

The ITU has considered principles for the management of Next Generation Networks in [i.23].

A.4 NGOSS, OSS/J and TOM/eTOM (TMF)

The approach taken by the TMF's NGOSS (New Generation OSS) principles can be summarised as follows:

- Centralised process flow.
- A common information model for shared data.
- A common communications infrastructure.
- Use of COTS components.

The NGOSS architecture is described using technology-neutral constructs. These include concepts taken from RM-ODP [i.24] as well as extensions to the basic UML metamodel to represent fundamental NGOSS concepts and principles. It does not prescribe a single new technology but it allows for a federation of different technological approaches, each of which offers particular advantages at the business and system levels. An NGOSS solution design specification may be implemented using currently available distributed systems information technologies or technologies that are yet to be defined. Critical to this process is the defining, sharing and reusing of common information and data, as this provides a common vocabulary and understanding of both business and system concepts used for analysing the structure and behaviour of a desired OSS solution. This is done using the **Shared Information and Data (SID)** model, which is designed as a set of UML models that cover various views of domain information.

In this approach, each OSS component interfaces with only one central component, the hub. The hub is therefore responsible for passing messages and handling transactions between the OSS components. The advantage of this approach is that, in principle, there only needs to be one interface per component, as opposed to the hundreds in the point-point approach. Of course, each of these interfaces has to support a wider range of processes, but nevertheless there are improvements in the cost of creating and supporting the interfaces.

The hub-based approach brings other advantages. With the point-point system, it is difficult to apply overall control to business processes, since each OSS component owns and controls a part of the overall process. Therefore changing or metricating the process becomes difficult and in some cases impossible. In a hub-based architecture it's the hub itself that is responsible for managing transactions, so it is also possible to use hub-based process (or workflow) engines to manage the overall process flow, with real benefits in terms of flexibility and control.

A.4.1 OSS/J

Originally a separate initiative promoted by Sun, OSS through Java (OSS/J) is now a TM Forum Program that addresses standards-based NGOSS interface implementations (OSS/J APIs) and design guidelines for the development of component-based OSS systems. OSS/J technologies aim to unify legacy systems and new applications quickly and at low cost.

The OSS/J APIs are multi-technology based and include Java, XML, and Web Services integration profiles. Each integration profile consists of specifications, a reference implementation, and a conformance test suite (TCK). All OSS/J APIs are publicly available.

A.4.2 TOM

An overview of what the OSS world is intended to cover is provided by the TM Forum organisation, via the Telecom Operations Map (TOM) process overview. This contains a detailed description of the most important processes involved in running a Network Operator operation.

The TOM is based on the FCAPS model described in clause 5.2. It has element and network management layers as in the pyramid in figure 1, but it splits the service management layer into a lower operations lifecycle layer (Service Development and Operations Processes) and an upper customer lifecycle layer (Customer Care Processes). The level of adoption of the TOM is such that some OSS software vendors include it in their literature to indicate which parts their software covers.

Figure A.5 shows a graphical presentation of TOM.

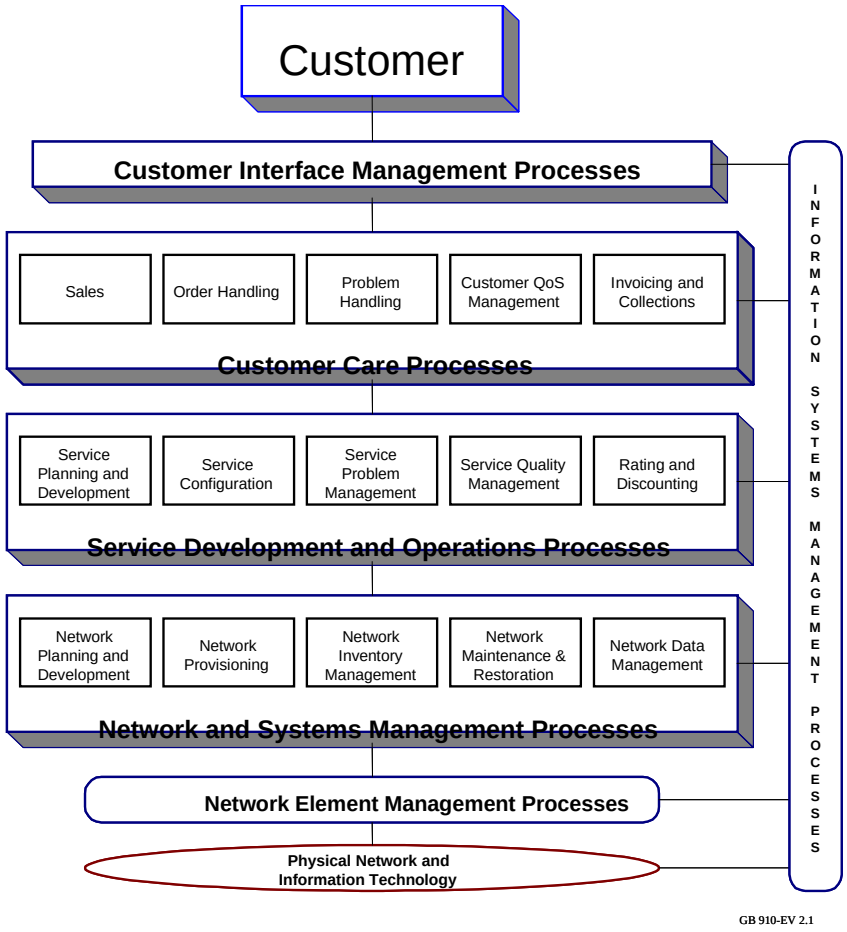


Figure A.5: The TOM

A.4.3 eTOM business process framework

Although it has been used for selling software and as a systems framework, the TOM is limited in that it was designed primarily for service providers and Network Operators.

The eTOM (enterprise TOM) overcomes this limitation by extending the applicability of the TOM to enterprises by developing its lowest layer: there is no network at the bottom, there is a more general 'resource management' and then the framework extends down to supplier / partner relationships.

eTOM is a business process model or framework that has the objective of describing and classifying the business processes required for a Service Provider; it analyzes the processes to different levels of detail according to their significance and priority for the business.

eTOM uses hierarchical decomposition to structure the business processes according to which all of the processes of the enterprise are successively decomposed. Process elements are formalized by means of a name, a description, inputs/outputs, etc.

The eTOM supports two different perspectives on the grouping of the detailed process elements:

- horizontal process groupings, in which process elements are grouped according to reference accomplished functionalities (e.g. Market and Product and Customer management, Service management, etc.);
- vertical process groupings, in which process elements are grouped within End-To-End processes (e.g. Fulfilment, Assurance, etc.) accomplished by the Service Provider enterprise.

The eTOM Business Process Framework is defined as generically as possible, so that it is independent of organization, technology and service. However it is not a Service Provider business model.

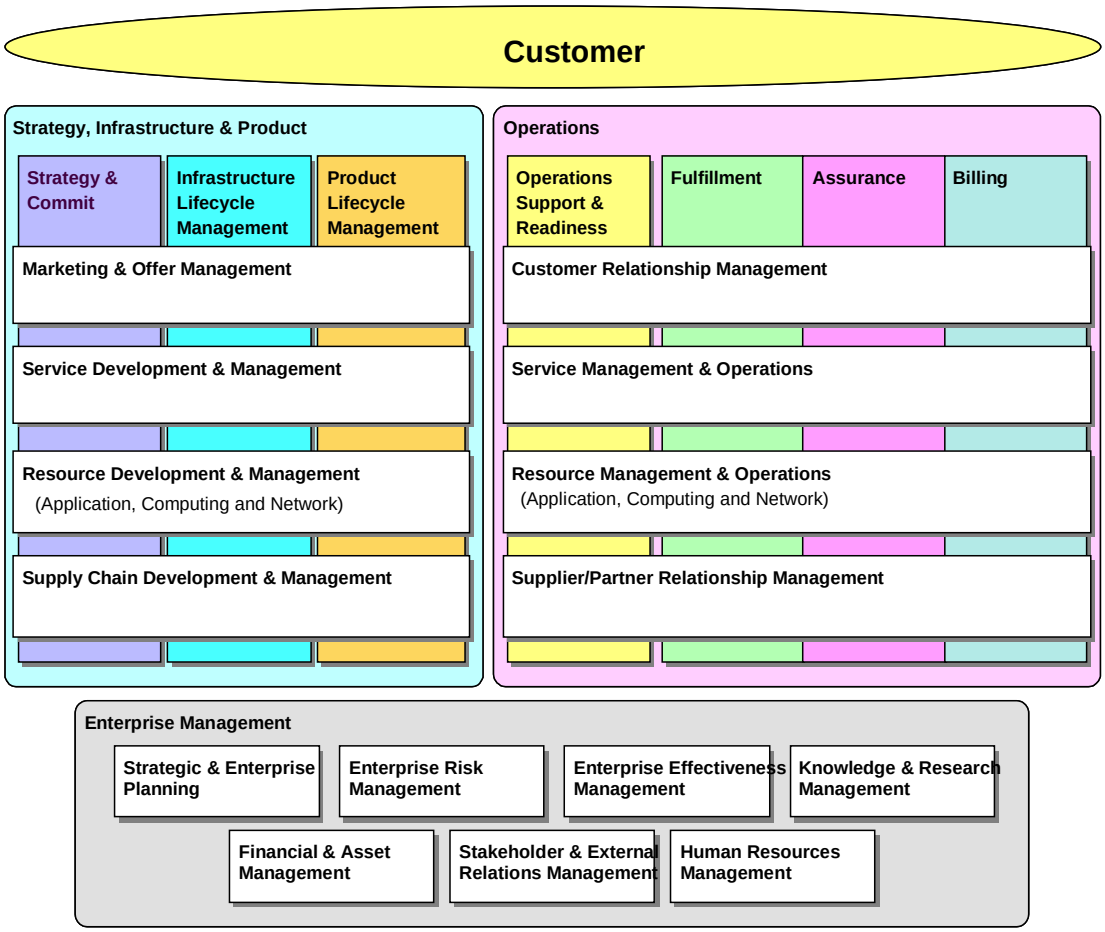


Figure A.6: eTOM Business process framework (TMF GB921, ITU-T Recommendation M.3050.1)

The other development in moving from the TOM to the eTOM is the inclusion of vertical classifications of Strategy, Infrastructure and Product on the left of the diagram, which contains processes for building a service, with Operations on the right.

Note that the eTOM does not have the ITU-T FCAPS as vertical layers, but these have been rationalised and re-classified as Fulfilment, Assurance and Billing (FAB). A fourth vertical layer is Operations Support and Readiness.

A.5 CORBA and OMA (OMG)

The Object Management Architecture includes the Common Object Request Broker Architecture (CORBA) from the Object Management Group (OMG) and uses a fully object-oriented information model. Objects are effectively defined through their interfaces, which are specified in the Interface Definition Language (IDL).

CORBA was once seen as the unifying management technology but, despite its success in service management, it has rarely, if ever, been used for network management despite support by some telecommunication equipment vendors. The key problems with CORBA are its relatively heavyweight and expensive technology. Core network devices such as switches and routers many contain more than a hundred thousand managed objects, and making each one of these a separate distributed object with its individual interface is very resource-expensive.

A.6 CIM and WBEM (DMTF)

The DMTF (Distributed Management Task Force) took over the DEN (Directory Enabled Networks) and CIM (Common Information Model) from Microsoft and Cisco.

The Common Information Model (CIM) is the basis for most of the DMTF standards, and is a conceptual information model (schema) that defines the subscribers, services and the infrastructure in an easily accessible LDAP directory as a common set of objects and relationships between them. It provides a consistent definition and structure of data, using object-oriented techniques.

Web-Based Enterprise Management (WBEM) defines a protocol known as CIM-XML (transported over HTTP/TCP) for the interaction between a manager and managed elements implementing CIM.

A mapping of CIM operations onto HTTP allows implementations of CIM to interoperate in an open, standardized manner and is one of the technologies that support WBEM, alongside the XML-CIM Encoding Specification which defines XML elements (written in Document Type Definition - DTD) to represent CIM classes and instances.

XML allows arbitrary structures to be defined through Data Type Definitions (DTDs) and thus can be used as a textual encoding mechanism for application protocols, object and interface specifications, etc. XML-based network management technologies are particularly attractive given the potentially easy integration of XML-based management data with that of other applications. In addition, combining XML with a Web-browser approach is attractive for its ubiquity, low cost, proven scalability and security features.

A.7 TISPAN (ETSI)

TISPAN NGN introduces the following views of NGN management (figure A.7):

- the Business Requirements view: this presents the business concepts, strategies and requirements, for Management in the NGN;
- the Functional/Information view: this presents the Service Oriented Architecture [i.23] including functions and their relationships and the information models and logical interfaces defined for supporting the business requirements;
- the Implementation view: this presents the technical components, the technical interfaces and the data models defined for supporting the Functional/Information view.

In this approach, the security of management aspects is transverse (i.e. the security aspects of NGN_OSS Management, rather than the Management of Security of the NGN itself, which is an integral part of the 3 views above), they cover the three architecture views: Business Requirements, Functional/Information and Implementation.

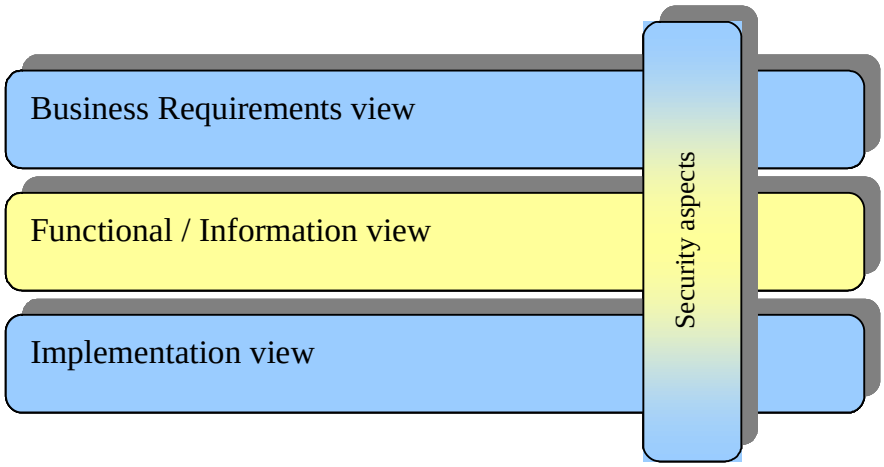


Figure A.7: NGN OSS management views

Further description of this concept can also be found in [i.23].

The main purpose of the NGN management views is to allow ETSI NGN to document the steps required to progress from a set of business needs to the creation of a functional/ information view to logically specify those needs. Then, from this Functional/Information View of the Architecture, an Implementation View of the Architecture can be derived that takes into account specific realization requirements such as cost, performance, integration or adaptation of legacy applications, and technology and other organizational preferences.

One of the architectural principles behind the architecture for management of Next Generation Networks is that of being a Service-Oriented Architecture (SOA). A Service Oriented Architecture (SOA) is a software architecture of services, policies, practices and frameworks in which components can be reused and repurposed rapidly in order to achieve shared and new functionality. This enables rapid and economical implementation in response to new requirements thus ensuring that services respond to perceived user needs.

SOA uses the object-oriented principle of encapsulation in which entities are accessible only through interfaces and where those entities are connected by well-defined interface agreements or contracts.

The present document concentrates on the Functional/Information Architecture of the OSS required for NGN Management. The rest of this clause describes the content of the other NGN management views (Business Requirements and Implementation) and the link between the three views.

A.8 Java/RMI

The Java Remote Method Invocation (JRMI) is, like CORBA, a distributed object approach that Sun Microsystems built into their Java programming language.

RMI applications typically comprise two separate programs, a server and a client. A server program creates some remote objects, makes references to these objects accessible, and waits for clients to invoke methods on these objects. A typical client program obtains a remote reference to one or more remote objects on a server and then invokes methods on them. RMI provides the mechanism by which the server and the client communicate and pass information back and forth. Such an application is sometimes referred to as a *distributed object application*.

Distributed object applications do the following:

- **Locate remote objects.** Applications can use various mechanisms to obtain references to remote objects. For example, an application can register its remote objects with RMI's simple naming facility, the RMI registry. Alternatively, an application can pass and return remote object references as part of other remote invocations.
- **Communicate with remote objects.** Details of communication between remote objects are handled by RMI. To the programmer, remote communication looks similar to regular Java method invocations.
- **Load class definitions for objects that are passed around.** Because RMI enables objects to be passed back and forth, it provides mechanisms for loading an object's class definitions as well as for transmitting an object's data.

The key difference between CORBA and JRMI is that the former supports bindings to many programming languages, including C, C++, Java and Smalltalk, while JRMI is tightly bound to Java, and this could be a problem for real-time applications. An additional difference is that CORBA has been enhanced with sophisticated services that are required by management applications, for example event notifications, while JRMI does not include services of similar sophistication. JRMI has mainly been used so far in the research domain of network management, and today it is being challenged by emerging Web-based management.

History

Document history		
V1.1.1	November 2009	Publication