Network Management Architectures: Overview and Evaluation

José Luís Oliveira

Resumo **- A expansão das redes de comunicação introduziram novos requisitos junto dos utilizadores e gestores. Diversos organismos internacionais desenvolveram arquitecturas de gestão com vista a aproximar as soluções de diferentes fabricantes.**

O objectivo deste artigo é a apresentação de uma síntese mais compreensiva dos documentos normativos bem como discutir e comparar as principais lacunas e potenciais cenários de aplicação de cada arquitectura.

Abstract **- The expansion of communication networks have been putting new requirements to managers and users. Some management architectures were developed in order to approach different vendor solutions.**

The intend of this paper is to provide a comprehensive tutorial of the recommendation documents and to discuss the main lacks and the application scenarios of each solution.

I. OSI MANAGEMENT MODEL

The last decade have recognised a great expansion on communications network. The increase has been observed on the number of connection elements, of the interconnected equipment and also on the total amount of network domains spread over the world. This phenomena puts new demands on the network planners and on the network managers. Due to the diversity of technological solutions soon specialists realise that they must agree on a global and standard framework that allow them to develop open management applications.

The ISO (International Organisation for Standardisation) developed from the '70s a pioneer work on the standardisation of local area networks. This work has delivered the OSI reference model (Open Systems Interconnection) [1] that is the base document for system interconnection. The OSI Management Framework [2] has add to this base the management architecture complemented later by the ISO10040 standard. Both establish the global directives of the management concepts inside the OSI reference model.

Though the OSI management model has its origins in ISO much of the work was developed in collaboration with the ITU-T (ITU Telecommunication Standardisation Sector, ex-CCITT) which publish the same norms with a different identification (X.700 series).

A. OSI Management Standards

The ISO documents to the management area form a large spectrum of standards and they are the first barrier to the beginner reader. In Figure 1 it is show a diagram of the relations between those documents [3].

These documents can be also grouped into five categories [4]:

1. Management model definition - includes the initial documents that define the general concepts of the OSI management.
2. Management information structure - establish the formalism of the objects through which the management operations must be performed.
3. Management services protocols - joins a set of standards that define the management services (CMIS) and the management protocol (CMIP).

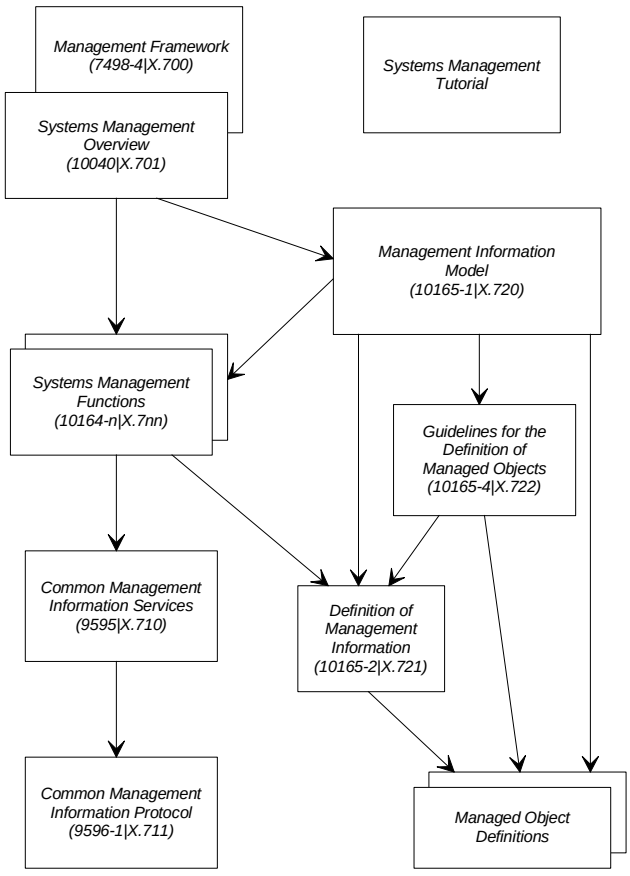

Figure 1 - Relations between OSI management model [3].

4. Management functions - this category includes all the documents that define specific management functions to realise in the OSI management framework.
5. Layer management - includes services, functions and management information related with specific layers of the OSI reference model.

B. Management Functional Areas

The management base document propose the division of management activities due to functional areas. It identifies five SMFA (Specific Functional Management Areas) some times named "FCAPS" as a result of its initials concatenation:

- Fault Management
- Configuration Management
- Accounting Management
- Performance Management
- Security Management

Though the main goal was the construction of a modular organisation to the management operations soon the following work show that those areas are not completely isolated. Management functions as Alarm Reporting, Event Report Management and Log Control included in the Fault Management were identified as important also in other areas. The development was shifted to the construction of atomic functions that can be used on the FCAPS [5]. This drives to the CMFA (Common Management Functional Areas).

C. Management Structure inside the Reference Model

The OSI management architecture allows different forms of information transfer that are organised in an hierarchical way inside the reference model (Figure 2).

- System Management
  Controls all the management actions within each system providing management information, as an agent, or requesting management information, as a manager. The communication is performed at the application layer through a special protocol that uses the already existing mechanisms shared by other common application.
  The system management have capture the main developments from the ISO since its a complete new framework inside the OSI model.

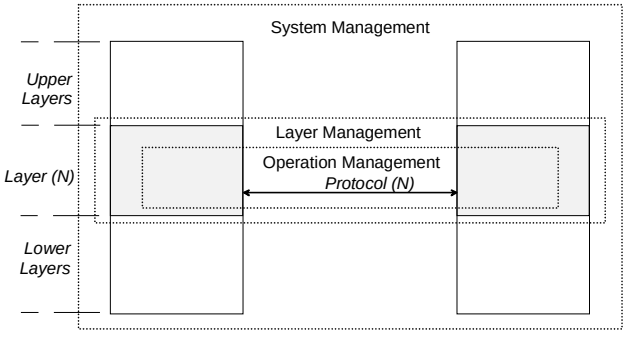

Figure 2 - Management categories inside the OSI reference model.

- (N) - Layer Management
  It allow to control of specific communication parameters at the N layer, to check the functionality of the (N-1) layer and to collect error and fault information of N layer. It can exist a special "management" protocol that is distinct from the N protocol through the addressing mechanisms of the (N-1) layer or through the discrimination procedures inside the N layer.
  An example is the ES-IS (*End System - Intermediate System*) [6] that allows to detect the presence of systems on the network.

- (N) - Layer Operation Management.
  It controls particular instances of a connection as a virtual circuit or a datagram one. It from the protocol responsibility to distinct the management information from other type of management. The flow control of a virtual circuit connection is an example of this type of management.

D. Management Information Model

Two important concepts are already introduced: the Functional Areas and the Management Organisation. The other issue of the OSI management framework is the information model.

The SMI (Structure of Management Information) provides a large range a concepts since the prototyping of the elements that allows and delivers management operations until the formalism through which these elements are identified and organised [7]. One of these concept is the Managed Object (MO).

Managed objects are logic representations of physical entities or resources associated with each system or sub-system. Managed objects are organised in classes that provide a common definition to a set of objects. The attribute concept is also related with the MO. An object mirrors some particular entity while the attributes maintain the values of its main characteristics. The MO defines a logical frontier between the entity and the management mechanisms. External management operations use this abstraction to access the entity and the system use it to issue notifications reporting internal states or events.

Beyond the microscopic association object-attribute it exists another element that joints in a organised way the managed objects. The MIB (*Management Information Base*) [8] is the macroscopic interface to deal with the system management information. In a simple approach management activities in each system can be seen as reading and writing operations of the MIB objects.

The structure of management information presents some powerful characteristics that is a result of a object-oriented methodology. Common concepts can be found like: class, object, inheritance, containment,

encapsulation, method, attribute, polymorphism, operation and message [9].

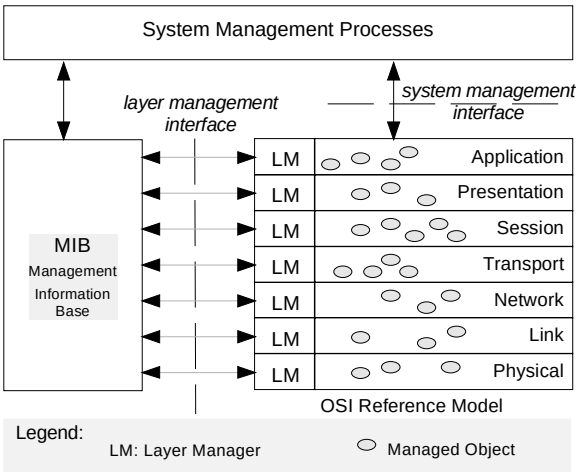

Figure 3 - Management information model.

The identification of a MO is provided by a OID (Object Identifier) that univocally specify the overall aspects of the OSI management framework (as classes, managed objects, attributes, operations, notifications and documents). The structure that organises all these identifier has a tree format in which top is based the main three paths of the hierarchy: ccitt(0), iso(1), e joint-iso-ccitt(2). Following the hierarchy each identifier is defined taking the layer numbers of the path (Figure 4). For instance the ROSE APDUs [10, 11] is {2 4 1} or a more compact {rm 1}.

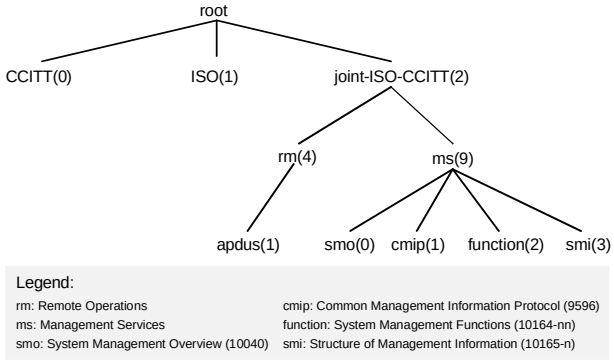

Figure 4 - OIDs tree

E. Communication Model

The communication model provides a set of rules to transfer management information between systems. This model is based on the application layer of the OSI model and it includes specific management element and common communication elements (Figure 5). This model is, as the overall management one, very rich in semantics and it includes a large set of acronyms and definitions. Some of those are define following to help clarify the communication model:

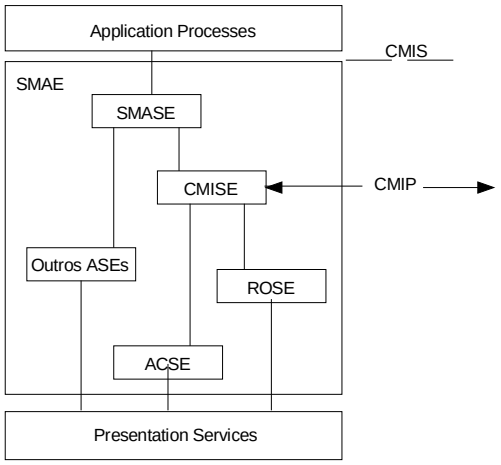

Figure 5 - Management communication model at the application layer.

SMAE Systems Management Application Entity - joins the mechanisms associated with the system management operations. The interaction between SMAEs is performed through the management protocol (CMIP) and each SMAE provides the management services to the applications (CMIS).

SMASE Systems Management Application Service Element - one of the main elements of the SMAE defines the semantic and the abstract syntax to the transmission of the management information.

ASE Application Service Element - is a generic identifier to all the elements that provide services in the application layer.

ROSE Remote Operation Service Element - a model that provides remote execution of processes [10].

ACSE Association Control Service Element [12] - used by the application protocols to establish an association between different system (AE-Application Element).

CMISE Common Management Information Service Elements - describes the procedures to the management information transfer. It uses the ROSE and ACSE services.

CMIS Common Management Information Service - the management services provides by the SMAE to the application processes.

CMIP Common Management Information Protocol - the CMIP is supported directly by the CMISE and represents the protocol used in the management connection.

From the above concepts it is important to highlight the rule of the CMIS/CMIP in the OSI management framework.

The management information services are used to the exchange of information and commands relevant within the system management [13]. Two type of services are identified: operation and notification (Table 1).

Table 1- CMIS: Common Management Information Service.

CMIS	Type	ROSE	ACSE
M-GET	confirmed	*RO-INVOKE/(RESULT)*	
M-CANCEL-GET	confirmed	*RO-INVOKE/(RESULT)*	
M-SET	both	*RO-INVOKE/(RESULT)*	
M-ACTION	both	*RO-INVOKE/(RESULT)*	
M-CREATE	confirmed	*RO-INVOKE/(RESULT)*	
M-DELETE	confirmed	*RO-INVOKE/(RESULT)*	
M-EVENT-REPORT	both	*RO-INVOKE/(RESULT)*	
			A-ASSOCIATE
			A-RELEASE
			A-ABORT

The event notification allow the utilisation of M-EVENT-REPORT service in confirmed and non-confirmed mode (Figure 6). This service, contrasting with the others, is initiated by the agent and it is used to report anomalous events. The operation services allow the reading (M-GET), the reading cancellation (M-CANCEL-GET) and the modification (M-SET) of management information. They provide also the tools for the request of specific (M-ACTION) and for the creating and destruction of managed object instances (M-CREATE and M-DELETE).

Table 1 includes as well the services to establish and terminate connections (from the ACSE): A-ASSOCIATE, A-ABORT and A-RELEASE.

The CMIS allow several facilities as: multiple response to a confirmed operation (through the *linked identifier*) and the extension of a single operation to multiple objects. The last is obtained by mechanisms as scoping, filtering and synchronisation.

The scoping identifies the managed objects through which the filtering must be performed. Four methods are allowed taking the MIB structure:

- the base object;
- all the objects below the base object (inclusive) until the *n*th-level;
- all objects of the *n*th-level below the base object; or
- the base object and all the tree below.

The filtering is constructed combining MO and its attributes with logical expressions. The final operation will be performed only on the objects that verify the pre-condition.

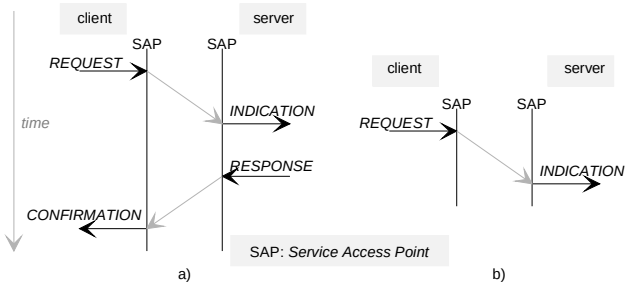

Figure 6 - Service type: a) confirmed e b) non-confirmed.

The synchronisation determine the mode of handling with errors during the response phase. Atomic synchronisation implies that all must be retrieved or nothing at all. In the best effort mode the agent will try to give the maximum operation results.

The CMIS functionality are delivered by a set of parameters included in each manager request (request e request-indication) and on the respective answer (response e response-confirmation).

The underlying protocol to all the services is the Common Management Information Protocol or CMIP [14]. It define the rules to be used in the information exchange between CMISEs. It uses the ROSE services (RO-INVOKE, RO-RESULT, RO-ERROR e RO-REJECT [10]) which PDUs (Protocol Data Unit) are mapped by the P-DATA service of the presentation layer [11].

F. Management Functions

Management functions as been defined in the context of the ISO/IEC 100164-x (or X.73x of ITU-T) document series. The propose is to create a base set of management procedures that can be used with success in several and more complex management areas. This type of approach avoid the duplication of function in different areas.

Most of the actual standardisation effort has been done on this functions implying a constant evolution and the emergence of new proposals. Some still are in a draft stage contributing to the indefinite state on the OSI management model. The main functions identified already are:

- Object management function
- State management function
- Relationship management function
- Alarm reporting function
- Event report management function
- Log control function
- Security alarm reporting function
- Security audit trail function
- Access control management function
- Accounting meter function
- Workload monitoring function
- Test management function
- Summarisation function
- Confidence and diagnostic test categories
- Scheduling function
- Management knowledge function
- Software management function

G. Evaluation of the OSI Management Model

The OSI management model suffers of a collection of problems some inherited from the normative process of the reference model others that are particular to the management framework. Other protocols families (as

TCP/IP, SNA, Novell, Microsoft Network) have today a greater importance on the market due to several reasons:

- The OSI protocols have been proposed without any practical evaluation that can show on the field and on large scale the applicability and acceptability from vendors and users.
- The ISO standards distribution are too bureaucratic, difficult to obtain and expensive. In opposite other norms (as the Internet Request For Comments - RFC) can be obtained free and quickly.
- The documents are too complex increasing the time of learning and consequently its full spreading.
- Some new technologies do not fit well in the OSI model (as ATM) or try to adapt to the architecture.
- The own reference model that was prepared to provide inter-operability between all systems allows different solutions at the transport layer (TP0 a TP4) a great drawback to the initial goal. The management model include also some concepts that are a bit far from the layer independence of the reference model (the MIB for instance).
- The standardisation process has been delayed to much increasing the frustration near the applications developer.

Even the management model is susceptible to some specific critics:

- The OSI MIB is too complex. It makes use of the O-O paradigm which simplifies the structure but can easily drive to huge objects.
- The data serialisation of the CMIP PDUs is provide through the BER (Basic Encoding Rules), which in spite of providing a powerful presentation syntax they increase the processing.
- The development of the management model is pointed as too expensive in terms of processing specially in small systems or in systems that do not provide the entire architecture pile (routers, bridges, repeaters).
- The system management is based on the normal systems used on typical applications. In case of faults in those services (ROSE, ACSE and below) management will be impracticable.

Some positive characteristics includes, for instance, a powerful group of services (CMIS/CMIP), scoping and filtering facilities that reduce the management traffic and a modular architecture that, in principle, will facilitates the implementation.

The positive factors are largely overlapped by the negative characteristics which have been the main motive to the successive degradation of this standardisation effort. The expectation still remain due to political position assumed by some communities, namely Europeans, that try to push the development of this solutions. However, not of all follow this position. The NIST (National Institute of Standards and Technology), for instance, that is responsible for the USA's normative development in the communication networks field, abandon the OSI to adopt the TCP/IP in the GOSIP (Government Open Systems) [15].

II. INTERNET MANAGEMENT MODEL

The TCP/IP protocols have its origins in the remote year of 1969 when the DoD (Depart of Defence) in the USA has decided to support the development of the first packet communication network (ARPANET). From this work it result five communication protocols for computer networks (TCP, IP, SMTP, FTP e TELNET). While the OSI architecture make its first steps this model go outside the military area and was used by several corporations in commercial applications. The Internet is today the result of this expansion and it serve millions of users all over the world.

During the 80th it was obvious that this growing can not be handled without having a organised management police that will substitute the current ad-hoc strategy.

Assuming a opposite tactic of ISO the Internet community has capture much of it adherence from the normalisation of already tested and accepted solutions. The standards are published as RFC (Request For Comments) by the IAB (Internet Activity Board). This organism is composed by two sub-groups: the IETF (Internet Engineering Task Force), responsible for the identify and provide solutions to problems and the IRTF (Internet Research Task Force) that intents to study the users needs.

As a result of this investigation work there were developed three proposals for a management protocol. The HEMS/HEMP (High-level Entity Management System/Protocol) [16][17], the SNMP (Simple Network Management Protocol) and the CMOT (CMIP over TCP/IP). The SNMP [18] have been chosen as the short-time while the CMOT [19] that was a interim compromise with the OSI framework was chosen as the long term protocol. Meanwhile, the successive delays and failures of OSI management architecture has driven the CMOT to complete abandon.

The SNMP demonstrated a large acceptance near developers and users. Although it was designed as an interim solution and it simplicity some times is not an enough advantage due to the lack of some important features. As a consequence of the CMOT/CMIP abandon it was introduced a second version of the SNMP (SNMPv2) intended to fill some of the SNMP gaps. Unfortunately, it did not realise until now a strong commitment from the management community.

A. TCP/IP Network Management

The Internet management is based on a reduced set of concepts that share some ideas with the OSI architecture. As an example it remains the manager and agent concept, the usage of a management protocol to the information

exchange, reading and writing operation over management information and the MIB concept.

Primary elements of this model are:

- Agents
- Manager station
- Management Information Base (MIB)
- Management protocol - SNMP

Optionally, it can be used the concept of:

- Proxy Agent

In spite of the reduced group of elements the IETF proposals are focus only on the MIB (contents and structure) and on the management protocol (SNMP) which makes the normative documents very accessible and simplifies the development of applications. Since there is none standard document that defines the overall Internet management framework, the main guidelines the have been dictated by some authors [20][21] [22]:

- Each system connected to the network must allow its own management through SNMP.
- The introduction of management mechanisms inside a system must have a minimal impact in costs and performance.
- The extension of management features must be easy to realise namely the addition or redefinition of management information.
- Management must be robust to still provide some functionality even in fault situations.

1. Managed Agent

Conceptually an agent represents each network element that can be provided with SNMP. Some examples are for instance: computer, printer, bridge, router, repeater and a switch.

An agent must respond to information reading and writing request, coming from the management station, or it can provide asynchronous notifications about internal events or conditions.

2. Management Station

The management station is usually based on a single system (PC or workstation) and its task is to control and centralise the management activities distributed by the agents. Since its architecture is not motive for standardisation work its development as be let freely to equipment and applications producers. The only important characteristic must be the "speaking" of SNMP.

3. MIB - Management Information Base

Since the initial strategy to the CMIP migration it becomes crucial to agree on a common organisation to the management information. The SNMP MIB is similar to the OSI MIB, though the attribute concept has replace the object one and there is none object oriented methodology.

The management information structure is defined by a set of syntactic rules semantically defined as the SMI (*Structure of Management Information*) [23]. The SMI is guided by simplicity and it admits only four ASN.1 syntax types to codify data (INTEGER, OCTET STRING, SEQUENCE, SEQUENCE OF). Each object is characterised by a set a rules that beyond its syntax (SYNTAX), shows other characteristics as [24]:

- ACCESS, reading and writing permissions of the attribute;
- STATUS, mandatory or not its inclusion;
- DESCRIPTION, textual explanation of the attribute;
- REFERENCE to other attributes;
- INDEX, how to index tables;
- DEFVAL, default value of the attribute.

Objects (attributes) are identified in a similar way to the OSI process. The Internet has a path on the Management Information Tree (MIT) rooted at:

```
internet OBJECT IDENTIFIER ::=
            { iso(1) org(3) dod(6) 1 }
```

The object identification is obtained by the association of all the number of the hierarchy. An example of a OID (OBJECT IDENTIFIER) can be:

```
iso org dod internet mgmt mib-2 system  sysDescr
 1   3   6     1      2     1      1       1
```

Its instance will be sysDescr.0 or “1.3.6.1.2.1.1.1.0”.

One MIB is normally defined to fulfil a special equipment management needs. The first one, however, was designed to serve a large base of systems. The MIB-I [25] was quickly replaced by a more complete version that remains until the present, the MIB-II [26]. Objects of each were organised in several groups as presented on Table 2.

Since MIB-II other MIBs have populated the standardisation route, driving to an impressive growing on the overall management information that a Network Management System (a more general concept than the management station) must be able to handle. Table 3 presents the Internet MIBs that are currently in the normalisation process (RFC).

Table 2 - MIB-I and MIB-II objects.

Group	MIB-I	MIB-II
system	3	7
interfaces	22	23
at	3	3
ip	33	38
icmp	26	26
tcp	17	19
udp	4	7
egp	6	18
transmission	-	0
snmp	-	30

4. Proxy Agents

Proxy agents allows the integration on the SNMP management framework of "dummy" equipment unable to include SNMP primitives either by performance reasons (small systems) either by the absence of underlying support (TCP/IP protocols). The proxy mission is to

Table 3 - MIBs in RFC.

MIB	RFC
MIB-II	1213 (1158)
IEEE 802.5 Token Ring	1231
AppleTalk	1243
OSPF version 2	1253
Border Gateway Protocol (BGP-3)	1269
IP Forwarding Table	1354
DS1/E1 Interface Types	1406 (1232)
DS2/E3 Interface Types	1407 (1233)
X.25	1461
Point-to-Point Protocol	1471-4
Bridges	1493 (1286)
FDDI	1512 (1285)
Token Ring Extensions to RMON	1513
Host Resources	1514
IEEE 802.3 Medium Attachment Units	1515
IEEE 802.3 Repeater Devices	1516 (1368)
Source Routing Bridges	1525 (1286)
DECnet Phase IV Extensions	1559 (1289)
Network Services Monitoring	1565
Mail Monitoring	1566
X.500 Directory Monitoring	1567
Interfaces Group of MIB-II	1573 (1229)
SNA APPN Node	1593
SONET/SDH Interface	1595
Frame Relay Service	1604
Domain Name System	1611-2
Uninterrupted Power Supply	1628
Ethernet-like Interface Types	1643 (1284)
Border Gateway Protocol (BGP-4)	1657
Character Stream Devices	1658 (1316)
RS-232-like Hardware Devices	1659 (1317)
Parallel-printer-like Hardware Devices	1660 (1318)
SNA NAU	1665-6
SMDS Interfaces	1694
ATM	1695
Modem	1696
Relational Database Management System	1697
RIP version 2	1724 (1389)
Remote Network Monitoring	1757 (1271)

collect management request to those equipment, realise ad-hoc communication with them to obtain the necessary information and respond (as a proxy!) to the manager.

Another potential utilisation can be the reduction of management traffic since this strategy can be adopted even in "no-proxied" situations where a front-end system is responsible for the management of "hidden" equipment.

5. Management Protocol

The management protocol is responsible for the exchange of information between systems (manager-agent) as the CMIP on the OSI management architecture. Most of the time, the term SNMP is used indistinctly to identify the management protocol or the Internet management model.

The management protocol completes with the agent, manager, proxy and the MIB concept the definition of this management model. The relation between them is presented on Figure 7.

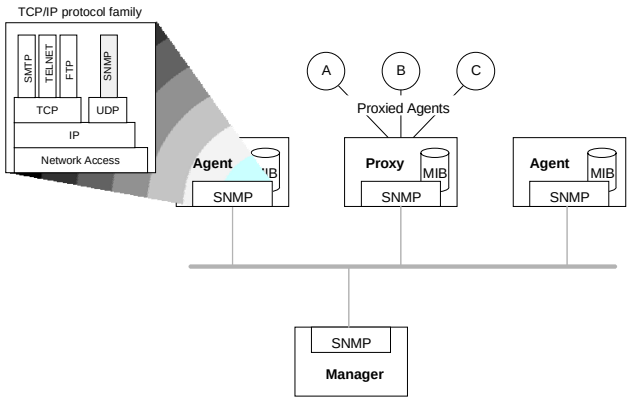

Figure 7 - Internet management model.

B. SNMP - Simple Network Management Protocol

The SNMP [18] is the base for the Internet management framework. The protocol provides only four operations (*get*, *get-next*, *set* e *trap*) that simplifies the implementation. Associated with each operation there is a security mechanism consisting on the identification through a special keyword known and shared by all the elements of a community. The authorisation is establish by the access type defined for that community (*read-only*, *read-write*) in conjunction with the access of each object (ACCESS clause in the SMI formalism).

The SNMP protocol is asynchronous i. e., an SNMP do not need to wait for response after send a request message. It provides five PDUs (with two different formats) to construct the operations:

- *GetRequest* and *GetNextRequest*, for reading of management information;
- *SetRequest*, to modify objects (or create lines in tables);
- *Response*, that delivers the results for any of the previous one; and the
- *Trap*, used to notify the manager of anomalous events.

From these primitives, three are confirmed with origin on the manager (*get*, *get-next* e *set*) while the other (*trap*) is non-confirmed and it is send by the agent (Figure 8).

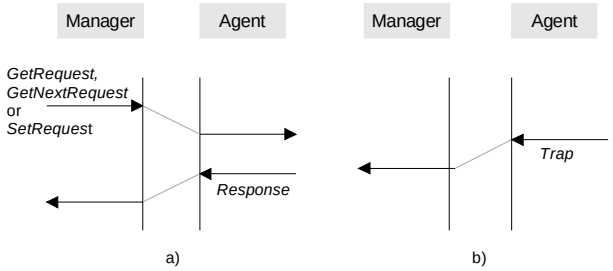

Figure 8 - SNMP primitives: a) confirmed initiated by the manager; b) non-confirmed initiated at the agent.

The *get* and the *get-next* operations are different in the way the objects OIDs are solved. In a *GetRequest* PDU the manager specifies the instances of the objects it want to retrieve. This operation implies the overall knowledge of the agent MIB at the manager side. Taking into account the dynamism of some tables it is difficult to maintain that type of information on the manager. The agent solves a *GetNextRequest* by respond not the instance value of the specified object but its successor in the numeration structure of the SMI. A obvious advantage of this primitive is to allow the learning of the MIB structure. Using a pseudo-code algorithm where 0.0 represents a virtual OID above the top of the MIB the overall capture can be done by:

```
currentInstance = get-next(agent, community, 0.0)
while currentInstance not equal ERROR do
    currentInstance =
    get-next(agent, community, currentInstance)
```

Another advantage is related with a greater error immunity that occurs on the object identification list of each request.

The *trap* operation will be active when some abnormal situation occurs on the agent. Since this type of events can easily overcharge the network and the manager it must be careful planned when designing the agent. One solution is to use thresholds to activate and deactivate the notification process. An alternative solution consist on the polling method that is used on the normal reading operations (*get*, *get-next*). This method has the disadvantage of lose the temporal information associated of the events though it implies more simplicity on the agents. Other disadvantage is related with the traffic overhead imposed specially when the presence of a large set of agents [20] [27].

A compromise still is the more effective solution: use the notification only to inform an abnormal situation and let the manager ask for more specific details about the problems.

C. SNMP versus CMIP

The first differences appear at the transport layer mechanisms. While the SNMP uses a connection-less association (CL) the CMIP is based on a connection-oriented model (CO) at the application layer.

The choice of a CL mode in the SNMP case was a deliberately option that intents to achieve more robustness. In fault conditions a datagram connection can still deliver frames while the virtual connection will compromise easily the exchange of data [4]. However a CL association demands additional error recovering mechanisms that must be include (or not) in the manager depending on the strategy due to retransmission. Another advantage of the CO mode came from the implicit detection of the agent operability while the connection remains establish.

The SNMP over UDP presents an important gap that results from the upper limit of the UDP frames. When a particular response is larger then that value it will be returned a error message. To avoid this type of situations the manager should not abuse on the dimension of the list of objects to retrieve.

Considering the services it is clear that the CMIP/CMIS present a great and more powerful set of services. However the SNMP allows, with much more simplicity, to solve almost of the functionality of the CMIP (for instance the *set* operation allows to replace the operations *action*, *create* and *delete*).

The SNMP presents some generic limitations as: absence of authenticated notifications, inefficient table retrieval, poor security mechanism and no support for management distribution. The SNMPv2 try to fix some of these problems.

D. SNMPv2 - SNMP version 2

The SNMP have since its inception a great acceptance in the market. Its limitations to handle current increasing management demands has been a drawback to be considered "The" Internet management protocol.

The expectation around the CMIP have been not corresponded by market adherence. Likewise the CMOT strategy was successively abandoned. New solutions are need to consolidate and enhance the SNMP. In July, 1992, were published the first set of documents that introduce the migration to a second version of the SNMP - the SNMPv2. The rebuilt protocol reflects some of the following goals:

- Ability to manage all type of resources (in agents or in managers) with an increase of efficiency on the table retrieval.
- Keep the protocol as simple as possible with a small impact on the systems.
- Better security mechanisms.
- SNMP(v1) compatibility.

The SNMPv2 shows how an increase in power and complexity can be as controversy as it was for the CMIP process. The SNMPv2 documents published in May 1993 as “Proposed Standard” [28], were been subject of a long evaluation and redefinition phase that at the end of 1995 drives to a retrocession on some of the major ideas of the initial work (namely the administration model and the remote management capabilities). Actually this protocol is recognised also as SNMPv2C (RFC1901..RFC1908).

1. Main differences to SNMP

The SNMPv2 presents a new set of characteristics beyond the already existing on the SNMP(v1):

- The SMI was enhanced by new data types and a systematic method for row table creation and elimination.
- The protocol includes new management operations: the *getBulk* used on table retrieval and the *inform* to allow the exchange of information between two managers.

- A more complete definition on the protocol mapping.

Other concepts as the Party MIB and the Administration model were removed in the last version - SNMPv2C.

All this scenario is only possible through a significant increase on the extension and on the complexity of the normative documents. While the SNMPv1 was presented in two single documents, SNMP and SMI (≈58 pages), the SNMPv2, on its initial version is spread over 13 documents (≈417 pages).

2. SNMPv2 (SNMPv2C) operations

The protocol provides three types of interaction between entities (Figure 9):

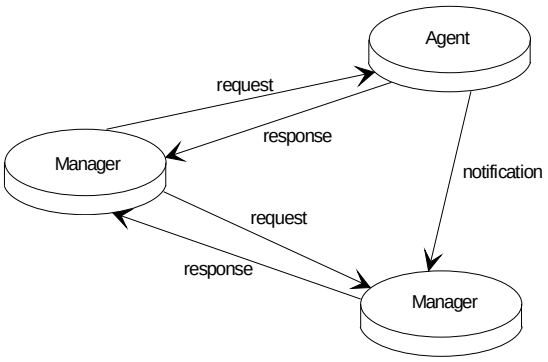

Figure 9 - SNMPv2 interactions.

a) a *request-response* initiated by the manager entity to request or modify information on the managed entity;
b) a similar connection but between two managers;
c) a non-confirmed communication initiated at the agent to notify abnormal events.

For the construction of these interactions there are specified 7 PDUs that use only two syntax types (PDU and BulkPDU) as the following ASN.1 description [29]:

```
GetRequest-PDU ::=     [0] IMPLICIT PDU
GetNextRequest-PDU ::= [1] IMPLICIT PDU
Response-PDU ::=       [2] IMPLICIT PDU
SetRequest-PDU ::=     [3] IMPLICIT PDU
      -- obsolete      [4]
GetBulkRequest-PDU ::= [5] IMPLICIT BulkPDU
InformRequest-PDU ::=  [6] IMPLICIT PDU
SNMPv2-Trap-PDU ::=    [7] IMPLICIT PDU
```

The syntax of the PDU is similar to the one of the SNMPv1 with more error codes, while the new syntax associated with the BulkPUD is represented as:

```
BulkPDU ::= SEQUENCE {
  request-id      Integer32,
  non-repeaters   INTEGER (0..max-bindings),
  max-repetitions INTEGER (0..max-bindings),
  variable-bindings   VarBindList
}
```

This PDU allows the specification in a single request of a larger set of attributes specially useful when reading tables. The existing association one-to-one in the SNMPv1 was replaced by a one-to-many association. The previous ASN.1 helps to identify the parameters that allow this functionality.

The non-repeaters and max-repetitions parameters control the way the expansion must be performed (Figure 10). Considering T the number of attributes (variable bindings) specified in a *GetBulkRequest-PDU*, the non-repeaters value represents the first N attributes with one-to-one relation, while the max-repetitions (M) indicates the amount of attributes that must be returned by each one of the enumerated (one-to-M relation). The repetition consist on returning the indicated variable plus the following M-1 for each variable of the R set (=T-N). The amount of returned attributes is obtained from N+(M*R).

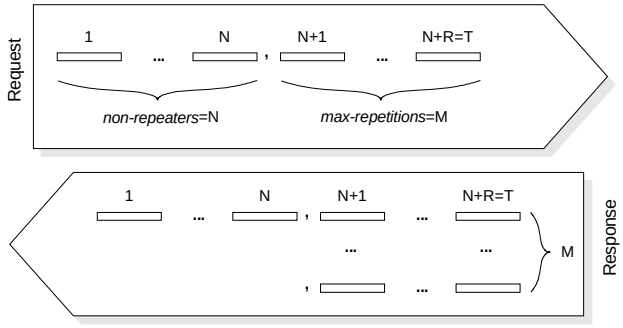

Figure 10 - Attributes expansion in the *GetBulkRequest-PDU*

E. Evaluation of the Internet Management Model

The Internet management presents some commons aspects with the OSI management framework that are result of similar origins either in timing as in motivation. The Internet one has, however, a bigger acceptance in the market as a consequence of a more realistic and practical approach: simple solutions, on field trial with proved results and, probably more important, the real open philosophy of the Internet community.

The SNMP was developed on the finals of '80s with the goal to solve management problems in a short term program, having in mind its future substitution with the CMIP.

Though the SNMP environment presents some limitations it was quickly accepted due to its simplicity and also due to an great "hungry" for management platforms. On the other side, the OSI disillusion has push the development of a new architecture - the SNMPv2.

The current version of the SNMP is already a step further from its initial proposal. The spreading of this protocol over almost all the computer systems and network equipment let guess too much barriers for replacing it in the near future. Any modification must careful proposed guarantying the actual compatibility and a smooth migration to eventually different solutions.

III.TMN MANAGEMENT

The TMN (Telecommunications Management Network) is special network developed to interface the

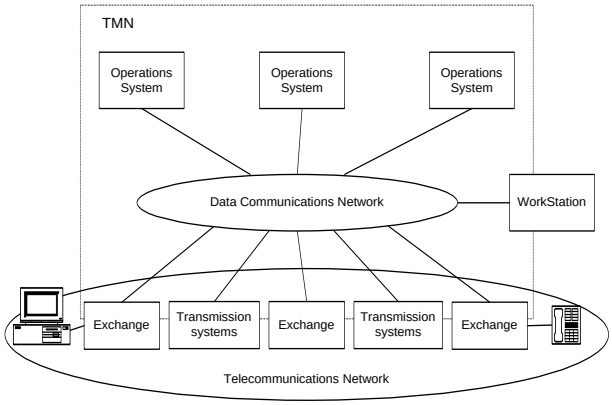

Figure 11 - TMN integration on telecommunication network

telecommunications network at several different points in order to realise management tasks [30]. In Figure 11 is presented the relationship between both networks. The interface point are formed by *Exchanges* and *Transmission Systems* which are connected to one or more *Operations Systems* by the *Data Communications Network*. The TMN defines these elements and interfaces.

A. The TMN standardisation

The TMN standardisation process started in 1985 by the CCITT Study Group IV and since then and specially until 1992 it has produced a set of related recommendations as exposed in Figure 12 [31].

The TMN share some concepts with the OSI management architecture as:

- Manager-agent concept
- Object-oriented approach
- Management domains

However there is a big difference between the two approaches as can be observed on the Figure 11: the TMN is based on a separated network for the transfer of management information.

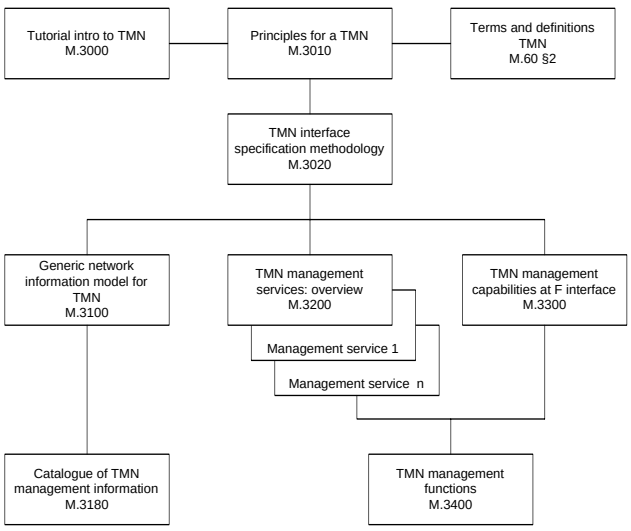

Figure 12 - TMN recommendations

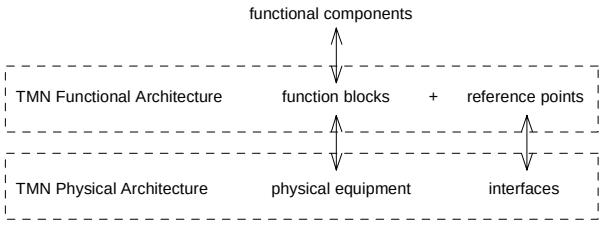

Figure 13 - TMN architectures.

TMN's recommendations define three different architectures (Figure 13):

- A functional architecture
- A physical architecture
- An information architecture, that describes basically the concepts already defined in session I, for the OSI management model.

The functional architecture is defined in terms of *function blocks* and *reference points*. The firsts contain *functional components* and are similar to the OSI protocol entities. The lasts are used to interconnect *function blocks* and can be compared to the services providers of the OSI model.

The physical architecture is defined at a lower level at maps the *function blocks* into physical equipment and the *reference points* into *interfaces* (Figure 13).

B. Functional architecture

The functional architecture defines five types of *functions blocks* that can be supported by each TMN configuration. These five types are represented on Figure 14. According to the diagram, two types (OSF and MF) are inside the TMN square which means that they are completely specified by the TMN recommendations. The other three are only partially specified by TMN (QAF, NEF and WSF).

Besides the previous elements there are identified also five reference points that specify the interface to access each of the function blocks. The `q` allows two different versions: the `qX` and the `q3`. The reference point `x` (not represented) only applies to interconnect different telecommunication networks.

The Network Element Function (NEF) are functions performed by network elements (NEs) of the telecommunications infrastructure that are relevant to management goals. Examples are the *exchanges* and *transmission systems* as presented on the overall picture of Figure 11. TMN define these functions as:

- Primary telecommunications functions, which are not covered by TMN.
- Management functions, that allows the NE to operate as a management agent.

The Operations System Functions is a manager specific entity that initiate operations and receive notifications. The communications between OSFs or with the NEs is performed through a q_3 reference point that represents the CMIS (of the OSI model) Whenever exist a

communication between different telecommunications operators it will be done over a x reference point.

The Work Station Function (WSF) provides the mechanisms to handle the information at the user interface and is largely defined outside the scope of TMN.

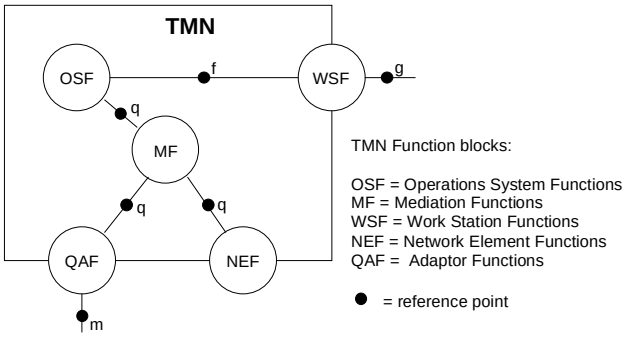

Figure 14 - TMN *Function blocks.* and *Reference points*.

The Q Adaptor Function (QAF) is used to connect to the TMN entities that do not support TMN reference points (the proxy concept of the SNMP framework).

The Mediation Function (MF) provides processing and filtering tools over the information that is passed between NEFs or QAFs, and OSFs.

C. Physical architecture

The physical architecture defines how the function blocks and reference point can be implemented. It defines the following building blocks each one implementing the function block with the same name (multiple if needed):

- Network Element (NE).
- Mediation Device (MD).
- Q Adaptor (QA).
- Operations System (OS).
- Work Station (WS).
- Data Communication Network (DCN).

The DCN is the exception since it does not implement a function block but is used by the others building blocks for exchange management information (see Figure 11).

Interfaces are the physical implementation of the reference point abstraction as the protocols are the implementation of the OSI layer services. The mapping is described in Figure 15.

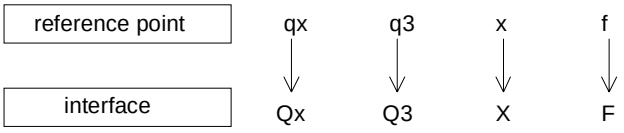

Figure 15 - Mapping between *reference points* and *interfaces*.

D. Responsibility Model

TMN also recognises a set of hierarchy of management responsibilities likewise the management functional areas of the OSI management model. Such hierarchies can be described in terms of management layers (and there function blocks):

- Business Management layer (OSF).
- Service Management layer (OSF).
- Network Management layer (OSF).
- Network Element Management layer (OSF and MF).
- Network Element layer (NEF).

E. Evaluation of TMN

The TMN includes many ideas of OSI management and so it inherits also some of its problems. Despite the similarities there still are several differences.

TMN defines multiple and related architecture at different levels of abstraction (functional and physical architecture).

A second difference comes from the responsibility model of TMN that mirrors what exist in the real world (no similar approach is provided in OSI). This strategy simplifies the implementation since it becomes easier to understand.

Finally the major big difference resides on the separation of the communication network from the management network. This out-of-band management allows to keep an eye on the network even in severe anomalies that do not allow any type of transmission in the communication network. Although the DCN can itself have failures which implies the DCN management also. This choice can be understandable in the telecommunications network but it may became too expensive on smaller networks (as LANs and CATV). Nevertheless it can always be realised in the Internet or in the OSI management environments by constructing a separated management network that interconnects the main communication equipment.

It is clear that beside the similarities and differences, TMN was special designed for telecommunications network while the OSI, and its management model, were created for data communications networks. The SNMP based management is a direct concurrent of the OSI market but is also be used on TMN applications that integrates the existing SNMP equipment through Q_3 adaptors.

IV. CONCLUSIONS

The discussed management architectures present some similarities namely the agent-manager duality, the existence of a special designed management protocol and the structuring of management information. Nevertheless the conciliation between normalisation strategies and market demand is not always achieved. The past has show that the impact of largely spread solutions have great importance and typically they tend to became *standard de facto* in detriment to other existing standards. Although the implementation of management solutions must have a minimal impact on the users and, if possible, on the budget.

The OSI normalisation process has been to costly to developers since it is successively delayed, it is a complicated model, it drives to expensive applications and it inherits the OSI reference model that shares a (very) small “piece of the cake”.

The TMN, in spite of being developed under the same principles of the OSI model, has a great market (telecommunications network) that can push it in a different way. Even in this field the solutions pass very frequently by other type of management environment, namely SNMP equipment.

Finally the Internet management, or simply the SNMP, have demonstrate that the simpler solutions are easier to accept than complicate even more powerful ones. Management equipment existing today are mostly based on the SNMP protocol. This is a reality that must be faced because it has a bigger importance on strategy planning.

V. REFERENCES

[1] ISO 7498, Information Processing Systems - Open Systems Interconnection - Basic Reference Model.

[2] ISO/IEC 7498-4, Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management Framework.

[3] ISO/IEC 10040, Information Processing Systems - Open Systems Interconnection - Systems Management Overview.

[4] William Stallings, *SNMP, SNMPv2 and CMIP, The Practical Guide to Network-Management Standards*, Addison-Wesley, 1993.

[5] Y. Kobayashi, “Standardization Issues in Integrated Network Management”, in *Proc. of the IFIP TC6/WG6.6 Symposium on Integrated Network Management*, pgs. 70-90, North-Holland, 1989.

[6] ISO/IEC 9542, Information Processing Systems - Data Communications - End Systems to Intermediate System Routing Information Exchange Protocol for use in conjunction with the Protocol for the Provision of the Connectionless-mode Network Service.

[7] ISO/IEC 10165-1, Information Processing Systems - Open Systems Interconnection - Structure of Management Information - Part 1: Management Information Model.

[8] ISO/IEC 10165-2, Information Processing Systems - Open Systems Interconnection - Structure of Management Information - Part 2: Definition of Management Information.

[9] B. Meyer, *Object-Oriented Software Construction*, Prentice-Hall, 1998.

[10] ISO/IEC 9072-1, Information Processing - Text Communication - Remote Operations - Part 1: Model, Notation and Service Definition.

[11] ISO/IEC 9072-2, Information Processing - Text Communication - Remote Operations - Part 2: Protocol Specification.

[12] ISO/IEC 8649, Information Processing Systems - Open Systems Interconnection - Service definition for the Association Control Service Element.

[13] ISO/IEC 9595, Information Processing Systems - Open Systems Interconnection - Common Management Information Services Definition.

[14] ISO/IEC 9596, Information Processing Systems - Open Systems Interconnection - Common Management Information Protocol Specification.

[15] “Regulatory Watch”, Data Communications, Vol. 22, Nº 13, pg. 17, September 1993.

[16] C. Partridge, G. Trewitt, “High-level Entity Management System HEMS”, *Internet Request for Comments 1021*, October 1987.

[17] C. Partridge, G. Trewitt, “High-level Entity Management Protocol HEMP”, *Internet Request for Comments 1022*, October 1987.

[18] M. Schoffstall, M. Fedor, J. Davin, J. Case, “A Simple Network Management Protocol (SNMP)”, *Internet Request for Comments 1157*, October 1990 (STD 15).

[19] L. Besaw, B. Handspicker, L. LaBarre, U. Warrier, “The Common Management Information Services and Protocols for the Internet”, *Internet Request for Comments 1189*, October 1990.

[20] A. Ben-Artzi, A. Chandna, U. Warrier, “Network Management of TCP/IP Networks: Present and Future”, IEEE Network Magazine, pgs 35-43, Vol.4, Nº4, July 1990.

[21] M. T. Rose, “Network Management is Simple: you just need the right framework!”, in *Proc. of the Second IFIP TC6/WG6.6 International Symposium on Integrated Network Management*, pgs. 9-25, North-Holland, 1991.

[22] M. T. Rose, *The Simple Book, An Introduction to Management of TCP/IP based internets*, Prentice Hall, 1991, 0-13-812611-9.

[23] K. McCloghrie, M. Rose, “Structure and Identification of Management Information for TCP/IP-based Internets”, *Internet Request for Comments 1155*, October 1990 (STD 17).

[24] K. McCloghrie, M. Rose, “Concise MIB Definitions”, *Internet Request for Comments 1212*, March 1991 (STD 16).

[25] K. McCloghrie, M. Rose, “Management Information Base for Network Management of TCP/IP-based internets”, *Internet Request for Comments 1156*, Maio 1990.

[26] K. McCloghrie, M. Rose, “Management Information Base for Network Management of TCP/IP-based internets: MIB-II”, *Internet Request for Comments 1213*, March 1991 (STD 17).

[27] Steven L. Waldbusser, “The Truth About SNMP Performance”, *The Simple Times*, Vol. 1, Nº 3, pgs. 7-8, 1992.

[28] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Introduction to version 2 of the Internet-standard Network Management Framework", *Internet Request For Comments 1441*, May 1993.

[29] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, "Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)", *Internet Request For Comments 1448*, May 1993.

[30] CCITT Recommendation M.3010, "Principles for a Telecommunications Management Network", Geneva 1992.

[31] Aiko Pras, *Network Management Architectures*, Ph., D-thesis, University of Twente, Enschede, The Netherlands, 1995