Submitted to IFIP *"Second International Conference on Local Communication Systems - LAN and PBX"*, Palma, Spain, June 1991

EFFICIENT NETWORK MANAGEMENT FOR A HIGHLY DISTRIBUTED SYSTEM

Martin Siegel
Institut für Nachrichtenvermittlung und Datenverarbeitung
Universität Stuttgart
Seidenstraße 36, D-7000 Stuttgart 1

Klaus Sauer
TELENORMA GmbH Bosch Telecom
Mainzer Landstraße 128-146, D-6000 Frankfurt 1

Abstract

Future Inhouse communication architectures will be characterized by their key elements namely integrated voice/data service, distributed processing, high performance and fault tolerance as well as an efficient network management. But management functions will lead to an additional overhead on these communication systems. To achieve high performance and a minimum processing overhead, the architecture and capabilities of a network management must be adapted to the chosen architecture of the communication system /1/,/3/.

This paper deals with a highly distributed multi-service Broadband-ISPBX designed for the private area with a network management architecture providing high efficiency and capabilities for decentralized network structures.

1. Introduction

Todays international telecommunication area is characterized by the growing interest on distributed network architectures. The major goals achieved by distributed system structures are the modularity of network components to achieve fault tolerant services and resource sharing of the switching capabilities. The aspect of modularity also enables the network provider to improve the reliability of the system. By-pass mechanisms, decentralized processing elements and capabilities of process migration offer protection against network damages.

The efficient handling and monitoring of communication networks is the task of the network management. ISO (International Standardization Organization, a list of abbreviations can be found at the end of the document) is currently establishing a set of standards covering the management of telecommunication networks. The framework of the OSI management is defined by the basic architectural model /4/.

Network management is identified as a tool for coordinating and controlling the resources logically represented by managed objects. Thus, developing a highly distributed communication system, the requirements for the requested management must be evaluated carefully.

A centralized network management approach reduces the reliability concepts of distributed systems. It should be noted that one global management master process, as proposed by the SNMP (Simple Network Management Protocol, /6/), results in a complex functionality which leads to big problems in load sharing and fault tolerance but needs very simple management clients.

The management architecture we suggest in this paper is a highly decentralized approach. Every unit of the distributed system contains its own management block. Thus, the structure of the network management is similar to the architecture of the communication system. The drawback of this approach is the increasing complexity of each unit management block and the increase of data exchange between different management entities within the distributed system. The advantages are the higher reliability of the management tasks, the splitting of the network management functions into smaller pieces which allow the migration of management functions in the case of system failures. Another advantage of the coupling of management functionality to the associated unit is the flexibility of adding new components due to the direct linkage of network component and related management functionality.

A rough overview of the ISO management concepts is described in the following section. The architecture of the distributed Broadband-ISPBX is introduced in Section 3. The reasons to extend the ISO management definitions and the applied structure of the network management are discussed in Section 4. Some implementation aspects of the hierarchical management structure are described in Section 5. An outlook concludes the paper.

2. OSI Management Concept

Fig. 1 represents the structure of the OSI Management from the architectural

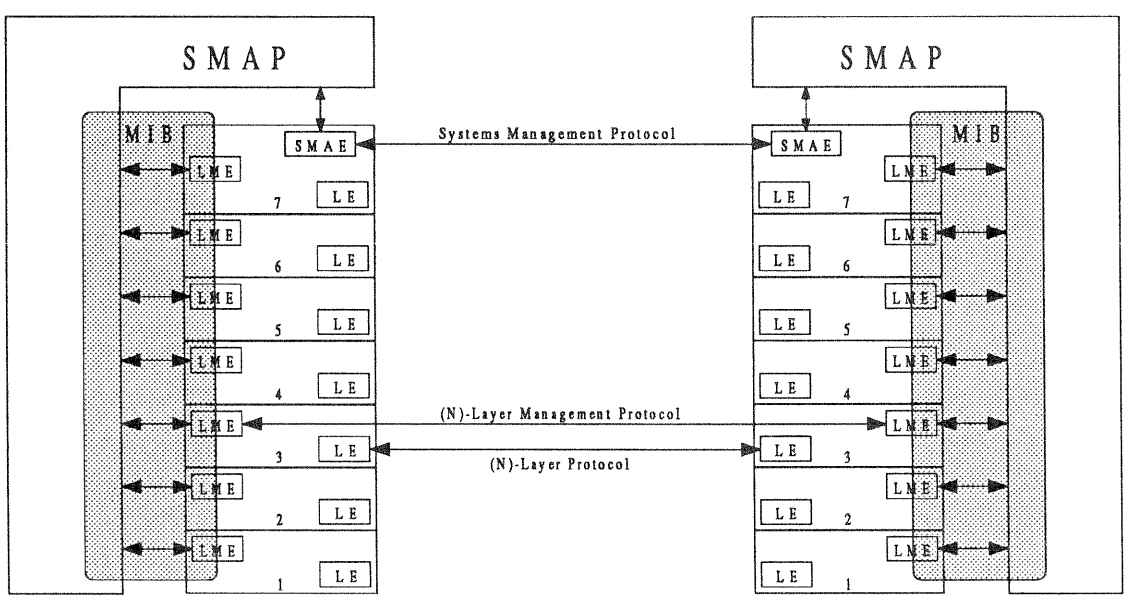

Figure 1: OSI Management Model

point of view. The System management application process (SMAP) acts as the logical master process and will be the only instance for providing an interface to the administrator or other applications.

To provide the extendability of protocols and procedures an object oriented approach is derived for the OSI management to describe the context to be managed. The logical representation of the communication resources are given by managed objects which are defined in terms of attributes, actions and events.

3. Architecture of the distributed ISPBX-System

Until the present voice and data services are handled by separate networks. One main objective of new inhouse communication systems is the integration of these services within the business environment. Another important goal is the implementation of the Asynchronous Transfer Mode (ATM) as the switching principle for future broadband services.

An architecture for new ISPBXs must be capable of integrating all existing services as well as providing a migratory concept to the future B-ISDN solution. Although the well-known requirements in terms of variable and flexible system configuration must be solved in a cost-efficient manner. Taking into account the above mentioned requirements a structure of a distributed Broadband-ISPBX can be introduced as depicted in Fig. 2.

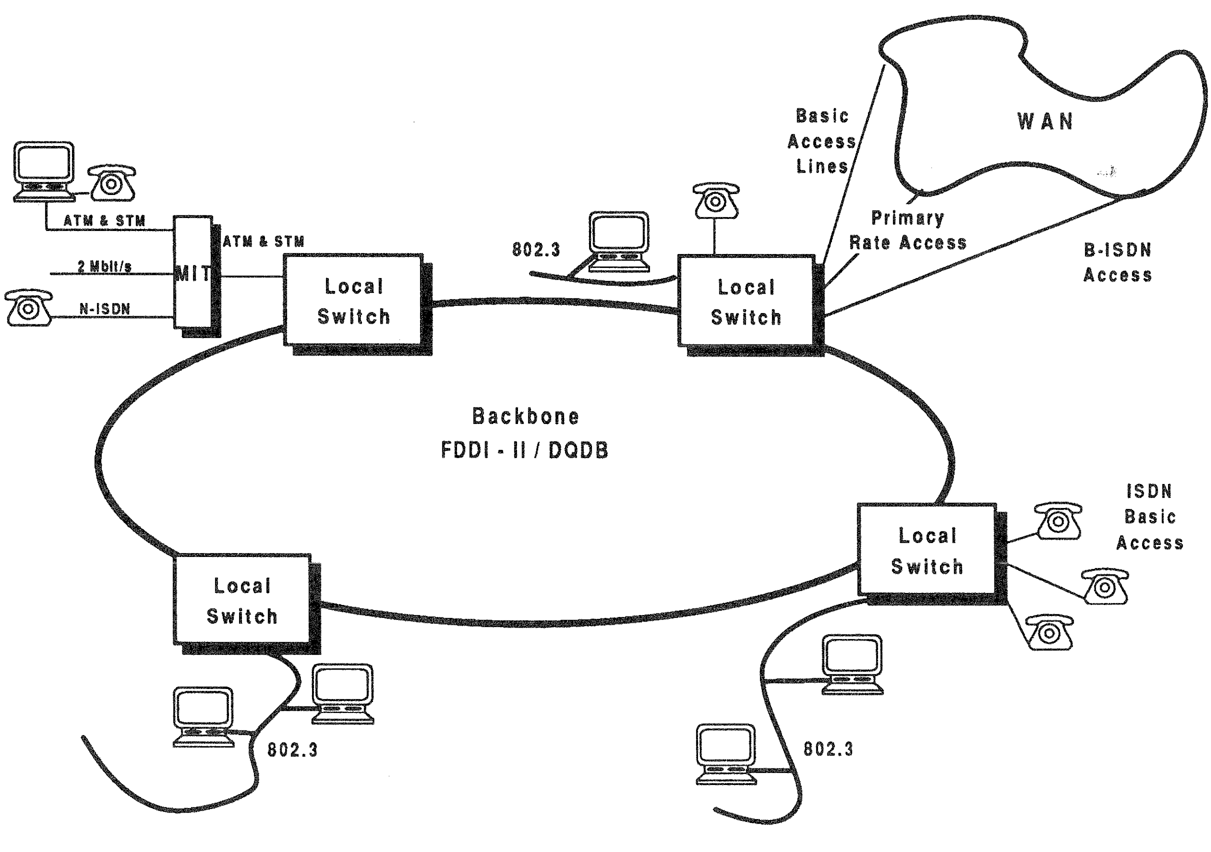

Figure 2: Architecture of a Distributed ISPBX System

The overall system consists of *Local Switch*es with hybrid switching capabilities. This means, every Local Switch is able to transmit isochronous traffic - e.g., voice or video - and ATM cells, which are intended to carry all kinds of traffic, simultaneously. This hybrid switching capability is suitable to migrate from todays available PBXs to future Broadband-ISPBXs in an easy and cost-efficient way.

A variety of terminals like POTs, Narrowband-ISDN, LANs, workstations, mainframes, videophones can be connected to a Local Switch via *Port Units*. All Port Units are connected to the Local Switch via an service independent interface called Standard Internal Interface (SII). A Local Switch can act as a stand-alone system. To achieve flexibility in terms of system size and adaptability of user demands many Local Switches can incorporate together using one or more backbone systems.

Key element of this distributed Broadband-ISPBX system is the Local Switch, which is based on a folded bus structure with an internal bandwidth of 262 Mbps. The main reason for using a shared medium as the switching media is that this technique is well understood and that it provides a flexibility in terms of access protocol and distribution of traffic (broadcast messages can be easily handled). The folded bus structure is suitable to increase the bandwidth of the switch up to 800 Mbps which might be necessary in the future.

Each Local Switch consists of its own *subsystem control unit* and up to 60 Port Units which can be connected to each Local Switch via the SII.

The subsystem control unit handles the isochronous call control of that Local Switch and parts of the Local Switch relevant management tasks. To provide the dynamic migration of tasks and resource allocation a distributed real-time Operation System (dOS) is implemented.

The interconnecting backbone uses the same standard internal interface to communicate with the Local Switch. Thus, a hybrid HSLAN like FDDI-II or a MAN like DQDB can be easily adapted to the Local Switch.

From the architectural point of view the system can be subdivided into subnetwork domains: each Local Switch and the attached terminals represent one type of subnetwork domain, and one separate domain can be identified for the backbone. Each domain has its own *subnetwork management*.

4. Applied Management Structure

As mentioned in Section 2, management for networks consisting of heterogeneous components is based on a unique logical master process, which contains the System Management Application Process (SMAP) intelligence. This *master entity (manager)* needs *agent* SMAPs on remote stations (see Fig. 3), to get access indirectly to the remote managed objects (MOs) and their attributes or - using OSI nomenclature - to the remote part of the Management Information Base (MIB).

The manager SMAP can initiate actions, to be performed independently by an agent. However, these actions are exactly predefined and fixed parts of the agent's MOs. Thus all details of every component, possibly connected to the network sometimes, must be well known by the master SMAP. Getting all this knowledge during the development phase of new components seems to be a rather difficult task in real world environments. The integration of new and unknown components into an existing system leads to an huge modification of the management database structure. (It has to be reminded here, that until now, only the primitives and protocols to exchange management data has been standardized /5/ and not the form, number, name and content of attributes!)

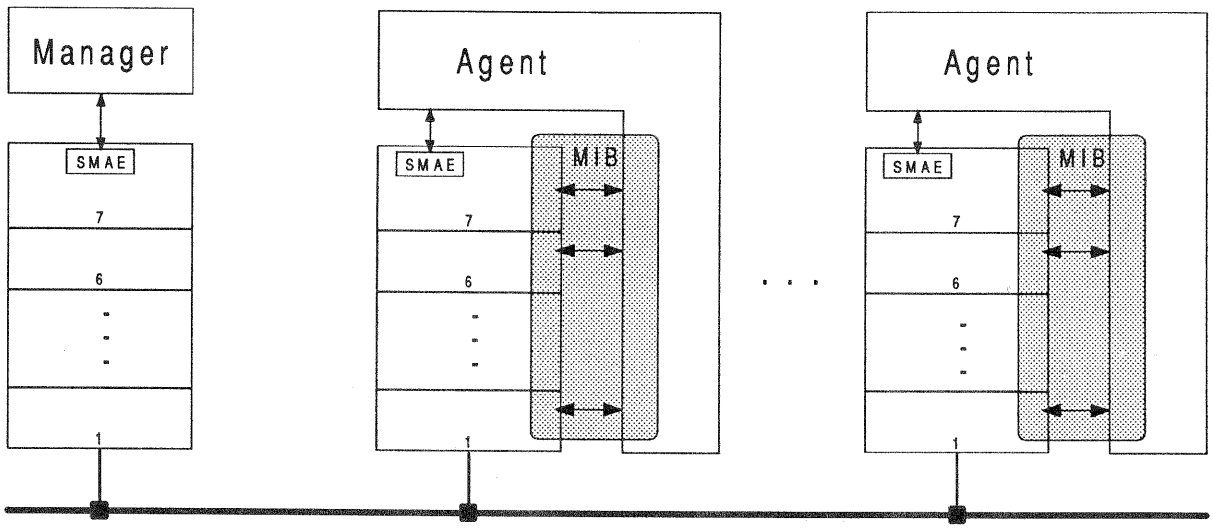

Figure 3: Master - Agent Relationship

Obviously this manager to agent model results in a large data volume to and from the manager and requires enormous processing power as well as communication recourses.

The drawback of this OSI client server structure is the inefficient usage of hierarchies, which are implicit available in distributed systems. Hierarchy can for example easily be determined, if the system contains more than one transmission medium, and additionally the transmission speed, traffic characteristics and/or distances between communication partners on these media are different. Our previously introduced system clearly contains such implicit hierarchy

The obvious solution, to install an own intelligent manager for every subnetwork domain is misleading because of two reasons:

First there is no manager-to-manager communication defined or standardized by ISO yet, and second a distributed system requires - additionally to the management of each subnetwork domain - some overall system management and control functions like alternative routing in case of subnetwork failures or user authorization. A management process is needed, which handles and extracts the information of each individual subnetwork manager.

As pointed out a decentralized and hierarchical structure of the management in respect of associating management functions and subnetwork domains seems to be the best solution for a distributed system.

The global resulting management structure is shown in Fig. 4 and consists of two subnetwork management types or domains: one is the nodal subnetwork domain and the other is the backbone subnetwork domain. The backbone subnetwork management domain shall cover all aspects which are only relevant for managing the backbone; thus, changing the backbone, only the backbone management domain must be changed. This structured approach also provides flexibility and adaptability for the management tasks of the whole system concept.

Obviously for the Broadband-ISPBX three layers of management hierarchy can be identified :

- Every system component - furthermore called *unit* - contains a local management directly responsible for its correct function (*Unit Management*).
- All monitor and control functions must be addressable for a logical higher management function. That next management level is responsible only for one subnetwork (*Subnetwork Management*).
- A network management coordinates the work of the different subnetwork managements (*Network Management*).

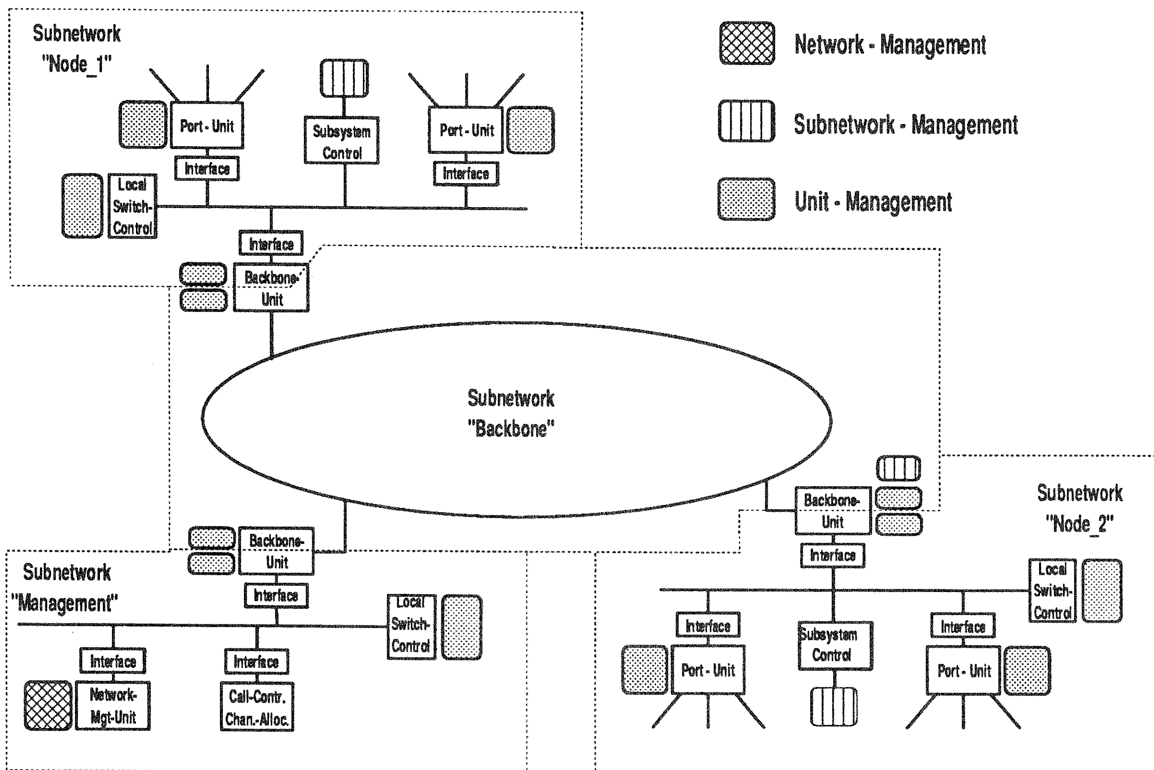

Figure 4: Management Model for the System

In Fig. 4 the different levels of management are drawn with different shadings. Each management block represents a software process which runs on the hardware components closed to it. The unit related management is dedicated to its unit, because it acts as an interface between the unit specific hardware and the subnetwork management.

The subnetwork managements should run inside their subnetwork to enable an autonomous operability of that subnetwork, but external locations are possible in principle (see the subnetwork "Management" in Fig. 4). The overall network management can be located anywhere in the system, but will be implemented in a distributed manner to increase fault tolerance.

As shown in Fig. 4, the backbone units contain two kinds of unit concerned management. One is responsible for the backbone side of that unit and is an agent of the backbone subnetwork management, the other part is Local Switch related and belongs logically to the subnetwork of the attached Local Switch (node subnetwork management).

5. Implementation Aspects

In opposite to Fig. 4 now the structure of the management in sense of hierarchical and logical communication relations is depicted (see Fig. 5).

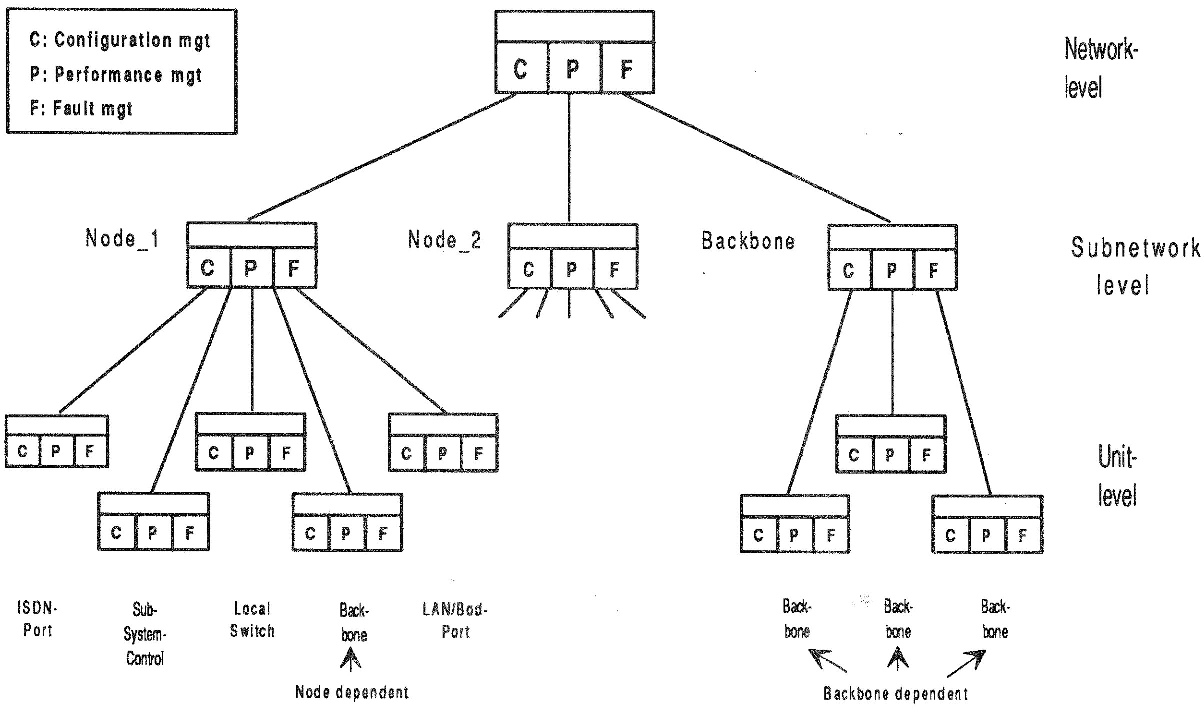

Figure 5: Logical Management Hierarchy

It is very important to understand, that the edges in Fig. 5 only represent *logical* communication links and do not represent physical connections between the management processes. Actually the edge between a subnetwork management and the network management can physically nearly cover the whole system.

To increase the flexibility, e.g., to enable the above mentioned removing of the whole backbone subnetwork, and also to reduce complexity communication restrictions have been defined. Only communication relations with exactly one level of hierarchy between the sending and receiving management entity are allowed. This implies two important cases:

1. No direct communication between the highest (network) hierarchy level and the lowest (unit) level is allowed.
2. A communication between management entities of the same level also is not permitted.

These types of communication have to be performed indirectly, if required at all. The disadvantage of an intermediate entity in that cases is overwhelmed by the possibility of hiding implementation details of underlying instances for not directly involved processes (black-box principle). Especially in a Broadband-ISPBX suitable for evolution to future communication services the exchange of parts of the system is extremely valuable due to the local dependencies between system elements.

The well known structure of the distributed communication system furthermore can be used to reduce the huge ISO overhead:

The higher ISO-layers at the moment are empty, because the applications and the architectural interfaces of the port units are known. As a result management communication can be done connectionless directly on top of the network layer.

The handling of the *two* ISO identification trees - *containment tree, registration tree* - can be simplified by using the system hierarchy. The resulting unique identification tree for all managed objects is shown in Fig. 6. The object classes of the ISO registration tree are represented by the *Type*-levels (Root, SN-type, Unit-type) and of course partially by the two lowest levels, which directly

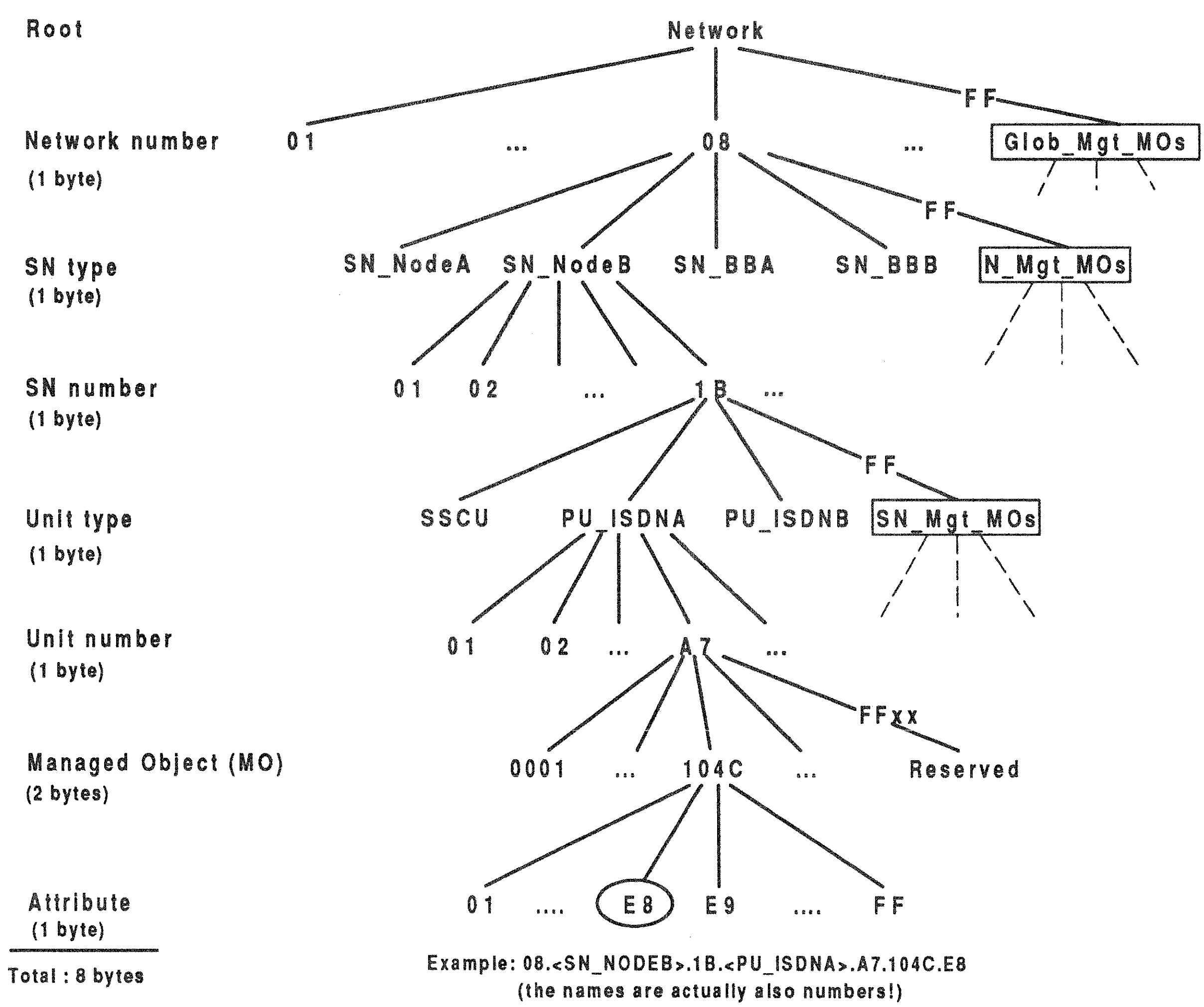

Figure 6: Management Identification Tree

address managed objects and attributes. The actual instances of managed object classes, i.e., the information out of the ISO containment tree, are located on the *Number*-levels (Network number, SN number and Unit number) and again also partially on the two lower levels. It has to be mentioned, that the type-levels are fixed at system set-up, however, the number levels are build-up and maintained dynamically during operation to support the request for a real dynamically changeable system!

With a relation of that identification tree to addressable processes inside the system every managed object can be addressed.

At this stage not all 5 functional areas covered by the ISO documents /4/, /5/ have been considered. The management *applications* to support accounting and security aspects, which are significant for the system provider will be considered in the next step. However, the underlying communication principles and the necessary attribute inclusions are also fixed for these two functional areas yet.

Following an overview about the main management applications out of the considered functional areas configuration, performance and fault management is given.

The most important task of the *configuration management* is the controlled initialization of the whole system after power-up. This is difficult, because

- the needed software is not resident available in each unit
- backing store facilities are not available at every subnetwork (in the worst case only one backing store unit is available)
- the system configuration need not to be fixed, thus no predefined configuration list will exists
- the sequence of being switched on also is arbitrarily
- each unit only knows its address, but nothing about its location in the whole system.

The initialization is done hierarchically in a bottom-up fashion, i.e., the units announce themselves to the own subnetwork management, which thereafter announces its availability to the network management. The information about the system configuration finally is distributed top-down back from network management to the subnetwork managements and from there to the unit managements.

After having reached full operability configuration management has to offer access to a complete map of the whole system. This *system map* obviously has to be as actual as possible. Hence, a permanent updating and maintenance is required to cope with possible failures and/or reconfigurations. The configuration management itself uses the system and management hierarchy for that system map by distributed handling of decentralized subnetwork maps and unit internal tables.

Performance management contains applications to evaluate and optimize the system's actual Quality of Service (QoS). Typical parameters for QoS evaluation are packet throughput, end-to-end delay, loss and error probabilities for packet switched traffic; call set-up and -release times and blocking probabilities for circuit switched traffic. To tune system performance setting of protocol parameters and administrating the available bandwidth resources are adequate mechanisms. A second task which permanently monitors the performance relevant attributes, is used to make long term statistics. Overload situations and/or weak points in the system also can be detected by the performance management.

Fault management generally has to detect and localize malfunctioning system parts and ideally also has to repair them. However, making a good error diagnosis with correlation of different fault symptoms is a very complex task on which lots of research is currently performed /7/. The *active* repair is even more difficult. As a result we implement the detection of faults, which is the prerequisite for every fault management. Sophisticated fault models and scenarios therefore had to be developed first.

According to the system hierarchy, prefiltering mechanisms have been introduced to hide underlying details. Units classify their internal state into one of three overall states: green, yellow and red. The subnetworks are actively informed using management event reports about state changes and have the possibility to inquire additional information if wanted. The same mechanisms are provided between subnetwork and network management. To cope with severe errors, which disable the communication, a periodical polling of the underlying entities also has been implemented.

Finally it has to be mentioned, that just assuring the communication between distributed management entities and diverse system processes is another important issue besides the functional areas.

6. Conclusion and Outlook

Distributed systems need an distributed management concept to fulfil their requirements efficiently. The proposed Broadband-ISPBX consists of a hierarchical distributed management approach. Reasons to extend the ISO management framework for distributed systems are discussed in this paper and some implementation aspects applied to the decentralized architecture are presented. A prototype implementation of the whole system including the aspects of the management is under work within an ESPRIT Project (see /2/).

Further activities will be done towards higher bandwidth and increased fault tolerance. From the management point of view, more sophisticated fault diagnosis is required to guide the system operator. The usage of expert systems in conjunction with enhanced fault models and artificial intelligence is the aim. This enables the system provider to install remote service diagnosis for all delivered systems from his maintenance centre, which reduces the overall maintenance costs of systems.

Glossary

ATM:	Asynchronous Transfer Mode
DAMS:	Dynamically Adaptable Multiservice System
dOS:	distributed (real-time and portable) Operating System
DQDB:	Distributed Queue Dual Bus
FDDI:	Fiber Distributed Data Interface

ISDN:	Integrated Services Digital Network
ISO:	International Standardization Organisation
(HS-)LAN:	(High Speed) Local Area Network
LE:	Layer Entity
LME:	Layer Management Entity
MAN:	Metropolitan Area Network
MIB:	Management Information Base
MO:	Managed Object
OSI:	Open System Interconnection
(IS-)PBX:	(Integrated Services) Private Branch eXchange
POT:	Plain Old Telephone
QoS:	Quality of Service
SII:	Standard Internal Interface
SMAE:	System Management Application Entity
SMAP:	System Management Application Process
SNMP:	Simple Network Management Protocol

References

/1/ Casel, L.N; Partridge, C; Westcott, J; *Network Management Architectures and Protocols: Problems and Approaches*, IEEE JSAC, Vol. 7, No. 7, 1989

/2/ Esprit Project 2146 - Dynamically Adaptable Multiservice System (DAMS)

/3/ Gavi, L; Vercelli, R.; Perretti, E; Ciccardi, A; Roffinella, D; *Architectural and Management Issues for Metropolitan Area Networks*; Proceedings EFOC/LAN 90, Munich, 1990, pp. 270 - 274

/4/ ISO 7498-4; Information Processing Systems Basic Reference Model - Part 4: Management Framework

/5/ ISO 9595-2; Management Service Definition - Part 2: Common Management Information Service (CMIS)

/6/ A Simple Network Management Protocol (SNMP), Internet RFC 1098

/7/ Schröder J., Schödl W.; *A Modular Knowledge Base for Local Area Network Diagnosis*, To appear in Proceedings of the Second International Symposium on Integrated Management, Washington D.C., April 1991.