

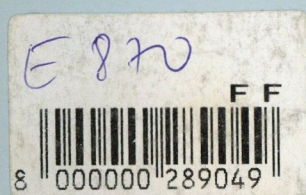
OT1
JOURNAL ON

COMMUNICATIONS

XLVIII. ÉVFOLYAM

MARCH 1997

NETWORK MANAGEMENT



Editorial	U. Schaumann	1
Introduction to network management	B. Frohnhoff and K.-P. Zeffler	2
PLASMA — an integrated tool for network traffic management in ATM/IP-based networks	M. Boda, Zs. Haraszti and A. Oláh	9
GSM network management	I. Maradi	15
Opening up network management	A. Bujara	21
MXP-2000: an accurate realization of the TMN concept	I. Gálfi and I. Kerecsen	24
Network management at MATÁV	R. Anderson and J. Wiener	28

Products — Services

PROTOS network management system at Deutsche Telekom	Deutsche Telekom	35
--	------------------	----

JOURNAL ON COMMUNICATIONS

A PUBLICATION OF THE SCIENTIFIC SOCIETY FOR TELECOMMUNICATIONS, HUNGARY

Editor in chief

A. BARANYI

Senior editors

GY. BATTISTIG

T. KORMÁNY

G. PRÓNAY

I. SCHMIDEG

A. SOMOGYI

Editors

I. BARTOLITS

J. ELEKES

I. KÁSA

O. KOVÁCS

J. OROSZ

M. ZÁKONYI

N. WILK

Editorial assistant

K. LESNYIK

K. GERENCSÉR

Editorial board

GY. TÓFALVI

chairman

T. BERCELI

B. FRAJKA

I. FRIGYES

G. GORDOS

É. GÖDÖR

I. MOJZES

L. PAP

GY. SALLAI

P. TÖLÖSI

Editorial office

Budapest I. Ostrom u. 23-25.

H-1525 Budapest. P.O. Box 75.

Phone: (361) 175-7777, (361) 201-7471

Fax: (361) 156-5520, (361) 201-7471

Subscription rates

Hungarian subscribers

1 year, 12 issues 8100 HUF, single copies 700 HUF

Hungarian individual subscribers

1 year, 12 issues 1000 HUF, single copies 120 HUF

Foreign subscribers

12 issues 150 USD, 6 English issues 90 USD, single copies 24 USD

Transfer should be made to the Hungarian Foreign Trade Bank,

Budapest, H-1821, A/C No. MKKB 203-21411

JOURNAL ON COMMUNICATIONS is published monthly, alternately in English and Hungarian by TYPOTeX Ltd. H-1015 Bp. Retek u. 33-35. Phone/Fax: (361) 115-1759. Publisher: Zsuzsa Votisky. Type-setting by TYPOTeX Ltd. Printed by Dabasi Jegyzetnyomda, Dabas, Hungary HUISSN 0866-5583

SPONSORED BY



SIEMENS

Siemens Telefongyár Kft

ERICSSON



NOKIA



MOTOROLA



Communication Authority, Hungary



FOUNDATION FOR THE
"DEVELOPMENT
OF CONSTRUCTION"



EDITORIAL

Changes — both in technology and regulation — have accelerated lately. Competition is growing steadily in business communications and mobile telecommunications in most countries. While the European Union will first see competition in conventional telephone services in 1998, competition is already present in many other countries.

In this competition the devices used are increasingly demanded to have control, supervision and maintenance features in addition to the regular functions.

The national standardization organizations are already drafting the appropriate recommendations and standards that basically originate from the ITU M3010 recommendation. This is the basic recommendation describing the TMN (Telecommunications Management Network) that underlies many additional recommendations, studies and standards not only in the ITU but also in the ETSI, ERUESCOM and other organizations.

If everything is so well regulated, why cannot the systems operating on those principles be generally accessed? The answer may be approached from two sides: from the side of telecommunications manufacturers and from the side of information technology suppliers.

Telecom suppliers can basically supply effective managing devices for their own equipment only.

The suppliers see several advantages to this approach. For example, the interface between the managing device and the managed device does not need to be redesigned to comply with the appropriate standard. There are large performance PCs and workstations on the market with which each supplier can sell his own managing system for his own device. These devices do not lend themselves readily to integration with other systems, or there are very few examples for such integration.

Although some telecommunications suppliers have made steps in that direction, these only amounted to TMN-like Q3-like results. This helps to keep up a situation where the buyer will also buy the managing system from them.

The other direction is that of information technology (computer and workstation) suppliers, manufacturers.

These are more likely to use open systems. Several IT suppliers have TMN model-based platform, but even these lack a fully-fledged TMN solution. Nevertheless, they stand closer to one. The access modules (AM) installed between the managing and the managed devices and the mediating devices (MD) allow for the use of solutions that follow most the principles of the TMN model.

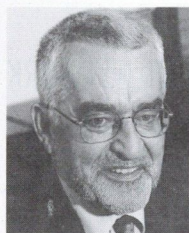
The first breakthrough in this area came with the appearance of GSM service providers because these were faced with international competition (because of roaming) already at the start. These platforms are the products of some sort of convergence since large computer and workstation suppliers integrated in the TMN platforms those ready panels that they had developed for managing computer networks (e.g. archivation, graphic display, access authorization, etc.).

We are at this point at the moment: we have recommendations, standards and studies for the operation and IT suppliers are ready to offer solutions that integrate several systems. Present and future suppliers are showing growing demand for the use of such devices, and telecom equipment manufacturers are also poised for a change. Essentially, the latter two players will say the final word in the respect of new solutions that integrate several systems and work on TMN principles.

Deregulation in 1998 will give a great uplift to this process. Traditional supplier-service provider relations will emerge in Europe, with one supplier having considerable market with one or two service providers. It cannot be predicted at this point whether these traditional relations will boost or reduce the competitiveness of a service provider.

A future decision depends on support of competitiveness when a telecommunications service provider will chose an information technology supplier instead of a telecom supplier for the supply of managing systems. Today the information technology suppliers have advantages in this field and some big service provider decision will influence it very much.

U. SCHAUMANN



Ulrich Schaumann graduated in 1967 as a Dipl.-Ing. in telecomm;unications at the Technical University, Munich. From 1967 to 1977 he held several leading positions within Deutsche Bundespost Telekom, in the field of switching, transmission and outside plants. From 1977, he was head of a project team in Teheran, Iran, for the DBP Telekom Development Project. In 1979 he became Head of the Telecommunications Office in Schwabisch-Hall, Germany. 1981–1983 he worked as Head of a project team in Cairo, Egypt, for the DBP Telekom Expansion Project. From 1985 he was Head of the DBP Telekom section in the Regional directorate of Koblenz. In 1990–1993 he worked as Vice President in the Federal Office for Post and Telecommunications and Head of DBP Telekom Telecommunications Office in Heilbronn. In December 1993 he was appointed Chief Technical Officer (CTO) of MATÁV in Budapest.



INTRODUCTION TO NETWORK MANAGEMENT

B. FROHNHOFF and K.-P. ZEFFLER

DEUTSCHE TELEKOM AG, TECHNOLOGIEZENTRUM DARMSTADT
RESEARCH GROUP "FUNCTIONAL ASPECTS OF NETWORKS"
POSTFACH 100003, 64276 DARMSTADT, GERMANY
E-MAIL: FROHNHOFF@TZD.TELEKOM.DE, ZEFFLER@TZD.TELEKOM.DE

To provide network services and additional services based on such networks, it is necessary to perform many coordinated operations in the network. In most cases, the equipment required for such provision is geographically distributed. The systems are produced by different manufacturers and have a variety of different interfaces. Moreover, as the number of customers demanding for international services is increasing quickly, it must be possible to provide and operate such services across boundaries between different operators. On the other hand, in the highly competitive telecommunications market the "time to market" period as well as the quality and security of the offered services are decisive for satisfying customers needs. Management systems for automating and optimizing the use of technical and human resources must be adapted to these important criteria. The economic success of communication providers depends critically on proper choice of a suitable hardware and software architecture including internal and external interfaces. In addition, the proper adaptation to customer and operational requirements is extremely important.

1. PRELIMINARIES

The basic concepts of the management of public networks are described in various ITU-T recommendations (International Telecommunication Union — Telecommunication Standardization). ITU-T Recommendation M.3010 [1] is the most important one. It defines the term "TMN" (Telecommunications Management Network) and describes the TMN architecture for structuring network management systems. It also establishes the most important methods for defining specifications in the TMN context.

This paper is organized as follows: Chapter 2 discusses the contents of the TMN architecture in detail. Chapter 3 focuses on TMN platform concepts for reducing the effort to implement management systems. Chapter 4 presents some alternative architectures for structuring management systems. Chapter 5 deals with aspects of interworking between management systems of different (network) operators.

2. TELECOMMUNICATIONS MANAGEMENT NETWORK

ITU-T Recommendation M.3010 defines the general architectural requirements for a Telecommunications Management Network (TMN) to support operators or providers in managing telecommunication networks and services, especially with regard to

- planning,
- provision,
- installation,
- maintenance,
- operation and
- administration.

This list includes all areas that could arise in the operation of telecommunications equipment or services. It should be noted that the recommendation's focus is on *architecture*. In other words, whenever "TMNs" are discussed within the context of network management, the term always refers to a specific architecture specified in Recommendation M.3010. Other standardization bodies have specified other architectures — either divergent or supplementary ones — for managing telecommunications networks. These architectures, however, have not become as widely accepted as TMN is.

It should also be noted, in general, that TMN is technology-independent. It does not require a specific technology in the transmission network or in the switched network. Nonetheless, it is obvious that management systems for automatic operation of extremely flexible networks — as implemented with ATM technology — must offer significantly more functionality than the management systems for rigid networks that must be manually reconfigured. On the other hand, only such flexible networks represent the environment where automatic management systems can prove their full effectiveness. In this environment, all potential operational and economic merits of automatic management systems can be exploited by the operator and all additional potential advantages of flexible services can be provided to the customer.

2.1. Functional areas of the TMN

The above TMN application areas can be divided into 5 different functional areas that are often referred to in combination with the abbreviation "FCAPS" [2]:

- **Fault Management:** comprises detection, isolation and correction of abnormalities in the operation of network elements or of parts of a network. It can include to carry out sequences of diagnostic tests.
- **Configuration Management:** comprises initialization, putting into operation, continuous operation and termination of communications services (for example, reservation and release of virtual paths in the ATM network, placing new cross connects into the network, etc.).
- **Accounting Management:** includes all tasks that arise in connection with accounting for services used.
- **Performance Management:** includes the collection and evaluation of data that provides information about the efficiency and performance of network elements, and of parts of the network and of services; it also refers to measures taken to optimize network performance.
- **Security Management:** provides the applications with the support they require when security mechanisms are used. Such support includes recording and displaying events relevant to security (for example, unauthorized access to protected files), administration of electronic

keys and installation and modification or removal of security measures in applications.

Note: The *execution* of security functionality (for example, password query or access denial) must be accomplished by the applications or the hardware *themselves* and is not part of security management.

Data and information that are exchanged and processed within the TMN may belong to several of these areas.

2.2. Key technologies of the TMN

The TMN according to Recommendation M.3010 employs a range of key technologies that come from the areas of data technology and protocol technology. These key technologies include

- systematic use of open systems,
- global use of a derivative of the classical client/server architecture (in the TMN: the "manager-agent" concept),
- general use of object-oriented techniques in specifications,
- extensive use of formal languages for specifications (especially ASN.1 and GDMO; an explanation is provided below) of interfaces between architectural components of the TMN.

These key technologies reflect the current technical development in the above-mentioned areas of protocol technology and data technology.

The use of open systems technology at least partly fulfils the demand for independence from proprietary standards. The TMN is based upon the OSI (Open Systems Interconnection) Standards developed by the International Standardization Organization (ISO). OSI takes an exclusively management-oriented perspective in considering aspects of interconnection of so-called "open systems" (it does not consider the transmission technology involved) and of communications between such systems. As a rule, a system consists of a number of distributed components: one or more computers, the pertinent software, peripherals, etc. The OSI Reference Model [3], Systems Management Model [4], Systems Management Functions [5] and five Management Functional Areas (FCAPS cf. section 2.1.) are of special significance with regard to the TMN.

Use of the manager-agent architecture permits flexible distribution of communication roles between applications running on distributed systems. In addition, the agent can respond to internal or external events by sending "notifications" spontaneously to the manager. This is to inform the manager about these events. The manager-agent concept is a component of the OSI systems management model.

By using object-oriented specification techniques it is possible to treat data and relevant access functions as a unit and to handle them jointly. The most important aim of this approach is to be able to adopt, modify or expand existing specifications for other purposes. The starting point for object-oriented considerations within the TMN are the objects specified in X.721 [6] and M.3100 [7], objects from which all specific object declarations should be derived.

ASN.1 (Abstract Syntax Notation 1 [8]) permits to specify data and protocol elements independently of systems and programming languages. By using all the sophisticated

possibilities provided by this language standard (including, especially, use of the sophisticated redefinition possibilities of ASN "macro technology") a derived language was established, now known under the name "GDMO" (Guidelines for the Definition of Managed Objects [9]). As this name indicates, it is used for specification of objects in the TMN.

2.3. Key definitions for the TMN

In this section, we define several key terms that are of importance in the context of TMNs.

Network management system:

A network management system provides technical support to the network operator in his tasks of planning, providing, installing, maintaining, operating and administrating telecommunications networks and services.

Operating system:

The operating system defines the control logic of a management system. The operating system collects, processes and, in some cases, stores data from the telecommunications network; it uses this data to control the network (for example, to bypass faulty communication links, to initiate repair of a network element, to optimize utilization of the capacity of individual elements, etc.). The fact that the term operating system is also used in the context of computers in general (the operating systems UNIX and MS Windows are typical examples) often causes confusions.

Resource:

A resource is either part of a system monitored by a network management system (for example, part of an exchange or of transmission equipment) or an element that supports certain management tasks (for example, the distribution or recording of messages).

Network element:

A device that is part of a telecommunications network (for example, a cross connect or a multiplexer) is termed a "network element" if it is monitored by a network management system. Consequently, a network element is a resource; a resource need not necessarily be a network element, however.

Managed object:

A managed object is the abstraction of a resource; it displays the characteristics of a resource in a form suitable for the network management system. Furthermore, a managed object is a realisation (instance) of a managed object class.

Managed object class:

A managed object class is a data declaration made to implement managed objects with the same characteristics. It is defined in terms of:

- *attributes*, which make the internal status of an object externally visible and which can be influenced by means of appropriate operations,
- *operations*, which can be applied to managed objects (in particular, to its attributes),
- *behaviour* of the managed object that can occur as a response to internal and external events and as the answer to operations,
- *notifications*, which the managed object can send out spontaneously.

Additionally, in a managed object class definition, inter-object-relationships (for example inheritance or aggregation relationships) are specified.

Information model:

An information model contains managed object classes and the protocol functions with which the managed object classes can be addressed, via interfaces. Model types include so-called "generic" information models (cf. [6] and [7]) and information models tailored to certain technologies — for example, for SDH or ATM technology, for the management of IN architecture components, etc. Through restriction to a specific information model, the TMN — which is fundamentally technology-independent — can be tailored to a certain given technology.

2.4. TMN architecture and interfaces

Management systems can vary greatly in their size and complexity. Consequently, the TMN architecture has to reflect those scalability aspects. A TMN can encompass one or more operating systems; one or more workstations, which give users access to management information; monitored and controlled network elements; and a Data Communication Network (DCN), which transports management information between the various components of the TMN (cf. Fig. 1). It should be noted that only those parts of a network element belong to the TMN that are actually controlled by the management system. As indicated on the left side of Fig. 1, a TMN can also include private equipment (such as PABXs or components of a private data network).

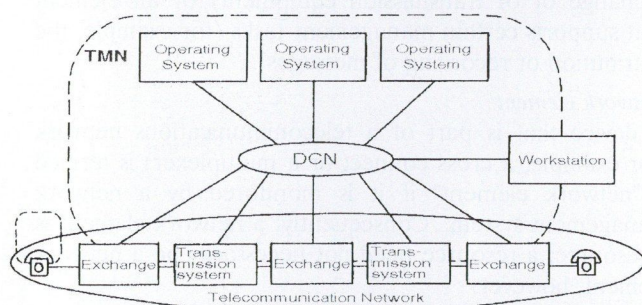


Fig. 1. General relationship between a TMN and a telecommunications network

In general, the DCN is not implemented as separate, isolated communication network; it may also be implemented with the help of parts of the controlled telecommunications network. The elements that are managed and controlled by the TMN include, of course, the components of the TMN itself (operating system, data communication network, human machine interface etc.).

Recommendation M.3010 includes three different perspectives of the general architecture of the TMN, each of which was considered separately in TMN standardization:

- TMN physical architecture,
- TMN information architecture,
- TMN functional architecture.

The present article does not include a discussion of the TMN functional architecture. That architecture provides an abstract description of the function blocks of which the components of the physical architecture consist.

2.4.1. TMN Physical Architecture

The TMN physical architecture consists of a number of components and a number of interfaces that separate these components. Fig. 2 shows an example of the TMN physical architecture.

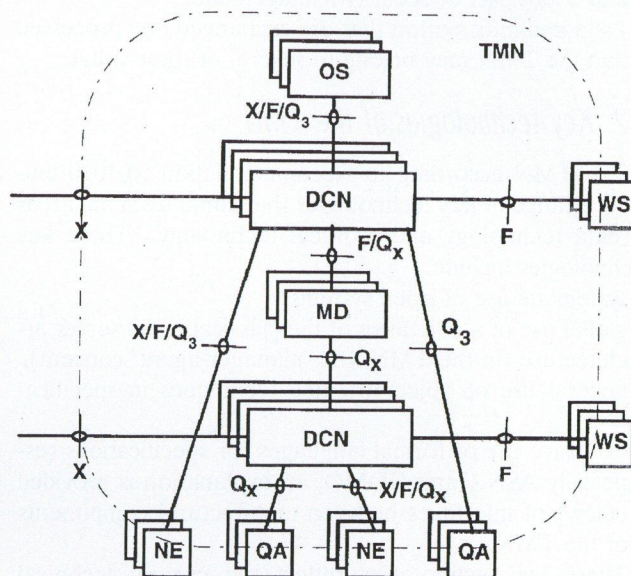


Fig. 2. TMN physical architecture

The components of the TMN physical architecture are as follows:

- **Data Communication Network (DCN):** The DCN is responsible for transmitting information between the various components of the architecture. It provides the transport mechanism for the exchange of management operations between managers and agents, and it can consist of a number of interconnected subnetworks (for example, a backbone network and linked local access networks). The various networks can be of different types.
- **Operating System (OS):** The operating systems are the heart of the TMN physical architecture. They process information from the telecommunications network in order to monitor and control that network.
- **Q Adaptor (QA):** The task of the Q adaptor is to connect network elements or operating systems with non-TMN compatible interfaces to the TMN, via a Q interface (syntactic translation of management information).
- **Network Element (NE):** Network elements are the components that must be monitored and controlled by the management system. Network elements carry out the actual tasks within a telecommunications network (for example, transmission of data via a physical circuit, switching of connections, etc.), including the functions with which these tasks are represented within the TMN. The first group of tasks is not part of the TMN, however. These parts of the network element lie outside of the TMN. A network element has one or more Q interfaces, and it may have F or even X interfaces if it provides operation system functionalities.
- **Mediation Device (MD):** Mediation devices ensure that information exchanged between Q adaptors and network elements, and between operating systems and

workstations respectively, is converted into the required form (semantic translation of management information). This function is of main significance, when components communicating with each other (for example a network element and an operating system) are referring to different information models. Mediation devices can store, adapt, filter and summarize information.

- *Workstation (WS)*: With the aid of the Workstation component, users can make inputs into the system and receive outputs from the system. Supporting functions at the interface to the user (for example, formatting of inputs and outputs, and graphic display of data) are part of the workstation component, but not of the TMN. The architecture features the following interfaces:
- *Q₃ Interface*: This is the interface between OS and MD, NE or QA; it provides full CMIP (Common Management Information Protocol [10]) functionality. If necessary, other protocols of the OSI layer 7 protocol family can be applied at this interface as well (for example, File Transfer, Access and Management (FTAM) [11]).
- *Q_x Interface*: This interface, in comparison with the Q₃ interface, has limited functionality (interface between MD and NE or QA).
- *F Interface*: It provides the interface between the management system and the user.
- *X Interface*: Connection of two OSs requires special information models and restrictions of permissible operations, as well as additional security functions — especially when systems of different operators are involved. In general, the X interface is based on the same protocol structures as the Q₃ interface.

2.4.2. TMN Information Architecture

The TMN information architecture introduces the concepts of manager and agent, shared management knowl-

edge, management information base, and management domains.

As a rule, management of a telecommunications network is a distributed application when TMN standards are used. Interactions between elements of a distributed application always take place in form of an information exchange between a manager and an agent. Allocation of a manager or agent role always applies to a specific association and can thus be changed.

A *manager* (managing system in Fig. 3) is responsible for one or more management activities. It applies operations and inquiries to the managed objects in the agent and receives notifications from the agent.

An *agent* (managed system) carries out commands (operations) received from a manager and applies them to his managed objects; it also answers to commands (responses). Its tasks include data manipulations (requests) asked for by the manager. Such manipulations are also acknowledged if necessary. Independently of any queries, an agent can also send spontaneously messages to the manager (notification).

As indicated in Fig. 3, there is not necessarily a one-to-one relationship between Managed Objects (MOs) and resources controlled by the network management system (Managed Resource, MRs). For example, a resource can be represented by several MOs, or several resources can be represented by one MO. In addition, there exist managed objects that represent logical resources of the TMN, instead of physical resources of the telecommunications network. Resources (R) that are not represented by a managed object cannot be controlled by the management system.

The so-called *Management Information Base* (MIB) contains all the managed objects required for controlling a telecommunications network. It exists only in systems, however, that have the role of an agent (managed system).

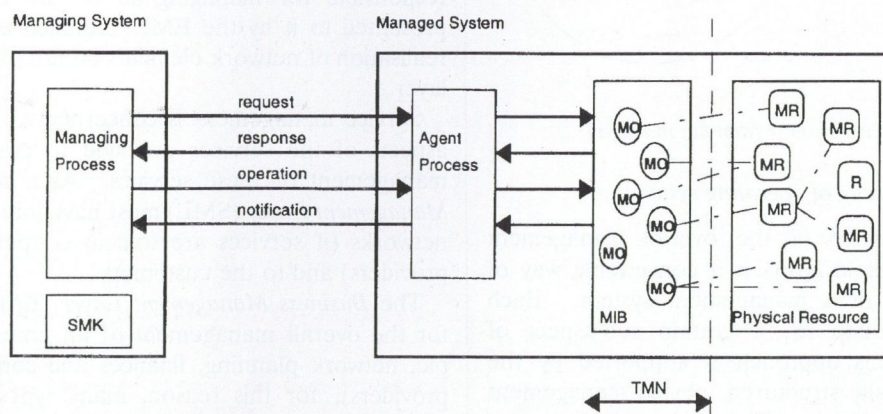


Fig. 3. Relationships between manager, agent and objects (according to Recommendation M.3010)

Typically, a manager will have relationships to several agents, and several agents will have relationships to one manager. An agent may refuse to execute an order issued by the manager, for example, if the order has been received from an unknown sender address.

As a rule, information exchange between manager and agent is carried out by the Common Management

Information Services (CMIS) and the pertinent protocol (CMIP). Since the protocol functions required to transmit one message are relatively extensive, and since the length of a message is limited, the FTAM protocol is used for transmission of large data volumes (for example, statistics regarding utilization of capacity).

When two architecture components communicate with

each other, they must have a common understanding of the significant TMN characteristics involved. Among these are supported protocols, services components (TMN Management Functions) and managed object classes, as well as realisations (instances) of managed objects classes present in the agent. They also include the manager's rights to access certain objects. This information, which must be known by both parties to a communication prior to an association, is known as *Shared Management Knowledge* (SMK).

Managed objects can be combined for different purposes (for example, for execution of certain security concepts) and in accordance with different perspectives (for example, as a function of certain management tasks, or in accordance with geographical, technical or organizational criteria). A group of managed objects, together with its manager, is referred to as a *Management Domain*.

Management domains can be either disjunct or overlapping; they can interact or contain other domains. Complex hierarchical structures can be built by nesting domains (cf. Fig. 4). Each domain can be viewed as a layer in such cases.

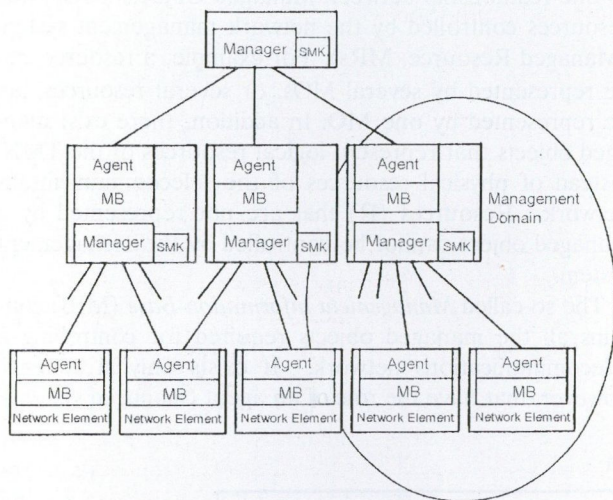


Fig. 4. Hierarchical systems (domain manager)

2.4.3. Functional hierarchy of operating systems

Hierarchical subdivision of the overall management functionality into multiple layers is a conceivable way of structuring the tasks of a management system. Each layer is then responsible for a certain sub-aspect of the overall task. This approach is supported by the concept of hierarchically structured, nested management domains as described above. The various layers, as a rule, are separated by means of Q_3 interfaces or q_3 reference points. A reference point separates two TMN function blocks (for example OSF and MF, for details see the description of the TMN functional architecture in M.3010) and — in contrast to TMN interfaces — must not necessarily be externally visible. Fig. 5 shows an example of a functional hierarchy of operating systems.

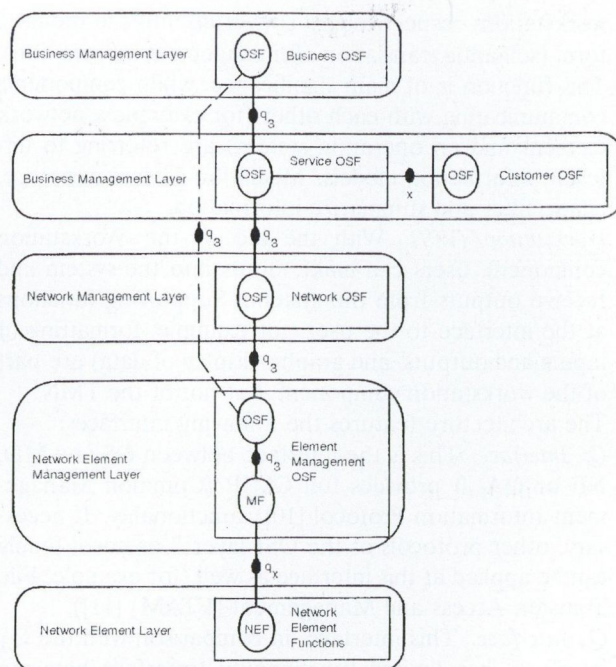


Fig. 5. Example of a functional hierarchy of operating systems
OSF: Operation Systems Function; MF: Mediation Function; NEF: Network Element Function

Operating systems that are assigned to the *Network Element Management Layer* (EML) control network elements on an individual basis. Each OS in this layer is responsible for a certain number of network elements. The EML abstracts the functions that are provided by the network element layer, in which the network elements to be managed by the OS are located.

The *Network Management Layer* (NML) has a general survey of the entire network; this enables it to perform its task of coordinating network-wide activities. It is responsible for managing all of the network elements presented to it by the EML. Detailed issues of technical realisation of network elements do not play any role in this layer.

Service management is concerned with the contractual aspects of the services provided to customers and with management of these services. As a result, the *Service Management Layer* (SML) must have interfaces to different networks (if services are sold in cooperation with other providers) and to the customers.

The *Business Management Layer* (BML) is responsible for the overall management of an enterprise (for example, network planning, finances and contracts with other providers); for this reason, many types of relationships with other network operators and services providers, and their management systems, are required. The main task implemented in this layer is to define aims, rather than to achieve them. This layer, therefore, is a sort of "strategic information system".

Current implementations of management systems cover the network element management layer, the network management layer, and the service management layer.

3. TMN PLATFORM

Standardization bodies that prepare recommendations and standards in the area of TMN (ITU-T, European Telecommunication Standards Institute (ETSI) and International Standardization Organization (ISO)), normally confine themselves to specifying the structure of management systems, as well as management services and subcomponents these services must provide. They do not supply specifications regarding the implementation of management systems.

Implementation of operating systems, mediation devices etc. is significantly influenced by current developments in the key technologies of the TMN (cf. section 2.2.). In addition, some initial experience in the implementation of systems which conform to the TMN architecture is now available. Needless to say, this experience will influence the refinement of TMN standards and the technologies used to implement management systems.

Due to the complexity of TMN protocols and TMN applications, specification and implementation of systems is a complex task. The concept of a "TMN platform" is becoming more and more accepted as a way of reducing the effort this task involves. A "TMN platform" is defined as the common computer architecture (including software) for all TMN tasks — the architecture upon which the management applications are based.

The aim is to extract from the applications any software components that can be jointly used by several applications and to provide these components to all applications as a basis ("platform"). This approach is seen as a way of avoiding duplication of work in specification and in implementation. In particular, having new applications build on software components that are largely already in operation, and thus are practically tested, is seen as a way of enhancing function security.

The following areas (no claim made to completeness) can currently be identified as main functions of a TMN platform:

- communications procedures as CMIP, FTAM and, possibly, TCP/IP,
- process management,
- directory functions for finding other processes,
- inter process communications and synchronization with other processes,
- transaction-oriented communications with other systems (which are not platform-like),
- interface to a graphic user interface ("Windows System"),
- general security functions (authorization to access functions, security logging etc., in cases where such functions cannot be implemented within the system to be protected),
- database functions (including data backup and, if possible, including access control in accordance with user profiles),
- print service, including services for logging functions,
- fault logging and fault diagnosis mechanisms (also for remote access if possible),
- operation & maintenance of the platform itself (also for remote access if possible),

- logical access to disk-storage media, disk drives and mass storage media (CD or magnetic tape/removable disks),
- generic management applications such as MIB or log file browsers.

Overall, then, this effort has to do with expansion of functions provided by standard operating systems (especially UNIX) and middleware products (for example, DCE [12] or CORBA [13] for implementation of distributed applications). The extent and contents of platforms must be dynamically defined: New requirements for applications can lead to expansions, and obsolete requirements result in removal of components from the platform. Not every implementation of a platform must comprise all areas. A platform upon which only one application runs, or just a few applications run, can do without providing all components. The "TMN platform" is thus more a generic model than a specific implementation.

4. ALTERNATIVE MANAGEMENT ARCHITECTURES

In addition to the TMN architecture described in the previous chapters, an architecture that has established itself in the area of management of public networks, there are other suitable architectures for structuring management systems. These are briefly presented in this section:

- *Proprietary architectures*: These are the basis for structuring older operation-support systems and management systems for closed "island networks". The functionality of older operation support systems is normally limited. It ranges from functions such as signalling a failure by an electrical alarm (for example, through closure of a potential-free contact) to remotely controlling transmission links or exchange systems via complex terminal procedures. A characteristic of modern proprietary management systems is that while they provide a large number of functions, they have no external interfaces, or only proprietary external interfaces.
- *Internet management architecture*: It has become established in the area of local and private networks. The prerequisite for use of this architecture is relatively low complexity of the network and the network elements involved. This architecture is based on the Simple Network Management Protocol (SNMP) [14], a rigid manager-agent concept, which has no hierarchy of operating systems, and on the definition of a Management Information Base (MIB). The latter of these does not have an object-oriented structure, however. Instead, it is a collection of simple data structures as integers and tables, for example.
- *Common Object Request Broker Architecture (CORBA)*: This architecture was originally intended only for the implementation of distributed object-oriented applications. Newer efforts are now aimed at using CORBA to manage and control computer networks and services within such networks.

5. INTERDOMAIN MANAGEMENT

In addition to technical problems posed by interaction of management systems, such as differences in the applied information models or incompatibilities resulting from different management architectures, another important issue

has to be considered. It has to do with cooperation between management systems belonging to different administrative domains. In this context, it makes no difference whether the domains, for example, belong to two operators of public networks or an operator of a public network and an operator of a private network. This kind of cooperation involves problems of economic competition and security. These non-technical considerations can even include issues of European competition law (Open Network Provision).

Consequently, operations aimed at directly controlling network elements of an other network operator will be completely blocked or at least subjected to extremely restrictive control. Only automatic *inquiries* to the management system of the other operator will be allowed. Execution or denial of these inquiries will be performed under the control and responsibility of the latter. Furthermore, if the two operators are competitors, a restrictive approach will surely be taken to avoid disclosure of internal information about network status to the "other parties" management systems. For example, data regarding bottlenecks in the network of an other operator can be derived from

statistics about the utilization of capacities of nodes and connections circuits. A competitor could find it useful to make investments that would eliminate such bottlenecks, thereby enabling him to attract customers.

Thus, it is only logical to restrict information exchange to an absolute minimum. But this interest conflicts with the interests of customers who aim to get end-to-end services independently of the network operators involved. Customers will not be willing to give up their demand for end-to-end services and features simply because the involved operators have not been able to agree on the necessary information exchange. In cases of such non-agreement, customers will switch to other providers that can deliver the desired services.

Cooperation between network operators can largely be reduced, if necessary, to defining a commonly agreed information model. The basic rule for the design of this information model at the X interface can be reduced to the following formula: "As little information as possible, but as much information as necessary". In the final analysis, the extent of information to be exchanged via this interface will be determined by the customers.

REFERENCES

- [1] *Principles for a Telecommunications Management Network*, ITU-T Recommendation M.3010, Geneva 1992.
- [2] *Data Communication Networks — Management Framework Definition for Open Systems Interconnection (OSI) for ITU-T Applications*, ITU-T Recommendation X.700, Geneva 1992.
- [3] *Reference Model of Open Systems Interconnection for ITU-T Applications*, ITU-T Recommendation X.200, Geneva 1994.
- [4] *Information Technology — Open Systems Interconnection — Systems Management Overview*, ITU-T Recommendation X.701, Geneva 1992.
- [5] *OSI Systems Management Functions*, ITU-T Recommendations X.730-X.750, Geneva 1991-1994.
- [6] *Information Technology — Open Systems Interconnection — Structure of Management Informations: Definition of Management Information*, ITU-T Recommendation X.721, Geneva 1992.
- [7] *Generic Network Information Model*, ITU-T Recommendation M.3100, Geneva 1992.
- [8] *Specification of Abstract Syntax Notation One (ASN.1)*, ITU-T Recommendation X.208, Draft Melbourne 1988.
- [9] *Information Technology — Open Systems Interconnection — Structure of Management Informations: Guidelines for the Definition of Managed Objects*, ITU-T Recommendation X.722, Geneva 1992.
- [10] *Data Communication Networks: Open Systems Interconnection (OSI); Management — Management Information Service Definition*, ITU-T Recommendation X.710, Geneva 1991.
- [11] *Data Communication Networks: Open Systems Interconnection (OSI); Management — Common Management Information Protocol Specification for ITU-T Applications*, ITU-T Recommendation X.711, Geneva 1991.
- [12] *Information Processing Systems — Open Systems Interconnection — File Transfer, Access and Management (FTAM)*, ISO/IEC 8571 Parts 1-4, 1988.
- [13] *Distributed Communication Environment (DCE)*, Revision 1.0, Open Software Foundation (OSF), 11 Cambridge Center, Cambridge, MA 02142, USA.
- [14] *Common Object Request Broker Architecture and Specification*, Revision 2.0 July 1995, Object Management Group (OMG), Headquarters at 492 Old Connecticut Path, Framingham, MA 01701, USA.
- [15] *IAB, RFC 1157 Simple Network Management Protocol (SNMP)*, IAB, RFC 1905 Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2).



Birgit Frohnhoff received her diploma in electrical engineering with emphasis on communication systems from the Technical University of Aachen in 1993. Then she joined the research group of Mr. Zeffler. She is the head of an ATM TMN laboratory which is involved in several national and international TMN research projects. Her special interest is in formalizing the TMN interface description language GDMO and in interdomain management.



Klaus-Peter Zeffler got his Dipl.-Ing. from the Telecommunications Faculty at the Technical University of Hannover in 1982. He begun at this location as research assistant and continued as associate professor with emphasis on switching systems, ISDN protocols and operation support systems. In 1993, he joined the technology center of Deutsche Telekom AG. Now he is head of research group "functional aspects of networks", which is involved in Intelligent Networks including TINA and in TMN platforms, architecture, and development systems.

PLASMA – AN INTEGRATED TOOL FOR NETWORK TRAFFIC MANAGEMENT IN ATM/IP-BASED NETWORKS

M. BODA, ZS. HARASZTI, and A. OLÁH

ERICSSON KFT.
TRAFFIC ANALYSIS AND NETWORK PERFORMANCE LAB.
P.O.B. 154, H-1475, BUDAPEST, HUNGARY
PHONE: +36 1 265 7219, FAX: +36 1 262 7861; E-MAIL: ETHMBA,ETHZHI,ETHAOH@ARISTOTELETH.ERICSSON.SE

The dynamically changing telecommunications scene makes the management of modern networks more complex than ever. Performance or traffic management receives a special emphasis as real-time multimedia services with strict quality requirements are introduced. The paper proposes an architecture which is based on the integration of analytical performance evaluation methods, optimization algorithms, and a simulator in order to create powerful decision support system for traffic management. The design and implementation of a tool based on this idea is described and it is shown how such a tool can be applied to solve traffic management problems in different networks including public-switched telephony, ATM and IP-based networks.

1. INTRODUCTION

Ideally, the life-cycle of telecommunication networks can be divided into the following non-overlapping phases:

- *Specification phase:* The expected characteristics of the network are formulated. This involves the amount of traffic that the network is supposed to carry as well as the grade and quality of the service that should be guaranteed.
- *Design phase:* Based on the specification and on other external constraints the network is designed by skilled network designers using their analytical and heuristic experience. The plan contains the arrangement of both physical and logical resources and all the rules that control the access to those resources.
- *Implementation phase:* The network is implemented according to the plan, and then its operation is checked. Tests and measurements are made to compare the characteristics of the implementation with the specifications. Some tuning may be necessary at this point.
- *Operational phase:* Several tasks have to be performed while the network is in operation. These include adding/removing users, collecting and processing accounting information, and maintenance of equipment. As information about the offered load and the performance characteristics of the network becomes available, it is usually necessary to adjust configurable parameters.

The above process works very well as long as the requirements are well predictable and change relatively slowly. Unfortunately, this is not the case in telecommunication networks of today. Services that were not foreseen a few months ago are introduced today. For example, the fast growth of the Internet is driving operators to solve issues like large-scale Internet access or the efficient provi-

sion of real-time multimedia services. Furthermore, service penetration is unpredictable due to the sharp competition between operators.

This dynamic nature of the telecommunications scene makes it impossible to follow rigidly the life-cycle described above. Since services are introduced and phased-out rapidly, operators must reconfigure and/or redesign their network several times. And it has to be accomplished in parallel to the daily operational tasks. Surveys show that the time spent on different tasks can be represented by a pyramid (Fig. 1), where the time needed for daily operation is at the base.

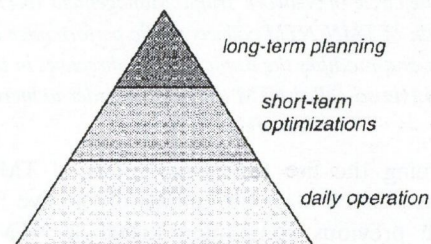


Fig. 1. The "operational pyramid": usually daily operational tasks consume the most time of an operator, considerably less time is spent on optimizing the current network, and even less remains for long-term planning

The tasks at the higher layers are at least as important. Proper network management tools can provide the necessary assistance to an operator in allocating its resources between the different tasks. A good management system supports the operator in different ways:

- reduces the load of daily tasks by helping the operator keep the network operating around the optimum;
- helps to evaluate alternatives for short-term optimizations or even proposes improvements;
- supports the long term planning phase by automatically collecting data about network load and performance indicators during daily operations.

This paper discusses the role of network traffic management, a specific function of network management, in different network architectures. Then we introduce the Plasma concept which combines simulation with analytical methods and optimization algorithms in an integrated framework. A traffic management tool using the Plasma concept is capable to support the operator in its tasks at all

of the levels discussed above. The design and implementation of such a traffic management tool is also discussed.

2. NETWORK TRAFFIC MANAGEMENT

The primary role of Network Traffic Management (NTM) is to supervise and maintain the traffic performance in the network during its operational phase, via collecting performance data and applying necessary modifications to traffic control functions in the network elements such that the performance is kept near to its possible maximum (Fig. 2). The most important traffic performance parameters are:

- *total carried traffic* in the network (throughput),
- *achieved grade of service (GoS)* e.g. call blocking probability.

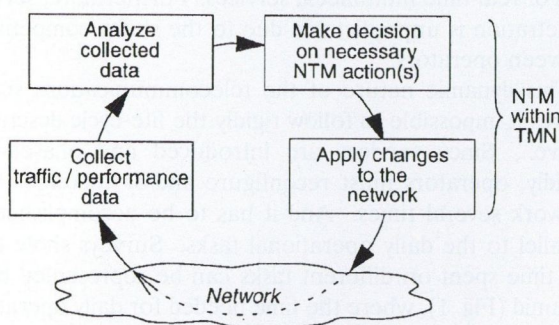


Fig. 2. The circle of Network Traffic Management (NTM). As a sub-function of TMN, NTM collects traffic performance data from the network and modifies the traffic control directives in the network elements (via so-called NTM actions), in order to increase the network performance.

Concerning the five functional areas of TMN (often referred as FCAPS after the initials of the five functional areas, see previous companion articles), NTM can be regarded as an interdisciplinary function within TMN, interacting primarily with three of the FCAPS areas, such as *performance management*, *configuration management* and *fault management*. Since NTM requires a network level view, it is most often implemented in the lowest layer of the network management hierarchy where such a view is available, which means usually the network management centers (Fig. 3).

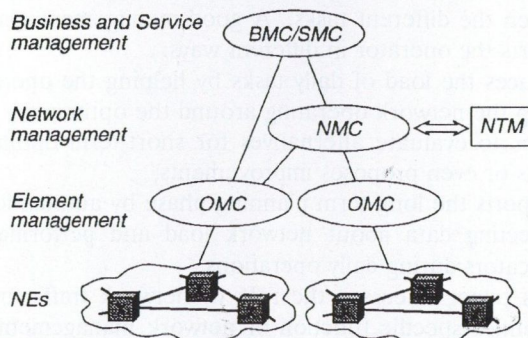


Fig. 3. The place of NTM in the TMN hierarchy: The NTM functions are typically implemented in an NMC. BMC/SMC: Business/service management center; NMC: Network management center; OMC: Operation and maintenance center; NE: Network element

In the following sub-sections we summarize the typical tasks of NTM in three of the most known communication networks.

2.1. NTM in PSTN

There is a relatively long tradition of NTM in ordinary public-switched telephone networks (PSTN), and a set of ITU recommendations defining NTM specific performance parameters and NTM actions for PSTN are also available. Some examples of such NTM actions are:

- activate/deactivate temporary alternate routing (TAR) tables,
- restrict connections based on origin or destination,
- trunk (circuit group) reservation,
- call gapping.

Fig. 4 shows a typical phenomenon in PSTN that comes from its connection-oriented nature: When the offered traffic approaches the traffic level for which the network was designed (engineered load), calls start to be lost. If a call that spans over a number of circuit groups is rejected near to its destination, there are circuits already allocated on previous circuit groups, which now have to be released. Such temporarily allocated circuits may prevent other calls to be successful, which further increases the call rejection rate in the network. Overloading call processors with unsuccessful calls has a similar effect.

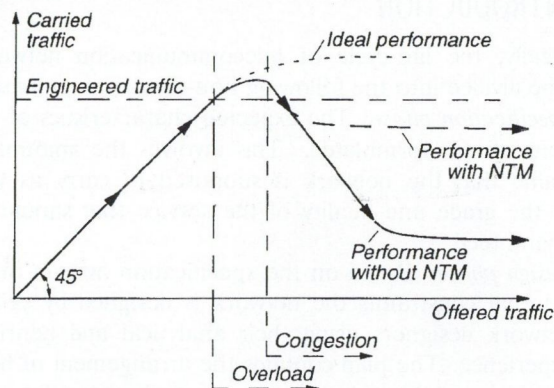


Fig. 4. One of the main roles of NTM is to preserve the throughput of the network in congested situations.

Expansive NTM actions such as activating TAR tables, can prevent the network from becoming congested in situations where the overload has not yet spread over the entire network. In overall congested state *restrictive actions* such as call gapping, destination blocking, can help by cancelling calls that has low probability to succeed before they enter the congested network. In that way, carried traffic can be kept near to the engineered level.

As of today, most of the leading switch vendors support a large portion of ITU compliant NTM functions, and the TMN infrastructure ensures the means for centralized data collection and NTM action activation. However, network managers have to have the ability to decide what action to take in a given situation. Considering the large number of parameters have to be taken into account, and the large set of possible actions available (together with their numerous parameters), it is not a surprise that in the lack

of intelligent decision support tools such NTM functions are hardly used today.

2.2. ATM related NTM tasks

Due to the fact that ATM also is a connection-oriented technology, it inherits the above behavior from PSTN. Moreover, further challenges arise, since

- NTM in ATM has to cope with many different types of connections,
- *Quality of Service* (QoS) parameters of the connections have to be considered,
- *virtual layers* of the network have to be maintained.

The latter challenge comes from the virtual path concept in ATM, with which logical networks can be formed within the same physical ATM infrastructure. Such logical networks (virtual networks) can be used to install *virtual private networks* over a public ATM network or can implement *virtual service networks* for the different bearer services (Fig. 5). Contrary to former networking technologies, virtual networks in ATM can be dimensioned real-time with changing the assigned capacity of the virtual paths and other switching resources, such that the capacity of the virtual networks are always in accordance with their needs. This feature — if used properly — can result in better resource utilization, but the fast and flexible adaptation of the virtual network system to rapidly changing mixed traffic patterns or to sudden failures requires the solution of the task called real-time dimensioning.

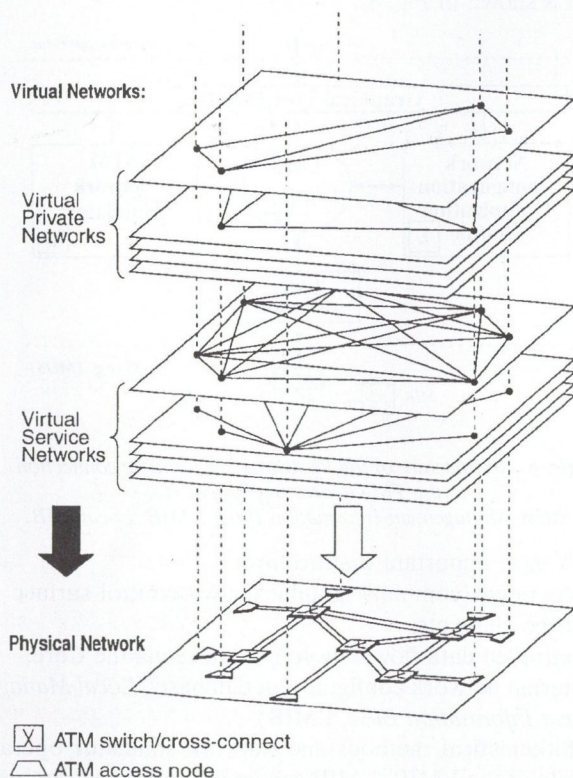


Fig. 5. One of the advanced feature of ATM is the possibility of designing Virtual Networks.

Hierarchical virtual structures in the network involve hierarchical approaches in network management and thus in real-time dimensioning. As a typical rule, whenever

a problem cannot be solved within a given logical layer, the solution requires the co-operation with the operational center of the higher layer. Different time-scales and different levels of dimensioning require different models and methods.

2.2. IP related NTM tasks

Traditionally, there was little space for on-line traffic management in IP networks. This was mainly due to the fact that IP provided only best-effort service without any QoS guarantees. Therefore the main concern was to maintain connectivity between sites which can be achieved by routing algorithms that do not consider the load on the network. The few traffic-driven decisions, such a load-balancing between parallel links, were automated eliminating the need for traffic management.

The above situation is going to change dramatically with the introduction of Integrated-Services (IS) into Internet. With the IS extensions, IP will support different service classes and users will have the option to reserve resources in order to achieve a certain QoS level.

ATM is a key technology in the development and deployment of the IS Internet. ATM clouds can be used to connect IP networks using technologies such as IP over ATM or LAN emulation. An even closer integration of IP and ATM is also a viable alternative, several proposals such as the Next-Hop Resolution Protocol (NHRP), tag-switching, and others are discussed by standardization bodies and the industry today.

Fig. 6 shows a possible configuration to provide IS-IP services over an ATM network. LAN segments are connected to ATM backbone via access nodes that use LAN Emulation. This allows the creation of Virtual Private Networks (VPN) to connect geographically separated LAN segments owned by the same customer. Some servers are connected directly to the ATM backbone, while others can be accessed through routers. The routers are also needed to route traffic between different VPNs. By appropriately configuring the virtual paths and virtual connections in the ATM network, the operator can provide a wide-range of services to its customers.

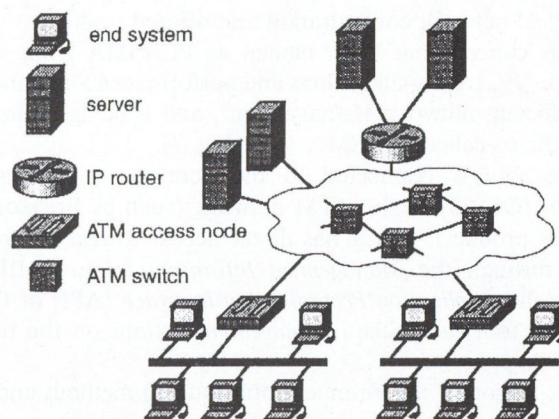


Fig. 6. Public operators providing Internet services over their infrastructure have to dimension the capacity and configuration of the connections according to the actual demands of the traffic.

The introduction of the IS model changes several aspects of IP networks:

- routing must take QoS into consideration;
- call-admission control decisions must be taken when a resource reservation request is processed;
- individual packets must be scheduled depending on the QoS assigned to their flow.

Of course, the routing of a reservation request or scheduling packets is out of the scope of traffic management. There are algorithms to implement these tasks. But due to the complexity of these algorithms, there are several parameters that influence their behavior. Different policies can be implemented by adjusting the parameters and the overall performance of the network depends heavily on the policy being used. This is where traffic management becomes important by supporting the operator in selecting the best policy for a given situation.

3. PLASMA CONCEPT

When searching for sources of programmable and reusable intelligence that can be integrated into the network management system, some of the obvious areas are:

- analytical (algorithmic) methods,
- simulators,
- artificial intelligence (AI).

Since AI approaches (such as expert systems, case-based reasoning, etc.) also presume some human experts, in the beginning the first two areas receive higher importance. That led us to the concept of introducing intelligence into the management system via the integration of:

- mathematical models and optimization algorithms with the capability of generating suggestions for management actions related to the logical configuration of the network (e.g. VP topology, VPC dimensions, assignment of offered traffic and service networks to VPCs, routing programs/tables, CAC parameters and other resource sharing directives).
- a network performance simulator with the capability of predicting Grade of Service (GoS) and Quality of Service (QoS) performance parameters (e.g. call blocking ratios, link utilizations, cell loss ratio and other cell-level quality parameters [2]) of an arbitrary physical and logical network configuration and offered traffic.

This concept has been named as PLASMA from the motto: "PLAnning-algorithms and performance Simulation for efficient network MAnagement", and is being realized with the so-called PLASMA Tool (Fig. 7).

The tool is connected to the centralized Operating System (OS) [3] of the ATM network (such as Ericsson's TMOS product), and it has direct access to real network data through the Management Information Base (MIB). Using the Application Programming Interface (API) of the OS, the tool can initiate management actions on the real network.

Integration of algorithmic (optimization) methods and a simulator into the OS offers the following capabilities:

- Management decisions can be supported (or generated) by analytical methods. Optimizing can start from real network data.
- Management decisions can be testified and compared

either with analytical performance evaluations or on the network performance simulator before applying them to the real network. The simulator can be initialized from real network data.

- Results of configuration optimization can be directly applied to the real network (e.g. new- or resized VPCs, updated routing tables, etc.).
- As a long-term goal, introduction of automated network control is also possible.

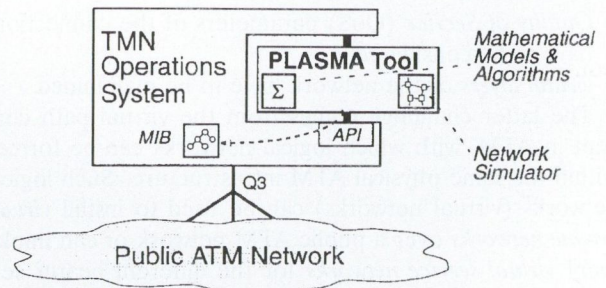


Fig. 7. PLASMA Tool as an add-on tool for the ATM Network Operating System.

API: Application Programming Interface;
MIB: Management Information Base

4. PLASMA TOOL

4.1. Architecture

The internal functional architecture of the PLASMA Tool is shown in Fig. 8.

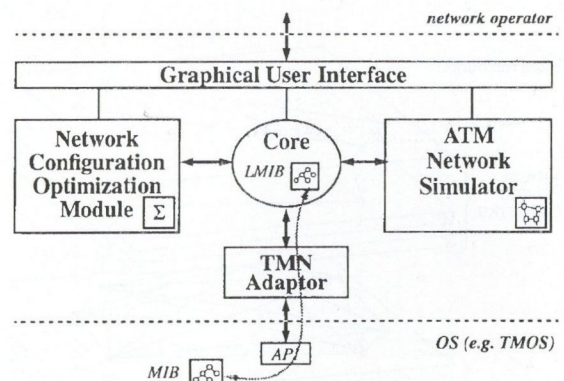


Fig. 8. Architecture of the PLASMA Tool and its connection to the TMN Operating System (OS).

MIB: Management Information Base; LMIB: Local MIB

It's most important features are:

- integrated (common) graphical user control surface to all the elements;
- controlled data flow between modules via the Core;
- internal network configuration database (Local Management Information Base, LMIB).

Mathematical methods and network simulator operate on data of the LMIB. LMIB can be different in its contents from of the actual MIB of the OS: temporarily isolated LMIB makes it possible to experimentally modify the network configuration (either logical or physical), thus enabling the comparison of several solutions e.g. via performance investigations.

4.2. Network Configuration Optimization Module (NCOM)

NCOM is a library of mathematical methods that offers analytical solutions for a large number of traffic management tasks. The intention is to offer a selection of algorithms for solving most of the problems, providing the manager with a degree of freedom via a *trade-off between accuracy and complexity*. The advanced methods apply various optimization and search techniques to optimize the virtual configuration, using different modeling assumptions. According to the output (purpose) of the methods, two classes are:

- Generator methods that can generate suggestions for modification of the logical network configuration. (Suggestions can be transformed into management actions then.)
- Evaluation methods that can predict network performance parameters for a given network configuration.

The two main sources of the current and the foreseeable methods are:

- *Teletraffic models* describing the traffic on different levels of accuracy, spanning a space of models from a single parameter description with link independence and reduced load approximations to more complex multiparameter estimations of the offered and carried load in a multirate traffic environment. In computing the route blocking probabilities the interdependence between call blocking and routing algorithms can be taken into account by well established models, such as the Erlang fixed point equation.
- *Algorithmic solutions* to find the optimum configurations in the above teletraffic models. The algorithms again provide a trade-off between accuracy and speed. They apply optimization techniques, such as gradient based hill climbing using estimations of network revenue derivatives, convex optimization, linear and integer programming, combinatorial optimization including network flow algorithms etc.

The method library of NCOM is open for the integration of new methods including new teletraffic models and new algorithmic solutions.

When a new calculation is initiated by the operator, the module offers a list of methods available for the particular problem. For each item in the list a short description of the method is presented, including details about the approximation taken by the method, limitations and expected running time. When the operator chooses a method, the selected algorithm with the input data is passed to an execution shell, which performs the calculations. Results are forwarded back to the Core.

NCOM can offer parallel execution of different methods, even on separated processors.

4.3. ATM Network Simulator (ANS)

ANS is an event-driven simulator, that is used for call-level simulation of an ATM based network. The same simulator is used to simulate PSTN networks. It has a built-in simulation model, but it is also open for

the integration of new models and accelerated simulation techniques.

For a given network configuration, a set of performance monitor points can be automatically or manually generated. During the simulation, connections are set up and released according to the offered traffic defined by traffic models and related parameters. ANS supports two levels of simulation:

- In *pure GoS simulation* only GoS parameters such as call blocking ratio, link utilizations, etc. are observed.
- When *QoS simulation* option is switched on, besides of the GoS parameters, QoS performance (e.g. cell loss ratio, cell delay, cell delay variation, etc.) of a predefined set of connections can also be monitored. (For QoS estimation an expandable QoS database is used for each type of the simulated network nodes.)

4.4. TMN Adaptor

Its primary task is to perform a mapping function between the LMIB and the MIB of the OS. Mapping may include translation of model (if the information model of the MIB and LMIB are different) and/or synchronization (if the contents of the two database are not the same). Two ways of synchronization are: when existing LMIB are synchronized to the contents of the MIB and when content of LMIB need to be applied to the real network. In the latter case, TMN adaptor searches for the differences between the MIB and the LMIB, and it translates differences into management actions (such as Set, Get, Create, and Delete operations) and actions are passed to the OS via the *Application Programming Interface* (API).

4.5. Graphical User Interface (GUI)

GUI offers a visual easy-to-use interactive interface to the tool, hiding its internal complexity. Even though GUI provides its own tool-specific dialogue surface, it must follow the style of the user interface of the OS in order to offer easy understanding to the network operators.

5. CONCLUSION

The integration of traditional voice and data communication services and the emergence of new real-time multimedia services requires telecommunication networks of such complexity that cannot be efficiently managed without the support of dedicated tools. The role of network traffic management is getting an increasing emphasis in the management of these. The powerful Plasma concept has been introduced in this paper which provides the foundation for building effective traffic management tools. The integration of analytic methods, optimization algorithms, and a powerful simulator plays a central role in this concept. The design of a traffic management tool based on the Plasma concept has also been discussed. Due to its flexibility, the tool can be easily adapted to many different areas of telecommunications. There are existing versions of the tool for traffic management of PSTN and ATM networks. The design of a version to support the management of IP-based network is the subject of our current research activities.

6. ACKNOWLEDGEMENTS

The first PLASMA demonstrator prototype for ATM real-time virtual network dimensioning has been developed

REFERENCES

- [1] Zsolt Haraszti, et. al: "PLASMA — An Integrated Tool for ATM Network Operation", *Proceedings of the International Switching Symposium ISS'95*, Berlin, April, 1995.
- [2] *The ATM Forum: 'ATM User-Network Interface Specification'*, Version 3.0, October, 1993.

at the High Speed Networks Laboratory of the Technical University of Budapest in cooperation with ELLEMTTEL Telecommunications Systems Laboratories, Sweden.

- [3] 'Principles for a Telecommunications Management Network', *CCITT Recommendation M.3010*, Geneva, 1989.
- [4] Henry Tarle: 'Network Traffic Management (NTM) Using AXE and TMOS Systems', *Ericsson Review*, No. 4, 1994.

Miklós Boda graduated in Physics at the Eötvös Loránd University, Budapest, Hungary. He received his Ph.D. in solid state physics at the University of Uppsala in 1971. Then he joined HAFO (Semiconductor Research Institute) Stockholm. From 1978 he worked as LSI expert for DATASAAB (now part of Nokia) and in 1980 he moved to Philips Elektronik as manager for LSI Design and Test Center. He joined Ellemtel Telecommunications Systems Laboratories in 1990 as manager of Advanced Technology Research. From February 1996, he helps establish the Ericsson Traffic Analysis and Network Performance Laboratory at Ericsson in Budapest as General Manager of Research & Development. He is the Chairman of Ericsson Concern Committee for Artificial Neural Networks and Artificial Intelligence and the founder and president of the Swedish Neuronet Society. He is the Coordinator for SWAP (Swedish ATM Platform) national project. He is a member of the Industrial Advisory Board of the Research Center for Advanced Communications and Computing, North Carolina, USA. He was on the board of MULTI-G and he is on the board of Stockholm Gigabit Network. He is a honorary member of the Hungarian Academy of Engineering.

Zsolt Haraszti is a researcher in the Traffic Analysis and Network Performance Laboratory at Ericsson in Budapest. He received his M.Sc. degree in Electrical Engineering from the Technical University of Budapest, Hungary, in 1993. Since that time he has been working on his Ph.D. degree at the Department of Telecommunications and Telematics, at Technical University of Budapest. His main areas are performance modeling and network traffic management. His special interest is in simulation techniques for communication networks with special focus on rare event simulation.



András Oláh is a researcher in the Traffic Analysis and Network Performance Laboratory at Ericsson in Budapest. He received the M.Sc. degree in electrical engineering from the Technical University of Budapest in 1991. From 1992 to 1996, he was a Ph.D. student at the University of Twente in the Netherlands, where he was involved in the verification, analysis, and design of transport protocol mechanisms for reliable communications. He has been employed by Ericsson since May, 1996. His main interest is the traffic management aspects of introducing real-time services in the Internet.

GSM NETWORK MANAGEMENT

I. MARADI

WESTEL 900 GSM
H-1114 BUDAPEST
KAPOSVÁR U. 5-7.

ETSI writes: "The concept of the Telecommunications Management Network (TMN) has developed as the result of a demand for a common management approach to the management of the diversity of equipment types, functionality and service provision inherent in modern telecommunications networks." As it can be seen from the ETSI quote, TMN should play vital part in all kind of telecommunications networks. The GSM networks are growing all over the world, the number of customers served exceed 40 million by the end of 1996, which indicates that the networks behind the scenes could be huge and complicated... GSM network management is even more complicated as international roaming is taken into account, because an average European operator has some 50-55 roaming partners around the globe. This article summarizes some of the key elements of the GSM network management functions, leading through all practical aspects of a daily Network Management.

1. INTRODUCTION

GSM networks are growing all over the world. GSM is the world's most widely deployed digital cellular technology. More than 40 million calls are made every day, and the annual market growth exceeds 50 percent. Not too many network suppliers exist on the world, but their number is enough to generate a multivendor environment for network operators. Fig. 1 shows the countries with GSM networks in Europe, Asia, Middle East, Africa and North America (from bottom to top).

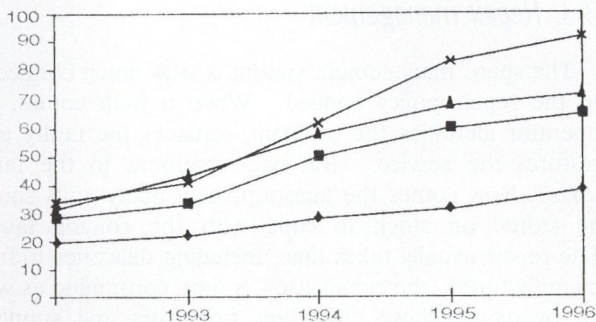


Fig. 1. Number of countries with GSM

This vast amount of calls require sophisticated network configurations and signalling solutions. All operators are hunting revenues to cover their capital expenditures. To provide quality service for the subscribers, and — consequently — generate income for the company, all network solutions should be reliable and properly managed. The task of the network operators is not simple: set up a network which is immune against network element failures, self healing, and keeps the customers' on the move even outside of his/her home country. The globalization of the mobile subscription made the network operators' life even

more complicated with subscribers roaming in more than 50-70 countries.

2. NETWORK MANAGEMENT SCOPE

Network management functionality is the least defined in the GSM standard. Though the Series 12.00 ETSI specification deals with generic issues for GSM, there is still plenty of room for more precise definition.

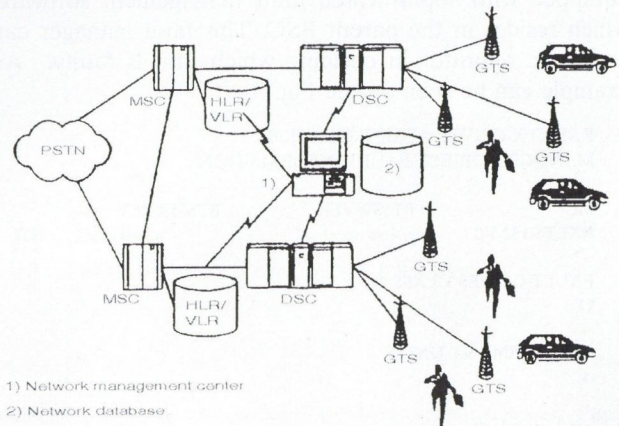


Fig. 2.

The main areas which are covered under the common name GSM network management, are:

- fault management,
- performance management,
- security management,
- configuration management (applications).

3. FAULT MANAGEMENT

Though the currently manufactured systems are more and more reliable, faults may occur. If a fault happens, depending on the seriousness of the problem, the operator can lose both revenue, and subscribers as well. Angry subscribers are the worse subscribers: they are willing to switch to the competitor without hesitation if a certain problem in the network disturbs their calling pattern.

The fault management consists of several interrelated areas, like:

- early warning systems (maintenance applications),
- alarm presentation and analysis systems (expert systems),
- spare management system,
- faulty board/unit repair system.

3.1. Before the fault strikes

The fault management has to concentrate on managed elements (switches, radio base station units, computer plat-

forms) and on network level (transmission lines, functional levels). The first one is usually covered by the manufacturer, who tries to produce highly reliable units. On the switch side usually the stand-by and the executive processors are the core of the security line, which continues with backup data systems for data and switch programs. The important parts of a radio base station is duplicated as well, like power converters and reference oscillators. In a switch the central processor CP is duplicated. The two sides operate parallel synchronous mode, enabling hardware faults to be detected immediately by comparison between data and program sides. If a failure occurs, the microprocessor controlled maintenance unit automatically isolates the faulty side and hands over the traffic handling responsibility to the other side. This process is so fast, that no corrective action is needed by the application programs.

The currently manufactured base station cabinets are equipped with sophisticated fault management software, which resides in the parent BSC. This fault manager can assist the operator in deciding which unit is faulty. An example can be seen on the Fig. 3.

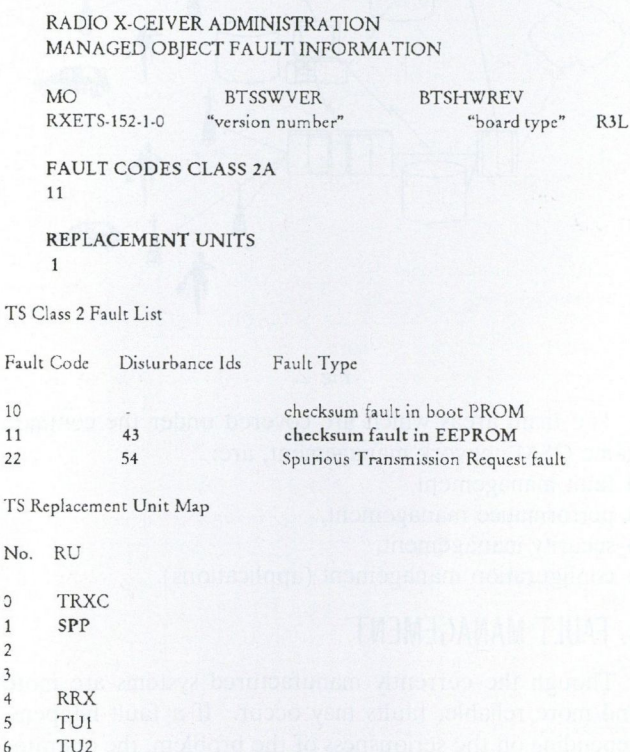


Fig. 3. (x axis indicate Years from today)

This example shows, that the RBS fault is caused by checksum fault in one of the EEPROMs, and the suspected board is the SPP unit, which is installed in the BTS cabinet (Ericsson terminology).

After receiving an alarm from one of the in-service base stations, the field support/maintenance engineer can have a first glance indication about the seriousness of the failure. Unfortunately these systems are driven by decision table, which often misinterprets the cause of the fault, and leaving the support engineer relying on his own experience and talent. There is still a long way before those expert

systems are really applicable. For a switch equipment, typical yearly restart intensities per exchange can be:

minor restart	10
major restart	1.5
major restart with reload	0.5

These numbers should be tightly connected to the time necessary to bring the system up. These numbers can be as:

minor restart	20-100 seconds
major restarts	20-100 seconds
reload from HD	2-5 minutes
reload from internal store	20 seconds

3.2. Spare management systems

For a network operator the spare parts management can be of great importance. Usually the operator spends capital to buy a certain amount of spare units for the system. This amount varies according to the support agreements with the relevant system suppliers, but as an average it can be as 5-8 % of the total network capital. Because of the wide distribution of the installed network elements, it's not easy to set up a simple model which produces the necessary amount of spare units for a certain number of installed base. Operators are usually very sensitive about the average repair time of a certain fault which affects the service offered. The rule of thumb (what a surprise) is that the shorter the wanted down time the closer the spares should be stored. And consequently more spare units are needed... The real optimum very much depends on the actual company policy. Reading the mobile literature it was very difficult to find reference data about average down time per base stations, switches or other managed objects, due to the sensitivities of this kind of information.

3.3. Repair management

The spare management system is very much connected to the repair policy applied. When a fault comes, the operator identifies the problem, replaces the faulty unit, restores the service. But what happens to the faulty units? Now comes the question, how many units should be stored on stock to cope with the coming faults? The repair usually takes time, including deliveries to/from manufacturers, the repair itself is time consuming as well. To overcome these difficulties operators and suppliers usually set up different categories for spares. As an example they can be as swap repair type or repair and return type, depending on the importance of the unit in question. Very sensitive issue is the average repair time of the faulty units. The longer the repair/return time, the more money the operator should invest in buying spares for the system, which is not the best solution. Usually the system supplier and the network operator set up common goals to keep the delivery times within an acceptable level, which is monitored regularly to keep costs down (incentives).

When a fault comes, the effect of it can be real damaging. To ensure fast and effective isolation and restoration of the network outage, highly sophisticated

alarm indication systems should be applied by the operator. An outage costs in two way:

- the lost revenue and the unhappy subscribers,
- the actual repair (manpower, faulty units).

When field engineers are targeting a network fault, they need fast and valuable information where the fault is and what the possible cause of the problem is. To ensure the flow of properly digested information, both network operators and system suppliers have developed different network management applications and systems. The motivations are slightly different on both sides. While the system supplier is interested in having reliable systems which were supplied by them, they rarely care about multivendor environments, the operators often face. This fact forced the operators to develop such systems which can be easily and flexibly attached to different suppliers' equipment. It can be a nightmare when two, three or more different terminals and monitor systems are installed at the operators premises (Network Control Centers). The standardization on that side was a bit slow, compared to other network solutions and standards. The so called Q3 interface standard will allow the operator to have common interface for each different vendors' equipment, allowing its staff to monitor and supervise systems effectively.

4. PERFORMANCE MANAGEMENT

The GSM standard (Digital cellular telecommunications system (Phase 2); Performance data measurements (GSM 12.04)) defines the vast amount of performance data which should be monitored and measured by the network operator.

Here is an abstract of the relevant ETSI definition:

"Performance measurement concept

Any evaluation of PLMN system behavior will require performance data collected and recorded by its NEs according to a schedule established by the OS. This aspect of the management environment is termed Performance Management. The purpose of any performance management activity is to collect data which can be used to verify the physical and logical configuration of the PLMN and to localize potential problems as early as possible. The type of data to be collected is defined by the equivalent annexes."

The performance data is used for several purposes:

- network engineering,
- network tuning,
- fault finding,
- traffic pattern prediction.

The data format what the network utilizes to produce the performance data varies between system vendors. It is always critical for the operator how much computing resources the data postprocessing requires. If the data is in plain text format, maybe the applications can easily digest the data, while the necessary memory space could be enormously high. Different network vendors use different kind of IO device to produce all kind of data about the network performance. To reduce the processor load of the IO device, they tend to compress the data and its format to the very minimum, and they use an intermediary device to decompress the data fed out from the switch. This could

be fast, though requires extra computing capabilities from the network operator, and reliability should be monitored as well.

According to the GSM standards, the measurements are divided into major categories, like:

- (G)MSC measurements,
- BSC measurements,
- BTS measurements,
- HLR measurements,
- VLR measurements,
- AUC/EIR measurements.

Each category contains couple of tens of different measurements, like traffic, success rate, handover, signalling interrogations, etc. One important factor is the availability of measurement data for the network operator. Some applications can check the network data pattern from irregularity point of view. While most of the HW is intelligent enough to detect and indicate a HW fault, some of the network problems can not be related to any direct HW fault. This can be, as an example, decrease of traffic on a certain cell due to receiver antenna performance degradation. If the receiver antenna is not checked regularly with ISWR detectors, this fault will be noticed by the subscribers only. To prevent those kind of problem, the traffic pattern indication method can be used. This method sets up a regular traffic pattern of the cell, and continuously compares the current traffic profile with the preset profile. If, let's say the traffic drops by 30 % compared to a previous days or weeks, an alarm should be generated for the network operator. This method intensively uses the traffic measurement data, and this data should be available as fast as possible. The faster the data from the network element, the more processor load it takes from the IO device. One optimal number could be 10–15 minutes. This provides relatively fast response time for the network operator, and keeps the load of the processors still on an acceptable level.

5. SECURITY MANAGEMENT

This is defined in ETSI document "Digital cellular telecommunications system (Phase 2); Security management (GSM 12.03)".

GSM security management concentrates on four major areas:

- subscriber identity (IMSI) confidentiality,
- subscriber identity (IMSI) authentication,
- data security over the air interface (mobile-base station),
- mobile equipment security.

Based on the experiences of the previous analogue systems, confidentiality and security received special attention in the GSM standard.

5.1. Subscriber identity (IMSI) confidentiality

Subscriber identity security was achieved by using TMSI (Temporary Mobile Station Identity) numbers during call set up and during further communications between the mobile station and the network.

The ETSI document defines TMSI as:

"Subscriber confidentiality in the GSM PLMN is provided by the use of the Temporary Mobile Subscriber Identity (TMSI) on the air interface. Avoiding the use of the

International Mobile Subscriber Identity (IMSI) over the air interface by substituting the TMSI, provides both a high level of confidentiality for user data and signalling, and protection against the tracing of a user's location.

As the frequency of reallocation of the TMSI has an effect on the subscriber confidentiality, a parameter is defined to provide control over it.

If the (old) TMSI is unknown to the Visitor Location Register (VLR) or wrong, the mobile subscriber can only be identified by using the IMSI. As encryption is not possible during that stage, the IMSI has to be sent unencrypted over the air interface. The occurrence of such an event (or similar) affects the quality of the subscriber confidentiality service. Counters are defined to provide information about this service."

From operators' point of view the introduction of TMSI provides the above defined safety, plus reduces load on the SDCCCH logical channels in certain cases.

5.2. Subscriber identity (IMSI) authentication management

All GSM networks provide a mechanism for the authentication of subscriber identity. With help of this feature the network operator can protect its subscribers from fraudulent intruders with unauthorized access. To support authentication, vectors are generated in the AuC. The VLR requests these authentication vectors for use in the authentication procedures. Under exceptional conditions, these vectors may need to be reused. This may have an effect on the security of the network, and should be under the control of the operator.

To provide authentication, so called Authentication Centers (AuC) are used. The AuC is usually connected to the VLR, with C7 signalling, using MAP protocols. A key factor for the operator, that authentication should be controlled on a secure way and should be on all the time. In some cases when the AuC is not available for the network (maintenance, software upgrades, failure), it may be necessary to utilize old authentication keys.

5.3. Data over the air protection

Beside the strong subscriber security features of the GSM networks, the data protection is solved and supported as well. When data is mentioned, both speech data flow and real data (like Internet access data) is protected. To achieve protection, ciphering algorithms are used in various part of the network. These algorithms are:

- Between the mobile station and the MSC up to seven versions of the ciphering algorithm -A5/1, A5/2...,A5/7- is used. If not all the algorithms are supported by the mobile, the MSC decides which one will be used. This algorithm is implemented in the mobile and in the BTS.
- Ciphering key generation algorithm (A8). This algorithm provides the necessary ciphering key (Kc). This algorithm resides in the AuC.
- Authentication algorithm (A3). This resides in the SIM, and uses the secure Ki, which is unique to the subscriber. This Ki is stored in the SIM during

manufacturing, and stored in a secure SIM memory area.

Data security is vital for several customer applications, like Home Banking or transfer of Credit card information. The data speed over a GSM network is currently 9.6 kbit/s, though the tendency is to increase the speed using multiple timeslot techniques. Data security will play even more important role in the GSM systems in the near future if data speed is increased. Some examples can be seen for higher data speed applications over GSM networks in Table 1.

Table 1. Higher data speed applications over GSM networks

Data communications bit rate	Single slot 9.6 kbit/s	Double slot 19.2 kbit/s	Multiple slot 76.8 kbit/s
Application			
Simultaneous voice and data	Half rate + 4.8 kbit/s	Full rate + 9.6 kbit/s	Full rate + 76.2 kbit/s
Hi-fi music/voice	Wireline quality with enhanced full-rate coder	Hi-fi quality voice	Hi-fi quality voice and music
Multimedia/video	Still pictures, animation	Animation video	Video conferencing

5.4. Mobile equipment security

Due to the extensive roaming capabilities of each GSM network, the security of the mobile phones is of vital importance. The solution which is used and applied in GSM systems relies on an IMEI number (International Mobile Equipment Identity) securely stored in each mobile phone. This IMEI number is requested by the VLR, which is connected to the EIR (Equipment Identity Register). Each EIR stores information about stolen or suspicious mobiles, and if these IMEI number is in use, generates a message/alarm for the network operator. Each operator maintains a black, gray and white list, which are regularly updated.

When a mobile phone is manufactured and distributed all over the world, the manufacturer sends an IMEI range of their mobiles to a central EIR system in Europe. This central location would be used by other network operators to update their local EIR about listed mobiles phones to prevent international distribution of stolen phones. This central system is still not in use 100 %, which means that the operators are exchanging data about listed mobiles on per occasion basis. The data exchange is based on X.25 network, with security algorithms on both side to prevent tapping. The frequency of data exchange varies between operators, it varies between once a day to once a week, depending on the size of the network.

Each network operator can decide if he wants to use EIR or not. Most of the operators are using this security service since their service launch.

The EIR equipment itself is usually a simple, but very reliable computer with real time database handling capabilities. C7 connections carry the IMEI check request from the MSC/VLR to the EIR, and the same links are used backwards. The intensity of the IMEI check request can be adjusted by the operators: IMEI can be checked at call setup, location update or even at handover. The intensity of the checks increases the processor load both

on the MSC side, and both in the EIR, while the necessary C7 link capacity should be provided as well.

6. CONFIGURATION MANAGEMENT

ETSI describes the evolution of a GSM network as a three phase model:

"In the development of a PLMN, three general phases can be described which represent different degrees of stability. Once the first stage is over, the system will cycle between the second and the third phases. This is known as the network life-cycle and includes:

- *the PLMN is installed and put into service;*
- *the PLMN reaches certain stability and is only modified (dynamically) to satisfy short term requirements, e.g. by (dynamic) re-configuration of resources or parameter modification; this stable state of a PLMN cannot be regarded as the final one because each equipment or SW modification will let the PLMN progress to an unstable state and require optimization actions again;*
- *the PLMN is being adjusted to meet the long term requirements of the network operator and the customer, e.g. with regard to performance, capacity and customer satisfaction through the enhancement of the network or equipment upgrade.*

During these phases, the operators will require adequate management functions to perform the necessary tasks."

During these phases the operator has to be able to fully control the system's all parameters, which is usually referred to as configuration management.

In a GSM network the BTS, the transmission network (time slot assignment), the BSC and the MSC parameters are the most important parameters to control. Before a BTS is put into service, tens of individual parameters and controls have to be set up, and be maintained through their lifetime.

All the parameter management functionality has to have control over different versions (before modification, after modification, or even more states should be kept simultaneously in the database), logging about who, when, what did/made. The system has to be able to validate the database by frequent network audits, when the database is checked from consistency point of view. In that case the configuration management system compares the actual in-service data with its own database content, and makes the necessary corrections automatically or generates a flag about the inconsistency found. A highly complicated and relatively large system needs graphical user interface to help the networking staff to overview the status at a glance.

Sophisticated configuration management systems allow the operator to generate analysis of the network using modeling tools. In that case the operator can set up different scenarios, like "what if I move 13 BTS cells from BSC1 to BSC2?". The model can predict the status of the network after the change, and can provide answers for questions like:

- the traffic load of the two BSC concerned,
- the processor load variations in both network elements,
- handover, call success rate and other parameter changes, based on the actual network model.

This kind of modeling can be extremely useful for network operators, because some of the parameters can be set up prior the live network change. Practical examples showed that even a minor modification of the network structure (loading two sites from one BSC to an other) could deteriorate the call success rate due to SAE mismatch.

The range of, or necessity for, equipment management functions will vary depending on the nature of the implementation. The following are typical functions for the management of equipment by a remote managing system:

- Equipment Availability Management;
- Equipment Utilization Management;
- Equipment Identification;
- Equipment Redundancy;
- Overload Protection;
- Replaceability;
- Compatibility.

One of the pressure to develop a new, pan-European digital network was to overcome the world wide capacity problem of mobile systems. Soon the number of GSM subscribers served will exceed 40 million around the world, which will generate capacity problems again. Some of the network operators have already implemented new generation of radio network, using micro, picocells, applying frequency hopping. The capacity gain is shown on Fig. 4. Using these type of solutions, the configuration management functionality has to be of vital importance for all network operators.

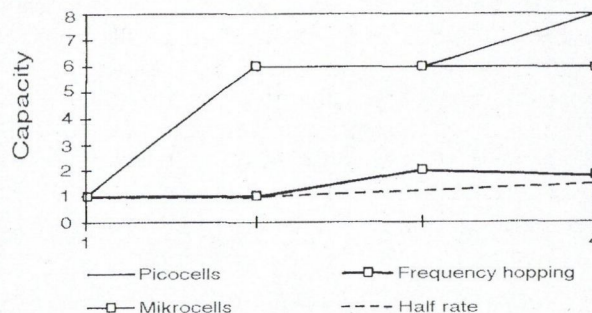


Fig. 4.

7. CONCLUSIONS

As it can be seen, the GSM network management is a sophisticated, complex matter which still has its own standardization problem for the future. Systems are in service around the world, millions of calls are switched daily, but the systems still evolve. Operators and system suppliers all over the world are searching for better and more reliable solutions to be able to manage those complex structures. And in the meantime, the subscribers just call...

8. APPENDIX

ETSI recommendations of GSM Network Management

12.00	Objectives and structure of GSM PLMN management	4.1.0	
12.01	Common aspects of PLMN network management	4.1.0	
12.02	Subscriber, Mobile Equipment and Service Data Administration	4.1.0	
12.03	Security management		Cs
12.04	Performance Management and Measurements for a GSM PLMN	4.0.0	
12.05	Subscriber related call and even data	4.0.0	
12.06	GSM Network Charge Control		Cs
12.07	Operations and Performance Management		Cs
12.10	Maintenance Provisions for Operational Integrity of Mss	3.0.1	Cs
12.11	Maintenance of the Base Station System	3.1.1	Cs
12.13	Maintenance of the Mobile-services Switching Center	3.0.2	Cs
12.14	Maintenance of Location Registers	3.0.2	Cs
12.20	Network Management Procedures and Messages	3.1.0	Cs
12.21	Network management Procedures and Messages on the A-bis interface	4.2.0	

REFERENCES

- [1] ETSI GSM recommendations, 12.xx series
- [2] Ericsson AXE technology, 1995.
- [3] Telecommunications Magazine, Internet Online Edition, <http://www.telecommunications.com>, 1996 January, April
- [4] Telecommunications Reference Book, Freeman, Wiley-Interscience Edition, 1995.



István Maradi graduated as electrical engineer at the Technical University of Budapest in 1989, specialized in mobile telecommunications. Previously he held positions at the PKI Research Institute of PTT (1989–1990) and Westel Radiotelephone Ltd. (1990–1995), operator of the first analogue mobile network in Hungary. He is involved in mobile communications in Hungary since 1990, when the first network was launched. From 1995 he is responsible for GSM network operations and switch network planning. This year he will finish his English language MBA course. He is at Westel 900 GSM as Director of Operations. He is author of several mobile communications related article and presentations.

OPENING UP NETWORK MANAGEMENT

A. BUJARA

SIEMENS AG. TELECOM MANAGEMENT NETWORK, INTELLIGENT NETWORKS, BUSINESS DEVELOPMENT, DIENSTE TMN/IN
D-81359 MUNICH, HOFMANNSTRASSE 51., GERMANY

Today there are over 40 000 different products flooding the telecommunications equipment market. This makes multivendor capability (MVC) one of the most important forces driving the evolution of telecommunications management networks (TMN).

Often TMN is reduced to the aspect of multivendor capability (MVC) or used as a synonym for standardized interfaces. Siemens has conducted interviews and workshops worldwide with operating companies to gain a through understanding of what the expectations are concerning MVC and TMN. The results have formed the base for the architecture and design of the Siemens solution to TMN.

Technology-oriented operating companies expect standardized interfaces that eliminate vendor-specific operations, administration, and maintenance (OAM – Operation, Administration, Maintenance) procedures and that allow for the automation of operations processes, to become available soon.

Customer-oriented operating companies do not believe that standardized interfaces will be available soon. Facing competition they either prefer single-vendor subnetworks or MVC management systems based on proprietary interfaces.

1. WHAT IS MULTIVENDOR CAPABILITY?

MVC is a characteristic always associated with an application that is acting as a manager (ITU-T Recommendation M.3010). A manager application is said to be multivendor-capable if it can interoperate with applications, that are acting as agents implemented by and running on systems supplied by different vendors.

It is important to note, that the term multivendor-capable management system does not mean that all management applications run by the system are multivendor-capable. In most cases it is only a well-defined subset of applications that is multivendor-capable.

2. BENEFITS OF MULTIVENDOR CAPABILITY

The benefits that network operators expect to gain from multivendor capability are cost reduction, and increased quality of service.

Cost reduction may be achieved by MVC in several ways. First of all MVC enables the complexity of management systems to be reduced since certain applications do not need vendor-specific management systems for each vendor-specific network element. Second, MVC is a prerequisite for the unification and simplification of operations, administration and maintenance processes. Those simplifications reduce not only training costs and the costs for maintaining vendor-specific hardware and software platforms, but also reduce the number of operator faults caused by the huge amount of vendor-specific OAM interfaces, commands, and procedures.

Moreover, it makes the automation of operations processes easier. Ultimately, however, MVC contributes to optimum network utilization and therefore to investment reduction and cost savings too.

Automated or flow-through operations processes also contribute to an increased quality of service. Reduced service provisioning times, reduced mean times to repair, improved utilization of network capacity, faster response to customer inquiries, improved accuracy of billing are only some examples of quality of service improvements that can be achieved by multivendor-capable management systems.

Multivendor-capable management systems are essential for applications such as centralized alarm surveillance or network performance monitoring.

3. HOW MULTIVENDOR CAPABILITY CAN BE ACHIEVED

MVC can be achieved in different ways. Basically there are three possibilities that are described in the following (Fig. 1):

- screen level integration;
- mediation;
- standardization.

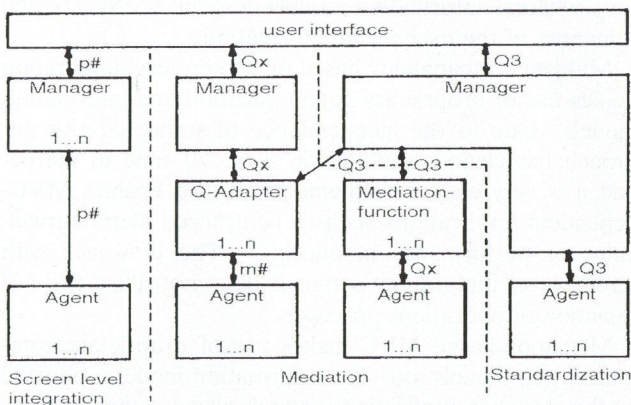


Fig. 1. Approaches to MVC. m#: any interface at the m reference point (see M.3010); p#: any proprietary interface

The term screen level integration refers to the case where user interfaces of different vendor-specific applications are integrated on a single screen, e. g. in separate windows.

The term mediation describes the scenario where an application massaging different vendor-specific agent applications supports a vendor-independent information model, and the agent applications support their own vendor-specific information model.

In this treatment, the term mediation summarizes mediation functions and Q adapter functions. Mediation functions transform a vendor-specific object model (Qx) into a standardized object model (Q3), where a Q adapter func-

tion transforms a non-object oriented information model into a proprietary (Qx) or standardized object model (Q3).

The mediation device may reside either on the same system hosting the management application, it can be a separate system, or it may be integrated into the systems hosting the managed application.

The term standardization describes the Q3 approach where the managing application as well as the managed agent applications both support a standardized object model.

4. WHERE MULTIVENDOR CAPABILITY CAN BE ACHIEVED

According the ITU-T Recommendation M.3010, multi-vendor-capable management applications can be realized on the element, network, service, and business management layer. Since the amount of information handled by management systems decreases from the bottom of the TMN hierarchy to the top it is easier to implement multivendor-capable management functions in the upper TMN layers than in the lower layers. On the other hand, the larger becomes the effect of multivendor-capable management functions in terms of the reduced number of vendor-specific management systems, the closer they are realized to the network element layer.

5. MULTIVENDOR CAPABILITY AND STANDARDIZATION

Interfaces are always defined by an information model and a communication model. Communication models describe the protocols required for the exchange of information, whereas information models describe the syntax and semantics of the exchanged information.

Multivendor capability based on screen level integration makes use of proprietary communication and information models. Due to the independence of standards, this approach has clear advantages in terms of time to market and it is very easy to implement. It also enables MVC-dependent applications such as centralized alarm surveillance or performance monitoring. The drawback with screen level integration is that it does not allow the automation of operations processes.

Mediation-based MVC makes use of proprietary communication models too. The information model supported by the manager application is standardized, either internationally (Q3) or in a proprietary way (Qx), respectively. Mediation enables process automation. In the case of proprietary standards mediation has as better time to market than standardization-based MVC. The disadvantage is that the introduction of a new type or a new release of a network element always requires the development of new mediation or Q adapter functions.

Standardization-based MVC requires both standardized communication models as well as standardized information models. The advantage of standardized MVC is that the introduction of new network elements does not require additional development efforts and thus allows real vendor independence. The disadvantage of standardized MVC is its dependence on internationally standardized object models.

6. STANDARDIZATION AND TIME TO MARKET

Since standardization-based MVC deploys Q3 interfaces, it is necessary to analyse the shortcomings of Q3 in more detail.

First of all, compared with the other approaches Q3 is very critical in terms of *time to market*. The reason is that OAM standardization up to now has always lagged behind the standardization of technologies. Table 1 shows the gap between technology standards and the associated OAM standards. Due to this delay, the architecture and design of network elements and management systems start in most cases with vendor-specific solutions before associated OAM standards become available.

Table 1. Time gap between technology and OAM related international standards

Technology	Technology standards (first technical standard)	OAM standards* (first management information model)
ATM	1989 (draft)	1994 (draft)
SDH	1987 (draft)	1994 (draft)
GSM	1988 (draft)	1992 (draft)
V5.1	1992	1934 (draft)
SS7	1989	1994

* The dates for OAM standard refer to the first information model, not to the complete OAM information model.

ATM: Asynchronous transfer mode; GSM: Global system for mobile communication (standard for digital cellular mobile radio); SDH: Synchronous digital hierarchy; SS7: Common channel signalling system no. 7

A second shortcoming of Q3 is that it doesn't guarantee *interoperability*, even though most believe that this is the very advantage of Q3. The recommended Q3 communications model, defined in the ITU-T Recommendations Q.811 and Q.812, allows a huge variety of different protocol stacks so that two systems offering a Q3 protocol stack may not be able to communicate with each other. If we consider the Q3 information models the situation is even worse.

The Network Management Forum (NMF) has decided to develop solution sets for selected OAM functions. Solution sets are conglomerates of internationally standardized information models that do not contain any options. These solution sets are more specifications than recommendations and are the only means of guaranteeing "plug and play" interoperability of management systems.

The seeming completeness of TMN standards may lead to unrealistic expectations by standards users regarding the low effort and high interoperability for the implementations of TMN interfaces.

Standardization bodies are focusing on information models for technology management, i. e. element and network management. They currently do not address the management of telecommunications services or operations processes.

Therefore the majority of OAM standards are associated with network and element management. Only a few recommendations are related to the service management and there are no standards covering the business management.

The service management layer (SML) is the level that allows operating companies to differentiate themselves from their competitors. Differentiation is not possible on the element or network management layer (EML/NML).

Since service management is always related to activities where the operator has contact with the customer, the way an operating company manages and provides services makes it different. As a result, the focus of standardization bodies differs greatly from the focus of the operating companies acting in a competitive environment (Fig. 2).

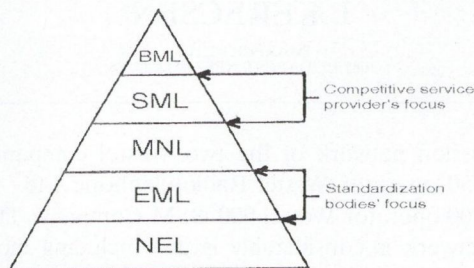


Fig. 2. Management focus of standardization bodies and competitive service providers

BML: Business management layer; EML: Element management layer; NEL: Network element layer; NML: Network management layer; SML: Service management layer

A deficit of the TMN framework is that it focuses only on the architectural model of telecommunications management networks. It does not cover the operations processes that have to be managed by telecommunications service or network, providers, respectively. Different TMN communications and information models describe isolated pieces of the whole TMN framework.

Instead of vertically integrating different TMN layers in a context of a certain operations process, Q3 standards focus on the horizontal integration of different network elements.

There is no doubt that international standards — especially the TMN framework — are important and necessary to promote multivendor capability. But in view of the costs and benefits of MVC it is important to recognize that TMN standards cannot take into account all the specifics of existing networks. There will always be vendor-specific OAM functions that are not modelled by TMN recommendations.

7. NETWORK ELEMENTS AND THE COSTS OF Q3

If we compare the time gap between the emergence of international standards describing a new technology (e. g. SDH) and the release of international standards related to the management of this new technology, we observe that the OAM standards are always delayed by a couple of years.

This means that up to now new technology has to be branded always with proprietary management systems. This is the reason why many operating companies have opted for the introduction of multivendor-capable management systems based on screen level integration or mediation.

With the emergence of internationally standardized management information models operating companies have to decide whether to migrate to a standard-based management system or not. Migration to standard-based management system also requires migration to standard-based network elements. Today, it is becoming more and

more a reality that network elements and management systems can simply be upgraded to a new release to migrate to a standard-based system.

But for a long time operating companies will have to continue managing older equipment they are not ready to replace. For such network elements management systems based on screen level integration or mediation are still needed and will coexist with standard-based ones.

An analysis of the costs and benefits of screen level integration-, mediation-, and standardization-based MVC deployed worldwide by different operating companies, provided the results shown in Fig. 3.

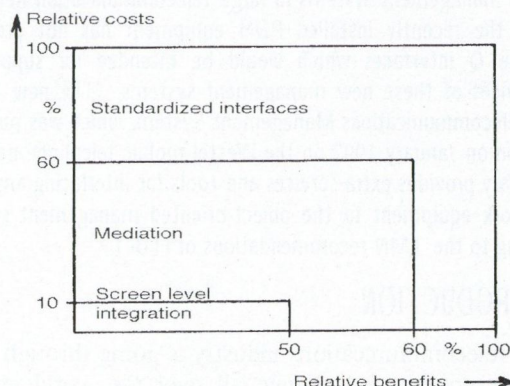


Fig. 3. Costs and benefits

The costs have been measured in system replacement costs, data conversion costs, system integration and process re-engineering work, training costs, and time-to-market.

The benefits have been measured by contribution to process automation, simplification and unification of operations processes, new management capabilities, and the reduction of life cycle costs.

8. CONCLUSIONS BY SIEMENS

Because the described disadvantages of Q3 sometimes force operating companies facing competition to choose alternative approaches to MVC, Siemens supports all approaches to MVC. Siemens TMN applications are object-oriented and are based on internationally standardized information models as far as they are already available today. Where no standard interfaces are available, Siemens uses internal information models and deploys mediation and Q adapter functions to adapt the widest variety of network elements and operation systems to its TMN applications.

Since all Siemens TMN applications are based on a common TMN platform, mediation and Q adapter functions share the same run-time and development environment as the TMN applications. This enables the quick and effective development of new mediation functions and allow them to be freely configured at any point in the TMN framework.

Finally, because of the lack of information models designed to allow standardized service management, Siemens' service management products will make use of mediation and screen level integration as well, in order to provide true multivendor capability.

MXP-2000: AN ACCURATE REALIZATION OF THE TMN CONCEPT

I. GÁLFI

WESTEL RADIOTELEPHONE LTD.
1034 BUDAPESTI, HUSZTI U. 32.

I. KERECSEN

MAXPERT LTD.
1081 BUDAPEST, NPSZNHZ U. 28.

The practical problem of direct applications of the TMN-compliant network management systems in large telecommunication networks is that the recently installed PDH equipment has not provided with the Q interfaces which would be intended for supporting the services of these new management systems. The new MXP-2000 Telecommunications Management System, which was put into operation on January 1997 on the Westel mobile telephone network in Hungary provides extra services and tools for interfacing any type of network equipment to the object-oriented management system according to the TMN recommendations of ITU-T.

1. INTRODUCTION

The telecommunications industry is going through considerable growth and change all over the world and in Hungary too. The rapid extension of mobile telephone services led to rapidly growing country-wide heterogeneous networks operating equipment of several manufacturers and integrating recent and new technologies. Consequently, these networks need comprehensive supervision, control, configuration, maintenance and management systems to provide reliable and cost-effective services for the customers.

The international standardization bodies since the early 1980s have been developing and specifying the collection of standards for managing telecommunications networks. But, the publications of the respective standards, called Telecommunications Management Network (TMN) recommendations, seemed to be late for building into the majority of equipment installed during the last few years. The situation was similar to the management of computer networks. The urgent need of management of fast-growing computer networks in the early 1990s implied the standardization of Simple Network Management Protocol (SNMP) technology, although, the ISO OSI management standards focused on the computer networks too.

To comply with TMN standards as far as possible seems to be the proper strategic decision of network operators, equipment manufacturers and system providers. The new MXP-2000, which was developed during the last two years by Westel Radiotelephone Ltd. and Maxpert Ltd., is trying to be an accurate realization of the comprehensive concept of TMN standards regarding the requirements of applications today.

2. MANAGING TRANSMISSION NETWORKS

At present, the services of MXP-2000 are focused on the transmission part of the telecommunication networks. From that it follows that the first application of the system is intended to operate, maintain and manage the common

transmission network of the two Westel companies: the NMT-450 operator Westel Radiotelephone Ltd. and the GSM-900 operator Westel 900 GSM Company. This common network is considerably large: including more than 700 sites (radio base-stations, repeaters, exchanges, etc.) all over Hungary. The network is a typical heterogeneous, multi-vendor network. Additionally, the MXP-2000 has to provide the supervision, control and management of the whole outstation infrastructure machinery as well, such as fire extinguishers, power supplies and battery chargers, air-conditioners, door-security equipment, etc. on the remote sites.

3. SYSTEM HIERARCHY

The TMN-architectural-model of management services supporting the whole possible activity of network operators places the services on five levels forming a hierarchical system of these services such as: network element level, network element management level, network management level, service management level and business management level.

The physical realization of the first applied MXP-2000 system is shown on Fig 1. The figure shows that the MXP-2000 represented by computers is combined by the EL-90 service network represented by the SME symbols.

The EL-90 is a general purpose, vendor-independent supervisory and control system. This system was designed in 1990, and the Westel network has been equipped by the EL-90 outstation equipment SME since 1991. The EL-90, in fact, is not a TMN compliant system, but its architecture follows the concepts of the early TMN publications. Also, the network function is strictly separated from the supervisory and control functions, its information transmission system follows the ISO OSI layered architecture and the system is able to transmit not only the alarm-status and control information but any type of information. The EL-90 has a personal-computer-based central system operating on either Microsoft DOS or UNIX (Linux) operating systems. The PC-based central system was operating till January 1997 on the Westel network. Besides, the EL-90 has many other applications in Hungary. A 120-station EL-90 system with special PC and Linux-based central system was installed last year which, as an SNMP proxy agent, interfaces the private telecommunication network of the Hungarian Oil and Gas Company to the applied TeMIP management platform of Digital Corporation. The EL-90 system was designed by the Maxpert Ltd., and is manufactured by the Hungarian Elektronika Co-operative Company having ISO 9001 quality certification.

The presence of EL-90 equipment on the networks, on the one hand is a fact we must adapt the MXP-2000 to. On the other hand, the EL-90 has the considerable benefit that through this service network any type of equipment having non-standard interfaces and protocols may be connected to the management system.

The network-element-management and the higher-level

services are realized by the MXP-2000 running on the computer system, as shown on Fig. 1. The MXP-2000 is built on an open systems architecture, enabling solutions to run on different hardware platforms. Native support is implemented for SUN SPARC servers and workstations running on Solaris operating system and personal computers running the Linux operating system.

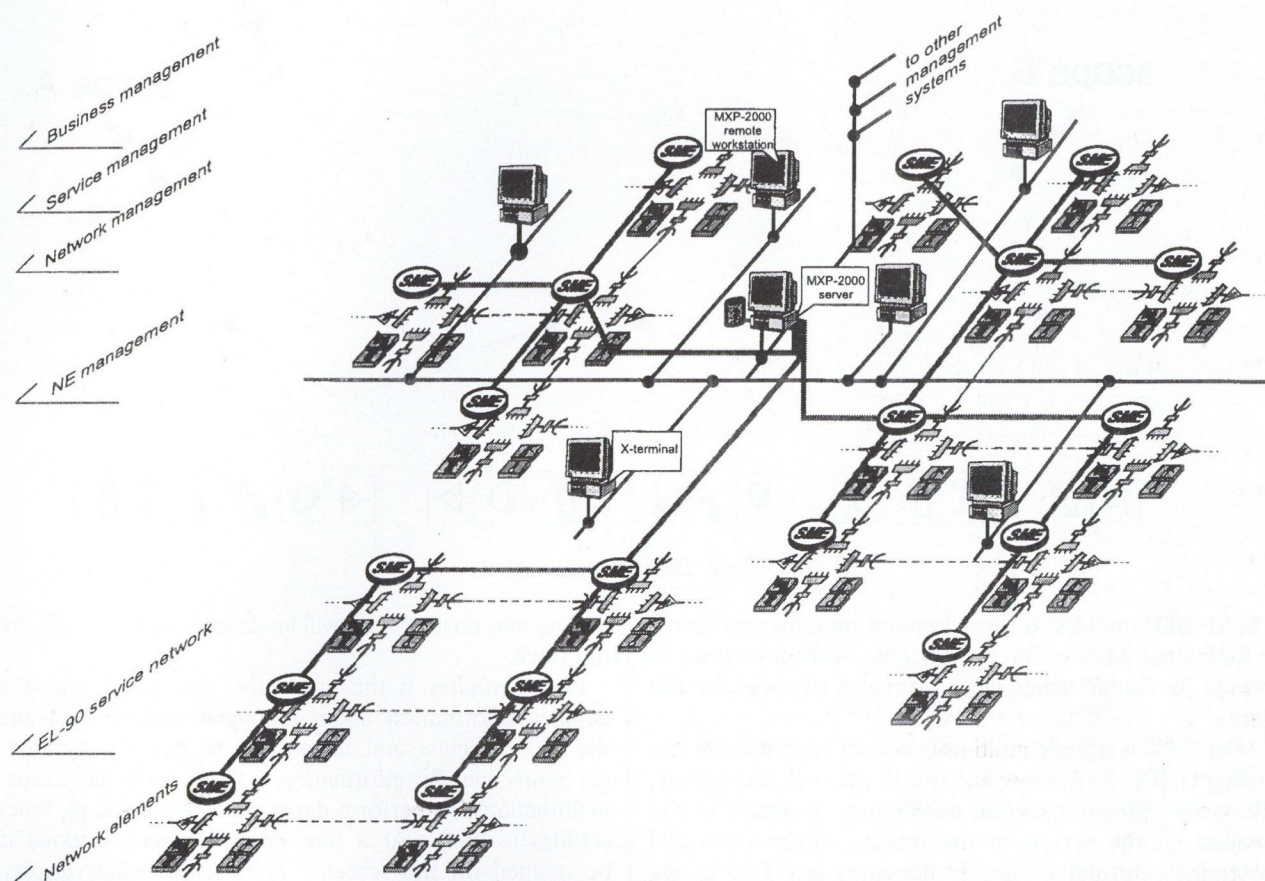


Fig. 1. The physical realization of the management system

Recently, the MXP-2000 framework and the network-element-management-level services such as fault-, performance-, configuration- and security functions have been elaborated, tested and applied. The corresponding pre- and on-line system-configuration modules have been realized as well. The higher-level services are planned to be realized in the near future.

4. OBJECT ORIENTATION

TMN systems management relies heavily on the concepts of object-oriented design. This method is destined for setting order within the heap of network equipment (managed objects) and the associated management services. The managed object classes are the models for managed instances that share similar characteristics. These classes are defined in terms of their attributes, operations that can be performed upon it, notifications that they may emit, and their relationships with other managed objects. A managed object class can be defined for any resource that an organization wishes to monitor and control. Managed objects may represent single resources, structured-

(trail, ring, star) or non-structured sets of single resources and subsets, and so on.

MXP-2000 provides fine object-forming facilities for accurate modelling of telecommunication networks via the above mentioned object-oriented design. Even a very small resource having one or two status-attributes may be represented as individual object. Vertically, MXP-2000 enables many levels of composing complex objects.

On the Westel network approximately 120 simple object classes are currently defined, which represent more than 8,000 resource instances. The vertical structure of the complex objects is currently of up to 10-level.

5. DOMAINS AND SCOPES

In case of large telecommunication networks the selection, association and processing of the management information is influenced not only by the physical system hierarchy, but the actual requirements of the given operation and maintenance organization. Also, people performing different tasks must be provided by different management services.

Fig. 2 shows the example as the infrastructure resources and the transmission resources of the network are managed by the same system. For system experts being responsible for the transmission resources (scope A) we must

provide different services from those for the staff being responsible for the infrastructure of the sites (scope B). At the same time the personnel on duty have to be informed about the whole network (scope C).

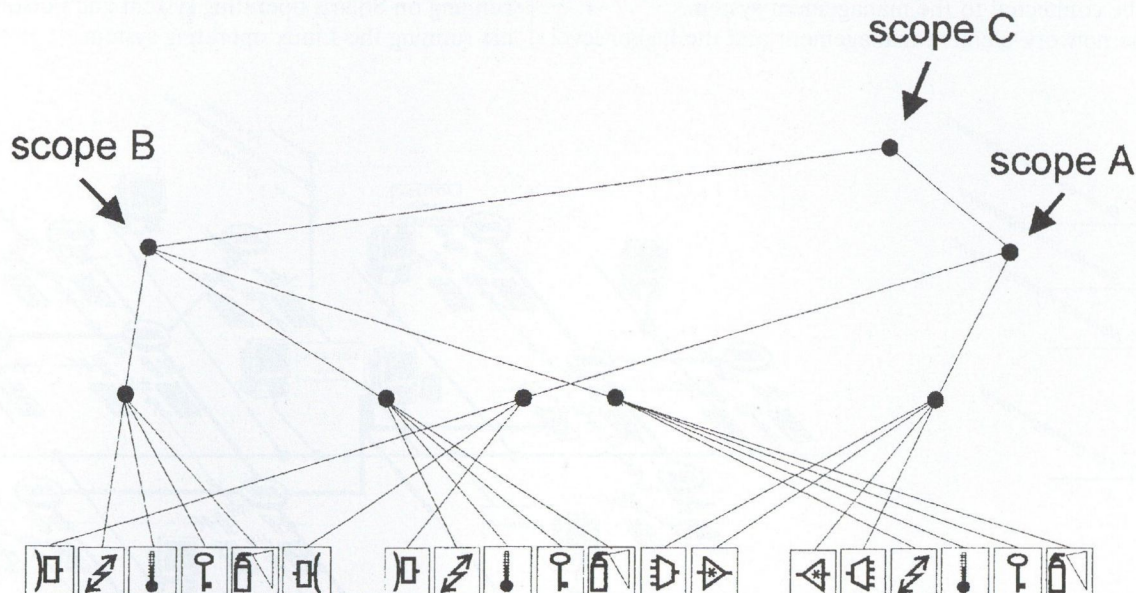


Fig. 2. Domains and scopes

MXP-2000 enables to form domains on either territorial or functional basis within the system. Also, it enables to provide particular management services (scopes) for the users.

MXP-2000 is a fairly multi-user system supported by the applied UNIX, X-Window and the IP network technology. The system provides several possibilities to access to the services: at the server, at the remote workstations and X-terminals through computer networks (see Fig. 1), via dial-in through PSTN, and from the sites through the EL-90 service network.

The users are identified by passwords. Scope and competency belongs to a password. Competency means different rights, such as viewer, operator and configurator. One user may have several passwords. At present, on the Westel network more than 100 users are registered in the system.

6. NETWORK ELEMENT MANAGEMENT

MXP-2000 provides a fairly easy way to handle the network resources and their occasional faults. The design of the services was performed according to the suggestions and the requirements of the organization and the management staff.

MXP-2000 services are realized as X11 OpenLook applications, which are specific for the logged in user's scope and competence. Fig. 3. is a snapshot of the screen holding all information, that helps personnel on duty to solve a management problem.

Fault stack shows the number of pending alarms and the detailed list of objects being in problematic status together with perceived severity. The last object getting into the faulty state appears on the top of the fault stack. Objects

getting into normal state will be deleted automatically from the stack.

Object window is the interactive tool which shows the detailed information about managed objects considering the object's class and helps user to perform actions to get more specific information on the probable cause of malfunctions, to perform direct commands and parameter settings as well. At a time several object windows can be opened on the screen. Peer relationships displayed automatically. Selecting an object having peer relationship the object windows its peer appears automatically on the screen.

For examinations of the long-term behaviour of the managed objects and their attributes are intended the *event log* and the *history-on-calendar* services. History-on-calendar is a graphical tool which in a form of a calendar presents those time intervals while the managed objects were in an abnormal state.

Network map displays the networks and the status of the elements in it. Managed elements are represented by icons of their object class on the map. The colour of the icons shows the actual status information. It can be customised by creating logical domains or views of the network to help the operators' orientation in large networks.

7. CONCLUSIONS

We consider that the TMN concept and the TMN recommendations provided for the MXP-2000 development project very useful guidelines and effective support to realise that perspective management system which will be able to receive the new network management products of the present telecommunication technologies, and the future technologies as well.

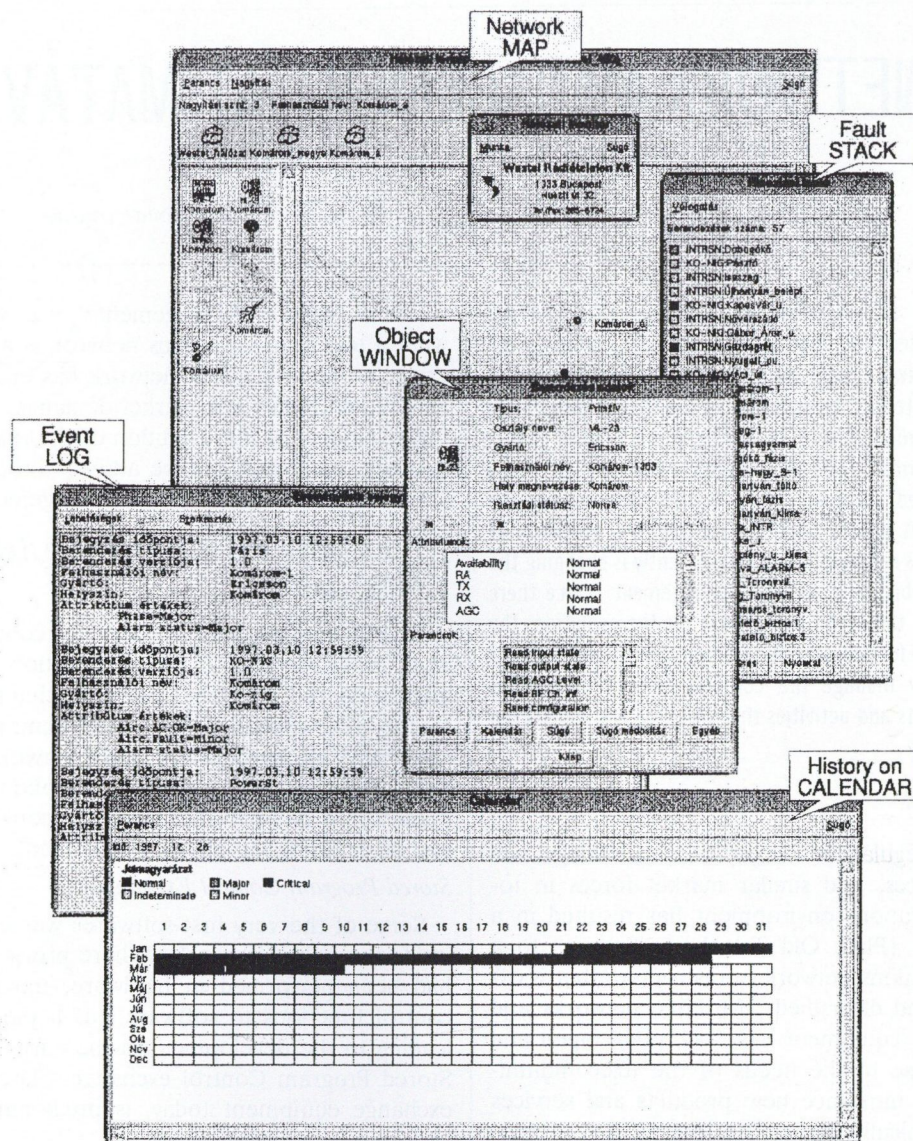
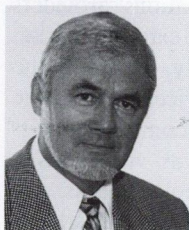


Fig. 3. MXP-2000 NE-management services

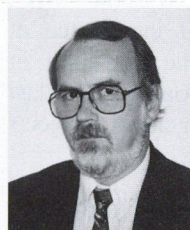
8. ACKNOWLEDGEMENTS

The authors express their acknowledgements to Ferenc Tóth and Zoltán Tesch (Maxpert Ltd.), and György Tóth

(Westel Radiotelephone Ltd.) whose professional dedication and enthusiastic work has contributed to the rapid realization and application of MXP-2000.



István Gálfi graduated in 1970 at the Faculty of Electrical Engineering of the Technical University of Budapest. He received Dr. Univ. degree in 1977. He started his career at the Microwave Department of the Faculty of Electrical Engineering. His main activities were related to microwave telecommunications, measuring systems and instruments. In 1994 he joined Westel Radiotelephone Ltd. He was responsible for operation and maintenance of the radio base-stations and the transmission networks of both Westel companies. He is currently the technical director of the Westel Radiotelephone Ltd.



István Kerecsen graduated in 1973 at the Faculty of Electrical Engineering of the Technical University of Budapest. Till 1991 he had been working at the Research Institute for Telecommunications in the field of microwave systems development, especially for supervisory, control and protection systems. In 1991 he founded the Maxpert Ltd., and since then he has been managing this firm as executive director. The main activity of Maxpert relates to developing, producing and providing supervisory, control and management systems for telecommunications applications.

NETWORK MANAGEMENT AT MATÁV

R. ANDERSON and J. WIENER

HUNGARIAN TELECOMMUNICATIONS COMPANY, MATÁV
MANAGEMENT SYSTEMS DEPARTMENT OF THE OPERATION AND MAINTENANCE DIRECTORATE
H-1541 BUDAPEST

The article describes the projects and activities that MATÁV has undertaken to effectively manage the complex, multi-vendor telecommunications network that is being deployed within Hungary. It first provides a brief history of the evolution of the telecommunication network, from the introduction of Stored Program Control (SPC) exchanges to the current MATÁV network consisting of many diverse and interrelated networks. The article then reviews the technology and market drivers that are causing the evolution of the telecommunications network, which subsequently is changing the definition and responsibilities of network management. Once there is an understanding of the cause and drivers for the evolution, the article reviews the need for new standards-based Operational Support Systems to effectively manage the complex telecommunications network and the projects and activities that MATÁV has undertaken to meet these needs.

1. INTRODUCTION

Privatization, deregulation, competition, technology, new products and services, and similar market forces in today's telecommunications environment has resulted in a shift from a POTS (Plain Old Telephone Service) to a new telecommunications network infrastructure that is extremely complex and diversified. Multiple networks and telecommunications equipment have been developed and deployed in response to the needs of the telecommunications provider to introduce new products and services quickly and economically, reduce the overall cost of providing service, improve customer satisfaction, and to meet the diversified needs of the market place. As a result, the role of Telecommunications Network Management has evolved from managing a simple, hardware-driven, single network to managing a complex variety of networks that are software-driven, supporting different products and services utilizing proprietary environments.

MATÁV, a leading telecommunication service provider of the region, understood the importance of the new management principles, and started projects to deploy its own intelligent, state-of-art management system(s). The system(s) will be based on the TMN (Telecommunication Management Network) principles of ITU-T.

The intention of this article is first to show 'What is Network Management' and how is it interpreted at MATÁV. Second, the article explains the principles of TMN, shows possible and practical approaches, and last presents some selected Network Management projects within MATÁV.

2. EVOLUTION OF THE TELECOMMUNICATIONS NETWORK

In order to answer the question, 'What is Telecommu-

nications Network Management?', it is best to review first what a telecommunications network is and how the modern telecommunications network has evolved to meet the new requirements and market demands. Once there is an understanding of the evolution of the telecommunications network, only then can we answer the question 'What is Telecommunications Network Management?'.

2.1. Exchange and Inter-Exchange Telecommunications Network

The evolution of the modern telecommunications network really starts with the introduction of the computer and the Stored Program Control Exchanges (SPCs). Prior to the SPC exchange, the telecommunications network was a physical, hardware provided network with limited capabilities, other than processing telephone calls. Telecommunications Network Management consisted of installing and maintaining the physical equipment.

Stored Program Control Exchanges

Some of the very first softwares was developed for use inside the public network. Where previously all functions had been performed in hardware, moving some of the control functions to software was a pioneering advance, leading to the development in the early 1960s of the first Stored Program Control exchange. The development of exchange equipment today, is predominately a software endeavor.

With the growth in the volume of telecommunication traffic, the increase in the mobility of the users of the telecommunications network, and the introduction and use of new services being offered, telecommunications providers were pressured to determine new and better ways to handle the telecommunications traffic. Taking advantage of the advances in computer technology and the SPC exchanges, the telecommunications providers started layering the telecommunications network: local exchanges for local traffic, Tandem (Secondary) exchanges for inter-connecting the local exchanges, and gateways (both local and international) for traffic outside of the telecommunications providers network.

During this period, the telecommunications providers were starting to feel the pressure from the external market to reduce expenses, improve profitability, improve the reliability of the service and offer new services to meet the needs of the customers. The layered-telecommunications network, utilizing the SPC exchanges was viewed as a major obstacle in meeting these new requirements and market demands. The SPC exchanges were costly to purchase and maintain, the cost and time it took to introduce new features was enormous, and the proprietary software platforms restricted the introduction of new

services. This problem was realized as early as the 1970s, and the idea of separating the control of calls from the transport and the development of new services in a separate computer was born. As telephone service providers realized that they needed to deliver new features and functionality quickly and economically to maintain and grow their customer base, the industry began developing a more unified and open approach — the Advanced Intelligent Network.

Advanced Intelligent Network

The Advanced Intelligent Network provides a standards-based network architecture enabling the network operator to rapidly deploy new services to meet its customers' needs, while providing the capability to increase the volume of traffic over the existing telecommunications network. The Advance Intelligent Network is a layered-architecture, consisting of: Service Switching Points (SSPs): Service Transfer Points (STPs): Service Control Points (SCPs): and eventually, Service Management Points (SMPs), and Service Creation Environment Points (SCEPs) for the in-

troducton of new services. The Advance Intelligent Network introduced an additional layer of telecommunication equipment and software that needed to be integrated into the already existing network, further increasing the complexity of Telecommunications Network Management (Fig. 1).

In addition to the Public Switched Telephone Network (PSTN) and the Advanced Intelligent Network described above, other networks were developing and be implemented that required integration into the basic telecommunications network: Telex Network, Public Packet Switched Network, Data Communications Network, Mobile Telephone Network, Satellite Network, and the Internet Network. In the near future, the Cable TV, Video On Demand (VOD), and Multi-Media networks will be introduced and require integration into the basic telecommunications network. These additional networks were developed and implemented during different time-frames, utilizing different technology, different hardware and software, and requiring different Telecommunications Network Management.

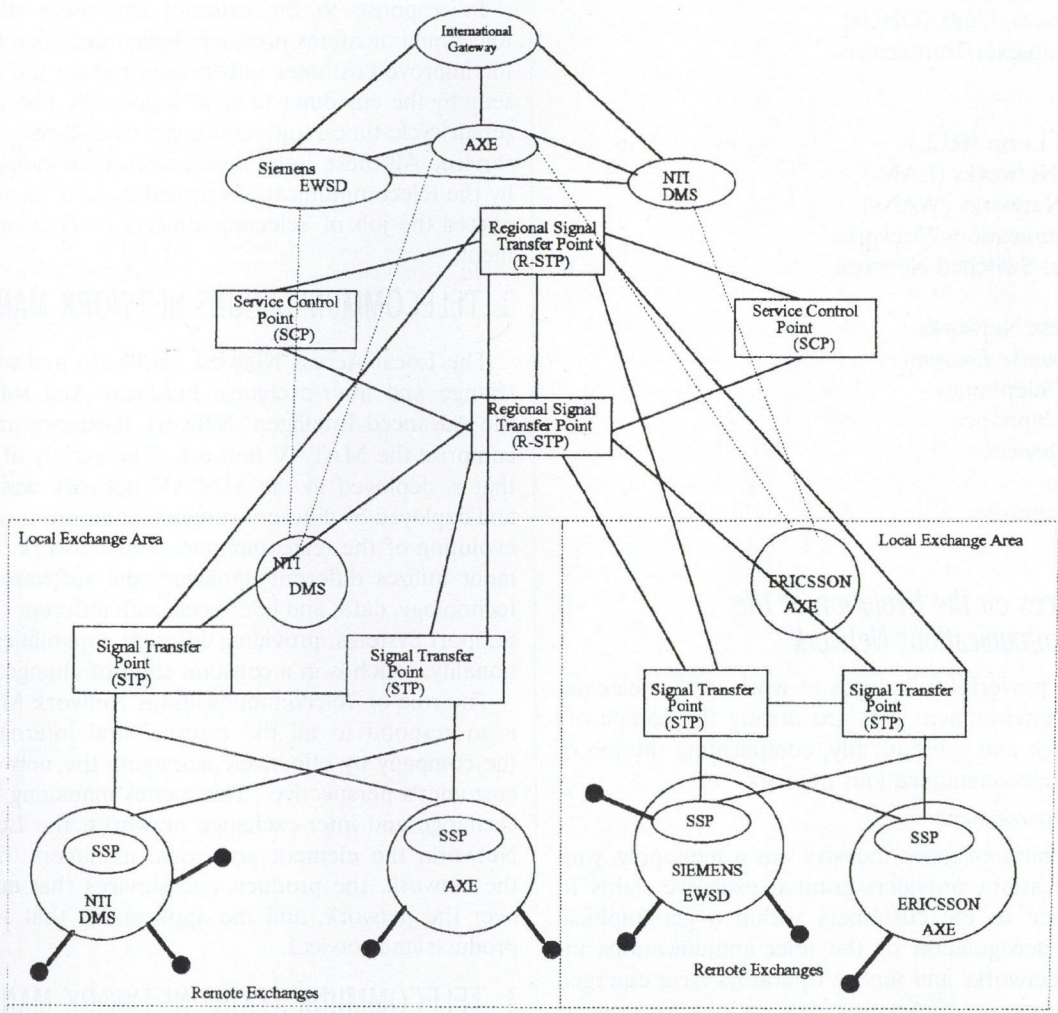


Fig. 1. HTC Network — exchanges and CCS

2.2. Local Access Network

The Local Access Network is defined as the telecommunications software and hardware which provides the customer access to the exchanges and the Public Switched Telephone Network (PSTN). The categories, types, and capabilities of equipment that make-up the Local Access Network is so varied that it would not be of benefit to describe each of these networks and equipment. In order to provide at least a basic understanding of the Local Access Network and its' complexity, the following is a list of the basic categories of equipment involved:

Cables

Lead

PIC

Twisted-Pair

Fibre

Network Equipment

PCM

Digital Loop Carrier (DLC)

Multiplexers

Digital Cross-Connect Systems

Channel Banks

Optical Network Units (ONUs)

Optical Multiplexer/Transceivers

Networks

Telephony

Radio Local Loop (RLL)

Local Area Networks (LANs)

Wide Area Networks (WANs)

Data Communications Networks

Public Packet Switched Network

PDH/SDH

Optical Access Networks

Customer Premise Equipment

Single-Line Telephones

Multi-line Telephones

Answering Devices

Fax Machines

Personal Computers

PBXs, etc.

2.3. Influences on the Evolution of the Telecommunications Network

There are powerful influences at work in the telecommunications environment that are driving the complexity of the network and subsequently, complicating the job of managing a telecommunications network.

Regulatory Environment

The telecommunications industry was a monopoly, with telecommunications providers granted exclusive rights to provide service to the customers within a geographical area. With deregulation of the telecommunications industry, new networks and service operators have emerged causing telecommunications providers to look for ways to meet the needs of the market place, increase revenues, while reducing the cost of providing service.

Effects of New Technology

The telecommunications industry has been the most attractive industry in the world, representing approximately

6 % of the Gross World Product in 1994. Combining this fact with the deregulation of the telecommunications industry, new technology is being developed and deployed to attempt to capture a part of the potential market that exists. The different technologies translate to a number of different networks and/or sub-networks that are overlapping, inter-working, or stand-alone.

New Products and Services

New services are being invented and introduced at a much faster pace than in the past. In some cases, the services are related to a technology. In other cases, the technology provides a substantial new capability which is exploited to offer a wide variety of services, driven directly by the market place. In either case, the telecommunications provider is driven to offer new services quickly and in a cost-effective manner in order to compete in the market place.

Rising Customer Expectations

Customers have increasingly come to expect reliable service, restored quickly in the event that it breaks down or degrades.

In response to the external influences stated above, telecommunications providers have intensified their efforts to: improve customer satisfaction, reduce the defect rates seen by the customer to zero, reduce the provisioning and repair cycle-times, and reduce the overall cost of providing service. All these influences and corresponding responses by the telecommunications providers have significantly impacted the job of Telecommunications Network Management.

3. TELECOMMUNICATIONS NETWORK MANAGEMENT

The Local Access Network hardware and software, exchange and inter-exchange hardware and software, and the Advanced Intelligent Network hardware and software comprise the MATÁV network. The variety of equipment that is deployed in the MATÁV network was developed and deployed by different vendors, at different stages of the evolution of the telecommunications network. The equipment utilizes different hardware and software platforms, technology, data, and interfaces, with different Operational Support Systems, providing different capabilities and functionality, which is in a constant state of change.

The role of Telecommunications Network Management is to respond to all the external and internal needs of the company by effectively managing the network from a customer's perspective. This means managing the diverse exchange and inter-exchange networks, the Local Access Network, the element and nodal managers that support the network, the products and services that are provided over the network, and the applications that support the products and services.

4. TELECOMMUNICATIONS NETWORK MANAGEMENT OPERATIONAL SUPPORT SYSTEM

In order for MATÁV to meet the requirements of effectively managing the telecommunications network that has evolved, MATÁV is required to move from managing the networks and sub-networks independently and from

a geographical point-of-view, to managing the networks from an end-to-end customer perspective, regardless of the network and sub-networks that are involved in providing the customer's service. In order to accomplish this, the organization that is required to manage the telecommunications network requires the necessary tools to manage the diversity of equipment in the network and the overwhelming amount of data that is generated. A modern network management Operational Support System (OSS) is required that provides the ability to inter-operate with other OSSs to rapidly detect and resolve service-affecting events and service degradation problems before the customer is even aware that a problem exist.

4.1. System Description

The evolving full service network requires an advanced network Management Operations Support System that exceeds the limited characteristics of the current legacy systems. What is needed is a new generation of layered, 'open' OSSs that can support rapid service deployment, easy customization and process simplification. Important characteristics of the new Telecommunications Network Management OS that MATÁV is in the process of selecting include: layered distribution of operations functionality, separation of operations data from operations functionality, rapid customization capabilities, and practical standards implementation.

Layered Distribution of Operations Functionality

Layer architectures logically partition the operations of network elements from network-wide and service-specific operations functions, helping to insulate the services management from changes in network technology or equipment suppliers. More significantly, these architectures allow increased flexibility and speed in introducing and managing new services over a hybrid network infrastructure.

In support of layered, open-operations architectures, national and international standards bodies have defined the Telecommunications Management Network (TMN) model and interface standards. The TMN model consists of five layers: Element, Element Management, Network Management, Service Management, and Business Management. At the two lower layers, the TMN model is implemented so that individual network elements are managed by individual element management systems (Fig. 2). Element management systems typically are grouped with corresponding network elements, reflecting the current business environment in which network element vendors often supply proprietary element management systems with their products.

A growing trend called 'Domain Management', provides integrated management over all network elements that make up a single common sub-network or domain (SDH, Optical Access Network, exchanges, etc.) regardless of the network element supplier (Fig. 3). Domain Management allows integrated management of all these devices by augmenting the individual element management layer operations in a sub-network with a common set of sub-network wide functions. The Domain Manager then can present a single interface to higher network management-layer OSS.

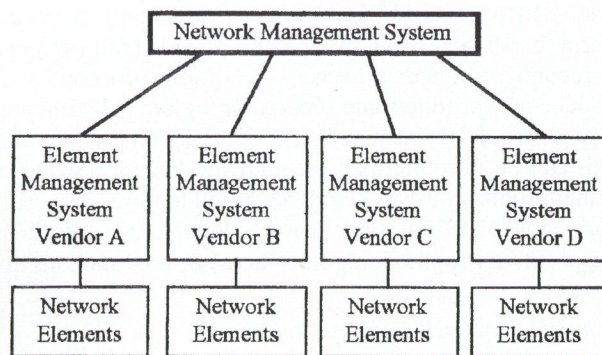


Fig. 2. Basic TMN Model

Separation of Operations Data from Operations Functionality

In order to provide maximum flexibility, it is important to increase the accessibility of corporate data. Ideally, OSS applications should be able to access data independent of its format or location. This is especially true of network management OSS applications that are required to deal with a multi-vendor environments. Without associating data with specific operations functionality, complex legacy-style process flows can be avoided, allowing greater flexibility in adding and customizing new services.

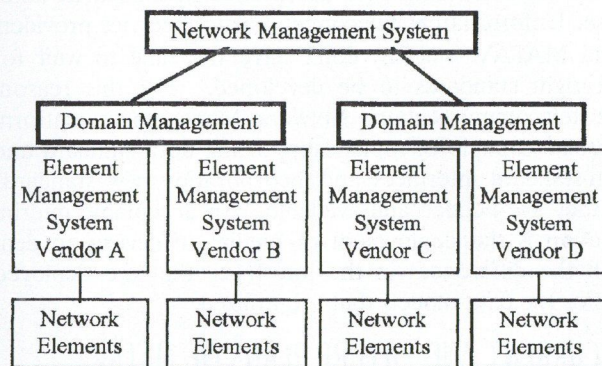


Fig. 3. Domain Management Approach

Rapid Customization Capabilities

The Telecommunications Network Management platform must support rapid development, prototyping, and customization capabilities for two important reasons: network technologies continue to change, and MATÁV requires custom operations capabilities to meet the unique competitive needs. As new trends continue, the need to manage new services quickly and uniquely will continue to drive the demand for rapid OSS application development and customization. In a rapidly changing industry with increased competition, MATÁV cannot afford legacy-style OSS development environment. With legacy-style OSS development environments, by the time the OSS is actually deployed, the needs will have changed and the system obsolete.

Not only should OSS suppliers have the ability to rapidly implement and reconfigure operations applications themselves, they should ideally be able to provide the capabilities to MATÁV. The Telecommunications Network Management OSS must be designed with a degree of 'open-

ness' that permits MATÁV to do more than just change alarm thresholds. MATÁV must be provided the capability to reconfigure major aspects of operations procedures, introduce new products and services, integrate new functionality, and support new network elements and technology. This can be accomplished through the licensing of development toolkits, use of standards-based hardware and software, and platforms that provide documented interfaces (Application Programming Interfaces) to the functions and services.

Practical Standards Implementation

As new OSSs are developed, attention is being given to industry standards. But in the evolving telecommunications industry, it is just as important to understand the current limits of standards as it is to continue to incorporate them. Interface standards generally consist of a set of communications protocols, communications services, and an object model defining the scope of the information that can be exchanged between managed and managing systems. But standard object models define only the behavior of individual components and functions modeled in a system. Simply loading a generic object model into a standards-compliant OSS does not automatically allow that OSS to manage the modeled system, it merely ensures that the OSS and managed system can communicate.

The establishment and acceptance of standards takes time. Unfortunately, telecommunications service providers (and MATÁV is such) don't have the time to wait for the right standards to be developed. For this reason, the Telecommunications Network Management platform must be capable of rapidly supporting both standard and non-standard interfaces and incorporating new standards as they are needed and available. An acceptable interim solution is the deployment of mediation devices to deal with the differences in the interfaces that are deployed and/or the data models that are utilized.

5. CURRENT AND FUTURE PLANS OF MATÁV

The questions are: how to deploy TMN-based OSS systems in the rapidly evolving environment at MATÁV; how to evolve the existing telecommunication equipment; how to provide smooth present and future interworking with the new management systems and services; and how to overcome the problem of missing standards, lack of willingness of vendors to cooperate, etc. What strategy shall be followed in order to reach a consolidated TMN solution in a limited timeframe, and with limited resources?

The basic concept has been shown in the previous chapters. In this concept Element Managers are critical issues. Integrating existing systems will be done by the help of EMs. Also, new technologies and systems are always introduced together with their EMs. Unfortunately, EMs have different functionalities, and their interfaces are often proprietary. The EMs are never hard-coded but software-driven, which facilitates easy (but not inexpensive) implementation of standard interfaces in a new EM software version.

It seems to be attractive to establish an "integrated" OSS, which includes all technologies, both switching and transmission, Advanced Intelligent Networks, Access Networks, ATM, Frame Relay, etc., covering each level of the

network. However, with the present technology and the state of standardization, this would take an extremely long time and would require a huge investment. And, while developing and deploying an integrated OSS, new technologies and services would need to be introduced, causing the whole process of integration to start again...

Utilization of Element Managers allows several developments and deployments to run parallel, almost independently - but always keeping in mind interfacing to other systems. If a Element Manager fails, it has a relatively small impact on other parts of a company-wide system.

5.1. PDH transmission

According to several opinions, PDH transmission should not be included in a NM system, because PDH is too primitive and will be replaced in the future with SDH.

However, PDH will probably survive for an additional 10–15 years. No doubt that it's role will decrease, but will serve MATÁV for years. There are several cases where the possible flexibility and additional services of SDH are not needed, and the transmission system needed will only be required to transmit signals from the input to output, as is the case of PDH. As long as PDH is in the network, it requires management and integration. The question is, what kind, and what level of management is required? Since PDH usually does not have any (or has only limited) possibility for configuration management, only alarm management can be and shall be realized with a moderate cost. This means collecting alarms in the form they are available (sometimes only from relay output), transfer them to the management centre where processing can be performed. This gives the chance — together with a sophisticated work flow control — to send "the right person at the right time to the right place". If the maintenance staff knows both the actual state of the PDH and SDH network as well as the available free resources, they can distinguish and select the best solution (this is the essence of NM, is it not?): the maintenance staff may:

- send somebody to repair the faulty equipment;
- provide some capacity from the available SDH free capacity and schedule the required repair activity;
- introduce some limitations in the traffic until repair happens;
- do nothing; etc.

The devices performing this kind of alarm monitoring, can be considered as special Element Managers with limited functionality.

Another aspect of NM is Performance Monitoring (PM) according to ITU-T rec. G.821 and G.826. PM can be performed (there are monitoring systems available for this task) for PDH, as well as SDH, but the solution for PDH is expensive, and will only be used in exceptional cases.

An additional issue is, if the PDH management shall be integrated with SDH management, or not. According to our present knowledge, this seems to be uneconomical, and needs more investigation.

In summary, we can say, that PDH transmission will be managed by Element Managers with limited functionalities. Further integration is possible (Standard Q3 interface is available), but not likely.

5.2. SDH transmission

MATÁV has completed the system selection for SDH transmission network. When specifying the SDH systems in the tender, MATÁV placed great emphasis on its management system. Not only SDH equipment, but also Element Managers were purchased. Presently, the SDH equipment has one type of EM, and another type of EM for managing DXCs (Digital Cross Connects).

A SDH-EM is able to manage not only its NEs as individual equipment, but has also some capabilities to manage trails in a subnetwork formed by its own NEs (if the trail does not pass through a DXC). One SDH-EM can not manage all the SDH equipment of MATÁV (due to the limitations of processing power), but a central Work Station can be connected to several SDH-NEs simultaneously, and an operator can work with the entire SDH network from one screen.

DXCs have their own EMs. One DXC-EM is able to manage all the DXCs presently existing at MATÁV. The central DXC-EM is located in the same room, as the central Workstation of the SDH-EMs, which facilitates a fast and effective "human-human Q3 interface" between the operators of the two systems. This is obviously not the final solution. After a short consolidation period, MATÁV will continue with the integration of the existing systems. We will integrate SDH-EMs and DXC-EMs of the same subnetwork under the control of Domain Managers (Fig. 3), with high-level integration being performed via the Domain Managers and Element Managers. The Domain Managers will interwork via Q3 interfaces.

5.3. Switch management

After careful study of the state-of-the-art network management solutions, MATÁV decided to start a project for establishing a network management system for its switches. This system is referred to as the SNOMS (Switch Related Network Operations and Management System). One important goal of the project to select a common management platform not only for switch management, but also for future management applications.

The organization utilizing SNOMS will have two main management centres with other functional units established for performing specific functions, as depicted in Fig. 4 showing the physical architecture.

- The SAMAC (Switch Alarm Monitoring and Analysis Center) will continuously monitor the switches, analyse alarms, perform actions and tests if required, configure the switch, etc. They are responsible for all activities related to the network elements (switches), with the exception of dynamically changing the network for Network Traffic Management.
- The CTSC (Central Technical Support Centre) is co-located with the SAMAC. They have access to the entire SNOMS, and take over problem handling, if the other responsible users are not able to solve a problem.
- The SNMC (Switched Network Management Centre) is more than 100 kilometres away from the SAMAC/CTSC. It consists of two main parts:
 - The NTMC (Network Traffic Management Centre) shall provide maximal flow of traffic which is possible

under the actual situation in order to generate maximal revenue for MATÁV. NTMC will have the tools to monitor the network, and to take the necessary control actions. Pre-planned actions, scheduled and ad-hoc actions will also be available.

- The SS7MC (Signalling System 7 Management Centre) will be part of the SNMC, and will have the responsibility for the CCS7 network of MATÁV.

Though the overall purpose is to establish centralized support of the work, some distribution of functions are also possible. Regional Management Centres (RMC) will be established. SAMAC and RMCs will be able to perform the same task with the exception that a RMC can manage only its (geographic) area, while the SAMAC will manage the whole network. Distribution of functions will be controlled by SAMAC by the help of the security system.

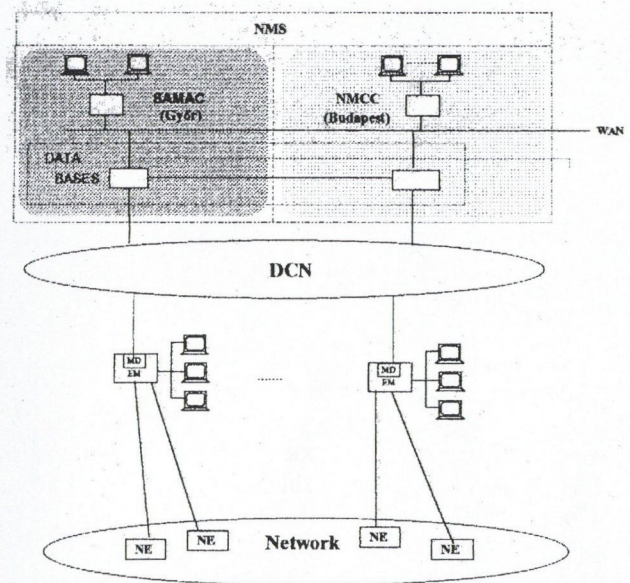


Fig. 4. Physical architecture of the NOMS

There are several management categories which can be and shall be realized in such a system. In the SNOMS, all functions are distributed, and none of the management categories can be associated with a single center. Fault and Alarm Management is performed by all centres: SAMAC receives alarms from the switches (Alarm Management for the Network Elements); NTMC is responsible for network-wide (Traffic-generated) alarms, and SS7MC will handle the SS7 network triggered alarms.

Configuration management is also distributed between the centres: SAMAC changes the configuration of the switches (Static changes); NTMC can apply controls by changing the switches (dynamic changes) and SS7M controls the configuration of the SS7 network.

Performance Management is implemented only at the Performance Monitoring level. Again, this is also distributed amongst parts of the system. Results of monitoring are either utilized for management (e.g. initialising control actions) or stored for further post-processing.

Security Management is used to control user access. Different users have access to different parts of the man-

aged network, and can perform different functions. This is realized on the basis of two main concepts: forming management domains and defining their operations context.

Availability of the system is not a TMN question, but is a critical issue. Usually vendors offer so called fault tolerant computers to provide the required availability. However, fault tolerant computers, disk mirroring, etc. are only one issue in providing high availability systems. Other — and perhaps more important — point is the architecture and topology. In the SNOMS, the SAMAC and SNMC are located in different towns, and will be able to take over the work of the other side in the case of emergency. Also, the distributed architecture with the RMCs (and their associated Element Managers) increase the availability. Should anything happen to both centralized sides of the SNOMS, the RMCs are able to control their area at the Element Management level without any limitations.



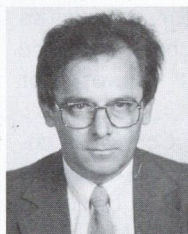
Roy Anderson received his Bachelor of Arts from Indiana University in 1977. He joined Indiana Bell Telephone Company (now part of Ameritech Corporation) in 1974. From 1974 to 1995, he held numerous jobs in Commercial and Operations and Maintenance. Prior to accepting a position with Ameritech International (MagyarCom) and relocating to Budapest in 1995, he was responsible for the estab-

lishment of the Work and Force Management, Testing, and Network Management systems at Ameritech. Currently, his primary responsibility is the establishment of a Work and Force Management and Testing platform in MATÁV and Network Management.

6. CONCLUSIONS

Needs of new services, faster customer service, rapidly changing technology, economic operation of the telecom network and several other factors led to dramatically new requirements against the management of the network. In order to meet these new requirements, the concept of TMN was formulated. TMN means a new approach to the management systems, which was explained in this paper. Several practical considerations were also made showing how to overcome the problems of missing standards and limitations of the presently available system.

The existing telecommunication infrastructure (transmission and switching) represent a great value, which can be expressed in billions of dollars. Since replacing takes time and a lot of cost, introducing the new management concept shall be performed in phases. MATÁV is in the initial phases of creating the new network management infrastructure that will effectively manage the network and provide the highest level of service to its customers.



József Wiener received his M. S. degree in Telecommunications from the Technical University of Budapest in 1976, then the Ph.D in 1989. He joined the Research Institute of the Hungarian PTT (PKI) in 1976. He participated in the introduction of new technologies both in transmission and switch. He made several studies and performed developments on the field of supervisory systems. In 1992, he joined

the newly formed Operation and Maintenance Directorate of MATÁV. His latest work was to conduct the tendering and evaluation process of the Switched Network Operations and Management System. Now he is heading the Management Systems Department of the Operation and Maintenance Directorate, and is responsible for the introduction of management systems.

PROTOS NETWORK MANAGEMENT SYSTEM AT DEUTSCHE TELEKOM

Introduction

PROTOS is an operating system for remote control and monitoring of transmission networks.

In conjunction with controllable network elements, PROTOS provides network operators with the following advantages:

- fast and flexible provision of connections,
- monitoring of their quality and availability,
- restoration in case of failures and quality impairments,
- information regarding network capacity, usage and availability,
- effective resources management.

PROTOS is a non-proprietary management system. It supports the TMN standards of ITU-T Recommendation M.3010.

PROTOS manages the controllable network elements of different manufacturers, via an open interface (Q3).

PROTOS is used by Deutsche Telekom for remote control and monitoring of the company's NKÜ 2000 (DXC 4/1) network nodes.

The PROTOS software was developed in accordance with Deutsche Telekom's technical concept, in close cooperation with Siemens-Nixdorf.

Requirements and technologies of a modern transport network

Existing and future telecommunications services are placing, and will place, more and more demanding requirements on transport networks. Among the significant aspects of such requirements are the quality, provisioning times and fault-clearance periods of the transmission paths used.

The technology for meeting such requirements is SDH transmission technology. It permits flexible monitoring of, and direct access to, digital signals with different bit rates. For some years, equipment employing this technology has increasingly been used in the transport network. SDH also is the transport infrastructure for a future ATM network.

The NKÜ 2000 synchronous transport network

Deutsche Telekom's transport network uses very high-performance synchronous network elements, the NKÜ 2000 network nodes produced by the Siemens/Philips and ALCA-TEL-SEL/Bosch Telecom manufacturer consortia. They offer the following functions:

- switching of digital signal connections with 140 Mbit/s, 34 Mbit/s and 2 Mbit/s bit rates, plesiochronously and synchronously within the 155 Mbit/s frame,
- integrated multiplexing between the switching layers,

- conversion of PDH signals into SDH signals and vice-versa,
- continuous monitoring of connections,
- provision of protected connections with automatic restoration,
- provision of uni- and bi-directional connections.

Network management interface

The NKÜ 2000 can be controlled remotely and monitored through a network management interface. The network management interface is based on the ITU and ETSI standardization bodies' international recommendations for Q3 interfaces. This interface was specified and successfully implemented by Deutsche Telekom, in cooperation with the manufacturers of the NKÜ 2000.

The Q3 interface comprises a standardized protocol stack in keeping with the OSI seven-layer model. The elements used in the application layer include CMISE, which provides services for manager-agent interaction. On top of this layer, the Q3 interface contains an infomodel. In it, the management view of the physical resources is described in object-oriented fashion, with the help of managed objects. In the NKÜ 2000 (agent), all of the managed objects are kept within the management information base; the manager can modify them by changing attribute values and object instances. The agent within the NKÜ 2000 provides the manager with information regarding status changes in resources.

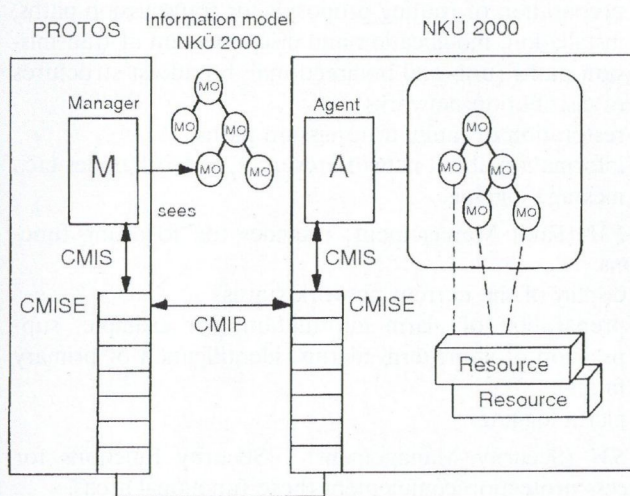


Fig. 1. Principle of the Q3 adapter

The PROTOS network management system

The PROTOS network management system is an operating system (OS) within the meaning of ITU Recommendation M.3010 for a TMN; it controls and monitors the NKÜ 2000. It was developed in close cooperation between Deutsche Telekom and Siemens/Nixdorf. Communications between the components of the TMN take place via a data communication network (DCN) on an X.25 bases. Users work with the system via graphic user interfaces on workstations.

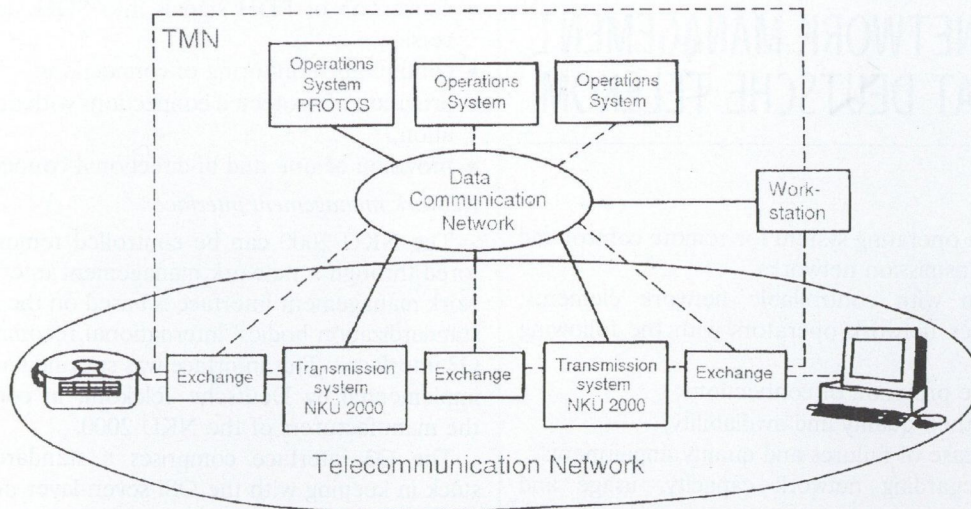


Fig. 2. Relationship between PROTOS and NKÜ 2000

Functionalities

The functionalities of PROTOS can be divided, pursuant to X.700, into the following functional areas:

CM (Configuration Management) permits configuration of a complete network on the basis of available resources. It comprises the following functions:

- installation, modification and expansion of an SDH transport network,
- preparation of routing proposals for transmission paths,
- installation, modification and disconnection of transmission paths (uni- and bi-directional; broadcast structures of distribution networks),
- restoration of faulty transmission paths,
- information about network reserves, network nodes etc.,
- message logging.

FM (Fault Management) provides the following functions:

- display of the current network status,
- preparation of alarm information (for example, suppression of short-term alarms, identification of primary faults),
- alarm logging.

SM (Security Management). Security functions for access protection complement these functional areas.

Architecture

The PROTOS architecture is a client/server architecture that permits distribution of components within the network. The operating system is divided into three levels, pursuant to M.3010. Each level functions simultaneously as a client and as a server, and as manager and agent (layered client/server architecture).

• Network element level

This level knows the objects within the network elements that represent the physical world and that communicate with the local element managers within the network element via the Q3 interface. The local managers within the NE function as agents for the element manager in the OS. In its role as agent, the element

manager communicates with network-level managers.

• Network level

This level knows logical objects of the network such as traffic relations, transmission paths, circuits, time slots (channels), and routes. The network manager uses the services of the element manager to control and administer network-level objects. It communicates, as an agent, with the service manager. Network managers can be duplicated; each duplicate can separately administer and control a subnetwork.

• Service level

This level administers logical objects such as customers and transmission services provided, including the relevant orders required.

Hardware

The PROTOS hardware consists of the following components:

- high-availability computer for the OS, with a database system and DCN accesses: Siemens Nixdorf RM600,
- workstation for presentation and control: Siemens Nixdorf RM200,
- communications network between WS and OS: Ethernet LAN.

The PROTOS workstations provide the user with a graphic user interface that was developed on the basis of OSF/Motif.

Use of PROTOS by Deutsche Telekom

Deutsche Telekom has been using the PROTOS system since early September 1995. For this purpose, a PROTOS switching center was established in Düsseldorf; from it, all NKÜ 2000 (currently about 80) can be controlled and monitored via a highly available DCN. Remote workstations have been provided within the International Transmission Center in Frankfurt a. M. (WN-ITC) for control of all international transmission paths.

DEUTSCHE TELEKOM, Trier



telescon[®] 97

BUDAPEST



Between the eighteenth and nineteenth International Telecommunications Energy Conference a Telecommunications Energy Special Conference **Telescon '97** will be held at Thermal Hotel Hévia in **Budapest**, beginning April 22, 1997 and ending on April 24, 1997. The motto for telescon '97 : **East and West grow together**

Scope of the conference

Telescon '97 is an international forum for the presentation of new developments in telecommunications energy systems.

In 1997 **Budapest** offers a platform for all concerned experts and companies in the field of telecommunications power supply systems, new technologies and solutions. Recently Central and Eastern Europe is an area of intensive investments of telecommunications systems. Some special regional aspects of power systems will be detailly discussed.

We should like to follow the TELESCON tradition started in Berlin in 1994.

Representatives from Eastern and Western parts of the world are expected to prove through technical presentations, posters and exhibition how East and West grow together in the field of telecommunications power supply systems.

Papers arrived from all over the world. The Organizing Committee accepted 68 papers. The speakers are from Western Europe (27 papers), Central and Eastern Europe (21 papers), North America (12 papers) and from Far-East (8 papers).

TECHNICAL SESSIONS

PLENARY

Topics include:

- * General aspects for telecommunication energy systems
- * Challenges of Network Development to the Powering Solutions in Hungary

SYSTEMS I-II.

Topics include:

- * Research and development issues * Power supply planning and architecture * Powering of broadcasting systems
- * Alternative power storages * System dimensioning * High-power-density power plants * Long run perspectives
- * System specifications * Power options

CONVERTERS I-II.

Topics include: * AC-DC converters * DC-DC converters * Switching converters * Active and passive filters * Analysis of switching processes * Power factor correction * Frequency transformers * Circuit topology * Bidirectional fed

BATTERIES I-II.

Topics include: * Forming processes * Lead-acid batteries * Nickel-Cadmium batteries * Metal hydride batteries * VRLA batteries * Life time and life test of batteries * Selection principles

POWER SUPPLY FOR MOBILE AND REMOTE SYSTEMS

Topics include: * Portable batteries * Photovoltaic systems * Thermoelectric systems * Powering in remote sites
* Indoor/outdoor applications

OPERATION, RELIABILITY AND QUALITY I-II.

Topics include: * Secure power supplies * Management and control of energy flows * Monitoring * Remote supervisory systems * Cost effective solutions * Availability of power systems * Quality control in manufacturing * Safety aspects
* Intrusive tests * Reliability analysis

EMC

Topics include: * Electromagnetic hazard of power systems * Damages of lightning discharges * Filters * Overvoltage protection

COOLING AND AIR CONDITIONING

Topics include: * New energy conservation techniques * Displacement cooling * Thermal management
* Indoor/outdoor systems * Ground thermal characteristics * Simulation methods * Cost of power and cooling

The Proceedings of the Conference is available at the Telescon Secretariate. Costs: DM 75 + postal costs DM 10.

For further information please contact: Scientific Society for Telecommunications, Telescon'97 Secretariat


H-1055 Budapest, Kossuth Lajos tér 6-8.

Tel: 36-1 153 1027, Fax: 36 1 153 0451

Internet: hiradastechnika@mtesz.hu



It's all about
communication
between people.
The rest
is technology.



Find ERICSSON at stand
201/F in pavilion A
in IFABO!

Telecommunications has become an inseparable part of our everyday lives. It gives us power to maintain most of our personal and business connections. Ericsson's sophisticated communication systems and equipment are intended to connect people all over the world. It's all about communication between people. The rest is technology.

Let's talk a little!

IFABO
BUDAPEST
1997

Ericsson Kft., 1146 Budapest, Hungária krt. 162.
Tel.: 265-7100, Fax: 265-7467

ERICSSON 