John von Neumann Computer Society

Austrian Computer Society

Eighth Austrian-Hungarian Informatics Conference

CON '93

The Challenge of Networking

connecting equipment, humans, institutions

PROCEEDINGS

D. Sima - G. Haring (eds.)

Szombathely (Hungary)
November 17-20, 1993.

D. Sima - G. Haring (eds.)

THE CHALLENGE OF NETWORKING

CONNECTING EQUIPMENT, HUMANS, INSTITUTIONS

PROCEEDINGS of the CON '93

Szombathely (Hungary)

D. Sima G. Haring (eds.)

THE CHALLENGE OF NETWORKING

CONNECTING EQUIPMENT, HUMANS, INSTITUTIONS

SPONSORS

Federal Ministry of Science and Research (Austria)
National Committee for Technological Development (Hungary)
MATÁV Institute of Telecommunication and Informatics (Hungary)
BankNet Ltd. (Hungary)

THE CHALLENGE OF NETWORKING

Connecting Equipment, Humans, Institutions

edited by

D. Sima
G. Haring

R. Oldenbourg Wien München 1993

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

The Challenge of Networking: connecting equipment, humans, institutions; [Proceedings of the CON '93, Szombathely (Hungary)] /
D. Sima ; G. Haring (Hrsg.)- Wien ; München :Oldenbourg, 1993
(Schriftenreihe der Österreichischen Computer Gesellschaft; Bd 70)
ISBN 3-85403-070-3 (Österreichische Computer-Gesellschaft)
ISBN 3-7029-0372-0 (Oldenbourg Wien)
ISBN 3-486-22732-7 (Oldenbourg München)
NE: Sima, Dezsö [Hrsg]: CON <1993, Szombathely>;
Österreichische Computer Gesellschaft: Schriftenreihe der Österreichischen ...

Druck: Corner BT
Budapest, Ungarn

ISBN 3-85103-070-3 Österreichische Computer Gesellschaft
ISBN 3-7029-0372-0 R.Oldenbourg Verlag Wien
ISBN 3-486-22732-7 R.Oldenbourg Verlag München

The Challenge of Networking
Connecting Equipment, Humans, Institutions

Szombathely, November 17-20. 1993

PROGRAM COMMITTEE

Chair D. Sima *Co-chair* G. Haring

Tutorial chair
P. Hanák

Hungarian members
L. Csaba, B. Dömölki, Gy. Papp, L. Polacsek, B. Ree, P. Ritter, I. Tétényi, F. Telbisz

Austrian members
V. Haase, M. Haberler, H.Hoffman, H. Jeram, R. Posch

ORGANIZING COMMITTEE

S. Bognár, W. Grafendorfer, M. Kiss, P. Nagy, L. Polacsek, M. Tóth (Chair)

Preface

It seems that the chosen theme of the Eighth Austrian-Hungarian Conference in Informatics could be a real hit. This subject fits excellently into the major trend of systems integration and has attracted a great number of speakers and participants. We are glad to welcome internationally well known experts as keynote speakers namely, Prof. Babai, Prof. Goos, Dr. Metakides and Prof. Terplán who will outline major trends in their field of interest.

The Program Committee is highly delighted having got an excellent response and a balanced participation from universities, industry, service providers as well as user organisations and state administration.

The Program Committee Chairman is pleased to note that this basically bilateral conference is nicely augmented by speakers from Germany, the EC headquarters, Switzerland, Sweden and the US.

The conference sessions cover the key topics related to networking such as

- network services,
- networks of humans and institutions,
- networks and related issues,
- network applications.

On the field of *network services* inter alia multimedia groupware systems, privacy enhanced mail as well as electronic data interchange and electronical committee management will be highlighted.

Special attention is paid to the very actual topic of *networks of humans and institutions* like Networks of Excellence, European Software Quality Network or international research and development through computer networks.

A number of papers are focusing on *network applications* like in the state administration, insurance or travel agencies.

It is fortunate that the *practical aspects* of network management, reliability or security issues are duly covered in a number of papers.

A novelty of the conference are *tutorials* held by highly recognized practitioners on the attracting subjects of

- security issues in computer networks,
- X.500 directory services,
- LAN-management and,
- WAN-management.

Organising this conference has been a real joint venture connecting many people from many countries.

Both organizing societies highly appreciate the financial support given by the National Committee for Technological Development (Hungary) as well as by the Ministry for Research and Technology (Austria).

I would like to thank all keynote speakers for accepting our invitation as well as all speakers shaping this conference.

Special thanks are due to the members of the Program and Organizing Committee as well as to all referees for selecting and assessing the papers.

It is my duty to thank to Dr. B. Dömölki, Dr. L. Polacsek, Mrs. M. Tóth, Prof G. Haring and Dr. W. Grafendorfer as well as to the secretariats of the NJSZT and OCG for their invaluable help in organizing the conference.

Last but not least I would like to express my appreciation to Prof. Pusztai, principal of Berzsenyi Dániel Pedagogical College, for hosting our conference.

I am sure that the Eighth Austrian-Hungarian Conference in Informatics focusing on the *Challenge of Networking* will be a success and will contribute to the tradition and recognition of our conference line.

D. Sima
Program Committee Chairman

CONTENTS

NETWORK SERVICES

Chair: D. Sima, R. Posch

CONFERENCE 1993

THE NETWORK IS THE COMPUTER

Author: Dr. Kornel Terplan
Consultant and Industry Professor
Polytechnic University Brooklyn

Abstract:

After briefly summarizing present networking status and expectations for the next 10 years, generic networking elements of enterprise networks, and transmission, standard, and value-added-services are addressed. In order to understand to needs of future networking, four basic networking structures will be shown: they are terminal networks, client-server networks, distributed networks and open networks. Depending on the applications that are driving these networks, bandwidth demand and performance criteria may differ. The paper will explain evolving technology represented by frame-relay, sonet, high-speed switched services, FDDI, asynchronous transfer mode, ISDN and broadband ISDN, satellite and wireless services. The paper will prove that future networks are able to support multimedia communications, anyto-any connectivity, high performance for reasonable service charges. Evolving enterprise networks do not know any geographical and political boundaries. The paper ends with defining the management requirements of such multivendor, multinational and multimedia networks.

1. NETWORKING IN THE NEXT 10 YEARS

Network managers are constantly under pressure to improve the efficiency and effectivity of the u of computing and communication facilities. They must be prepared to offer communicati alternatives to various application portfolios, including hierarchical, peer-to-peer or client/serv computing. In most cases, the move of information between computing facilities and databases transparent to users. The present status of networking can be characterized as follows: (TERP92)

- Sectionalization of communication networks by applications, suppliers, communication forms, users and geographical segments.

- Lack of integration between physical and logical networks.

- Lack of integrating multimedia and multivendor networks into one unique enterprise network due to the lack of incompatibility.

- Uncontrolled growth of workstations, applications, users, and as a result transmission volumes.

- Standalone PCs and LAN segments that are targets of internetworking.

- High overhead in communications due to protocol conversions in highly complex networks.

- No breakthrough of standardization in form of really open networks.

- No quantification of user and application needs.

- Mistification of the technology.

- Certain networks became unmanageable due to their complexity.

- Little willingness to innovations.

The next decade seems to be essential in terms of renovating communication networks. Doing so, the following conditions must be carefully interpreted and evaluated (GANT88):

- The combined computing/communications industry will be reforming, causing a growing polarization among suppliers and a growing importance of communication managers.

- The number of end-users with heavy networking demand will be doubling within the next few years.

- The communication network will remain a multivendor, multitiered, and multimedia entity.

- Network control and management will be a matter of managing various physical and logical segments of wide, metropolitan and local area networks.

- Backbone transmission will be an interchangeable commodity. Network access will vary from a commodity to a value-added item.

- Traffic will become increasingly digital and will significantly change in nature. The bandwidth demand will come from new applica tions and not from the growth of existing ones.

- Transaction data processing and timesharing traffic will grow at much higher rates than the capacity of computer equipment.

- Voice-band data can be expected to grow a little slower than the rate for packet switching or data communication expenditures.

- Voice telephony will grow proportionally by the number of handsets; fax may contribute to traffic pattern to a larger extend than expected.

- High-speed data will increase due to CAD/CAM, telecommuting and due internetworking LANs.

- Teleconferencing will grow constantly, and the growth rate will depend on acceptance, rather than on technology.

- Customer premise and nodal processor types will be of such varying characteristics that a substantial part of network management will have to be devoted to keeping track of equipment, cabling, and vendor contracts.

- Management of networking resources will remain to some extent application dependent. Thus, the concept of a single, comprehensive corporate network is not realistic within the next 10 years.

The level of integration of the network of the next decade will depend on the environment of the enterprise, including the master architecture for voice and data.

2. NETWORKING ELEMENTS AND STRUCTURES

The responsibility of network designers and planners is to provide optimal network performance by combining network elements and networking facilities. Figure 1 offers a generic view of a typical communication network, connecting various local area networking segments by wide area networking facilities.

The importance of individual networking elements depends on the structure of the communication network. Usually, one of the next four types or a combination is implemented: (TERP91)

Terminal networks

These networks consist of a powerful mainframe controlling local and remote communication front-end-processors. Those processors are connected to local or remote control units which serve most usually unintelligent terminals or workstations. Peer-to-peer connections at low level are not frequently supported. Besides physical connections (lines) both basis and value-added services may be utilized for connecting network elements (Figure 2).

Client-Server-Networks

There are just two types of elements: Servers offering various kinds of services, such as processing, file management, printing, storing information, and workstations of clients which are generating requests towards the servers. Dedicated servers may take management responsibilities (Figure 3).

Open networks

Assuming a number of elements offering service and even a greater number of elements requesting service, de-facto and OSI-based architectures may help to logically connecting all elements. In both cases, participating suppliers and users have to ensure efficient protocol conversion at network entry points. Within the open network, a variety of transmission services may be offered. Control and management functions are provided by the suppliers (Figure 4). Many users are connected to the open networks via terminal networks.

Distributed systems

As a result of networks and systems growing together, one may take advantage of using very different servers, multiple processors, a distributed operating system and distributed control and management modules, called since recently cooperative management (Figure 5).

Implementing and changing networks is an evolutionary process. Strong customers are very likely using all four types. Other users may start with the terminal network, but step-by-step replacing the terminal clusters by local area networks and thus migrating to a mixture of terminal with client-server networks (e.g., Ethernet or Token Ring).

Participating in electronic mail or electronic data interchange may require the use of an "open" network offering those services (e.g., SNA with Token Ring supporting X.400 E-Mail). Finally, for performance or for price reasons the central computing facility maybe replaced by a distributed solution. The ultimate goal of the evolutionary process is enterprise networking.

The basic concept of enterprise networking is to move digitalized information from everywhere to anywhere without the intermediate step of converting it to human-readable form. By eliminating unnecessary conversions, the enterprise can get the maximum benefits from what computers and communication facilities do much better than humans - access, process, and move information - leaving humans more time to do what they do best: make decisions and exercise creativity.

The price/performance ratio of computing and of digital transmission has improved dramatically over the last few years. In order to get most out of investments, many companies are in the process of combining their computing and communication facilities. In most cases, networks become the center and computers the periphery.

3. NETWORKING SERVICES

In terms of networking services offered by private and public suppliers, three levels can be differentiated: transmission services, standard services and value-added-services. The emphasis in this chapter will be onvalue-added-services.

Transmission services

These services offer the physical connectivity by selling circuits to customers. Despite the present popularity, this service is not expected to be very crucial in building enterprise networks during the next decade.

Standard services

Standard services offered by public and private companies may be grouped in accordance with the four communication forms of voice, data, image, and video. In many cases, however, combined services are offered. Service examples include among others: telex, teletex, telefax, electronic-mail, voice mail, videotex, and teleconferencing.

Value-added services

In this case, design, capacity planning and management of the networks are the responsibilities of the suppliers. There are a variety of offers in the industry. In order to enhance the cooperation between suppliers and users, the so called virtual or software defined networks give some insight into the status of physical components to the users.

Packet switching networks permit the transfer of information between two users by routing addressed packets of information through the network. Both the links and the network nodes are completely timeshared among all users. Unlike other networks, each packet-switching node implements the store-and-forward technique for switching each packet. All packets are switched according to the first-in first-out scheme, unless packet priorities are employed. Future applications will require a flexible combination of packet and circuit switching technology.

Message switching networks receive the entire message and store it in secondary storage. When the output link is available, these networks transmit the message to the various subscribers. The major customer facilities offered by message switching systems are complete end-toend assurance, extremely good utilization of expensive user links, and long-term protected storage. In terms of the future, message switching will tend to become just another facility within a public data network. When the office of tommorrow becomes a reality, message switching is bound to play an even greater role in distributing a large amount of interoffice memos and mail and storing and retrieving a large amount of word-processing data for later retrieval or printouts. In many countries, teletex will offer similar services.

Electronic Data Interchange (EDI) is the computer-to-computer exchange of business information between business parties in a structured format. EDI helps to replace paper documents with communication offering increasing efficiency. Additional benefits include the elimination of redundant business procedures associated with paper-based systems; reduction of potential for errors; acceleration of doing business; and support of increased automation by increasing EDI with electronic funds transfer, bar code printing, and database applications.

Future applications will require hybrid packet/circuit switching scenarios, most likely supported by ISDN. It is assumed that the fixed bandwidth assignment of ISDN will give place to more flexible solutions. Performance improvement is imperatively necessary with packet switching.

New switching techniques, called "fast packet" engines are already in development, and they are expected to support 150 Mbps to 600 Mbps bandwidth. It is expected that Dual Queue Dual Bus (DQDB) represents a true performance breakthrough. Based on distributed scheduling and separate channels for data and control information, it is a complete departure from present systems.

On the way to fully implemented fast-packet switching, the frame relay technique will give a significantly higher throughput rate - 10,000 to 100,000 LAPD-based frames per second - by minimizing packet layer processing. Frame relay does not request the change of present packetprocessing hardware.

Value-added networking services will take advantages of the opportunities offered by broadband services. Broadband services will track the requirements of global networking. Figure 6 illustrates the bandwidth requirements, and the communication services offered to meet the bandwidth challange.

Performance is usually unsatisfactory with packet switching due to the fact of many confirmation and checking steps included at Layer 3 of the open communication architecture. The significant quality improvements of the communication technology, measured by considerable lower error rates, helps to introduce fast packet services. The fast packet concept has generated two different technology approaches, and a number of product and service solutions (Figure 7).

Both the terms frame relay and cell relay refer to fast packet-based technologies. From an architectural perspective, frame relay is a layer 2 and cell relay is a layer 3 service. Frame relay solutions are based on both public and private networks. Cell relay solutions are planned or currently available include B-ISDN and SMDS.

4. EVOLVING TECHNOLOGIES

Fast packet switching will be enhanced with the development of new high speed switching fabrics. The term fabric is used to describe the design and structure of switching activity. The new technology applies "on-the-fly"-switching where switching stages are fast hardware gates triggered by a tag bit associated with a virtual channel number. A three-stage switch requires a three-bit tag. A packet arriving on any input line and carrying the same tag will be directed to the same output line. This technique is much faster and more efficient than software switching. Figure 8 illustrates the two techniques of fast packet: cell relay (top of the figure) and frame relay (bottom of the figure). Frame relay systems take the user information, e.g., a local network packet, and encapsulate it in a larger unit called a "frame". The frame header and trailer fields typically contain addressing, control and error checking information. Frames can vary greatly in length usually from around one hundred to over a thousand octets. This is in contrast to cell relay that uses fixed length that is chosen by the network designer. Variable length user data are distributed across several cells. Each cell has a header containing routing and other information. Cells may be full, partially full, or empty.

Frame relay is well suited to applications such as LAN interconnect; interactive transaction services, such as airline reservation systems; and bursty, bandwidth intensive requirements such as computer-aided design. Frame relay brings together the capacity, flexibility, and control of private networking with the universal access, convenience and survivalability of public networks.

Prototypes of packet switches based on synchronous transfer mode (ATM), or so called fast-packet operation have already been demonstrated. These perform almost no software-based processing and instead perform packet-manipulation functions based on silicon-embedded logic, which is much faster. Throughput rates up to 1 million 53 byte cells per second is the target. This technology is the basis for the switched multi-megabits/s data services to be applied for metropolitan area networks, mainly as a network facility for linking multi-megabits/s LANs.

Switched Multimegabit Data Service (SMDS) provides what is known, in terms of the open systems architecture as a media access controller (MAC) service. This is the equivalent of the services provided by local area access services such as IEEE 802.3 (bus) or IEEE 802.5 (ring). The significance of this is that the SMDS can act as a MAC-bridge. In turn, this allows the logical link control protocol to operate across the SMDS network directly between the end-users.

The SMDS protocol between the end user and the network provider is called SMDS Interface Protocol. Above the link layer users could operate any desired network protocols such as TCP/IP or OSI.

Cell relay technology to be examined is called the Asynchronous Transfer Mode (ATM). ATM is being promoted as the information transfer mechanism for broadband information services. ATM is high capacity, low delay, packet-based but cell switched technology. It accomodates very high speed multiplexing based on a label in the header of the 53 octet cell. ATM is connection-oriented service indicated guarantee of delivery. This is in contrast with the connectionless SMDS service. ATM does not use asynchronous transmission. The term refers to support of asynchronous traffic streams such as local network generated packet streams.

For the metropolitan area, two technologies are in heavy competition:DQDB (Dual Queue Dual Bus) and FDDI (Fiber Distributed Data Interface).

DQDB uses a fault tolerant looped dual bus topology. This is a special case of the dual bus where a single node acts as the head and end of the bus. The two buses, called bus A and B support full duplex communication between any pair of nodes. The busses transmit in opposite directions. Transmissions are in fixed length slots. A key feature of the topology is that the operation of the bus is independent of the individual access units. Attached nodes may be added or removed or may fail without affecting operation. Another feature is automatic reconfiguration in the case of cable failures.

FDDI is a 100 Mbps network capable of supporting 500 nodes spread over 100 km. The nodes could be bridge connected, e.g., for interconnecting LANs. FDDI is receiving major support from vendors such as IBM and DEC. Both are planning to use FDDI as a backbone network to support token rings and Ethernets. FDDI is also a good candidate to connect mainframes in a computer room. DQDB, on the other hand, is being touted as public offering at 45 Mbps with the capability of going to 150 Mbps. It is being heavily supported by network providers and so will probably continue as a public network service. Table 1 (CONA92) displays the comparison between these two technologies. At the moment if the need is to interconnect among organisations, DQDB may be the best choice. If the need is to interconnect within an organisation, FDDI should be considered.

In seeking a transfer mode for broadband networking, the industry was looking for a technique that had the real time characteristics of circuit switching and the flexible capacity of statistical multiplexing that was characteristic of packet switching. Synchronous Transfer Mode (STM) was an early candidate for B-ISDN. STM is based on time division switching and multiplexing. It is simple but not as efficient as ATM for a dynamically changing load. STM can be compared to ATM as TDM compares to STDM. ATM's flexibility derives from separating, or decoupling, the bit rates required by the users from the bit rates of the physical transmission medium. By allocating capacity to a user on a guaranteed reservation basis, ATM can handle voice and video. By allocating capacity on demand, ATM can efficiently support data users.

Table 2 compares packet, frame and cell switching technology across a number of important attributes (CONA92). It is important to understand that each of these methods is based on the concept of switching packets of information. The differences lie in the size of the packet and the architectural level at which switching takes place. In general, it may be assumed that the lower the architectural level the faster the process.

Should a decision be made to use cell relay technology, a choice needs to be made between two solutions: SMDS or ATM. Althrough cell switching will not become prevalent before ATM arrives later in this decade, cell relay is usable in the form of SMDS. Many trials are underways in many countries. ATM is faster and more adaptable to more applications and higher speeds, but will not be readibly available until sometime after 1995.

The basic building block for Sonet is the 51.84 Mbps STS-1 signal. The frame format for this signal is the 90 byte by 9 byte array illustrated in Figure 9. The transmission order of this frame is from left to right, top to bottom in the illustration. The 810 byte (octet) frame is divided into two main areas. These are the transport overhead and the Synchronous Payload Envelope. The transport overhead of 27 bytes supports operations and maintenance and includes a network data communication channel between network elements. This overhead consumes 1.73 Mbps of the STS-1 rate. The envelope carries the information by the frame. It includes 763 bytes payload capacity of 50.11 Mbps. The total frame of 810 bytes is repeated every 125 microseconds for a transmission rate of 51.84 Mbps.

Integrated Services Digital Networks (ISDN) will try to bring much more visibility into the services area. ISDN may be considered as a solution for all three previously introduced alternatives. ISDN enables the integration of communication forms. In the wide area, there is no difference among networks, because mixed transmission is accomplished via 64 Kbps channels. Simultaneously, multifunctional customer terminals are developed and implemented. B-ISDN will be evolutionary next generation of the ISDN. It will be different in a number of ways. Most of these differences are related to the need to provide greater speed as well as support for multimedia services. The higher rates, 150 Mbps versus 65 Kbps for channel rates and 6000 Mbps versus 2 Mbps for interface rates, will require fiber to be used as a transmission medium. The need for high speed switching will dictate cell relay rather than frame relay, and ATM rather than STDM multiplexing. Even as the industry deploys existing broadband technology, planning is underway for the next generation of communication capabilities. The future beyond broadband will be one of optical switching,

megapacket-per-second networks, and broadband residential service. Symbolic compression, based on human perception of visual material, will permit three-dimensional video transmission. Speech may be used to directly set up connections because of advances in speech processing. As huge arrays of distributed antenna now gather information about the universe, so arrays of parallel processors linked by broadband communications will attack problems like athmos-pheric and oceanic modelling.

Personal communication systems, processing satellites and gigabit-persecond global networks will permit anyone to communicate with virtually anyone about virtually anything.

5. REQUIREMENTS FOR MANAGING THE ENTERPRISE NETWORK

Without management, no productivity and no quality of service can be expected by using such complex networking structures. Due to the fact of unsatisfactory attention to network management functions, instruments and lacking human resources, certain networking structures are no longer manageable. At the moment, there are too many instruments, and too little support for processes to support human resources in the area of configuration, fault, performancve, security and accounting management. The principal requirements may be summarized as follows:

- Renovating existing processes and applications by taking advantage of state-of-the-art technology of operating systems, graphics, and databases.

- Selecting the right management platform product offering excellent presentation services, applications for key functions, systems services, and communication interfaces to existing and future management systems and to managed objects.

- Implement a powerful configuration database on relational basis and connect it to the platform by populating it with existing data files and data bases.

- Educate and cross-train network management staff to take full advantage of the available technology.

6. SUMMARY

The network is the computer means that distribution of processing, databasing and communication responsibilities is on the way. The future will bring more bandwidth to support bulk data transfer with high quality, sophisticated switching and routing alternatives in

order not to delay transmission and reasonable communication services making outsourcing a very attractive offer. But, human creativity in evaluating opportunities, selecting the right technology and instrumenst, making the right decisions to fix problems, and coordinating users, manufacturers and services suppliers, is more important than ever before.

REFERENCES

(CONA92) Conard, J.: Broadband Technologies, CAP Gemini Seminar Records, Henley upon Thames, United Kingdom, 1992

(GANT88) Gantz, J.: The Network of 1998, TCT Networking Management, January 1988, p. 22-36

(TERP91) Terplan, K.: Communication Networks Management, Prentice Hall, Second Edition, Englewood Cliffs, USA, 1991

(TERP92) Terplan, K.: Effective Management of Local Area Networks, McGraw-Hill, New York, USA, 1992

FIGURES

TABLES

Table 1: FDDI and DQDB comparison

Table 2: Switching technologies comparison

VITA - Dr. Kornel Terplan

Kornel Terplan is a telecommunications expert with more than 20 years of highly successful multi-national consulting experience. His book, Communication Network Management, published by Prentice Hall (now in its second edition), and his book on Effective Management of Local Area Networks, published by McGraw-Hill, are viewed as the state-ofthe-art compendium throughout the community of international corporate users. He has provided consulting, training and product development services to over seventy five national and multi-national corporations on four continents, following a scholarly career that combined some 140 articles, eight books and 110 papers with editorial board services.

Over the last ten years he has designed five network management related seminars and made some fifty five seminar presentations in 15 countries. He has received his doctoral degree at the University of Dresden and completed advanced studies, researched and lectured at Berkeley, at Stanford University, University of California at Los Angeles and Rensselaer Polytechnic Institute.

He is on the Advisory Board of the Datapro Network Management Service. His consulting work concentrates on network management products and services, outsourcing, central administration of a very large number of LANs, strategy of network management integration, implementation of network design and planning guidelines, products comparizon and selection.

The most important clients include AT&T, GTE, Walt Disney World, Boole and Babbage, Kaiser Permanente, BMW, Siemens, France Telecom, Commerzbank, German Telecom, Union Bank of Switzerland, Creditanstalt andState of Washington.

Distributed Object Management,

a Survey

Dr. Miklós Biró, András Micsik, Dr. Tibor Remzső
MTA SzTAKI
H-1111 Budapest, Lágymányosi u. 11.

Abstract

This paper gives an introduction to distributed object management. Objects and classes are explained, and usual relationships between classes are listed. Distributed object management systems provide services for object handling, request-communication and resource management. The Object Management Group is the biggest forum on object technology in the world. We look over their goals and activities. Their CORBA specification also gives an idea about distributed object management. The overview of two DOM products and our experiences conclude the paper.

Supported by OMFB 91-97-11-0005

1. Introduction

During the last few years, the computer industry has been filled with news of the coming revolution in object-oriented (OO) software. The development in an OO environment dramatically cuts down the time and effort needed to complete an application. Now after OO technology revealed to be powerful on single machines or on small networks, the next step is to make objects work through large, heterogeneous networks. Computing environments of American and West European companies often include a complex patchwork of incompatible mainframes, minicomputers, personal computers and systems software. Enormous profit could be taken by simplifying the operation of such environments. Distributed object management (DOM) as a new class of OO technology is able to do this work.

The organization of this paper is as follows. In section 2 we quickly look over the fundamental concepts in OO programming. Afterwards we give an overview of desirable properties and usual

functionality of a distributed object management system. This section is based on the article of R. S. Chin and S. T. Chanson [1]. Section 3 gives an introduction to the specifications evaluated by the Object Management Group, including the Object Model [4] and the Common Object Request Broker Architecture [2]. Further sources about OMG are [3,5,6]. Section 4 briefly outlines two DOM software, HyperDesk DOMS and Arjuna [7]. Finally in Section 5 we shoot a glance on our development work in the laboratory.

2. Basic concepts

2.1. Objects, classes and inheritance

An *object* encapsulates state information or data, a set of associated operations that manipulate the data, and possibly a thread of control. There is no other way to examine or modify the state of an object than making requests on the operations of the object.

An object may or may not contain processes. If it contains processes, those processes are bound to that object and their activity is limited to servicing the requests made to that object, or to the maintenance of the object's state. This is called the *active object model*. On the other hand, in the *passive object model*, processes execute within several objects during their lifetime. When a process makes an invocation on another object, its execution in the current object is suspended, and the process is mapped into the object space of the other object. After completing the invocation, the process returns to the first object and resumes execution.

Objects can be characterized by their relative size and the relative number of interactions they make with other objects. It is called the *granularity* of objects. Large-grain objects usually have few interactions with others, and make a lot of processing to service a request. These objects are obvious to use with the active object model. Examples for large-grain objects are an editor window, a single-user database or a spreadsheet. Systems can provide finer granularity than large-grain objects. Then medium and fine-grain objects are contained by large-grain and medium-grain ones, respectively. Medium and fine-grain objects are not worthy to own processes, and can cause big overhead in the program. The benefit of finer granularity is the consistent programming model. Examples for medium-grain object is a spreadsheet cell or a paragraph, and for fine-grain object an integer or a logical value.

Objects that differ only in their state or data, but have the same set of methods are grouped in a *class*. Reusability and error-safeness inspire different relationships between classes. *Inheritance* means that a new class takes the methods and behaviour of an existing class as a starting point, that is the new class specifies only the changes with respect to the old class. Multiple inheritance occurs when a class inherits from more than one class. Another way of reuse is to *encapsulate* an object of another class into one object. In this case the encapsulating class ties looser to the implementation of the encapsulated class, the latter one can be easily modified unless its specification is changed. *Subtyping* can also be applied to classes. A subtype is a specialization or a refinement of the

supertype. Operationally this means that any object of a subclass can be used in any context which expects an object of the superclass. Another rarely mentioned mechanism is *delegation*. This mechanism permits an object to delegate responsibility for servicing a request to another object. This differs from inheritance in that it can be class independent. The class does not determine the class and instance of the objects that are delegated by its own objects. All these relationships can be drawn as directed graphs. The properties of these graphs differ from system to system. One thing that makes the chaos even bigger is *genericity*, or parametrized classes. Generic classes can take classes from a given set as parameters, and they can generate useful structures based on different classes. In fact genericity can be solved using inheritance, but in the other way it is not true. Still the use of generic classes is very comfortable.

The behaviour and meaning of classes also show a big variety in programming environments and object models. Some systems treat classes like objects, so they can have methods and state information. The best example for this is SmallTalk. Other models claim the inverse of this; classes maintain no state and perform no methods, they exist only at compile time, while objects exist at execution time. The most popular OO languages fall into this category, like C++ and Eiffel. Older languages (e.g. ADA, Modula-2) support objects as language feature, but they do not support any inheritance mechanism. These are called *object based languages*. Newer languages with inheritance mechanisms are called *object oriented languages*.

2.2. Distributed object management systems

A distributed object management system is the marriage of an operating system and a programming environment, both object-based or object-oriented. This means that the system must give solutions for the following tasks:

- object handling,
- communication capabilities between objects,
- and resource management.

Furthermore a distributed object management system must provide these features together with a distributed and decentralized computing environment. The environment spreads over several computers, which can be PCs, workstations of various type. The hardware can be very heterogeneous. This is already the case in many computing environments. The main idea is to make all the machines at one site work together. There can be more done than disk and printer sharing. All the processors and every piece of hardware can be combined together.

Users are not interested in the place of the computing or their files or any other details. If they have objects, in a DOMS they can create their objects, get them stored somewhere in the system, and after a while destroy them. In a DOMS one should be able to make requests to objects in a uniform way, whether the object is on another workstation or in secondary storage. This is *location transparency*.

The system may decide on which machine it activates the object. The important things are to be able to find objects that provide the services we want, to be able to find our own objects, and to be able to make restrictions on the use of our objects.

An object is called *persistent*, if it is automatically stored in secondary storage and thus it is not destroyed after its use or due to a failure. *Data integrity* in a DOMS means that persistent objects are always in a valid state, that is unsuccessful termination of an operation does not spoil the state of the object.

In order to operate reliably, the system should have mechanisms to reveal the inavailability and failure of objects, and restore the normal state. *Reliability* advises that none of the computers should play such role in the system, that the failure of that machine could cause the whole system to stop.

Security issues are very important, since a user can access all machines on the network. One should be able to restrict the use of the objects that he created or owns.

The resources can be put fully under the control of the DOMS. It can balance processor loads and memory usage between machines. Large objects are especially suitable for distributing them on several machines, allowing concurrent execution.

2.3. Object handling

This enables objects to be created, maintained and destroyed. Creating an object can be as simple as activating a menu and as compound as writing source code fulfilling a set of system dependent rules. Usually an object management system offers an object-based or object-oriented language and a programming interface for the system.

Typically all parts of the system, from the kernel to the applications are treated as objects. The identification of objects is needed to make references for an object. Security mechanisms can restrict the use of objects. Multiple access to objects is also an aspect which can hardly be avoided in a DOMS.

Last but not least an object should be made persistent. A persistent object has an image in secondary storage. With that image the object can be constructed and made to work by the system when it is requested by other objects. This is called the activation of the object. Persistence gives also a good way to solve fault tolerance. Persistent object failures can be repaired using the stable image. In some systems all objects are persistent, in other systems the owner or the creator of the object can make the object persistent, for example by inheriting persistency properties from a base class.

Besides persistence a DOMS may provide atomicity. The chain of invocations resulting from one request is called an *action*. A DOMS can provide atomic actions, which means that a unit of computing is indivisible from the programmer's view, it either completes successfully, or has no

effect at all. Furthermore the effect of a successful action in a persistent object should be permanent, to avoid loss of computing results and information in case of smaller failures.

Other interesting issue is synchronization and serializability. Concurrently executing actions should be scheduled in such a way that the overall effect is as if they were executed sequentially in some order. This is serializability. The synchronization is needed to keep back actions from observing or modifying the state of an object that has been modified by another atomic action that has not completed yet.

Object replication mechanisms manage multiple copies of the same object on different workstations. This increases availability of the object and makes the system more tolerant to workstation failures.

2.4. Communication between objects

When an action makes an invocation request, the system must locate the specified object, take the appropriate steps to invoke the specified operation, then possibly return the result.

A DOMS should provide location transparency so a client makes an invocation with a reference to an object, then the system determines which object was invoked and on which workstation it currently resides. The mechanism for locating an object should be flexible enough to allow objects to migrate from one workstation to another. Several such mechanisms exist, for example using name server objects or a cache/broadcast scheme.

The system-level invocation handling depends entirely on the object model of the system. In case of the active object model message passing is used. The parameters of the invocation are packaged into a request message. The server process in the invoked object accepts this message, unpacks the parameters and performs the method. The result is packaged into a reply message which is sent back to the client.

Direct invocation is used with the passive object model. A process will migrate from method to method and from object to object in the order of subsequent invocations of an action.

The most interesting part of invocation handling is detecting invocation failures. A mechanism is needed for both the client and the server to detect the failure of the other. The easiest to detect is when the server object cannot be found. If the client does not notice that its server has aborted, it can wait for indefinitely long time. If the client aborts and the server continues executing, it wastes system resources.

2.5. Resource management

A DOMS like any other distributed operating system must give mechanisms to manage physical resources including memory, secondary storage devices, processors and workstations of the network.

Objects that are lost if the workstation on which they reside fails are said to be volatile. Persistent objects can survive the break-down of their workstations. These objects reside in secondary storage, while the modifications are done on their working copies which reside in memory. When a persistent object has no working copy, it is said to be inactive.

The managing of processor load can be done in two ways. With object scheduling an object is assigned to a processor before activation. Then the object will execute on that processor until deactivated. The assignment can be done explicitly by the user or implicitly by the system. The other way is object migrating, which permits object to be moved from one processor to another, in some cases even while they are in the middle of servicing an invocation. This mechanism attempts to reduce the loads on heavily loaded processors and to minimize the distance of cooperating objects so communication costs can be reduced.

3. The OMG specifications

3.1. The role of the Object Management Group

Up to now several experimental DOM systems has been implemented at universities and laboratories. Some efforts were also taken in commercial software products to begin evolving DOM environments. The future is inevitably for DOMS. But the spread of DOM systems is not enough in itself, because these systems may also happen to be so heterogeneous and incompatible as personal computers today. The Object Management Group (OMG) is working toward a common goal: the development of a framework of specifications to maximize the portability, reusability and interoperability of commercial object-oriented software. The OMG membership lists nearly all the significant software or hardware companies in the world. Among the more than 250 names we can find IBM, DEC, NCR, HP, Canon, Apple as well as Borland, Symantec, SunSoft, Lotus or even Microsoft. Since 1990 OMG provides a reference architecture with terms and definitions upon which all specifications are based. This is called Object Management Architecture. This framework (OMA Guide) and other forthcoming specifications are publicly available, and the process of the specification is open and well-documented. Finally, OMG invites lively industry discussion via open forums, education and conferences.

3.2. The OMG Object Model

The OMA Guide also contains an object model, which is used by all OMG-compliant technologies such as the CORBA. In section 2 it was revealed, how many opportunities should be cleared up and composed into an object model. This model is very simple, but contains a mechanism for extensions called components. While the Core Object Model serves as the common ground, components may add capabilities that are required for special systems, but not obliged to be supported by all systems. These components are grouped in profiles for technology domains, for example there can be an Object Database profile.

The Core Object Model is based on a small number of basic concepts: objects, operations, types and subtyping. Objects have identifiers (OIDs) to refer to them. The notion of type corresponds to our notion of class. Types describe the operations applicable to objects of that type. Types are arranged into a type hierarchy that forms a directed acyclic graph. The root of this hierarchy is called *Object*. There can be denotable values other than objects, like in C++ or in CORBA. These are called non-objects and have types, but their types have no hierarchy.

Each operation has a *signature*. The signature includes the operation's name, list of parameters, and list of return values, if any. There is a special parameter, the controlling parameter, that refers to the object on which the operation is to be executed. The argument passing semantics is pass-by-value. The *interface* of an object contains the operation signatures of the object`s type.

Subtyping and *inheritance* are coupled in the Core Object Model. If S is declared to be a subtype of T, then S also inherits from T. Inheritance is applied to all operations of the parent type.

3.3. The Object Management Architecture

The Object Management Architecture creates a very simple classification of objects and programs, dividing a distributed object environment into four parts.

The basic part of the architecture is the *Object Request Broker* which communicates requests between objects. With an ORB an object can construct a request, send it to another object using an object reference, and receive the results of the requests.

The second part contains *Object Services*, which manage the naming, lifecycle and persistence of objects, stores the interfaces and implementation of objects. Essentially it provides services for using and implementing objects.

The third part is called *Common Facilities*, it is a collection of general objects, useful in many applications.

Application Objects is the last part, the objects of an end-user application.

These parts are using each other in increasing order. Without the ORB objects are isolated from each other. Object Services are also implemented as objects and interfaces, so they use the ORB for communication. An object service may even use another object service, if it is allowed in the specification. The Common Facilities means common building blocks of applications and they can be built using the ORB and Object Services.

The increasing order also shows the flow of standardization. The specification of the ORB, called Common Object Request Broker Architecture (CORBA) is available since the end of 1991. The Object Services specification is in the Request for Proposal state. It will contain lower-level interfaces mostly important for developers. The Common Facilities specification will provide standard interfaces for applications, but there will not be any specification for Application Objects.

3.4. The Object Request Broker

In a CORBA-compliant system installed objects are stored in two separate parts; their implementation is stored in the Implementation Repository, their interface is stored in the Interface Repository. The interface description of an object contains enough information for a client to make a request on the object. The Interface Description Language is used to describe the interfaces of objects.

From the viewpoint of the ORB Client and (Object) Implementation are distinguished. There exist several interfaces for both the Client and the Implementation to communicate with the ORB Core. Both the Client and the Implementation can use the ORB interface, which provide general services, and manages object references.

The Client can build requests dynamically with the Dynamic Invocation Interface, using the information of the Interface Repository. There is also a possibility for the Client to call stubs, which is a static and more comfortable way of making requests.

All requests arrive to the Implementation through an Object Adapter, which is an up-call interface. The Object Adapter is responsible for activating the implementation of the object and the object itself. The Implementation may provide so-called skeletons for its methods. The Object Adapter calls the skeleton of the appropriate method to service a request.

The Client needs only an object reference to make a request on that object. With the object reference it queries the interface of the object, creates and fills a parameter list, and then sends it to the ORB. The ORB Core finds the Implementation and delivers the request to the appropriate Object Adapter. If the object is foreign, it passes the request to the ORB or object management system which is the manager of the requested object.

A language mapping contains the mapping of ORB interfaces, stubs and skeletons to a particular programming language. The developer writes the interface of the object in IDL, and the implementation using the language mapping and the routines of the object adapter. Therefore the object is portable to all ORBs which provide the same language mapping and object adapter.

There are a number of ways how an Object Request Broker can be implemented. For example ORB can be provided as a basic service of the operating system or as a server and client programs or simply as a collection of libraries.

3.5. Benefits of OMG specifications for programmers

Now we are going to see how these specifications of the OMG support the three famous terms, namely portability, interoperability and reusability. These three goals are very close to each other. Each of them holds the essence that the effort to design, implement and operate a software should not be repeated somewhere else in a community. Portability means that fundamental assumptions

about the objects of a system are supported across different software or hardware. With other words it is easier to move the software to another system than to reimplement it. In this sense the portability may hold for the design, the source code and the executable code of the object.

Reusability is very similar to portability. Many objects once written could be used in more than one application. This is natural inside the area of one particular OO programming language. In this case the object code is reusable. There could be cases when reusing of objects implemented in different programming languages and operating systems was possible. It can be done either by cross-compiling, or by making requests to the object (interoperating it), or just by reusing the design of the object.

Interoperability is the most ambitious objective of the three. This presumes runtime compatibility between different systems. If we stay in an OO environment, it means that one can perform invocations on objects of different systems probably residing on remote machines. Interoperability can be achieved at different levels. At the lowest level a protocol is enough for making and managing requests. At higher levels there can be common object formats or common object semantics.

A common object model like the one of the OMG ensures that the basic design of a large application will be portable to other systems. So the object model at this stage aims at design reusability and portability.

ORBs can achieve source code portability as well, to other ORBs supporting the same mapping for the programming language in which the source code is written. This is because object interfaces are defined in CORBA IDL, so they can be called through the standard ORB interfaces. How objects call and are called in the programming language is clearly the question of the language mapping. How ORB communicates the request to the implementation depends on an object adapter. Object adapters give the ORB the possibility to target particular groups of object implementations that have similar properties with interfaces tailored to them. So in fact the support of the same object adapters is also needed to source code portability. Therefore it is planned to be a few number of widely available object adapters, and one standard CORBA mapping for each programming language.

An ORB achieves interoperability in a sense that objects in an ORB can be used throughout the workstations that connected to the ORB. In addition by connecting ORBs objects will be able to service clients from different ORBs. On one hand the ORB establishes a protocol for making and managing requests, but this protocol works only in that ORB. To communicate requests between different kind of ORBs the protocols need to be translated. On the other hand the Interface Definition Language gives a common syntax and semantics for the object interfaces.

The OMG Object Model is the basis of the Interface Definition Language. The Object Model defines such fundamental things as object identity, types, classes, inheritance etc. So its role is to provide common object semantics.

4. DOM software

4.1. HyperDesk-DOMS

The first software to implement an Object Request Broker was the Distributed Object Management System of HyperDesk. HyperDesk is a Data General spinoff that helped found the Object Management Group and was instrumental in the creation of the Common Object Request Broker Architecture. This is not the only product offering an ORB. Digital, IBM, HP and SunSoft are all working on CORBA-based software, but we have no information about these.

The HyperDesk DOMS solves problems of heterogeneous office environments. It enables users of Unix and Microsoft Windows environments to access each other's objects across a network. The system offers a set of basic object types. One can create new object types from these by modifying or subtyping any existing type. The major components of the DOMS are the object request broker, object services including persistent object storage, Windows and Unix clients that can communicate with the object request broker, programming tools and interfaces.

An object can request the execution of operations on other objects inside or outside the system. The ORB Engine is a process that handles requests from clients, and communicates with other ORBs, object databases or any other object managers. When the ORB Engine receives a request, it determines the manager of the requested object. If the Engine can manage the object itself, it locates the appropriate code for the requested operation and invokes the request. Otherwise it forwards the request to the object`s manager. The ORB-API is the interface to send requests to the ORB Engine and to receive results.

The DOMS have several object services. The Authentication Service provides system security. The Location Service maintains a database of distributed objects. Object Adapters are used to create and manage object references and deliver parameters. The Object Storage gives the basis of the Interface and Implementation Repository.

Tools coming with the system include HD-DOE, a graphical user interface for browsing, creating and modifying objects, and HD-TSL, a scripting tool for testing.

4.2. Arjuna

The Arjuna distributed programming system was developed at the University of Newcastle upon Tyne. It is one of the newer systems which already supports inheritance. In fact the major services of the system are provided by a C++ class hierarchy. The system may contain several workstations, with or without disk. The disks are organized as object storage using Unix file system. An instance of the ObjectState class can store the state of any Arjuna object in a format that can be stored in Unix files and transmitted between workstations. Therefore an object can be activated on a remote machine. Arjuna allows multiple access to objects and multiple activation of an object on different

nodes. Concurrency control is provided to implement serializability of atomic actions. Operations on remote objects are invoked with remote procedure calls. An underlying remote procedure call system manages the calls and detects failures.

The root class of the class hierarchy supports object activation, deactivation and recovery. User-defined classes are derived from the LockManager class which provides concurrency control. Instances of the AtomicAction class are used to automatically record locks, modifications and remote calls of an atomic action. Then the abort or commit can be performed on that action.

A remote object can be referenced by an object identifier which is opaque for the user. Objects can be searched using the information of name servers. One can fill parts of a node-class-objectname triple, and the name servers try to fill the rest and find the object.

5. Our work and experiences

Nowadays commercial systems begin to show more and more features of DOM. For example in Microsoft Windows applications and windows can be considered as objects. Communication between windows can happen in two ways; by sending messages to another window, or by the Dynamic Data Exchange (DDE) protocol. DDE is a facility for applications to share data. Our laboratory has extended the DDE protocol to work between applications on different PCs of the network. This application called NDDE [8,9] was a move toward making Windows more distributed. A year after our project has completed, Microsoft released Windows for Workgroups which already contained a similar facility to NDDE.

Other efforts we made in implementing DOM facilities are coupled with NewWave, a Hewlett-Packard product. NewWave is a Windows software highly improving the object handling of Windows. NewWave provides an object storage and uniform handling of objects. We contributed to the development of an object passing tool on the network. Afterwards several applications were born based on this tool, one of those to mention is Office Viewer [10]. Office Viewer gave the possibility to a NewWave user to open a window on his desktop in which he could see the desktop of another user. Then that user could move objects between the two desktops by dragging and dropping icons.

6. References

[1] Chin, R. S. and Chanson, S. T., Distributed Object-Based Programming Systems, ACM Computing Surveys, March 1991

[2] The Common Object Request Broker: Architecture and Specification, Revision 1.1, OMG TC Document 91.12.1

[3] Dyson, E., Domain of objects: the Object Request Broker, Hotline on Object-Oriented Technology, June 1991

[4] Object Management Architecture Guide, OMG TC Document 92.11.1

[5] Object Services Architecture Revision 6.0, OMG TC Document 92.8.4

[6] Osher, H. M., Software Without Walls, Byte, March 1992

[7] Shrivastava, S. K., Dixon, G. N. and Parrington, G. D., An overview of the Arjuna distributed programming system, IEEE Software, Jan. 1991

[8] Feasibility Study of the Implementation of Cooperation between MS-Windows Based Systems, MTA SzTAKI Document for OMFB 91-97-11-0005 (1991). (M. Biró, L. Böszörményi, Gy. Gyepesi, K. Kovács, E. Knuth, M. Szabó) (in Hungarian)

[9] NDDE Windows DDE Network Extension, MTA SzTAKI Document for OMFB 91-97-11-0005 (1991). (Gy. Gyepesi, K. Kovács, J. Takács)

[10] Implementation of Distributed Object Functionality in the Newwave Environment, MTA SzTAKI Document for OMFB 91-97-11-0005 (1992). (F. Jamrik, G. Janek) (in Hungarian)

Multimedia Groupware Systems

László Kovács *†
Ecole Normale Superieure de Cachan
Laboratoire d'Informatique Fondamentale et Appliquée de Cachan
61, avenue du Président Wilson 94235 Cachan Cedex, France
E-mail: kovacs@lifac1.ens-cachan.fr

June 4, 1993

Abstract

This tutorial paper summarizes the actual research issues on development of multimedia groupware applications. It gives a classification scheme about the different types of groupware applications and describes the operations of the different systems from the user point of view. The implementation structures and the formal models of groupware are also given. Multimedia user interface design problems will be touched upon as well.

Key words *CSCW, groupware, multimedia, multimodal, user interface, distributed system*

1 Introduction - Basic Definitions

Computer Supported Cooperative Work (CSCW) is an interdisciplinary research area which uses different models, information, computer etc. technologies for the purpose of cooperative work of a group. This term entered into the computer jargon following the 1st International Conference on CSCW (Austin, Texas, 1986). CSCW currently includes workflow and group coordination systems, advanced messaging systems, multimedia desktop conferencing, group aware tools like shared editors, shared drawing tools and the traditional communication systems like distributed bulletin boards etc.. The key CSCW theoretical research areas include the analysis of groupwork and special group requirements for CSCW applications, the design of multi-user shared interfaces, distributed architectures, organization modelling and the theoretical research in the area of models of group coordination.

The CSCW opens a new area for the application of computer networks and distributed systems. New types of distributed architectures are under the development where different multimedia and communication modes (like synchronous and asynchronous communication within a single application) are applied. CSCW challenges the research into the direction of multi-point communication protocols from the point-to-point protocols and the research of the concurrency control and synchronization in distributed systems.

*On the leave from: Computer and Automation Institute of the Hungarian Academy of Sciences, Informatics Research Laboratory, H-1111 Budapest XI. Lágymányosi u. 11. Room 415. Hungary, E-mail: h93kov@ella.hu; kovacs@next.ilab.sztaki.hu

†Work partially supported by OTKA grants #2571 and #2575

Groupware (GW) (group supporting system) is a computer based system that supports of people engaged in a common task (goal) and that provide an interface to a shared computer environment. Generally the groupware is a hardware/software system which incorporates the scientific research results of CSCW area and the available computer and communication technologies.

Group communication (GC) is carried out when two or more partners (human and non-human agents) communicate as a functionally organized set. Group communication systems are usually based on traditional communication systems with additional functions to handle the partners' parallel acts, the group enter and leave.

Multimedia human-computer interaction associates different carriers of information to each other forming a composite input/output channel between human user and computer. Via this composite information transfer channel differently encoded information (like text, images, video, audio etc.) can be emitted or absorbed by the computer. Low level encoding is used as the meaning of the medium which is more explicit than the generally used text, pictures etc.. As a consequence of this definition, the differenly encoded eg. texts are considered as different media altough this interpretation doesn't generally accepted but can be very useful during the technical design of multimedia user interfaces.

Human-human communication is inherently multimedia/multimodal. This type of communication is more effective than using only one individual communication channel. As a result of this fact researchers and computers manifacturers tried to find the ways of the introduction of multimedia communication facilities between human users and computers.

Multimodality has several meanings. It can refer to the sensory modality where the sense by which information is perceived is noted. The second widespread use of this term describes the "modal interfaces". A modal interface is equivalent to an interface with state of interaction and the nonmodal interface is stateless. The multimodality can describe the style of the interaction. At the same moment for initiating the same operation of function different interaction styles (like mouse or keyboard or voice input etc.) can be performed.

2 Taxonomy of Groupware Systems

Dimensions:

- spatial distance (short (co-located), medium (virtually co-located), long (remote))
- temporal distance (short (synchronous), long (asynchronous))
- number of participants (1, 2, small groups, large groups)
- association of participants (1: 1, 1: n, n: m)
- flow of information (one-way, multi-way)
- information sharing (low sharing, high-degree of sharing)
- transferred information (textual, structured (code), multimedia)
- application area (communication/computer technology, collaboration)
- control modes (procedure-, communication-, form-, conversation-oriented)
- control time-spans (seconds, hours, days or more)

2.1 Characterization Based on the Spatial Distance

The spatial distance based characterization is more logical than geographical.

In the case of **co-located** systems (short distance) users are present locally. Usually this type of the groupware system is similar to a meeting room with large projected computer screen. Users usually have LAN connected PCs or workstations. The usual organizationware includes the meeting support systems augmented by different co-authoring (e.g. CoAuthor) systems. The meeting support system is usually a decision or negotiation support system with graphics and textual communication facilities. The co-authoring system usually provides cooperative authoring of (possible multimedia) documents. Addition to these functions several other software can be provided for supporting the different phases of meetings like agenda planning, voting etc..

Virtually co-located users can be far away but real-time video and audio link connect the users and create the feeling of (virtual) co-location. This multimedia technology created media space can be augmented by real-time multimedia conferencing system (e.g. MMConf, Cruiser) which gives an additional control over the usu. analog multimedia communication facilities. Besides the audio and video links the available high-speed communication facility makes the multimedia computer communication feasible and users can share computer screens as well.

Remote type system assumes the cheapest available communication service (usu. E-mail or dial-up services).

From this classification one can realize that the spatial distance based classification is more communication cost dependent than real geographical distance dependent. Therefore a good classification can be based upon the used physical communication lines performance and speed. Traditionally LAN (Ethernet) provides 1-10 MBit/s throughput. The new technology (FDDI) can access the 100 MBit/s throughput. This is more than necessary for full motion video transfer. Using up-to-date compression technology 1.5-2 Mbit/s bandwidth is enough for a motion video transfer (with time delay). In the area of WAN the development of technology is more rapid as the ISDN offers 64 KBit/s, broadband ISDN offers 155 MBit/s throughput. The metropolitan area networks MAN are located between the LAN and the WANs. (DQDB offers throughput up to 100 MBit/s.).

The multimedia information transfer raises the serious problem of the synchronization of different multimedia channels. Simultaneous transfer of video, audio and eg. animation assumes lip-sync synchronization. Nowadays workstations architectures usually do not support multimedia information handling and even the integration of high-speed protocols into workstation architectures is an open problem.

2.2 Characterization Based on the Temporal Distance

Temporal distance based characterization divides the systems into two categories. Users interact either **synchronously** or **asynchronously**. Synchronous interaction assumes the presence of the communicating users at the same time. Asynchronous communication doesn't require the simultaneous presence of users and therefore this type of communication usually takes longer time.

Synchronous systems are typically used for fast communications. Users are simultaneously present and usually investigate interesting problems (real-time conferencing, brainstorming activities). Shared screen technique and simultaneous audio and video links are the most frequently used in this type of groupware systems.

2.3 Characterization Based on the Size of the Group

Different systems are developed for different group sizes. The ftp, telnet, rlogin traditional tools support the individuals and make possible the remote communication or file transfer. Traditional computer conferencing systems or the message handling systems are usually for large groups (national or international wide MHSs). The support of small groups is an open area for the research and development of groupware applications.

2.4 Characterization Based on the Association of Participants

The **one-to-many** communication (multicast) in distributed computer networks is a message transmission mechanism that delivers messages from a single source to a set of destinations. Special cases of multicast are the **unicast** (one-to-one or peer-to-peer) communication which is the traditional area of communication protocol design or the **broadcast** (one-to-all communication). The broadcast mechanism is an abstraction from network (LAN) broadcast while the group communication is an operating system level abstraction as the definition of a group is usually not supported by hardware/firmware mechanisms.

Theoretically a group is a composite object sharing common semantics. The groups are usually formed for

- abstraction the common characteristics of group members or services they provide
- encapsulating the internal state and hiding the inner communications of the members
- providing uniform interface to the world.

The groups of human beings are usually formed according to the same basic rules as other abstract objects presented here.

Characterizations based on the information kind and on the flow of information are well known.

Characterization based on the shared dimension means the classification on the amount of shared information of partners.

Examples:

Message Handling systems

spatial distance: long
temporal distance: asynchronous
number of participants : 2 or more
association : 1: 1 or 1: n
flow : one-way
sharing: low-sharing
transferred information: usually textual

Teleconferencing:

spatial distance: long
temporal distance: synchronous
number of participants : more
association : 1: n, n: m
flow : multi-way
information sharing: high-sharing
transferred information: multimedia

2.5 Characterization Based on the Application Area

The application area taxonomy is based on the intention of the groupware systems. The use of computer and/or communication technology is common for all kinds of groupware applications but different emphasizes exist. The technology oriented system (eg. message handling system) is more concerned about the communication issues than the collaboration oriented one (like GDSS (Group Decision Support System)).

Examples:

Message-Handling Systems : technology oriented

GDSS (Group Decision Support System): collaboration-oriented

Multi-user editor: technology and collaboration oriented

2.6 Characterization Based on Control Modes

The most important part of the group applications is the control of the cooperation of partners. This feature can be considered from two points of view. The first point of view is the *description* and the second is the *prescription* of the control.

The control of cooperation means how the completely unstructured problem is transformed into a structured one having prescriptive rules (explicit controls) to guide the communication between the partners. The software development is one of the best example for unstructured problems. In this type of activity the partners usually cannot describe the steps, the details of the phases of the collaborative task in advance. There are routine cooperation patterns (like office procedures) which can be considered as having the most structured types of control. Between this two extremities different levels of structured patterns of cooperation can be considered.

The description of control in real world groupwork belongs to the scientific research areas of human researches. The prescription of different levels of control is an engineering problem. There is always a trade-off between the completely prescribed control and the unstructured control. In the latter case usually the well known social protocols substitute the prescriptions of control. Different paradigms are available to describe (or prescribe) the control.

2.6.1 Procedure-oriented Control

The office procedure systems try to describe the control using the well-known objects and acts of an office. Usually this means the description of the procedures as composite procedures where different subtasks are combined using a set of operations. The office procedures can be described by (formal) procedural languages. These languages (usu. interpreted by the system) are used for the explicit control purposes. (e.g. COSMOS, AMIGO projects). This approach is more processing oriented than the others described below.

2.6.2 Communication-oriented Control

This paradigm describes the control implicitly and partly. Cooperative work is considered as a series of communications, interactions among partners or active objects. The partners are considered as acting autonomous agents with different roles. The roles correspond to the real life responsibilities of human users. This is very close to the object-oriented programming style where objects communicate via messages. (see. Object Lens)

2.6.3 Form-oriented Control

Form-oriented model belongs to the communication oriented coordination abstraction. It utilizes fill-out forms which are usually used in office environments to transfer the information from one office to an other.

2.6.4 Conversation-oriented Control

This paradigm is based on the observation that human beings usually cooperate through conversations. Therefore it applies a linguistic approach for the description of control. Speech-act theory considers language as a series of actions. Different system describes the cooperation as a network structure with the description of the message exchange patterns.

2.6.5 Control-free Control

More loose mechanisms exist including the control free systems where only very limited control is prescribed or not prescribed at all. The control-free systems are not completely free from any kinds of control as social control is always working. Traditional conferencing systems usually provide basic and minimal control mechanism as a conference moderator is responsible for the communication rules. The task of the moderator can be automatized with floor-control mechanism which decides who can access to the shared workspaces (screen etc.) at any given moment.

In an another type of the systems the partners can agree upon the actual protocols on-the-fly, which control the conversation. These are the most flexible systems although additional phase(s) about the negotiation of the rules are necessary for the work of this type of systems.

Examples:

form-oriented control (forms are usually used in office environments)

procedure-oriented control (the roles of the partners, processing activities)

communication-oriented control (e.g. mail paradigm)

3 Components of Groupware Research

3.1 Interdisciplinary Research of Groupware Systems

The research in the area of groupware systems include the research in the areas of

- social research (psychology, sociology, cognitive science)
- communication technology research
- human-computer interaction research
- distributed system research
- organizational theory research
- multimedia research
- artificial intelligence research
- decision system research

These different disciplinaries can be considered as the different views of the research of groupware systems (group supporting systems). In the following sections selected chapters from distributed system and multimedia user interface research will be presented.

3.2 Social Sciences Research

In the area of groupware research (in CSCW, to be more accurate) the group sociology and group psychology research deal with the problems of human behavior in groups. The behavior of human beings is very dependent from the size of group. From groupware point of view the behavior within small groups is the most important.

3.3 Distributed Systems Research

Distributed systems are natural approaches to the groupware projects as they support the different kinds of cooperations of computers connected by computer networks. It has to be emphasized that distributed systems target the problem of the cooperative work of computers instead of the support of the cooperative work of human users. Therefore it can only be used as a metaphor in the area of CSCW but not directly. The two different approaches have different aims and as a consequence of this fact different solutions are given.

3.3.1 Traditional distributed systems used for groupware applications

- PC networks Autonomous PCs are interconnected and form a PC network. The high-level services of this kind of network incorporate the electronic mail, file transfer protocol. In this network global control doesn't exist the PCs are independent. Users interact by e-mail asynchronously.
- Resource sharing systems The shared resources can be accessible from the connected workstations but the individual workstations provide local environments. The resource sharing is mainly motivated by the high costs of maintaining special resources like disk spaces or ultra-fast CPUs. In this type of systems the control of the shared resources can be centralized or distributed but both cases the users are unaware of the other users' acts. The distributed transparency is usually limited to the access and location and concurrency transparencies.
- Distributed operating systems. The complete control of all resources of the distributed systems is under the control of the operating system. All kinds of the transparencies are maintained. Besides the other kinds of control mechanisms of the distributed operating systems the most frequently used is the client-server model of communication.

These three kinds of distributed systems form a line toward the direction of increased machine cooperation. This can be mapped into the groupware applications. Synchronous groupware systems require highly cooperative distributed system where the components are very dependent of each other. Asynchronous groupware systems can be based on the most autonomous distributed systems like e-mail, therefore the asynchronous group applications can be implemented using loosely coupled workstations (PC networks), where the most important network service is the e-mail.

3.3.2 Transparency in Distributed Systems

Distribution transparency is the collective name of different kinds of transparencies. These transparencies mask out various features of distributed systems. Therefore the control is embedded into the distributed system and cannot be tailored as it is required in the area of groupware.

- Location transparency hides the location of and object in a distributed environment. The location of a server for particular service is not known for the user. The decision about the location of the server is taken by the system and not by the user. (see. naming service in distributed operating systems)
- Access transparency hides the different access methods used inside the distributed systems. The distributed system gives a homogeneous way to access all of the objects of the system. E.g. the RPC (remote procedure call) service completely hides the difference between the local and remote procedure calls.
- Migration transparency hides the moving of the objects inside the system. The users are completely unaware about the migration. Again the decision about the migration is taken by the system. (see load balancing strategies in distributed os)
- Concurrency transparency hides the concurrent access of objects therefore the users are not aware about the shared use of the same object.

- Replication transparency hides the problem of the maintaining of copies of an object in a distributed environment. The system decides about the consistency of the copies of an object. Replication is used to increase the reliability of the global distributed system.
- Failure transparency masks out the problems given by the malfunctions of parts of the system.

3.3.3 CSCW and Distributed Systems' Transparencies

While the distributed systems tend to make the distribution as transparent as possible, groupware doesn't completely want to hide the inner communications and the inner structure of the system from the user. The users of a groupware tool have to have an awareness about the current state of the system and about the actual operations others do. These may affect the future operations of the user. The second important difference between the distributed system approach and the groupware approach is the tailorability of the control structure of the groupware system. The groupware control has to be presented to the users and they may change it according to their needs.

3.4 Multimedia and Multimodal Human-Computer Interaction Research

Computers can be considered as universal machines for information processing tasks. Unfortunately uptill now very few information representation forms could be used by computers as they lack multimedia information gathering tools like the analogues of eyes, ears and other sensors for smell, touch and taste. This limitation limited the application areas of computers as well as the effectivity of the man-machine communications. Altough there are domains where the visual communication is inherent (like picture creation and processing etc.) but the integration of the different media within one system is not well understood. This section provides short introductions to selected areas of multimedia iteraction research.

3.4.1 Interface Models for Multimedia User Interfaces

Conversational Model

Multimedia user interfaces (MUI) are timevarying. This differs from the traditional graphical user interfaces (GUI) where the UI is more or less static. Events are mostly initiated by the user and not by the system. The video, the voice are highly dynamic media where the material moves constantly with few or without logical separators. They extend in time in linear sequences. Animation has few logical divisions which is similar to the gestures what is the newest form of multimedia communication.

Once a time-varying event has happened, the user must either remember the event or replay it to see it again. This raises a new type of UI abstraction: the user can move backward or forward in time. The roots of this abstraction are in the multi-level undo operations of the traditional GUIs or the version control subsystems where one can ask for previous versions (past versions) of an object or document. In the presence of timevarying media this task is more difficult. When the user asks for a repetition, the whole previous state of the MUI have to be revitalized including all media types. And further, it is not so simple that the media have to be repeated, because the previous state of the synchronizations between media have to be repeated as well.

From the elementary abstractions more structure abstractions can be built. This leads us to the models of the conversation. In the verbal communications the backward move in time is called repetition. When an incomprehensible statement is heard by one, he or she can ask for to repeat it again. Sometimes this doesn't help to much. The repeated sentence is as incomprehensible as the original was. A different model would be necessary from comprehensible point of view.

The mapping of the natural verbal conversation into the MUIs can be considered as a new way in the design of MUIs. In the case of natural verbal communication people can interrupt, query, repeat, repeat using an other phrase etc. thus the moving in time backward and forward is the everyday practice. The conversation consists of small fragments which are considered as basic blocks of the conversation. During the conversation some blocks have outstanding status. These blocks constitute

the semantical environment of the conversation. The participants can refer to these blocks directly or indirectly. They can repeat, rephrase, explain etc. these elementary blocks. Navigation in the semantical environment is controlled by human interaction protocols, agreed procedures well known for the participants. Turns, corrections, confirmations etc. are the protocol elements of these types of protocols. During conversations usually one element of the semantical environment is focused therefore the indirect referencing can be frequently possible which can speed up the conversation a lot.

Cognitive model incorporated into multimedia user interface design

In the design of MUIs the previously described features of the natural human communications can be applied. From theoretical point of view MUI can be considered as a two-party conversation between the human user and the computer system. In both parties' "minds" a conceptual model of the other participant can be built.The conceptual model of MUI can be described in manuals therefore it can be easily accepted by human. Unlikely the model of human beings which can be assembled only during the session on-line, real-time. During the conversation these models are changing according to the information sensed about the other participant. The conceptual model of the human user can help for the MUI to predict the future behavior of human being, the next user initiated actions which are mostly likelihood. Based on this prediction MUI can prepare the different media' channels for the possible user action. The conceptual model of human behavior can be built using FSM-NLP cognitive model. In the case of the new media types this preparation can be time consuming, CPU intensive operations (rendering the next frame, decompressing the stored video chunks etc.). Using even the state-of-the-art multimedia technology for gaining the best response time the prediction of the next user action is necessary. Modeling of the human users and their multimedia interactions therefore is one of the most critical research direction which can be directly applied in the MUI design process.

The two-party conversational model can be modified in such a way that the role of the MUI is played by an intelligent agent thus the previously described asymmetric situation becomes more symmetric. This agent acts like anthropomorphic agent and guides the human users through the complex navigation process in the multimedia semantical state space. We can go further. This intelligent agent can not only predict the user next actions but anticipating the user behavior it can suggest particular way to the direction of the users goal. This is a more active behavior than in the previous case when only a mechanical prediction could help in the more efficient utilization of the available resources.

3.4.2 Audio in Multimedia User Interface

Although almost all modern computer interfaces contain audio input/output devices, nowadays the usage of the audio interface is limited to signaling some primitive sounds like beeps etc.. From practical point of view two types of audio output can be used. The use of the speech type is obvious. Recorded or synthesized speech can guide the user or can give a user feedback. One excellent example is the NeXT computer system where prerecorded voice of a British accent women will let you know that "your printer is out of paper". The non-speech type of audio communication is a relatively new area in the UI design. Although non-speech audio signals have been used by societies for centuries, the usage of these type of audio in computer conversation is rare and primitive. The non-speech communication is considered more ancient than the verbal one but this doesn't explain the infrequent application of it. Even in our modern society different voice signals (like doorbells etc.) are used. The music is considered as one of the most effective way of communication where the main goal is emotion transfer. Unfortunately the understanding of music (musical language) needs deep education but in different societies this education can be received via non-formal educational methods. The information as well as the emotion transfer capability of music can be used in the MUI design. As the researches about human perceptions pointed out that the perception of audio works parallel with the other human sensors, the application of the human audio channel gives an untouched opportunity to the direction of the most efficient multimedia information transfer from a computer to a human being.

The **audio icon** concept was suggested by different researchers. The audio icon is a digitalised sound (knocking, falling etc.) which can remember the human user about an event has happened

parallel.

Another similar construction called **earcon** suggested by Blattner contains audio message. The earcon is composed from musical fragments (motives) of different audio (musical) parameters like rithm, pitch or timbre etc. From the elementary motives more complex earcons can be combined. The compositional methods can include the simple sequencing of the different motives after each other or it can include more sophisticated methods like musical transformations of the motives. After the transformation the inherited musical attributes of the original motives have to be recognized by the user therefore the "c[illegible]sible distance" between the original and the transformed motive have to be kept inside an interval. A very early application of the earcon concept could be found in the late sixties. In different machines the instructions of the CPU are mapped into voices with different frequencies which can be heard by the human operators. At that time the state of the operating system, the actual instructions under the execution could be heard and the operator could be notified about it. An infinite cycle produced noise ("music") could be identified easily.

The phase attributes of voice make 3D spatial information. This can be transferred if more than one audio channel (at least three for 3D effect) is offered by MUI. The modern computers can process voice real-time using attached digital signal processor (DSP). DSP can create different **3D audio** illusions. This tends to the area of virtual reality therefore it will be discussed there.

Interesting new idea is the data retrieval using audio effects. Different kinds of data is visualized using small 2D visual icons. The shape of an icon corresponds to the data it represents. The small icons cover the surface of the display and it gives a texture. Moving the mouse over this texture an audible noise is generated according to the shapes of the small icons. In this way the texture can be audible and it can give an additional information for searching a particular kind of data piece.

3.4.3 Smelling

The smelling system of human body is one of the most sensible sensor as very small quantity of material can be sensed by it. Unfortunately the information transfer speed with smell is one of the lowest among the other possibilities as the distribution of the smell based on the rules of the thermodynamics. The second problem with the human smelling system is the fast adaptability of the sensor (hiding effect). Due these problems the user interface designers are not considering the problem of how information transfer by smelling can be implemented. The virtual reality researches may incorporate this possibility but in very few special cases.

3.4.4 Gestures

Besides the audible information the natural verbal communication is usually associated with nonverbal, gesture communication. This itself belongs to multimedia information transfer as the gesture gives the feeling of spatial, time-varying information transfer synchronized with the speech. The gesture communication is a very new area of research. One direction in this field uses and transfers the gestures of human users in a collaborative environment. Here the gestures give an additional communication channel to the other channels.

One can try to use the gestures in an other way. In this case the gesture is mapped into useful actions. For this type of approach new kinds of sensors are necessary. Besides the optical recognition of gestures other new input devices can be developed. One candidate is the DataGlove of the AT&T Bell Labs which can sense the hand gestures of the human users.

3.4.5 Virtual Reality

The ultimate territory of computer user interface design is the research in area of virtual reality. This is nothing more but the artificial construction of a 3D reality where user interacts in real-time with objects generated by the computer system. The creation of the illusion of reality is mainly depends on the interactive computing power used for the generation of these virtual objects. This is still behind the abilities of the present computer systems.

Computer graphics algorithms are used to create this illusion. The development in this area is pretty fast. Only a matter of time when the real illusion for the human visual sensor can be created. But as virtual reality must use all the senses besides the visual aspects, the auditory and tactile aspects are important as well. The 3D sound system can give an attractive solution. However the research in the area of the tactile sensation and tactile user feedback (tactile feeling) of the virtual objects is relatively new and active area. Minski et al. have been studying the problem of feeling of textures of virtual objects. The synchronization between the different multimedia types is again a serious question.

From multimedia groupware application point of view the problem how the multimedia information can be shared and can be transferred from one geographical point to another is considered an important question. Even if we consider the simple replicated software architectures the amount of information to be shared is growing exponentially and as a consequence of this fact it can easily outgrow our present multimedia information handling possibilities.

3.4.6 Conceptual Modeling of Multimedia Documents

A conceptual model of traditional documents was developed by ISO, ODA/ODIF (Office Document Architecture and Interchange Format) standard. This model is more or less finished conceptual model of traditional paper documents consisting of pages. A page can contain formatted text, graphics and image. In this model the document is represented by two conceptual structures namely the logical structure and the layout structure. The logical structure of a document describes the usual volume, chapter, section subsection etc. structures of the document. The layout gives information about the presentation formats of the different logical structures. Using this two syntactically similar but semantically different structures one can describe the whole document where the pieces of content are mapped to the elements of these structures. The content can be uninterpreted text or image or graphics. This model can be augmented by multimedia type information where the content pieces can also include voice, video, animation etc. Unfortunately this augmented model cannot give more information about the semantics of the document. One can conclude that the model described above can handle only the syntax of the document (the logical structure can be considered as semantics mapped into syntax) but the semantics is uninterpreted. For a more sophisticated retrieval a new model would be needed about the semantics of document, which is more challenging as the formal model may include model of pure text and visual images, voice, video etc. as well. A separate standardization activity is the EDI (Electronic Data Interchange) direction.

Example: MULTOS model

Besides others the MULTOS ESPRIT project is one of the first approach to deal with multimedia documents. It uses a multilevel representation formalism for document presentation. The levels of the representations are the following:

- conceptual,
- logical,
- layout

views. These representation levels (views) are unified into a unique representational framework in order to allow the user to manipulate on these views uniformly without distinction about which views object is used e.g. for a query etc. The MULTOS document model incorporates the standard ODA model for the logical and layout levels but the conceptual level is defined outside ODA. The conceptual view is given by a conceptual structure in addition to the logical and layout structure. The conceptual structure elements are connected with the elements of the logical structures in different levels of details. The conceptual structure is also considered as a tree of conceptual elements. These two trees can be connected by the leaves when the connection simple refers to a basic content portion of the content or by higher levels where the conceptual structure is associated with a high

level logical element (e.g. a conceptual element describes the semantics of a possibly large logical part composed of several paragraphs or chapters etc.).

The MULTOS model support the generalization idea as well. Document types can be defined and after individual documents can be instantiated having the same structure. This can shorten the description and can give the possibility to build efficient access methods to a class of documents. The weak document type was introduced as a way to deal with the different types of multimedia documents. The weak type allows partial specifications where some of the components are unspecified. Even the types of substructure is not defined in advance. This gives the possibility to specialize the unspecified component into different types. In this way a family of specifications can be constructed.

The conceptual structure (with the connections to the element of the logical structure) can be considered as a restricted object-oriented semantic data model where the "part of" and the "is as" relations are used. The levels of the conceptual structure give the "part of" relations and the connections can be considered as "is as" relations.

The problem of the conceptual modeling of multimedia information (e.g. images) is one of the most difficult question. The problem is how can the different visual objects be recognized and how to recognize the relations of the recognized objects. Different image recognition procedures can be used to recognize the basic objects on images. The set of basic objects is application dependent and more or less fixed for the different application areas. The building structures of the complex visual objects are domain-specific as well. Therefore the recognition of the basic objects and the derived complex objects can be considered as the recognition of a domain-specific visual language. After the analysis of the current image, the search for similar images can be performed to a certain degree. Combined approach based on the uncertain images analysis and the more exact text oriented retrieval can also be used with better effectivity.

3.4.7 Multimedia Retrieval Problem

Multimedia documents are pieces of structured information containing text, image, graphics, voice, animation, video etc. The manipulation on these documents can be classified into different categories including the create, edit, store, retrieve, delete etc. operations.

The multimedia retrieval problem is to identify the multimedia documents that contain information match to user queries. Conventional document retrieval systems can be divided into two categories:

- keyword based retrieval system
- full-text retrieval system

Keyword based text retrieval systems are based on the textual records associated with the documents. These records can be created manually or automatically. The searching strategy is equivalent to the text search strategy in record database. Here the document model is a simple set of keywords attached to the original text of the textual document.

Full-text based retrieval systems based on the whole text content. Here associated attributes can enrich the document model but the document model can be considered as a list of words which can be searched. The search strategy is usually supported by different types of index mechanisms. Beyond the flat file model more structured document model can be built on the top of this system where the document can be divided into smaller blocks, chapters, subchapters, sections etc. The attributes can be distributed and attached into the blocks. The complete document model can be mapped into a tree structure where the chapters etc. are represented by nodes of the tree and attributes are attached to the nodes. In this case the retrieval algorithm is more complex.

The retrieval efficiency and the effectiveness are the two most important measurable parameter that can be used to compare different retrieval systems.

The efficiency is measured by the

- system response time,
- user effort to perform the retrieval and the
- form of the presentation of the searched document(s).

The effectiveness is the parameter of the

- recall of relevant documents and the
- precision of the recall.

Multimedia documents containing text, voice, images or video etc. require more effort to retrieve. The retrieval of multimedia documents would be equivalent to the retrieval of text based documents if the attached media information (voice, image etc.) do not give more searchable possibility to the user. The image, graphics, voice enriched text offers a new dimension of retrieval. This new dimension can be classified by two coordinates. The first attribute which can be used in a search is the syntax and the second one is the semantics of the attached multimedia information.

Example: Multimedia Query Language

Based on the abovementionden multimedia document model a new query language was defined. This query language has the capability to

- navigate through the different document structures (using the path construction).
- specify the conditions on both the content and conceptual structure of the documents including the content of images
- querying complex components (applying the conditions to all subcomponents of the complex one)

Natural Language as Multimedia Query Language

The use of the natural languages as multimedia query languages is one of the most wanted target. The research into the direction of natural language understanding (syntax and semantics of natural languages) will fertilize this subdomain.

Handling of Distributed Multimedia Documents

An approach to extend the multimedia document model into direction of the distribution can be developed. Here two different main areas can be considered. The first is dealing with the different spatial locations of the parts of documents. The hypertext, hypermedia document handling systems tend to this direction.

The second direction belongs to the areas of groupware where the users of the multimedia documents are distributed and the documents are shared by the possible remote users. The problem of handling distributed documents by distributed group of users can be considered as the most general idea where the cross-fertilization of different research areas (like groupware, hypermedia, shared workspace research etc.) can conclude interesting new ideas.

4 Open Problems

1. Generalization of the conception structures in order to incorporate connections to the other (like layout) structures as well.
2. Dealing with the uncertain questions and fuzzy ideas

3. Handling the cultural background (the conceptual model of the user and the application domain)
4. Prediction based on the conceptual model of the user
5. Development of new query languages based on the new hierarchical model of documents
6. Conceptual description of media types like video and audio
7. Automatic classification of documents based on the conceptual descriptions

References

[BBB92] Thomas Baudel, Michel Beaudouin-Lafon, Annelies Braffort, Daniel Teil "*An Interaction Model Designed for Hand Gesture Input*" LRI Research Report No. 772, University de Paris-Sud, Centre d'Orsay, Laboratoire de Recherche en Informatique, Sep 1992.

[DBl91] Paul Dourish, Sara Bly "*Portholes: Supporting Awareness in a Distributed Work Group*" Technical Report EPC-91-133 Rank Xerox EuroPARC, 1991

[BDa92] Meera M. Blattner, Roger B. Dannenberg "Multimedia Interface Design" ACM Press, Addison-Wesley Publishing Comp. 1992,

[BDM91] Victoria Bellotti, Paul Dourish, Allan MacLean "*From Users' Themes to Designers's DReams: Developing a Design Space for Shared Interactive Technologies*" Technical Report EPC-91-112 Rank Xerox EuroPARC, 1991

[Bea91] Michel Beaudouin-Lafon "*User Interface Management Systems: Present and Future*" Eurographics, Vienna, September 1991, in:Construction d'interfaces et nouvelles dimensions de l'interaction homme-machine, LRI Rapport no. 766. Universite de Paris-Sud

[BHa91] Liam Bannon, Richard Harper "*Computer-Supported Cooperative Work, A Brief Introduction*" Technical Report EPC-91-115 Rank Xerox EuroPARC, 1991

[BHI93] Sara A. Bly, Steve R. Harrison, Susan Irwin "*Media Spaces: Bringing People Together in a Video, Audio and Computing Environment*" Communictions of the ACM, Vol. 36, No. 1 January 1993 pp. 28-47.

[BBK92] Miklós Bíró, Ede Bodroghy, Attila Bor, Elöd Knuth, László Kovács "*The Design of DINE: A DIstributed NEgotiation Support Shell* Decision Suport systems: Experiences and Expectations. Proceedings of the IFIP TC8/WG8.3 Working Conference Fontainebleau, 1992, North-Holland, 1992, pp.103-114. (IFIP Transactions A-9)

[Bla92] Meera M. Blattner "*Messages,Models and Media*" Multimedia Review Vol.3.No.3. Fall 1992. pp.15-21

[DMo91] J. Dittrich, E. Moeller "*BERKOM Reference Model, Application - Oriented Layers, Groupware Report*" DETECON, Technisches Zentrum Berlin, September 1991.

[Dou91] Paul Dourish "*Godard: A Flexible Architecture for A/V Services in a Media Space*" Technical Report EPC-91-134 Rank Xerox EuroPARC, 1991

[Fin92] Alain Finkel "*Une formalisation de l'expérience subjective*" Rapports de Recherche, Laboratoire d'Informatique Fondamentale et Appliquée de Cachan, 92-4, December 1992 pp. 1-33

[FKR93] Robert S. Fish, Robert E. Kraut, Robert W. Root, Ronald E. Rice "*Video as a Technology for Informal Communication*" Communictions of the ACM, Vol. 36, No. 1 January 1993 pp. 48-61

[Gav91] William W. Gaver "*The Affordances of Media Spaces*" Technical Report EPC-91-132 Rank Xerox EuroPARC, 1991

[GMM91] William W. Gaver, Thomas P. Moran, Allan MacLean, Lennart Lovstrand, Paul Dourish, Kathy Carter, William Buxton "*Realizing a Video Environment: EuroPARC's RAVE System*" Technical Report EPC-91-121.1 Rank Xerox EuroPARC, 1991

[Gra91] William W. Gaver "*Sound Support for Collaboration*" Technical Report EPC-91-101 Rank Xerox EuroPARC, 1991

[GOS91] Nicolas Graube, Tim O'Shea "*An Architecture for User Control of Active Badge Systems*" Technical Report EPC-91-123 Rank Xerox EuroPARC, 1991

[KBL92] Alain Karsenty, Michel Beaudouin-Lafon "*An Algorithm for Distributed Groupware Applications*" LRI Research Report No. 785, University de Paris-Sud, Centre d'Orsay, Laboratoire de Recherche en Informatique, Dec 1992.

[KCa92] Simon M. Kaplan, Alan M. Carroll "*Supporting Collaborative Processes with Conversation Builder*" Computer Communicatios Vol. 15 No. 8. October 1992, pp. 489-501

[KMW91] Herb Krasner, John McInroy, Diane B. Walz "*Groupware Reserarch and Technology Issues with Application to Software Process Management*" IEEE Tansactions on Systems, Man, and Cybernetics Vol. 21. No. 4. July/August 1991 pp. 704-712.

[KRB92] Alain Karsenty, Christophe Tronche, Michel Beaudouin-Lafon "*GROUPDESIGN: Shared Editing in a Heterogeneous Environment*" LRI Research Report No. 804, University de Paris-Sud, Centre d'Orsay, Laboratoire de Recherche en Informatique, Dec 1992.

[Kov92] László Kovács "*Experimental Distributed Document Preparation System* NSC'92, Network Services Conference, Pisa, Italy, 1992

[LCN90] Luping Liang, Samuel T. Chanson, Gerald W. Neufeld "*Process Groups and Group Communications: Classifications and Requirements*" COMPUTER Februar 1990, pp. 56-66.

[MRT91] Carlo Meghini, Fausto Rabitti, Costantino Thanos "*Conceptual Modeling of Multimedia Documents*" COMPUTER October 1991, pp. 23-29.

[MOS090] Margaret Minsky, Ming Ouh-Young, Oliver Steele, Frederick P. Brooks, Jr "*Feeling and Seeing: Issues in Force Display*" Computer Graphics, Vol. 24. No. 2. pp. 235-243. March 1990

[NEL91] William M. Newman, Margery A. Eldridge, Michael G. Lamming "*Pepys: Generating Autobiographies by Automatic Tracking*" Technical Report EPC-91-106 Rank Xerox EuroPARC, 1991

[RCJ91] Jonathan Rosenberg, Gil Cruz, Thomas Judd "*Presenting Multimedia Documents Over a Digital Network*" Bellcore, October 25, 1991, in: Computer Communications May 1992,

[RBl91] Tom Rodden, Gordon S. Blair "*CSCW and Distributed Systems: The Problem of Control*" ECSCW'91, Amsterdam, September, 1991

[RBl92] Tom Rodden, Gordon S. Blair "*Distributed systems support for computer supported cooperative work*" Computer Communicatios Vol. 15 No. 8. October 1992, pp. 527-538

[RKG91] Jonathan Rosenberg, Robert Kraut, Louis Gomez, C. Alain Buzzard "*Multimedia Communications: a User-centered Viewpoints*" Bellcore, September 18, 1991

Privacy Enhanced Mail - Concepts and Experience

Dr. Peter Lipp
Institut für Angewandte Informationsverarbeitung
Technischen Universität Graz

Abstract:

This Paper gives an overview on Privacy Enhanced Mail, which is a standard currently under development in the Internet Environment and discusses experiences made in the COSINE P8 Project.

1. Introduction

As electronic mail has become widely used all over the world, its privacy has become more and more important. Traditionally, electronic mail was secured only loosely: at least the superuser of every machine the mail went through was able to read it. This is still true, but as the awareness of users has increased, things have started to move. In 1987 the members of the IAB privacy task force published the first concept of Privacy Enhanced Mail (PEM) in the Internet RFC 989[1]. Since then, discussions and development was ongoing, and only recently the PEM Working Group published the (maybe nearly) final version of the PEM-Standard in the RFC's 1421-1424. And work is still ongoing. This paper gives an overview on PEM and discusses the experiences made with using PEM in the Cosine-P8 Security Pilot. COSINE is concerned with the objective of creating a common operational OSI interworking infrastructure to support all European research. Security has been identified as a key element in the generation of user confidence in the service.

[1] RFC stands for *Request for Comments*. All internet-standards are published in that form.

The COSINE P8 Security Project, *Development and Proving of Security Mechanisms*, was a two-phase pragmatic project. Its aim was:

- to specify a general security architecture for COSINE and to specify how this architecture will be implemented for the P8 Pilot applied to selected services.
- to implement the design and to test and evaluate the operational pilot security services [COSD6].

PEM was one of the main elements of the implementation phase of COSINE and thus enabled the participants to gain experiences in the usage of PEM.

2. Privacy Enhanced Mail

Privacy Enhanced Mail (PEM) offers privacy enhancement services on top of existing mail systems through the use of end-to-end cryptography between originator and recipient processes, which are integrated into the user-agent (UA) or, alternatively, pre- or post-process messages. There is no processing required in the message transfer agents (MTA), so that any existing mail-infrastructure can easily be used without change (as long as it confirms to the RFC822 rules). The following attributes of PEM makes the goal of keeping up with the Internet's heterogeneousity more clear [RFC 1421]:

- The mechanisms allow interoperability among a broad range of systems.
- All enhancements are implemented at the application layer and are independent on any features of the lower layers.
- The defined mechanisms are compatible with non-enhanced internet components.
- The defined mechanisms are compatible with a range of mail transport agents.
- The defined mechanisms are compatible with a broad range of mail user agents.
- The defined mechanisms allow electronic mail privacy enhancement to be performed on personal computers separate from the systems on which UA functions are implemented.
- The defined mechanisms are support privacy protection of mailing lists.
- The defined mechanisms are compatible with a variety of key management approaches (manual pre-distribution, key-distribution centres based on symmetric cryptography, public-key certificates).

In detail, PEM provides the following facilities:

- disclosure protection
- originator authenticity
- message integrity measures
- non-repudiation of origin (if asymmetric keys are used)

PEM does not address

- access control
- address list accuracy
- assurance of message receipt and don-deniability of receipt
- message duplication detection
- replay prevention

The sender of a message determines, if privacy enhancements are to be performed. Thus he has to consider the ability of the recipient to handle privacy-enhanced messages. Messages can be transmitted in one of three forms:

ENCRYPTED: confidentiality, authentication, integrity and non-repudiation of origin security services have been applied.

MIC-ONLY: authentication, integrity and non-repudiation of origin security services have been applied. Messages are not encrypted but are encoded to protect their text against modifications. A message-integrity-code (MIC) is appended to the message.

MIC-CLEAR: the same services are applied as for a MIC-ONLY message. The messages are not encoded. Thus a message of this type can be read by a recipient without the necessary PEM-software.

2.1. Message processing

The basic element for providing the facilities is encryption. Currently two algorithms are supported: DES in CBC[2)] mode as a symmetric method and RSA[3)] for public key cryptography. Both methods need keys. PEM uses a two-level key-hierarchy: **Data encrypting Keys** (DEK) are used for encryption of messages and for computation of a message integrity checksum; **Interchange Keys** (IK) are used for encrypting DEK's for transmission within messages. The same interchange keys are normally used for all messages exchanged between a given originator to a given recipient over some period of time. DEK's are different for each message transmitted. The DEK usually is a key for a fast symmetric algorithm. The IK used for DEK encryption can be a key for a symmetric algorithm or the public key component of the private/public key pair of the recipient. For calculating MICs, the same IK is used in the symmetric case while if using an asymmetric algorithm, the private component of the originator is used.

When an outgoing message is processed, a new DEK-key is generated. Then a four-phase transformation procedure is employed:

1. A plaintext message is accepted in local form using the host's native character set and line representation.
2. The local form is converted to a canonical representation, defined as equivalent to the inter-SMTP representation of message text. This representation forms the input to the MIC computation and encryption processes.
3. The encrypted message (or the unpadded canonical form for MIC-ONLY messages) is then encoded into a printable form. This form is composed of a restricted character set which is chosen to be universally re presentable across sites and which will not be disrupted by processing within message transfer entities.

---

2) Data Encryption Standard / Cypher Block Chaining-mode

3) Rivest, Shamir, Adleman

```
-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type: 4,ENCRYPTED
Content-Domain: RFC822
DEK-Info: DES-CBC,BFF968AA74691AC1
Originator-Certificate:
MIIBITCCASCCAWUwDQYJKoZIhvcNAQECBQAwUTELMAkGA1UEBhMCVVMxIDAeBgNV
BAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMQ8wDQYDVQQLEwZCZXRhIDExDzAN
BgNVBAsTBk5PVEFSWTAeFw05MTA5MDQxODM4MTdaFw05MzA5MDMxODM4MTZaMEUx
CzAJBgNVBAYTAlVTMSAwHgYDVQQKExdSU0EgRGF0YSBTZWN1cml0eSwgSW5jLjEU
MBIGA1UEAxMLVGVzdCBVc2VyIDEwWTAKBgRVCAEBAgICAANLADBIAkEAwHZHI7i+
yJcqDtjJCowzTdBJrdAiLAnSC+CnnjOJELyuQiBgkGrgIh3j8/x0fM+YrsyF1u3F
LZPVtzlndhYFJQIDAQABMA0GCSqGSIb3DQEBAgUAA1kACKr0PqphJYw1j+YPtclq
iWlFPuN5jJ79Khfg7ASFxskYkEMjRNZV/HZDZQEhtVaU7Jxfzs2wfX5byMp2X3U/
5XUXGx7qusDgHQGs7Jk9W8CW1fuSWUgN4w==
Key-Info: RSA,
I3rRIGXUGWAF8js5wCzRTkdhO34PTHdRZY9Tuvm03M+NM7fx6qc5udixps2Lng0+
wGrtiUm/ovtKdinz6ZQ/aQ==
Issuer-Certificate:
MIIB3DCCAUgCAQowDQYJKoZIhvcNAQECBQAwTzELMAkGA1UEBhMCVVMxIDAeBgNV
BAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMQ8wDQYDVQQLEwZCZXRhIDExDTAL
BgNVBAsTBFRMQ0EwHhcNOTEwOTAxMDgwMDAwWhcNOTIwOTAxMDc1OTU5WjBRMQsw
CQYDVQQGEwJVUzEgMB4GA1UEChMXUlNBIERhdGEgU2VjdXJpdHksIEluYy4xDzAN
BgNVBAsTBkJldGEgMTEPMA0GA1UECxMGTk9UQVJZMHAwCgYEVQgBAQICArwDYgAw
XwJYCsnp6lQCxYykNlODwutF/jMJ3kL+3PjYyHOwk+/9rLg6X65B/LD4bJHtO5XW
cqAz/7R7XhjYCm0PcqbdzoACZtllETrKrcJiDYoP+DkZ8k1gCk7hQHpbIwIDAQAB
MA0GCSqGSIb3DQEBAgUAA38AAICPv4f9GxtY4+p+4DB7MV+tKZnvBoy8zgoMGOx
dD2jMZ/3HsyWKWgSF0eH/AJB3qr9zosG47pyMnTf3aSy2nBO7CMxpUWRBcXUpE+x
EREZd9++32ofGBIXaialnOgVUn0OzSYgugiQ077nJLDUj0hQehCizEs5wUJ35a5h
MIC-Info: RSA-MD5,RSA,
UdFJR8u/TlGhffH65ieewe2lOW4tooa3vZCvVNGBZirf/7nrgzWDABz8w9NsXSexv
AjRFbHoNPzBuxwmOAFeA0HJszL4yBvhG
Recipient-ID-Asymmetric:
MFExCzAJBgNVBAYTAlVTMSAwHgYDVQQKExdSU0EgRGF0YSBTZWN1cml0eSwgSW5j
LjEPMA0GA1UECxMGQmV0YSAxMQ8wDQYDVQQLEwZOT1RBUlk=,
66
Key-Info: RSA,
O6BS1ww9CTyHPtS3bMLD+L0hejdvX6Qv1HK2ds2sQPEaXhX8EhvVphHYTjwekdWv
7x0Z3Jx2vTAhOYHMcqqCjA==

qeWlj/YJ2Uf5ng9yznPbtD0mYloSwIuV9FRYx+gzY+8iXd/NQrXHfi6/MhPfPF3d
jlqCJAxvld2xgqQimUzoS1a4r7kQQ5c/lua4LqKeq3ciFzEv/MbZhA==
-----END PRIVACY-ENHANCED MESSAGE-----
```

Fig. 1: Example for a privacy enhanced message.

4. The output of the previous steps is combined with a set of header fields (so-called *X-header-fields*), containing information about the details of the transformations applied to the original message, and are necessary to enable the receiver to decrypt or verify the integrity and authenticity of the message. The message is then transmitted to the recipient as a normal mail message. An example for an output of this process is figure 1.

2.2. Certification

A key problem when using PEM is the distribution of keys between users. In the symmetric case, each pair of users has to agree upon one pair of interchange keys, which then are used to encrypt the DEK's. The better alternative is to use a public key system, which is easier to handle: a

Fig. 2: a certification authority

directory can be used, which contains the public keys of all or a subset of possible recipients. To be sure that no fake keys can be distributed that way, PEM uses a X.509 based certificate mechanism. A certificate is a data structure that contains the name of a user, the public key component of that users key and the name of the issuer of the certificate (called certification authority). This issuer guarantees that the public component is bound to the named user. This data is signed cryptographically with the private component of the issuers key. So, if an application sees such a certificate, it can verify its contents by using the well known public key component of the issuer. This could be the case if e.g. two users A and B were member of the same organisation and a

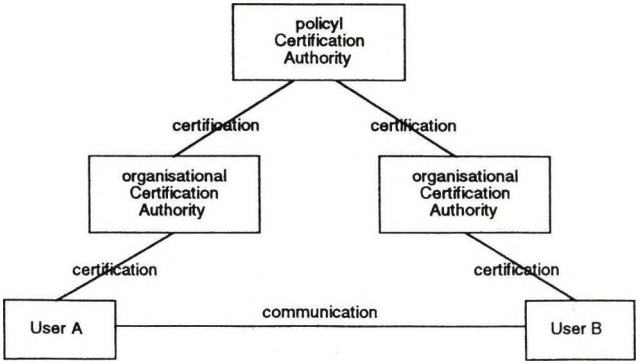


Fig. 3: hierarchical certification scheme

certain department in that organisation would implement the local certification authority (Fig. 2). If two users A and B of different organisations or even countries want to communicate, they might not know or even trust the other users certification authority and their public key component respectively. So this mechanism introduces an hierarchy of certification authorities: the certificate which binds user A's name to his public key component is signed by certification authority C1. This can be an organisational CA (for users bound to some organisation) or a residential CA (for other users, resident in their CA´s area). This certification authority owns a public key component (which can be used to verify the signature of C1's certificate) which itself is signed by another certification authority, say C2. This normally would be a Policy CA (PCA), which could be establish one per country or similar and have published their policies for registration of users and organisations. Each PCA is certified by the *top level certification authority*, the IPRA (Internet Policy Registration Authority). Any user or PEM-software has to know the public key component of the top-level certification authority.

Certificate have a limited lifetime. If one e.g. looses his private key component, or it was stolen, any thief or finder could impersonate his electronically. In this case, I'd better revoke my certificate at the certification authority. Each certification authority sends out revocation lists so that all the users can check other users certificates for validity.

3. Cosine P8

As already was said above, COSINE is concerned with the objective of creating a common operational OSI interworking infrastructure to support European research. One of the key elements for creating user confidence in the services identified was security. COSINE P8, a sub-project of COSINE, specified a general security architecture and specified implementation guidelines for a pilot project.
Discussions with potential participants of a pilot project made clear, that users are essentially interested in end-to-end security. A wide range of potential applications could have been supported with security services. In practice, however, only a few of them are used regularly on a wide-spread scale. Among those, electronic mail and remote access were chosen. These applications were the most promising to find enough users to set up a pilot project with reasonable size, such that the results could be considered convincing. Therefor it was decided to add PEM-functionality to electronic mail and to implement access control and secure association for remote access.

3.1. Electronic mail

For electronic mail, X.400(1988) would have been a good and logical candidate, because security services are explicitly supported (which is not the case for X400(1984)). However, no implementations of X.400(1988) were available in COSINE and it was thought unrealistic to install the software and its security functions in time. Time restrictions were also responsible for not considering the use of X.500 as a directory service, which also supports the necessary security services defined in X.509.
For the COSINE P8 pilot, PEM-formatted mail was carried over X.400(1984) MHS and Internet-SMTP infrastructure. During the pilot, an implementation of PEM by Baltimore Technologies, Dublin, Ireland, based on the SECU-DE library by GMD, Germany, was used. This library

provides users with all functions necessary for developing secure applications: encryption with RSA and DES, key management, calculating MICs and also provides PEM-functionality. The participants tested the implementation by sending around 10000 messages among 40 users. The participants were:

- JANET, UK
- SURFnet, Netherlands
- Trinity College, Ireland
- Technische Universität, Graz
- Fachhochschule Rheinland-Pfalz, Germany
- Universitat Politecnica de Catalunya, Spain
- GMD, Germany
- University College London, Great Britain

3.2. Access control and secure association for remote access

The second application chosen was secure access control and secure association for remote access to the Cosine Security Domain Certification Authority (CSDCA). It was realised as an application program without need for system modifications. The initial dialogue-procedure authenticated both the Certification Authority to the user and the user to the CA. After initialisation, all communication is done in a secure way (by using stream-encryption).

The purpose of the CSDCA is to provide the necessary certification functions for the COSINE Security Project, including the secure generation of RSA-key-pairs; secure issuing of the secret key to the owner and the publication of the certificate. Two possibilities exist to generate a certificate:

- The user is well known to the CA. In this case, there are means to communicate with that user and the private key component can be delivered by mail or courier or so. Initial members of the project and official representatives of participant groups fell in this category.
- If the user is not personally known to the CSDCA, he must be "recommended" by a user who is already known and already has a private key component. The private key component is then created and delivered to the recommendor, whose responsibility then is to forward it secretly to the recommended user.

4. Experiences made using PEM

In November 1992 the testing phase began. Every participant site had to nominate five users, whose responsibility it was to send one message each week to every other user. A rota was produced by Baltimore, which informed every user, if he should send either a

- correct privacy enhanced message or a
- privacy enhanced message created for a different user (such that the recipient should not be able to read that message) or a
- privacy enhanced message which has been tampered with (manually, by the sender; either the encrypted message or the key information was changed).

Receiving the message, the user had to try to read it and then fill in the rota with the results.

Technically this procedure proves the correctness of the implementation. The results as are known today (the final evaluation has not been published yet) show, that practically

- no message that should have been readable was unreadable and
- no message that should have been unreadable was readable.

In the rare cases in which the opposite was the case, the reasons were

- the sender used an old public key of the recipient (either because he did not care to contact the CA or he had technical problems connecting to the CA),
- the sender sent messages not confirming to the rota or
- the sender did not manipulate the messages correctly: the modifications were lost or not done at all.

To a much larger extent, lots of mail messages sent (or claimed to having been sent) did never reach the recipient. For example, no message sent from Graz to Janet ever reached its destination. It was beyond the scope of this project to clarify the reasons for those events, but it showed, how unreliable the existing mail systems still are.

There is another view of the experience made with the system: the user side. Because of the hetereogeneousity of the users environment (machines, operating systems, user agents, message transfer agents) it was inconceivable to integrate PEM-functionality seamlessly into all those systems. Thus, only a rigid command line interface was available, which was improved on some sites by simple scripts to ease the usage of the software. It was a generally accepted fact, that this was o.k. for the pilot phase but inconceivable for regular use. The participants were somewhat urged to find other users and uses of the package, but it seemed reluctant to try not having it integrated into the user agents. So the usage of the software was mainly limited to the pilot project.

Moreover the certification procedure was too inflexible. Technically an X.25 interface was needed. In Graz, we had lots of troubles with our interface and were not able to connect to the CA most of the time. Still, if those technical problems would not have existed, there was the need to contact the CA for downloading the new certificates and revocation lists. This has to be replaced by an online directory service (e.g. X.500) to be of practical use.

5. Conclusions

Discussions during the last meeting of the projects participants showed, that the drawbacks are currently weighing more than the advantages: none of the participants is willing to use the system as is, even if he or she knows very well about the dangers of current email security. Nobody has spare time to invest in improving the useability. But still, Privacy Enhanced Mail will come, will have to be integrated into User Agents by the manufacturers and will have its place in daily life. Much discussion will follow about validity of electronic signatures in daily life, but for "normal" use PEM will be the standard for secure electronic mail.

6. Literature

[COSD6] Baltimore Technologies Ltd., *Cosine Sub-Project P8, Final Recommendations for Phase 2*, Version 1.2, Deliverable D6, May 1992.

[RFC1421] Linn, J., *Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures.* RFC 1421, DEC, February 1993.

[RFC1422] Kent, S., *Privacy Enhancement for Internet Electronic Mail: Part II: Certificate Base Key Management.* RFC 1422, BBN, February 1993.

[RFC1423] Balenson, D., *Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes and Identifiers.* RFC 1423, TIS, February 1993.

[RFC1424] Kaliski, B., *Privacy Enhancement for Internet Electronic Mail: Part IV: Notary, Co-Issuer, CRL-Storing and CRL-Retrieving Services.* RFC 1424, RSA-Laboratories, February 1993.

ELECTRONIC DATA INTERCHANGE (EDI) AND THE TRADE POINT CONCEPT

Dr.Péter Sugár
SZÁMALK SOFTEC Ltd.

Abstract:

The paper defines the term EDI and summarises the history of such systems. It overviews EDI standards and the typical architectural questions. Some points of consideration are discussed which should be taken special care of before any EDI implementation. Finally, the concept of UNCTAD's Trade Point is presented, which is built on multilateral EDI cooperations.

1. What is EDI?

EDI, Electronic Data Interchange, is a generic term used for the interchange of structured data between computer systems of cooperating partners. Historically, EDI has been associated with orders and invoices of business practice. However, as EDI applications were developed in newer and newer segments such as in administration, finance, health care and constructing sector, it has become clear that EDI can not be limited to certain kinds of applications. What is essential in EDI the exchange of such data, which are structured by strict rules to represent any kinds of documents used in either banking transactions or in CAD related cooperations.

Another important point that, unlike e-mail systems that are of inter-personal communications nature, EDI is based upon inter-program communications.

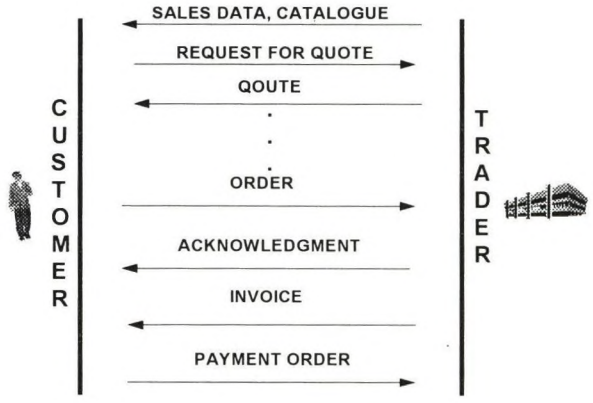


Figure 1

2. History of EDI systems

By the increase of number of cooperations in business or administration, both the number and the significance of the related documents grow.

In a typical business transaction such documents are exchanged between trading partners as sales data or catalogue, request for quote, quote, order, invoice, payment order (see Figure 1). It is not unusual that such documents as request for modified quotes, modified quotes or modified orders and invoices are also used, moreover, even several times in loops. Clearly, the traditional way of exchanging documents on paper is very slow, expensive and

it delays the flow of goods and money. It is especially true in the frequent case when both trading partners have business oriented application programs on their computers, respectively, to process documents, moreover, their computer systems could cooperate, since they are interconnected by some network.

Realising the bottlenecks of the traditional paper-based way of document exchange, such multinational companies developed the first EDI systems as the General Electric, or the Chrysler in the USA about 20 years ago. They developed company- wide document standards and computerised all the document preparation, interchanging, auditing, processing, and archiving stages. About the same time, banks also developed their first Electronic Fund Transfer systems for inter-banking transactions. The solutions above were the first forms of EDI.

Following the first experiences, among others such sectors as the automotive industry, insurance, banking started to use EDI in the USA.

Studies show that business administrational expenses are 10 percents of the total value of a product on average. By using EDI, that expenses are estimated to be reduced by 50 percents, i.e. 5 percents of the total value of a product can be saved on average. Since the average net profit of a trading company is on the range of 3-8 percents, by using EDI the net profits can roughly be doubled [1].

Governments realised the significance of EDI, too. The European Community launched its TEDIS (Trade Electronic Data Interchange) project to help in propagating EDI. The first phase of the project had a budget of 5.3 milliard ECU in 1988 and the second phase had 31.5 milliard ECU in 1991 [2]. In all countries PRO committees have been organised, e.g. AUSTRIAPRO, HUNPRO, FINNPRO for introducing EDI.

The Stanford Research Institute estimates 50 percents annual increase in the number of EDI systems in the USA, till the year 2000. Other studies predict 88 percents for that figure. The SITPRO expects 100 percents annual increase in the UK [1].

3. Standards

Standardisation launched even the first time. Sector standards, such as ODETTE for the automotive industry or TDCC for transporting sector, and national standards, e.g. ANSI X12, followed company standards soon.

Realising the significance of EDI, the United Nations Economic Commission for Europe (UN/ECE) undertook the task to develop a common multisector international EDI standard, the UN/EDIFACT (Electronic Data Interchange for Finance Administration Commerce and Transport). The two basic EDIFACT standards are the Application Level Syntax Rules (ISO 9735) and the Trade Data Element Dictionary or TDED (ISO 7372).

The ISO 9735 standard defines a syntax hierarchy of <interchange - functional group - message- data segment - single or composite data element - component data element - value> . An important property of the standard is that all the messages (UN Standard Message or UNSM), corresponding to documents, are compiled from the same TDED dictionaries of lower level elements in the hierarchy, ensuring the generality and the application sector-independence this way.

Assuming that EDI partners can communicate by some EDI network, Figure 2 shows the business example of Figure 1, by substituting each earlier document with the related EDIFACT standard message name.

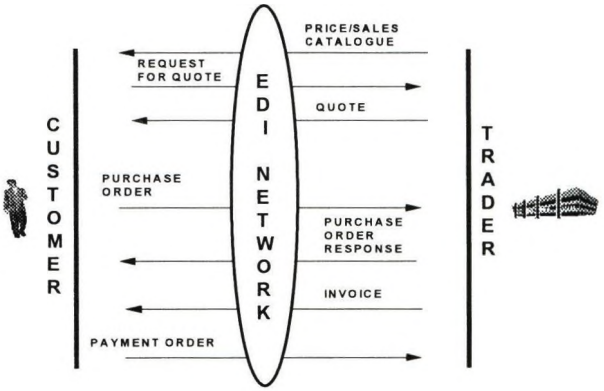


Figure 2

The use of X12 in the USA is quite general, while anywhere else EDIFACT is applied in more and more applications. EDIFACT is expected to become quite general all over the world, in a couple of years.

4. EDI networking environment

In a real system, application programs communicate with each other by some EDI subsystems (see Figure 3). Such application as for example an ordering system prepares in-house format document files and passes them to the EDI subsystem. The latter one converts them to standard EDI format messages, such as EDIFACT UNSMs, and transmits them to the partner EDI subsystem by using the services provided by some network, called Message Handling in Figure 3. The target EDI subsystem translates the standard EDI messages into in-house format documents of the recipient application. Note that the in-house formats of the cooperating systems are generally different, being characteristic to their own local systems. Besides format conversions, EDI subsystems are expected to provide many other functions as well, such as access control, reliable interchange of documents, logging, and audit trail [3].

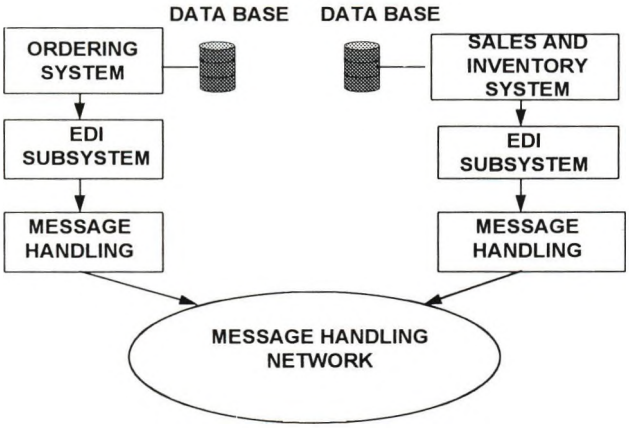


Figure 3

In the context of ISO OSI, EDI is within the Application layer 7 of the Reference Model. It uses typically the services of CCITT X.400 compatible message handling systems (MHS), since such systems can assure the privacy of the particular EDI systems and that the cooperation of EDI partners is independent of time. Unfortunately, the X.400 standard supports only inter-personal communications but not inter-programming ones as EDI. Therefore, a new standard has been developed, the CCITT X.435 or Pedi to

support EDI. However, X.435 compatible networks need a few years yet to become generally available.

In practice, for several years many networks have been providing some VANS, Value Added Network Service, functionally similar to X.435 in order to support EDI based message handling, such as EasyLink by AT&T and the Information Exchange Service of the IBM Information Network. Most EDI software packages support the access to many VANS and provide with other types of transmission means, too, such as OFTP (Odette File Transfer Protocol), asynchronous file transfer and even off-line transmission way in such media like floppy in order to support some form of communication in the absence of VANS or simply to reduce the expenses and charges of VANS.

5. Some remarks to EDI

The following remarks on my personal experiences are intended not to reduce the importance of EDI but to underline some points that are to be considered with special care when planning any EDI project.

As for the EDIFACT standard, the following points should be considered when implementing EDI.

1. EDIFACT messages are too general in order to cover all the possible needs for that particular kind of document. Therefore, they should be customised for each particular application. It means that their special subsets should be defined. That activity needs a good level of expertness.

2. Compatibility between EDIFACT systems is not so evident. Even if two different systems use the same EDIFACT message, there are two sources of incompatibility between them as follows:

   - if the systems use different customised versions of the same EDIFACT message, or

   - if they use different versions of the EDIFACT standard. Although the standard prescribes that any implementation should support all the earlier versions, apart from that declaration, it does not give any support for that. Moreover, newer versions not only add new dictionary element but omit many elements available in earlier versions, too. In such circumstances, the compatibility between different standard versions

depends only on the particular EDI software packages. My personal experience is that most of them fail to solve that problem.

3. EDIFACT does not specify a full protocol standard. It means that for example it depends on the particular EDI software, if the receiving party returns error data when it has failed to translate the message to its in-house format. The discrepancy on that function can be a source of incompatibility between different EDI packages again.

The following issues should be taken into account either.

- There is no general rule for legal aspects. It means that all the members of a particular user group should develop and sign common contracts stating that they accept electronic documents from each other.

- Some security issues, such as the problem of non-repudiation and identification or digital signature, are still to be solved generally.

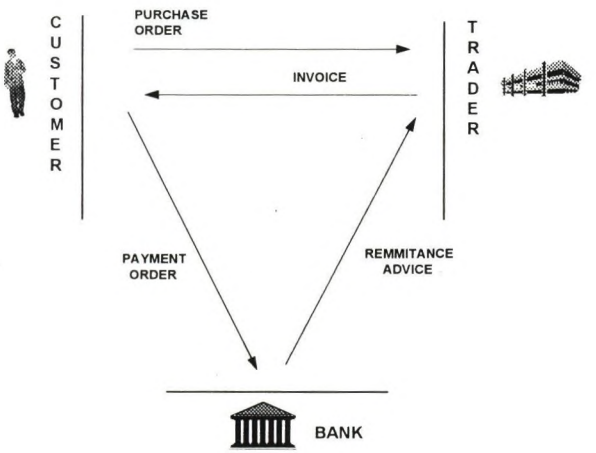


Figure 4

6. The Trade Point concept

Studying the business example in Figure 1, it can be seen that an intermediate bank is necessary for the action of sending the payment order document. Figure 4 shows the solution by standard EDIFACT message names. Studying the example further, it can be clear that for the related business transaction, not only the intermediate bank but such other contributors are also needed as freight forwarders, insurance companies and customs. The original bilateral business cooperation is the result of a multilateral one in reality (see Figure 5).

The United Nations Conference on Trade and Development, UNCTAD, introduced the concept of Trade Point, which is a trade facilitation centre where all participants are interconnected by EDI [4]. A Trade Points is aimed to support whole business transactions by EDI in a multilateral way, facilitating trade and reducing the time and cost of trade procedures.

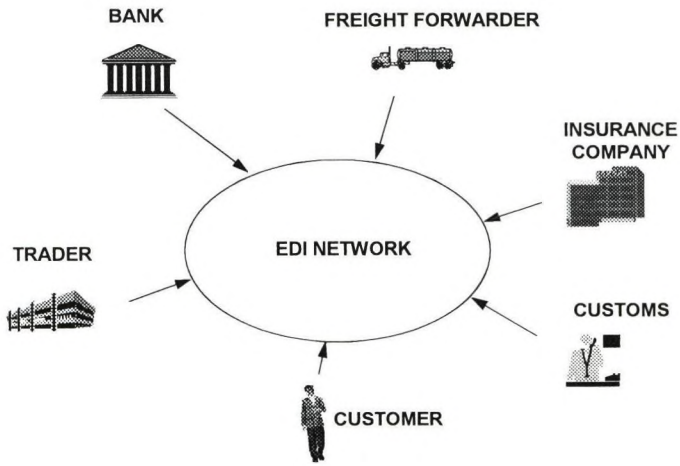


Figure 5

7. References

[1] The EDI Handbook - Trading in the 1990s (Blenheim Online, London)

[2] EDI-Perspektiven (Kommision der Europaischen Gemeinschaften, EGK Brussel, 1988)

[3] Sugár Péter: Az Elektronikus Adat Csere - EDI (NETWORKSHOP'93 Pécs, 1993.április)

[4] Trade Efficiency Initiative - The Trade Point Programme (Preliminary draft - UNCTAD, October 1992)

NETWORKS OF HUMANS AND INSTITUTIONS

Chair: G. Haring, B. Dömölki

COOPERATIVE RESEARCH IN INFORMATION TECHNOLOGY

G. Metakides

COMMISSION OF THE EUROPEAN COMMUNITIES

Since the emergence of digital computing in the late 1940s, the use of information technologies has been extending ever forther into economic and social life. For the first three decades this way largely a matter of individual computers with limited local networking, installed in companies and administrations to do specific tasks. They were small islands of information technology, difficult to use and expensive to run. In the last ten years,with the energence of the personal computer, digital communications networks, international standards, end open systems, all driven by the sometimes astonishing pace of technological advance, the islands have grown and are beginning to merge.

Information technologies now increasingly underpin all production and service industries, as well as the provision of societal services such as health, education, transport and entertainment. We are at the begining of the transition to a new **information infrastructure** of socicty and indusrtry.

This information infrastructure is set of services and technologies providing easy access to usable information to any citizen or enterprise, at any time, in any place. It brings together information processing, information storage and retrieval, information transmission and information content itself.

At the same time the information technology industries themselves find margins squeezed and profits falling even while the application of information technologies becomes ever more widespread. Boundaries are being eroded, between supplier and users, between the professional and the consumer market, and between the IT industries and other industrial sectors. A new "digital industry" is growing up. The return to a strong economy and fuller employment, not just in the information technology sector but in all industries, will be heavily influenced by the speed and succes with which the new information infrastructure can be put into place and the the structural adjustment of industry can be completed.

But behind the growth of information technologies, and of the information infrastructure of the future, lies a massive research and development effort. As technological development accelerates and competitive pressures increase, as the complexity and cost of R&d grow, enterprises and institutions need to look more widely to find the expertise and critical mass they need. The Community IT R&D programme ESPRIT has been a key part of this effort at the European level since its inception in the early 1980s.

The next major phase in the Community R&D effort, the Fourth Framework Programme, is currently at an advanced stage of planning. For the IT programme this planning is against the background of the major transformations in train in the role of IT in industry and society. To respond to these changes, the programme will need increasingly to be driven by user needs and market needs. One of the ways of ensuring that this happens is through the methods and approaches used in the support of R&D.

My presentation highlights two such innovative ideas for the implementation of R&D programmes, Networks of Excellence and Focused Clusters. We have been using Networks of Excellence in the IT programme for two years now. Focused Clusters, on the other hand , are a new idea which we a still in the process of refining.

NETWORK OF EXCELLENCE

Networks of Excellence were devised to offer the critical mass and catalytic effect of a Centre of Excellence but in a manner intimately linked to local industry and spread over the entire Eeuropean Community. They achieve this by bringing together expertise, interdisciplinary skills and resources from a wide range of research groups covering all aspects of a given research area. Industrial enterprises participating in a network of excellence gain access to a wide pool of talent and knowledge, putting them in contact at an early stage with scientific breakthroughs and enabling them to seize market opportunities.

A Network of Excellence comprises a group of academic and industrial research teams in a paricular area of RTD. The teams share long-term technological goals, and coordinate their policies for research, training, and information dissemination in order to reach these goals. Each team, working in its home institution, forms a node of the network to which it belongs. The nodes share a common infrastructure, including electronic mail links and databases. Together the teams of a network posses a critical mass of top-flight experts, and interdisciplinary skills in all technology areas pertaining to their reserch goals. The nodes thus collectively attain an innovation potential and leverage far than when considered in isolation.

A network brings the benefits of a Centre of Excellence to all the regions in which its nodes are located. Access to one node gives access to the expertise and skills of the whole network. Technology transfer to local industry is enhanced, a benefit of particular importance in peripheral regions. In addition, reserchers do not need to move away from their home regions to participate in state-of-the-art research. This helps remove one of the causes of a brain drain. While a small institution in a more outlying area has little scope for building up a Centre of Excellence, it can still have a viable node in a Network of Excellence.

By their very nature, Networks of Excellence will tend to improve industrial competitiveness by accelerating the exploitation of research results, bringing down any artificial barriers between industry and academia, and coordinating the research effort.

The collective srength of a network makes it a pole of attraction for young researchers who may be able to spend part of their time in different nodes of a network which collectively provide the interdisciplinary skills needed. The majority of researchers trained this way, through researchers itself, will eventually find their future in industry, supplying the skills industry really needs.

Turning to management structure, each network has its own internal structure, most suitable to that network's goals. This structure is open and accomodates activities such as research coordination, technology transfer, international cooperation, training cooperation, training and others. These activities are usually coordinated and supervised by a network executive board, composed from representatives of industrial and academic nodes. In addition, the consideration of the industrial viewpoint and needs may be facilitated through the formation of an Industrial Working Group. The intimate coupling of industrial needs to the broad range of expertise and resources available in a network should accelerate the transition from the research lab to the market.

Currently nine Networks of Excellence are in operation, with four more in the pipeline. Three networks were set up in 1991, in the areas of speech and natural language (ELSNET), computational logic (COMPULOG-NET), and ditributed network architectures (CABERNET).

The succes of the these three led to the estabilishment in 1992 of a further six networks. These new networks cover multimedia and database systems (IDOMENEUS), organic materials for electronics (NEOME), multifunctional microsystems (NEXUS), high-temperature electronics (HITEN), machine learning (ML), and meoscopic systems (PHANTOMS).

Four new networks are due to be launched soon. They are HPCNET in high performance computing, ICIM covering computer integrated manufacturing, NEURONET in neural networks, and CVNET in computer vision.

Well over 400 nodes have been estabilished within the nine existing networks. The actual configuration of a network, and the number of nodes, can change quite often as new nodes are brought in. For example HITEN, which started off with 19 nodes, has grown to around 150 nodes of associate partners. The number, distribution and nature of the nodes of each network vary depending on the technology area concerned.

Networks of Excellence initiate a wide range of activies. **Defining a common strategy** to achieve the network`s technological goals, by identifying the technologies needed to achieve them, is a condition for the existence of a network as a single entity. Integrating industry`s views and needs into this dynamic process is of paramount importance. For example, the Industrial Working Group of NEXUS recently produced a Strategy Paper, reflecting the common position of most major European companies engaged in microsystem technology R&D, and demonstrating how industrial needs can be embraced in leading-edge R&D.

Coordination of research, in interdisciplinary areas in particular, is another preoccupation of networks. For example, ELSNET was instrumental in bringing together the speech and natural language research communities, exploiting the multilingual constitution of Europe.

The **technology watch** function is related to the above. The network can maintain an inventory of research in relevant areas, analyse the emerging or available technologies, and recommed action ranging from large cooperative project down to individual doctoral thesis. NEXUS went through a series of contacts with American and Japanese officials and is currently completing such a Status Report on Microsystems Technology in North America and the Far East.

Infrastructure development is a primary concern of new networks. CABERNET has already installed a data communications network and is coordinating the implementation of a common solution in all nine networks.

Training and education activites fall in the networks' primary objectives. For instance, NEXUS makes an inventory of the European curriculum in Microsystems Technology, while many of the networks submit joint proposals to the Human Capital and Mobility Programme of the European

Community. The principle that acess to single node gives acess to the resources of a network as a whole enhances temporary mobility of researchers who wish to work closely on an individual project, while at the same time making permanent migration unnecessary.

The **dissemination of research results and information** is another important activity. The networks publish newsletters, participate in international technology fairs and organise workshops. CABERNET, in cooperation with IEEE, is organising the first European conference on Dependable Computing(EDCC-1 in October 1994).

Networks of Excellence offer considerable scope for **international cooperation.** Existing Networks have extended their contacts to nodes in countries of Central and Eastern Europe. The benefits gained by nodes in the peripheral regions of the European Community are equally realised by third countries. These include technology transfer, industrial cooperation, access to state-of-the-art research, exchange of researchers, and avoidance of a "brain drain".
A number of assessment studies on potential cooperation with various countries have already been undertaken. Several cooperative activities with the US are coordinated by networks IDOMENEUS, NEXUS and COMPULOG-NET, while NEXUS has a task force working on linking central and eastern European laboratories specialised in microsystems to the network.

Networks of Excellence can provide mechanisms for the implementation of Article 130g of the Treaty on European Union, which empowers the Commision to promote cooperation with third countries and international organisations. Each network is currently reviewing its involvement in international relations, with a wiev to developing a framework for appropriate third-country involvement.

As regards funding, each network commonly gets between 500,000 and 1 million ECUs of Community backing. The funding is intended for welding the individual nodes into an entity with an idenity of its own. It helps provide the glue that joins the nodes. The networks may then seek funding for research, development or training activities elsewhere in the public or private sector. In this sense, Community funding is seed money, a leverage when getting the network started.

Networks of Excellence represent a new concept: they maintain a dynamic R&D strategy, act as clearing houses for research results, promote mobility of researchers, desing curricula and interdisciplinary course material and also promote personnel exchanges between industrial and academic nodes ensuring continued training and technology transfer through people.

But to achieve the full potential Networks of Excellence have,certain conditions must be satisfied:

- The research community must continue to demonstrate its willingness to coordinate research and training activities in a long term perspective of meaningful social and economic impact.

- A high performance telecommunications infrastructure to allow the networks to behave as single entities is essential. Substantial progress has been made in implementing data communication networks, but a lot still remains to be done towards advanced high performance networks.

- The ability to innovate must go hand-in-hand with creating the appropriate conditions that will allow converting such innovation to wealth. Significant progress has been alerdy achieved in this respect, and we must continue fostering links between industrial, academic and venture capital at the local level.

The fulfilment of these conditions will allow Networks of Excellence to present a real opportunity to innovation and excellence for European R&D.

FOCUSED CLUSTERS

The idea of Focused Clusters is very new. It is concept that we envisage implementing in the next phase of Community R&D, the Fourth Framework Programme, which we expect to start in 1994. This means of course that our ideas are more in outline than for Networks of Excellence, and that we are still in the process of refining the concept.

Our starting point is the observation that the funds available for Community-supported R&D are limited, and that we need to ensure that they are used to maximum effect. To avoid spreading resources too thinly, effort must be focused and concentrated where it is most needed. At the same time it is of prime importance to ensure the flexibility and responsiveness needed to react rapidly and effectively to changing needs. It is direct response to these challenges that we have devised the idea of Focused Clusters.

A Focused Cluster is a group of projects with a clear and well-defined goal, bringing together a number of disciplines and technology areas, and involving a wide range of organisations. The purpose of establishing a Focused Cluster is to ensure that R&D concentrates on real needs. All the activities within a cluster should contribute in a well understood way to the achievement of the goal of the cluster. This means that the goal itself must be well defined in the first place. By ensuring both the objective itself and that the relationship of activites to the objective are clear, the possibility is created for effective monitoring of the progress and sucess of work within the cluster.

A Focused Cluster may embrace many kinds of activities apart from collaborative research projects, among them networks of excellence, supplier/user collaborations, working groups, conferences and workshops. Training, dissemination, technology transfer will have an important role. Coordination with national initiatives and with EUREKA will be actively promoted, as will collaboration with third countries. Each cluster will have a coordinating panel drawn from industry and users, which advises on overall strategy and helps ensure the continuing focus of the cluster.

By its nature a Focused Cluster is a relatively long term operation. But the rapid pace of technological change means that it is not always possible to foresee all specific R&D needs four or five years ahead. Flexibility in the funding arrangements of a cluster, and in the timing of project and other activities, ensures the necessary responsiveness to change.

As the work of the v\cluster proceeds, participants, industry, goverments and the Community have the opportunity to refine or redefine options in response to changing needs or changing understanding of needs. Induvidual activities may have a life span shorter than the duration on the whole cluster. An activity may reach completion and pass projects may take over work from precompetitive R&D projects to convert results into products. This dynamic process of determining specific activites ensures that the sharp focus is maintained over time, and aviods wasted R&D effort.

I have been stressing the newness of the idea of Focused Clusters. But it is of course based upon the experience that has been gained in the IT programme. In particular the Open Microprocessor Systems Initative (OMI), wich has been in existense for two years now, already presents a number of the characteristics of a Focused Cluster. We anticipate that in the Fourth Framework Programme, from 1994 to 1998, there will be some three adittional clusters in addition to OMI.

CONCLUSION

In summary, Networks of Excellence and Focused Clusters are two pillars of the Community IT R&D programme for 1990s. Each approach is designed to adress a particular set of needs. What hey have in common is the objective not just of promoting reserach collaborations of the highest quality, bit also of ensuring that the maximum benefit is derived from the R&D by through training, technology transfer, and the effective dissemination of scientific results. They aim to help the IT programme act as a catalyst to bring industry and universites together, to catalyse collaboration between industrial enterprises and to built an European reserach community in information technologies.

NETWORK MANAGEMENT

THE CRITICAL SUCCESS FACTOR FOR RELIABLE NEW FORMS OF COOPERATION

K. Bauknecht, B. Studer
Institut für Informatik der Universität Zürich

Abstract

Most future activities will be based on an appropriate and reliable communication infrastructure. Networks form the backbone for effective and efficient information exchange in various areas. To do this well, several key requirements have to be fullfilled. The highest priority should be given to the realisation of an effective network management strategy. This paper elaborates on necessary frameworks and discusses the required features for effective network management. Experiences gained during the planning and implementation of various networks are compiled to form an action plan. The action plan serves as a guideline for the different steps required in designing and implementing networks.

1. Introduction

Many organizations are dependent on a modern information infrastructure in their efforts to improve business results. The traditional goal of an infrastructure is to enable more effective use of information while insulating people from underlying complexities. This goal is important because the effective use of information offers enhanced efficiency, informed decision making, and improved business results. However, the complexity of the modern infrastructure, and the changes affecting it, produce

significant management challenges [1].

The typical information infrastructure of the 1990s is composed of networks of computer systems, peripheral devices, and often multi-layered network components (e. g. routers, gateways). This modern infrastructure is directly involved in delivering business results. In addition to serving in the traditional support role, this kind of infrastructure has become the environment in which many companies execute their mission-critical processes [2].

A driving force in the information infrastructure has been the trend to replace a few, large, proprietary, centralized mainframes with many small, open, geographically dispersed, client-server systems. This technology trend has created many new types of network components, and has caused an explosion in the number of components to be managed. Open architectures and standards for interoperability provide the flexibility to implement needed solutions without being dependent on a single vendor. Unfortunately, interoperability doesn't automatically enhance mangeability. In fact, the trend toward open systems has complicated the management problem by diminishing the scope and effectiveness of proprietary, centralized management systems.

Network management is the process of controlling and planning complex communication networks so as to maximize its efficiency, reliability and productivity [3].

2. Requirements for Network Management

In today's enterprise environment, the communications network to be managed is typically a combination of many inter- and intra-facility networks. This combination may serve part of an enterprise, an entire enterprise, or multiple enterprises. Thus, a network is a complex entity, which encompasses a wide mix of communication resources and services. The general capabilities required for managing enterprise networks can be summarized as follows:

- The ability to manage all the subnetworks in the network, regardless of the protocol suite used.
- The ability to manage a combination of inter-facility (telecommunications) and intra-facility (local) networks.

- The ability to manage a wide range of network resources, from low-level devices (e. g. repeaters, modems) to intermediate systems (e. g. bridges, routers) to end systems (e. g. systems with full protocol stacks).
- The ability to provide a set of basic management functions.

In the literature there is a general agreement on how to classify the subject of network management, namely in six activity areas with the following functions:

- *Configuration management* for providing data for all other activity areas
- *Fault management* for supporting operational decisions
- *Performance management* for supporting tactical decisions
- *Security management* for ensuring low risks of operating the network and its network management systems
- *Accounting management* for supporting costing and charging
- *Network planning* for supporting tactical and strategic decisions

In [4] a more detailed list of network management requirements is presented. Network management should offer the following features to users:

- ensuring end-user service level
- the capability to correct, bypass, or circumvent failed elements
- the capability to operate despite element's failures
- monitoring possibilities
- real-time performance analysis
- statistics and historical data availabilit
- a comfortable user interface
- conformance to OSI standards
- improved security
- more accuracy of accounting data
- a network management database

These requirements describe the technical capabilites needed for managing communications resources. However, a purely technical solution is insufficient in the enterprise environment. Strategic and organizational aspects also have to be taken into

consideration for good network management solutions [5] [6]. It is from the corporate perspective that we must develop the requirements for effective network management. Fig. 1 expresses this fact by presenting the essential guidelines for an integral network management, namely:

- the information systems strategy is derived from the corporate strategy and depends on the long-term goals of the corporation
- organizational guidelines depend on the corporate structure and the business processes
- technical guidelines which depend on available technology.

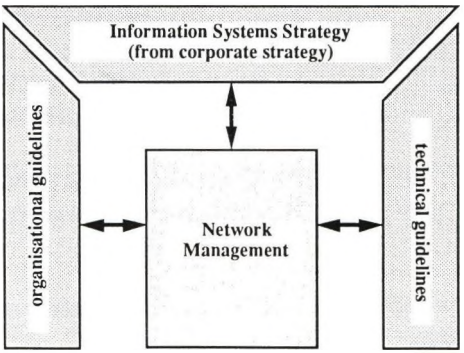


Fig. 1: Guidelines for integral network management

3. Critical Success Factors

Critical success factors are those few key areas of activity in which favorable results are absolutely necessary for an organization to reach its goal [7]. The goal for managing networks is to maintain the customer's service level and thus to ensure that the communication network is operating effectively and efficiently at all times, in order not to cause any problems in the short-, middle-, and long-range operation of the lar-

ger organization. This goal is supported by operational, tactical, and strategic decisions, and plans.

To achieve an effective and efficient network management, special attention should be given to the following critical success factors:

- Methodology
- Frameworks
- Human resources

The *methodology* is a systematic approach for using the communications infrastructure to support the corporate strategy. The information systems strategy which is derived from the corporate strategy, is an important factor for the telematic strategy. We describe in chapter 5, a methodology for developing a reasonable communication infrastructure.

To realize good network management, it is necessary not only to develop a top-down concept which is often theoretical and difficult to implement, it is also necessary to consider a bottom-up approach which starts from existing network management *frameworks*. A short description of the most important network management frameworks is presented in chapter 4.

Behind every activity, there is the human who actually accomplishes and executes the tasks. Network management demands extensive knowledge and experience thus making qualified personnel difficult to find today. For this reason expert systems are discussed and evaluated in terms of applicability as support tools for any of the personnel's responsibilities.

Other authors are giving a more technical-oriented rating of the critical success factors. Terplan [4] for instance mentions as critical success factors for network management:

- *Processes and procedures:* Sequences of application steps including guidelines for how to use tools necessary to execute network management functions.
- *Instruments:* Hardware and software, or both, for collecting, compressing, data-

archiving information, and predicting future performance of network components.

- *Human resources:* Individuals involved in supporting network management functions.

Based on our experiences, one of the most important critical success factor is how to embed the network and the management thereof into the enterprise architecture to fulfill the corporation´s requirements.

4. Network Management Frameworks

In the last few years, various organizations have developed network management frameworks. Choosing the right framework is not easy, because there is no single solution adequate for all requirements. OSI management, the Internet SNMP, the Open Software Foundation's Distributed Management Environment, and the Network Management Forum´s OMNIPoint are all appropriate solutions in some circumstances. In this chapter, we desribe briefly the above mentioned frameworks and their potential for managing corporate networks.

4.1 OSI-Management Framework

The OSI model provides a framework for defining data communication standards and the physical and electrical interface characteristics of network equipment and services [8]. The network management model consists of a manager and agent that communicate using the object-oriented Common Management Information Protocol (CMIP) (Fig. 2).

The organizational model describes ways in which OSI management administration can be distributed across various management domains as well as across management systems within a specific domain. The information model provides guidelines for defining managed objects and their respective interrelationships, classes, attributes, actions and names. The functional model describes the five areas: configuration management, performance management, fault management, security management and accounting management. The adoption of these models makes robust management

possible [9] through the sharing of network management information between management systems. The OSI management framework consisting of several models allows users to specify which system acts as manager and which plays the role of an agent.
The OSI management standardization process is not finished yet. Therefore only a few implementations of the core concepts are available. But OSI management has a rich functionality, thus it is suitable for managing complex corporate networks in a middle-range term.

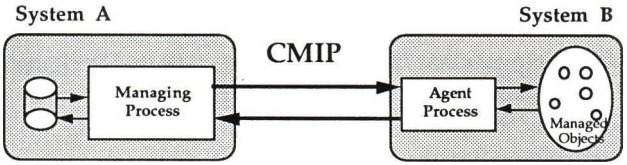


Fig. 2: OSI model with manager and agent

4.2 Internet-Management Framework

The network management protocol in the TCP/IP suite is called Simple Network Management Protocol (SNMP) and is based on a manager/agent relationship. SNMP was introduced as the Internet-standard network management framework in early 1988, when it was created to solve the pressing network management needs of the rapidly growing Internet. Since then, SNMP has enjoyed wide commercial success and provided stable and effective network management of the Internet. SNMP has been successful for many reasons. The most recognized and important of these reasons is SNMP's simplicity. The simplicity inherent in SNMP lowers the cost of entry into SNMP network management which allows SNMP to be ubiquitously implemented on a wide variety of platforms. An enhanced version SNMPv2 was published in the summer of 1993.
SNMP operates on three basic concepts: manager, agent, and the management information base (MIB). An agent is a software program housed within a managed network device (such as a host, gateway, or teminal server). An agent stores management data

and responds to the manager's requests for this data. A manager is a software program housed within a network management station. The manager has the ability to query agents using various SNMP commands. The management information base is a virtual data base of managed objects, accessible to an agent and manipulated via SNMP to achieve network management.
SNMP concepts are pragmatic and many implementations are available. For this reasons SNMP is suitable for managing many networks currently.

4.3 OSF Distributed Management Environment

The Open Software Foundation (OSF) has defined with its Distributed Management Environment (DME), a powerful toolbox for distributed network and system management. It is comprised of generic management applications, administrative services for the objects, support for the CMIP and SNMP protocols and application programming interfaces. It is generally assumed that the environment OSF DME will become an industry standard [10]. The first versions are expected to be released at the end of 1993. Fig. 3 shows the DME framework.

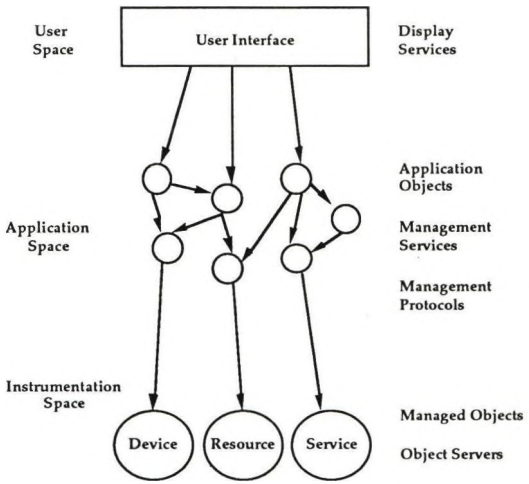


Fig. 3: OSF DME framework

The DME framework will provide four major services:

- graphical user interface, to built management solutions into consistent models
- object services, to divide the applications into sets of independent, distributed objects, which cooperate with each other
- instrumentation access - APIs to access management protocols like SNMP and CMIP
- event management services, to deal with management events and notifications in a secure, distributed fashion.

DME is not available today, but it will be suitable for managing networks in Unix environments.

4.4 OMNIPoint Framework

The Network Management Forum is an international consortium of 100 major computer vendors and service providers that are working to accelerate the availability of standards and technology for managing complex global networks. The main result of the Forum's efforts to date is a series of Open Management Interoperability Points, or OMNIPoints. Each OMNIPoint is a stable set of implementation specifications including a selection of formal standards and industry agreements that satisfy the full range of requirements for managing today's most complex networked information systems [11]. Fig. 4 shows the OMNIPoint framework.

Due to the fact that the focus of OMNIPoint is the enterprise-wide management of networked information systems (in order to deliver cost-effective services to end-users), its main emphasis is on achieving integration of management information through systems interoperability. However, OMNIPoint also starts to address the integration of management applications by specifying APIs which should be implemented within management systems. This allows the concept of open management platforms to be realised.

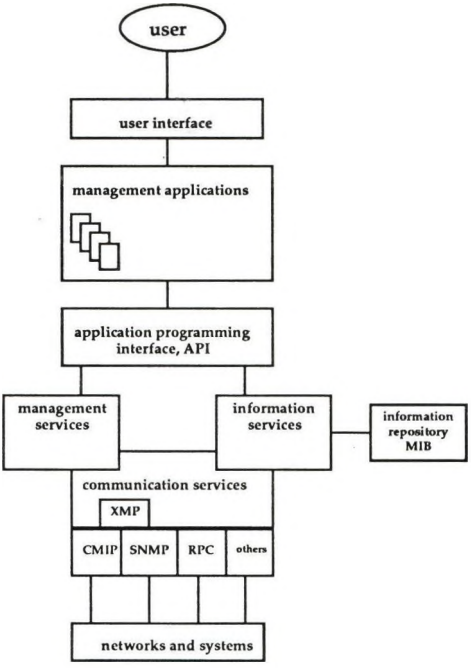


Fig. 4: OMNIPoint framework

5. Action Plan and Guidelines

As already mentioned in chapter 3, one of the most important critical success factors is a methodology for a systematic approach to building a communications infrastructure which supports the corporate strategy and is based on network management frameworks. Such a communications infrastructure is a key factor for new forms of cooperation (e. g. group communications, videoconferencing, mobile communications, multimedia communications) in the corporation.

In our proposed methodology, we are presenting a combined procedure which is vi-

sualized in Fig. 5: On one side, the methodology begins with a top-down approach starting with the corporate strategy and identity. On the other side, the methodology is based on frameworks and standards. We call that the bottom-up approach.

The top-down approach has the following steps in which answers for the following questions should be given:

1. Corporate strategy: What is the future development of the corporation? Are we moving to a networked firm (e. g. decentralization)? What is our IT-strategy (e.g. electronic data interchange, just-in-time concepts)? What role does the communication infrastructure play?
2. Corporate identity: What is the communication culture? Who needs to communicate with each other?
3. What are the communications requirements today and tomorrow?
4. What does the relations network (between entities) look like?

The bottom-up approach has the following steps:

1. What kind of networks do we use? Which frameworks do we want to use?
2. Which sort of standards do we prefer (e. g. de-facto and/or international standards)?
3. What does our communications architecture look like?

After answering the above questions, you can define your telematics strategy which you can group in these categories:

1. Subscribers: e.g. numbers, profiles, support,
2. Services: e. g. applications, security, resources,
3. Technology: e. g. systems, topology, protocols, equipment,
4. Environment: e. g. buildings, distances, products, costs
5. Communications and cable strategy: e. g. kind of cables, mobile transmission

Then you should be able to plan your logical and physical corporate network. The last step consists of realizing the network and managing necessary modifications.

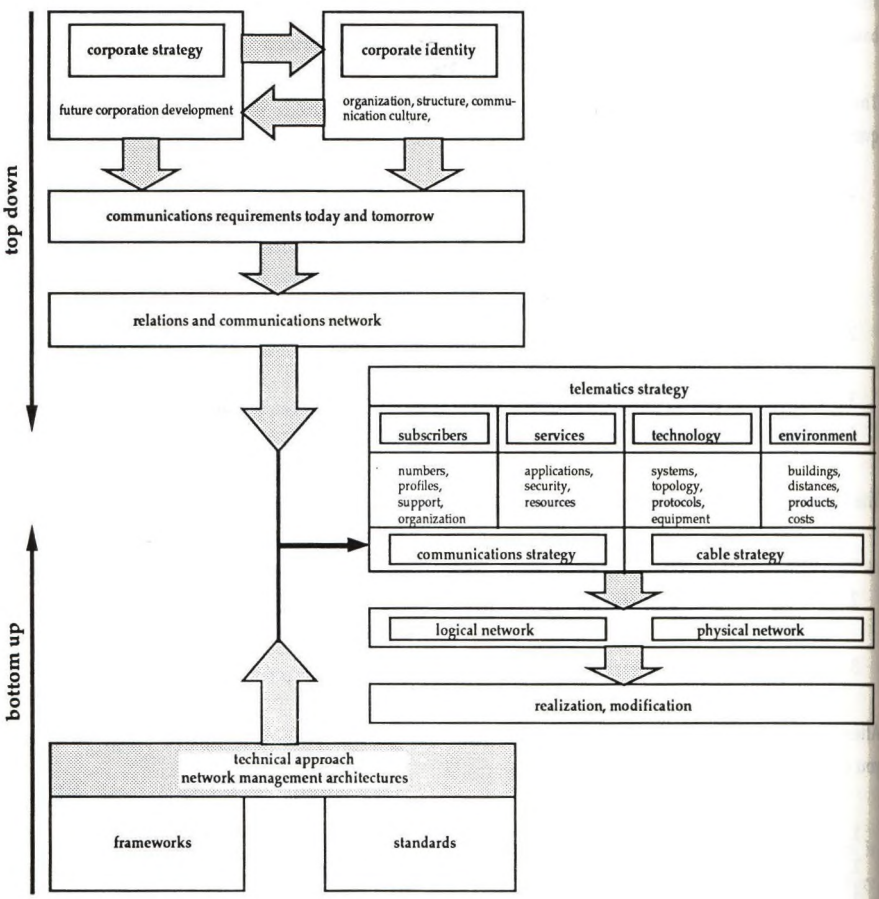


Fig. 5: Methodology for building an enterprise-wide communications infrastructure

6. Conclusions

Just as railroads and highways provided the infrastructure to support the Industrial Age, networks provide the obvious infrastructure for this emerging Information Age. The long-term success of an organization depends upon the proper planning and implementation of a comprehensive communication network and the effective management thereof. The strategic direction and position of an organization defines, in many cases, the network management architecture. An open organization-wide communications system is being given to an important factor in the success of any organization, but without careful attention to network management, sub-optimal utilisation is likely to occur. In suggesting that network management is a critical success factor for reliable new forms of cooperation (e. g. group communications, videoconferencing, mobile and mulitmedia communications) we are proposing that without the meta-level of information regarding on networks we cannot maximize the effectiveness of the communication infrastructure.

Acknowledgements

We would like to thank Thomas Abdallah and Andrew Hutchison for reading and correcting the manuscript.

Abreviations

API	Application Programming Interface
CMIP	Common Management Information Protocol
DCE	Distributed Computing Environment
DME	Distributed Management Environment
IP	Internet Protocol
ISO	International Organization for Standardization
MIB	Management Information Base
OSF	Open Software Foundation
OSI	Open Systems Interconnection
RPC	Remote Procedure Call
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TMN	Telecommunications Management Network
XMP	X/Open Management Protocol

References

[1] Gilbert, W. E., The five Challenges of Managing Global Networks, IEEE Communications Magazine, October 1992.

[2] Scott Morton, M. S., The corporation of the 1990s, Oxford University Press, New York, 1991.

[3] Leinwand, A., Fang, K., Network Management - A Practical Perspective, Addison-Wesley, Reading, Massachusetts, 1993.

[4] Terplan, K., Communication Networks Management, 2nd ed., Prentice-Hall International, London, 1992.

[5] Studer, B., Integrales Netzwerkmanagement, telekom praxis der Deutschen Bundespost Telecom, 9/92.

[6] Ball, L. L., Cost-efficient Network Management, McGraw-Hill, New York, 1992.

[7] Rockart, J. F., The Changing Role of the Information Systems Executive: A Critical Success Factors Perspective, Sloan Management Review, 1982.

[8] Recommendation X.700, OSI Management Framework, CCITT Geneva, 1990.

[9] Yemini, Y., The OSI Network Management Model, IEEE Communications Magazine, May 1993.

[10] Stucki, H. R., Telecommunications Management Architecture as a Strategic Position of Success, Bulletin Technique PTT 6/1993, Swiss PTT, Berne, 1993.

[11] Murril,B., OMNIPoint: An Implementing Guide to Integrated Networked Information Systems Management, Proceedings of the International Symposium on the Integrated Network Management III, North-Holland, Amsterdam, April 1993.

Navigation and Activity Networks

Karl Kitzmüller
Gerhard Chroust

Systemtechnik und Automation
Kepler Universität Linz
Altenbergerstr. 69
A-4040 Linz
Austria

Abstract:

A process model acts as a template for individual development processes. A major problem in following a process model is to decide in each individual project (which can be considered as an instance of a process model) in what specific sequence the individual activities should be performed. Computer support is necessary to help the user in following the model, in applying tools and administering deliverables. This yields a so called Software Engineering Environment. Considering the current trends in system architecture it becomes more and more important to distribute the functionality of such Software Engineering Environments in a network. This paper shows the network aspects of process models and their additional components e.g. resources, tools, users and help information. These concept are related to the activity network of Softlab's MAESTROII and IBM's ADPS.

1.0 Computer Assisted Process Models

Today's software development is characterised, amongst other things, by the need to enhance quality and productivity and the aspiration to provide a total system solution. A major step to improve quality and productivity are Software Engineering Environments (SEE) [2] which provide a Process Model [9], a standardised tool interface and a repository, all under the common shell of a process interpreter shown in Fig. 1.

In order to gain a general and holistic view, all system interdependencies must be maintained and made explicit.
The main functions of a SEE are:

- Guiding and supporting the user with respect to the process model
- associating and accessing the attached tools
- storing all intermediate and final deliverables, and applying the necessary version and configuration management.

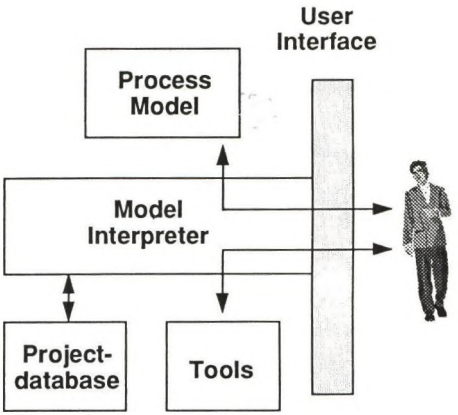


Fig. 1. Process Model and Model Interpreter

2.0 Activity Networks

Of special interest are obviously those parts of the process model which define the strategy and tactics of the development process: the activities, their sequencialisation constraints and the means to navigate through them.

In the literature (cf. [4]) many different ways to represent the navigational part of the process model have been used. They all have the following objectives in common:

- to state which activities may/should come next when work on one activity ends (not necessarily finishing the activity).
- handling regression, i.e. the situation when due to some circumstances (error, changed requirement, infeasible implementation choices) previous activities have to be taken up again in order to change some previous decisions.

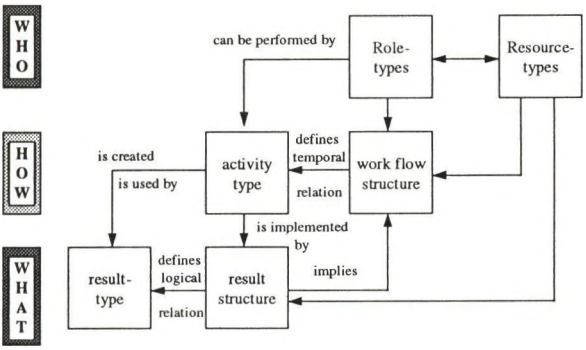


Fig. 2. Cascade Model of Software Development

2.1 Activity Networks: types and instances

An established process model is a template for future projects. Such a process model contains only descriptions of activity, role and deliverable types, not individual instances. Certain properties of the desired process are defined in the model, other individual properties not and they will vary from project to project. A typical situation is the inability of the model to describe how many instances of a type (activity, deliverable) will be created in a specific process (Fig. 3).

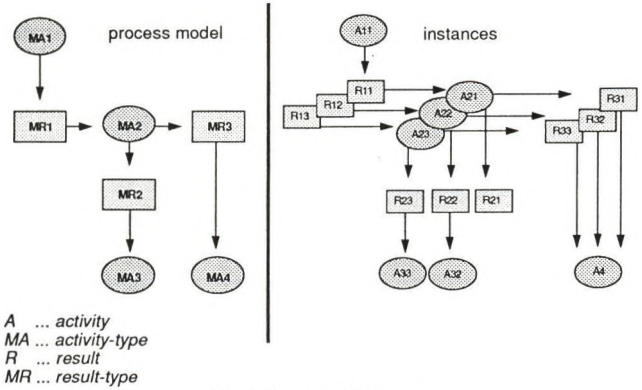


Fig. 3. Types and instances

2.2 Representation of Activity Networks

We introduce different representations of activity networks used by two common SEEs, IBM ADPS(Application Development Project Support) and Softlabs MAESTRO*II*.

2.2.1 Result correlated Activity Network (ADPS)

The representation chosen by ADPS [2] can be called a result-correlated activity network [4], e.g. Fig. 4. Here no stringent association between individual activities exists. The individual activity classes are described with their inputs and outputs. The sequencing between activities is not fixed, it is only assumed that equally named result classes correspond to one another. A tacit assumption is that inputs are finished before an activity starts using them.

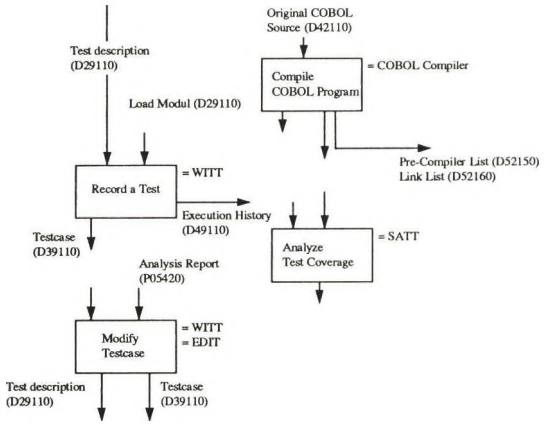


Fig. 4. Result correlated activity network

2.2.2 Project Process network (MAESTRO*II*)

MAESTRO*II* [12] on the contrary provides a relationship between an activity hierarchy and a deliverable´s hierarchy (Fig. 5). The sequencing of activities (tasks) is explicit defined in the task model via a relationship called ´predecessor´ and its inverse ´successor´.

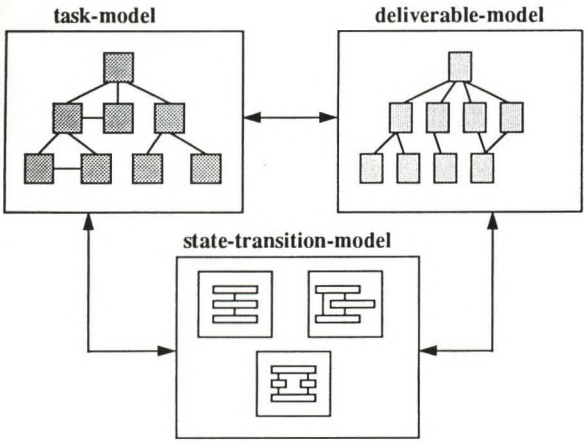


Fig. 5. MAESTRO*II*s Process Model representation

- **Task model**: describes the tasks of a project, their hierarchical structure and the logical connections existing between them. It consists of task classes and the standard relations between them.
- **Deliverable model**: describes the deliverables of a project, their hierarchical structure and the logical connections existing between them. It consists of deliverable classes and standard and freely definable relations and attributes.
- **FSM model (State Automaton model)**: standardizes sequences of operations for tasks or deliverables in MAESTRO*II* by means of state automata. State automata consist of states, state transitions and state transition functions (A MAESTRO*II* procedure that is assigned to a state transition in MAESTRO*II* and executed together with the state transition).
- **Intermodel Connection**: the functionality which connects the individual models (described above) to one another. Example for the connection between task model and the deliverable model are: ´task produces deliverable´ or ´task requires deliverable´.

2.2.3 Advantages and Disadvantages

- ADPS has difficulties when tightening the control of the flow, e.g. with respect to the ETVX paradigm [15]
- MAESTRO*II* has difficulties with very long leash control where very little control of the sequence is done.

2.3 Additional Support

The availability of computer support allows some additional productivity aids to be provided to the user. By providing online help texts, information about standards, and standardized skeletons for the deliverables to be created, a more uniform and professional application results. Further support should be available for:

- tools and their integration in the activity network
- functionality for project management
- functionality for configuration management
- support of quality assurance mechanism

3.0 Navigation

The prime reason for a process model is the definition of how the development process should proceed. This means that the Process Interpreter should give help to the user in finding the 'next' activity. The choice of a strategy (we call it Navigational Flexibility) depends on a large number of factors like criticality of the project, experience of the development team, company culture, customer requirements, development strategy (see below), etc. We distinguish

long leash

- **passive**: The interpreter presents all activities ready for execution to the user, the choice is done by the user.
- **suggestive:** All ready activities are shown, but the interpreter suggests one or more for immediate action.

short leash

- **imperative:** The system offers just one activity to be done next to the user.
- **automatic**: This is only meaningful for activities not involving human intervention (e.g. compilation). In this case the system can automatically trigger the activity.

In praxis several ways to express and support navigation have been used (To do List, ..).

3.1 Multiple execution of activity types

[4] observes that an activity class may be 'visited' more than once for various reasons.

If we consider an activity type as an identifier of its instances, we can speak of the execution of this activity type as soon as one of its instances is executed. There are many reasons why not all instances of an activity type can be executed together in sequence.

Interruption of an activity: A trivial way of interrupting is spontaneous (i.e. coffee break) or forced (by the project manager in order to continue with another activity).
Multiplication of deliverables of a deliverable type: One deliverable type can have several instances, which are generated at different times [5].
Refinement: Many times information are first defined in a coarse way and are further detailed later on. Terms like ´preliminary design' and ´detailed design´ [18], high level design and low level design, are typical.
Iterative Software development: Today it's well known that the´waterfall model´ is only an idealised form of the real development process [3]. Many authors [1] [19] pointed out, that the final software product can only be created by several iterations of the necessary activities.
Sub model: It is necessary that in different places of the software development process the same subprocess has to be executed with slightly modified deliverables. This is performed with an activity type that has different instances which are expanded in a subnet of activities on different places in the process model.
Work ahead: For practical reasons it is sometimes useful to begin with a successor activity without having fulfilled all preconditions. We are working ahead. Later on we have to ensure that all preconditions are fulfilled.
Change of requirements: There are many reasons for the change of requirements during a project [7] [14], which result in a change of the product. I.e. a rework of already existing deliverables is necessary which means a repetition of already done activities.
Errors: Errors which occur during the execution of an activity, have to be corrected by repeating the corresponding activities.

3.2 Navigation levels

Similar to the levels Information Model, State Model, Process Model and Boundary Statement/Requirements Definition introduced by [16] we have to distinguish between the following three architecture levels:

- **Navigation in the object and the object class network (operational):** This level describes the operational layer of the navigation. Typical examples are the different entry points to the project, supported via history lists, marked positions and logical mapped names.
- **Navigation through the systolic connection network architecture (tactical):** In most cases this navigation level is used for the automation of activities. Example: Changing a state of a deliverable or a task results in activating other state transitions. This behaviour could be compared with a chain reaction.
- **Navigation on process interrelationship level (strategic)**: Describes the strategy of the project process, by defining how the different sub processes (Project Management, Quality Assurance, Development Department, ...) are working together (refer to 5.3).

3.3 Knowledge-based Navigation

By navigation we understand the selection of a single activity for further processing. The term means that the user is moving through a net of activities like a ship from one harbour to another. An activity is only selectable if its input is valid at this specific moment. The following possibilities exist:

- The completion of the activity is guaranteed.
- The activity can be started, but its completion is not guaranteed
- Using the 'Work ahead'-mode: means that the activity can only be started with proviso

Fundamental data for the decision are:

- process relevant data
  - state of the input results
  - state of the output results
  - predicate
  - state of activity
- tactical considerations about the whole work flow as given by Project Management

In order to find the right decisions it is necessary to look back to already finished projects. The different needed information for Project Management, Quality Assurance and Development decisions can only be provided by knowledge based decision systems [11]. A simple example can be:

- realisation of a critical situation (Project Management: costs run out of plan, Quality Assurance: bad educational standard of the involved developers)
- solving the problem (start a new C++ course, outsourcing by company xyz)
- automatic online updating of the knowledge base [8]

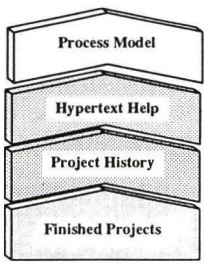


Fig. 6. Different knowledge bases involved in navigation

3.4 Navigation level, User Roles and Knowledge base

According to the different roles of users involved in a project they need different information of the knowledge bases.

User role	Level	Knowledge Base			
		PM	H	PH	FP
Administrator	o/t/s	++	-	o	+
Modeler	o/t/s	++	o	++	++
Manager	s	+	o	++	+
Developer	o/t	++	+	o	o
Observer	o	+	++	o	-
Others	o		++		

Tab. 1. Relation between Navigation level, Knowledge base and User role

PM: Process Model, **H**: Help information, **PH**: Project history, **FP**: finished projects
level: **o**: operational, **t**: tactical, **s**: strategic
Evaluation: ++ very important, + important, o neutral, - not needed

4.0 State automata

The object class model denotes the static structure of a process model. The dynamically behaviour of the conceptual entities and relationships which is prepared afterwards can be described via Moore automata [13]. A Moore automaton consists of states, state transitions and their state transition functions.

States provide information on the progress of a task, the status of a deliverable, or on the status of a specific version of a document. All tasks and deliverables can run through various states (see Fig. 7.): a task, for instance, can be ´awaiting start´, ´in production´ or ´completed´, deliverables, for instance, can be ´in production´, ´internally released´ or ´externally released´.

A state transition function is an algorithm which is executed when due to some events a state transition is carried out. Typical transition functions are shown in Fig. 7.

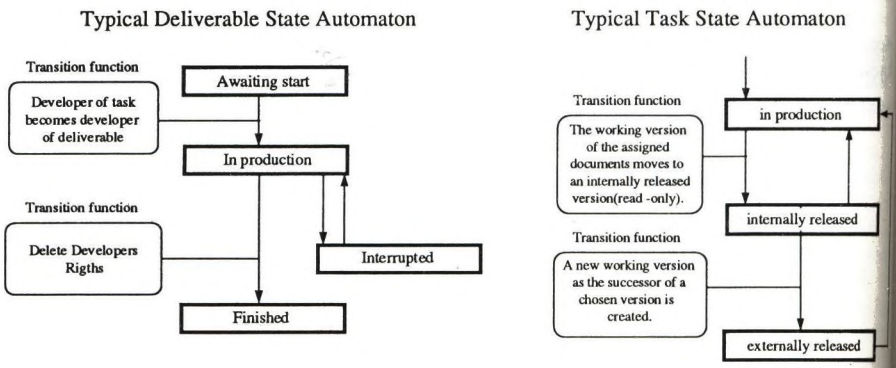


Fig. 7. Typical State Automaton

In MAESTRO*II* this concept has been implemented to provide powerful navigation support.

5.0 Networked Information

Thus in current SEEs a considerable ´interrelationship net´ of information can be found. These interrelationships occur within and across development levels and within and across subsystem boundaries. We have to distinguish between 3 important levels of information networks:

- **Object class network** (Activities, resources, deliverables, tools, their relationships and their attributes)
- **State automata network** (Local life cycles of the individual object classes)
- **Process network** (Project Management processes, Development processes, Integral processes see Fig. 9.)

5.1 Object class networks

In this network the conceptual entities of a project process are identified and formalised. At the moment there exist no generally accepted form of description. In literature there exist many different forms. We recommend the terminology of database description, defined by [17] who talks about an Entity Relationship Database, which consist of entity sets, relationships and attributes.

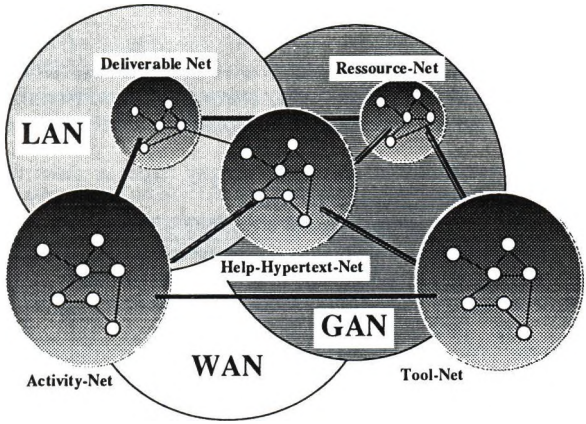


Fig. 8. Nets between different subsystems

5.1.1 Intraclass Relationships

The networks introduced below, could be considered as intra class networks, establishing relationships between classes of the same type or between instances of the same class. Major relationship nets are:

- **Activity class Network** Individual activity classes in the model are interrelated at least by relationships indicating their sequentialisation and their hierarchy.
- **Activity (instance) Network** For most activity classes more than one instance will exist. These instances will have relationships of their own.
- **Deliverable class network** Describes the deliverable types of a project, their hierarchical structure and the logical connections existing between them. It consists of deliverable types and standard and freely definable relations and attributes.
- **Deliverable (Instance) Network** similar to activity (instance) network
- **Help text Hypertext Network** Represents a network consisting of help documents, glossaries and keywords which are assigned to help documents, context information and connections between the keywords.
- **Tool Network:** Tools have to cooperate by exchanging data. Their interaction is largely defined by the relationships of the activities or deliverables to which they are attached.

Comparing MAESTRO*II* to ADPS we note that only MAESTRO*II* provides the first 4 networks to their full extent, while ADPS only can provide the hierarchical information. Help text is provided by both in hypertext form, while the tool network is not directly visible in either.

5.1.2 Interclass Relationships

They relate objects or classes of different categories to one another. These relationships are especially important in the realm of SEEs since they link together its various components. Typical examples are:

- **Activity input/output relationship:** relating an activity (type) to those deliverables (types) which specify the input/output of that activity (type).
- **Interphase deliverable relationships:** Phases are strongly related to the over-all strategy of development. Those relationships which relate deliverables (classes) of different phases to one another have special importance since they show the transformation of information in the development process and allow tracing of individual design elements e.g. Software specification --> code.
- **Tools / Activity relationship:** Tools are the workhorses of the software development. Tools have to be fitted to the appropriate activities or activity types.
- **Help Text association:** Help-informations are associated to activities and deliverables.
- **Activity task relationship:** For planning purpose Project Management groups activity types on a coarser level of granularity [6].

5.2 State automata / Network

Activity State Automata relationship: The deliverable model, activity model and the relations between them represent the static elements of projects. The state automata tracks how the project is progressing and they can be assigned to activity types. Activities in these types are always bound to the state automata assigned to them.
Deliverable State Automata relationship: similar to ´Activity State Automata relationship´.

A few object classes (tasks, deliverables, roles) actually go through their life cycles independently. In any real process model, the dynamic behaviour of an object class is correlated to that of other object classes. The correlation is based on process dependencies, project management policies, quality insurance rules and other of the project domain. Here are some examples.

Deliverable to Deliverable communication: Changing the state of a parent deliverable to the state ´finished´, should also change all children deliverables to state ´finished´.
Task to Task communication: Changing the state ´awaiting start´ to ´in production´ should also change the state of all parallel tasks to the state ´start possible´.
Deliverable to Task communication (and inverse): The interruption of the top activity e.g. ´carry out project´ by the project manager have to have consequences to all deliverables in the project for example changing their states to ´interrupted´ and delete all access rights for all users.

5.3 Process network

A process is a function that must be performed in the software application development. A process is composed of activities. Fig. 9 gives a feeling which processes are involved during the development process and how they communicate. The process is a more general view of the underlying objects, object classes, attributes, their relationships and the attached state automata.

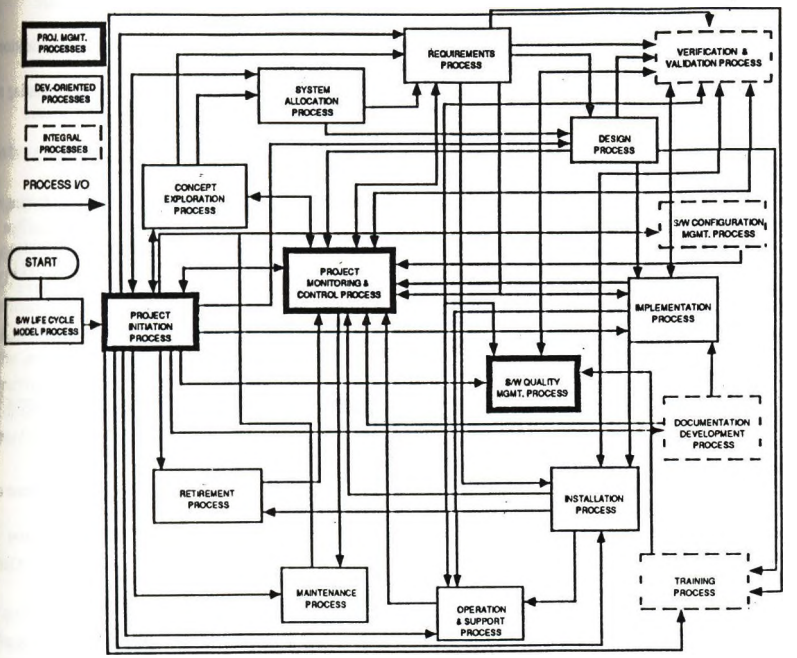


Fig. 9. Communication between different project processes [10]

6.0 Summary

In this paper we have shown the interrelated ('networking') structure of SEEs in general and we gave some special views on ADPS and MAESTRO*II*. Special focus was put on activity network

and navigation within them. Special emphasis was put on separating passive navigation means from activities like navigation via state automata.

7.0 References

[1] Boehm B.: A Spiral Model of Software Development and Enhancement.- ACM SIGSOFT - Software Engineering Notes vol. 11 (1986) No. 4, pp. 22-42

[2] Chroust G.: Application Development Project Support (ADPS) - An Environment for Industrial Application Development.- ACM Software Engineering Notes, vol. 14 (1989) no. 5, pp. 83-104

[3] Chroust G.: Duplicate Instances of Elements of a Software Process Model.- Tully C. (ed.): Representating and Enacting the Software Process - Proc. 4th Int. Software Process Workshop, May 1988.- ACM Software Engineering Notes vol. 14 (1989), no. 4., 61-64

[4] Chroust G.: Modelle der Software-Entwicklung Aufbau und Interpretation von Vorgehensmodellen.- Oldenbourg Verlag, 1992

[5] Chroust G.: Models and Instances - Some Thoughts on Concurrency in Software Development.- Software Engineering Notes vol. 13 (1988) no. 3, pp. 41-42.

[6] Chroust G., Knotter S.: Vom phasen-orientierten zum task-orientierten Vorgehen in Informatik-Projekten.- Elzer P. (ed.): Multidimensionales Software-Projektmanagement.AIT-Verlag München 1991, pp. 81-111

[7] Hommel G., Kroenig D.: Requirements Engineering -Arbeitstagung der GI, Friedrichshafen Okt. 1983.- Informatik Fachberichte, Springer, Berlin, Heidelberg, New York 1983

[8] Horn W.: Expertensysteme - Funktionen und Systeme - ein Überblick.- ™GAI-Journal vol. 2 (1983), No. 1, pp. 2-30.

[9] Humphrey W.S.: Managing the Software Process.-Addison-Wesley Reading Mass. 1989

[10] IEEE: IEEE Standard for Developing Software Life Cycle Processes, Institute of Electrical and Electronics Engineer, Inc., 345 East 47th Street, New York, NY 10017, USA, 1992

[11] Krallmann H.: Entscheidungsunterstützende Systeme.-Mertens P. et al. (eds.): Lexikon der Wirtschaftsinformatik.2. Auflage, Springer 1990, p.164-166

[12] Merbeth G.: MAESTROII - das integrierte CASE-System von Softlab.- Balzert H. (ed.): CASE - Systeme und Werkzeuge.- 4. Auflage, B-I wissenschaftsverlag 1992, pp. 215-232

[13] Moore F.: Gedanken-experiments on Sequential Machines, in Automata Studies, pp. 129 - 153, Princeton University Press, Princeton, New Jersey, 1956

[14] Ohno Y. (ed.): Requirements Engineering Environments, Proc. of the Intl. Symp. on Current Issues of Requirements Engineering Environments, Kyoto 1982.- North Holland Publ. Comp. Amsterdam, 1982.

[15] Phillips R.W.: State Change Architecture: A Protocol for Executable Process Models.- Tully C. (ed.): Representating and Encating the Software Process.- Proc. 4th Int. Software Process Workshop, May 1988 ACM Software Enfineering Notes vol. 14 (1989), no. 4., pp 129-132

[16] Shlear S.: An Object-Oriented Approach to Domain Analysis - ACM SIGSOFT - Software Engineering Notes vol. 14 (1989) No. 5, pp. 66-77

[17] Ullman J.D.: Principles of Database and Knowledge-Base Systems Vol I., Computer Science Press, Rockville, Maryland 1988

[18] Vetter M.: Strategie der Anwendungssoftware-Entwicklung.- B.G.Teubner Stuttgart 1988

[19] Zvegintzov N.: What Life? What Cycle? AFIPS (ed.): National Computer

BOOTSTRAP and ISCN
A Current Look at the European Software Quality Network

M. Biró[1], É. Feuer[1], V. H. Haase[2], G.R. Koch[2], H.J. Kugler[3], R. Messnarz[2], T. Remzső[1]

[1] Computer and Automation Institute, Hungarian Academy of Sciences
Budapest, Kende u.13-17. H-1111

[2] BOOTSTRAP AUSTRIA KEG, Graz, Austria

[3] K&M Technologies, Dublin, Ireland

Abstract

Hungary has recently joined the BOOTSTRAP network . BOOTSTRAP is a leading methodology for software process assessment and improvement developed in the framework of an ESPRIT project which was carried out by a consortium of European software companies and universities. BOOTSTRAP designed a very detailed process quality attribute hierarchy and enhanced the American SEI's method by taking into account the ISO 9000-3 guidelines for software quality and the ESA PSS-05 software engineering standards. An international BOOTSTRAP database is "fed" by the assessors' network and the summary results are presented and statistically analysed for comparison purposes. BOOTSTRAP will cooperate with the recently formed International Software Consulting Network (ISCN) which is a consulting and technology transfer organization aiming to support improvement strategies in the European software industry.*

1. Introduction

The quality of the software process determines the quality of the end product, or service, provided to the customer: quality is customer satisfaction! What is needed is integrated quality commitment throughout the process, rather than quality checks at the end. Product quality evaluation provides feedback on the quality of the process leading to constant improvement approaches that have long been a feature of quality-minded industries, especially in Japan.

Software quality and its improvement have been the aim of many different initiatives world-wide, such as the Capability Maturity Model (CMM) of the Software Engineering Institute (SEI) in the USA, various European R&D efforts in the framework of ESPRIT, EUREKA and the European System and Software Initiative (ESSI), and international and national efforts concerning ISO 9000.

*Supported by OMFB 93-97-67-0517

Software process measurement represents an evaluation of all the management activities, methods, and technologies that are used to develop a software product. In the next section we describe BOOTSTRAP, the most advanced network for quality assessment in the software field in Central Europe.

Last but not least we report on the formation of the International Software Consulting Network (ISCN) which is a consulting and technology transfer organization aiming to support improvement strategies in the European software industry.

2. BOOTSTRAP

In the United States the SEI (Software Engineering Institute) developed an assessment method for the DoD (Department of Defense) to assess the software development process of its contractors. Only those contractors are awarded further contracts in the field of software engineering, which are assessed and reach a high quality level [8].

Five maturity levels have been introduced for the measurement of the software development process: [3], [5], [6] Level 1: Initial Process, Level 2: Repeatable Process, Level 3: Defined Process, Level 4: Managed Process, Level 5: Optimizing Process. A new version of the maturity model has recently been published [9].

Software process assessments are based on a questionnaire about the SPU (Software Producing Unit), which is a software company or a department of a company, producing software. The SPU develops software products in the framework of specific projects.

BOOTSTRAP is a European ESPRIT project which was carried out by a consortium of European software companies and universities. The aim of this project was to develop a method for software process assessment and improvement. BOOTSTRAP enhanced and refined the SEI method for software process assessment and adapted it to the European software industry, including the non-defense sector such as administration, banking, and insurance. BOOTSTRAP designed a very detailed process quality attribute hierarchy and enhanced the SEI Questionnaire by taking into account the ISO 9000-3 guidelines for software quality and the ESA PSS-05 software engineering standards. Additionally, it refined the maturity level algorithm to be able to calculate a maturity level for each of the individual process quality attributes. Thus we get a process quality profile that provides a representation of the strengths and weaknesses. This quality profile serves as a quantitative basis for making decisions about process improvements. Having based the work on the ISO 9000-3 standard, BOOTSTRAP can calculate about 85% of the ISO attributes as well whether they are satisfied or not. Therefore BOOTSTRAP can also be used as a preparation for the ISO certification.

BOOTSTRAP emphasises that organization is most important and that methodology is more important than technology. A project without organisation is nearly certain to result in a disaster. On

the other hand, it does not help to buy a technology when the software engineers either cannot understand the method of the technology or do not accept the underlying technology.

BOOTSTRAP uses separate questionnaires, one for the SPU and another one for the projects. The questionnaire for the SPU is called Global questionnaire and asks information about the existence of certain procedures, methods, standards and technologies. In the Project questionnaire the target is the use of these procedures, methods, standards and technologies.

BOOTSTRAP defines software quality attributes and assigns all questions to these attributes as well as levels. Therefore it is possible to calculate a maturity level for each attribute as well as for the whole SPU and for the project.

Individual Attributes of an SPU According to BOOTSTRAP:

ORGANIZATION

Quality Assurance

Resource Management
Staffing
Training

METHODOLOGY

Process Related Functions

Process Description
Process Measurement
Process Control

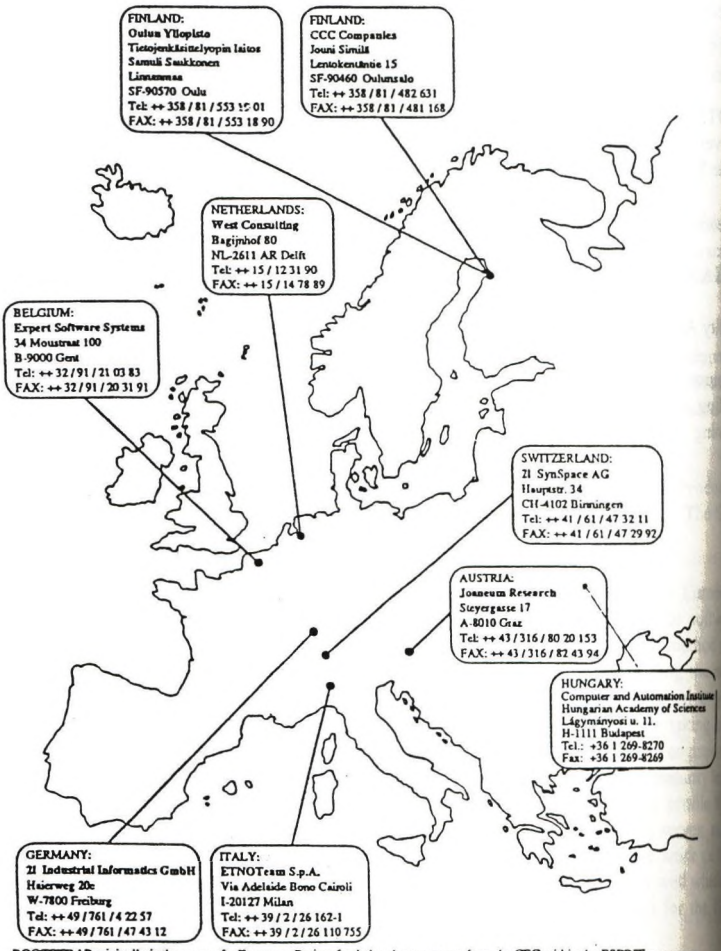
Life Cycle Independent Functions

Risk Avoidance & Management
Project Management
Quality Management
Configuration & Change Management

Life Cycle Functions

Development Model
Requirements
User Requirements
Software Requirements
Architectural Design
Detailed Design
Testing
Unit Testing
Integration Testing
Acceptance Testing & Transfer
Operation & Maintenance

The Presence of BOOTSTRAP in Europe: Our Consultants are close to you



BOOTSTRAP originally is the name of a European Project funded under a contract from the CEC within the ESPRIT programme.

Fig. 1 The BOOTSTRAP Network in Europe

In order to reach more precise results the BOOTSTRAP questions can be answered not only by yes or no as it was initially in the SEI questionnaire, but by a more differentiating scale of four possible answers. (0 % / weak or absent, 33 % / basic or fair, 66 % / significant or strong, 100 % / extensive or complete, and of course some questions may be not applicable). The dependency of the questions is taken into account, this means that the answer of a dependent question can not be scored higher than the original.

The BOOTSTRAP Institute, formed by the ESPRIT project partners in 1993, has assessors all over Europe. Fig. 1 shows the locations. In the last two years about 40 assessments with 70 projects have been performed by the assessors of the BOOTSTRAP network to determine the profile of SPUs in several European countries. The data is collected from every assessed SPU to a common database, analysed and compared with the average values of the appropriate subsets. Thus we can determine a profile of the European software industry and determine the position of an SPU in the European market [4], while the confidentiality of the SPU's data is highly guaranteed by appropriate contracts which constitute an integrated part of the methodology itself.

Hungary has recently joined the BOOTSTRAP network. The Hungarian BOOTSTRAP team is planning to contribute to the quality and competitiveness of Hungarian software in the European and World market.

3. International Software Consulting Network (ISCN)

ISCN (The International Software Consulting Network) is a consulting and technology transfer organisation consisting of experienced software professionals aiming to support improvement strategies in the European software industry. ISCN employs its own quality consulting process that is subjected to constant improvement. ISCN co-operates with the European Software Institute (ESI), the European System and Software Initiative (ESSI) and with leading European ESPRIT projects (ami, BOOTSTRAP, METKIT, SCOPE) in the software metrics and quality engineering field to set up a technology transfer initiative which combines the approaches of many ESPRIT projects and European programs.

ISCN SEMINAR ORGANISATION

The ISCN seminar is the first comprehensive technology transfer event in Europe to address all the aspects involved in software quality improvement - *Process Analysis, Process Modelling, Product Quality Evaluation*, and *Practical Process Improvement and Installation*. It shows how methods and techniques in these various areas can be combined to multiply their beneficial effect - both in the management and technical dimensions of the software process. The seminar creates a unique opportunity for leading-edge training on practical European advances in process and product quality measurement and improvement.

The seminar presents current methods and strategies to improve the software process, provides guidelines, methods and techniques to evaluate product quality and cost benefits, and facilitates continued technology transfer and support in process improvement installation through making available a contact network of experts.

Each of the topics will be addressed by talks of experts in the field. Panel discussions and workshops will give participants an opportunity to discuss problems and solutions.

Audience: Participants of the ISCN seminar will be managers and development engineers who are concerned with, or who are interested in quality engineering in the European software industry, be it for in-house development or use, for bespoke development, or for the development and supply of standard software products.

Benefits: Attendees will be able to analyse and understand software processes in their own organisation to identify bottlenecks, to plan and action improvement steps, and to identify the right expertise needed to carry out these steps.

Organisers: This technology transfer seminar is organised by ISCN in co-operation with leading European ESPRIT projects in this field: ami, BOOTSTRAP, METKIT and SCOPE. The support of COMETT is gratefully acknowledged.

ISCNs TECHNOLOGY TRANSFER INITIATIVE

- **Background**

"ami" is a European ESPRIT project which developed a software process improvement method comprising 4 steps: Process Assessment --> Analysis --> Goal Definition (Goal Question Method) and Metrification of the goals --> Implementation & Quantitaitive Evaluation if the goals have been met. For the Process Assessment and Analysis steps BOOTSTRAP provides a proper method. Based on the results of the analysis step a goal tree (major goal is defined; major goal is subdivided into subgoals; and subgoals can also be recursively refined into further subgoals) is designed and software metrics are assigned to the goals to be able to measure if the goals have been achieved. "ami" also provides an overview about which metrics (process and product metrics) can be used to verify and evaluate the goals.

BOOTSTRAP is the European ESPRIT project described in more detail in the previous section.

SCOPE is a European ESPRIT project which concentrated on the development of a product evaluation guide and method. They defined a number of quality attributes of software products, assigned software metrics to the quality attributes to be able to get quantitative feedback about the product reliability and quality, and produced a guideline about how to plan and specify the product evaluation and about a standard format and structure of a product evaluation report. "ami" provided

an overview about which metrics can be used to verify if the defined goals have been met. Thus the results of SCOPE can be used to measure and evaluate the goals which are related to the product.

METKIT is a European ESPRIT project which did research on a vast array of product metrics but mostly concentrated on product complexity measures. Most product metrics are related to the complexity of a software product such as size, complexity, error rate, quality, coverage, etc. Thus METKIT provided a lot of results about "how to scope with software complexity" and "how to measure software complexity". "ami" provided an overview about which metrics can be used to verify if the defined goals have been met. Thus the results of METKIT can be used to measure and evaluate the goals which are related to the product.

- **The Initiative**

ISCN's technology transfer initiative combines the approaches of all four ESPRIT projects to one overall improvement and consulting methodology. We use BOOTSTRAP to do the process assessment and analysis. "ami" then sets up a goal tree and assigns metrics to the goals to be able to quantitatively measure if the goals have been met. BOOTSTRAP and "ami" provide a number of process metrics which can be assigned to goals related to the software process. METKIT and SCOPE provide a number of measures and guidelines which can be used to evaluate the product related goals. After the implementation phase (implement improvements: process modelling to improve the organisational processes, introduction of methodologies and technologies) the goals are evaluated and the gained benefits are measured. And with the next process assessment and analysis we are entering the improvement cycle. Thus we have achieved an overall improvement cycle covered by the results of four ESPRIT projects in the software metrics and process improvement field. ISCN provides a cooperation platform of the four ESPRIT projects mentioned above and defines a comprehensive technology transfer and process improvement initiative.

There is a direct relationship between ISCN and ESI (European Software Institute). ISCN defines a technology transfer initiative which is based on all improvement methodologies developed by different institutions (e.g. ESSI) and European ESPRIT projects (AMI, BOOTSTRAP, METKIT, SCOPE). Thus it is the first time that a realy comprehensive technology transfer event is set up which addresses all aspects of software process and product improvement: process analysis, process modelling, product quality evaluation, and process improvement and installation. It is one goal of ESI to strategically support the ongoing refinement and adaptation of all the software process and product improvement methodologies, and it is ISCNs interest to transfer these methods and strategies into the European software industry. Thus ISCN operates as a technology transfer bridge between ESI and the European software industry.

There is also a direct relationship between ISCN and COMETT. COMETT enables researchers to participate in industrial projects to be able to introduce the most current research results to industry. ISCN is specifically set-up to manage a technology transfer function for software process and product improvement methods and strategies.

And there is a direct relationship between ESSI and ISCN as well. ESSI strategically supports projects that introduce new and modern methodolodies and technologies to the software process, measure the benefits and discuss the experience they gained with the new method or technology, and disseminate the experience in workshops and at conferences. This will accelerate the process of finding the best practices in methodologies and technologies so that the best practices can finally be used by all European software houses. However, the disseminated experiences have to be taken into account at the establishment of BOOTSTRAP Action Plans and the definition of "ami" Goal Trees. The output of the ESSI initiative will enable ISCN to select the right methodologies and technologies to improve software processes.

4. Conclusion

The BOOTSTRAP partners have already performed and are currently performing a number of assessments throughout Europe, including Austria, Belgium, Finland, Germany, Hungary, Italy, The Netherlands, and Switzerland. Large companies in Germany, France and the UK have become or are interested in becoming BOOTSTRAP licensees. BOOTSTRAP's analysis and consulting approach is well accepted by the European software industry. Direct cooperation with ESI, ESSI and the cooperation of ESPRIT projects in the software metrics field in the ISCN will have a multiplying effect on the use of improvement methodologies in the European software industry.

References

[1] T.B. Bollinger, C. McGowan: A Critical Look at Software Capability Evaluations. IEEE Software, July 1991, pp.25-41.

[2] ESA Board for Software Standardization and Control: ESA Software Engineering Standards, European Space Agency, Paris, France: 1991.

[3] ESPRIT Project 5441 BOOTSTRAP: Phase I Interim Report. Composite Deliverable 7, Commission for European Communities (CEC), July, 1991.

[4] V. Haase, R. Messnarz: A Survey Study on Approaches in Technology Transfer, Software Management and Organization. Report 305, Institutes for Information Processing Graz, June 1991.

[5] Humphrey W.S., Bill Curtis: Comments on "A Critical Look". IEEE Software, July 1991, pp.42-46.

[6] Humphrey W.S.: Managing the Software Process, 494p., SEI Software Engineering Institute, New York, Amsterdam, Bonn, Madrid, Tokyo: Addison - Wesley Publishing Company 1989.

[7] ISO 9000-3: European Standard for Quality Management and Quality Assurance, European Committee for Standardization, Bruxelles: 1987.

[8] M.C. Paulk, B. Curtis, M.B. Chrissis: Capability Maturity Model for Software, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, August 1991.

[9] M.C. Paulk, B. Curtis, M.B. Chrissis, C.V. Weber: Capability Maturity Model, Version 1.1, IEEE Software, July 1993, pp.18-27.

Experience of international R & D work through computer networks — the Gigalips project

Péter Szeredi*
IQSOFT (SZKI Intelligent Software Ltd.)
H-1142 Teleki Blanka u. 15–17.
Budapest, Hungary
E-mail: szeredi@iqsoft.hu

Abstract:

The talk presents some impressions on the role of computer networks in cooperative research and development work. The author spent three years in the United Kingdom, working in an international project with principal partners from U.S. and Sweden, and continued this collaboration for the last three years after returning to Hungary.

Following a brief description of the collaborative project, we discuss various aspects of network-based R & D work. We also outline the issues involved in setting up a suitable communication infrastructure in the Hungarian environment.

1 The collaborative project

The author is one of the main authors of the Aurora or-parallel Prolog system[1]. Aurora [6] is a prototype or-parallel implementation of the full Prolog language for shared memory multiprocessors, currently running on Sequent, Encore and BBN machines. It has been developed in the framework of the Gigalips project, a collaborative effort between groups at the Argonne National Laboratory in Illinois, the University of Bristol, and the Swedish Institute of Computer Science (SICS). IQSOFT (Budapest) joined the Gigalips consortium in 1990.

Aurora is built of two main components: the Prolog engine and the parallel scheduler. There is a strict interface between these two components [8], that enabled the development of several schedulers based on different principles and algorithms.

[1]Part of the work reported here has been carried out while the author was at the Department of Computer Science, University of Bristol, Bristol BS8 1TR, U.K.

2 Project organisation

The Gigalips project is an informal collaboration of several research groups. The bulk of interactions is carried over electronic mail. Meetings of researchers at various participating sites are held regularly. The meetings often include a workshop, with talks on various aspects of the project and related work. The other main part of a Gigalips meeting is a so called "hacking session", the main purpose of which is to synchronise the development of the prototype software.

The development of the various components of the Aurora software system is done at different sites. SICS is responsible for the Prolog engine [5], based on the SICStus Prolog system. Various schedulers have been developed at Argonne [3], Manchester [4], SICS [2] and Bristol [7] [1]. Other contributions, such as visualisation and tracing tools, performance analysis and various experimental applications have also been developed at the Gigalips sites.

At the hacking sessions a "checkpoint" of the software is produced. This is a version of the system including all components. All the changes, which have been developed in the preceding period at all sites are merged into the checkpoint version and the resulting system is fairly carefully debugged.

The checkpoint is archived and the RCS revision control system is used to keep track of the new developments at each site. Merging of the different improvements is aided by the public domain `diff` and `patch` programs.

Between the hacking sessions the bug fixes and the most important new developments are communicated to partner sites as `diff` files with respect to the latest checkpoint.

3 Networking aspects of the project

Initially the project relied almost exclusively on email as a communication means. Subsequently remote logins using the X25 connection were also employed. More recently, as most of the sites are being established as Internet nodes, higher level and more convenient communication programs are used, such as telnet, ftp, talk and others.

Interestingly enough, the network changes the working style as well. One is forced to think over and write down the arguments in a discussion before sending them away. Often such careful formulation helps to clarify the issues much more rapidly than in a "real" interactive discussion.

The delivery time of email messages has a significant impact on the work. Prompt delivery of email makes it possible to have several rounds of discussion messages during a day. On the other hand, if the email links are down or slow, one feels cut off from the colleagues and the work slows down.

It may be interesting to note that several megabytes of email messages on Gigalips matters have been archived by the author. With such archives it is relatively easy to locate messages on a given decision point and use them in subsequent work.

4 Using networks in Hungary

It is a trivial fact, that Hungary is behind the Western world in computer networks. It took quite a bit of effort to establish a minimal communication infrastructure at IQSOFT. Initially, in 1990, electronic mail was only available through the ELLA PC-based system. In 1991 IQSOFT was one of the first companies to join the Hungarian Unix Users Group and to establish a Unix-based (uucp) email-link. Telephone and X25 are the two complementing physical transfer means for this email-link.

Initially the X25 network was used for remote login to the Western European sites, from where U.S. sites could be reached via Internet. More recently we switched to using Hungarian Internet nodes to reach the Western sites. The bottlenecks in the Internet communication between Hungary and the outside world sometimes force us to resort to using direct X25 connections to Western Europe.

The remote login facility has enabled us to use multiprocessors at Western sites, unavailable in Hungary. On the other hand IQSOFT still lacks the proper Internet connection, that would bring the full integration of the development environment with our partners.

Although the fairly slow and sometimes unreliable communication links require much more patience, the possibility for communication with, and remote work at Western sites is established and functioning.

5 Conclusion

Computer networks play an increasingly important role in international collaborative efforts such as the Gigalips project discussed in this talk. The development of the ideas and the software for the Aurora or-parallel Prolog would have been impossible without various forms of electronic communication.

Acknowledgements

The author wishes to thank all his colleagues in the Gigalips collaboration, and especially Tony Beaumont, Mats Carlsson, Bogdan Hausman, Rusty Lusk and David H. D. Warren.

The author has been supported by ESPRIT projects 2471 ("PEPMA") and 2025 ("EDS") and by the U.S.-Hungarian Science and Technology Joint Fund under Project No. 031/90.

References

[1] Anthony Beaumont, S Muthu Raman, Péter Szeredi, and David H D Warren. Flexible Scheduling of Or-Parallelism in Aurora: The Bristol Scheduler. In *PARLE91: Conference on Parallel Architectures and Languages Europe*, pages 403–420. Springer Verlag, June 1991. Lecture Notes in Computer Science, Vol 506.

[2] Per Brand. Wavefront scheduling. Internal Report, Gigalips Project, 1988.

[3] Ralph Butler, Terry Disz, Ewing Lusk, Robert Olson, Ross Overbeek, and Rick Stevens. Scheduling OR-parallelism: an Argonne perspective. In *Logic Programming: Proceedings of the Fifth International Conference*, pages 1590–1605. The MIT Press, August 1988.

[4] Alan Calderwood and Péter Szeredi. Scheduling or-parallelism in Aurora – the Manchester scheduler. In *Logic Programming: Proceedings of the Sixth International Conference*, pages 419–435. The MIT Press, June 1989.

[5] Mats Carlsson and Péter Szeredi. The Aurora abstract machine and its emulator. SICS Research Report R90005, Swedish Institute of Computer Science, 1990.

[6] Ewing Lusk, David H. D. Warren, Seif Haridi, et al. The Aurora or-parallel Prolog system. *New Generation Computing*, 7(2,3):243–271, 1990.

[7] Raed Sindaha. Scheduling speculative work in the Aurora or-parallel Prolog system. Internal Report, Gigalips Project, University of Bristol, March 1990.

[8] Péter Szeredi, Mats Carlsson, and Rong Yang. Interfacing engines and schedulers in or-parallel Prolog systems. In *PARLE91: Conference on Parallel Architectures and Languages Europe*, pages 439–453. Springer Verlag, June 1991. Lecture Notes in Computer Science, Vol 506.

NETWORKS AND RELATED ISSUES

Chair: L. Csaba, H. Jeram.

ATM

The Future Technology for Enterprise Networks

As Driving Force for B-ISDN

Dr. Peter Tomsu

Schoeller Electronics

Abstract

ATM (Asynchronous Transfer Mode) is a technology, which describes a new transmission method for all kind of data (computer data, voice, pictures and video). ATM splits each type of information into equal long units - so called cells. This method was developed by CCITT as base technology for Broadband ISDN (B-ISDN) and was initially intended to transport information with highest speed (gigabit per second) via Wide Area Networks. All these advantages make ATM also interesting for Local Area - and Enterprise Networks and in the meantime a big number of manufacturers in this area adopt this new technology in order to solve all the requirements of bursty applications with the need for high bandwidth.

The following article gives a short overview about the development of Enterprise Networking. It is shown, how ATM becomes the most important one of all the emerging backbone technologies in order to provide seamless integration of different types of data into a single network and how ATM Switches will become the central points of networking in the future. The availability and the usage of ATM in the local - and enterprise area will be the driving force for B-ISDN and therefore it will be the first step towards a future end to end ATM connectivity over LANs and WANs.

1. Introduction

The ATM concept has been the result of the convergence of two innovative network technologies, developed at the beginning of the '80s, namely ATD (Asynchronous Time Division) and FPS (Fast Packet Switching).

ATD, which was developed at the CNET Laboratories was a switching and multiplexing technique employing short fixed size packets, very similar to ATM. ATD could be best described as a new PCM (Pulse Code Modulation) scheme, in order to carry video (isochronous) traffic. FPS was developed at Bell Laboratories and consisted of a much simplified version of traditional data protocols, similar to Frame Relay with the additional emphasis on integrated services. Switching technology and also the support of voice were investigated, with the variable data frame size playing a key role for the efficient support of both. The intended main application environment was to offer of a wide area connectivity service for large corporate networks generating data and voice traffic.

CCITT developed the framework of B-ISDN (Broadband Integrated Services Digital Network), leading to a set of 13 draft recommendations on ATM and B-ISDN in the middle of 1990. Since the negotiation process was carried out on purely technical issues and did not take into account any underlying network assumptions, the standards which resulted out of this process are on the one side agreed upon worldwide, but carry with them many ambiguous and undeveloped points which have to be interpreted when implementing a specific network application. Future standardisation activities are focusing mainly on signalling protocols and traffic management issues can be expected not to have any more these difficulties.

The evolution and adoption of ATM technology is opening up new application horizons for networks and their users. ATM will play an important role in all facets of multienterprise networking. This includes backbone networks, where it will provide higher aggregate throughput than conventional shared media networks. It includes also workgroup and departmental Local Area Networks (LANs), where ATM will offer high performance connectivity for workstations and servers. And finally it includes Wide Area Networks (WANs), where ATM will allow remote offices and branch locations as well as key customers, partners and suppliers to tie into corporate networks in ways that were never before possible.

ATM also offers a number of advantages that optimize it for todays emerging wave of demanding applications (see Figure 1 - Emerging Applications). This is particularly true in the case of compute intensive multimedia applications, such as advanced graphics, audio, video conferencing and other uses that exceed the capabilities of todays existing networks. This support for complex multimedia applications, along with ATMs high performance, scalability, compatibility with existing network investments and ability to seamlessly integrate LAN and WAN technologies, marks ATM as the driving force behind the next generation of networking solutions.

It is for sure, that ATM will start up first in Enterprise Networks and therefore the driving force for ATM will come from this area, although ATM was designed for WAN use first. It will be outlined throughout this article, what significant role will be played by ATM in the Enterprise Networking world and thus will also be one of the driving forces for B-ISDN.

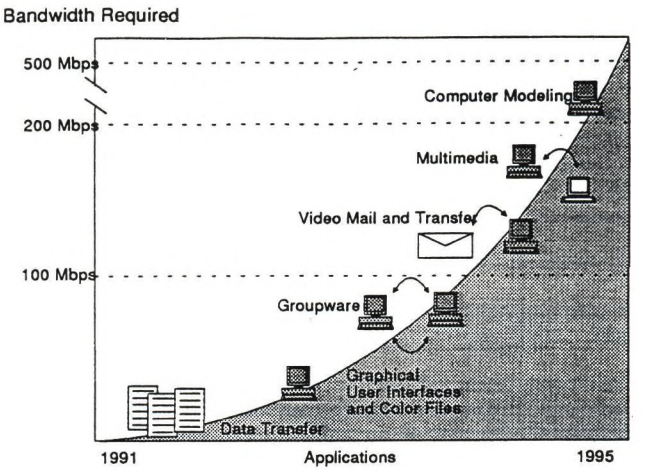


Figure 1: Emerging Applications

2. Enterprise Backbones and Structured Cabling

To keep pace with the ever increasing number of users needing high bandwidth access to the full complement of enterprise communications services, the first information backbones emerged in the mid 80s. The primary goal of those backbones was to provide the necessary bandwidth for up-the-riser, host-to-terminal communications within the building or campus. In addition, the first backbones were devised as a way of combining multiple protocols accross one common data path, while allowing those protocols to be centrally controlled and mangaged.

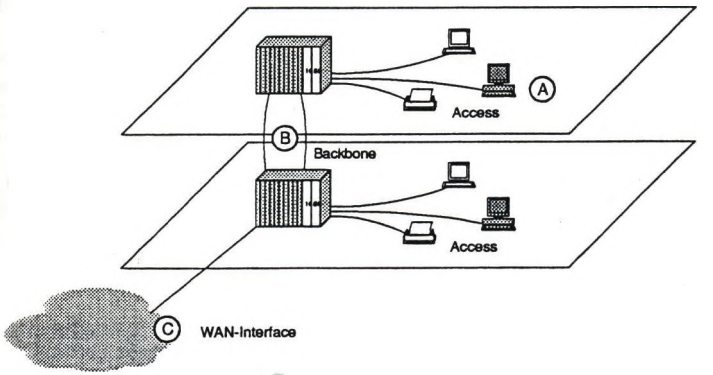


Figure 2: Typical Enterprise Network

In its purest definition an enterprise backbone can be defined as an aggregate data path (in essence, a central communications highway) for the transport of all signals to users located throughout the enterprise (see Figure 2 - Typical Enterprise Network). Based on that criteria, the first true backbones were multiplexers. The companies utilizing backbone technology, then and now, typically have one or more of the following characteristics or communications needs:

- Multiple data protocols and signals (data, LAN, voice and video) and heavy network traffic that need to be supported simultaneously.
- Multiple workgroups, networks and facilities that need to be internetworked.
- Mission critical applications, where the need for high reliability and data security are mandatory.
- A need to support varying media and device types, with a high degree of upgradeability, so that existing equipment can be preserved and higher performance hardware and software solutions can be implemented seamlessly.
- A relatively high degree of network moves, adds and changes, requiring that the enterprise network be highly manageable.

Since this article intends to describe the status and the future of private enterprise backbones, public backbones will not be treated. Enterprise backbones can be separated in the three following categories:

- Multiplexers (or those based on multiplexing technology)
- LAN backbones (based on FDDI, Ethernet, Token Ring, ...)
- Collapsed Backbones (based on high speed router technology)

Sometimes these three backbones have been viewed as competing, but within the last several years a significant distinction between the uses of backbones has manifested itself in the information systems community. At present there are significant differences between various backbone technologies and they serve unique applications. The selection of one backbone type over another is dependent on the required support.

2.1. Multiplexer Backbones

The first devices to be known as backbone solutions were multiplexers. They are mainly used in the mainframe environment, because the technology upon which multiplexers are based has been optimized for transmitting host-to-terminal, synchronous and asynchronous, voice and real-time data. Any of todays multiplexers can also forward LAN traffic (packetized data).

A multiplexer simultaneously transmits several messages or signals across a single channel or data path. It is best to think of a multiplexer as a pair of devices, one that gathers signals at one end, combines those signals and then transports them. Another device receives those signals demultiplexes them and distributes them to the local addresses. There are two primary types of backbone multiplexers used today, Time Division Multiplexer (TDM) and Statistical Multiplexer.

TDM is the method which is most prevalent in todays enterprise networking environments. TDM technology has the goal to efficiently transfer real time data simultaneously with LAN data. A TDM combines signals onto high speed links and then sends those signals sequentially at fixed intervals, where each user interface is allocated a specific, dependable time interval, within which data can be transported (see also Figure 3 - The Way How TDM Works). Typically TDM is capable of transporting signals at rates in excess of 100 Mbps, but from the users perspective the transmission speed is the same as the native speed of the original signals being sent. The largest drawback of TDM is, that it allocates bandwidth to devices that have nothing to send which means an inefficient use of bandwidth.

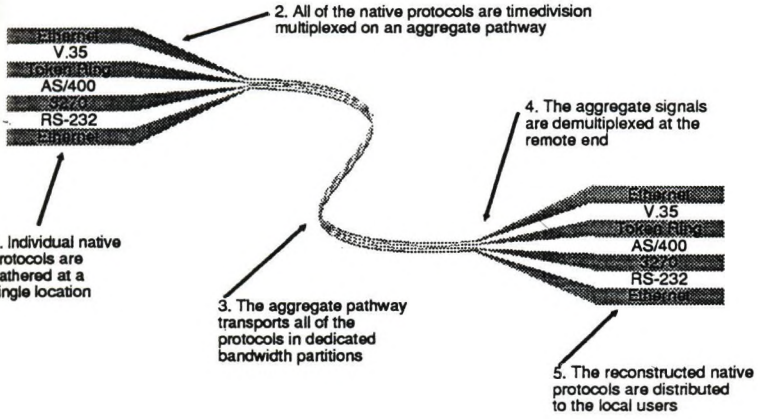


Figure 3: The Way How TDM Works

Statistical Multiplexers attempt to move as much data as possible across a transmission path, dividing a channel into independent lines, the sum of which often exceeds the line's transmission speed. It is based on the premise that devices rarely need to transmit or send data constantly at full available speed. The weaknesses of this scheme are that Statistical Multiplexers require more management in terms of initial set up and increased user intervention, which makes them more expensive to operate and finally they can not guarantee availability of bandwidth.

2.2. LAN Backbones

Unlike multiplexers which are capable of transmitting an array of data, host to terminal, voice and video signals LAN backbones are exactly what the name implies - they are dedicated exclusively to transferring local area network communications. Of course also slower LAN technologies as Ethernet and Token Ring can be used as backbones, especially if not the speed is the key issue, but the advantages of structured cabling are interesting to introduce a backbone.

However, the key LAN standard that has a more far reaching backbone based application is FDDI - Fiber Distributed Data Interface. FDDI is the dominant LAN backbone of today and provides standards based connectivity for both Ethernet and Token Ring (see also Figure 4).

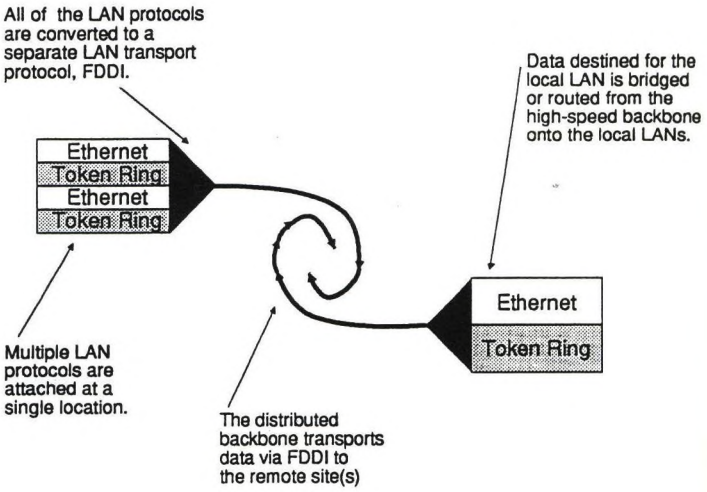


Figure 4: FDDI Backbone

FDDI is a token passing ring network utilizing fiber to transfer data at 100 Mbps. An FDDI ring can be as large as 100 km with a 2 km distance between adjacent nodes. FDDI specifies dual counter rotating rings for reliability reasons. The greatest strength of FDDI is that it is optimized for use as a high speed LAN, providing standards based physical connection and backbone support. Modern routers and bridges work on base of the translational method which means that frames coming from Ethernet or Token Ring are converted to FDDI frames and vice versa. This allows all stations on a FDDI ring to understand all frames coming along the ring and passing them through, or sending them out to the attached network.

2.3. Collapsed Backbones

Recently a powerful new backbone trend emerged that attempts to cull some of the best features of multiplexer and LAN backbone technology and convert them to an open, scalable backbone solution based on the functionality of todays high speed routers or HUBs.

This technology is called Collapsed Backbone, since it collapses vast amount of data onto the backplane of a high throughput router or HUB. LAN connections are starred back to the central collapsed backbone for high speed internetworking (see also Figure 5 - Collapsed Backbone Model). The Collapsed Backbone thus serves as the gatekeeper for the entire Enterprise Network and provides sophisticated protocol conversion and routing along an ultra high speed gigabit backplane. Furthermore it provides an efficient interface for LAN-to-WAN connectivity and gives network managers an efficient way to centrally service and maintain their networks. Collapsed backbones do not have to translate LAN signals into an intermediate signal (like FDDI) to transport them, rather Ethernet LANs can talk to Token Ring LANs directly via an internal backplane.

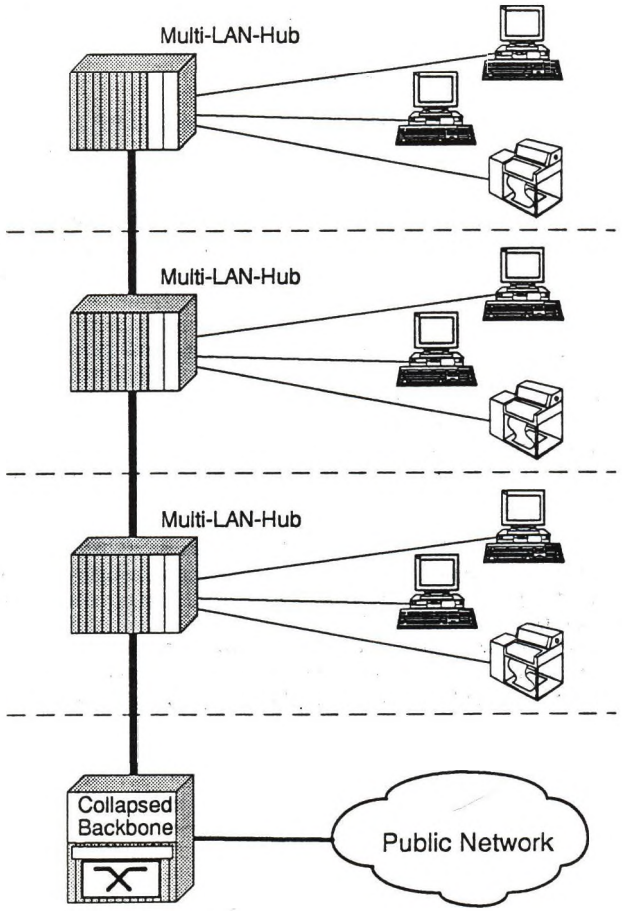


Figure 5: Collapsed Backbone Model

In the progressing evolution towards a seamless enterprise network the Collapsed Backbone is positioned to play an important role, since it enables users to transparently access services regardless of their location and to form user groups throughout the enterprise without limitations due to network architecture and location of the single users - this technology is commonly called Virtual Networking.

There are of course some drawbacks of todays Collapsed Backbones. First they are processor and software intensive and require more maintenance than typical HUBs. Second todays typical backplanes are based on bus type technologies, which means that all users have to share the bandwidth of the bus and can not expect a certain dedicated bandwidth. Finally the use of variable length frames instead of fixed length cells (as usual with ATM) does not give them the capability to transfer isochronous traffic (voice and video) together with arrays of data.

3. Emerging Backbone Technologies

Future backbones need to accomodate more protocols and applications and require greater processing speeds. There exist a number of emerging data communications technologies which will have a profound impact on how backbone solutions are implemented. Three of the most promising ones are Asynchronous Transfer Mode (ATM), Synchronous Optical Network (SONET) and FibreChannel. ATM is a transport protocol, which works on top of any physical media (for example SONET or FibreChannel) and seems to have the most significant impact on the implementation of enterprise backbone solutions.

ATM is a switched, connection oriented LAN and WAN technology that allows a virtually unlimited number of users to have dedicated, high speed connections with each other and with high performance network servers. It is extremely scaleable in terms of desktop interface speed, aggregate bandwidth and geographic scope. There exist three primary differences between ATM and conventional shared media networks: ATM uses dedicated media (use of switching), fixed length cells and connection oriented communication.

Todays Collapsed Backbones are mainly based on Routers and HUBs, which make use of shared media backplanes. Collapsed Backbone solutions of tomorrow will be based on switching technology, with ATM being the core of the switching scheme (see Figure 6 - Future End-to-End ATM Network). The ultimate vision for ATM is of course not to be restricted to the Enterprise Network, but to be the end-to-end network, carrying all traffic from a wide variety of resources. Thus ATM will be the first solution that can erase the barriers between Local Area Networks and Wide Area Networks.

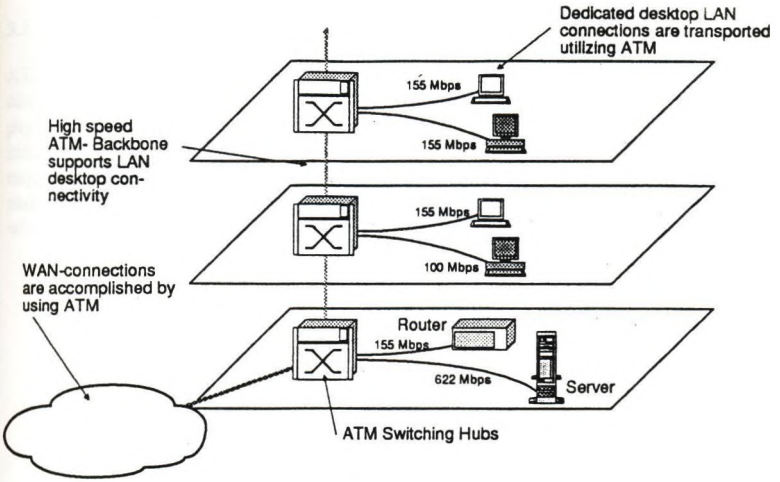


Figure 6: Future End-to-End ATM Network

Todays barriers between LANs and WANs are significant. LANs are optimized for data transmission and peripheral sharing. WANs are by contrast primarily suited for telephony. Linking two LANs via a WAN means today, that data have to be converted once as they are sent from the LAN to the WAN and then on the receiving side back from the WAN to the LAN. This means in any case a significant overhead in conversion resulting in expensive and relatively slow equipment. As soon as end-to-end ATM connectivity will be available, traffic will travel from the originating workstation, server or host via the WAN to its destination without the need of any conversion. Furthermore pure data traffic can be intermixed with isochronous traffic, enabling multimedia applications and the usage of only one backbone network, instead of many different dedicated networks. This will finally result in a tremendous reduction in management and maintenance costs as well as equipment costs.

As already stated, ATM interfaces, protocols and network operation are currently defined for the use in Wide Area Networks by a set of recommendations developed by CCITT. These recommendations have been adopted for use in both Local- and Wide Area Networks by the ATM Forum, an organization comprised of network users, equipment vendors and service providers. Because the same standards serve as the basis for both LAN and WAN ATM implementations, seamless integration of these two environments can finally be achieved (see Figure 7 - ATM Standards Shared by LAN and WAN).

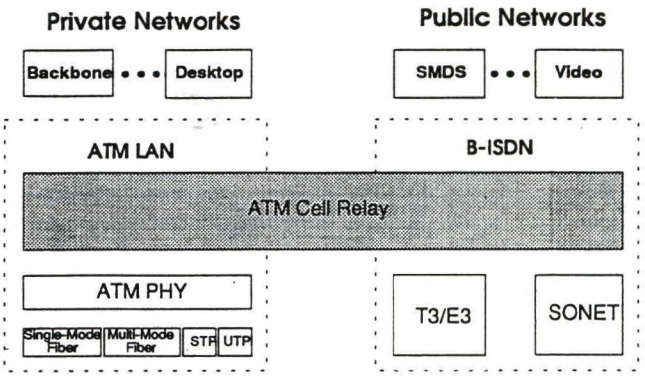


Figure 7: ATM Standards Shared by LAN and WAN

3.1. ATM Switching versus Shared Media

In a typical LAN backbone or a bus backplane the bandwidth is fixed and individual user bandwidth is determined by dividing that bandwidth by the number of users. ATM users in a switched ATM network have no effect on each other and are not impacted by the amount of bandwidth other network users occupy. This is due to the fact, that network or aggregate bandwidth is determined by the sum of the bandwidth required by the users. (See also Figure 8 for ATM Switching vs. Shared Media).

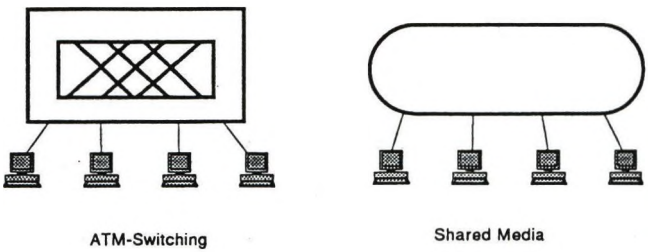


Figure 8: ATM Switching vs. Shared Media

3.2. ATM Cells versus Packets

ATM cells have a fixed length of 53 octets (containing a 5 byte header with address and control information and a 48 byte payload). The information in the header and the payload are always in the same place (see Figure 9: ATM Cell Format). Thus processing incoming cells in hardware is simple. Buffers as well as high processing power are not required, since switching can be easily and instantly done in hardware since the length and the content of the cell are known (the header of the cell contains the address field, which determines the route through the switching matrix).

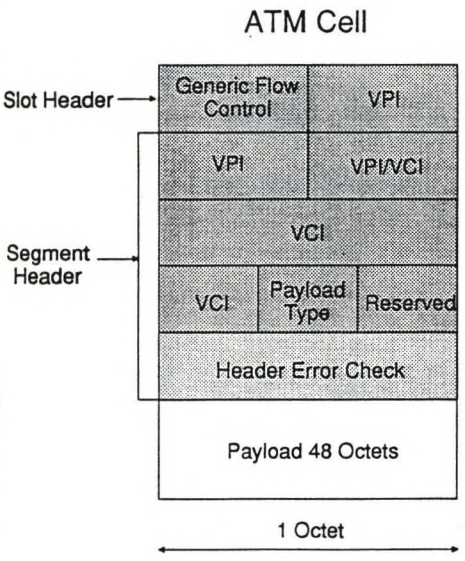


Figure 9: ATM Cell Format

By contrast Ethernet, Token Ring or FDDI packets vary in length. Thus every incoming packet must be buffered, to ensure that it is complete and error free, before it is sent on its way. This takes additional memory, processing power and of course time and therefore it is not applicable for isochronous traffic.

ATM takes the variable length packets and maps them into fixed length cells. These cells are then transmitted on the ATM network, and the original data in the packet is reassembled at the destination by concatenating the cell payloads (see Figure 10 - Mapping Packets/Cells).

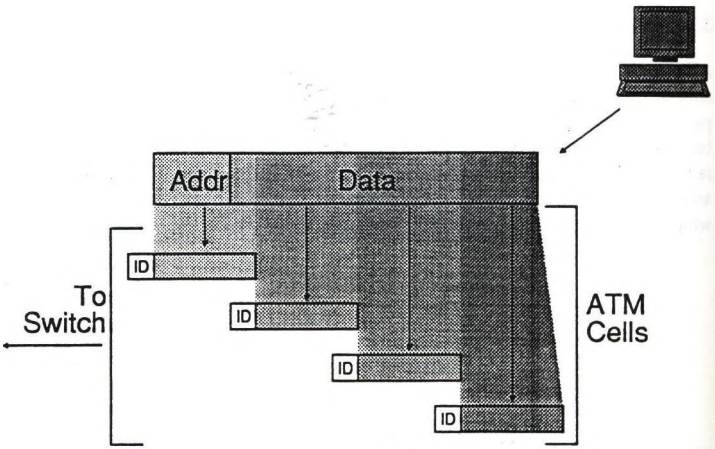


Figure 10: Mapping Packets/Cells

3.3. Connection Orientation

ATM accomplishes communications by setting up a virtual channel between the sender and receiver and then transmits the information via so called Virtual Channels - VCs (see Figure 11 - Virtual Channels). This allows network managers to gather end-to-end data on network traffic and charge users only for the actual time they have accessed the network. Virtual channels provide for multiple dynamic paths between sources and destinations, thus accommodating load balancing and bandwidth allocation. This approach also supports redundancy, so that traffic can be automatically rerouted if a link or switch fails.

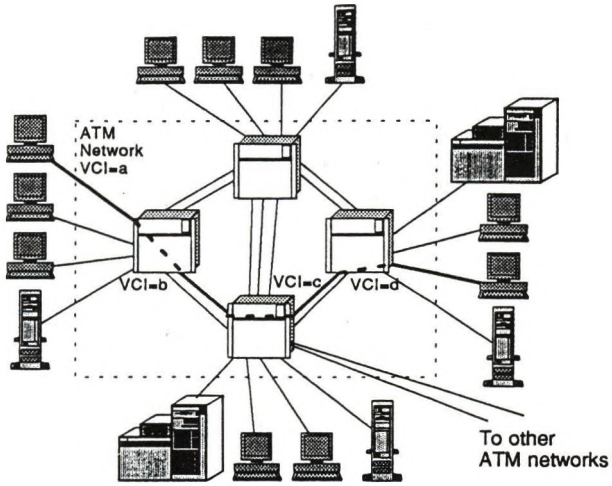


Figure 11: Virtual Channels

3.4. How ATM Works

As already discussed, ATM is based on the concept of fixed length cells, which are defined as 53 octets. The fixed length optimizes the movement of data throughout an enterprise. ATM is a transport protocol that operates roughly at the equivalent of the MAC sublayer of the data link layer, allowing it to operate above a variety of physical layer protocol such as SONET and FibreChannel.

ATM combines features of multiplexer and LAN backbones, making it able to support LAN, data, voice and video signals concurrently. ATM can provide dedicated data paths for real time signals and flexible, configurable bandwidth paths for non real time signals. This allows the amount of network traffic to dedicate bandwidth usage.

ATM has been identified as the universal transfer mode for all Broadband ISDN (B-ISDN) services. In the B-ISDN protocol stack, the ATM or common layer sits on the physical layer which is defined as SONET (though other physical layers will be defined in the future). As can be seen from Figure 12, the ATM common layer is where all cell formatting is done. All higher level services, such as Ethernet and Token Ring are mapped/converted to this common layer.

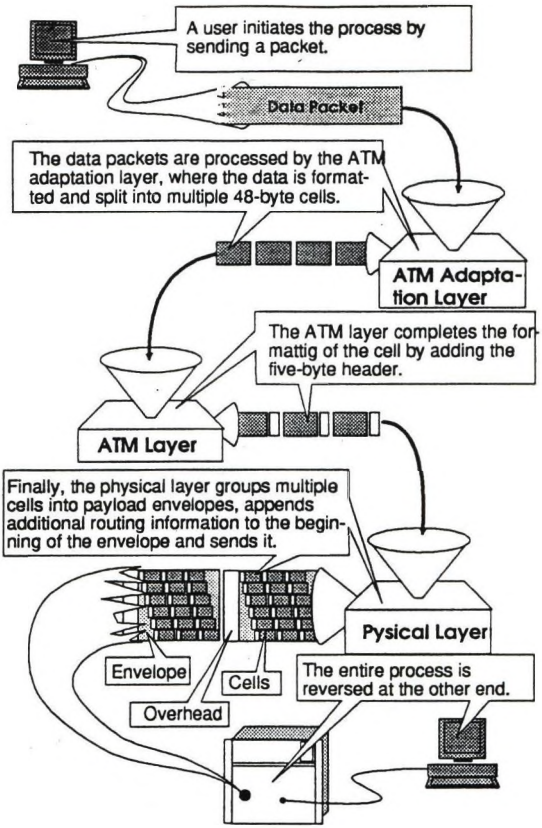


Figure 12: Data Moves Through an ATM Network

The ATM Adaption Layer (AAL) sits on the ATM common layer and performs two key functions. It prepares higher level data for ATM conversion, and then it takes that prepared data and segments it into fixed length ATM cells. Once ATM cells reach their destination, they are reassembled into higher level data and transmitted to the respective local devices.

The complete B-ISDN protocol reference model is depicted in Figure 13. The ATM and Physical Layer functions are present in any network element, while the AAL (ATM Adaptation Layer) contains the edge adaptation functions. A specific AAL protocol (AAL 1 to 4) is defined for each of four general services clases, AAL 5 is a high speed oriented protocol which can substitute AAL 3 and 4).

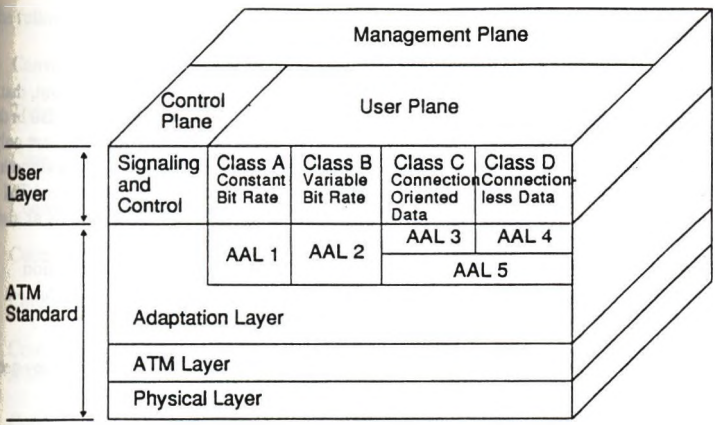


Figure 13: B-ISDN Protocol Reference Architecture

AAL 5 is the most important AAL today, since it is the one which is de facto implemented in all available products of the first generation. It exists already a draft RFC for AAL 5 (Figure 14 - Draft RFC Multiprotocol Interconnect over ATM Adaptation Layer 5), which shows how different types of protocols are mapped onto AAL5 or AAL 3/4 respectively.

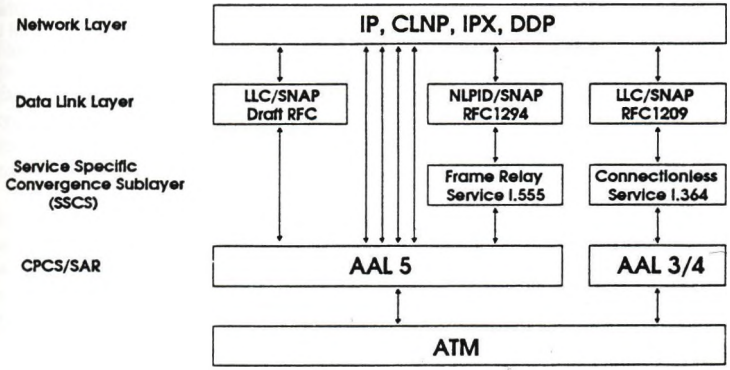


Figure 14: Draft RFC Multiprotocol Interconnect over ATM Adaptation Layer 5

4. The Optimal Migration Towards an ATM Based Enter Backbone

Talking about future ATM based Enterprise Networks we must take into account, that most users have already installed equipment, which they want and have to use also in the future ATM world (investment protection). Another fact is that ATM solutions are only helpful, if they support todays widly used services as E1, E3, FR and provide a smooth migration path for tomorrow by offering future standard services as for example ATM UNI or others.They must offer high scalability to higher speeds in both the LAN as also the WAN area and they have to provide mission critical operation by means of redundancy and fault tolerant features as dual power supplies, advanced congestion control mechanisms or load balancing on redundant links. In order to improve the utilization of links they have to provide efficient bandwith management.

Only ATM solutions which fulfill all these criteria will give users the flexibility they need. These criteria will be mandatory for success of ATM products on the market.

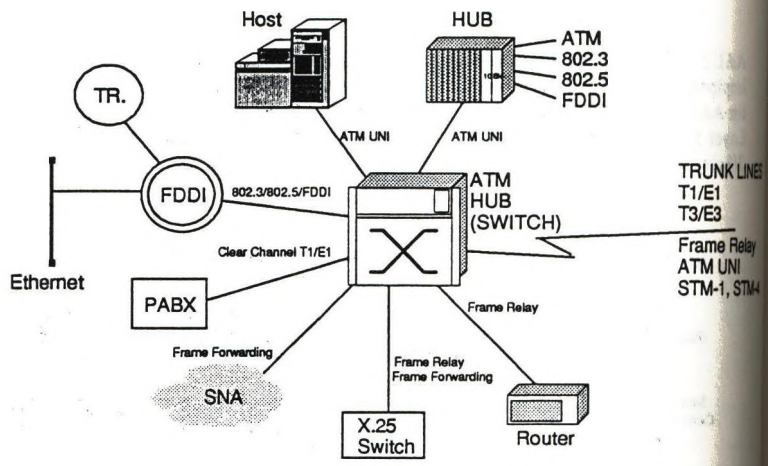


Figure 15: Typical First Step ATM Enterprise Network

To give an example of an optimal migration path into an ATM based Enterprise Backbone let us consider the needs for a first step ATM based Enterprise Network (see Figure 15 - Typical First Step ATM Enterprise Network). One or more ATM HUBs (switch based) will act as the Collapsed Backbone for a number of already existing network islands. These HUBs are a very powerful type of equipment, since they integrate most of todays stand alone functionality into one powerful box.

The following interfaces have to be supported:

- Conventional LAN Interfaces as Ethernet and Token Ring
- Todays de facto LAN Backbone Solution FDDI
- Connectivity of PABXs (via Clear Channel)
- Connectivity for IBM environment (via Frame Forwarding)
- Connectivity for X.25 networks (via Frame Relay or Frame Forwarding)
- Connectivity of routers (via standard LAN interfaces or Frame Relay)
- Connectivity of equipment, which uses already ATM as Hosts or ATM HUBs (via ATM UNI)
- Connectivity of high end desktop solutions

On the trunk side the following types of interfaces have to be available:

- T1, E1
- T3, E3
- Frame Relay
- ATM UNI
- STM-1, STM-4 (if available from the PTT)

Investment protection and smooth migration path means, that none of the existing equipment becomes obsolete, but can be connected to the new backbone by standard interfaces. For example an existing FDDI backbone can become now the backbone of a workgroup, while the ATM Backbone becomes the enterprise one. The Collapsed ATM Backbone can be easily extended to form a private ATM WAN (support of ATM NNI), as requirements increase and if a private solution is cheaper than using public services.

If it is possible to extend existing installations with equipment of the same manufacturer(s), of course the highest investment protection is guaranteed (easy reuse of hardware in other parts of the network, interworking with new ATM equipment without any problems, support of network management which is already known to maintenance people,...).

5. Conclusion

We see, that ATM which was originally developed for the public WAN area will have its first impact on our information system driven world in the LAN/Enterprise area. A whole bunch of equipment is coming to the market, which utilizes the benefits of ATM and opens ways for new types of applications, which need the special features ATM offers and allows complete new ways of doing business.

But we must not forget, that the wide acceptance of ATM depends on the possibility to smoothly start up with this service for reasonable costs, fitting into todays existing networking world and to extend its usage as necessary without throwing away existing equipment.

Once ATM has found wide acceptance in the local and enterprise arena, the need for ATM in WANs will grow automatically. Nobody who makes use of the advantages of modern applications, which became possible through the usage of ATM, will accept to miss these benefits while working via WANs. From that point of time ATM in the Enterprise Network is smoothing the way for B-ISDN. We can assume that ATM gets the necessary acceptance in the Enterprise Network within the next 5 years, in order to become a significant driving force for B-ISDN.

Telecommunications Management Networks (TMN): Introduction and Usage within Broadband Transmission Networks

Heinz Weiskirchner (Alcatel Austria, Vienna)

Abstract

Due to the fact that network management of telecommunication networks is rather complex even if broadband telecommunication is taken into account, the basic concepts of standardizations provided by ISO, CCITT and ETSI are presented in this paper. The global concepts of OSI management (ISO), Information Modelling (ISO and ETSI) and Telecommunications Management Networks (CCITT and ETSI) are introduced. Alcatel is using these standards to develop the Alcatel 1300 Network Management Product Line. A short description of the products used to manage broadband transmission devices is given and an example of a typical network management topology is mentioned.

Keywords

Network Management, Telecommunications Management Networks, OSI Management, Network Management Standardization, Broadband Transmission Management.

1. Introduction

Until comparatively recent times the management of telecommunications networks was approached on a rather ad hoc basis. Network management systems were designed specifically for each particular telecommunications equipment set and service. This resulted in a plethora of network management systems which were limited in their applicability, presented a number of interworking problems, and which limited the scope for increasing automation of network management functionality. With the growth of complexity in modern telecommunications networks and the drive to reduce operational costs by increased automation in a more systematic and integrated fashion, the need for a more structured and architectural approach is evident. A TMN concept provides a framework under which this approach to telecommunications management can be investigated. TMN was introduced and defined by CCITT and ETSI based on ISO/OSI general management concepts. This paper gives a global introduction in TMN and OSI management and will point out then the importance of using these concepts for managing broadband transmission networks.

- Chapter 2 gives an introduction in OSI management,
- Chapter 3 gives an introduction in TMN,
- In Chapter 4 the important points of TMN for broadband transmission networks are mentioned including a network management system example.
- Chapter 5 gives the list of used abbreviations.
- Chapter 6 gives the list of used references.

2. OSI Management

OSI network management groups the activities needed to control, coordinate and monitor the resources which enable communications to take place in the OSI environment. Three concepts are presented in this area of standardization [1] (see also **figure 1**):

- The different activity domains covered by network management, named *System Management Function Areas* (SMFA).
- The means of exchanging management data between the open systems over which the application is distributed, named *Systems Management.*
- The grouping of *managed objects* in an open system called *Management Information Base* (MIB).

2.1 System Management Functional Areas (SMFA)

Management activities can be grouped into five System Management Functional Areas:

- **Fault Management** enables the detection, isolation and correction of any abnormal operation of the network.
- **Configuration Management** enables, first, to initialize and start up the operation of interconnection services, and then to ensure the continuity of this operation and possibly to stop it. Some functionalities are autonomous but others are widely used by other functional areas such as fault and security management.
- **Accounting management** enables charges to be established for the use of managed objects and costs to be determined for the effective use of those managed objects.
- **Performance management** provides means to evaluate the behavior of managed objects and effectiveness of communication activities.
- **Security management** enables the setting of specific security mechanisms to provide confidentiality.

References to standards: [3], [4], [5], [6], [7]. [8]

2.2 Systems Management

These management activities are carried out through a set of management processes. Because the environment being managed is distributed, they are not necessarily located at one local system but possibly distributed over a number of systems. Management processes which are not co-resident need to communicate with one another in the OSI environment in order to exchange management information.

Systems management is the recommended way to achieve this communication since it is the only means by which OSI management of multiple layers is accomplished. It provides the ability to manage information relative to all seven OSI model layers of an open system. It allows a global control on resources used in the network, by a particular system, in the OSI environment. Systems management communications take place through application layer protocols, between Systems Management Application Entities (SMAE). (see **figure 1**)

Beside Systems management, there are two other means available for management processes when either the full functionality to exchange management information through the SMAEs does not exist on an open system, or when the exchange is inhibited by the use of upper layer functions. They are (see **figure 2**):

- *(N)-layer management* concerning the exchanges necessary for a particular layer management. These exchanges may enable the control of several data exchanges on several communication instances. (N)-layer management protocols convey management information between peer (N)-layer management entities (which are different types from those (N)-layer entities which operate (N)-protocols as defined in the OSI model) and should not duplicate the services available from higher layer protocols. NCMS (Network Connection Management Subprotocol) is an example of a protocol specialized in layer 4 management.
- *(N)-layer operation* concerning the set of functionalities contained in (N)-protocols pertaining to the control of a single instance of communication. No new management protocol specifications are needed to carry out these operations. X.25, for example, enables charging data to be exchanged between the entities which participate to the communication.

References to standards: [9], [10]

2.3 Management Information Base (MIB)

The management information is structured in *managed objects*. A managed object may be an abstraction of a communication resource, either logical or physical, that is subject to management such as a layer entity, a connection or an item of physical communications equipments. It represents the resource properties for the purposes of management, i.e. its attributes, and its behavior. It may also represent a relationship between resources or a combination of resources.

A managed object may moreover exist to support certain management functions such as event forwarding.

The Management Information Base (MIB) of an open system is constituted by the set of managed objects in that open system [1]. It may be accessed in two distinct ways:

- from a user interface or software supporting management processes locally in an open system
- from remote systems through systems management, N-layer management N-layer operation

Management applications are made of processes which are allowed to take one of the two possible roles, either an agent role or a manager role.

The **agent** manages the objects within its local system environment, i.e. is responsible for performing operations on the objects and issuing notifications to the manager.

The **manager** has the responsibility for one or more management activities, by issuing management operations to the agent and receiving notifications from it.

The agent may deny a manager's directive for several reasons, e.g. security or information model consistency. The agent may also filter the notifications before forwarding them. Thus, as seen on **figure 3**, the role of the agent is, on the one hand to respond to directives issued by a manager (support access control), and on the other hand, to reflect to the manager the behavior of the objects it manages (support notification dissemination).

Each MIB is managed by its agent in its local system environment and can be accessed by several process managers, (and possibly from distinct functional areas), through the operations issued to the agent process. One manager may also exchange information with several agents. An open system can support agent processes and/or manager processes. This grouping matches some organizational requirements.

References to standards: [11]

3. Telecommunications Management Network (TMN)

The Telecommunications Management Network (TMN) is defined by CCITT; it conceptually is a separate network from the Telecommunications Network (TN) it manages [2]. A telecommunication network consists of many types of telecommunication equipments such as switching systems or transmission systems, referred to as network elements (NEs) when managed. The two networks have interfaces at several points to exchange management information for the control of the TN exploitation. However, a TMN often uses different parts of the TN for its communication. (see **figure 4**)

A TMN provides management functions and offers communications both within itself and between itself and the TN. To achieve this, the TMN provides an organized architecture with standardized interfaces. Three aspects of this architecture can be considered when planning and designing a TMN:

- the functional architecture
- the information architecture
- the physical architecture

3.1 The TMN Functional Architecture

The functional architecture describes the distribution of functionality within the TMN. This functionality is represented by **Function Blocks (FB)** which are general basic functions used in various management activities. When function blocks exchange management information, they are separated by reference points. The various function blocks are listed below and it it is noteworthy that some of the function blocks are partly in and partly out of the TMN (see **figure 5**):

- **Operations System Function block (OSF)** supports the various telecommunication management functions such as fault management or accounting management.
- **Network Element Function block (NEF)** includes the telecommunication functions which are subject to management but which are not part of the TMN and a representation of these functions to the TMN which is part of the TMN
- **Work Station Function block (WSF)** provides a means to interpret TMN information for the user. It includes support for interfacing to a human user which is not part of the TMN.
- **Q Adaptor Function block (QAF)** allows those NEFs and OSFs which do not support standard TMN interfaces to be connected to the TMN, by translating between TMN and non-TMN interfaces. Typical QAFs are interface conversion functions.
- **Mediation Function block (MF)** adapts information from NEFs and sometimes QAFs to the requirements of OSFs. It includes information conversion, application level functions and higher layer protocol interworking.

Each Function Block consists of several functional components which further describe the function provided by the function block.

Reference points enable the identification of the information passing between function blocks. Five classes of TMN reference points are defined:

- q (divided in qx and q3) between TMN entities
- f between WSF and TMN internal function blocks
- x between separated TMNs
- g between WSF and users
- m between QAF and non-TMN managed entities

The **Data Communication Functions (DCF)** of the TMN provide mechanisms allowing to transport information between function blocks. They provide it for layer 1 to 3 of the OSI reference model.

3.2 The TMN Information Architecture

The information architecture describes the nature of the information that needs to be exchanged between the function blocks, and also describes the knowledge that each block must have about the information held in other blocks.

This architecture is based on the object oriented approach of the management information described in chapter 2. It also takes into account the Manager/Agent concepts (see **figure 6**). Thus, in order to be able to communicate, systems must share a common view of a set of information and mainly containing:

- Supported protocol capabilities
- Supported management functions (e.g. state management)
- Supported managed object classes
- Available managed object instances and the containment relationship between them
- Authorized management capabilities

The Logical Layered Architecture (LLA) is based on a partition into a series of layers. The LLA implies the clustering of management components in layers that will be themselves separated by reference points. All the points of connection within the LLA implicitly have a Manager/Agent relationship associated with them according to the control authority. The scope of each layer is broader than the layer below it, the upper layer directs the lower. It is expected that upper layers will be more generic and lower layers more specific. The LLA uses a recursive approach to decompose a particular management activity into functions which are placed in a series of nested domains. Each domain forms a management domain under the control of the OSF. The scope of the top level domain is the TMN. It provides a partition of management components based on abstraction level (e.g. "service" as opposed to "supporting resources"). **Figure 7** gives an example architecture consistent with the LLA: the TMN OS functional hierarchy.

3.3 The TMN Physical Architecture

The physical architecture describes physical entities and interfaces within a TMN. TMN functions can be implemented in a variety of physical configurations. Each TMN building block, listed below, contains one characteristic and mandatory function blocks according to which it is named but it may also contain other optional function blocks (see **figure 8**):

- **Operation System (OS)** is a system performing OSFs and optionally WSFs.

- **Mediation Device (MD)** is a device performing MFs and optionally QAFs and WSFs. It converts for example, the less-complex Qx interface to Q3,
- **Q Adaptor (QA)** is a device performing QAFs. It connects NEs or OSs with non TMN compatible interfaces to Qx or Q3 interfaces.
- **Data Communication Network (DCN)** is a communication network within a TMN supporting the DCF. It is not necessarily physically apart from the network it supervises, the TN.
- **Network Element (NE)** is a TN component performing NEFs and optionally any of the other TMN functionalities, i.e. MFs, QAFs, OSFs and WSFs.
- **Work Station (WS)** is a system performing WSFs. When other TMN functionalities are present in the equipment with WSF, the block is named by a name related to one of the other functionalities.

Standard interfaces are defined as the physical implementation of the reference points. Thus, there are: Qx and Q3 to connect TMN entities, X to interconnect several TMNs, F to connect work stations. They allow external physical connections between building blocks. Each block supports several interfaces according to the various function blocks it contains. **Figure 8** presents a simplified physical architecture example considering that the building blocks only contain their mandatory functions.

As seen in **figure 9** the Q3 and the Qx interface can be represented by several **protocol suits**. **Figure 9** shows three examples of the OSI protocol stacks representing protocol suits.

4. TMN for Broadband Transmission Networks

Telecommunications operators are faced with increasingly complex tasks of managing their network. Many types of equipment have to be operated and maintained to guarantee performance and quality of the service for public telephony, high speed data transmission, intelligent network services, mobile communications and message switching.

In parallel there is an increasing need for improved facilities to manage the large number of advanced services now being demanded by users and service providers. The major obstacle to efficient overall network management has been that in the past management systems were developed to meet the needs of particular networks or parts of such networks. Consequently, until now systems capable of handling overall network management simply did not exist.

Today, however, new telecommunications management methods are being introduced which are capable of administering networks and services on a global rather than an individual basis. Alcatel has for some years been working closely with CCITT and ISO in the field of network management, particularly on defining the concept known as the TMN, and is now implementing it.

Telecommunications networks consist of a number of nodes which are already processor-controlled and interconnected by more and more powerful data communication facilities: SS7,

X.25, SDH, ATM, which realize the full potential of digital switching and transmission. These elements are the foundations for implementing sophisticated dynamic network management systems that conform to TMN principles.

For operators, the top priorities are:

- Overall control of existing network elements.
- Flexible and comprehensive management of external changes throughout the life cycle of the network.
- Adaptability to their organization.
- Provision of standard compliant network management functions (fault, performance, configuration, security and accounting management).
- Cost effective migration from installed management applications.
- Provision of an open interface to external network management systems.

In the further chapters the Alcatel 1300 management products will be presented and examples of their usage for broadband transmission network elements are give.

4.1 Alcatel 1300: A network management product line for today and tomorrow

Recognizing the market needs, Alcatel has developed the Alcatel 1300 series of network management products, integrating the latest standard recommendations, capable of managing all equipments and services of Alcatel or third party origin in an efficient and cost-effective way.

The broadband transmission devices are picked out to explain the network management products and their global functions.

The **Alcatel 1300 architecture** (see **figure 10**) is based on the CCITT TMN model. It respects the M.3010 recommendation and the OS hierarchy: Element Management Layer, Network Management Layer and Service Management Layer. It is designed to various environment evolution e.g. integration of new NEs and new applications. It defines all functionalities supported by the NEs, all information exchanges between network management objects as well as the appropriate means of communication and associated management protocols (Q3, SNMP and others).

Short description of the Alcatel 1300 network management products for broadband transmission devices, as there are SDH, PDH and ACCESS multiplexers, cross-connects and line termination equipment:

- **OS 1353NX/1354NX**: Network manager to provide configuration management, fault management, performance management and security management. Communication between management center and remote equipment is ensured via a DCN based either on Alcatel equipment built in digital service channels, or X.25 or Ethernet networks.
- **ME 1322NX/1323NX**: Mediation equipment to provide monitoring of status and alarm information, remote control of relays for station environment, alarm cut-

off or automatic protection switching, data buffering and conversion of data from Qx to Q3 protocol.

- **WS ECT 1320NX/OCT 1321NX**: Work station to provide windows driven, full graphic and colored HMI to monitor and act on several network management applications.

4.2 Example how to use Alcatel 1300 to manage a broadband transmission network

Figure 11 shows the network management system for a typical broadband transmission system.

5. Abbreviations

CCITT	Committee Consultative International Telephone and Telegraph
DCF	Data Communication Functions
DCN	Data Communication Network
ECT	Equipment Craft Terminal
ETSI	European Telecommunication Standard Institute
FB	Function Block
HMI	Human Machine Interface
ISO	International Organization for Standardization
LLA	Logical Layered Architecture
MF	Mediation Function
MIB	Management Information Base
NE	Network Element
NEF	Network Element Function
NCMS	Network Connection Management Subprotocol
OCT	Office Craft Terminal
OS	Operation System
OSF	Operations System Function block
OSI	Open Systems Interconnection
PDH	Plesiochronous Digital Hierarchy
QA	Q Adaptor
QAF	Q Adaptor Function
SDH	Synchronous Digital Hierarchy
SMAE	Systems Management Application Entities
SMFA	Systems Management Function Areas
SNMP	Simple Network Management Protocol
TMN	Telecommunications Management Network
TN	Telecommunications Network
WS	Work Station
WSF	Work Station Function

6. References

[1] ISO/IEC and CCITT. Information Technology - Open System Interconnection - Systems management overview. Draft International Standard DIS 10040 - Recommendation X.701, ISO/IEC and CCITT, Secretariat: American National Standard Institute, 1430 Broadway Street New York, 1990

[2] CCITT. Principles for a TMN. Draft Recommendation M.3010 - Version R4, CCITT, August 1991.

[3] ISO/IEC and CCITT. Information Technology - Open System Interconnection - Systems management - part 5: Event Report Management Function. DIS 10164-5 - Recommendation X.734, ISO/IEC and CCITT, Secretariat: American National Standard Institute, 1430 Broadway Street New York, 1990

[4] ISO/IEC and CCITT. Information Technology - Open System Interconnection - Systems management - part 6: Log Control Function. DIS 10164-6 - Recommendation X.735, ISO/IEC and CCITT, Secretariat: American National Standard Institute, 1430 Broadway Street New York, 1990

[5] ISO/IEC and CCITT. Information Technology - Open System Interconnection - Systems management - part 4: Alarm Reporting Function. DIS 10164-4 - Recommendation X.733, ISO/IEC and CCITT, Secretariat: American National Standard Institute, 1430 Broadway Street New York, 1990

[6] ISO/IEC and CCITT. Information Technology - Open System Interconnection - Systems management - part 1: Object Management Function. DIS 10164-1 - Recommendation X.730, ISO/IEC and CCITT, Secretariat: American National Standard Institute, 1430 Broadway Street New York, 1990

[7] ISO/IEC and CCITT. Information Technology - Open System Interconnection - Systems management - part 3: Attributes for Representing Relationships. DIS 10164-3 - Recommendation X.731, ISO/IEC and CCITT, Secretariat: American National Standard Institute, 1430 Broadway Street New York, 1990

[8] ISO/IEC and CCITT. Information Technology - Open System Interconnection - Systems management - part 2: State Management Function. DIS 10164-2 - Recommendation X.731, ISO/IEC and CCITT, Secretariat: American National Standard Institute, 1430 Broadway Street New York, 1990

[9] ISO/IEC. Information Processing Systems - Open System Interconnection - Basic Reference Model - part 4: Management framework. IS 7498-4, ISO/IEC, Secretariat: American National Standard Institute, 1430 Broadway Street New York, 1990

[10] ISO/IEC. Information Processing Systems - Open System Interconnection - Basic Reference Model - part 1: The Basic Model. IS 7498-1, ISO/IEC, Secretariat: American National Standard Institute, 1430 Broadway Street New York, 1990

[11] ISO/IEC and CCITT. Information Technology - Open System Interconnection - Structure of Management Information - part 1: Management Information Model. DIS

10165-1 - Recommendation X.720, ISO/IEC and CCITT, Secretariat: American National Standard Institute, 1430 Broadway Street New York, 1990

A. Appendix

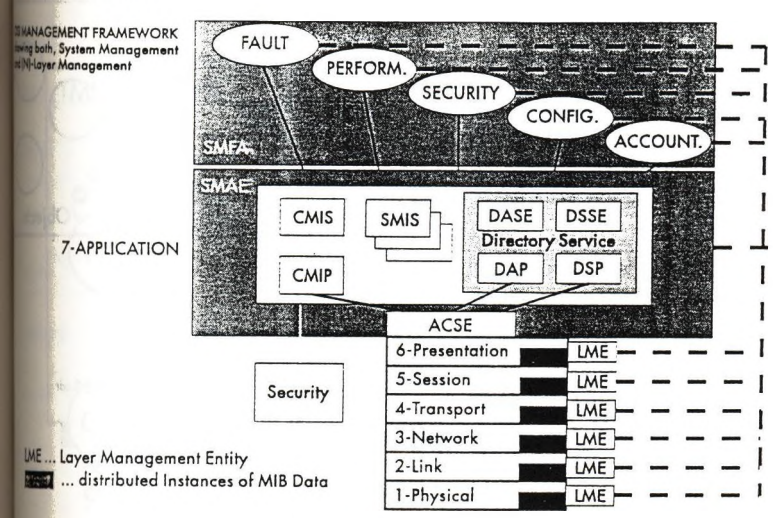


figure 1: OSI Management

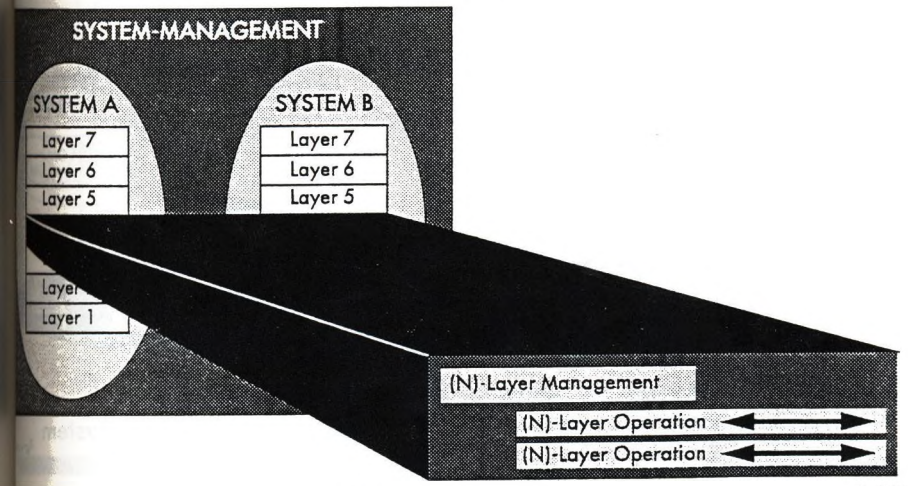


figure 2: System Management

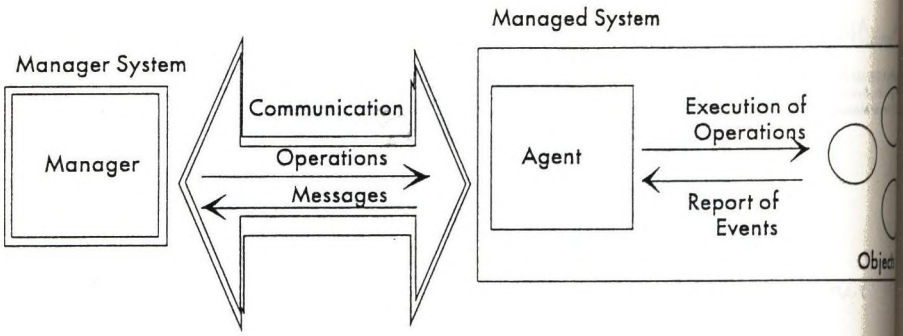


fig-3.cdr

figure 3: Manager <--> Agent Concept

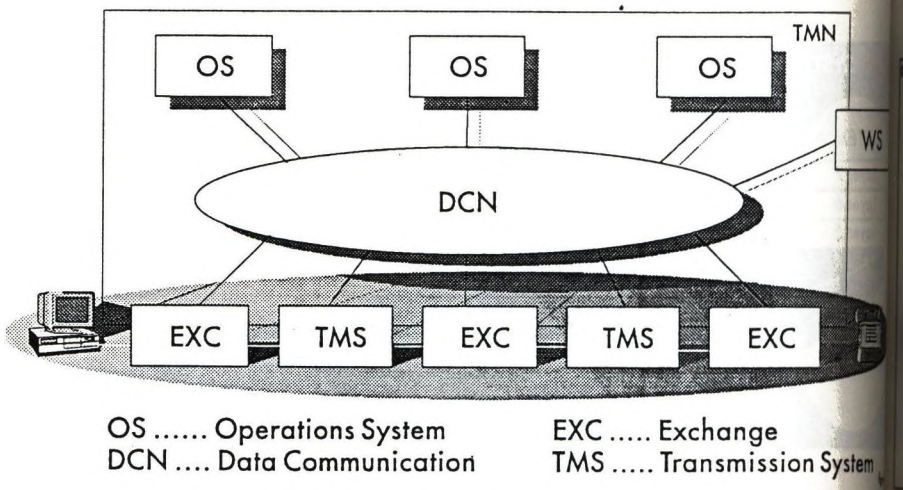


figure 4: TMN Basic Reference Model

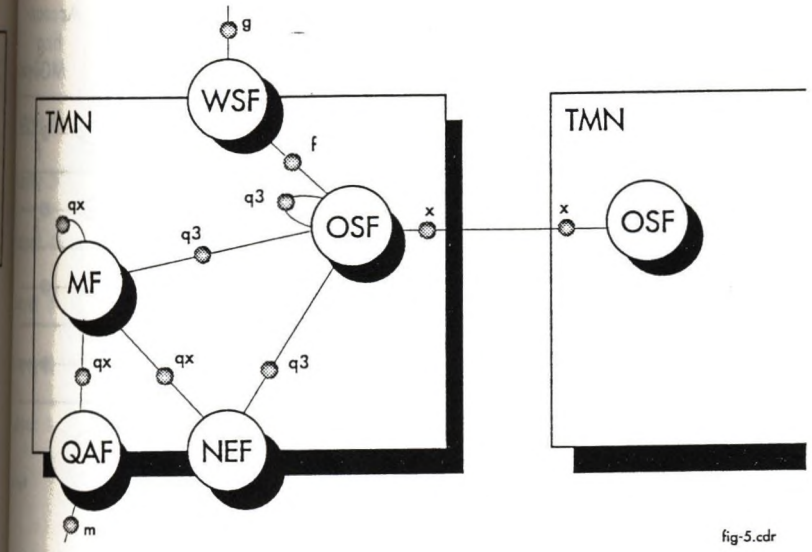


figure 5: TMN Functional Architecture

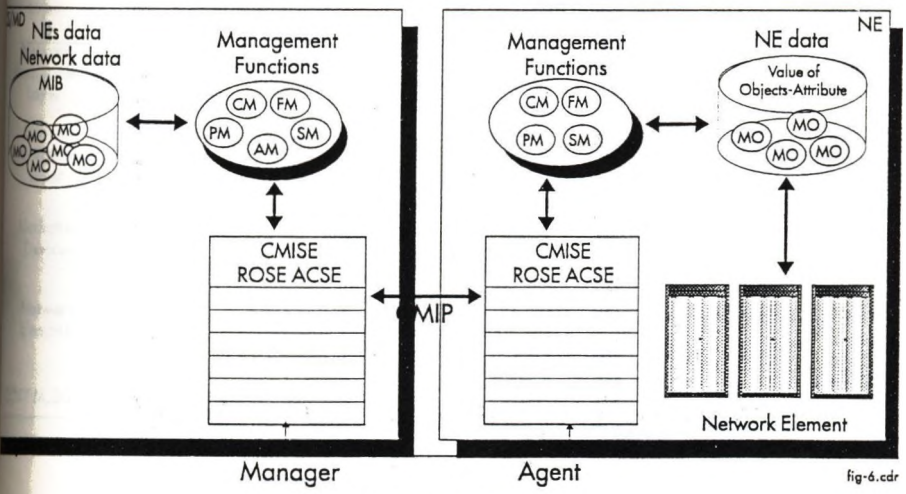


figure 6: TMN Information Architecture

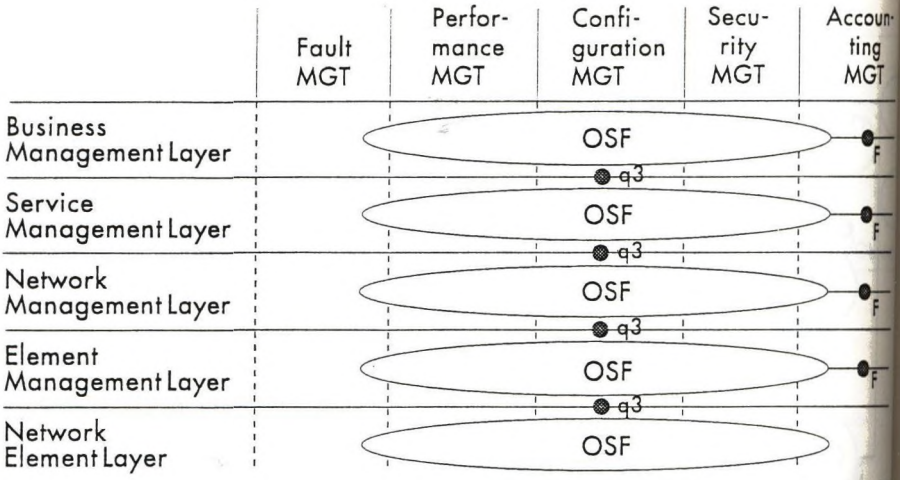


figure 7: TMN Logical Layered Architecture

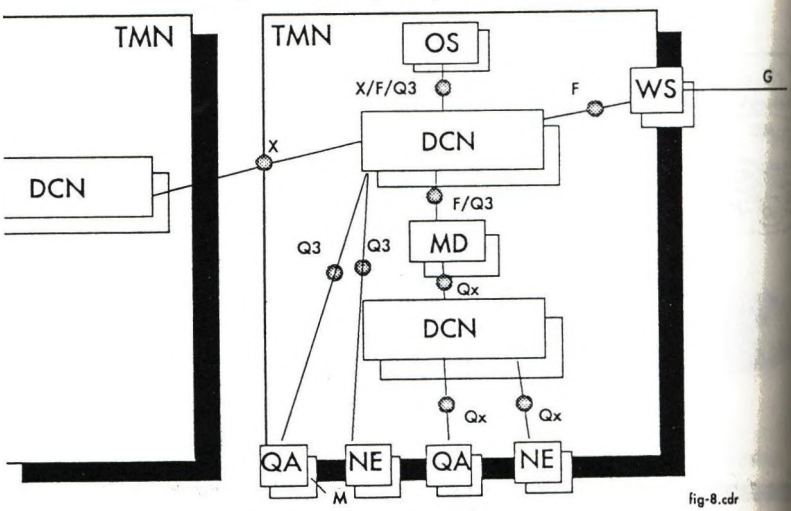


figure 8: TMN Physical Architecture

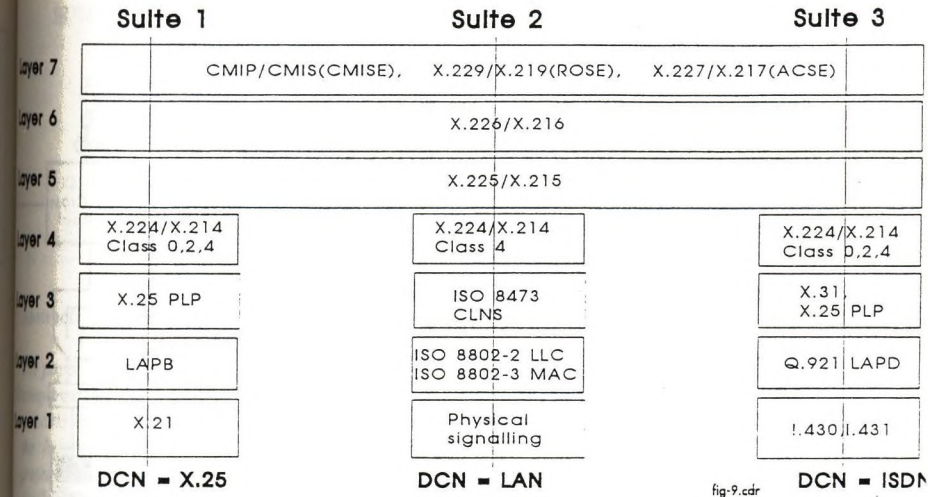


figure 9: Q Protocol Suits

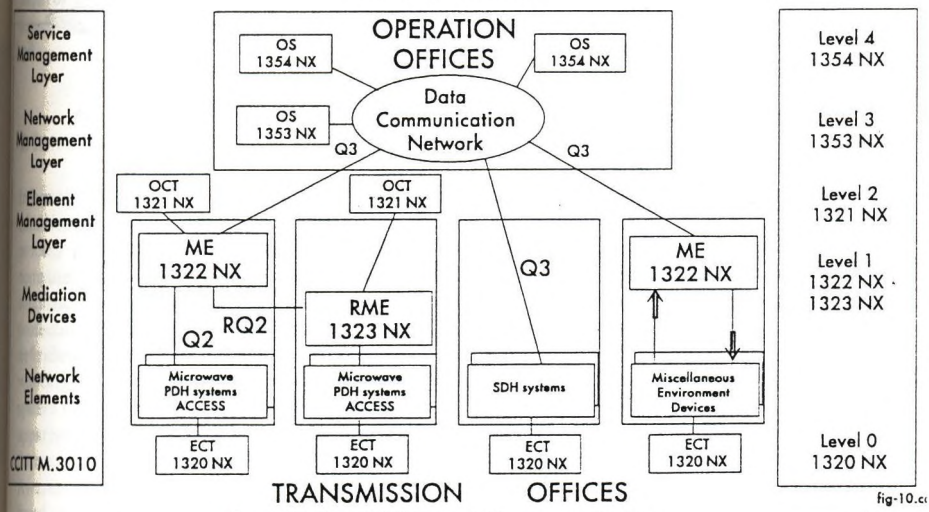


figure 10: Alcatel 1300 Network Management Products

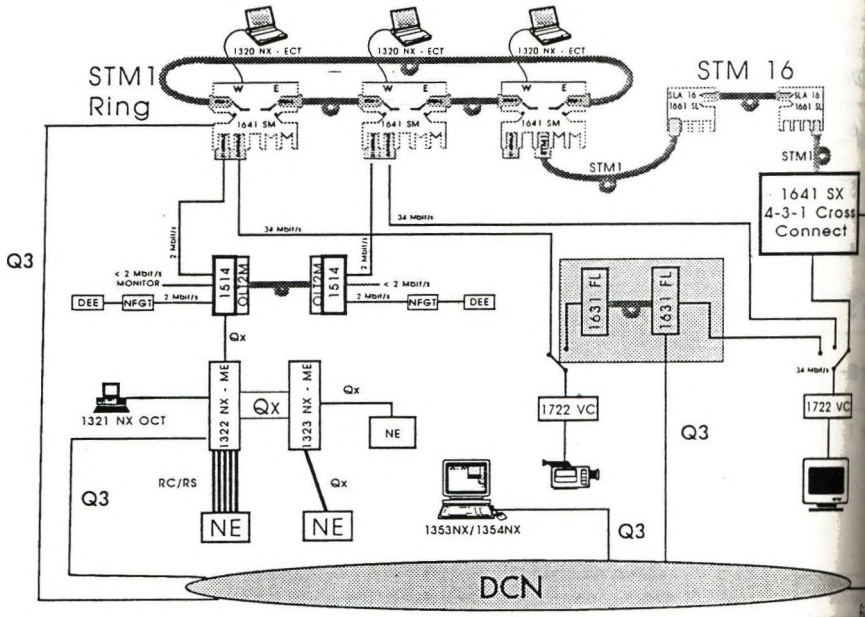


figure 11: Network Management System for Broadband Transmission Network

SURVEY OF THE COMPUTER AND NETWORK SECURITY ISSUES FROM EVALUATION CRITERIA TO OPEN SYSTEM

György PAPP

Prime Ministers Office,
Co-ordination Office of Governmental Information Systems

Abstract:

The paper is dealing with the challenges of the security issues in the open system environment. It compares the different security evaluation methods of computer and information technology. It presents the main elements of the DoD Trusted Computer System Evaluation Criteria (TCSEC) and the Information Technology Security Evaluation Criteria (ITSEC) and its Manual (ITSEM) prepared by EC DG XIII. There are important questions: Why do we need security and what is the challenge of the open system environment on the security scope? The article shows some real security solutions in X.25, X.400 and Kerberos methods. Finally it would like to present the key steps of the European Information Security Program within the Information Systems Services Infrastructure that is being developed.

1. Introduction

Information is the lifeblood of business and of central and public administration. Businesses and the administrations are increasingly dependent on the use of Information Technology (IT) systems to process information. As we can find in some publications the concentration of information in computer systems is similar to the concentration of cash in vault. It has mandated an increased sophistication of the controls which protect that information. Generally, security means a set of protecting measures against something, namely, danger and threats. To achieve security means defending a system against threats. To achieve information security in the information systems means working out such sets of protecting and preventing measures which if used the functionality of the system can be insured, the laws and regulations concerning data processing can be enforced, and the apparent and real effects of dangers and threats on the processed data and information can be decreased. Technological advances have made information more available and more vulnerable. Awareness of information control weakness has brought to light issues of personal privacy, computer fraud and legislation, and national security-related concerns.

In the information technology the most important objects are the computers and networks that are under attack from both inside and outside the enterprises and services. In an open network computing environment, a workstation cannot be trusted to identify its users correctly to networks' services. At the same time all enterprises world-wide, independently large or small, public or private, have become dependent on the efficient and reliable operation of computer and telecommunication.

One of the preventing measures is the security evaluation. Information professionals must clearly understand the concepts of security classification and evaluation for computer systems because management will need to be advised on matters of security in information systems. Security managers might have legal responsibilities and are thus dependent on assertions or claims made by manufacturers and vendors of both hardware and software.

2. Trusted Computer System Evaluation Criteria (TCSEC)

The primary standard against which the National Computer Security Centre (NCSC) in the US government measures the security capability of commercially produced and supported computer products is the Department of Defense (DoD) Trusted Computer System Evaluation Criteria (DoD 5200.28-STD, December 1985), also known as the "Orange Book". TCSEC is one of the NCSC security publications known familiarly as the "Rainbow Series". This book defines the basic requirements needed to build security control levels (security features and security assurances) that can be classified into one of NCSC's definitions of trust; provides a metric for evaluating the degree of trust that can be placed in a product for processing sensitive information; offers a basis for specifying the security requirements in acquisition specifications.

2.1 TCSEC requirements

Security policy
must be explicit and well-defined
Marking
all objects in the system must have control labels associated with them
Identification
the individual subjects have to be identified
Accountability
audit information is selectively kept and protected
Assurance
system contains hardware and software mechanisms that can be independently evaluated
Continuous protection
Trusted systems must be continuously protected.

2.2 TCSEC divisions and their classes

Division D - Minimal Protection

Evaluated systems that fail to place to higher divisions.
No classes.

Division C - Discretionary Protection

Providing for discretionary protection and accountability of subjects and their actions through audit capabilities

Class C1 - Discretionary Security Protection

Separation of users and data with enforcement of access limitations on an individual basis

Class C2 - Controlled Access Protection

Enforce a more stringent form of discretionary access control, capable of making users individually accountable for their actions through login procedures so that access permission can be assigned only by authorised users.

Division B - Mandatory Protection

Preserving the integrity of sensitivity labels for objects through the provision and specification to the system of a security policy model and using them to enforce a set of mandatory access control rules, by means of "reference monitor concepts" (an abstract machine that mediates all accesses by subjects to objects).

Class B1 - Labelled Security Protection

More than C2 with the addition of an informal statement of security policy model, mandatory labelling of all data and enforcement of access control over named subjects and objects. The exported data can be labelled.

Class B2 - Structured Protection

More than B1 with the following: The Trusted Computing Base (TCB), the combination of hardware, software and firmware that provides the protection mechanisms that enforce the security policy, is created around a clearly defined and documented formal security model. This model extends the discretionary and mandatory access control in class B1 to all objects in the system. In addition the problem of covert channels, means of communication between processes that may violate the security policy, must be addressed. Essentially the system is seen being relatively resistant to penetration.

Class B3 - Security Domains

The TCB must mediate all access of subjects to objects and has to itself proof of touching or making changes without permission and small enough for careful test and analysis. Essentially the system is highly resistant to penetration.

Division A - Verified Protection

Using of formal security verification methods to ensure that discretionary and mandatory security controls function properly. The trusted computing base (TCB) must meet these

security requirements in all aspects of its design, development and implementation with supporting, extensive documentation of that.

Class A1 - Verified Design

These systems are functionally the same as those in Class B3 but at this time the evaluation and verification of features are rigorously executed through analysis of the formal design specification and its formal verification. Testing demonstrates that the TCB implementation is consistent with the formal top-level specification.

3. Information Technology Security Evaluation Criteria (ITSEC)

The four leading European nations in the field of information security standards - the United Kingdom, Germany, France, and the Netherlands - decided to bring together the work combining the best features from each of the various national initiatives. While the TCSEC may be well known in Europe, they are not officially recognised as a standard outside the United States. They accepted the defence-oriented standards unsuitable in many respects for the needs of commercial organisations. A new set of harmonised Information Technology Security Evaluation Criteria (ITSEC) was constructed, with the aim of careful consideration being afforded to compatibility with existing criteria. They agreed with six objectives:

- an agreed set of terminology would be published
- the criteria produced would be applicable to all sectors - commercial, governmental, and defence
- both products and systems would be covered
- the criteria would be covered by all classes of security policy
- confidentiality, integrity, and availability would all be encompassed
- there would be the maximum possible applicability and compatibility with existing criteria, in particular the TCSEC.

Within these objectives, especial consideration is given to ensuring that the criteria be flexible, with differentiation between functionality and assurance. The ITSEC shall be used as a guideline for evaluation of the security of IT. Security in the ITSEC context means confidentiality, integrity, and availability. It is supposed that some threats to security can already be excluded by non IT measures like physical access control. Remaining threats are countered by IT measures that are the subjects of evaluation.

The ITSEC differentiates between systems and products. Each system or product has its own unique requirements that will be met by *security functions* operating in such scopes as auditing and access control, in which the users must have confidence. For systems there is a combination of hardware-, software-, and firmware tailored to the needs of a specific operational environment. For products there is a set of standards in hardware, software and firmware that can be incorporated into systems. The main difference regarding security is that the security of the products in the operational environment of systems is less known. But both, the TCSEC and ITSEC, have common property

referred to as "targets of evaluation" (TOEs). In the security target, functionality is considered at three levels:

- Security objectives (why?)
- Security functions (what?)
- Security mechanisms (how?)

3.1 ITSEC functionality classes

F-C1 discretionary access control like for TCSEC C1
F-C2 finely grained discretionary access control like for TCSEC C2
F-B1 mandatory access controls like for TCSEC B1
F-B2 extension mandatory access controls like for TCSEC B2
F-B3 distinct security administration roles and expanded audit like TCSEC B3 and A1
F-IN higher integrity requirements for data and programs (e.g. database systems)
F-AV high requirements for availability of a complete "target-of-evaluation" or special function of it (e.g. manufacturing control process)
F-DI high requirements for safeguards on data integrity during data exchange
F-DX networks with high demands for confidentiality and integrity of exchanged information (e.g. exchange of secure data via insecure or public telecommunications services)

3.2 ITSEC assurance

E0 inadequate assurance
E1 security "target" exists and an informal description of its architectural design also exists. Functional testing determines that a submitted product or system (TOE) meets its security target.
E2 in addition E1, an informal description of the detailed design. Configuration control system and approved distribution procedures exist.
E3 in addition E2, evaluation of system software source code and hardware schematic drawings, and so on that correspond to security mechanisms
E4 in addition E3, an underlying formal model of security policy with security enforcement functions, architectural design and detailed design expressed in semiformal style
E5 in addition E4, close correspondence between detailed design and source code and/or hardware schemes
E6 in addition E5, security enforcement functions and architectural design expressed in formal style

3.3 Criticism of ITSEC

Number of different opinions and questions have arisen about the ITSEC. Many comments criticised the definitions offered by ITSEC as being too restrictive or inconsistent with other sources. Some reviewers were unhappy with the scope of the criteria, feeling that insufficient consideration is given to such areas as accountability, non-repudiation, integrity, and trustworthiness. Vulnerabilities that are not covered by the criteria could be detected and systematically exploited by an attacker. This would be especially severe after the evaluation closed criteria gave rise to a security monoculture. A few reviewers said that the aspects of confidentiality, integrity, and availability did not really cover the security features, therefore, ITSEC was unsuitable for Open Systems. Cost of evaluation is a major concern to vendors because, according to an estimate, the evaluation could represent as much as 20 to 25 percent of the total costs over the development life cycle. This must be reduced. Most of commentators suggested that a more holistic approach to systems security was required. It was advanced that the systems should be evaluated in their entirety, with people and procedural aspects being considered alongside the hardware, software, and firmware.

4. ITSEM

The Information Technology Security Evaluation Manual (ITSEM) provides a manual of techniques needed for the evaluation of target-of-evaluation (TOE) as set out in the ITSEC. Besides, the document sets out techniques in mutual recognition between parties and in certificates of compliance with security parameters worked out in ITSEC. In this regard the mutual recognition of results the ITSEM defines the measures required to meet the objectives of *reproducibility*, *repeatability* and *objectivity* in evaluation of the information products and systems as well as defining requirements to "fully conform from the objective of *impartiality*" till the description of organisational rules and procedures for the performance of evaluations. The main aim is to give a method to the evaluators who wish to do evaluations of the security of information products and systems, but in a more important sense, the ITSEM becomes a document to be considered by all those involved in evaluations. This includes from organisations, such as users and manufacturers of computer systems concerned with particular systems, to Governmental or standards bodies responsible for the *accreditation* of evaluation laboratories and ultimately "national certification bodies".

5. Harmonising the criterias, international criteria

A harmonising program started for the security criteria of information technology among the expert bodies of USA, Canada and the European Community in order to work out an international recommendation. The aim of this project is to harmonise the criterias and help countries which do not have a criterion system or computer manufacturing industry but do have information industries and information processing systems.

6. Open System Security

By definition, an open system is one that encourages communications between different applications or users. Unfortunately, an open system can also encourage illegal eavesdropping and information theft or destruction. Recently, notorious examples of white-collar crime, corporate espionage, and network intrusions by computer worms and viruses have alarmed information processing professionals and raised a general awareness of computer security issues. The concepts of information security and open systems are antithetical; nevertheless, the ISO has taken steps to provide a secure environment within the OSI Reference Model.

International Standard 7498, Part 2 addresses a security architecture within the general OSI model. It describes security measures that can be provided by specific layers in the model. Specific security standards are not yet defined, however, but are under study by working group JTC1, Subcommittee 27 for Information Technology Security Standards, plus other subcommittees. The U.S. participant in this process is ANSI's X3 Committee.

This standard set out security services, specific as well as pervasive security mechanisms and defined the requirements of services and mechanisms at all of the seven layers. The security services are authentication, access control, data confidentiality, data integrity and non-repudiation. The specific security mechanisms are in encipherment, digital signature, access control, data integrity, authentication, traffic padding, routing control, and notarisation. In the widespread security mechanisms, it is separated trusted functionality, security labels, event detection, security audit trail, and security recovery.

As mentioned earlier, some reviewer of ITSEC said that this criterion was unsuitable for Open System. In spite of the several existing secure solutions in OSI, security is unlike other information technology disciplines yet is being developed as though the conditions for security are the same, purely technical issues. For other disciplines in information technology, there seems to be no devious adversary anticipated save the usual complexity and logical problems in information technology. In security, however, we must add the challenge of active, unpredictable human adversaries accidentally or intentionally causing failures and losses in systems for their own or for others' advantage (accidental offences inadvertently do this as well). Adversaries have total freedom to do as they wish in attempting to achieve their often-changing goals. Technologists and systems managers who are inexperienced in loss events and untrained in security must nonetheless protect assets, including new assets, created by users and fixed in time, place, and form, and often have little correct intelligence information about adversaries' plans or actions or about users' needs for protection. That is way some experts say that the foundation of information security has to be restated: The definition of three attributes of information security, namely confidentiality, integrity, and availability must be extended by authenticity (genuineness, conforming to fact or correct) and functionality (usability for a purpose), and the loss types must totally be replaced by the inverse of the purposes, e.g. loss of integrity. Computer systems must then have all five attributes at an acceptable, evaluated level to be secure in any combination of attributes or any single attribute. This would avoid the current attempts to extend the common meaning of integrity to include accuracy and correctness.

6.1 Security in X.25

The first step was protecting the communication in open system interconnection after recognising that ever-growing numbers of organisations are transmitting sensitive information over wide areas using both public and private X.25 networks. Unfortunately, the push to provide better communications services have left many security issues unresolved. Everybody agrees with that the simple X.25 packet-switching networks are not tamper-proof, they are weak in security; these networks can significantly increase the risk of exposure of confidential information. At that time, it was ironically, the computer technologies used to create the advanced communication that is also used to attack network security. Information travelled across an X.25 network is threatened in two ways: data held in mainframes connected with a network can be illegally accessed from network side, and information within the network itself can be observed and possibly altered while in transit between legal sites. To achieve the secure communication in X.25, several real solutions appear placing addition product in order to the following suggestions: network access control, access to security equipment, encryption-decryption, management aids. A number of products can be found in the computer market that guarantee the secure communication in X.25 and using them can be combined with the protecting features of OSI data-link and network layers.

6.2 Security in X.400

One of the real good solution at the application layer of OSI is the X.400 electronic message handling system. Wherever information is transmitted the communication partners expect the information transmitted to arrive unaltered. Security features are important prerequisites for a message handling system that is intended to transmit contracts, documents or even electronic bank transfer orders. Such security features include guaranteed integrity of transmitted messages, verification of originator, verification of submission and receipt and also confidentiality of transmitted messages and protection against loss or duplication of messages. Even the transmission of simple notes or a greeting requires some minimal security; a simple note that is diverted during transmission by a hacker to another destination may lead to confusion. In short, a totally insecure message handling system is only of limited use.

"Trusted" data resources must be securely transmitted and protected from possible threats. Message handling systems (MHSs), such as E-Mail and Consultative Committee on International Telegraph and Telephone (CCITT) X.400 networks, require special protection because of sensitive data traffic consisting of contracts, legal documents, personal messages, and even electronic funds transfers (EFTs). Managers must understand the possible threats against an MHS, be proficient in fundamental cryptographic principles and public keys, and apply security elements available in the X.400 standard.

6.3 Kerberos

In the Open Systems the main problem in the security is the identification of the users. In an open computing environment, a workstation can not be trusted to identify its users correctly to network services. Kerberos, an authentication system designed by Miller and C. Neumann, provides a possible approach by a third-party authentication is used to verify user's identities. So, Kerberos is a trusted third-party authentication service for client-server-user architecture. In the model, there is an independent trusted third judgement to identify each clients and users and these believe the trusted judgement. It is trusted in the sense that every client believes the judgement as to the identity of its other clients to be accurate. Timestamps (large numbers representing the current date and time) have been added to the original model helping in the detection of replay. Replay occurs when a message is stolen off the network and resent later. Kerberos keeps a database of its clients and their private keys. There are three phases in the authentication process. In the first phase, the user obtains credentials to be used to request access to other services. In the second phase, the user requests authentication for a specific service. In the final phase, the user presents those credentials to the end server. There are two types of credentials used in the Kerberos authentication model: tickets and authenticators. Both are based on private key encryption, but they are encrypted using different keys. A ticket is used to securely pass the identity of the person to whom the ticket was issued between the authentication server and the end server. A ticket also passes information that can be used to make sure that the person using the ticket is the same person to which it was issued. The authenticator contains the additional information that, when compared to that in the ticket proves that the client presenting the ticket is the same one to which the ticket was issued.

7. European Information Security Program

Within the European Communities Programmes a Security Investigations Programme has been started in 1992 that supports the implementation of some action lines on information security areas. The aim of this programme is to offer a secure European Electronic Information Environment in the future European Information Systems Services Infrastructure. The management of information and its use supported by Information Technology and Information Services in every sphere of economic, social and political life is all pervasive. It has permitted the integration of activities via a global communication system, connecting manufacturing plants, research establishments, data bases, computer centres, service providers as well as centres of political and economic decision-taking. The EC initiative on the security of information systems is one Europe wide action plan that is addressing the problem. It includes an overall consultative process and specific funded programme with individual tasks. The security investigations are some 14 strategic studies embracing a wide range of security concerns from public awareness through to the impact of specific security technology. The action plan in the field of the security helps to work out the provision of open systems security.

8. Summary and conclusions

The information security professional is responsible for the development, implementation, and maintenance of an information security program intended to protect the confidentiality, integrity, availability, functionality, and authenticity of the organisation's information assets. It is independent from the real system. It might be stand alone computers, local area network, small computer system, private network, distributed system or network in open system. To achieve information security means defending the system against threats and danger. One of the preventing methods is the security evaluation according to criteria. The large challenge is to harmonise the criteria in order to achieve world-wide security evaluation standard, to help different vendors and manufactures in security design and develop for the computer systems.

This idea helps to achieve the security design in open system environment too. There are several secure solutions in OSI further in the application layer, X.400, Kerberos approach, and so on, but there is no real trust system according to security evaluation criteria. The systems might have been infected by computer viruses, worms or might have been endangered by other threats. So, this is the reason why security management is very important. It also means security attack detecting measures and methods that must be used. There are some security management functions under development, such as the "Security Alarm Reporting Function (DIS 10164-7)"; "Security Audit Trail Function (CD 10164-8)"; and "Objects and Attributes for Access Control (CD 10164-9)".

Within the European Information Systems Services Infrastructure under development it is hoped that open system security aid resolutions and standards will be set out. Security investigations programme has started and within it, there are several numbers of tasks about that, for examples: "verification of security profiles", "commercial accreditation" and "conformance testing".

9. Bibliography

Bill Caelli: "Evaluating system security: an international requirement", Professional Computing July/August and September 1992.

"Information Technology Security Evaluation Criteria (ITSEC)" Version 1.2, May 1991, EC DG XIII

"Information Technology Security Evaluation Manual (ITSEM)" draft version 0.2, April 1992, EC DG XIII.

"Information processing systems. Open Systems Interconnections. Basic Reference Model. General requirements" - ISO 7498 : 1984.

"Information processing systems. Open Systems Interconnections. Basic Reference Model. - Part 2 Security Architecture" - ISO 7492-2 : 1989 (E)

"Protecting the security of X.25 communications" - Data Communications, 1988 pg. 123-139.

"Security in X.400 Electronic Message Handling Systems", Datapro ISG report, January 1993.

J.Steiner, C.Neumann, J.Schiller: "Kerberos: An Authentication Service for Open Network Systems", IFIP/SEC93

"Information Security INFOSEC'92 Security Investigations" 1992, EC DG XIII.

ELECTRONICAL COMMITTEE MANAGEMENT

Vesna RISTIC, Peter LIPP, Reinhard POSCH
Graz University of Technology

Abstract:

In this paper a secure application entitled "Electronic Committee" is presented. Its purpose is the automation of formal committee management using a decentralised organisation. In particular, committee work from all levels of a university administration is observed. Though forced to transmit their votes over an insecure network, participants can rely on the basic principles of democratic electoral systems. Special attention is paid to observing regulations and standing orders available from a local database. The committee chairperson can, according to circumstances, select a service from the set of available security services and, in this way, determine the committee proceeding. Because the purpose of this application is to provide an useful tool rather than to enforce observing specific regulations, it could easily be modified for use in other fields of administration and management communications.

Keywords: nework security, security mechanisms, security protocols, blackboarding

1. Introduction

Computer applications supporting various kinds of meetings and working groups is a relatively new and therefore poorly explored area. Some authors [1] have previously studied the impact of electronic systems on the effectiveness, efficiency and satisfaction of working groups. For this purpose they created a "meeting environment" intended to make group meetings more productive. To achieve this goal, they investigated the mechanisms of group work and developed tools and techniques for the creation of information systems. They found that the new technology could significantly improve group processes and outcomes, although some effects were dependent upon the situation.

The implementation of security services based on cryptographic protocols has a significant impact on the field of computer supported group work. The set of possible modes of computer supported communication between two or more parties has grown enabling many forms of human communication to be performed over the computer network. Moreover, it is now possible to implement some new communication facilities which are not practically or easily implementable without computer support.

Our aim was to create an application enabling the automation of formal committee management. There are certain standard procedures which are present in every committee proceeding; for example, agenda reviewing, action points processing, voting upon important decisions, collecting proposals, etc. All of these procedures are always performed according to certain rules and therefore can be formally described.

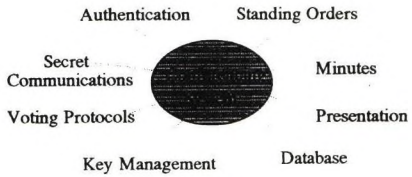


Figure 1.1 - The conferencing system's components

The scenario which we use was made by observing university committees meetings. It is now possible for committee members to be seated in their offices at their terminals while participating in a meeting over an insecure computer network. This application supplies a set of available security services to be used during the committee execution. This means that the secrecy of discussions, voting strategies and created documents as well as authenticity of attendees are provided. The set of regulations which must be observed is also available and conformed by "electronic" rules so that the committee work can proceed in concordance with the law. It is nevertheless possible to change the established protocol, if all attendees agree.

The primary purpose of the application is to provide an efficient software toolkit for committee meetings. It consists of the "working" elements common to all kinds of similar group works (Fig. 1.1). Although our aim was not to study the influence which such kinds of tools might have on the quality of the group outputs, we bore in mind the positive influence such an application could have on the efficiency of committee work.

2. Committee Meeting

In this section we give a general outline of a committee meeting. The given description corresponds to the usual university committee session.

In order to establish a particular committee, a constitutive meeting of the committee must first be held. During this meeting the committee members and their mandates and rights are to be determined. After the constitutive meeting, the general committee meetings can be held. If the committee has to be dismissed, the closing committee meeting terminates the committee activity.

The general meeting usually begins with a roll call of the members' presence (i.e. finding out who are the present attendees). The actual number of the participants is also important as the committee meeting cannot be held if the number of the present committee members is smaller than the required quorum. The committee member who are not able to participate may send their deputies to represent

them at the meeting, i.e. to eventually participate in voting in the name of the absent member. If the session is not closed, there may also be some attendees who are not in fact members of a particular committee but simply interested in attending the meeting. These attendees are informants and do not actively participate in the meeting unless asked for an opinion.

The meeting agenda can be determined beforehand or the attendees can make proposals for the action points. The first action point in the agenda is usually called "Review of Agenda", if the agenda has been determined in advance, so that the members may vote upon the approval of the proposed agenda.

The further proceeding of the meeting is based on the action points, which are processed one by one. The committee chairperson manages the meeting in concordance with the standing orders.

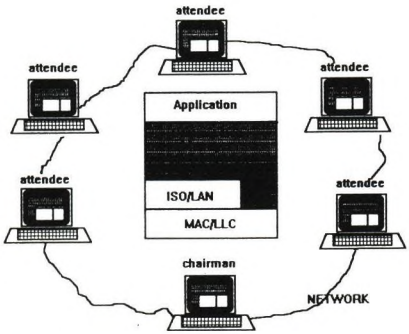


Figure 2.1 - The conferencing system in the network

During the processing of the particular action points different situations can occur:

- The chairperson may collect proposals about some actual topic, giving to every attendee who is an active member of the committee an equal opportunity to discuss and make proposals.
- The attendees may vote upon some important decisions or documents.
- A group of attendees may hold a short secret discussion and then return to the meeting.

The official record of the meeting is written in the form of minutes. Important documents are signed by all attendees who have taken part in the creation of the document.

3. Security Services

In this section the security requirements are described, i.e. what is to be secured. We stress some crucial points to which special attention must be paid as they require special treatment from a security point of view. This refers to the security services available to the committee which may but need not be applied to a particular meeting.

The proceeding of meeting must be in concordance with the standing orders. The observation of the prescribed regulations must be provided and supported by "electronic" rules (i.e. enforced by security mechanisms). For example, these mechanisms can protect fairness in discussions (distribution: every attendee has equal opportunity to discuss, timing: every attendee has equal time interval for discussion), equal information level for the members of the same security group, etc.. On-line information about the regulations is also available.

The security services we need are the following:

♦ First of all, the committee members must be identified and authenticated (Authentication Service). It is also necessary to determine the scope of their activities before the meeting actually begins, i.e. to authorise them. There can be many different group of attendees. A particular group is defined according to the members' permissions/rights. For example, the committee chairperson may have a greater scope of activities than a "normal" attendee, who in turn has more rights than an informant.
♦ Although forced to transmit their votes over an insecure network, attendees can rely on the basic principles of democratic electoral systems (Voting Service). The voting security services enable the voting procedure to be performed in different modes; which one to apply depends upon the demanded security level. In some cases it is not necessary to keep the voting strategy secret. The voting can be either public (the votes and/or voting strategies) or secret.
♦ It is often necessary that some subgroup of the attendees hold a short secret mutual consultation (Secret Discussion Service). They receive permission from the rest of the members and conduct the consultations within a given time interval. The content of this discussion remains unknown to the other committee members.
♦ Meeting attendees may sometimes want to exchange some private (and therefore secret) information without interrupting the meeting proceeding (Secret Message Service). Only the sender and the receiver are involved in the conversation and the other members are not privy to any information about it.
♦ The minutes of the meeting present the record for the committee proceedings and can contain some parts which should remain secret or known only to some closed group of people (Minutes Service). Therefore it must be stored in a protected database so that the access can be controlled. The attendees decide during the meeting which parts of the minutes must remain confidential if it is not already determined by previous regulations.

4. Security Mechanisms

In this section the methods are described by which the security services in the previous section can be implemented.

4.1 Authentication

Authentication is a two-way process: the application authenticates the attendees and the attendees authenticate the committee server. This security service is called peer-to-peer authentication [2]. The attendee is authenticated by means of his/her Personal Identification Number (PIN). One possible solution is Personal Secure Environment [13], which is a software implementation of the SmartCard.

After the authentication phase the authorisation of the attendee is performed, in which the set of the attendee's access rights is determined based on the information obtained in the authentication phase.

4.2 Voting

There are three types of voting protocol: Normal Voting, Secret Voting and Public Voting.

4.2.1 Normal Voting

The following requirements are to be satisfied:

1. Only legitimate voters are allowed to vote and each of them only once.
2. The voting authority can read the votes and publish them to other voters during the voting phase.
3. Only the voter and the voting authority know which strategy any given voter adopted.
4. After publishing the vote, a voter can check if her vote has been properly counted.

We have chosen the simple voting scheme proposed in [4]. The scheme is an application of multiple key ciphers and has two useful properties:

- no interactive behaviour is required between the voting authority (the voting server) and the voters
- no secret key is required from the users.

4.2.2 Secret Voting

The following requirements are to be satisfied:

1. Only legitimate voters may vote, and each of them only once.
2. Only the voter knows her voting strategy.
3. After publishing the outcome of the election, a voter may check if her vote has been properly counted. If not, she can complain without jeopardising the ballot secrecy.
4. (Optionally) Each voter can change her mind (cancel and recast her vote), also without jeopardising the ballot secrecy.

The chosen voting scheme is from [5,6]. We assume that the voting server (VS) sends to each legitimate voter her specific identification tag and then destroys the information which could reveal the identity of the voter having the specific identification tag. After this information has been made inaccessible, the second phase of the voting protocol can begin.

Let B be an individual voter with the tag t_B and voting strategy v_B. The voting protocol is then as follows:

1. B chooses a cryptographic hash function $h_B(x,y)$ and sends VS the pair $(t_B,h_B(t_B,v_B))$.
2. VS acknowledges the receipt by publishing the value $h_B(t_B,v_B)$.
3. B sends VS the pair (t_B,h_B^{-1}). VS can now compute v_B from $h_B(t_B,v_B)$, t_B and h_B^{-1}.
4. When the deadline for casting ballots is over, VS announces the outcome of the election by publishing, for each voting strategy v, the list of all numbers $h_B(t_B,v_B)$ such that $v_B=v$.

5. If B observes that her vote is not properly counted, she protests by sending VS the triple $(t_B, h_B(t_B, v_B), h_B^{-1})$.
6. If B wants to recast her ballot, she sends VS the triple $(t_B, h_B(t_B, v_B), v_B')$, v_B' being the new voting strategy. When the deadline for recasting is over, VS publishes the modified election results, where the numbers $h_B(t_B, v_B)$ have been reallocated in the list. The voter can also now check that her new vote has been properly counted. In this way the recasting of the ballot can be done only once.

4.3.3 Public Voting

The following requirements are to be satisfied:

1. Only legitimate voters may vote, and each of them only once.
2. The voting order is determined before the voting begins.
3. Every voter knows which strategy the other voters, who have already voted, adopted.

The voting order can be, for example, in alphabetical order. The voting protocol is as follows:

1. The voting server (VS) publishes the voting ordering list with n voters and the list of voting strategies.
2. The following steps are repeated for the each voter i on the list, in the order determined by the list.
3. VS sends the voting slip V=(*random number*, *redundancy component*) encrypted with the RSA public key of the voter with the position i on the voting list (voter v_i) to v_i.
4. The voter v_i creates a block (V, *voting strategy*), encrypts it with her RSA private key, and sends the encrypted block to the VS.
5. VS publishes the name and the voting strategy of the voter v_i.

4.2 Secret Discussion

The security service of secret discussion is defined in the following way:

1. The subgroup of attendees wishing to perform a short secret consultation asks the committee chairperson for the permission to do so and propose some duration.
2. The committee chairperson decides (or the committee members vote upon) whether the group may hold secret consultations. If yes, the maximal duration is determined.

The members of the secret consultation group requests a new session key (DES key) from the key management authority. The new session key is sent to the each secret consultation's participant in the form of the signed certificate (see [10]):

$$\text{Private\_RSA\_Key}_{Authority}(\text{Receiver\_Name, Time\_Stamp, Public\_RSA\_Key}_{Receiver}(\text{New\_Session\_Key}))$$

4.3 Secret Messages

The mechanism which enables the exchanging of secret messages between two attendees is based on the Privacy Enhanced Mail system [9]. The sender sends the message encrypted with the secret DES

key encrypted with the receiver's public RSA key which the receiver can decrypt with her private RSA key.
The exchange of the secret messages does not affect the meeting proceeding.

4.4 Minutes

The organisation of the meeting record is based on the meeting agenda, as it is in the case of the proceeding. Every action point is observed separately.

Everything should be noted: proposals, discussion contributions, voting results, decisions, breaches of the standing orders, etc., so that no one (not even the chairperson) can prevent the recording of some event. The names of the attendees are also recorded in the minutes and it is made impossible to eventually delete or add a name to the list.

Important documents are signed (digital signature, see [8]) by all competent attendees, either with agreement or disagreement. As only the particular attendee can generate her digital signature, she cannot later deny the fact of signing the document (non-repudiation service, see [2]).

The attendees who have signed a document determine the accessibility of this document. They decide whether this document should be kept confidential and determine the time when the document can be made public. This is important for the organisation of the database into which the complete record of the meeting will be stored.

The access to the information in the minutes database is controlled by capabilities (see, for example [3]). When a subject has access rights to an object (information), he gets the (object, access) pair, which is called the capability of the subject. The capabilities are dynamically managed. For example, if a document D can be made public, every user of the database gets the capability (D, read).

5. Software Organisation

The principal software organisation is based on the client-server model (Fig.5.1.1). The end users (attendees of the committee meeting) communicate with the application via the user interface. The users chooses one of the menu options and the application formulates, together with the necessary parameters, the task for the committee manager. The committee manager then performs the task by assigning various jobs to servers, i.e. sending requests to servers to perform some actions.

The basic elements of the software organisation are the following servers: *timing server, key server, access server, voting server, directory server, regulations server* and *minutes server.*

5.1 Timing server

Timing is very important for all security services. The role of the timing server is to provide the precise time information for the security protocols.

The rights owned by some subject are valid if certified by the certification authority. The certificate is always a temporary assignment of rights: it expires with the given date.

In the authentication phase it is also necessary to define the time-out interval (authentication deadline) so that after this interval has expired the session can begin.

In voting protocols the precise timing is of crucial importance. A deadline is determined for the duration of secret consultations.

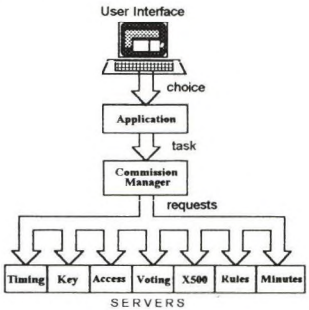


Figure 5.1.1 - The software components

5.2 Key server

The key generation is performed by the key server. The distribution of the RSA key pairs is accomplished prior to the session: these keys are stored in the Personal Secure Environment (a directory, for example). The key server generates keys for voting protocols, secret session keys for the service of the secret (closed group) consultations and similar purposes.

5.3 Access server

This server performs the authentication of the attendees and determines their set of rights, i.e. authorises them. The access server relies on the information obtained from the timing server.

If it is necessary to examine somebody's set of access rights during the meeting execution (after the initial authentication phase), the request is sent to the access server. This need may, for example, arise from the voting protocol, if only the subgroup of the attendees may vote. Because of this and similar situations, the authentification is performed on many levels.

5.4 Voting server

This server performs the voting protocols. It relies on the timing server and communicates with the proceedings server.

5.5 Directory server

This server is a Directory User Agent and enables the application's accessing the Directory Information Base [11].

5.6 Regulations server

The regulations server communicates with the local regulations database and ensures the validity of the meeting proceeding. In other words, the regulations server ensures that every official procedure is in concordance with the regulations. For every procedure certain conditions must be satisfied and the execution must follow the predetermined order. It is possible to neglect regulations, if the committee chairperson decides to do so and the attendees agree, but they are warned against breaking rules and informed that this event will be noticed in the minutes and submitted for arbitration.

5.7 Minutes server

The minutes server gets "reports" from all other servers and create an official report (i.e. stores the collected information into the minutes database). The data organisation is based on the time order, so that every information unit has a time stamp provided by the timing server.

6. Illustrative Example

Example : Voting service

The example of the communication between user and software components is shown in Figure 6.1.

The committee chairperson chooses the option "Voting" from the Menu with the available security services. She is then asked for parameters necessary for the voting procedure, i.e. what is the mode of voting (normal, secret or public), what is to be voted upon, who are the voters and what are the possible voting strategies.

From these parameters the application formulates the task and sends it to the session manager who co-ordinates the work of the servers. The manager sends the request to the rules server to examine the legal conditions of the voting. For example, if not all attendees are members of some very important committee they are, therefore, not allowed to vote upon the current subject. The rules server determines if some further security measures are to be taken - for example, to examine the access rights of the proposed voters. This request is accomplished by the access server.

After all legal conditions have been satisfied, the voting protocol can begin. The request is sent to the voting server which in turn requests keys and timing service from the key server and the timing server, respectively. After the voting has been completed, the minutes servers makes a report which is appended to the meeting minutes.

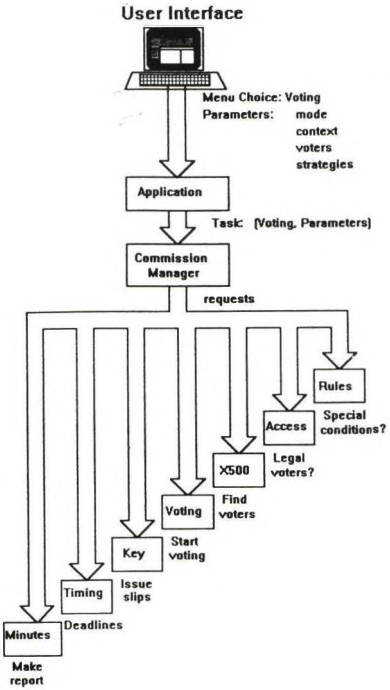


Figure 6.1 - The voting service

7. Summary

In this paper a model of the secure application for the automation of the committee work is presented. The purpose of the application is to supply an appropriate working environment comprising all important elements of the committee proceeding. This working environment enables collaboration over a computer network.

Special attention is paid to legal and security aspects. The committee proceedings consist of prescribed elements which require a certain security level of processing. These elements are defined as security services and create a set of tools available to the attendees. Attendees and committee chairperson may choose the security service. However, the chosen service must be in concordance with the legal regulations.

The mechanisms used to implement the security services are described. The application is organised based on the client-server model. The client in this scheme is application which proceeds the user's request to the committee manager. The committee manager co-ordinates the servers' activities.

The model described has not yet been implemented. Our aim is to make an experimental system which could assist in the better understanding of the processes mentioned.

References:

[1] Nunamaker, J.F. et.al., "Electronic Meeting Systems to Support Group Work ," *Communications of the ACM* , Vol. 34, July 1991, pp.41-61

[2] Muftic, S., *Security Mechanisms For Computer Networks,* Chichester: John Wiley & Sons, 1989

[3] Denning, D.E., *Cryptography and Data Security,* Addison-Wesley, 1982

[4] Boyd, C., "Some Applications of Multiple Key Ciphers," *Lecture Notes in Computer Science* , V330, 1988, pp.455-467

[5] Salomaa, A., "Verifying and Recasting Secret Ballots in Computer Networks," *EATCS Bulletin*, 44, 1991

[6] Nurmi,H., A. Salomaa, and L. Santean, "Secret Ballot Elections in Computer Networks," *Computers & Security* , 10 (1991), pp.553-560

[7] Diffie, W., and M.E. Hellman, "New Directions in Cryptography," *IEEE Trans.Inf.Theory*, Vol. IT-22, No.6, November 1976

[8] Rivest, R.L., A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of the ACM* , Vol. 21, February 1978, pp.120-1261.

[9] Linn, J., Privacy Enhancement for Internet Electronic Mail: Part I -- Message Encipherment and Authentication Procedures (RFC 1113), August 1989

[10] Denning, D.E., "Protecting Public Keys and Signature Keys," *Computer*, February 1983, pp. 27-35

[11] CCITT, "Recommendation X.500: The Directory - Overview of Concepts, Models and Services," Melbourne, 1988

[12] Akl, S.G., "Digital Signatures: A Tutorial Survey," *Computer*, February 1983, pp. 15-24

[13] Schneider, W., "SecuDE: Overview (Version 3.0)", Institut fuer TeleKooperationsTechnik, Darmstadt, March 1992

[14] Desmedt, Y., "Society and Group Oriented Cryptography," *Advances in Cryptology - CRYPTO '87, Lecture Notes in Computer Science* , 293, 1988, pp.120-127

CHALLENGES IN GOVERNMENTAL ACTIVITIES

Kálmán NAGY
Prime Ministers Office,
Co-ordination Office of Governmental Information Systems

Abstract:

The lecture is focused on the IT management of governmental institutions. I would like to give a brief overview of the main elements, objectives and organizational framework of the governmental IT policy. I would like to present the most important laws and resolutions that regulate the IT activity of the government and also, would like to outline our achievements so far. Finally I will introduce you to some governmental IT projects of high significance and our future plans.

1. Introduction

The backward telecommunications services have been a source of serious losses for the national economy and also the most important barrier to the modernisation of the country. As it is well known, proper telecommunication is an indispensable condition for economic growth which has a decisive impact on the speed and efficiency of the flow of information.

The availability of a network structure is an indispensable condition for technical development. Recently a recognition has become more and more acceptable according to which development may only be accelerated if the operation and development of the telecommunications sector, which has been operating as a public utility to date, is gradually put on a business basis. As part of the privatisation process, the privatisation of MATÁV is also being prepared. The privatisation of MATÁV will enable the integration of foreign capital, integration of technical knowledge and the acceleration of technical development. The current MATÁV development is aimed at a brand new national digital backbone network structure, which will be implemented in approximately 3 years.

In addition to large state-owned companies the new large users primarily include financial institutions, insurance companies, large business and trade centres. The increase of efficiency of enterprises will involve another growth in telecommunications demand. The appearance of international capital also involves the appearance of international private networks. The demand for telefax and mobile services has also increased significantly. Regarding data transmission services, a dynamic increase in demand may be expected in the area of package switched and rented line capacities in almost all areas of public administration.

Following the change in state administration and economic control, the telecommunications and data transmission demand of the various sectors of control (local authorities, health crimes, CUSTOMS, finance, etc.) has also increased. The reconstruction of telecommunications system in public administration has also been put on the agenda within the framework of this programme, but I shall talk about that issue in detail later.

2. Organisational structure and conditions of governmental activities

As part of the acceleration of economic processes, a decision was made on the implementation of the comprehensive reform ideas of public administration. The reform covers the functions, tasks and scope of authority of public administration, the operation of public administration, its organisational framework and the personal staff.

The Government establishes various inter-ministerial committees to carry out the tasks of harmonisation occurring at different levels. Among others, these committees perform tasks related to the preparation of decisions for the Prime Minister and the Government, give their opinion in special issues, and carry out tasks on the basis of separate assignments.

In order to fulfil the IT harmonisation tasks of public administration, in accordance with the Government's resolution No. 3296/1991. (VII.5) the Inter ministerial Committee for Information technology was established and led by the permanent state secretary of the Prime Minister's Office. As a result of the legal status of the Government and the inter-ministerial co-ordination tasks, the organisation performing the operational and secretarial tasks was also established within the structure of the Prime Minister's Office.

The general objectives are the following:

- modernisation of the telecommunications and information system of public administration related to the public administration modernisation defined in the resolution of the Government No. 1026/1992.(V.12.) Korm.
- co-ordination tasks related to the Governmental information technology development defined in the resolution of the Government No. 1039/1993.(V.21.) Korm.
- support of the legislative, decision supporting and expert system of the Government
- definition of general basic principles related to telecommunications and information technology in public administration
- issue of Governmental recommendations complying with the EC regulations
- the enforcement of the open system principle related to information technology
- introduction of strategic planning in information technology
- enforcement of data security and data protection requirements

The implementation of Governmental resolutions involves the continuous performance of the following tasks:

- the operation of the Information Technology Inter-Ministerial Committee (ITC) and its work organisations,
- situation analysis in the related areas,
- analysis of development options, definition of directions, strategic planning,
- establishment of international relations, provision of continuous opportunities for consultation
- adaptation of international standards and recommendations,
- organisation of education, information and assessment for,
- launching of specific applications (pilot projects),
- provision of instruments for the execution.

The Frame Programme aimed at the Development of Governmental Information Technology was prepared as part of the activities of the Inter-Ministerial Committee for Information Technology. The programme set out the main requirements and objectives related to governmental information technology, naturally also including the IT harmonisation tasks resulting from the preparation of our integration into the EC.

Regarding the implementation of the public administration reform, the Government set out the programme including the directions and principles of the modernisation of public administration in its Resolution No. 1026/1992 (V.12.). The various parts of the programme define tasks for telecommunications, and also in relation to the content and formal elements of information technology.

A study entitled the "Development of Information Technology Infrastructure in State Administration" was prepared in order to ensure the implementation of point 9/c of Resolution No. 1026/1992.(V.12.). In addition to the conceptional and infrastructural issues, the study also dealt with the necessity of comprehensive solutions to the organisational and personal issues.

In order to co-ordinate the information technology-telecommunications development of central governmental organisations, in its Resolution No. 1039/1993. (V.21.) Korm., the Government made a decision on the establishment of conditions affecting the information technology area of integration into the European Community and on the harmonisation tasks related to the information technology, investment and financial activities of the organisations of state administration.

The experience of the recent period, the prepared studies (Governmental Infrastructure Development Concept - National Committee for Technical Development (OMFB), Governmental Information Technology Framework Programme, others) drew the attention to the necessity of the review of the present structure.

The activities of the ITC during the last period may be summarised as follows:

- It defined the objectives and tasks of the framework programmes aimed at the development of the Governmental Information Technology, and laid down guidelines and recommendations on the regulation of strategic planning in information technology and the methodology to be applied in development.

- It requested a situation analysis from ministries and organisations with a national sphere of authority on the information technology activities and strategy in the related areas, and also asked them to prepare a development action plan for information technology.

- EDS Electronic Data Systems Ltd. was assigned to work out, jointly with the Information Technology Foundation of the Hungarian Academy of Sciences (HAS), a review plan for the co-ordinated development of information technology infrastructure of public administration. As a result of that, a study entitled " Development of Information Technology Infrastructure in State Administration" was prepared which was accepted following the assessment of affected institutions which took place in several stages.

- On the basis of the subject material concentrating on strategic planning and prepared using the supplementary material of British public administration, and within the organisation of IKI, the Information Technology Foundation of the HAS launched a training programme for the concerned managers and experts of the Governmental organisations.

- As the first specific element of the action plan, a recommendation was prepared for the uniform introduction of Hungarian character codes of computer word processing in the entire public administration.

- A proposed budget was prepared for 1993 for the investment programme entitled "The development of information technology infrastructure of central Government"

On the basis of the above, the following conclusions may be drawn from the experience collected during the performance of tasks resulting from the Resolution of the Government.

- There is a very strong and common demand for a uniform telecommunications and information technology system which would be task specific and would not violate the independence of each ministry.

- The hardware and software equipment of the various Governmental organisations reflects a mixed picture. Their purchases were primarily focused on office electronics and not the comprehensive requirements of information technology. The main reason for that is the lack of available financial resources, and even more that of strategic planning and co-ordination.

- In order to handle the apparent contradiction of "central influence" resulting from the rights of ITC, and the independence of ministries and manage the implementation of the Resolution of the Government, the best definition of utilisation of all the public funds (planned within the

budget of various institutions, and within the scope of authority of the ITC) available for information technology should be found.

- Very clearly defined, scheduled and accountable projects must be launched, and the role of the ITC most be increased. Through the projects, an information technology system must gradually be developed which allows electronic communications between the various governmental agencies.

Analysing the experience of the last 2 years, the proposal making role of the Information Technology Inter-Ministerial Committee will probably be extended with an executive scope of authority, co-ordination functions, its role will extend to all organisations falling within the scope of the Act on Public Servants, the organisation of the Co-ordination Office for Information Technology will be strengthened, or a new independent organisation will be established, the infrastructure providing a link between ministries will be developed and the contextual and organisational framework of IT activities performed in the ministries will be reviewed.

And now I would like to move on to the activities and experience in the ministries.

As a result of tasks and functions, which were specific to ministries, different solution options were developed which involved different structures. The subordination of the IT organisations, their place in the ministry, their staffing level and financial resources are different in each ministry. In the various organisations the staffing level of IT organisations is relatively low compared to their size. There are no uniform organisations which could provide a suitable framework for the management of planning, operational safety and purchase tasks.

The tasks of IT organisations within the ministries include the support the IT activities in the subordinated organisations both at regional and national levels, and also the management of tasks requiring inter-ministerial co-ordination, which is insufficient at the moment.
The development of the background organisations fulfilling the additional tasks of IT activities does not support the activities of the ministries as much as it should. With increased utilisation of the basis of background institutions, we wish to provide an opportunity for more efficient decision preparation, preparatory organisation, analysis, and data processing activities in the ministries or their possible contracting.

A proposal was prepared for the preparation of changes but no decision has been made in that respect, therefore I cannot give you more information on that at the moment.

During the analysis of IT activities it was stated that the way of development of Governmental information technology should involve the domestic adaptation of the recommendations and working solutions of the EC, because the harmony of political objectives, efficient fund utilisation and desirable technical standards may be ensured best.

Our commitment to the Open System Standards is clearly shown by the fact that the government declared its intention to introduce the Open System Standards and in consequence became a member of the Users' Council at the end of 1992. (The decision was important because of the statement of EC orientation.)

ITB intends to take the necessary measures to make sure that, according to the international standards, the government and the administrative authorities will use the environments suitable for the improving, operating and adjoining of the user applications only where the replacement of hardware elements would not cause a significant cost for the conversion of programs. This requirement naturally includes the most important features of open systems, such as portability, connectivity and compatibility.

Apart from the above mentioned it is also a highly important issue to enforce the system of requirements set in the ISO 9000 Standard with the suppliers (of products and services) as well as with the users (governmental institutions, public administration). At the same time another important task is to make use of the results of Total Quality Management System and to enforce its use in the entire public administration.

3. Projects

Recognising this challenge, in its resolution No. 1039/1993.(V.21.), the Hungarian Government decided on the establishment of an integrated data transmission telecommunications system for the Government and the study of its material organisational conditions. The issue requires very deep and multilateral study, including the technical economic calculations and security requirements.

Among others, the advantages of the replacement of the old telecommunications infrastructure and telephone exchanges are the following:

- The diversified services of new telephone exchanges increase the efficiency of public servants
- The telephone conversation charges may decrease
- Maintenance costs would significantly decrease
- The equipment and rental fees may be saved.

I wish to mention here that some Governmental institutions rent the telephone exchanges from MATÁV, and in the new system the new telecommunications means and the network would be owned by the Government. The performed economic calculations showed tat almost 80% of the outgoing calls are directed at public administration institutions. The logical conclusion of the survey is the establishment of a private network which would allow direct connections based on optical cables between the digital exchange and sub-exchanges of public administration institutions, which will enter the system soon. The study showed that in 7 years nearly 980 million HUF expenditure could be saved considering only telephone services. However, if we take into consideration that the application of modern digital technology allows the development of data transmission services and other integrated services, perhaps the establishment of an ISDN network, further significant savings may be shown, not even mentioning the further benefits resulting from the higher standards, and I do not think I need to go into details about those now.

As the first step of the programme, the feasibility study of integrated telecommunications system of the Prime Minister's Office, Parliament and the Offices of the Members of Parliament. The tender issued in the meantime was won by the Kapsch company partially owned by North and Telecom. The next step will include the study describing the telecommunications and data transmission connections between the main government agencies in Budapest. Without going into too many details, I can say in advance that in the area of data transmission naturally the X.400, X.500 directives, complying with international recommendations, were taken into consideration.

Regarding the application of satellite communications tools we may state that this modern technology is spreading more and more for special tasks in Hungary. The only serious barrier in the

wide scale of application of satellite instruments is public administration is the very high turnover costs. With minimum turnover, the east European connections may represent monthly 100,000 HUF. minimum expenditure in each country if we only consider the work in foreign representations, but if we consider the average costs, it is 12-15 USD./minute.

Public administration has and will use mobile telecommunications and data transmission means. At the moment in the case of part of the services public administration also uses the mobile telecommunications services of public suppliers at 450 MHz. I do not think it is necessary to stress the benefits resulting from the introduction of GSM services which will be available for the participants in the entire Europe as part of a uniform communications system. The tender competition issued by the Ministry of Transport, Communications and Water Management proves how seriously the Government considers the establishment of a uniform European mobile telecommunications network.

In the case of information technology systems, simultaneously with the social economic growth, the establishment of conditions of co-ordination and integration between the various systems is becoming more and more important. In the large public administration sub-systems (financial, statistical, duty, etc.) more and more information is collected which must be integrated at a managerial level during the preparation of decisions. The Hungarian Government also recognised the need for the acceleration of the process and wished to do its best to complete the restricted Hungarian budgetary funds with various foreign funds, aid funds, and provide the necessary financial background for development and integration processes. At the moment in ministries and main authorities nearly 3500-400 PCs operate. Nearly 0.8% of the generated national product is spent by public administration to purchase and operate IT systems. However, in addition to internal resources significant external funds also support development.

Some data: The National Headquarters of the Customs and Finance Guard received nearly 8 m ECU within the framework of the PHARE programme to establish the national computer network of the Customs Guard, to register private turnover and foreign trade activities and accelerate the collection of customs duty revenues. Also within the framework of the PHASE programme, the National Statistical Office received 10 mECU for the modernisation of the statistical system of the Office. Training is also a natural consequence of technical development . The implementation of the public administration reform programme is supported with 5 mECU, of which 300,000 ECU is allocated for IT development at local authorities, 400,000 ECU for the implementation of IT projects of the

central Government and for strategic planning and the training of public servants. I wish to note here that in three months nearly 400 people from the various regions of public administration participated in the 1-3-day series of lectures related to strategic planning. In 1993 nearly 240 m HUF, and the own budgetary resources of the Ministries will be available for the IT objectives of the central Government.

The 1994 projections recommend nearly 650 m HUF. for IT development in central public administration and nearly 500 m HUF. is recommended to finance telecommunications plans. That includes only the financing of central target programmes, in addition to which there are also the state funds incorporated in the budget of various ministries, and the funds coming from the PHARE, Know How Fund and other foreign aid projects may also be taken into consideration.

4. Conclusion

In summary, I feel that the technological and technical development taking place as part of the public administration reform involves an enormous task for all regions of public administration. The final objective is the establishment of an efficient, cost saving, citizen friendly public administration infrastructure which corresponds to the technical standards of these days, the European system of requirements, or at least tries to be close to them As it is said, it is also true for technological development that the only thing needed is money and money. Talking seriously now, I feel that human beings are at the end of the process, who use and serve modern technology, which has broken into our everyday life and changed our life completely. Our objective is to be able to meet that challenge, to be able to apply the technology and be able to use the benefits provided by IT. I think that one of the most important messages of such and similar meetings is to give an answer to all questions involved in the technological challenge, so that technology and the fight with technology should ease our life in the end.

Bibliography

[1] Inter Ministerial Committee: "Hungarian Government Information Technology Improvement Programme"

[2] EDS - IMC: "Information Technology Infrastructure Development for Public Administration"

[3] National Office of Technological Development: "Information Technology Development Project for Government Administration"

Changes in information technology and networking in the Hungarian public administration

András Gerencsér, Chief Counsellor,
Department of Elections and Informatics
Ministry of Interior
1903 Budapest, Pf.314/24
Hungary

Abstract

The informatics and information technology are indispensable tools and supports of the bureaucracy, of the high quality services in the state and public administration in Hungary too. There are 13 ministries and more than 30 offices with nation-wide authority in Hungary. The number of the various offices on the middle level of the public administration is more than 600. Nowadays the authorities in the central level and the various associations of the 3133 local governments are planing their own information network. The broader offer on the market of the information technology means big challenge in the growing democratic structure. However, it means some dangerous decisions in the hard economic environment of the present days. The changes of the past years let conclude: it is time to think about the nation-wide data communications network for the Hungarian public administration. It would be more effective and economical to use a common transport layer and maintenance instead of the occasional or individual end points provided by MODEM or at the packet switched public service.

1. Introduction

It is noticeable in countries more developed than Hungary, that intelligent services satisfying individual needs are gaining more significance than would be expected from industrial societies characterised by the evolution based on uniformity and mass production. Informatics play increasingly important role in the everyday life, so those societies justly call themselves the societies of information. If we try to compare our information infrastructure with those countries, we would realise that our level only reaches the level of those in the seventies or early eighties. Inevitably, it raises the questions: what are the causes and how can we catch up? It is worth studying how the social expectations can be satisfied the soonest, out of the Western resources that have been far less than hoped for in the field of the public services. To fulfil the expectations that a Hungarian or Central-Eastern-European citizen expected from the public administration in 1989-90 following the example of developed Western democracies. The satisfaction of such expectations by informatics means is not just 'improving the general mood' or an investment

aiming to make the job of civil servants easier. We have to believe the Clinton administration's paper entitled "Technology for America's Economic Growth" [1]. It points out, that one of the most important factor of the six proposals of the economy vitalising program is the development of informatics; the building and usage of the high-speed data backbone, a national fibre-optic network.

Informatics and information technology are essential tools and help the work in the public administration here in Hungary too. The possibilities of the information technology (IT) include applications towards different directions, from the support of the 'work at the desktop' (word processing, spreadsheet handling, electronic mail) to the more complex applications (such as, file transfer, remote databases, GIS-LIS, on-line access to distributed databases and other information systems by any workstation, document interchange, video conferences, voice-mail, etc.). With the widespread use of digital technology it may become evident to everybody in Hungary, too, that all these are different forms of appearance of the information. Basically, voice, data, text and video (some mention graphics as separate item) carry information, and we are talking about generating, and/or gathering, transferring, processing and storing of different forms of information, allowing for the transparency of the individual forms or operations [2].

2. Changes

Voice communication, the Edison-Hughes telephone from 1877-78, the first form of electric telecommunications, usable by all non-experts have been publicly used from the introduction of the telephone switchboard invented by Tivadar Puskás in 1877. On 1 May 1881 the telephone exchange office (PBX) was opened in Budapest. By the time of the legislation of Act XXXI./1888. regulating 'the operation of telegraph, telephone and other electric equipment', PBX-s operate in nine other cities in Hungary. The Act declared the installation and operation of the equipment a state monopoly. It ordered to connect the existing 279 private lines to the state national network. The evolution was fast and it kept pace with the world. According to a newspaper article published at the turn of the XIX. century [3] "We do not think much of a town nowadays, that does not have even a local telephone. Interurban telephones are also rather ordinary....**The businessman, the officer of public safety, the journalist can view it as a tool to be used very advantageously.**"

It was the business, rather than the state organs that expressed interest in the first telephone exchange office of Puskás. Entrepreneurs created the PBX-s and businessmen were the subscribers. Such initiatives had been excluded by the central state control following a different path during the last few decades, until the new Telecommunications Act LXXII./1992. that provided for non-state initiatives again. The title to the unified interurban, rural and basic networks, after having been in State hands since 1888, was passed to the Magyar Távközlési Vállalat (MATÁV: Hungarian Telecommunications Company) in conclusion of the restructuring of Magyar Posta (Hungarian PTT). MATÁV has been formed into a private company with a reserved majority shareholder of the Hungarian State aiming to attract foreign and domestic capital investment.

As the COCOM restrictions were relaxed, all the large mainframe manufacturers entered the

Hungarian market establishing representative offices or even forming Kft.-s (Hungarian Limited Companies), resulting in the long overdue replacement of the obsolete ESZR equipment (the ancient COMECOM unified computing system 'project'). By now, IBM, DEC, Bull, Siemens, Phillips and Hewlett-Packard all are present here. We must also mention Apple, ICL, Compaq, SUN, Silicongraphics, Unisys out of the hardware manufacturers, and the list is still far from complete. It has also significance that companies engaged in software and databases, like Computer Associated, Microsoft, Oracle, Sybase, Informix are also present, considering that Hungarian software developers have completed different tasks successfully worldwide on appointment basis. France Telecom, Inmarsat and other VSAT service suppliers are also here, together with significant technical and economic advisory service companies.

Exploiting this background, one of the most significant programs within the market sphere is the large project for the development of the telecommunications network, financed partly by loans from the World Bank, aiming to improve the availability of telephone lines, but by the creation of a digital backbone has another importance in the transfer of non-voice information too. These developments had already been planned back in the organisation of Magyar Posta within a long-term plan up to year 2000 to improve the untenable position of Hungarian telephone line supply (one of the worst in Europe) somewhat, and, at the same time, to start off the catching up in the area of technology. For the last decades, domestic experts had been offering evidence to demonstrate the negative consequences of the under-development of the telecommunications infrastructure, and the urgent need for its development. There was not, or hardly at all, development of citizens' telecommunication at the time, when in the West the telecommunications branch went through a constant expansion and boom.

The "K-network", established before the Second World War and the telecommunications networks of the security forces, which represents the level of the technology in the 1970-s and 1980-s, there are our present public service telecommunications, which complies with the past needs of the central governing. The situation today is characterised by the challenges from both organisational restructuring and technological developments. The network of the Ministry of Interior, for instance, developed during the last decades, must be capable to satisfy the requirements made by police, fire-brigade, border-guard, etc. and the public administration. It is a justified question, how the existing networks and equipment can be utilised amongst the new circumstances. It stands to reason, that the implementation of the new technical solutions shall start on smaller areas within the private sector - as it universally happens - apart from special governmental and defence tasks. Within the Hungarian conditions, technical evolution itself cannot be the justification for developments, but the necessity of it for creating an essential tool helping the functioning of the organisation is unarguable.

The central level of the state and public administration having established after the 1990 elections consists the 13 ministries and more than 30 national authorities with regional, county, etc. organs. All these prepare and implement independent development plans serving their requirements. The developments, due to the nature of de-centralisation, use different individual networks (advisory, training, data gathering, etc.) including the establishment of communications and information links. However, the public administration organs not being represented at regional levels, also have nation-wide data connections. The demands for lines of the various national organisations, subscribed from MATÁV, range from one each per region (a total of 9) or county (a total of 20)

up to a maximum of 200 nationwide figure. Looking at the middle level of public administration only, we estimate more than 600 offices, directorates and branches, and that does not include the 3,133 local governments. All these public and local administration units have significant information contacts, presently carried basically on telephone, telefax, paper or floppy disks.

The characteristic of the domestic changes:

- Subsequent to the change of the regime, the most up to date hardware, software and expertise are present in the domestic market. The large international information technology companies all have representation in Hungary. The formerly known only by hearing, e.g. Internet, Bitnet, CompuServ, TCP/IP, systems running at the X.25, X.400 and X.500 standards are all within reach.

- The communications, information technology equipment, systems, created in the course of central state development during the last decades are going to be obsolete, modernisation of those would incur significant expenses and would only be possible with the help of foreign capital.

- Changes in the organisation as a result of the first free elections, the new legal regulations and the new requirements must also be followed by information technology.

- The organisations of the central and local administration have been engaged in continuous development in their quest of finding new solutions. The fragmented, relatively low IT investment expenses add up to significant sums, and the utilisation of these sums is not cost-efficient.

- The private sector will have primary role in the developments, the public sector can only follow the developments, or become end user of them.

The existence of the telephone offers the facility for electronic communications. The resulting number of the world average number of telephone lines per 100 people influences the countries in Asia as follows: China 0.6%, Mongolia 3.48, Malaysia 8.88%, Australia 47.3%, Brunei 12.96%, Macau 20.17%, South Korea 31.52%, etc. [4]. Hungary, in terms of telephone lines, is at the bottom of the league out of the European countries. The 9.6% value achieved in 1990 as a result of significant investments during the last few years, was a step forward (being above the world average of 7%) which MATÁV intended to better up to 14.5% by the end of 1993 in their short-term plan [5]. In 1992, 12 counties of the country had less than 7% telephone lines, in 1993, we can only expect 2-3 backwards counties. Having said that, in 1993, 1/3 of the 3092 settlements still have manual PBX, practically excluding the residents from using their phones 24 hours a day, not even mentioning the lack of more up to date facilities. Access from the larger Hungarian cities to some of the line switched network of X.21 ("NEDIX"), or MINITEX, Videotext, Teletext, telex services had already been available during the last decades, and the packet switched X.25 network has also increased its participation. However, this has not been true for 91%, of the settlements, the ones with a population below 5000. In order to solve this later problem, MATÁV declared its village program. The growing number of formation of telephone companies initiated by the local governments is a more progressive phenomenon. In these, MATÁV is only one of the potential

partners in the competition. There are some 900 local governments considering the formation of such telephone companies. The names BakonyTáv, Budatáv, Digitel-2001 Kft-s have become increasingly familiar recently.

Whilst more than 1/3 of the domestic settlement has a slow development, banks in larger locations established their virtual private network within the X.25 network operated by MATÁV-PLEASE with the planned system (to be completed in 1993) of 400 subscriber lines and 856 terminal connections [6]. This is a relatively minor project compared with the planned development of computerisation of OTP Bank due to start in 1993. The infrastructure may evolve on the basis of computerisation of inter-bank accounting; the development of services like credit cards will need individual services, servers and systems (e.g.: radiocommunications: WESTEL-Ericsson MOBITEX, US/H Supracom, etc.).

3. Application of information technology, networks

During the last few years, there were not only the market oriented companies like IBUSZ, MOL and the banking sector (Giro system, OTP) who prepared development concepts, investment plans in the area of informatics based on the using of the MATÁV network. The switched line data transfer through the national network had been already used by SZÜV earlier. The organisations of the Ministry of Finance still use it together with APEH's (Inland Revenue) public packet switched network. Significant users of MATÁV lines include Central Statistical Office, National Health and Pension Insurance, National Labour Center and National Customs and Finance Police with the planned nationwide computer network, but the land registry systems and the company registration court data file systems could also be mentioned. There are individual companies operating their own network, but even they are taking advantage of the MATÁV network and infrastructure at a certain point. These are for instance MVM Rt. (Hungarian Electricity Works), MÁV (Hungarian Railways), the ÁBKSZ (water management organisation) apart from the Ministry of Interior and the Ministry of Defence. They may also act as enterprising suppliers; for instance ÁBKSZ or PTN (Professional Telecommunications Network), an enterprise of MÁV, Antenna Hungária, KFKI and foreign investors.

One of the key notions of our age is network. We can hear more and more about the establishment of nationwide, or international systems, private networks, and such services are offered by an increasing number of firms. According to the findings of studies of economy, it is the development of IT networks that has a strategic importance amongst the conditions of economic progress [7]. The EC Commission stated that the level of development of public administration informatics is the indicator of the economic life of the country as a whole.

If we only look at the last two hundred years of history, we can follow the development of the nationwide, later international, inter-continental networks in line with its relation to economic growth. The history of networks convincingly corresponds to the changes of economic development phases (it can be matched to the Kondratiev analysis of periodic phases of economic development). Today, the global standardisation and connection of telecommunications networks are on the agenda. The fundamental importance of building the communications links has been

emphasised by the re-shaping of the EC Committee DG XIII. at the beginning of 1993, and by the recognition of the significance of the telecommunications develpoments. As a result, the prospects by the turn of the century will be the establishment of the society of information, meaning the widespread use of information technology in the areas of production, trade, commerce, services and public administration. It will result in, for instance:

- in industry: fast production of goods satisfying individual needs, structured manufacturing of products for the personal needs geographically close to the customer;

- in business: reduced operational costs through information technology operations and communications links, reliable scheduling through electronic stock control, settlement and transfer, shorter delivery times, rational use of human resources.

Through the higher level of unification of different forms of services from an informatics aspect will enable the user to be in direct contact with the service and the provider of the service faster and cheaper without the need for clerks or agents. Simple examples for this are the modernisation of car registrations for police organisations, seat reservation on railway carriages or the different banking services (such as the development of seat reservation with MÁV or Automated Cash Tills at OTP bank, introduction of magnetic cards, etc.), the development of management, decision-making information systems.

Information technology: establishment internal and external links for the organisation. It is the development of the paperless office, it is service to the client instead of the authority over the citizen, it is cooperation based on trust instead of bureaucratic pitfalls. Security and data protection will have specially significant role at the times of the creation of large networks. This is the time when the information technology security features are of important use; application of authorization codes, passwords according to the different levels, participation of third parties the so-called security service providers.

The changing of national and multinational activities into everyday events is helped by informatics and logistic connections. The networks will provide the best expertise necessary to carry out the task and the most efficient path to the goal.

The managerial approach and decentralisation play significant role also in the central and local public administration. Market-oriented service instead of the authoritative action, emphasis on the service to the citizen, the transfer of central administration tasks to the de-concentrated, perhaps, the private sector, will result in significant changes. All these, together with the authorities' trustful assumption of the citizen's carrying out his duties, will emphasize the application of information technology in the authority, administration procedural and controlling activities at the extent that goes far beyond the scope of office automatisation, the equipment of the administration with multi-functional computing facilities. The changes in Europe in the 90-s require very wide international contacts (due to migration, refugees, international crime-fighting, social security and other social affairs, etc.).

4. A national public administration network?

Looking at the domestic infrastructure of informatics, we are, in comparison, at the position as the developed countries were in the late seventies and early eighties. It is not an insignificant condition of joining the European Community that we should catch up with them in this aspect too. The evolution of information technology is very fast. According to the findings of academic research, the task of controlling the development of informatics should lie with the masters of information systems at ministry level, i.e. at the level of Government. The decisions concerning investments in informatics serve three purposes: an automated support to the office routine operations, the increase of the general technical operation capacity of the entire organisation through the reduction in human work activities and, thirdly, modernisation of planning and control in the management of the organisation.

In 1986, MTA (Hungarian Academy of Sciences) and OMFB (National Committee of Technical Development) jointly started the five years Informatics Infrastructure Development Program (IIFP) of scientific research, technical development and higher education for ensuring the professional, economic and organisational coordination. This network was built basically for the research and development, for the education. Its services mean a special significance, as it triggered off the establishment of the domestic packet switched technology with the support of the Magyar Posta (X.25 network, SOKBOX switching equipment development).

The key word of the development of a national infrastructure is cooperation, the foundation of which was established at the time of the installation of the so-called academic network. The electronic mail system, operating over 8,000 electronic mailboxes by the beginning of 1993 means a significant information infrastructure that is capable of facilitating international data communications too.

MTA, OMFB, MKM and OTKA defined the terms of membership concerning the extension of IIFP program during the period between 1991-94 as:
"We consider those organisations, institutes of independent legal entity and corporations to be IIFP institutions, that accept the basic objectives of the IIFP program and wish to cooperate with the participating institutions."

At the beginning of 1993, out of the 436 IIFP member institutions (nearly 240, i.e. 55% of which is connected to public data network), 26 public administration institutions (6%) are listed [8], constituting one of the 12 groups of the Applications Council. The number of strictly academic (research, education, public collections, so-called HUNGARNET) institutions are 306 (70%), enjoying special advantages, support in the course of the development and use of the network.

The agreement made in May 1991. by MTA, OMFB, MKM and OTKA set out the objectives for 1991-93 as development and education and specify the development and application areas as follows:

1. Data network development
2. Establishment of regional and discipline centres

3. Development of electronic mail
4. Development of database and library services

These tasks are of general nature. From the point of view of public administration it is interesting to study the conditions of introducing and extending electronic mail. The most interesting task would be the regional development, and the establishment of the INTERNET Protocol (IP) technology HBONE, a leased private digital backbone. Thus, exploiting the advantages offered by the public X.25 MATÁV-Please Kft. network, in 1993, a digital network will be established with nodes in Budapest, Gödöllő, Debrecen, Szeged, Pécs, Miskolc, Veszprém. Later, in 1994, it reaches Sopron, Győr, Keszthely, Kecskemét and Nyíregyháza too. The total number of nodes will reach 30 finally. Thus they will include all the residences of the Commissioners of the Republic and all the county towns. It must be mentioned here, that MATÁV will establish a total of 54 digital primary node centres in the country, according to their plans in 1993.

Not mentioning the University FDDI in Budapest (as the ministries and the national authorities, due to the nature of their activities, require a separate network here), there are welcome initiative plans under development of the different provincial universities for town and regional networks (MAN-s and WAN-s). All these, together with the citizens and entrepreneurial initiatives, the good practical examples of the information infrastructure and can link to the informatics needs of the local governments, middle-level or regional public administration. In, amongst others, Veszprém and Nyíregyháza such MAN (town network) plans have been prepared.

It might have been noticed from the above, that several nation-wide information systems concerning every significant town of the country have come to being, operated by entirely different organisations. Apart from some negligible exceptions, the only common feature of those systems is that, for the transport media, they all use the national network that has been continuously built and traditionally developed from the end of last century and presently is operated and in the ownership of MATÁV Rt. and it's Kft.-s. The new Telecommunications Act provides for the possibility to establish of offers for different networks by several suppliers, especially in the fields of non-voice services and networks for private use. These offer the designers the scope for designing cost-efficient and reliable informatics networks.

In August 1992, the Hungarian Prime Ministers Office declared the governmental intention to join the open system users' camp. The X/OPEN Users' Council has a member representing the Hungarian Government too. In order to achieve the aim, it serves the purpose to study the operational conditions of the national information systems according to the seven layers of the OSI reference model used in open systems. From the point of view of the end user, it is irrelevant what the transport media are, if we do not mean what the economic and financial consequences are. This characterises the situation today. However, the demands are of many different kinds. The main overall requirement should be the cost-effective satisfaction of those demands. Nobody can claim today, that the spark-telegraph of the nineteenth century, or long-distance shortwave radio connections, or the domestic UHF radio transmissions and telephone networks, the kind of communications as voice and telex could provide - apart from the basic communications needs - the facilities for transferring sufficient data for decision-making in a market-leading shipping and forwarding company, or a national/multinational firm with several plants in different locations, or, indeed, security forces or public administration. Exactly for this reason, the remote end-users on

moving objects, or temporary plants, or far from densely populated areas, exploit the terrain or satellite microwave communications facilities nowadays. Similarly, it must be admitted that the telex, telephone and telefax communication facilities that presently dominate the domestic technology (over 90% of all communications), cannot satisfy the requirements of even the smallest local government considering the budgetary, tax and regional development data supply, or, even if the present level of telecommunications facilities satisfies those now, very soon, they will be the foremost stumbling block in development.

Today, the most common method of fast information exchange is using MODEMs connected to the telephone line - together the actual telephone sets - from the personal computers. In 1990, according to Peter Norton, approximately 18 million MODEMs were used worldwide by small companies, by homes and travels. Popular applications for MODEMs are the different electronic bulletin boards (BBS) besides the electronic message systems (MHS). No wonder, they are on the increase in Hungary too. There is no question about it, however, the average 1,200 bps characterising data transfer speed, together with the present reliability and security specifications of domestic telephone lines, are not offering satisfactory facilities for professional application by users requiring large amount of data transmission as, for instance, public administration. But it is inversely true as well, data transfer using the so-called asynchronous MODEMs are technologically unsuitable for solving the modern information technology tasks at a large scale. In other words, there is a need for digital data communications besides the telephone. The technical performances of the old, analog telephones sufficient for transferring the intelligible speech (bandwidth, noise, crosstalk), but they are too poor for providing communication facilities between servers of local area computer networks, i.e. for the establishment of wide area networks (WAN-s).

Besides the planned quality improvement of the domestic traditional twin copper cables, the establishment of application of other technologies more suitable for data transfer are in progress, such as the twisted 4-core copper wires, co-axial cables, the optical-fibre or microwave links together within the process of changing from analogue to the more up to date digital technology. Even in the short term, according to the experiences gained in connection with the World Expo in Seville, the ratio of voice and data transfer may be 1:1 soon, due to the spread of 'informationalisation' in the everyday industrial, trade and commerce, office and administrative activities.

The significant amount of interurban connections of the non-market-oriented public administration organisations as mentioned above, the large number of different services supplied by MATÁV Rt., also the experience gained by users of own IT infrastructure over many years, the requirements for data security and data protection, these all justify that the information technology requirements of the **Hungarian public administration shall be satisfied by a dedicated private network separated from the public system**.

What does it all mean? It means, in terms of open systems, the provision of independent use of the application and transport oriented layers by organisation. Furthermore it means the joint operation of the network oriented layers, using leased lines and/or virtual digital network from the service supplier market, occasionally own physical layers. All these, based on the existing equipment and network. The requirements for an independent physical network development

considered earlier, based on the example of USA, UK, etc. do not appear justified from the aspect of interurban links. At the same time, the existing cable network in the towns, e.g. owned by the Ministry of Interior, thanks to its quality and capacity could serve several different demands. The large domestic data communications is, due to the lack of really large data bases, only the promise of the future. It seems a handy solution that the recently started modernisation of PABX's (digital PABX purchase) at the main authorities could be the base of a public administration ISDN to be gradually developed, as its 64 kbps speed data transfer channels provide satisfactory capacity for the needs of administration in the long term too. Thus, a study must be carried out to find out whether the network designed to serve the existing and expected public administration IT needs shall operate as an integrated service digital network (ISDN), or as an intelligent computer network. This is not the key issue from the aspect of the end-user. There are from 100 to 600 thousand ISDN channels in three Western European countries with a wide range of international links. However, the short-term plan of MATÁV does not include ISDN. There is more experience in the domestic operation of computer networks. A good example of it is the university, academic society national network with several international links. Due to its size and the cumulated expertise associated with it, it is worth to take into consideration the academic network in the conceptional development of the network for the Hungarian public administration.

5. Conclusion

The use of informatics is unavoidable for the efficient operation of the changing structure of Hungarian public administration in the long term. In a market with expanding supply, public administration, representing different interests whilst being short of funds, can only invest into a system that keeps its value, amongst uniform and regulated conditions. The recognition of this in consideration of networks will result in the establishment of the national public administration network.

6. References

[1] Via Satellite, May 1993, vol. vii. Num. 5. p. 12.

[2] Davis, S.M. and Davidson W.H.: 2020 Vision, Simon Schuster New York, 1991. p.25.

[3] Quoted by Miklós Kamody in his book "100 éves a miskolci telefonközpont" (100 Years of the Miskolc PBX), HTE- Miskolci Postaigazgatóság 1988

[4] Public Network, April 1993. Vol. 3. No. 4. pp.xv-xix

[5] Three-year (1991-1993) telecommunications program of MATÁV published in 1991.

[6] Jánosi, J.: New Giro system in the Hungarian banking world; János Neumann SZT V. National Congress, Proceedings Vol. i. pp. 153-160. Debrecen 21-24 June 1992.

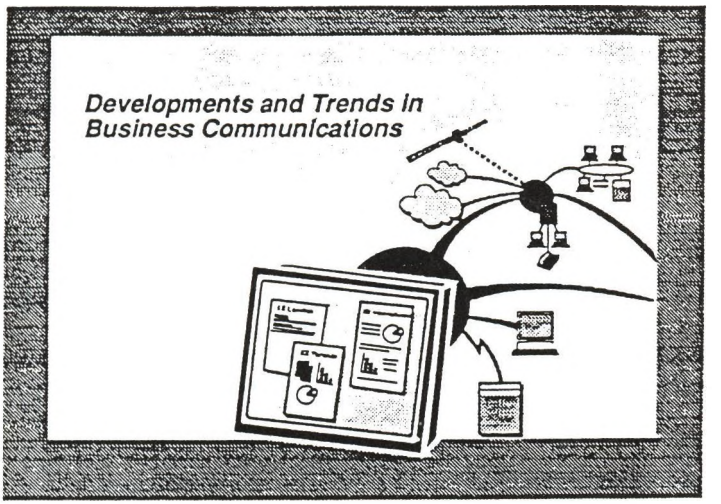
[7] Gerencsér, A.:"Networking '91 The Senior Executive Roundtable on Information Technology and Infrastructure Development in Public Administration" Editor A. Gerencsér, BM kiadó 1992. pp.9-13.

[8] Csaba, L.: Hol tartunk ma? (Where are we now?), Networkshop '93. Conference paper pp.7-16. Pécs 14-16th April 1993.

NETWORKS APPLICATIONS

Chair: V. Haase, Gy. Papp

Developments and Trends in Business Communications



Börje Lindström

Ericsson Business Communications

Scenario of the evolving enterprise network

We are living in the Information Age. Information systems have for some time now played an important part in business life. In fact, a well functioning information system has become a prerequisite for any company of significance.

The typical enterprise network today encompasses a mix of traditional hierarchical terminal-computer architecture and a growing number of Local Area Networks, often of mixed types.

The challenge of a network planner today is to design a network able to encompass a:

multi-desk-top;
PCs, Macs, and workstations are there, alongside the traditional terminal

multi-application;
The network is used for different applications, all demanding their separate needs: high speed, high security, batch traffic and on-line applications -- they all share the same backbone and have to live in peaceful co-existence. In addition, voice traffic as well as video can for cost-reasons share the same backbone network as the data traffic, with the distinct demands that this type of traffic creates.

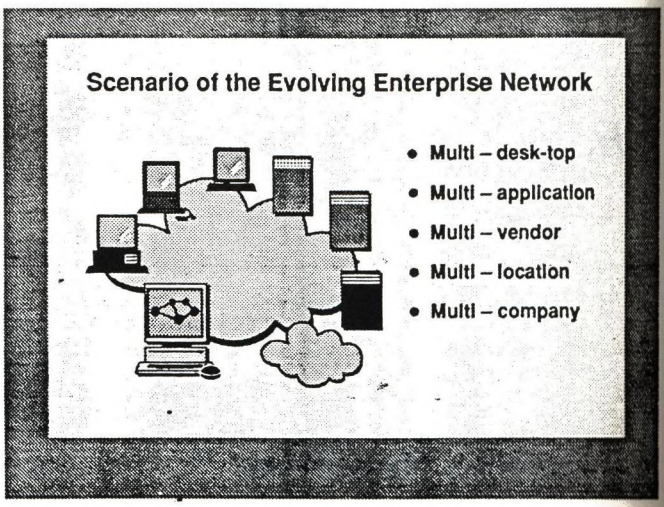
multi-vendor;
Different equipment has been bought at different times, and from different vendors: modern and older equipment with different technologies all have to share the same resources.

multi-location;
Computer Centers are located at different sites in the company, users are spread out over a vast geographical area.

and **multi-company** environment.
the scope of the network spreads into other organizations as electronic data is interchanged across company boundaries.

Conclusion

Openness and flexibility are two very important concepts if one is to meet the requirements for multiple product suppliers and extensibility for the future. Network management will be a key issue in complex networks.



Intelligent workstations

Maybe the most evident characteristic of a network of the nineties is the increased computing power in the local workstation. The intelligent workstation uses images and graphics as everyday tools, in applications where text-only was the only option just a few years ago. Today, the workstation is equipped with user-friendly and understandable features. This means not only that the user has a nicer environment to work with, but also that technically complicated applications are easier to use, and are therefore used more often and by a greater number of people than before.

The traffic pattern from a workstation is different compared to a traditional terminal which behaves more predictably. Some characteristics of a workstation:

Windows;
The workstation can use windowing techniques to work with multiple tasks at the same time, local or remote;

Graphics with full color;
Graphic files are a great deal larger than text-only files.

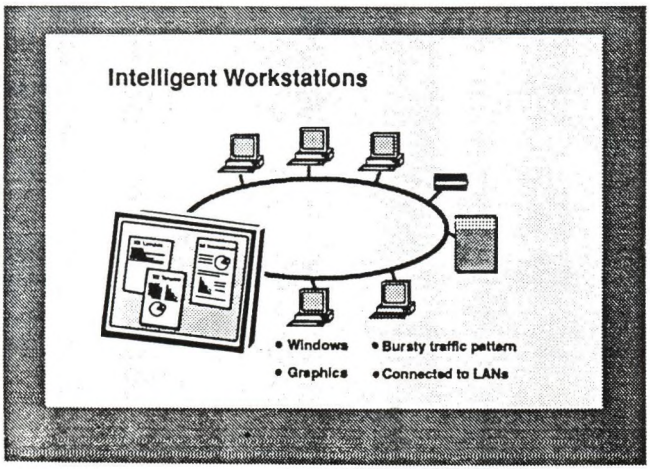
Bursty traffic pattern
Workstations frequently exchange files or download programs from the file servers in the network. Programs or files can be fairly lengthy and require bandwidth - at least momentarily when the transmission is taking place.

Local Area Networks

A parallel evolution to the "PC revolution" is the increased use of Local Area Networks. The LANs are used to connect the workstations to access common resources such as printers, file servers, or to exchange information. The use of LANs is expected to increase in the nineties, leaving only a few per cent of the total PCs used unconnected.

Conclusion

Communication patterns of the nineties have changed from screen-oriented transactions to bandwidth-demanding image-oriented transactions. This trend comes from the increased power in the workstation, but has been made possible because of the characteristics of the Local Area Network (LAN). The LAN's are used to connect the workstations to access common resources such as printers, file servers, or to exchange information. The high-speed LAN (4-16 Mbits/s) is able to handle the increased workload from the intelligent workstation, and the flat information structure of a LAN is well suited for the emerging applications.



The client-server model

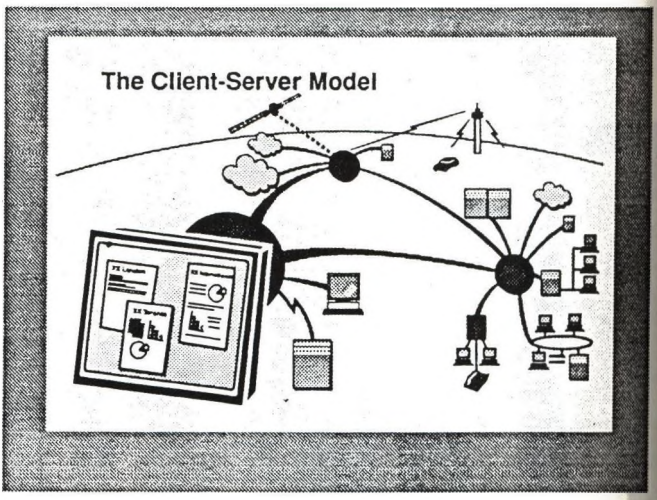
The client-server model is an overall framework for designing applications and network architectures. It is, in a way, the opposite of the traditional host-terminal relation, where all processing and storage was situated in the Mainframe.

The idea with the client-server model is to take advantage of the increased cost / performance ratio in PCs and workstations, moving the processing of information closer to the end user. Most interactive transactions are served locally, which means that the user can work with the PC-program he is familiar with. The local workstation acts as the "client". The network is used occasionally, to transmit queries or data subsets to the "servers", probably a Mainframe. Processing requirements and data are transmitted as one entity across the network, creating a traffic pattern quite different from the traditional host-terminal applications.

Conclusion

The historical transaction consists of a line into the host and a screen of data back to the terminal -- a very moderate amount of bandwidth being needed for this. The client-server environment, however, can generate bursts of bandwidth of several Mega-bytes, only to leave the line idle a couple of moments later.

A well-functioning network is a prerequisite to access relevant data in this environment. The network can actually be thought of as a part of the computer itself; the network effectively acts as an "extended bus" connecting the different processors together and enabling them to act as one larger computer. The network is, however, transparent in the process: locations or types of processing environments are not of importance to the application. The term "client-server computing" is used to reflect the new way of looking at the information the computer contains, rather than focusing on the machine itself.



The hunt for bandwidth

The intelligent workstation uses images and graphics as everyday tools, and several new "bandwidth-hungry" applications have arisen with characteristics which directly impact the network. The file types typically sent by these applications require higher speed networks in order to give reasonable response times. This table demonstrates the difference in response times on a 64Kbits/s link, traditionally used in many Wide Area Networks, and a 2Mbits/s line:

File type	64 Kbits/s	2 Mbits/s
2 pages of text	1/4 second	1/100 second
1 page spreadsheet	5 seconds	1/6 seconds
1 page drawing	12 seconds	1/3 seconds
PC program	1 minute	2 seconds

Below are a few examples of applications requiring large peaks of bandwidth. Characteristic of all of them, is the bursty nature of the applications: When they use the network, they need a large peak of bandwidth momentarily. In between these peaks, they perform processing locally, and do not use the network at all.

CAD/CAM

CAD/CAM applications (Computer Aided Design / Computer Aided Manufacturing) are bandwidth hungry in nature. A CAD file can typically be several Mbytes. In the application lies also a need to transport the CAD file to a machine where the construction is to take place, the CAM-part.

Compound Documents

Compound documents is an example on how the enhanced workstation is used to create documents that can include images as well as text. An example is a sales report. Instead of merely writing down what has happened, a sales report today can consist of text, data from a spreadsheet program, and a graph to describe results. This complete file can be sent over the data network to be collected centrally.

Electronic Data Interchange

Electronic Data Interchange is a growing application, making exchange of information more efficient. For example, instead of sending orders from company A to company B, writing it down on paper and sending it by mail, the companies A can through a network transmit the information electronically, reducing the paperwork and speeding up routines.

EDI is not necessarily bandwidth-demanding. It all comes down to what types of information are being sent in the electronic document. A page of text does not demand a lot of bandwidth. But, as soon as there are graphics or spreadsheets involved, the size of the file sent can easily increase by a factor ten or more.

Interactive Multimedia

Interactive multimedia is something that is going to be increasingly used in the latter half of the nineties. Interactive multi-media applications allow users to create interactive presentations that include not only text and image, but also moving pictures, music or voice applications. This opens up a new world for marketing, training, trade-show presentations etc. Interactive multi-media is very bandwidth demanding, especially with moving pictures, coming very close to video quality.

Image Applications (X-ray Pictures, etc)

Image processing, e.g. used by hospitals and medical institutions to send digitized images of X-rays, is becoming increasingly popular. Image processing can at times use a tremendous amount of bandwidth. Yet, since the bandwidth is only needed sporadically, the application is extremely bursty in nature.

Extensive communications networks

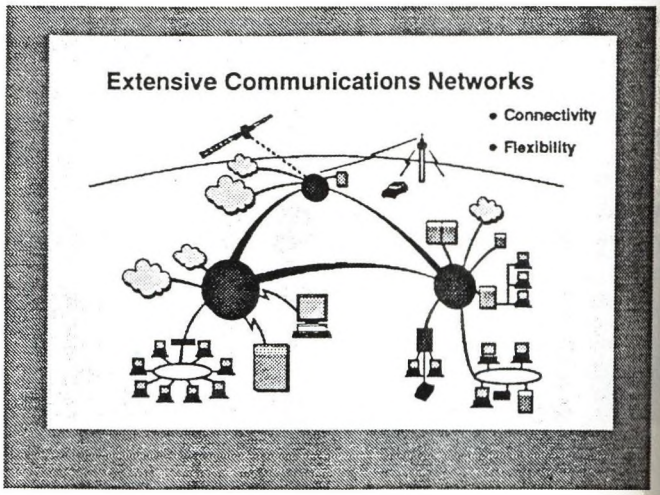
Entering a global marketplace, the information system will have to become global, too. In the case of multinational firms, the network will in many cases become the base for operation, enabling geographically dispersed organizations to exchange information, cross borders and time-zones. The communications network has to be able to handle a multi-vendor environment, and be **flexible** enough to handle any future mergers or acquisitions the organization might experience.

However, for the network of the nineties, communications is not only an internal issue. The information system will have to have interconnection to external networks, or to other private networks. The network might have these extensions to reach interesting data at other sites, or the network might extend to the customer site to link the customer closer. **Connectivity** will be a key word, whether it is driven by the need for applications such as Electronic Data Interchange, Electronic Mail or searching through databases, all over the world.

Out-sourcing, i.e. leaving parts of the network to be controlled by another party, is becoming increasingly attractive as companies would like to extend their networks, but do not necessarily have the resources to handle it by themselves. With the deregulation of the PTTs in Europe, new carriers are emerging to serve customer needs. The borders between what is public and what is private is slowly diminishing, and the demands on network security and integrity as well as on management will be even higher as networks have to adapt to this new situation.

Conclusion

Flexibility in a network is crucial, to handle the changes and the evolution of the organization. Connectivity is also a key issue in a network of today. The market for network services will increase during the next years, both public transport services and a wide spectrum of value added services. These services will be attractive for companies with private networks and create requirements for integrating these services into public or "semi-public" networks.



Management

The importance of efficient network management will sharply increase during the next few years.

This is due to the increased
- sophistication of enterprise networks; and
- the ever increasing reliance on communication.

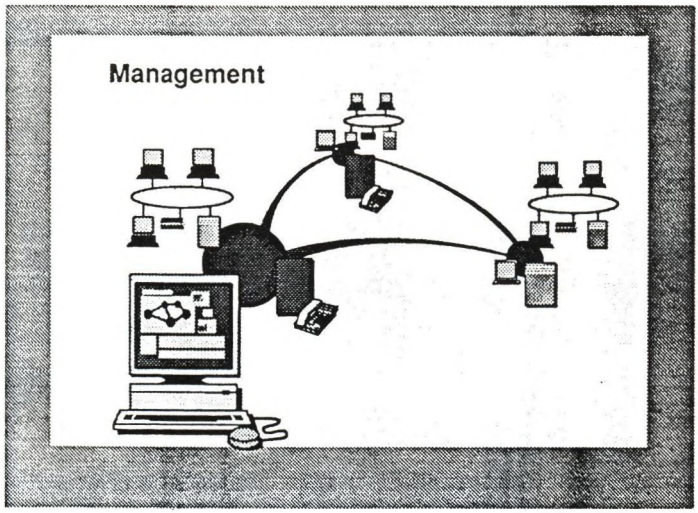
In many organizations it will be easy to see the amount of business lost due to failing communications, even if the system is down only for seconds or minutes.

Backbone networks are more and more multi-service oriented. We will see hybrid technology networks, serving LAN users as well as terminal-host and host-to-host applications. Voice networks may in some cases share the same transportation network. In addition, users are increasingly turning to services both in the public network and in other private networks, which makes traffic patterns even harder to predict.

On the economic plane, significant advantages are expected:
- For network operators, the development of modern management tools promises considerable productivity gains, in operations and personnel.
- For the network "owner", the advantages are being able to manage increasingly complex multi-service networks and mastering interconnections between private and public networks, permitting maximum tradeoffs between them.

Conclusion

Network management is more important than ever. Being able to control the network of today and tomorrow, and all the phases in between, requires major consideration in the choice of network management systems.



LAN, MAN and WAN – terminology overview

Before we go any further on the LAN interconnection issues, let us stop for a minute to sort out the terminology.

A **LAN**, or a **Local Area Network**, is a network within an office, a building or a small area designed to connect intelligent workstations to common servers. Effectively the term LAN is now only used for a specific type of local area network which conforms to the standards defined by IEEE 802-committees. A LAN operates at speeds typically between 4 and 16 Mbits/s.

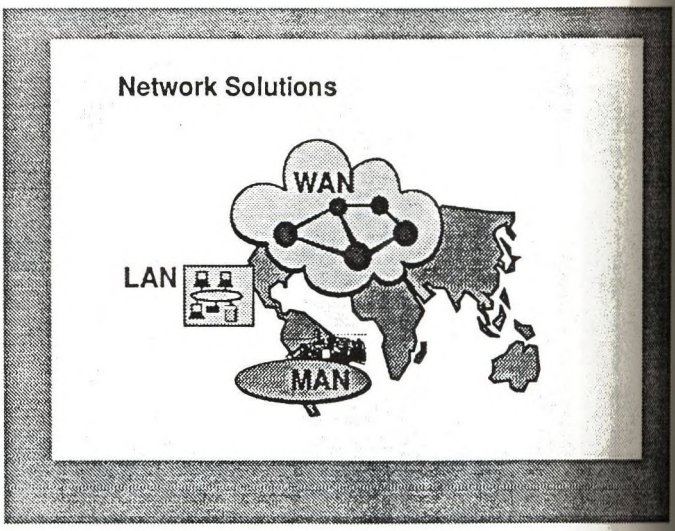
A **WAN**, **Wide Area Network** is a voice/data transmission facility connecting geographically dispersed sites via long-haul networking facilities. Wide area data networks were originally designed for a host-terminal-type application, although technology has evolved over time to encompass new applications. Typically, the WAN uses 64kbit/s but speeds up to 2 Mbits/s or more are possible in the newer wide area data networks.

A **MAN**, **Metropolitan Area Network** was originally designed mainly for interconnecting LANs over a limited geographical area, such as a campus or a city. (Sometimes, smaller MANs are referred to as Campus Area Networks) The MAN technology is designed for:

- medium distances
- high speeds (more than 100 Mbits/s); and
- diverse forms of information (voice, data, image, video).

Blurring of the borders

As the price of lines -- especially prices of high-quality, high-speed digital lines -- drop, LAN, MAN and WAN borders are getting very blurry. LAN and MAN charachteristics are propagating into the WAN world as we move towards the next century.



LAN interconnect

The evolution of LAN technology and the increasing use of LANs in companies has been quite dramatic in the eighties and the trend will continue through the nineties. LANs of many sorts, using everything from twisted-pair cable to hyperfast optical fiber, have found their way into offices and labs. Internetworking protocols, therefore, are now a necessity. This "internetworking of networks" takes place within single buildings as well as across continents as corporations attempt to provide access to electronic files, services and resources.

Internetworking technology has yielded three types of products: **bridges**, **routers** (and combination products of the two). or **gateways.**

Bridges

A **bridge** connects two LANs of the same type and protocol on a one-to one basis. A bridge enables two LANs to form one, logically unified network. Bridges operate at the Media Access Control (MAC) sublayer of layer 2 of the OSI model. Forwarding decisions are based on the MAC-layer addresses only, enabling multiple protocols to be used transparently across the bridge. Bridges are typically used to connect networks with the same physical and MAC protocols, e.g. Ethernet - Ethernet or Token Ring - Token Ring.

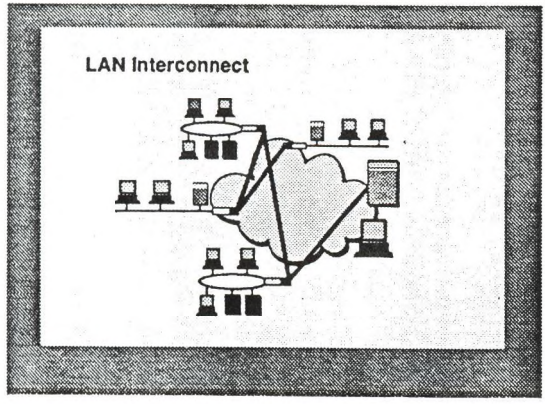
Routers

Routers operate at the network layer (layer 3) of the OSI model. A router forwards packets based on information in the header of the used network layer protocol. Because the information in the network layer header is specific to each protocol (such as IP, IPX or XNS), the router is protocol dependant. Routers may support several protocols, and they can connect LANs and other networks with different physical and MAC protocols. Routers, as opposed to bridges, interconnect separate subnetworks rather than forming one logically unified network.

Gateways

Gateways operate up to level 7 in the OSI protocol stack and thus provide a link between dissimilar architectures. For example, the gateway can be used to connect a workstation on a LAN to a host computer. This require protocol conversion, e.g. NetBios to SNA, and thus the gateway perform this conversion.

Other applications (e.g. electronic mail and EDI) can also be achieved via a gateway. The gateway must contain both the OSI version and the proprietary version of any application requiring gateway services.



The transition to broadband

Leased lines, multiplexers, router networks, X.25 switches, frame relay switches and Cell Relay technologies -- it is not an easy task to find the way through the technology jungle of the nineties. In fact, maybe the only thing a network planner is sure of, when he makes a major network investment, is that the network is going to change, and grow over time...

The *Yankee Group*, an American communications consultancy company believes that by 1996, all major long-distance carriers in the U.S. will have deployed a network platform so that Asynchronous Transfer Mode (ATM), SONET/SDH and and Switched Multimegabit Data services (SMDS) will be a reality.

The Yankee Group continues:

> *"Even though this acronym laden list of future services sounds great, we have to put our reality hats on and realize that broadband will not truly "arrive" before 1995. Although the carriers are beginning to talk in concrete terms about broadband, no one is exactly sure what switching fabric, equipment platform, or even speed will drive the broadband networks of the late 1990s."*

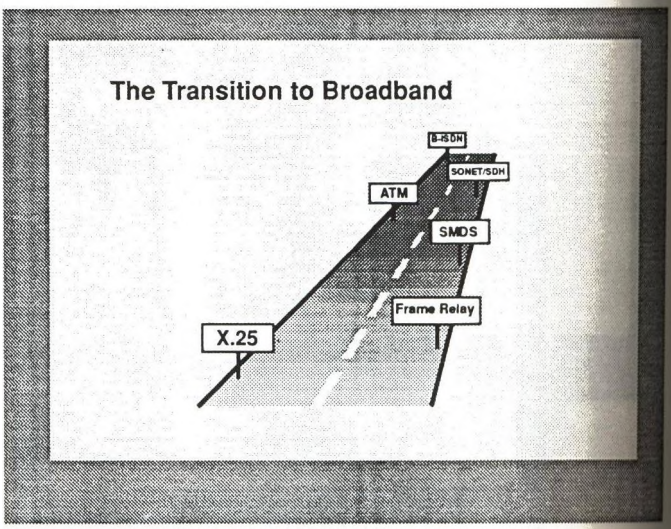
The key here is, that at the moment, there are a number of user requirements that have to be fulfilled, and they cannot wait for emerging technologies to come. What we, Ericsson, offer, is a backbone network that can satisfy current user requirements while simultaneously laying the foundation for the transition to the broadband world.

Frame relay and X.25 are two services that will become a very important part of this transition.

Conclusion

As tomorrow´s switching techniques are not here yet, and because they are really not needed at all times, the solution is to find a partner in networking that can show a future-proof solution that also works today.

Ericsson provides a safe migration strategy from existing technologies towards tomorrow´s switching techniques, via X.25 and frame relay.



X.25 packet switching

Packet switched X.25 networks use a communications technique where a message is broken into packets. This packaging of data allows a user to get bandwidth on demand, as much as needed, so the protocol uses bandwidth in a more efficient way compared to the multiplexer. The connection is one-to-many. . X.25 carries data only, and the traffic either follows the X.25 protocol, or a PAD function has to convert existing protocols to X.25.

X.25 is popular for its cost-efficient switched communications service. However, X.25 was developed in an environment where most traffic was terminal to host, and where high quality lines were not necessarily available. This is why X.25 goes to great length to ensure that transmission errors are corrected on a link-by-link basis, thus delaying the packets through the node. These error correcting procedures are not necessary when transmission lines are of good quality and the end-points have error checking protocols themselves. Different applications have of course different requirements on the network, and X.25 still has some major advantages:

Reliability
The fact that X.25 offers a reliable service by performing error correction is a drawback from a throughput point-of view. However, emerging technologies without extensive error control rely on high-speed / high-quality lines. This is not always a reality.

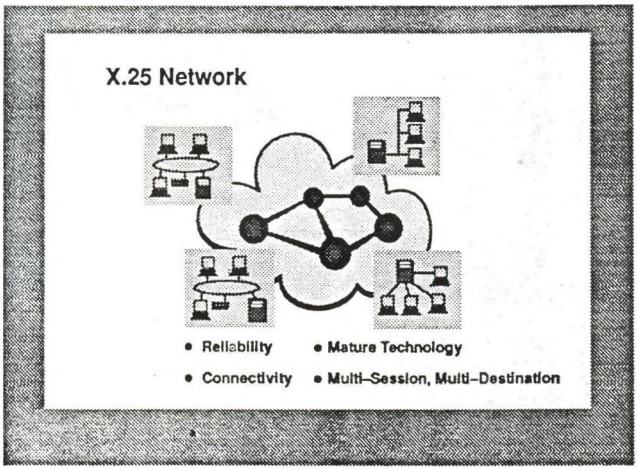
Connectivity
X.25 offers excellent cooperation with public networks. On the international arena especially , there is really no reasonable alternative.

Mature Technology
X.25 has been here for quite a while. All major computer vendors have excellent support for this way of transporting data, giving the user freedom of choice and vendor independence.

Multi-session, multi-destination
The real properties of X.25; multi-session and multi-destination are going to be even more used in the nineties, as intelligent workstations really can take advantage of these benefits.

Conclusion

X.25 packet switching networks carry more overhead than a multiplexed solution, but give outstanding advantages on reliability. It is a world-wide and well accepted standard.



Frame relay

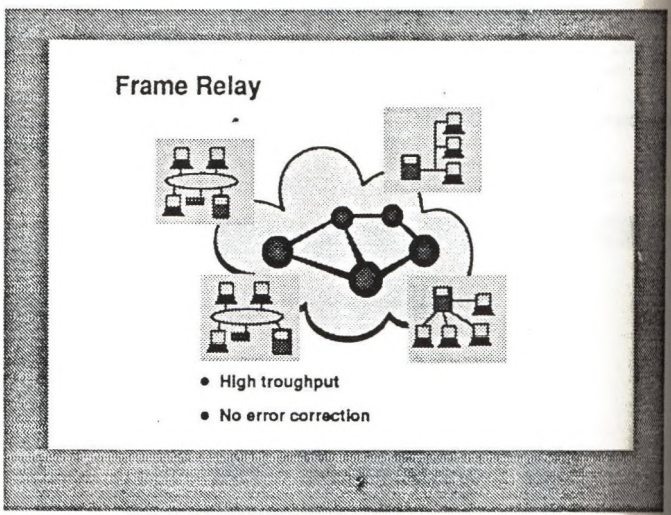
In order to combine the idea of bandwidth sharing used by X.25 networks, with the higher speed, and lower delay communication of circuit switched networks, a new technology has emerged. It is called **frame relay** and it has traded off some of the congestion and error recovery procedures of packet switching to gain the lower delay and higher speed capabilities of circuit switching.

Frame relay distributes bandwidth on demand by sending the data in frames. A frame relay end-point gets as much bandwidth as needed, when needed. This gives a substantial enhancement in bandwidth utilization, especially compared to router network previously connected via leased lines. With frame relay, several routers may share the same 2 Mbit trunk, which has proven an improved bandwidth utilization of as much as 60%.

The frame carries address information and gives a one-to-many connection possibility. However, unlike X.25, the frames pass a minimum of control through the network node, following a simple "if it is not correct - discard it" - instruction. The correction of errors is trusted by the end points. This increases throughput and minimizes delay. But the success of a frame relay network is dependant on a high-quality link: otherwise retransmissions end-to-end of discarded frames can really slow down the response times.

Conclusion

Frame relay combines "the best of circuit switching with the best of X.25". The combination of the bandwidth efficiency and high throughput certainly makes it better for specific applications, typically interconnecting LANs, over low bit-error rate lines.



Frame relay

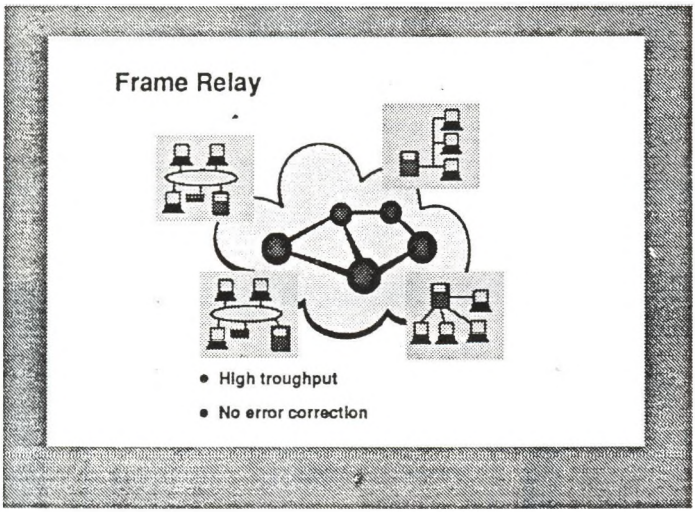
In order to combine the idea of bandwidth sharing used by X.25 networks, with the higher speed, and lower delay communication of circuit switched networks, a new technology has emerged. It is called **frame relay** and it has traded off some of the congestion and error recovery procedures of packet switching to gain the lower delay and higher speed capabilities of circuit switching.

Frame relay distributes bandwidth on demand by sending the data in frames. A frame relay end-point gets as much bandwidth as needed, when needed. This gives a substantial enhancement in bandwidth utilization, especially compared to router network previously connected via leased lines. With frame relay, several routers may share the same 2 Mbit trunk, which has proven an improved bandwidth utilization of as much as 60%.

The frame carries address information and gives a one-to-many connection possibility. However, unlike X.25, the frames pass a minimum of control through the network node, following a simple "if it is not correct - discard it" - instruction. The correction of errors is trusted by the end points. This increases throughput and minimizes delay. But the success of a frame relay network is dependant on a high-quality link: otherwise retransmissions end-to-end of discarded frames can really slow down the response times.

Conclusion

Frame relay combines "the best of circuit switching with the best of X.25". The combination of the bandwidth efficiency and high throughput certainly makes it better for specific applications, typically interconnecting LANs, over low bit-error rate lines.



Cell relay

The next generation of switches will be based on cell relay technology. Cell relay is used as an umbrella term for technology used in B-ISDN and MAN technology and because of its fixed cell length format, is practical for integrated voice, data or video applications. Cell relay networks will be able to carry traffic at speed up to several gigabit, because of the very efficient switching technology.

There are two different implementations of cell relay being developed in parallel:

- **ATM**, Asynchronous Transfer Mode, which is for broadband ISDN (B-ISDN)
- **DQDB**, Distributed Queue Dual Bus, which is for SMDS Metropolitan Area Networks.

It is important to distinguish between technologies and services:

SMDS (Switched Multimegabit Data Service)

SMDS is a service to interconnect Local Area Networks over a metropolitan area. SMDS is a new, public service offered by some of the Regional Bell Operating Companies in the US. Users can use the **DQDB** protocol to access the service.

It is believed that ATM technology (when available) will be used as a *switching* technology in an SMDS network, although DQDB is currently used both as the access and the switching protocol in SMDS networks in the United States.

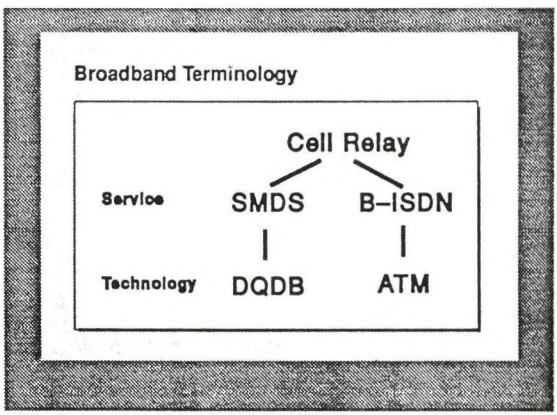
B-ISDN (broadband ISDN)

B-ISDN is a public, and not yet existing service. B-ISDN, when installed, will give the user access to a range of voice, data and image services, at gigabit-speeds. However, B-ISDN requires a new infrastructure to function. Up till now, focus on the B-ISDN service has not been on the services that will be offered, but rather on the technologies "behind" it:
- the transmission format; **SDH (SONET)**
- and the information transfer mode; **ATM**.

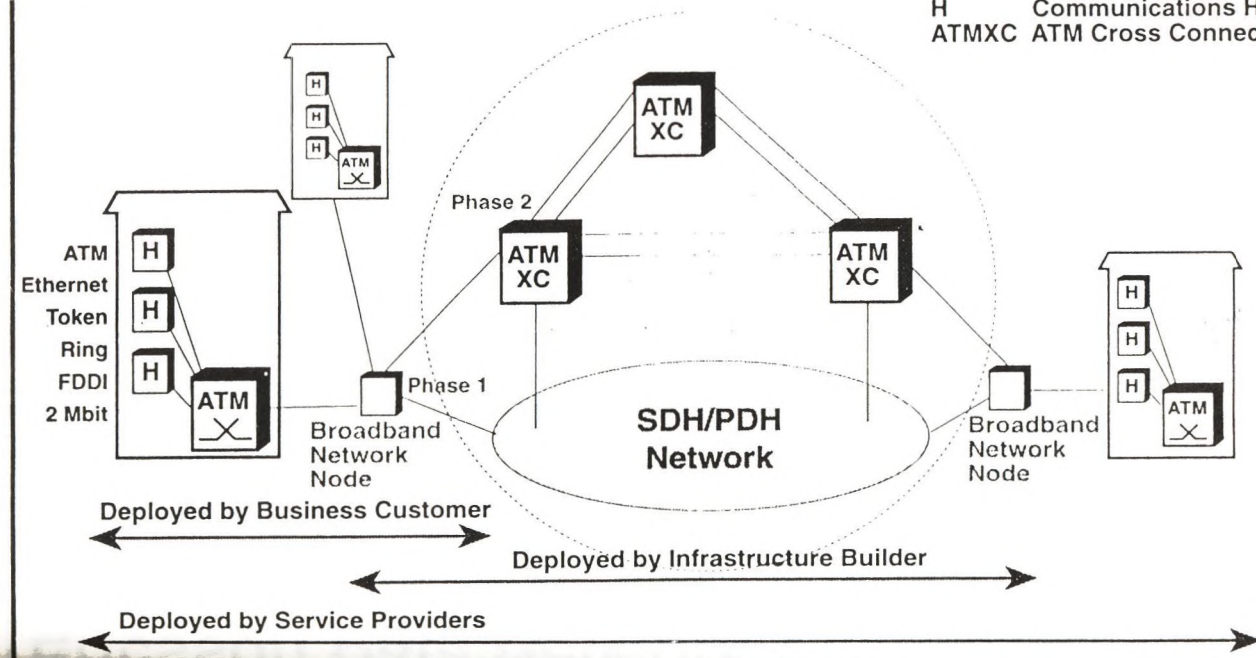
Initially, ATM and B-ISDN were used in an almost equivalent fashion, which was very unfortunate. Today, everybody should understand the difference between B-ISDN which is an infrastructural concept, and ATM, which is an information transport mechanism: a high speed packet-mode information transfer.

Conclusion

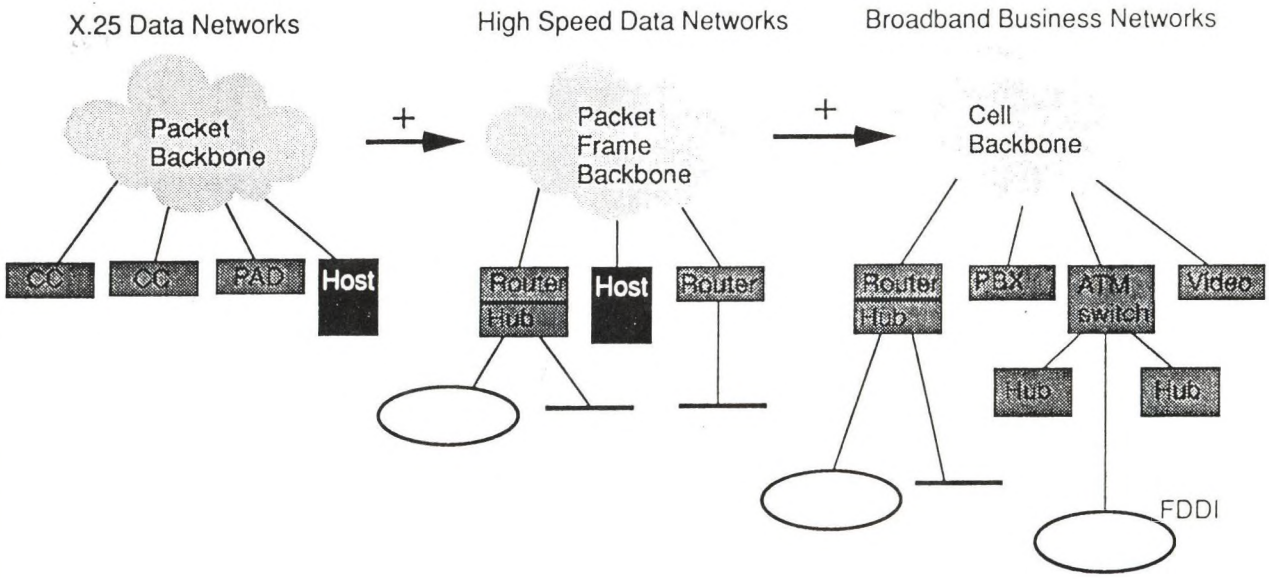
The implementation of cell relay, compared to frame relay, is further in the future, as *cell relay requires a new generation of hardware technology*. Cell relay implementations in public networks are planned for the mid to late 1990s.



Deployment of ATM into the Network, First Phases



Ericsson Data Network Evolution



The network jigsaw puzzle - a case study for Hungarian players

(Stages of development in the Hungarian R&D network)

István Tétényi

Computer and Automation Institute
e-mail:h050tet@ella.hu

Abstract:

The difference between a jigsaw puzzle and the evolution of a research network is obvious. In spite of this the author's conclusion is that solving networking problems is similar to fitting together pieces of a jigsaw puzzle. In this paper the author points out to some of "jigsaw pieces" and the way these were fitted together in the Hungarian R&D network.

Preface

The difference between a jigsaw puzzle and the evolution of a research network is obvious. In spite of this the author's conclusion is that solving networking problems is similar to fitting together pieces of a jigsaw puzzle. Brave souls even can refine this picture for multidimensional puzzles. They will not be far from truth.

The similarities of the industrial revolution and the communication revolution of our age are astonishing. The **old** story started with the steam engine, the railways, etc. Our one started with simple data communication equipment like modems and continued with switches. Both lead to the establishment of networked infrastructures.

It is also common-sense that within one or two decades our continent became networked first with railways now with computers.

The somewhat delayed introduction of the networks throughout Europe is also a common characteristics.

In this paper the author points out to some of "jigsaw pieces" and the way these were fitted together in the Hungarian R&D network.

Introduction

The Hungarian R&D network has a long history. It spans at least seven full years.

The story had started back in the mid seventies. That time different small groups started the development of academic/research networks. Between 1977 and 1987 there were very many abortive attempts to establish the hardware and software platform of networking. By 1987 the first X.25 switch and PAD was developed. No one at that time thought that **history** begun. The very first puzzle element was put on the table. The question was what to do next.

This paper has an unconventional structure in order to identify the problems, dilemmas and also to draw attention to the selected solutions and its consequences.

1. Highlight of the events

1987. Network access equipment
1988. Semi public X.25 network for IIF
1989. Service over X.25 - ELLA/e-mail
1990. International e-mail connectivity
1991. Bitnet, Lan client for ELLA
1992. first IP networks, Bitnet proliferation, e-mail gateways,
1993. HBONE, regional centres, X.400, X.500, client/server applications, USENET news, FDDI networks

2. Network evolution in an isolated era 1987-1990

♦ Select piece:
Is it necessary to set-up a networking organisation for R&D networking or not ?

The set-up of Information Infrastructure Programme in 1987 was a corner stone from organisational point. It is now obvious that the establishment of IIF programme was in-line with similar academic and research network organisations of that time like JANET, DFN, or SURFNET.

♦Select piece: DECNET phase III/IV or X.25

DECNET networking was important in the 80's. Cocom restrictions were strict so computers with networking facilities could only be illegally imported. The price of clone VAX/DEC machines was also high. The development of a home grown small X.25 switch with PAD eased the choice.

♦Select piece:
Private R&D network or PTT operated network for the R&D community

The choice was - and still is - difficult. Should we buy switching services from a service provider or should we lease lines. The question can be reformulated: with or without the PTT shall we set-up a research network.

My guess is that organisations can successfully operate their private data network only in those countries which already have their own digital-optical overlay network. The maze of leased analogous circuitry can not be operated by an outsider. Therefore it was reasonable to decide in favour of a PTT operated network.

We found out later that the management of **just one** leased, analogous, international link between Budapest and Linz was very difficult for the Hungarian PTT. We "enjoyed" more then 25 percent average down time.

Imagine the consequences of the opposite choice !

• Corollary I.: How to meet the requirements of a PTT operated X.25 switch

My personal view is that one of the greatest technical achievement of the 80's in Hungary was the SOKBOX X.25 switch. Its modular design, flexibility in configuration, its performance, its network management functions and the smaller and bigger tid-bits altogether made it a great success. Many thanks to the original developers. The Hungarian PTT still uses the original switch which was put into operation in late 1988.

• Corollary II.: Can we use it internationally ?

The international interconnectivity was one of the hot issues for the Hungarian R&D community. Being an ITU member Hungary was allowed to connect its public X.25 network to that of the rest of the world. So a big **YES** is the answer.

♦ Select piece:
.Own applications vs. OSI applications vs. de facto standard applications

In 1988 the latter two options were not viable due to its unavailability, etc. By 1988 a home grown X.25/X.29 based solution was developed. The ELLA e-mail system was invented. A protocol was

designed. It can now be classified: it has the functionality of the Internet IMAP protocol from 1992, but it was designed and implemented in 1988 ! During the same period the JANET network pushed its own "coloured book" protocols.

The operation model of ELLA is a client-server one. A PC based client with Hungarian user interface, with built in directory, mail groups, confirmation of reading, and the option of sending messages in binary or with accented characters (in Hungarian) still could not be matched. Mind you: over the last six full years the number of registered ELLA users grow to more then 8000 with the daily traffic of over 5000 messages.

Other applications - based on similar approach - were developed like a bulletin board and a common file store for public information.

The results has justified the choice.

- Corollary: Select the server platform

The platform choice was IBM 3031 with VM/SP. The X.25 connectivity for the IBM machine was developed on home grown equipment and protocols. Network application programming experience was rare, examples were not available. Notions like sockets, streams or transport level interface were unknown.

Results of phase one

By 1990 Hungary entered the group of nations with its own R&D network, network organisation, with a PTT operated semi-public X.25 network, with services like E-MAIL and remote login, and with databases to provide information through networks.

3. Network evolution since 1990

The political changes have speeded up the growth of the R&D network. It also has created a better climate for co-operation with western R&D organisations like EUnet, EARN, RARE, Aconet, Ripe, etc. The Cocom regulations slowly melt away. Different sources of support became available like PHARE, etc. The introduction of TCP/IP technology became a very significant driving force. Managed LAN-s, big campus networks, MAN-s based on FDDI or ethernet, and the HBONE project are all signs of a very rapid expansion of networking in the R&D sector.

- Fit piece: Extend services for LAN-s - 1990

The very first LAN-s appeared by the end of the 80's. It became obvious that users on the LAN's wanted the same services as the users connected to the PAD interface of the X.25 switch. So the idea

of having PAD services over LAN became necessary. It allowed the users accessing ELLA and X.25 related services on LAN-s.

• Fit piece: Proliferation of LAN-s - since 1991

The proliferation of LAN-s became one of the biggest driving force for R&D networking. To have managed LAN-s, quality cabling, stable services on a LAN was easier to require than done. Fortunately private enterprises had been set-up with the very type of services on their offer. Cabling and LAN provision is not an issue anymore. One can easily choose from at least 5-10 reliable supplier.

One of the most important consequence of the set-up of LAN-s was that the importance of servers for users grow significantly. The R&D community usually choose TCP/IP, Novell, Decnet protocols on the LAN. It has become a commonplace that TCP/IP offers the most homogenous services between different platforms.

• Fit piece: Proliferation of services over X.25 - 1991/1992

The availability of X.25 throughout Hungary, the special charging agreement between IIF and PTT served as a sound basis for building up services over X.25.

In excess of the traditional IIF services - like ELLA/MAIL, remote login, X.25 services for LAN - new type of services was introduced in the period of 1991/1992.

• Piece No 1: BSC over X.25 - since 1991

The encapsulation of BSC protocol to X.25 allowed BITNET's NJE/BSC traffic to be used over packet switched networks. BSC protocol is not "supposed" to run over X.25 unless there was no other option. The JATE - a big university in Szeged - became one of the very first EARN nodes in January 1991. Colleagues from Szeged has reassured me many times about the impact of EARN services had made on informatics teaching, usage in the past two and a half years.

• Piece No 2: SLIP over X.25/X.29 - since 1991

SLIP over PAD is one of the unconventional solutions. However sites with simple PC connected to X.25/X.29 equipment use it. It turned to be a quick and cheap solution.

• Piece No 3: MAIL-11 over X.25 - since 1991

Mail-11 is an option of sending - receiving mail between VAX computers with DEC's X.25 package. This is now obsolete due to the MX package. It is still in use in some sites which has not upgraded to VMS 5.0.

- Piece No 4: SMTP over X.25 - since 1991

SMTP over X.25 is an RFC. The MX mail exchange package has a support for it. This functionality has allowed to provide stable RFC-822 mail for many sites connected to the X.25 network. There are roughly 30 institutions in Hungary who opted this solution.

- Piece No 5: Decnet over X.25 - since 1992

The idea of having a nation-wide Decnet was many times dismissed. However at least five sites run a co-ordinated Decnet IV. This piece also have been successfully fitted.

- Piece No 6: NJE over X.25 - since 1992

Network Job Entry is Bitnet's store and forward protocol. NJE is widely used in some universities. The number of NJE over X.25 sites is more then five. These sites consume at least 35 percent of the total IIF X.25 monthly traffic.

- Piece No 7: TCP/IP over X.25 - since 1992

TCP/IP over X.25 was debated in the past. It turned out that the limitations at the available X.25 access speeds - max. 128 kbit/sec - do not constrain the usage. Practice has shown that sites with 9.6kb/s access speed can enjoy 6600 bit/s FTP rate. Keeping in mind that PTT actually shares the X.25 links between its customers this result is noticeable.

◆ Select choice: Separate mail protocols/systems vs. integrated IIF mail

One of the biggest issue in late 1991 was the formulation of the e-mail concepts of IIF. The question was: should we select only one mail transport protocol and mail application protocol or can we have a heterogeneous system with mail gateways between them. At the time of decision the platform was not selected on which a gateway could be operated. The final decision based on the MX package which do have SMTP, SMTP/DECNET, SMTP/X.25, BSMTP/NJE, UUCP mail transport option. The ability of extend MX with user defined gateways for protocols had also great importance. We could integrate ELLA to MX and could establish an integrated IIF mail system. The adoption of RFC-822 addressing was a fairly obvious choice.

We were reassured in our right choice in Spring 1993 when it turned out that MX was scaleable for higher traffic. It was just ice on the cake when we understood that NORDUNET uses the very same solution under the command of Eric Thomas the "Listserv/kid".

Of course all these knowledge could not have been gained without the integration of Hungary to the Internet/BITNET networks.

• Fit piece: Integration of users on Novel LAN-s - 1992/1993

Novell LAN-s became very popular in Hungary. It was not clear how users on Novell LAN-s should be integrated to the world of e-mail. There are many solutions to the problem. One of them is that ELLA is usable with a gateway on the LAN. Another option has emerged: the Pegasus Mail with Charon or Mercury programs. Users found it very beneficial.

• Fit piece: International mail transport strategy - since 1991

Users in a network first enjoy a new service. Later they try to benefit from the very limits of it. Services like BITFTP, TRICKLE, USENET News, and very active e-mail lists can overload links at low speed. We needed in spite of the heavy loads a reliable service, with guaranteed delivery. BITNET's store and forward mechanism, with its BITNET II structure and with Listserv is the "goods train" which secures the constant flow of vast amount information internationally.

• Fit piece: Regional centres - since mid 1992

The concept of a regional centre was envisaged in early 1991. A regional centre is a centre of networking excellence which could provide services for a region. The regional centre in itself is a typical configuration of networking equipment which is a unit of service. It consists of a Unix server, workstations, X-terminals, TCP/IP, X.25 connectivity, with X.400 and SMTP e-mail functionality.

It is obvious that the networking activity at the first sites has been improved significantly. In 1993 another 20-30 regional centres are to be purchased.

• Fit piece: Educate users - since 1992

At present there are two co-ordinated way to improve the knowledge within the community.

One is the Networkshop organised yearly. It's programme is a mixture of the Joint European Networking Conference and the User Services Conference. Technology and services are both on the programme. Exhibitions are also held accompanying the conference to tighten the connection between vendors and community.

The second is the support of network schools for users. This school do have a three weeks long programme which include many aspects a computer networks. Special support is also available for Unix courses, etc.

In addition to this, one should not forget about the significant help Hungary has received from many organisations in the form of education. ACONET and INFN in Trieste were the most remarkable organisers of international network schools.

- Fit piece: Software purchase

The Hungarnet association was established in 1992. Its members are all the non for profit institutions. In order to achieve a bulk purchase price for software several steps had been taken. The notion of campus licence has been extended for the whole Hungarnet community. Special agreements has been reached which Digital, IBM, Sun.

- Fit piece: TCP/IP applications for users without TCP/IP connectivity

One of the biggest challenge in R&D networking in Hungary was to provide services to every member of community. Novel services appear on one network but members of a different network/organisation cannot benefit from it. The classification below tries to ease the selection.

Categories

Class I. full member of a network
- full access to services provided in the network
E.g. member of Internet, Bitnet, EUnet

Class II. relayed access of network services
- mail with enhanced features - like Trickle
- the original service remains hidden but its results relayed or gatewayed or converted for the user
E.g. BITFTP, Trickle

Class III. Client access of a network service
- partner in accessing services

Category I. and II is not a novelty. Solving the problem of Category III. is a big step forward.

The original intention was to provide News reading access to every member of the R&D community. Solutions belong to Class I or Class II can not be generally applied to **every** member of the community. We have recognised that Unix machines with TCP/IP, DECNET, X.25 connectivity can be general servers for the whole community. The key of the solution is that TCP/IP client programs run on UNIX servers. The UNIX clients built to use only the UNIX curses interface. The clients can be activated with logging into the servers from remotely. The only thing what is needed from the user side is a simple terminal emulation. Consequently the importance of remote login has been increased again.

The table below is a summary of the access unit, access protocol, network protocol, and network service quadruple. It describes a path on which the IIF network and users got through.

access unit	access protocol	network protocol	network service
PC/RS-232	PAD	X.25	X.25 services
PC	PAD	ELLA/X.29	e-mail
PC	PAD	Trilla,3270/X.29	bulletin board
PC/LAN	PAD/LAN	Trilla,3270/X.29	bulletin board
Unix	PAD	ELLA/X.29	e-mail gw.
VAX/VMS	PSI	ELLA/X.25	e-mail gw.
VAX	NJE	X.25	Bitnet services
VAX	SMTP	X.25	mail
PC	TCP/IP	various	internet services
PC	PAD	X.25	internet services

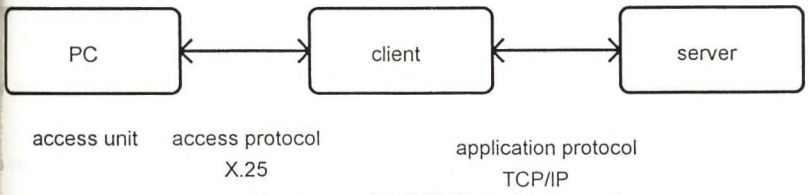


Fig. 1 Accessing TCP/IP services remotely

Initially a Gopher client was installed at the end of 1992. In March 1993 a News reader client was installed. Several other clients are planned to be set-up. The daily usage of News/Gopher is more than 100 access.

The importance of this **fit** cannot be over emphasised as it provides a solution today. With this step our community succeeded in demolishing a **wall**. A wall that separated the big institutions from the small ones. The access to free, up-to-date and relevant information became a general right of the whole community. It is also a clear proof that networks are for providing services.

- Fit piece: HBONE the Hungarian IP backbone

The newest piece in the puzzle is the HBONE. HBONE is a private TCP/IP network. The primary aim of HBONE is to provide a TCP/IP backbone service for the Hungarian R&D community. The first step of establishing the backbone happened in Christmas 1992. The ELTE and SZTAKI networks had been connected, forming the core of HBONE. With that step forward the Hungarian R&D community had established a dual EBONE connected system that was key for the future.

The very next step was the inter university FDDI ring connection to the HBONE. The EuropaNet connectivity has been achieved during May 1993.

Several major steps forward are expected during 1993.

There are many open questions of HBONE like network management, the provision of TCP/IP services for non Hungarnet members, etc.

The challenge of networking

New data communication methods have been developed. ATM meets many requirements of wide range of applications for the tomorrow. Mass production will finally lower the price of bandwidth of communication channels.

Countries will be compared with not only the GNP per capita but Gross National Bandwidth per capita.

The challenge of networking is however to fit together the pieces of the networking jigsaw, to build up the Brave New World of a networked society.

In this paper we have summarised some important steps on the route leading to the present state of the Hungarian R&D network.

Finally I would like to stress that one aspect of the jigsaw puzzle is absolutely wrong. One can fit pieces of jigsaw alone. To the very contrary of it research networks cannot be built without the strong co-operation of institutions, people and machines. The only way we could have done it was together !

The development of SZOTENET

I. Győri, J. Jánosi, J.Karsai, I. Mizsei, T. Szofrán
A. Szent-Györgyi Medical University, Department of Medical Informatics
H-6720 Szeged, Korányi fasor 9, tel/fax: (36)[62] 311 084

Historical review

The history of computer techniques and informatics of SZOTE began at 1971 by the establishing of the Computing Center. Although at the earlier time the computing devices were a little bit primitive but the networking concept was dominant permanently. There were real remote terminal applications on the R-10 machine like Irradiation planning system, Laboratory system, Donor recording system and others. An important application was the statistical evaluation of hand-collected data with a self-developed statistical system. The main storage and peripheral devices were of small capacity consequently there was no real chance to develop large database system for health care.

By the revolution of PC-s on the market of computing devices a large number of IBM compatible machines appeared at our university, too. Few years later this fact made a good impact on creating and developing of local area networks. In our institutes the NOVELL operating system was the almost exclusively used networking software providing a wide range of easy-to-use file server services. It was followed by a considerable growth in data collecting, data processing. The spread of the personal computers made a good impact on supporting the research and education. The desktop devices were handled immediately by the users and it got possible to computerize the local administrations, documentations, text editing and to use scientific program packages. A NOVELL-based inpatient and outpatient system was installed on the clinics providing health care information and reports required by the financial reform program of health care.

At the same time arose the claim to connect these distributed systems to a central computer to build a central data processing and evaluation system. Because of financial difficulties the serial connection was the only way to integrate these systems. In 1988 the TPA-11420, a PDP 11/70 compatible machine, working as a main computer was installed using the old serial lines of the previous computer. The terminals were single PC-s with the intelligent terminal emulation software PROCOMM Plus. This machine served as a window to the world controlling the Electronic Mailing system providing a real connection to the X.25 network. The laboratory reports as a daily routine were transferred until July, 1993 on electronic way managed by the TPA.

The main tasks of the computing staff were the managing the local database systems, adaptation of the coding systems for the local habits, the coordination of centrally managed softwares such as MS-Word, StatGraphics, regular consultations about statistical, hardware, software and networking problems, to develop particular systems for special purpose. Finally, a huge part of the tasks is the teaching of students and endusers.

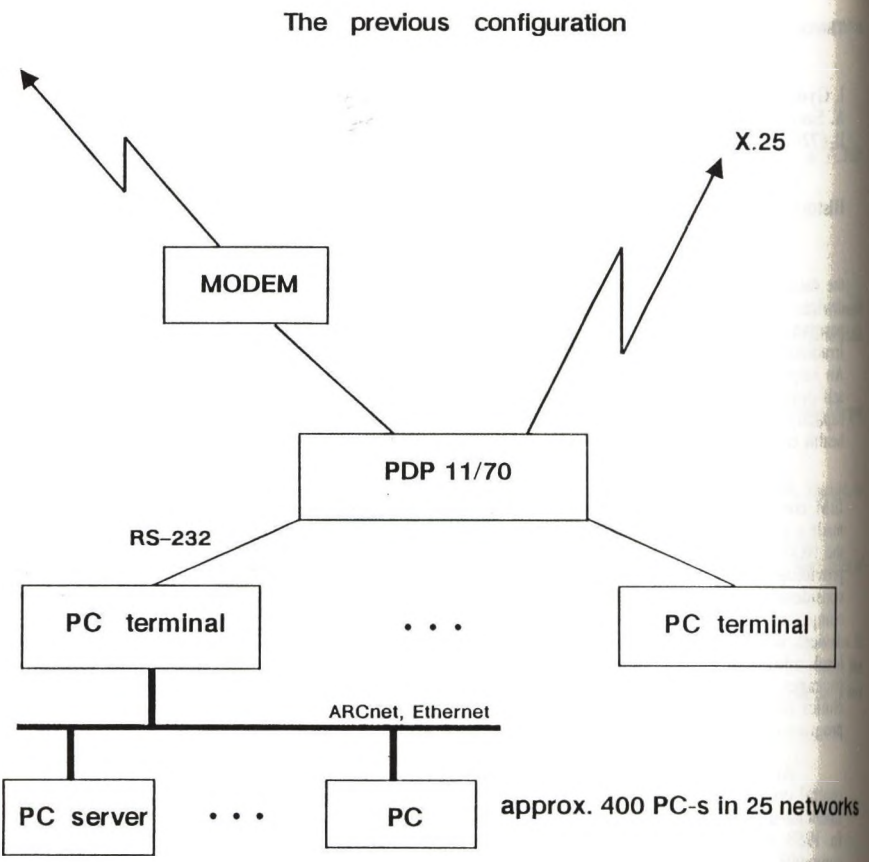


Figure 1. The old situation

After several difficulties, interactions and variations of technical possibilities, growing demands from the clinics, we have arrived to the present state when the informatics is the organic part of the every-day life at the university. There is a new integrated information system just before introduction, which is based on modern hardware equipments. The system includes the inner and outer communications, central databanks, health care, education and research supporting features.

Description of the new network SZOTENET

Planned applications, purposes

- **Integrated Hospital Information System**
  It is a comprehensive developing project, so it is detailed later.
- **Electronic Mailing system**
  It includes both the inner communication system among the clinics and institutes, and the international mailing system ensuring the connection to the Internet, Earn, Compuserve and many others. Our local Mail-server is a VAX 4000/200 computer. It has a network connection to a Cisco router situated on JATE university providing an Internet access on a 64Kbit/sec speed rate and an X.25 connection on 4800 baud rate.
- **Library Information System**
  It is only at a planning level but we made a solid work to review the market although we have to keep on applying for grantsand other financial support necessary to satisfy this type of expectations.
- **Scientific Databases**
  There are many scientific databases on CD-ROM disks such as MEDLINE, Excerpta Medica, Citation Index and many others. In addition, there is a regularly published Current Contents on Diskettes. To achieve a comfortable access to these databases we had to solve a fast disk service on the network. We have a fast CD-ROM server with seven CD-drive at the present time, but we plan to extend it with a new seven-drive tower.
- **Scientific data analysis with central software packages**
  We have to maintain the regular consultation and scientific data analysis services, and we want to support the biological modelling research; therefore, we needed computers with high computational capacity and excellent graphical presentation facility. We have received an IIF grant to get some RISC-based Silicon Graphics Model 4400 computers and a RISC 6000 Model 370 with high RAM and disk capacity and graphical features.
- **Supporting the Multimedia applications**
  Our long-term purpose is to solve the sound and image transfers throughout the network, to process the images originating, for example, from the Department of Radiology or any other sources, to fit these images in a document or create a slide for a lecture and etc. The Token-Ring network can easily transfer huge amounts of data, even the images of several Mbytes, and the high-quality image processing can be solved with the help of the above mentioned RISC computers.

Concepts and requirements

- The network must be **OPEN** from that point of view that different protocols should work simultaneously, namely the NOVELL IPX, IBM SNA, DECNET and TCP/IP, because we have central computers originating from several vendors.
- Let the total network and the network devices be **centrally manageable**, because the buildings are scattered on a large area; furthermore, the structure is complicated and the error trapping and repairing is practically an impossible mission without the central management.
- The data exchange and transfer among and inside the clinics must be **fast** and **safe**. We have to ensure the maximum **security** requirements.

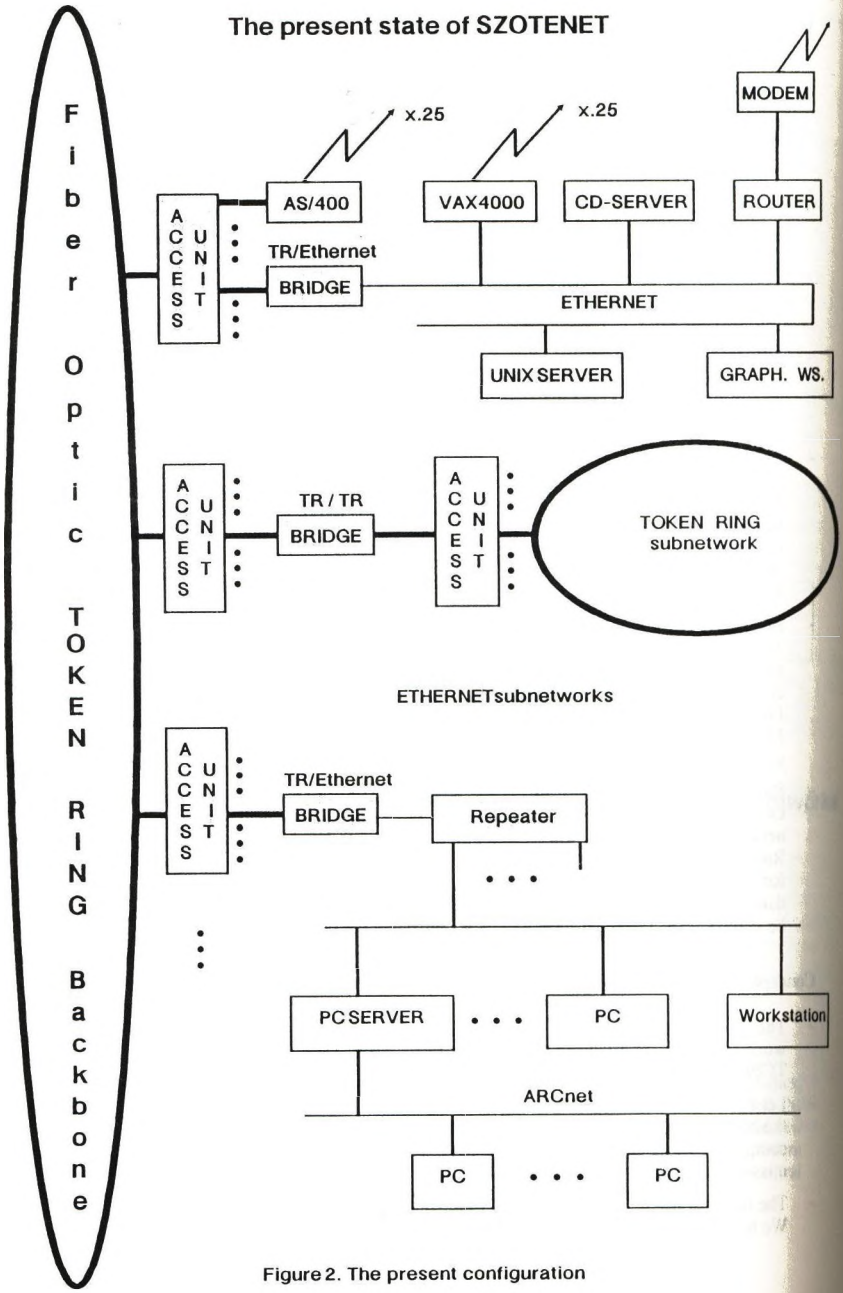


Figure 2. The present configuration

- The network must be **modular** and **flexible** for the further developing. The introduction of different systems can be solved only **gradually**.
- The present **PC stations must be integrated** into the network. Because there are about 600 PC-s at the university the network services and applications should be accessible everywhere at a glance.

These motivations necessitated to ensure powerful central computing resources and reliable multiprotocol network connections among the workstations. Because of the probably large amount of health care data transfers we had to apply only well-performing high-capacity network techniques. Thus, the IBM Token-Ring backbone with fiber optic media was chosen combined with copper-based Ethernet subnetworks. The Ethernet Segments are connected to the backbone via TokenRing-Ethernet bridges. There are many NOVELL servers at the subnetworks. To keep in hand the error handling, the Netview 6000 management software was installed. A useful management tool is the LANalyzer developed by NOVELL. We can analyze the traffic on the network, the utilization and errors. Finally, the most important feature is that the network is transparent to the mainly used protocols like TCP/IP, DECNET, IBM SNA, NOVELL IPX, providing a real open connection of different systems. These protocols can work simultaneously even on one PC, so we can state that SZOTENET is a heterogeneous network providing a real open system connection among extremely different platforms.

Integrated Hospital Information System (MEDSOLUTION BASE)

It is today's necessity to introduce a comprehensive Hospital Information System connecting all departments of the university. What are the main goals and requirements of this project?

The first aim is to build up a central health care database which contains the most important information about the patients and order communications, while ensuring safe data storage and security. All users have proper competence and can not see or change unauthorized data.

The hardware platform must provide a universal connectivity to other PC and NOVELL-based systems, let the terminal capacity of the system be suitable to handle about 1,000 PC stations. It is preferable to have an SQL-based database handling system. The health caring system must be modular, easy to develop or tailor to the local environments.

The best choice for us was the IBM AS/400 Model E50 computer with an SQL-based developing system. The AS/400 computer is connected to the Token-ring backbone directly, therefore it can be accessed from each department of the university. Because the SQL is running it can produce ad hoc retrieval and report of vertically and horizontally selected data at any time, naturally according to the competence of the person. The Information system is the MEDSOLUTION BASE Integrated Hospital Information System. It has 3 fundamental modules.

The main functions of the **PATIENT Management Module** are the following:

- management of patient data (demographic and medical data, previous encounters) and making it available to authorized persons;

- handling different types of patients (inpatients, outpatients, emergency room patients, infants);
- basic functions of a Hospital (registration, admission, preadmission, readmission, discharge, transfer, profile and diagnosis, information desk);
- Clinic Appointment Bookings;
- patient related reports (patient basic data, visit history, doctor and diagnosis information, transfer history);
- census-related reports (all beds, vacant and occupied beds, patient list by department or doctor, etc.).

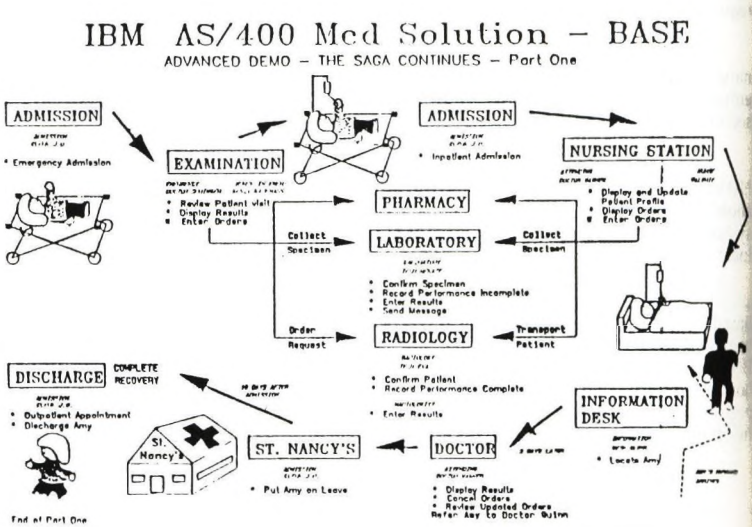
The **ORDER Management Module** provides application support for endusers, such as doctors, nurses and medical technicians

- in-patient-related Treatment Areas (nursing stations, outpatient clinics);
- in Performing Departments (laboratory, radiology, cardiology, pharmacy, care and treatment nursing station).

The **SUPPORT and MAINTENANCE Module** allows to maintain clinic-specific information, such as:

- rooms, beds, doctors, nursing stations;
- security information, restricted access to sensitive data, tailored master screens for each type of user, etc.

The overview of basic functions



THE RISE PROJECT: APPLICATION OF ODA FOR DOCUMENT INTERCHANGE

Hermann Jeram
Fernmeldetechnisches Zentralamt

Abstract:

ODA/ODIF has been standardized as a means to allow for interchange of documents that not only contain text but also graphics and other contents as well.
Whereas for international standards, international concensus is mandatory and takes some time, the delay for mailing working papers and drafts of the standards can be shortened considerably by just applying the electronic means that were standardized.
The RISE (Retrieval and Interchange of Standards in Europe) project, part of the European Nervous System is an example sponsored by the CEC for the establishment of means to speed up the process of standards-production.
Of course, the same means could be used in other environments.

1. Overview

The basic idea behind RISE is to allow for rapid access to working documents.
This requires
- establishment of an access mechanism to documents
- means for the archivation and maintenance of documents
- independence from the package used to produce documents by providing conversion mechanisms.

During the pilot phase, there was the need to bring up these mechanisms speedy, using mechanisms that were readily available. This leaves room for further enhancements of the project when implementations of further standards e.g. DFR [1] that are already specified but not yet implemented, become available.

2. Access to RISE documents

The RISE document server is implemented on a DEC Ultrix machine located at ETSI in Sophia Antipolis.
There are already some initiatives available that allow for access to document stores on some servers. Examples are the Teledoc project at CCITT, the PODA-SAX, and a COSINE project.
These projects all use a gateway between an X.400 mailing system and the document server.
RISE, in the pilot phase uses a similar approach by implementing an Automatic Answering Mailbox that allows a user to access the document server at ETSI either via X.400 [2] or via a VSAT system.
In addition, there are further access means allowing access to the document server via other networks such as PSTN, X.25, and ISDN.

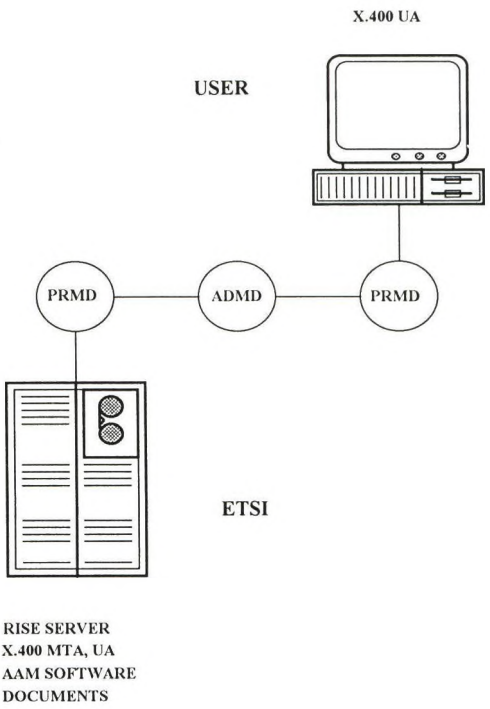


Fig 1: Access to the RISE server

The Automatic Answering Mailbox (AAM) provides the interface between the X.400 system and the document server. It interprets the commands that a user sends in the body part of an X.400 message.
The following set of commands is available:

- **START:**
  This command marks the beginning of the commands to be processed by the AAM.

- **LIST:**
  The command returns a list of documents and sub-directories contained in the specified directory.

- **GET:**
  The command requests the retrieval of the specified document from the document store. When X.400 is used, the document will be a binary attachment, containing the requested file. The AAM checks the user`s authorization before sending the document.

- **PUT:**
  The command will store the document that the user provided as a binary attachment on the RISE servers user`s temporary group space.

- **HELP:**
  The command returns a help message describing the commands available.

- **TEST:**
  The command can be used to test the connection between the user`s mail system and the RISE document store. The AAM returns a reply.

Documents stored in the RISE document store use a filename extension to indicate the format, the document is stored in:
"WW" indicates a MS-Word for Windows v2.0 document e.g. GET /ETSI/exampe.ww VSAT
"WP" indicates a WordPerfect v5.1 document
"O" indicates an ODIF document.

3. Terminal Emulation

Besides the access via MHS and VSAT, access via a VT100 terminal emulation is also provided.
It allows for browsing through documents, searching on document profile attributes or on textual content, viewing of profiles, document transfer and administration of documents and directories and of users.
In order to access the RISE server via VT 100 the user first gets a screen, where he can select browsing, user profile specification or submission. Selection of browsing allows the user either to

select documents to be transferred or directories or subdirectories on which a search will be performed and the specification of search attributes like author, title, creation date, language, etc.

Help	Up	Down	Selall	uNselall	Profile	Transfer	sEarch	Quit

/RiseRoot

Groups	Documents	Selection
ETSI	TC1	TC1
CEN	TC2	
CENELEC	TC3	
NNI		
UNI		

Fig. 2: Browsing screen

Document profile attributes are a subset of the attributes specified in the ODA document profile. Multiple Search results can be sortet.

Help	Next	nExtdoc	pRevdoc	Document	Quit

1. Title	ETSI Stylesheet Manual v.1.0.
2. Original Name	Mysheet.doc
3. Author	B. Mc Arthur
4. Organisation	ETSI
5. Subject	This manual describes ...
6. Document reference	
7. Stylesheet	
8. Abstract	
9. Keywords	STYLE; SHEET
10. Number of pages	45
11. Language	English

Help	Previous	nExtdoc	pRevdoc	Document	Quit

12. Type of Reference	Standard
13. Reference to other doc.	
14. Integration date	
15. Integration	
16. Creation date	1/1/70
17. Last modification date	1/1/93
18. Security level	Public
19. Version number stored	3
20. Document formats stored	WordPerfect, Winword, ODA
21. Distribution list	

Fig. 3: Document profile screens

Document transfer can be accomplished via several transfer protocols: Kermit, FTP or FTAM [3].

Help	Document submission	Quit
Destination directory (optional): /ETSI Medium KERMIT FTAM FTP		

Fig. 4: Submission screen

4. Administration

There is one administrator for the RISE system. His task is the administration of documents and directories and the administration of users. Similar to DFR, both users and documents can be grouped, building a hierarchy.
The RISE administrator is responsible for creation, update, and removal of user registration and user group registration, for updating of RISE access rights, for creation, update, and removal of document collections and for addition and removal of documents.
RISE access control is based on an Access Control List (ACL) for each directory that contains the list of users and user groups allowed to access documents in that directory together with their respective access rights.
Users are allowed to store documents in a shared non-structured filestore, distinct from the RISE document base. The administrator is responsible for insertion of documents in the RISE server.

5. Document conversion

ODA [4] has been identified as the standard format for the exchange of documents. At the time being, however, there is still an insufficient number of ODA users and thus users are still working on propriatory platforms such as MS Word for Windows, WordPerfect or DECwrite.

It is thus necessary to provide for document conversion between these platforms and ODA.
This conversion will be carried out by the administrator.
Key component for that conversion at the ETSI RISE server is an ODA/CDA Gateway that introduces CDA and DDIF as an intermediate format.
The creation of an ODA document is performed in two main steps:
- from the original format to CDA.
  Converters are provided for RTF, MS Word for Windows, WordPerfect, and DDIF,
- from CDA to ODA.

Documents submitted to RISE in ODIF format are converted to the above PC formats in two similar steps.

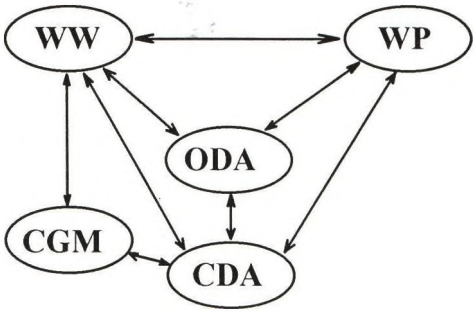


Fig. 5: Conversion paths at the RISE server

With help of the ODAC (the ODA consortium) toolkit the current Q112/CDA [5] gateway will be enhanced to FOD 26 [6]. In addition, some extensions to FOD 36 [6] will be made available including the processing of tables, lists, references, and indices.
It is assumed that a FOD 36 toolkit will become available by the end of this year, thus allowing the rapid implementation of FOD 36 converters by those companies that have already been engaged in the ODAC and have already been working on the FOD 26 converters.

It is further assumed that the reader is familiar with concepts of ODA. It should thus not be necessary to give a description of the features of ODA.
For convenience, however, a short description of the profiles is given, primarily to see the differences between FOD 26 and FOD 36.

From the user's viewpoint, the functionality of ODA is represented by the implemented Document Application Profile (DAP). These profiles have been internationally harmonized between the regional workshops by the PAGODA (Profile Alignment Group for ODA) group.
This work has resulted in the ISPs 10610, 11181, and 11182 [6].
Each of the profiles allows for the exchange of documents in formatted, processable, and formatted processable form.

The profiles FOD 11 [6], FOD 26 and FOD 36 are hierarchically arranged, FOD 11 being the profile with the lowest and FOD 36 the profile with the highest functionality. Each profile is a true subset of the next higher one, both in functionality and in the datastream.
The CCITT recommendations T.502 and T.505 correspond to the profiles FOD 11 and FOD 26, a future recommendation will be compatible to FOD 36.

5.1 FOD 11

This profile supports simple logical and layout structures with character content. It is used for exchange of documents containing text as used in simple textprocessing systems. The content contains a series of paragraphs. Paragraphs can be arranged in groups, each paragraph or each group of paragraphs may have different layout and presentation features. The content of the document can be laid out into pages in a single column of text. A part of the page can be reserved for header and/or footer.
Presentation of every paragraph can be controlled. This refers to indentation, tabulation, various forms of emphasis, different line, and character spacings, different character sizes, widows, and orphans etc.
It can also be specified whether a group of paragraphs should start at a new page or whether some characters or words should be italicised or underlined etc. Automatic pagenumbering is supported.
Further a page can be layed out in landscape or in portrait.
Fig. 6 gives an overview of the constituents available in FOD 11.

5.2 FOD 26

This profile allows for complex logical and layouts structures of different content. It allows for the interchange of simple multi-media documents.
Documents may have text, raster graphics, and geometric graphics as content, thus diagrams and illustrations are supported. The profile has been defined in order to support modern textprocessing systems.
A FOD 26 document may be structured in a hierarchy of segments, defining chapters, sections, and subsections that may be nested. Chapters can be automatically numbered, segments can contain pictures. Footnotes are supported with automatic administration of references from within the document.
FOD 26 allows for international charactersets, vertical writing, and support for orientalic documents. Further it allows for multicolumn presentation allowing for synchronization between the columns e.g. for multilingual documents.
Fig. 7 gives the constituents for FOD 26 together with some of the additional constituents of FOD 36 marked extra.

5.3 FOD 36

This profile allows for even more complex logical and layout structures with multiple types of content. In addition to FOD 26 tables, lists, and overlapping illustrations are supported. It aims for desktop publishing applications.
A general referencing mechanism is supported allowing for automatic references from text and pictures.
In addition, further layout options are supportet. E.g., text can flow around pictures or other text, figures can be positioned on given positions within a certain page.

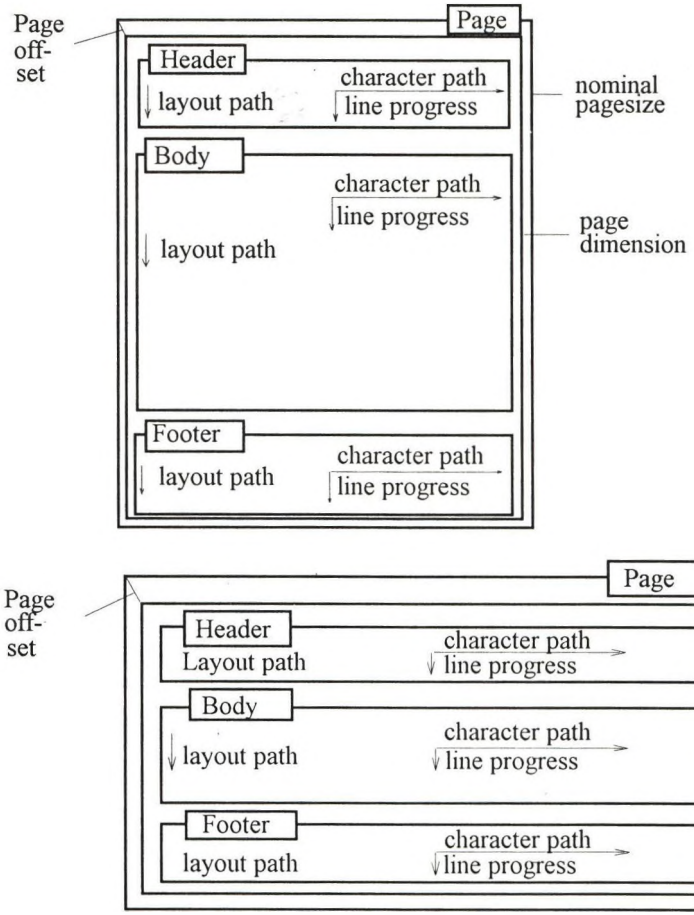


Fig. 6: FOD 11 functionality

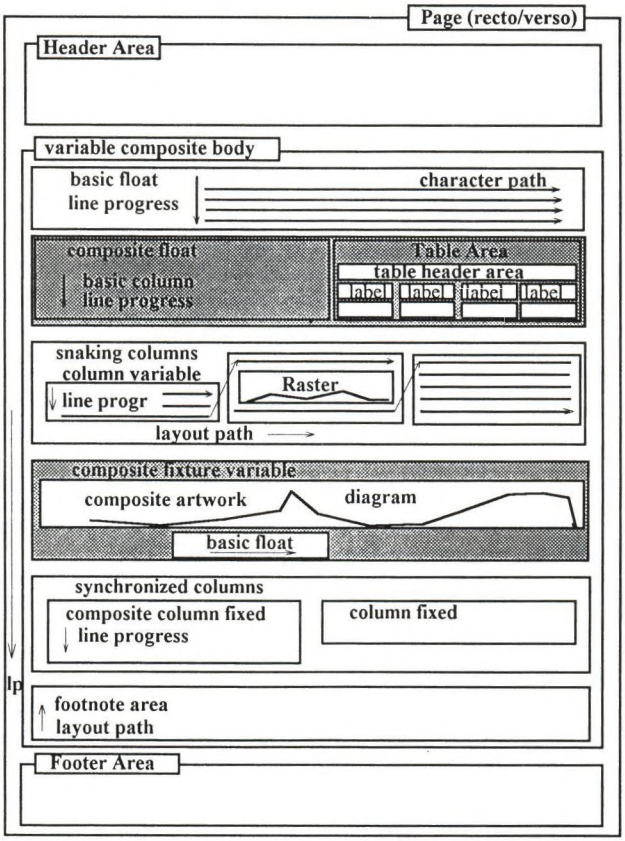


Fig. 7: FOD 26 and FOD 36 functionality

6. Resumé

As for the time being, the RISE pilot project will be presented to the user community, however, the converter used is the Q.112 converter. Until the end of 1993 the converter will be enhanced to FOD 26.

At the moment the Austrian PTT plans to participate in the project by contributing in the areas of DFR and DTAM [7], if accepted. As things are for the moment, it might well be that the project turns out to become a service provided not only for standards organizations but to the public as well. It will in any case be a major breakthrough for the acceptance of ISO standards that still are hampered by the appearance of being complex and difficult to handle.

References to International Standards:

[1]	ISO/IEC 10166-x:	Document Filing and Retrieval (DFR)
[2]	CCITT X.400 series	Message Handling Systems (MHS)
[3]	ISO 8571-x	File Transfer, Access and Management (FTAM)
[4]	ISO 8613-x	Office Document Architecture (ODA) and Interchange Format (ODIF)
[5]	ENV 41 510	Office Document Architecture (ODA) - Document Application Profile Q112 - Processable and Formatted Documents - Extended Mixed Mode
[6]	ISO/IEC 10610-1	International Standardized Profile FOD 11 - Office Document Format - Simple document structure - Character content architecture only - Document application profile
	ISO/IEC 11181-1	International Standardized Profile FOD 26 - Office Document Format - Enhanced document structure - Character, raster graphics and geometric graphics content architecture - Document application profile
	ISO/IEC 11182-1	International Standardized Profile FOD 36 Office Document Format - Extended document structure - Character, raster graphics and geometric graphics content architectures - Document application profile
[7]	CCITT T.430 series	Document Transfer and Manipulation (DTAM)

DISTRIBUTING DATA
in
SOFTWARE ENGINEERING ENVIRONMENTS

Gerhard CHROUST
Systems Engineering and Automation
Kepler University Linz, Austria

Abstract:

Current trends in systems architecture favour distribution of functionality by down-loading work to work stations. This means that the **distribution of the components** *of a software development process has to be carefully evaluated: they can be placed on the host, on a single work station or distributed within a network (LAN). The optimal choice need not be the same for:*

- *tools (implementing development methods),*
- *libraries (storing intermediate and final results) and*
- *control (imposing the desired strategy as laid down in the process model)*

Based upon experience with environments for development, restructuring and maintenance, the paper discusses alternatives for placing various elements and the consequences of these choices.

1.0 Components of Software Engineering Environments

1.1 Basic Considerations

When developing software we by necessity enact a development process (implicitly or explicitly), like every carpenter when building a chair. In order to achieve quality and productivity the process has to be supported by appropriate tools implementing the desired methods.

The individual methods/tools have to be performed/applied in their proper logical order which is largely independent of the individual product to be produced: One needs a **Process Model.** A process model describes all steps in the development process and thus acts as a template for an individual software development process. While for simple processes (like building a chair) it is sufficient to learn and memorize the process model, complicated industrial endeavors like software development [21] need a pre-defined process model and computer support for its execution [6] [8] [9] [12]. Adding support like help texts, library management etc. eventually creates a **Software Engineering Environment** [11] [17] [20], also called **IPSE** (Integrated Process Support Environment) [18]. Computer support for software development can essentially be characterized by Figure 1.

Thus a Software Engineering Environment combines

- tools,
- administration of the results,
- a description of the intended process (the **Process Model**), and
- an interpreter for the Process Model (called **Process Interpreter**).

Further enhancements include project management tools to control resources and schedules [7], but are not discussed here any further.

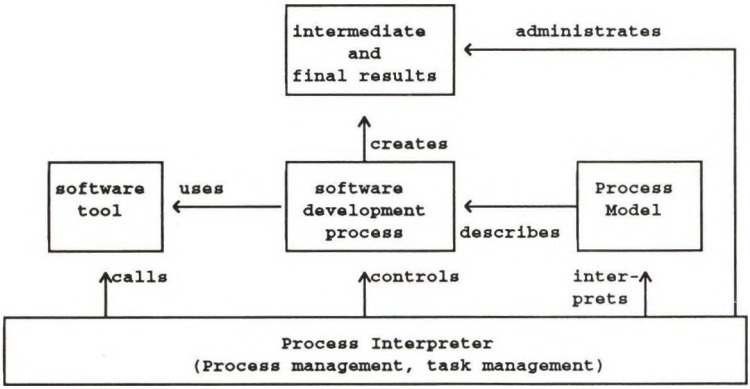


Figure 1. Result, process, process interpreter

Conceptually the Process Model is the central component of a Software Engineering Environment. It can be structured according to the cascade model (Figure 2): On the lower level we see the description of the results ("result types") and their complex relationships ("result structure") on the upper level the description of the activities ("activity types") which allow to derive results from prerequisite results. The strategy of software development is expressed by the "work flow structure", which specifies the choice of a development paradigm. Examples are the Waterfall-Model [2], the prototyping approach [1], the Spiral-Model [3].

1.2 Layers of Software Processes

A software development process covers 3 layers (Figure 3). Within each layer we distinguish **active** ('tools') and **passive** ('data') components.

PROCESS: Everything which is concerned with performing the necessary activities of the process in their proper order. This includes maintaining the status of the various results and deciding on the individual sequence of activities ('navigation').

PRODUCT: The description of the results to be produced and the activities/tools used for producing them.

USAGE: The application of the created software product. This usually occurs *outside* the Software Engineering Environment. For testing purposes, however, one must provide for execution of the product, too.

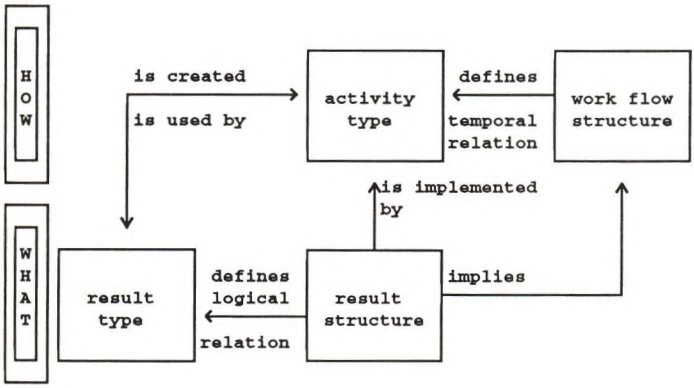


Figure 2. Cascade Model of Software Development

More specifically we distinguish (Figure 3):

process dialogues: These dialogues are the means by which the development process is controlled. They work primarily with the process data and are basically concerned with
- deciding which activity to perform next,
- defining for a given activity the method, the tool and results to be used/updated/created.

process data: This comprises all data about the process and about the individual partial results created. Typical examples are:
- the description of the intended software development process, i.e. the Process Model,
- description of the intermediate and final results, e.g. load modules, source code, specifications, panel definitions, messages, documentation about them,
- description of the applicable tools,
- dynamic information like status code of results and activities,
- help texts for the individual components.

development activities and tools: These dialogues and tools provide the actual work horse of development. Using them the intermediate and final product(s), described by the software products, are created. Typical examples are general tools like editors and specialized tools like ADW [17].

software products ('results'): These are the result of the application of development tools. Examples are specifications, load modules, source code, panel definitions, documentation etc. They are described by the process data.

application execution: The application developed is usually not executed in the Software Engineering Environment, except for test purposes, e.g. prototyping [1], but usually in a different environment, or even a different processor.

application data: The actual data a created application works with are usually not part of the development environment, except for testing purposes [10].

With respect to Figure 2 'result type' and 'result structure' belong to *process data*, 'activity type' belongs to *process dialogues*. The Cascade Model qualifies as *process data*, while the dialogues of the Process Mechanism (Figure 1) belong to *'process dialogues'*.

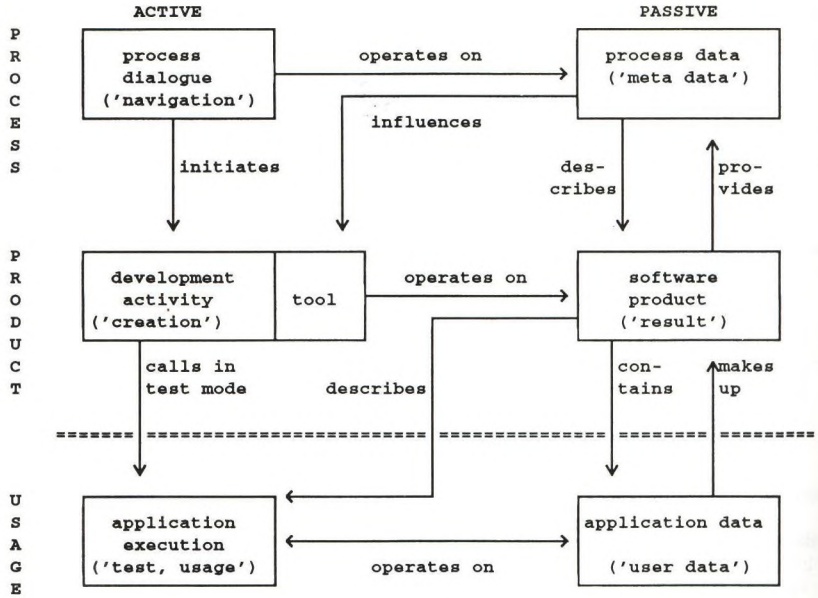


Figure 3. Elements of software processes and their interaction

1.3 Activating a Tool

When a tool is activated, several steps can be distinguished (Figure 4). We describe the most basic ones, finer-grained analysis may identify more. In a cooperative environment each step can be performed on a different processor. Some of the steps are relevant only if functions are distributed between different processor.

Access process data: The decision on the next step must be based on the current status as reflected in the process data.

Select/define activity, inputs and results: Based on the process data a decision has to be made about the next activity to be performed. This includes specifying the results which are to be input and output. In this step these results are not actually fetched, they are only identified, i.e. it is established, which results are needed and where they reside.

Provide inputs: The identified results are made physically accessible. In a cooperative environment this often means transferring, fetching or copying them to a different processor.

Execute a tool: The tool is actually executed, using the provided inputs, creating some results.

Store results: The results are stored in the appropriate location, as defined in the process data.

Undo definitions: It may be necessary to remove some effects of defining an activity. This may include releasing storage, eliminating tool definitions, removing entries in to-do-lists etc.

Store process data: The status of activities and created results has to be appropriately set, and the status of the project changed accordingly, etc.

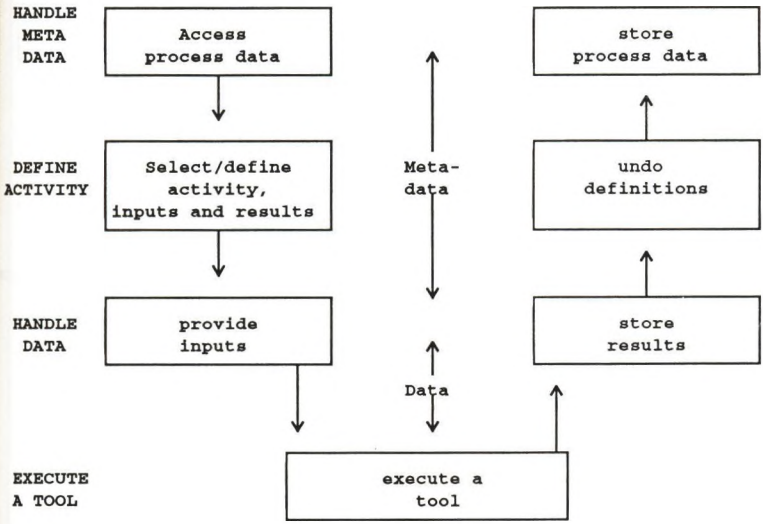


Figure 4. The Tool Activation Process

2.0 Distributed Environments

The question is not only how support a given component but also where.

Tools are the real workhorse of software engineering. The last few years have seen an explosion of software tools, mostly for work station. The reasons for the preference of work stations are manifold. In a multi-user environment several developers have to work in parallel on the same project on different processors. Cooperative environments can have different forms (Figure 5):

- A central **host** with non-programmable terminals
- A central host with work stations running **3270-Terminal Emulation**, i.e. effectively simulating a non-programmable terminal.
- A central host with **work stations** running truly in workstation-mode.
- A **LAN server** with work stations with or without a host in the background.

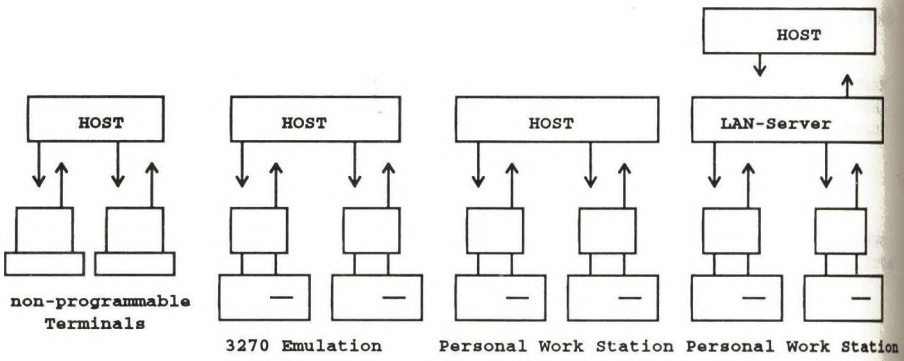


Figure 5. Alternative system architectures

Each of these arrangements has advantages and disadvantages as shown in Table 1. Initially results can reside on any of the processors, but must usually be moved around, in order to exchange status information and to **share** data.

2.1 Distribution Considerations

For the components of the software development process (Figure 3) one has various alternatives of placing them. Generally speaking data have different functions and thus different usage. Typically we have to consider:

usage:

preset data: They keep their value beyond project boundaries. Examples are: process model, printer assignment, company wide forms.

static data: They are set once and then read several times ('read-mostly' data), e.g. final requirements document, project order, names of team members, ...

dynamic data: They change their value frequently.

volume: For performance reasons high- and low-volume data often have to be handled differently. For example the control data for some software module (creation date, owner, ...) can more easily be transferred between processors than a complete code of several kilobytes.

synchronization requirements: A distinction has to be made, whether inconsistent values can be tolerated for some time or not. Typically a status change of an intermediate result should be immediately propagated whereas a new version of an editor may be made available to developers at different times.

Table 1. Advantages and disadvantages of environments

environ.	advantage	disadvantage
work station	• user friendly dialogues available due to graphic capabilities • many convenient tools available • tools can run fast as long as resources are available • response time is independent of the load of the whole system and can be made much better than on the host • work can be pursued even if line connection breaks down • work arrangement and work environment can be independently structured • data and programs are under user control • privacy can be easier enforced	• sharing patterns for data require complicated protocols • locking is difficult, only via LAN or host • communication with another work station only via LAN or host and therefore interrupt-prone • maintenance complicated • personal responsibility for work station (safety, backup, installation, ...) • no reliable fast backup without LAN or host • space problems with mass data • status information may be out-of-sync in different processors
3270-emul	• behaviour almost identical to host • some of the services of the workstation can be utilized • host-processes run in a workstation window in parallel with other tasks	• similar to host version • possible interference with other tasks • response time worse due to competition with other tasks
LAN server	• communication easy within a LAN • locking easy within a LAN • no permanent host connection needed • maintenance more centralized than on work station • backup of group data easy (centralized) • often economical (without a host)	• work station necessary for actual work • maintenance more complicated than on host • locking difficult between different LANs • communication more complicated between different LANs
host	• centralized maintenance • efficient access control (locking) • only one copy of all data • easy communication within team • easy backup of mass data • size of tools and other resources nearly unlimited • hardware usually already in place (no new investment)	• dialogues rather old-fashioned, with limitations of 3270 terminals • line connection necessary during whole session • response time hampered by line delays, especially for large data volumes (e.g. graphics) • distance of terminals limited or requiring expensive technology

Table 2. Distribution considerations	
Process Dialogues	Running the development process on the work station is possibly the best solution because the dialogues are not changed very often. Maintenance is infrequent and usually exact synchronization between different processors is not necessary. Therefore the advantages of speed and user friendliness using the graphical capabilities of the work station should prevail.
Process Data	*Process model*: The model is rather stable and used in a read-only fashion. It is rather large and not all of it is needed at all times in all processors. Parts of it should be down-loaded to a work station. *Tool options:* Options needed by a tool can have two aspects: either they are standardized and therefore rather tool-oriented or dynamically result-oriented. In the first case they should be stored as close as possible to the tool, in the latter case in the same processor as the appropriate results. *Process data:* One should keep only those process data on the work station which are private. The bulk of the data should reside on the LAN-server. Since the communication between a LAN server and a user is very efficient, this solution is usually better than copying the items to the user's work station, especially in view of the fact that probably all developers on one LAN should see the same values of process data (e.g. status codes). Process data common to more than one LAN should reside in the most central processor (usually the host).
Tools	Tools should run as close to the user as possible. Therefore work station should be preferred to LAN and LAN to a host. Of course many tools are only available on a specific processor.
Software Products	The software products in their final form must reside in the most central processor (usually the host) for later access and shipment. Data will pass through the work station->LAN->host chain when promoted, and in the other direction, when changed again. Library systems [13] could handle such movement of data.
Application	The elements of the application must finally reside in the environment where the application (or the relevant part of a cooperative application) will be run. This applies to those parts of the software product which represent executable code. With respect to testing it is desirable to integrate a test environment into the development environment, which by necessity must be a mirror of the execution environment. There are several tools around (e.g. WITT [14]) which support the integration of testing into the development environment.
Application Data	Application data will reside on the anticipated execution environment, usually different from the development environment. Test data have to mirror the actual application data and thus be placed in the processor for which the application is designed.

3.0 Examples

Currently we see a trend to increased (often exclusive) use of the work station. Table 3 shows the distribution of the components of the examples below.

Example 1: ADPS, host-only version: The initial version of ADPS (1987) was based on a rather conventional development paradigm and conventional development techniques [4] [5].

Example 2: ADPS, with workstation attachment: In order to provide access to work station tools, in 1989 ADPS was extended to activate tools on the work station [16]. Process dialogues, process data and activity definitions remain on the host. The command lists for tool activitation are prepared on the host and then down-loaded to the work station. Data are also kept on the host and only down-loaded, if a tool needs them. After a tool has finished, the files are transferred back to the host.

Example 3: MAESTRO II: MAESTROII [19] is a LAN-based system with a common repository for all workstations.

Example 4: SEE (Delphi-Group): SEE is a single-user control environment primarily used for controlling software development.

Table 3. Distribution of components

	ADPS host	ADPS workstation	MAESTRO II	SEE
process dialogues	Host, 3270-Emulation	Host, 3270-Emulation	LAN	Workstation
process data	Host	Host	LAN	Workstation
development activities	Host, 3270-Emulation	Host, 3270-Emulation, Workstation	Workstation	Workstation
software products	Host	Host	LAN	Workstation

4.0 Summary

The availability of high-power personal workstation has changed the quality of software development. A work station offers many options which were infeasible on a host equipped with non-programmable terminals.

The introduction of the work station has somewhat overwhelmed system designers. Upper case tools like ADW, IEF, IEW, BACHMANN and many others only run on the work station, but also the number of lower-CASE tools running on the work station is increasing (e.g. SATT [15] and WITT [14]). It becomes necessary to consider a new way of interaction between the host and work station.

Going from a host-only environment to a cooperative one, brings several new alternatives which have to be evaluated carefully. It turns out that an optimal distribution of the components of a Software Engineering Environment is one of the keys to an economically and technologically acceptable solution. This has brought about a greater flexibility for the system designer with respect to distributing the various components of the software development process but at the same time has increased the responsibility and the chances of errors.

In this situation we can afford the luxury to use the **user friendliness** of a work station, the **flexibility** of a LAN and the **power** of a host.

5.0 References

[1] Agresti W.W.: New Paradigms for Software Development.- IEEE Computer Soc. Press, North Holland Publ. Comp. 1986

[2] Boehm B.W., Elwell J.F., Pyster A.B., Stuckle E.D., Williams R.D.: The TRW Software Productivity System.- IEEE (ed.): 6th Int.Conf.on Software Engineering, Tokyo, Sept 82, pp. 148-156

[3] Boehm B.: Applying Process Programming to the Spiral Model.- Dowson M. (ed.): Representing and Enacting the Software Process.- Proc. 4th Int'l Software Process Workshop, IEEE 1988, pp.1-11

[4] Chroust G., Gschwandtner O., Mutschmann-Sanchez D.: Das Entwicklungssystem ADPS der IBM.- Gutzwiller T., &Oe.sterle H. (eds.): Anleitung zu einer praxisorientierten Software-Entwicklungsumgebung, Band 2.- AIT Verlag Muenchen 1988, pp. 123-148

[5] Chroust G.: Application Development Project Support (ADPS) - An Environment for Industrial Application Development.- ACM Software Engineering Notes, vol. 14 (1989) no. 5, pp. 83-104

[6] Chroust G., Goldmann H., Gschwandtner O.: The Role of Work Management in application development.- IBM System Journal, vol. 29 (1990) no. 2, pp. 189-208

[7] Chroust G., Knotter S.: Vom phasen-orientierten zum task-orientierten Vorgehen in Informatik-Projekten.- Elzer P. (ed.): Multidimensionales Software-Projektmanagement.- AIT-Verlag Muenchen 1991, pp. 81-111

[8] Chroust G., Heger G., Pfann P.: Integrating the Use of AD/Cycle Tools under ADPS (A Restructuring Environment).- Proc. SHARE Lausanne, April 1991, pp. 15-27

[9] Chroust G.: Modelle der Software-Entwicklung - Aufbau und Interpretation von Vorgehensmodellen.- Oldenbourg Verlag, München 1992

[10] Hein P.: DevelopMate: A new paradigm for information system enabling.- IBM System Journal vol. 29 (1990) no. 2, pp. 250-264

[11] Huenke H. (ed.): Software Engineering Environments.- Proceedings, Lahnstein, BRD, 1980, North Holland 1981

[12] Humphrey W.S.: Managing the Software Process.- Addison-Wesley Mass 1989

[13] IBM Corp.: AD/Cycle Concepts.- IBM Corp., Form No. GC26-4531, Sept 89

[14] IBM Corp. (ed.): Workstation Interactive Test Tool - User's Guide.- IBM Corp. Form No. SC26-4677-1, June 1990

[15] IBM Corp. (ed.): Software Analysis Test Tool - User's Guide.- IBM Corp. Form No. SC26-4678, June 1990

[16] IBM Corp.: Application Development Project Support/ Application Development Model and Process Mechanism - General Information.- IBM Corp.,Form No. GH19-8109-2, 1990

[17] Martin J.: Information Engineering, Book I: Introduction.- Prentice Hall, Englewood Cliffs 1989

[18] McDermid J. (ed.): Integrated project support environments.- P. Peregrinus Ltd. London 1985

[19] Merbeth G.: MAESTRO-II - das Integrierte CASE-System von Softlab.- Balzert H. (ed.): CASE - Systeme und Werkzeuge.- 4. Auflage, B-I Wissenschaftsverlag 1992, pp.215-232

[20] Sommerville I. (ed.): Software Engineering Environments.- P. Peregrinus Ltd. London 1986

[21] Weber H.: Software-Technologie mit AD/Cycle - eine einführende Betrachtung.- Corzilius R. (ed.): AD/Cycle - Ziele, Konzepte und Funktionen.- Oldenbourg-Verlag München, Wien 1992, pp.57-87

The Computing System of Hungária Insurance Co. With Networking Details

Détári György és Lukács Katalin
Hungária Computing Ltd.

1 Introduction - auld lang syne

Back in the 80's the Hungária insurance used only Hollerith machines to manage its contracts (except the car insurances). This method is usually working, but the firm was getting far too big for this method. The poorly managed contracts caused problems in calculation of statistics, tariff, prices etc. The insurance company has tried to find a solution, so they have asked one of the major institutes of the Hungarian computer science, the MTA SZTAKI to build a computing system which could deal with the about 240 offices spread around Hungary. We must know, that in those years the networking meant leased lines. A part of the car insurance and the car claim settlement for Budapest and county Pest have been managed by the firm named PSZTI (now Pillér Ltd). They have had a SIEMENS computer with some terminals connected by leased lines. Only the branch offices with car claim settlement had terminals.

The cost of a bigger network connecting all of the offices was too high even for the insurance company (not to mention the cost of a host computer big enough and the problem of the embargo). So the system was developed to use PC-s which were connected with LAN-s in every office. The PC-s were running MSDOS 3.0 with a multiprogramming support package called MISS. Over this the next layer was the Database Manager called LATOR. Both of them were developed in the MTA SZTAKI. The user interface was the ABLAK, which means WINDOW in Hungarian. ABLAK is a character mode window oriented interface with programmable masks. Later on the whole system was referred as ABLAK.

The result of this system meant faster customer support, improved statistics and financial data. The financial part of the database was sent to the headquaters on floppy disks four times in a year, so the expenses and tariffs could be calculated on these bases.

There was a basic problem with this system, which is still working today (in a slightly modified form). From the customer's point of view the insurance company was working like 200 separated small companies, i.e. the customer could only do everything in his 'home' branch office, because all data were stored there, and no access was available in any other places.

2 Car liability insurance - the first challenge

There were some deep changes in the life of the company and even in the life of the country when in 1990 the privatization was started. The German insurance giant ALLIANZ AG has bought a majority ownership in Hungária Insurance. Till this time the fee of the car liability insurance was included in the fuel prices, and the income was shared among the insurance companies. A decision was made by the new government to change this situation: each car owner has to make contract with one of the companies, and the central control is made by the police. Each company has to give its contracts on a magnetic tape to the police.

The car insurance becomes one of the major business at Hungária, so the estimated number of the contracts was about 1.7 million. To be able to deal with so many contracts, Hungária had to establish a computing base. This was the Hungária Computing Ltd. (HCL) using an MVS/XA operating system on an IBM 4381 processor. The applications were developed in COBOL-II running under CICS 2.1. Accepting the current situation, the databases at the offices stored in the ABLAK system were encountered as the up-to-date databases, and the central database was used only for the financial part of the insurance. The payments are coming from several sources, e.g. payslips from the Hungarian post, magnetic tapes from the banks, and certificates from the offices. The payments are recorded in the database and the information about it is sent to the police.

2.1 Selecting a communication method

The problem of the telecommunication arises again, the offices need to access the central database to check for each particular accident to find out whether the car has liability insurance or not. In the last years the networking possibilities have been improved. Hungária could choose from the followings:

- *VSAT.* The required bandwidth is some times 64 Kbps at the centre, and about 9.6 Kbps at the branch offices. We could make a tree structure with VSAT transceivers at the county centers, and leased lines to the branch offices but the costs were higher than the all leased line solution.
- *Leased lines.* To get 240 leased lines from the country to Budapest was almost impossible, but we would have to make a tree structure with a concentrator

on each county center. Because the fee depends on the distance, this is a better choice, but the additional cost of the concentrators makes the choice unusable.

- *X.25 public network.* This is a dynamically extending area of the HTC (Hungarian Telecommunication Company). Using X.25 means to spare the concentrators, getting 9,6 Kbit at the office and 64 Kbit at the centre. And the costs are not too high, and didn't depend on the distances.

Analyzing the estimated traffic based on the daily number of customers in an office, the result is that the public X.25 network fits the requirements best, with 9,6 Kbit at the office, and some 64 Kbit lines at the host side. Even the 9,6 Kbit is too much in some cases, and is used only for the proper response time. For the security, our firm has to use the closed user group feature of the X.25 recommendation.

2.2 Selecting a communication equipment

The given structure is: a LAN at the office, connection over X.25, and an IBM host with 3270 application. These points involve to use the QLLC protocol, which means the SDLC/SNA transfer over X.25. It requires only one special software on the host side, the NPSI, which is a 37xx software addendum to the ACF/NCP. The variable part of the solution contains several possibilities:

- *IBM 3174-61R.* This remote controller (like any of the 3174's) has the capability to use the QLLC protocol. The PC LAN can be connected via token ring LAN or through the RS-232 port if the controller has the AEA (Asynchronous Emulation Adapter) feature. The problems with this solution are the relatively high price when selecting the token ring version, and the fact that the AEA does not support the ROECE East Europe (870 code page) screen and keyboard standard (not to mention the asynchronous terminal emulation software which has to be bought and must support the 852 code page and keyboard).
- *IBM LAN's with either DOS or OS/2 and with IBM X.25 card.* This involves the change of the currently existing LAN's at the offices together with a rather high cost factor.
- *EICON card.* This card along with it's software is able to make a gateway in almost any LAN, which is available from all of the workstations, and can have multiple sessions even with multiple hosts and/or calling numbers. It also supports the graphic interface for GDDM and the remote (VTAM) printers. The code tables for the screen and keyboard can be user defined, so the implementation of the Hungarian charset has no problem.
- *NCP card.* The capabilities are similar to the EICON card.

Comparing the previously listed solutions from the economic point of view the EICON card seemed to be the best. The required features were provided by any of the solutions. The problem with the NCP card was only the price.

2.3 Backup connection possibilities

The X.25 network or a part of it could fail. There should be a solution for the case, when only some part of the network is down. The user interface for the backup connection has to be the same as for the main one i.e. it must be a fullscreen 3270 interface. For this connection we must consider the same points of view as for the normal one, i.e. the PC's LAN network, and the minimal cost. Analyzing the prerequisites, the switched telephone line and VSAT connections can be used. The asynchron emulation via IBM 7171 or a central IBM 3174-61R with AEA have the problem with the Hungarian (ROECE - East Europe 870) charset. So we should look for solutions with synchronous connections:

- *VSAT - SATNET service of the Please ltd. (HTC).* This solution means, that the Please ltd. builds a backup connection for a failing X.25 one for proper fee. The charges are too high to accept them.
- *VSAT service at the HCL (Hungária Computing Limited).* We buy a fixed station at the HCL, and a moveable one. In case of failure we install the moveable station to the branch office till the connection is corrected. The cost of this solution is still higher than the switched telephone line.
- *Switched telephone line with synchronous 2.4 Kbps modems and SDLC protocol.* The cost estimation is good for this, the problems are the reconfiguration of the EICON card at the site (branch office), and a telephone line must be assigned for this purpose at the branch office and at the Mainframe side too.

Currently no backup connection is implemented.

3 Optimizing the network

There are many points of view how to optimize the network. In an X.25 network the cost and response time have similar physical requirements - to minimize the number of segments flowing through the network (i.e. the X.25 cost depends on the number of segments (packets) sent and received). Another two components are the calling and the connect time fee. What can we do to make these minimal? The source of the main problems is the concept difference between SNA and X.25. SNA uses leased lines, or switched lines. The cost of a leased line is fixed, and for a switched line it depends only from the number of calls and the connect time. The difference partially may be reduced by some customer procedure and parameter.

3.1 Physical level optimization

- Two parameters have to be tuned together to get minimal number of packets. The MAXDATA parameter in every PU, and the NCP buffer size determine, how many packet required to transfer a RU. To calculate the resulting packet sizes, we should know some NCP internals. We assume, that the RU size is big enough to transfer a screen without chaining. The RU is stored into integral number of NCP buffers, but in the first buffer there is an ECB (18 bytes) and 20 bytes padding, because the NCP containing the NPSI also contains the BF (boundary function), so the INN TH (26 bytes) is changed to BNN TH (6 bytes). The first buffer also contains a RH (request header, 3 bytes). Now the NCP gets integral number of NCP buffers to assemble into a packet till the packet length is less or equal than MAXDATA. Taking into account that the packet size is 128 byte and the HTC charges for segments where a segment is from 1 to 64 bytes we must keep the parts equal to or below 64 or 128. Calculating with a small program, we get a table like this:

MAXDATA IN PU	NCP BSIZE	FIRST SEGMENT	LAST SEGMENT
...			
200-229	112	58	118
...			
450-485	240	58	118
...			
502-521	108	118	54

  We have some typically good lines listed above. Another aspect of the NCP buffersize, that the size should not be too large, or there is a memory waste at every short buffer like responses (e.g. DR1, DR2), BID, RTR etc. Based on this, our choice was:

  MAXDATA=521, NCP-BSIZE=108

  The results are 118-128-128-54 packet length series.

- The connect time fee and the call fee determines the inactivity timeout. One call is 1.50 Ft, the connection is 0.25 Ft/min. This means that after 6 minutes of inactivity better to disconnect, because the call fee is lower than any other connection fee.

- There is a traffic dependent fee of segments. If the traffic is over the limit, the price of the segments gets lower. The limit is rather high, and even in case of using the reverse charge, the allowance is valid only for the caller. This

means, that the center should call the offices (about 10 million forint spared in a year) otherwise the allowance cannot be used (it is calculated on monthly base).

3.2 Optimization on CICS level

- Basically the CICS uses DR1 (definite response mode) on the SNA level. This means, that every SNA buffer gets a response. The response is only some byte, but costs a full segment over X.25. Much more practical to specify EXRSP (Exceptional Response) for CICS, so only in case of error comes a response back.
- You may specify for CICS to gather all outbound messages into a single transfer. This results a better packet filling rate.
- You may spare to send unwanted data out, if the input fields are not filled. The only thing (resulting from write gathering) to send the blocks together with an erase-write.
- You may write an exit routine for all of the terminals. It can compress the output before sending using the RA (Repeat to Address) in-stream command to suppress multiple blanks and/or nulls. You may use another software for this purpose (see 4.2 point).

4 The next stage for Hungária

Our solution was made for the car liability insurance. But a modern insurance company needs an integrated insurance and monetary system. To develop such a system needs time, and time is money (not only because of the popular saying, but for the costs of the computing centre). There are two ways, buying a ready-made system and tailor it, or buy a fourth generation language tool like Sapiens, and build a system with it. The second way is not cheap, for the tool is expensive, and the resulting system needs a big CPU to run well. The first way is not easy, for not too much system is available on the market.

The selected solution was to get a system named SYSTEM-80 from the Anglo-Elementar Insurance (which is another ALLIANZ-owned firm) and taylor it for our purposes. The advantage of this system is that it is a running system with 10 years of experience behind it. The disadvantage is that it is designed 10 years ago, based on the old tools and computing technical elements. Another problem that the legal, monetary and insurance-technical requirements are different in Hungary and Austria. The result is that we have to make efforts to adopt an old system because we think this way is the fastest, and when it is ready, we may design and construct a new modern system and then we may migrate to the new one.

The SYSTEM-80 is IMS-DB/DC based system, developed for IMS 1.3. The databases are VSAM-organized. There is no on-line update in the databases except a special database called 'DAILY', which gathers all of the updates. At the end of the day, batch jobs are updating the real databases from the contents of the DAILY database. The system contains some other elements integrated, like TPX from Legent, CONTROL-D/M from the Bool And Babbage, SORT and SRAM from the Computer Associates and many other items from IBM.

4.1 IMS/DC facilities for optimization

- *Response/Non-response mode.* This mode allows the user to enter new data before the IMS ends the previous entry processing. For the non-response mode there is an extra (short) packet for keyboard unlock, so response mode is better (if we don't count DRi definite responses). The default for 3270 is the response mode.
- *Definite/Exceptional response mode.* For the terminal output this depends on the transaction type. The only transaction which doesn't want definite response is the non-recoverable one. Both recoverable and update transactions need DR2. The only way to avoid this to use IMS Fast Path feature, for this feature uses Response Mode with exceptional response, which is the best for X.25 NPSI (except for output messages, when another message is waiting for the terminal).

The SYSTEM 80 transactions cannot handle response mode, and do not support Fast Path.

4.2 External terminal handler over the applications

Using a software switching and multisession software (like TPX) may improve the available services, and also the performance. For example the TPX from LEGENT can do the 3270 data compression for you and for any application. The compression replaces any multiple characters with a 4 character RA (repeat to address) sequence, which is decoded by the 3270 controller (line 3274, 3174 etc.). In case of an average application it means about a 30the application does not precompress the data to be sent).

5 Summary

Our goal was to build a network which is effective in the point of view of the response time and cost including both the setup and the operation costs. Based on the traffic of the branch offices we found out that the X.25 public network is the best

for the IBM 3270 applications. The advantage of the 3270 protocol is the buffered operation i.e. the user fills the screen and the transmission occurs only when she is ready and presses the Enter key. For this reason there is almost no contention between the end users of a branch office.

Selecting the EICON card as a communication tool resulted in a good quality/price ratio.

We are just planning our backup connections, for we have got some serious communication break in the X.25 communication.

We hope that our experience will help you in building your own network.

IBUSZ INFORMATION SYSTEM (IBISZ)

Gabriella IVÁNKA, György LEPORISZ, Gábor FARKAS
Computing, Communication and Innovation Technology Corp., Hungary

Abstract:

The greatest system integration work of SzKI was the development and realisation of the IBUSZ Information System (IBISz) for IBUSz Co. and IBUSz Bank Co. between 1990 and 1992. IBISz is a nation-wide information system to which are connected more than 100 offices of IBUSz Co. and IBUSz Bank Co.

IBISz is a computer system with hierarchical structure, it consists of three levels connected to each other. The central resource of IBISz is an OLIVETTI LSX-4240 fault-tolerant (FT) computer. It operates at the highest level of the system. NOVELL SFT NetWare fault-tolerant local area networks are forming the second level, they are connected via an X.25 private network developed bz SzKI. At the third level high quality PC based workstations are working. In the local area networks there are more than 450 local or remote workstations integrated.

On IBISz are running banking and tourist applications developed by SzKI and other companies (e.g., internal accounting of foreign currency, handling of travels, etc.).

1. Introduction

IBISz is operational since June of 1991. At the beginning of 1989 IBUSZ entered into an agreement with our institute to draw up our proposal for a computerized system based on the screening of their company. The proposal for the system had seen accepted by the middle of 1990 and that was followed by the effectuation of the work.

Our aim was to carry out a computerized information system which enables the user, without having any knowledge on computers, to take advantage of the computer services at more than one hundred workstations intalled in the whole country.

The main stand points when forming the system were as follows:

- the using of standard, generally marketed, professional hardware and software components
- the application of standard telecommunication interface

- planning the maximum (meeting the requirements of the banks, too) reliability (fault-tolerant tools, transaction oriented processing)
- the application of communication saving solutions considering the insufficiency of communication infrastructure in Hungary
- creating a shared database in order to decrease the telecommunication loading
- a moderate price comparing to the complexity of the task
- the application of unified technology when using the services
- openness for the possibility of extension, and for the integration of new elements into the system.

2. Features of the Strategic Elements

We have formed a strategic tool basis which meets the requirements of the above standpoints, and which is generally applicable. It is divided up as follows:

- SYSTEM PLATFORM: includes the typical elements of the system building, the solutions, the principles and the methods of the interfaces in the system
- SYSTEM PANELS: tools specially developed for creating integrated services, which are transportable for building different systems
- TOOLS FOR DEVELOPMENT AND INTEGRATION: transportable tools for connecting the system modules, developing the applications, and for effecting the integration tasks.

In the building of the system the transportable 'BASIC SYSTEM' of general purposes and the specified 'APPLICATION SYSTEM' characteristic only of the given task can be distinguished.

The 'BASIC SYSTEM' reflects the architecture and contains the general services of the system. This includes that part of the system, SzKI is going to use in the future and can use in its system building experience, of course, taking into consideration the local needs and the results gained during the development of the system.

In this case the 'APPLICATION SYSTEM' meets the specific requirements of IBUSZ and the actual solutions of the system form a joint property with IBUSZ.

3. Architecture of the Basic System

In case of a system has been built up conventionally - i.e. display terminals, each job is done effectively on the central machine - the requirements of the hundreds of workstations must be calculated by only one machine, which is large enough (e.g.appx. as much input channels as workstations). The other solution is that we decrease the loading of the central machine. We have chosen this latter one, not only for the reason that we could radically reduce the size (and the price!)

of the central machine, but at the first solution the telecommunication of appropriate level cannot be quaranteed by the present postal lines, in case of an extremely high loading.

In the model chosen by us the intelligence and the database are shared among the different components of the system. Fig.1.shows the architecture of the system, the system, the database and the three levels of the communications.

The local networks are connected to the central computer, consequently, the three levels of the system include the workstations, the LAN server and the central machine. The client service takes place on the workstations. This is where the user-friendly application programs run, which can query the database and modify it at different levels of the system, according to the client's need. By day, the central machine answers the questions arriving from the workstations and after the working hours, the running of the evening processing programs and the printing of the central reports are effected.

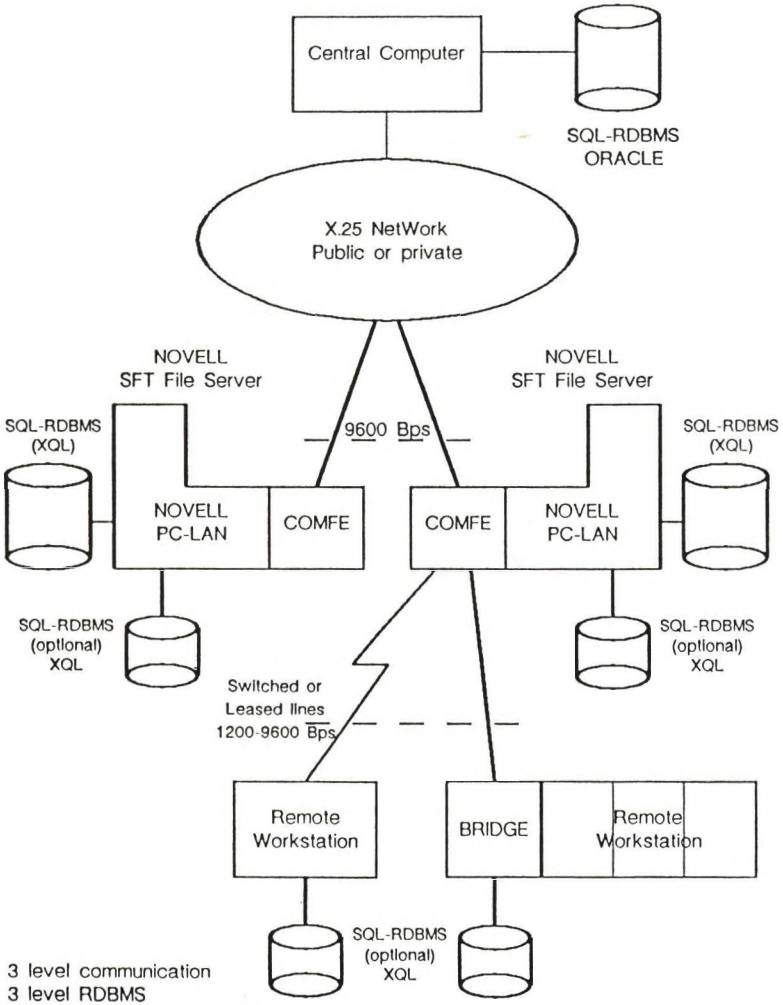
The three levels of the database are in accordance with the levels of the system mentioned above. Only those data are stored at the workstations which are rarely have been changed (containing descriptive, informative data) and respectively, which are necessary at the site. On the servers the common database and the temporary databases of several workstations can be found. Temporary databases are created during the download of databases and new versions of the programs from the central machine to the workstations through the server. On the central machine those data are stored which must be always in up-to-date state and must be available for the workstations.

From the three levels of the telecommunication the middle one is the local area network as mentioned before. The upper level is the X.25 packet-switching network effected between the LAN machines dedicated to communication (GATEWAY, COMFE)and the central machine. At present, the building of a private X.25 network on hired postal lines has been realized, since there has not been any public network throughout the country. Special attention has been payed to the building of the network, in order to easily enable the transformation into a public X.25. network at any time. The lower level means connection of the remote workstations to the LAN-s through asynchronous lines (leased or switched telephone lines).

Besides integrating the ready-made products into the system and interfacing them each other, the components which are not available as ready-made ones had to be developed.

4. Characteristic Services of the Basic System

- SERVER/CLIENT transaction processing
- Message sending system
- File to file transfer
- Download from the central machine to the servers and to the workstations: file, database table, program
- Diagnostics: X.25 monitoring system, Novell trace system, error-monitoring, output on the central machine, creating check-summa and comparing it with the workstations.



Typical processing is the Transaction control based on RDBMS

COMFE = COMMUNICATION FRONT END for NOVELL NetWare

FIGURE 1

5. Tool Basis of the System Platform

- Workstation: Wearnes 286 sx PC (ALR standard)
- Server: ALR 386PC
- Central machine: Olivetti LSX 4240 fault tolerant machine
  processor: 3 x 2 M68030
  memory: 32 x 2 Mbyte
  disk: 1,2 x 2 Gbyte
  operation system: VOSv10.0
- LAN: NOVELL v2.15, v3.11
- X.25: switching center and XENIX based monitoring machine (SzTAKI) X.25 PC board to the COMFE machines (SzTAKI)
- Modem: Bullet ETECH 2400, 9600 Bps
- Database: ORACLE RDBMS v6.0 on the LSX machine, NOVELL SQL on the servers, Clipper v5.0 on the workstations and on the servers.

6. Developed Components of the System Platform

6.1. On the Workstations

Since the operation of the workstations takes place in offices without any computer knowledge and computer discipline, their protection against unwarranted access had to be solved by us. We had to modify the BIOS of the computers in order to accept only those floppies which were specially prepared by us for this purpose, and no other floppies could be read or used to load the system. (Of course, the modified BIOS is compatible with the original one). Thus, we have succeeded in operating the system virus-freee.

The memory map of the workstation can be seen on Fig.2:

- BLEND: The program captures the own error message is of the system (operation system, network). In case of error, it ensures the recall of the workstations of the NOVELL network.
- LANCOM: It converts, cuts then sends the data from the ROUTER, to be transferable (physical container) through the X.25 network to the LAN GATEWAY machnine. Network error message is also available.
- ROUTER: It compresses the data received from the application program in a defined data structure (logical container). The container can comprise database operation requests or messages. It directs the container to the proper destination (own server, central machine, other server, other workstation). Practically it can be used by application programs written in any program language.
- UNIUSER: To the application programs it is a unified, menu driven user interface using windows. It is available for C and Clipper languages.

Memory Map of the WS

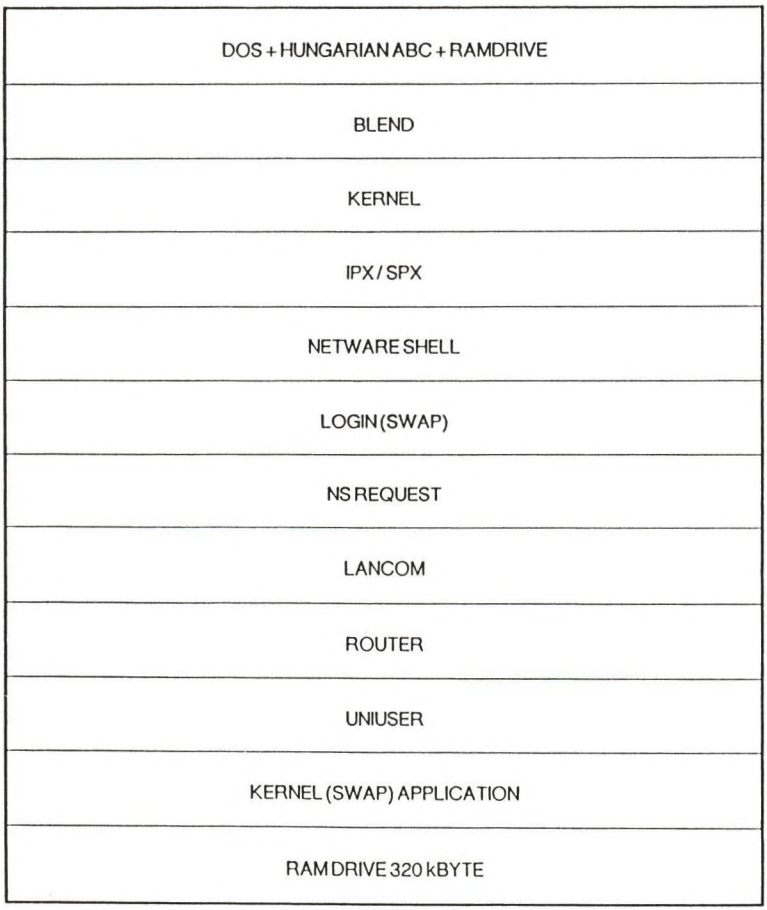


Figure 2

- FRAMEWORK: Following the switch on of the workstation is starts automatically, and for safety reason the user cannot exit from it to the operation system. It carries out the identification of the user, controls the user's access-warrant, and respectively, loads the special applications to the memory.

6.2. On the servers

The NOVELL servers are dedicated machines, MS-DOS applications cannot be run on them. For special needs so-called Value Added Process-es (VAP) can be written. Such processes carry out for example, the refreshment of the databases at the workstations and servers when downloading the data from the central machnine. Also program download, file-transfer, message sending and receiving are available with them.

6.3. On the Central Machine

The architecture of the programs written for the central machine can be seen on Fig.3:

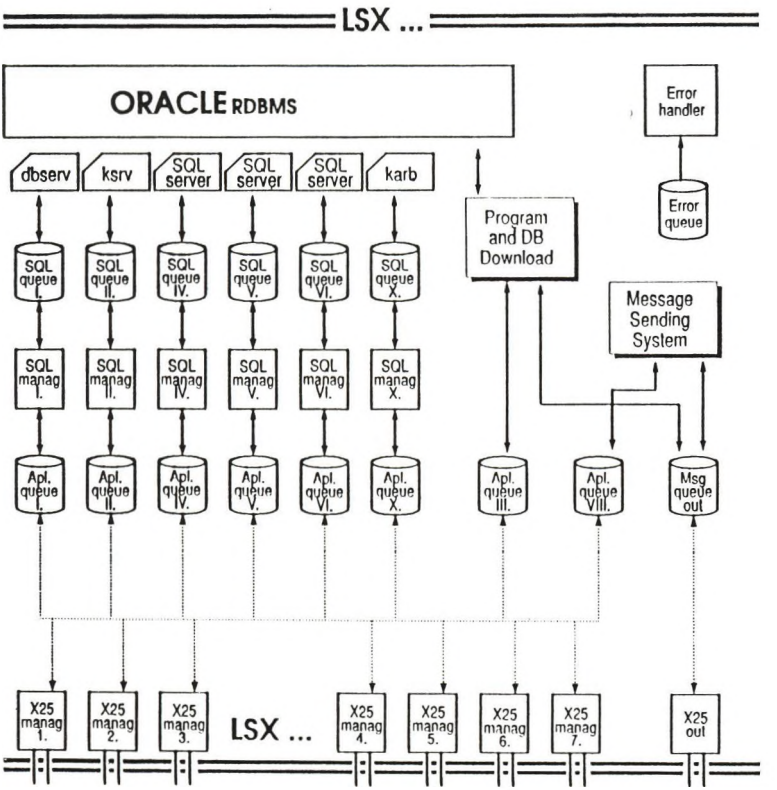
- X.25 Manager: Program based on the X.25 services of the Olivetti machine which receives the physical containers from the network, converts - those which belong together - into logical containers, then transfers them to the SQL Manager.
- X.25 Out: When loading down the program and the data, and at message transferring it initiates calling, and it transmits the containers to the X.25 network.
- SQL Manager: Mostly it serves the SQL Servers which it forwards the containers to. In the case of a line brake it ensures fault protection, e.g. it ensures that the same container requesting the modification of the database should not be transferred twice to the SQL Server. Due to the necessary limitation of the communication load, a workstation is allowed to request only a certain amount of data from the central computer. If the request provides more data than this, the data are stored by the SQL Manager. The workstation gets the other pages of the data from the SQL Manager, without accessing the database again.
- SQL Server: It mees the requirements of the applications running at the workstations by carrying out the requested database operations, it returns the result to the workstation through the SQL Manager.

7. The IBISZ Application System

The IBISZ application program involves the whole software system meeting the applicational requirements of the different business areas of IBUSZ.

The division ot the application system is parallel with the different business areas of IBUSZ.

SW Components on the LSX Machine



X25 Connection

Figure 3

First the account management system was effected which was followed by the travel system. While using these two systems effectively, the development of further applications is going on, e.g. program planning, hotel reservation system, time-limited deposits, etc.

In the national computer network of IBUSZ and IBUSZ Bank the Olivetti central computer has been installed in the IBUSZ computer center, and the workstations of the local network can be fund in the offices. According to the present state, appx. 60 servers and 450 workstations are involved in the system. By this system the DATAPOINT system of IBUSZ-'central computer - terminals without intelligence' has been replaced. The countrywide extension and the main features of the system can be seen on Fig.4. and Fig.5.

8. Extension of the SYSTEM PLATFORM

The SYSTEM PLATFORM of SzKI is open, which means applying not only new communication protocol standards, interfaces, HOST systems, but also the integration of tools representing a higher technical and servicing level of the integrated communication. The extended SYSTEM PLATFORM can be seen on Fig.6.

The SYSTEM PLATFORM has been extended by:

- TCP/IP protocol layer
- Initiating of UNIX machines

In connection with the SYSTEM PANEL and TOOLs:

- the TCP/IP version has been under elaboration
- The forming of the tools for initiating ISDN like communication has been started

In the tool basis:

- UNIX,
- UNIX based SQL
- MS-DOS v5.0
- Windows v3.0

have been integrated.

The extended SYSTEM PLATFORM opened the possibility for the typical bank applications (e.g. ATM).

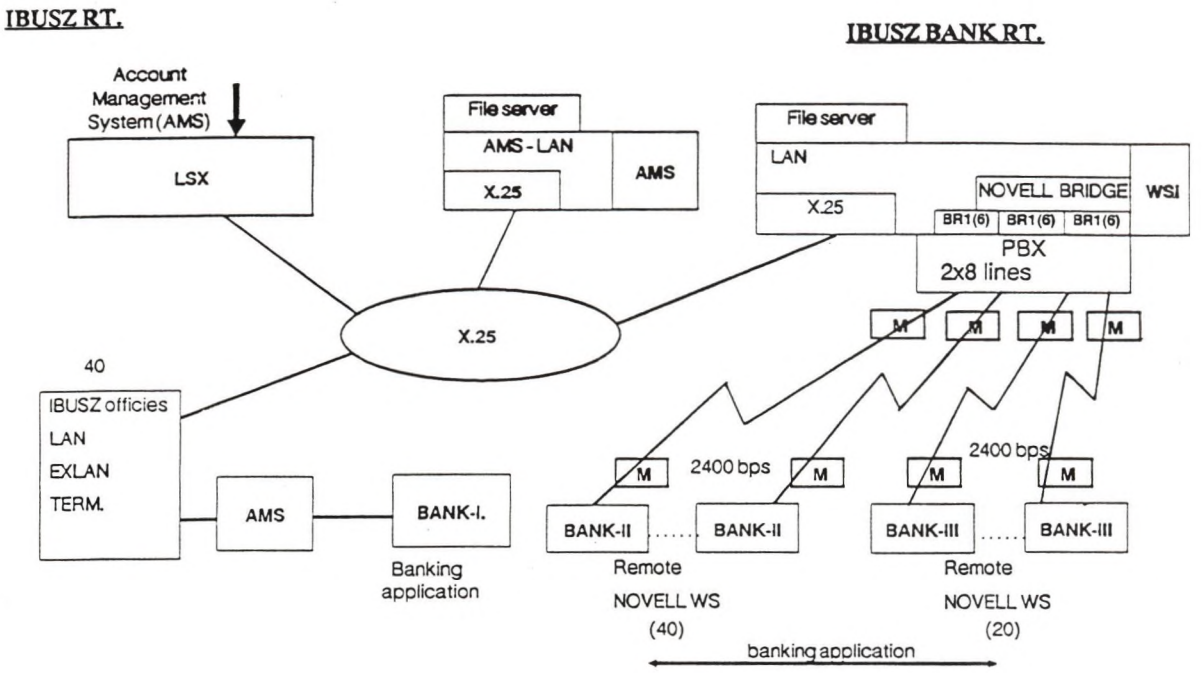

IBUSZ RT.
IBUSZ BANK RT.
Account Management System (AMS)
LSX
File server
AMS - LAN
X.25
AMS
File server
LAN
X.25
NOVELL BRIDGE
WSI
BR1(6)
BR1(6)
BR1(6)
PBX
2x8 lines
X.25
M
M
M
M
40
IBUSZ officies
LAN
EXLAN
TERM.
AMS
BANK-I.
Banking application
M
2400 bps
M
M
2400 bps
M
BANK-II
BANK-II
BANK-III
BANK-III
Remote
NOVELL WS
(40)
Remote
NOVELL WS
(20)
banking application

Figure 4

Nationwide Information System of IBUSZ-RT and IBUSZ-BANK-RT

Main features:

- Olivetti LSX 4240 fault tolerant central computer,
- some 100 offices around the country,
- 40 LAN systems, 60 external connections,
- some 400 workstations,
- private X.25 telecommunication system,
- 100 connections via modems,
- on-line transaction processing,
- message and download system,
- LSX-LAN and LAN-LAN connections,
- SQL,CLIENT-SERVER data communications,
- ORACLE based distributed data management

Figure 5

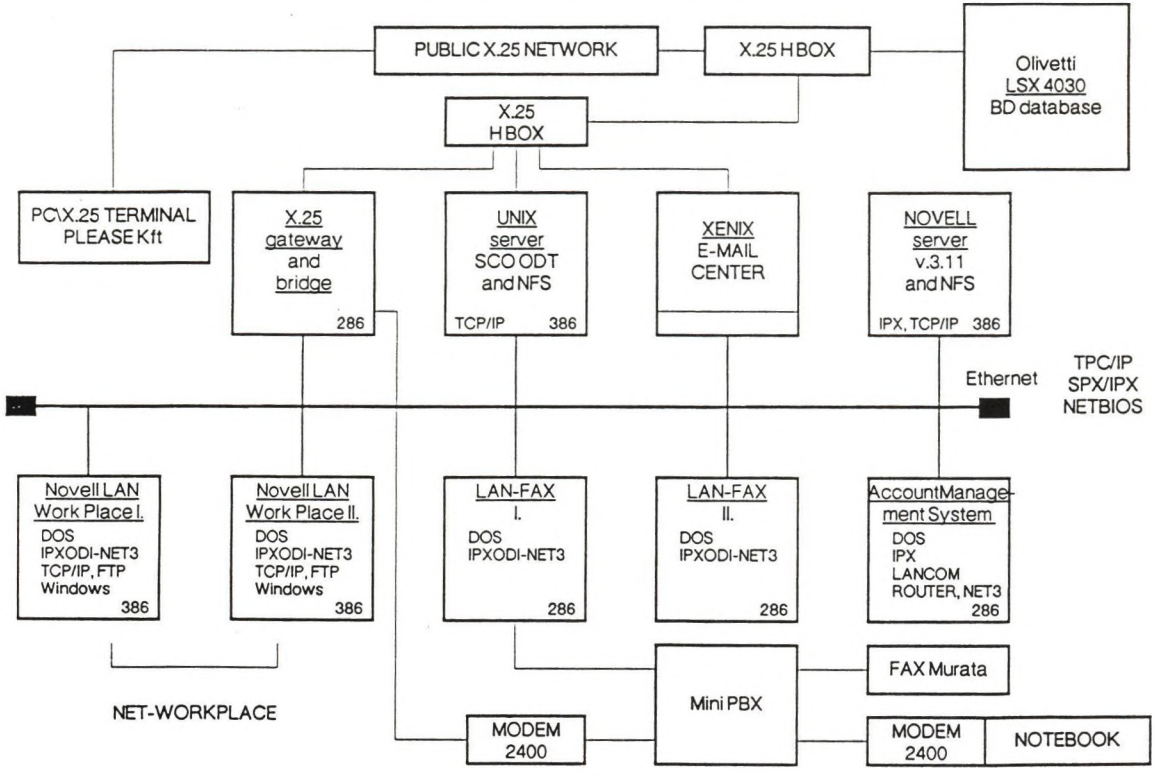

PUBLIC X.25 NETWORK
X.25 HBOX
Olivetti
LSX 4030
BD database
X.25
HBOX
PC\X.25 TERMINAL
PLEASE Kft
X.25
gateway
and
bridge
286
UNIX
server
SCO ODT
and NFS
TCP/IP 386
XENIX
E-MAIL
CENTER
NOVELL
server
v.3.11
and NFS
IPX, TCP/IP 386
Ethernet
TPC/IP
SPX/IPX
NETBIOS
Novell LAN
Work Place I.
DOS
IPXODI-NET3
TCP/IP, FTP
Windows
386
Novell LAN
Work Place II.
DOS
IPXODI-NET3
TCP/IP, FTP
Windows
386
LAN-FAX
I.
DOS
IPXODI-NET3
286
LAN-FAX
II.
DOS
IPXODI-NET3
286
AccountManage-
ment System
DOS
IPX
LANCOM
ROUTER, NET3
286
NET-WORKPLACE
MODEM
2400
Mini PBX
FAX Murata
MODEM
2400
NOTEBOOK

Figure 6

9. Application Development

The planning and specifying of the applications take place within the framework of the IBUSZ and SzKI cooperation. During the course of planning the applications it is very important to build the distributed database correctly, to decide the storing site of the certain databases and the through specification of the connection between them. Consequently, the final decisions are preceded by carefully, numerically defined analyzis and examination for database consistency. The effectuation of the system is carried out according to the software technology defined in the SYSTEM PLATFORM.

The forming of the SYSTEM PLATFORM compatible applications is promoted by the obligatory usage of the DEVELOPING TOOLs, within which the unified application level towards the user are ensured by the UNIUSER, and the ROUTER enables access to the databases stored at different levels of the system and also the message sending.

For supporting the development we have created the so-called PILOT system, in which each component is parallel with that of the real system, and there is only quantitative difference. The system integration, the development and the testing of programs take place in the PILOT system. The tested program is also transferred by the 'in-house' developed DOWNLOAD system to the servers and workstations of the IBUSZ network.

BANKNET

Data Communications Made Easy

- Do you need to exchange data with your head/regional offices outside and inside Central Europe and the CIS?
- Do you have difficulty in getting good quality, reliable lines?
- Do you spend hours sending the data when you should spend minutes?
- Do you wish there was a system which would give you highly reliable, high speed, readily available data communications?

If your response to any of these questions is "YES" then *BankNet* has the answer.

- BankNet provides a highly cost-effective data communications service everywhere in Europe and the CIS.
- BankNet uses low-cost satellite links and you, therefore, do not have to rely on the poor terrestrial infrastructure in the region. Plus the cost does not increase with distance.
- BankNet gives you instant access to your own virtual private data network.
- BankNet guarantees 99.5% availability, high speed links and can install anywhere in the region in a very short space of time.

For further information on how BankNet can make your intra-company communications more cost-effective call (36-1) 202-7083.

Budapest Office: **BankNet kft, 1016 Budapest, Naphegy tér 8, Hungary.**
Tel: (36-1) 202 7083 & 202 6246 & 175 6722 & 118 8683 Fax: (36-1) 175 8364

John von Neumann Computer Society

Austrian Computer Society

HIGHLIGHTS OF COOPERATION

1984 COOPERATION AGREEMENT SIGNED
1988 INTERNATIONAL COMPETITION FOR CARTOONS ABOUT COMPUTINC
1991 JOINT PROPOSAL TO HOST IFIP '96
1992 WORKING CONFERENCE ON TRANSPUTER APPLICATION
1994 JOINT EXHIBITION EXPONET WIEN '94
1998 JOINT CONGRESS IFIP '98

REGULAR JOINT CONFERENCES

1984 LOCAL AREA NETWORKS (BUDAPEST)
1987 INFORMATICS 2000 (SOPRON)
1988 BEYOND NUMBER CRUNCHING (GRAZ)
1989 MAN AND MACHINE (BUDAPEST)
1990 FUTURE TRENDS IN INFORMATION TECHNOLOGIES (SALZBURG)
1991 INTELLIGENT SYSTEMS (VESZPRÉM)
1992 SHIFTING PARADIGMS IN SOFTWARE ENGINEERING (KLAGENFURT)
1993 THE CHALLENGE OF NETWORKING (SZOMBATHELY)