42

Experiences in Multi-domain Management System Development

D Lewis
Computer Science Department, University College London
Gower St., London, WC1E 6BT, U.K., tel: +44 1713911327, fax: +44 1713877050, e-mail: d.lewis@cs.ucl.ac.uk

S O'Connell and W Donnelly
Broadcom Eireann Research Ltd
Kestrel House, Clanwilliam Place, Dublin 2, Ireland, tel: +35 316761531, fax: +35 316761532, e-mail: soc@broadcom.ie, wd@broadcom.ie

L Bjerring
TeleDanmark KTAS
Teglholmsgade 1, DK-1790 Copenhagen V, Denmark, tel: +45 33993279, fax: +45 33261610, e-mail: lhb@ktas.dk

Abstract

The deregulation of the global telecommunications market is expected to lead to a large increase in the number of market players. The increasing number of value added data services available will, at the same time, produce a wide diversification of the roles of these players. Subsequently the need for open network and service management interfaces will become increasingly important. Though this subject has been addressed in some standards (e.g., ITU-T M3010) the body of implementation experience is still relatively small. The PREPARE[1] project has, since 1992, been investigating multi-party network and service management issues focusing on a multi-platform implementation over a broadband testbed. This paper reviews the problems encountered and the methodologies followed through the design and implementation cycle of the project.

Keywords

Multi-domain management, TMN, implementation methodologies, management platforms

---

[1] This work is partially sponsored by the Commission of the European Union under the project PREPARE, contract number R2004, in the RACE II programme. The views presented here do not necessarily represent those of the PREPARE consortium.

A. S. Sethi et al. (eds.), *Integrated Network Management IV*

1. INTRODUCTION

The RACE II project PREPARE has investigated the development of a Virtual Private Networks (VPN) services using heterogeneous, multi-domain, multi-technology, broadband network management systems. This culminated, in December 1994, with the public demonstration of an implementation of such a system working over a broadband testbed network. The complexity of such a combined service and network management system and the large number of key players involved in the VPN service (i.e. network providers, third party service providers, customers and end-users) made it clear from the outset that a development methodology to support the full design and implementation cycles of the service was required. It is the aim of the authors to present an overview of the approach taken by PREPARE in realising this prototype VPN service, in order to provide some insight into how to address such problems of inter-domain management system development in future Integrated Broadband Communications networks.

2. PROJECT AIMS

The PREPARE project was proposed with the aim of investigating network and service management issues in the multiple bearer and value added service provider context of a future deregulated European telecommunications market. The specific example selected for implementation in PREPARE was of a Value Added Service Provider (VASP) co-operating with multiple bearer service providers to deliver a VPN service to a geographically distributed corporate customer. In order that these investigations had a realistic focus a broadband testbed network was assembled over which the VPN service would be demonstrated. This testbed consisted of several different but inter-working network technologies. Each of these sub-networks possessed its own network management system that was developed according to the principles laid down in the ITU-T Telecommunications Management Network (TMN) recommendations (ITU-T, M.3010) and using platforms supporting the OSI CMIP mechanism (ITU-T, X.700). The investigations into such multi-domain management involved the development of an architecture that allowed these separate network management systems to co-operate in providing end-to-end management services. This architecture was also developed to be conformant with the TMN reference model.

The make-up of the project consortium added a further important and realistic aspect to these investigations in that many project partners play roles that will be relevant to the realisation of future multi-domain management. The project partners and their relevant roles are:

- a network operator (KTAS), interested in integrating wide area network management with multi-domain service management based on TMN principles,
- a network equipment vendor (NKT Electronik), interested in the management of Metropolitan Area Networks (MANs) and the management of heterogeneous network inter-working,
- a customer premises network and management platform vendor (IBM: Token Ring and Netview/6000), who are interested in using their products in a multi-domain environment,

- a vendor of network management platforms (L.M. Ericsson A/S in co-operation with Broadcom Eireann Research), interested in the application of the TMOS Development Platform to value added service provision,
- researchers into advanced network management techniques (University College London, Marben and GMD-FOKUS), interested in applying their platforms to the multi-domain environment,
- researchers into multimedia applications (University College London), interested in the interactions of these applications with service and network management.

Each project partner, therefore, brought to the project their own specific interests, sometimes overlapping but often different or even contradictory. Therefore, though we were not operating in a true commercial environment, the view points of the customer, the value added service provider, the bearer service provider, the end user and management platform vendor were all genuinely represented. We can therefore assert that the methods we chose in arriving at our implementation were not purely influenced by the needs of a collaborative research project but reflect an environment in which future broadband management systems will be defined.

3. MULTI-DOMAIN MANAGEMENT SYSTEM DEVELOPMENT

The process of defining management services and information models in an environment that contains several different types of player and corresponding administrative domain has received some theoretical attention but the body of actual experience with large scale developments is still very limited. This section reviews the standardised methodologies available for management system design and their relevance to the PREPARE work. It then describes the process actually followed in PREPARE to develop a multi-domain management system.

3.1 Standardised Methodologies

The need for a methodology to support the identification and specification of the management requirements and capabilities related to the management of telecommunications networks, equipment and services is well understood by the standards and other related bodies. The main methodologies proposed to date include the ITU-T's M.3020 (ITU-T, M.3020), the Network Management Forum's Ensemble concept (Network Management Forum, 1992) and ISO's ODP framework (ITU-T, X901).

The TMN interface methodology, as defined in M.3020, forms part of the wider TMN management framework as defined in the M.3000 series of recommendations. The methodology is primarily designed to aid the specification and modelling of management functionality at any well-defined TMN interface.

Though in general the standards concentrate on the specification of generic solutions for general management problems, there is a need to tailor these solutions to solve specific management issues. The Network Management Forum group proposes the use of the Ensemble concept as a solution. The Ensemble approach is to select from the pool of standards outputs a solution appropriate the management problem and to enhance these with other support items (management information libraries and profiles) to produce maximum effectiveness. An ensemble template is provided in OMNIPoint 1 recommendation.

The ODP framework provides five key viewpoints and corresponding languages to support the specification of the problem domain. These are the enterprise, information, computation, engineering and technology viewpoints.

The major difference between the Ensemble and TMN methodology process is the scope of the two methods. The scope of the Ensemble is more focused in that ensembles are defined for specific management problems whereas M.3020 aims more at generic solutions, being intended more for use by standardisers rather than customer implementors. The Ensemble concept also defines conformance and testing requirements. The ODP framework is complementary to both methodologies in that the five viewpoints may be applied in both cases to enhance their approaches.

The major limitations of all these approaches in the case of PREPARE are that they either do not have sufficient scope or, in the case of ODP, are too general and the mapping onto TMN is not well defined. Furthermore the PREPARE project required a methodology that covered the service specification, design and implementation phases of the demonstrator work, whereas the scope of these methodologies only covers part of the specification and design process. Finally, and significantly for PREPARE, the three approaches are designed implicitly more to support single system design. None of the methodologies provide sufficient specific support for designing and implementing co-operative, multi-domain management systems. These facts resulted in no standard methodology being adopted for PREPARE. This was compounded by the fact that the pressure to provide an implemented result over-rode the desire to follow methodologies that were at that time immature and therefore not well understood by the project members. The project required instead that a mixture of the three approaches be taken. In effect it was realised that a pragmatic approach was necessary that would be primarily driven by the experience accumulated by the project members as a result of their involvement in similar work in other projects (e.g., RACE 1 Research Program). This approach is detailed in the following section.

3.2 The PREPARE Methodology

From the outset, the project followed a plan consisting of the following stages:

1. The definition of the management scenarios we wished to demonstrate, together with the supporting TMN architecture, management service definition and information models. This was conducted through 1992.
2. The implementation of the intra-domain systems required to manage the individual sub-networks making up the demonstrator testbed and the implementation and integration planning for the inter-domain management components, conducted through 1993.
3. The testing of the inter-domain components and their integration with the intra-domain management components and the actual testbed network. This work culminated in a public demonstration event in December 1994.

The broadband testbed used for the VPN management service consisted of an ATM WAN, ATM multiplexers, a DQDB MAN, a Token Ring LAN, and multimedia workstations. The enterprise context in which the VPN service was assumed to operate dictated that the WAN and MAN were separate public networks while the ATM multiplexers and Token LANs were Customer Premises Networks (CPNs). Both the public networks and the CPNs had their own separate management Operation Systems (OSs). To provide the VPN management

service a separate third party Value Added Service Provider OS was introduced. This coordinated VPN resources management via X-interfaces to the public network OSs and provided customer access and control to the VPN service via X-interfaces to the CPN OSs (see figure 1).

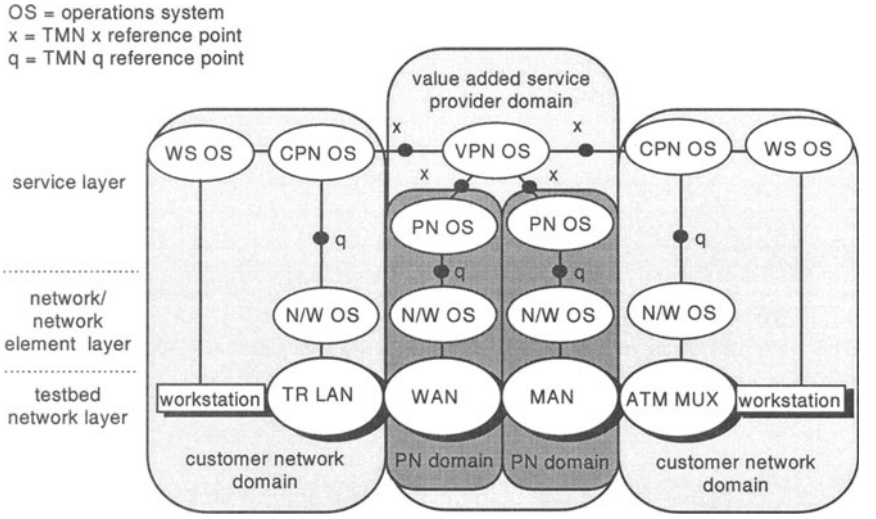

Figure 1.: PREPARE TMN Architecture

The fact that a different project partner was to implement the management systems for each of the different public networks and CPNs emphasised from the beginning of the project the administrative and human communication problems encountered in attempting to develop multi-domain management systems. This led to an emphasis on the X-interface where the different organisation's management systems had to interact.

Against this background the first stage of the work proceeded with four different groups being formed to generate; management scenario definitions, a TMN based management architecture, management service definitions and management information model definitions. The objectives of these groups were respectively as follows:

- The aim of the scenarios group was to produce a set of scenarios that would detail what would be demonstrated over the testbed network. Due to the large number of participants, components and requirements involved, these scenarios were essential in order to focus the work onto a manageable subset of demonstrable operations while at the same time presenting a coherent and realistic description of what was to be demonstrated.
- The architecture group had the task of interpreting the TMN recommendations in order to produce an implementable framework that specified how the components in the different domains should be interfaced to each other in order to provide end-to-end services.

- The management services group had to define a set of services that operated between the different management domains in accordance to the Abstract Service Definition Convention recommendation (ITU-T, X.407).
- The work required from the information modelling group consisted of defining the information models required by the various OSs that were involved in inter-domain relationships, according to the Guidelines for the Definition Managed Objects recommendation (ITU-T, X.722).

Due to restrictions of time and man-power these group's activities were in general conducted in parallel. At the beginning of 1993 a review was conducted of the work performed in the first stage and its suitability for supporting the implementation work. The output from the scenarios group described the roles of the human users and organisations involved in the VPN service as well as the motivations for the operations performed. This was supplemented by documentation of the commercial service that the VPN provider should provide to its customers. The architecture group identified all the management components required for the intended end-to-end VPN services and the different interfaces required within a TMN framework. It soon became apparent that the scenarios contributed greatly to everyone's understanding of the problem while the architecture was generally agreed upon as being suitable for the implementation of the VPN service. However it was also recognised that the outputs from the management services and information modelling groups suffered in many respects. Firstly these two sets of output were not mutually consistent, nor were they totally aligned with the output of the scenarios and architecture groups. Co-ordinating this work while running the groups in parallel had proved too complex a task given the man-power available. Secondly it was felt that, given the goal of demonstrating the scenarios; the service and information model specification were not complete and did not contain the level of detail required by the implementors. For example, although the detailed GDMO specification of all the agents in the architecture was essential, the managed object (MO) behaviour descriptions could not accurately convey the functionality of the operation systems which needed to be supported. Furthermore it was felt that a complete ASDC description of the management services would still require much additional integration with the information model to satisfy the implementors.

A path was therefore chosen which involved abandoning the further definition of management services and concentrating on refining the scenarios. The existing scenarios were therefore refined from a level where they described the player's roles and their relationships, to a state where the same scenarios were described in terms of OSs with detailed descriptions of the management information flowing between them. Adopting this technique, a full GDMO specification for the whole inter-domain information model was quickly arrived at. This approach also had the intrinsic advantages of ensuring that all information modelling was directly focused on the desired implementation areas and provided an informal but relatively brief description of the functionality associated with the information model.

The entire information model for all inter-domain components was maintained in a single document referred to as the Implementor's Hand Book (IHB). It was apparent that although the aim at this stage of the design work was to arrive at a stable version of the information model, there would inevitably be changes required to the IHB as our understanding of the problem grew. For this reason the IHB was maintained as a living document. This task was

made considerably easier with the help of Damocles a GDMO parsing and checking tool developed by GMD-FOKUS. This was used to check the IHB for GDMO syntax errors, open references but more importantly it checked for consistency and completeness throughout the information model. This was especially useful considering the number of partners involved in

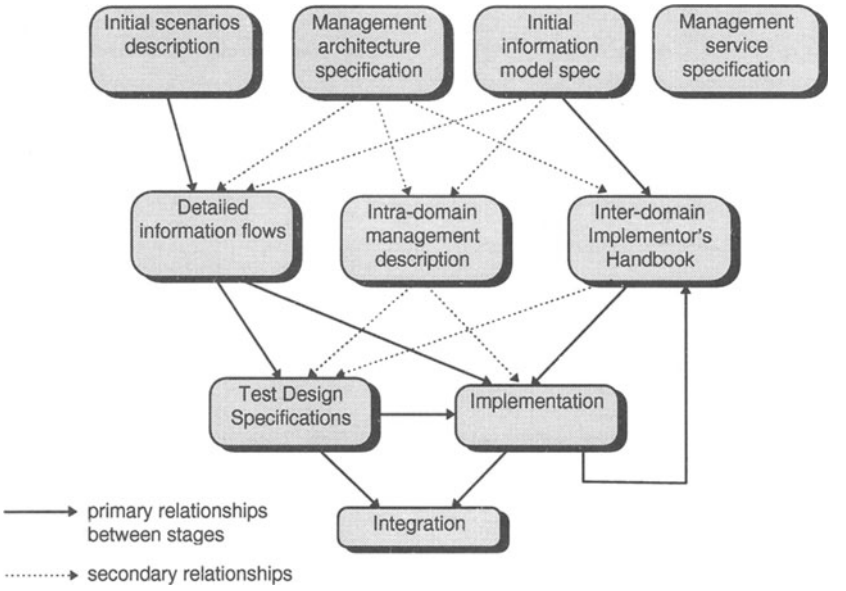

Figure 2.: Overview of Inter-domain Management System Development Methodology adopted in PREPARE

the writing of this document. A mechanism for requesting updates or modifications to the information model was also adopted since changes inevitably effected more than one partner's implementation work.

The IHB did not address intra-domain issues. However since each of the partners involved in intra-domain component implementation was represented during the scenario refinement and inter-domain information modelling, this work could be performed separately. The more difficult inter-domain modelling therefore became the principle group activity in the project, while the intra-domain definitions and implementations were the responsibility of individual partners.

As the IHB became stable and the inter-domain implementation began, the planning for integrating of the various hardware and software components commenced. This was conducted broadly following the IEEE standard 829-1983 (IEEE, 1983) which involved the generation of Test Design Specifications (TDSs) for all tests that would involve components from more than one partner. When this was performed for inter-domain management software components some interesting effects were observed. Firstly the refined scenarios proved to be

ideal templates for defining the interactions that should be tested, ensuring once again that the work performed directly supported the final aims of the project. Secondly, the TDSs were written to a level of detail that defined the actual CMIS primitives that should be exchanged between the OSs and the syntactical information required. This process of writing the TDS to such a level of detail provided much valuable insight for the implementors, in that it raised many issues that had not yet been recognised and allowed these problems to be resolved before the implementation work had progressed too far.

To summarise therefore, the method followed in PREPARE was focused on achieving a demonstrable result in a limited time frame. It was heavily influenced by its multi-domain context and the requirement to co-ordinate the different partners involved in the work. Figure 2 summarises the approach adopted.

4. IMPLEMENTATION PLATFORMS

In addition to the development methodology, another key factor in management system design is the choice of platform. Due to a combination of individual partner's interests in this area and the large monetary investment often required in network management platforms, no single platform was adopted by the project. Instead each partner was free to select one, provided the platform was able to support (PREPARE, 1992): a Q3 and X TMN interface, the development of manager and agent management applications and the implementation of custom managed object classes.

The following platforms were used in the PREPARE testbed:

OSI Management Information Service (OSIMIS): This was developed by the University College London (UCL, 1993) as a result of participation in a number of EU funded projects from the RACE and ESPRIT research programs. An object oriented API is provided for implementing management applications working in either the agent or manager roles. Within PREPARE, OSIMIS has been used to implement the Inter-Domain Management Information Service (IDMIS), (RACE, 1993- H430), Q-adapters for nodes of the ATM WAN and ATM multiplexer and the OS that provided network management facilities and a service level X-interface for the DQDB MAN.

Netview/6000: The management information associated with the Token Ring is made available to other OSs via IBM's NetView/6000 management system.

OpenView: Hewlett-Packard's OpenView CMIP development environment was used to develop the OS that managed the ATM multiplexer based CPNs at the VPN service level.

Telecommunication Management and Operations Support (TMOS): This platform developed by L.M. Ericsson was used by L.M. Ericsson and Broadcom Eireann Research to develop the VASP OS and its operator's user interface.

In order to test and adjust the various platforms so that they could interchange management data using CMIP, a test MO (based on the Network Management Forum test object) was initially used. This MO contained the basic GDMO structure of a generic managed object (i.e., packages, notifications, attributes, etc.) so that when implemented over the various platforms the interchange of its management data could be tested and any problems identified.

A number of different platform related problems were identified while implementing this test managed object and during the subsequent development of the different OSs. These included the variation in the use of name bindings varied with each platform. For example, the information model within the TMOS platform starts with the network object being at the top of the containment tree whereas in the OSIMIS platform the standardised system MO is at the top of the containment tree. To overcome this, a translation function was necessary.

5. OPEN ISSUES

The experience of the PREPARE project in designing and implementing its VPN services reinforces the fact that realising inter-domain services is an extremely complex issue and requires the support of a methodology to integrate the service specification, design and implementation processes. The PREPARE approach provides a window into the type of issues that need to be addressed in inter-domain management system development and some of these are outlined below.

5.1 Inter-domain Management and TMN

Where practical the project has attempted to base its approach on the work of the standards bodies. In particular the project's approach to defining an implementation architecture to support its design and implementation work is mainly based on the TMN architectural framework. The main conclusion of the project was that the TMN framework could support the design of inter-domain service management systems. However, having a view on the future IBC environment which emphasises dynamicity and openness it is clear that the framework requires extension to provide support for a number of issues. This includes support for a globally available information service for storing, accessing and maintaining globally relevant information. A typical example is information about service providers, their offered capabilities, contact names and addresses, and "operational" information, e.g., communications addresses of OSs, information models and other information related to shared management knowledge. The OSI Directory provides a standardised approach to implementing the required technologies (RACE, 1994- D370). An approach to using the Directory in this way is demonstrated in PREPARE with the IDMIS system. This however has implications for the TMN Architecture. A proposal to; add a Directory System Function and corresponding d-reference point to the functional architecture; add Directory Objects to the information architecture and add Directory components like Directory System Agents (DSA) and Directory Access Protocol (DAP) to the physical architecture, has been presented to ITU SG IV, (Q.23/Q.5 meeting, May 1994) and subsequent meetings. We expect it to be reflected in future versions of M.3010 (Bjerring, 1994).

5.2 Security

Security within the PREPARE VPN management framework and particularly TMN is an important issue that has not been addressed so far within the project. Generally security refers to the application of an appropriate set of logical and physical measures in order to ensure the availability, accountability, confidentiality and correctness of the management data accessible to other TMN-like systems (RACE, 1994- H211). Open Network Provisioning (ONP) is expected to be introduced by the European Public Network Operators (PNOs) by the late 90's. In technical terms, the ONP concept emphasises the need to define and adopt

open non-discriminatory standardised interfaces to the underlying public network infrastructure for the provision of new value added services (Plagemann, 1993). To address this new trend in the public telecommunications industry a high degree of security is necessary to reduce the possibility of large monetary losses being suffered by customer commercial organisations, the various PNOs and service providers as a result of allowing the use of services like VPN, etc. For example, US telecommunications fraud is currently estimated to be in excess of $2.5 billion per annum (Wallish, 1994).

5.3 Use of Open Platforms

As discussed above, the realisation of inter-domain services requires that the various service developers need to support the concepts of shared management knowledge and inter-operability over open interfaces. However if a customer already possesses a management platform they will be very reluctant to implement additional applications in order to get management access to a value added service which they are buying. Instead they will require the value added service provider to provide the service management application in a format compatible with their existing platform, in much the same way that LAN and router equipment manufactures are starting to do now. This would only be viable for the value added service provider if an open API of some form was available across all platforms. This has already been addressed to an extent by X/Open with the XMP/XOM API (X/Open, 1992), however in a multi-domain environment, issues of management application interaction to provide end-to-end services and support for inter-domain security and location transparency still needs to be addressed.

6. FURTHER WORK

In 1993 the PREPARE project received additional resources to sponsor an extension of its work in 1994 and 1995. This new work has two main aims; first to extend the physical testbed from Denmark, were it is currently situated, to include ATM sites in London and Berlin (Lewis, 1994), and secondly to extend its multi-domain TMN investigation to more complex multi-player situations, including the addition of multimedia teleservices and their management requirements. As part of the latter aim the project must go through another cycle of specification of demonstrator goals, architecture definition, information modelling, implementation and integration. This has to be performed in about half the time of the previous cycle and may prove more problematic since there are potentially more inter-domain relationships in the anticipated architecture. However the experience gained by project members in the work described in this paper should greatly mitigate these problems and has already led to a work-plan that follows the same scenarios centred development path. This work will give us an opportunity to investigate the integration of both the existing management systems into the ones being developed. This will be done both through he reuse of the VPN management system already developed, and also through the inclusion of more of the standardised information models that are now available.

7. CONCLUSION

The experience of the PREPARE project is that the development of multi-domain management systems is a very complex task made mainly so by the presence in the

development process of more than one party. It was found that though some standardised methodologies exist, none at this time address the complexity of multi-domain systems, nor do they address all the stages of the development cycle. PREPARE has therefore developed its own pragmatic approach to the development of such systems. This approach is centred around the establishment of a set of scenarios that embody the core aims of the system being developed and therefore ensure that all work remains explicitly focused on those aims. By documenting scenarios at a high level initially, any conflicts between the requirements of different parties may be identified and resolved early on in the development process. These scenarios are then refined into detailed information flows as part of the information modelling process and finally they provide the basis for integration and test documents. PREPARE has found this method well suited to developing, with limited resources, multi-domain management systems that satisfy core requirements. The project will reuse this method in a new cycle of multi-domain management system development it is currently embarked upon.

REFERENCES

ITU-T Recommendation X.407, Abstract Service Definition Convention.

Bjerring, L.H., Tschichholz, M. (1994), *Requirements of Inter-Domain Management and their Implications for TMN Architecture and Implementation*, Proc. of 2nd RACE IS&N Conference, Aachen.

RACE Common Functional Specification D370 (1994), *X.500 Directory Support for IBC Environment* (Draft).

PREPARE (1992), *D2.2A Open Architecture and Interface Specification*, CEC Deliverable No. 2004/IBM/WP2/DS/B/002/b1.

ITU-T Recommendation X.722, *Guidelines for the Definition of Managed Objects*

RACE Common Functional Specification H221 (1994), *Security of Service Management Specification.*

RACE Common Functional Specification H430 (1993), *The Inter-Domain Management Information Service (IDMIS).*

IEEE (1983), *Standard for Software Test Documentation*, IEEE Std. 829.

Lewis, D., Kirstein, P. (1994), *A Testbed for the Investigation of Multimedia Services and Teleservice Management*, Proceedings of the 3rd International Conference on Broadband Islands.

ITU-T Recommendation M.3010 (1992), *Principles for a TMN.*

ITU-T Recommendation M.3020, *TMN Interface Specification Methodology.*

Network Management, Forum (1992), *OMNIPoint1 Specifications and Technical Reports*, Book 1 & 2.

ITU-T, Draft Recommendation X.901 (1993), ISO/IEC JTC 1/ SC 21/ N 7053, *Basic Reference Model of Open Distributed Processing* - Part 1 Overview and Guide to Use, December.

Plagemann, S. (1993), *Impact of Open Network Provisioning ONP on TMN*, Proceedings of the RACE IS&N Conference, Paris.

UCL (1993), *The OSI Management Information Service*, Version 1.0, for system version 3.0, University College London.

Wallish, P. (1994), *Wire Pirates,* Scientific American.

ITU-T, X.700, *OSI Systems Management*, X.700- Series Recommendations, OSI Systems Management.
X/Open (1992), OSI-Abstract-Data Manipulation and Management Protocols Specification,

BIOGRAPHY

David Lewis graduated in electronic engineering from the University of Southampton in 1987 and worked as an electronic design engineer for two years. In 1990 he gained a Masters in computer science from University College London where he subsequently stayed as a research fellow in the Computer Science Department. Here he has worked on primary rate ISDN hardware development and Internet usage analysis before joining the PREPARE project in which he has worked both in B-ISDN testbed definition, integration of multimedia applications and development and implementation of inter-domain management systems. He is currently conducting a part-time Ph.D. on the management of services in an open service market environment.

Sean O'Connell qualified in 1991, with an honours degree in Computer Science from the University College Dublin (UCD) following the completion of his scholarship funded final year project in secure E-Mail. He took up a research position with Teltech Ireland at UCD where he spent two years working on various security related projects including secure FTAM, the Security Management Centre, the AIM Project SEISMED and his masters degree. He left UCD in September '93 to join Broadcom Eireann Research where he is currently working on PREPARE and related security projects. His main areas of interest include cryptography, open systems security, OSI management, TMN and ATM technology.

Willie Donnelly graduated in 1984 from Dublin Institute of Technology with an honours degree in Applied Sciences (Physics and Mathematics). In 1988 received a Ph.D. in Particle Physics from University College Dublin. From 1988 to 1990 he worked with the design and implementation of Industrial control and Monitoring systems. In 1990 he joined Broadcom Eireann Research is currently the group leader in the Network Management group and the project manager for the Broadcom team in PREPARE. He also active in the management aspects of a number of Eurescom projects (European PNO organisation). His main area of interest is the application of TMN to support ATM network management.

Lennart H. Bjerring graduated in 1987 as electronics engineer in Denmark. Since then he has been working for TeleDanmark KTAS partly in Systems Technology, partly in R&D. His main work area has been network management systems specification, implementation and operations in the Danish PSPDN, and, in recent years, participation in pan-European telecommunications management related projects. He joined the PREPARE project in 1992, working mainly on TMN-based inter-domain management architecture definition, information modeling, and definition of IBC-based Virtual Private Network (VPN) services.