A Framework for QoS Enabled IP-VPN Management

Sanjay Jha
School of Computer Science and Engineering
University of New South Wales
Kensington, NSW, Australia
sjha@cse.unsw.edu.au

Anil Sood
Telstra Corporation Limited
5/333 Exhibition St, Melbourne 3000
asood@telstra.com.au

Abstract

Emerging services such as Multimedia, Communities of Interest Networks (COINs), Intranets and Extranets which are required to meet the business and personal communications requirements for the next millennium depend upon Quality of Service (QoS) based IP Virtual Private Networks (IP-VPNs). From a service provider's perspective, their ability to exploit IP-VPNs will depend entirely on how they manage and deliver these services.

This paper assesses the issues and requirements related to the management of IP-VPNs, explores the various standards and their applicability to the realisation of IP-VPN management systems. It also provides an architectural framework for the management of QoS and policy based IP-VPNs services using a Directory Enabled Network platform based on a CORBA framework, the TMF model for process & operations management, and services & network management architectures proposed by the TINA Consortium.

1. Introduction

A Virtual Private Network (VPN) is private network constructed within a public network infrastructure such as the global Internet [ferg98]. Work has been done by a number of standards bodies, industry forums and research groups on management of specific types of VPNs implemented over a PVC based infrastructure such as ATM and tunnel based IP-VPNs [bjer97, bjer98]. The advent of newer technologies such as Asymmetric Digital Subscriber Loop (ADSL), Multiprotocol Label Switching (MPLS), IPSec [kent98, hein98] presents new opportunities and challenges both from the networking perspective as well as from the services and network management perspective.

This paper provides a flexible and highly adaptive architecture for network management system that incorporates business rules and enables process & workflow automation and which can effectively manage complex and changing services, product sets, business rules and processes commonly found within a service provider or telco environment. Section 2 provides requirement for buidling IP-VPNs. Section 3 defines scope of work presented in this paper. An overview of proposed architecture is discussed in section 4. Section 5 discusses Network Management Layer modelling using the TMF Business Process Modelling. Section 6 covers the architecture framework relating to the diverse data inventories which are required for the policy based and rule based implementation of IP VPNs. Section 7 discusses issues relating to Systems Management Layer (SML) and Network Management Layer (NML) interface. Section 8 proposes use of TINA service architecture for IP VPN session realisation. Finally configuration management, service provisioning , fault management and performance management issues are discussed in section 9-12.

2. IP VPN Requirements

The management of IP-VPNs to effectively meet business requirements, the following issues need to be addressed:

IP-VPN Service Configuration & Activation: Effective centralised management of activation and configuration is required.

Policy based differentiation: Management facilities need to cater for highly customised and differentiated services including QoS, Class of Service (CoS), and other resources based management.

Fault Management: Fault management for IP-VPNs includes IP-VPN visibility and end-to-end diagnostics, event and alarm correlation to reflect effect of events and alarms on services, and alarm management.

Usage Data Collection: Usage data collection should include traffic statistics for each IP-VPN including ingress and egress traffic volume per IP-VPN, traffic per tunnel and traffic per termination.

Performance Management and SLA Reporting: IP-VPN SLAs need to include metrics such as IP-VPN availability, QoS exceptions, delays and packet loss and indicators on

the Service Level Objectives (SLOs) associated with various servers used within the IP-VPN.

Security Management: Security management for IP-VPNs includes access authentication and authorisation, privacy and integrity of data within the IP-VPN as well as security associated with customer access to management information.

Customer Network Management: Customers need access to their specific service views. The Network Management System needs to represent IP-VPN management from a service (or IP-VPN) point of view. An additional requirement is for customers to have visibility of their services only.

Customer Self Care: Customer self care includes electronic access based on certificates/tokens for customers and the ability of customers to register, activate, and manage their services. Facilities such as the customer's ability to track trouble tickets monitor and pay for services online is an essential part of the customer self care model.

3. Scope

The scope of this paper is restricted to an architectural framework for the Network Management Layer (NML) regarding the management of IP-VPNs (figure 1). In particular it covers the functional areas described in the TMN model (ie. Fault, Configuration, Accounting, Performance and Security - FCAPS). As such, additional important issues such as Customer Self Care and Customer Network Management which are predominantly SML issues are not covered in this paper.

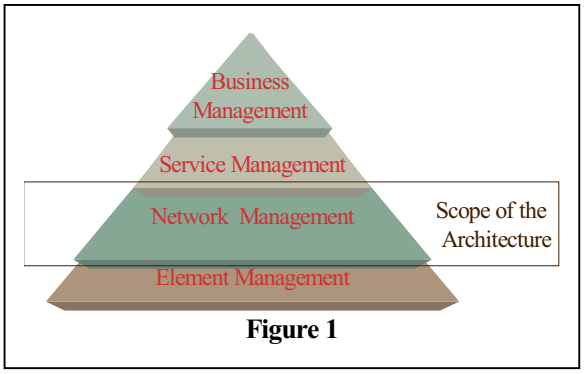

Figure 1

IP services typically span infrastructure provided by multiple ISPs. In the case of IP-VPNs, it is quite possible that a single IP-VPN may span more than one service provider (for example the access component at each termination end point could be via a separate ISP, while the core connectivity component may be from a traditional carrier). Issues relating to the provisioning of services across multiple administration domains have been covered to some extent in the TINA Service Architecture model [tina97j]. However, there does not as yet exist a clear standard for interoperability between administration domains. .Currently there is work in progress within the context of the IETF Internet2 Qbone Bandwidth Broker to resolve the inter-domain requirements [neil98o, rfc2475]. Within the context of this paper, it has been assumed that in the initial stages IP-VPNs will be offered within the domain of large integrated carriers who are able to offer nation wide IP as well as core connectivity services such as ATM and FR.

There is a distinct difference in the management of enterprise networks and the management of large scale and diverse telco or large service provider networks. While enterprise networks are limited in scope and size, telco or large service provider networks are extremely diverse and involve interworking between a myriad of technologies (for example while GUI based configuration tools may be attractive to an enterprise administrator, these are inappropriate from a telco perspective as they often do not scale well and are not adaptable to provisioning flow through). From a telco perspective, the following key principles apply:

Architecture choices should simplify network management: An increase in systems complexity leads to a disproportionately large increase in the cost and effort to manage it. There is a distinct need to reduce the number of systems and to rationalise and consolidate technologies, vendors, management domains, interfaces, and protocols.

Architecture should focus on an end to end view of the service: The primary aim of the architecture is to provide rapid and effective support to customer oriented systems and processes and therefore needs to reflect an end to end service view.

Architecture needs to be based on standards: A standards based architecture is mandatory for the coordination of diverse internal and external systems through common reference points for interoperability.

4. IP VPN Management Architecture Overview

The figure 2 describes the proposed architecture for the management of IP-VPN's. The architecture is based on:

- TMN model [itu95j, lewi96] for the overall management framework.
- TMF based process workflows [nmf98m, nmf98o] within the Cross Domain Manager (XDM) to provide an adaptive approach to implementation of workflows related to the provisioning of services within the XDM.
- TINA based component modelling within the Network Management Layer for the realisation of access IP-VPNs (Service Architecture [tina97j]) and the realisation of connectivity requirements for dedicated IP-VPNs (Network Resource Architecture [tina97f, tina97n]).
- Directory Enabled Network (DEN) [mso98, sju99] and Network Data Inventories (NDI) to store the diverse range of data relating to the IP-VPNs as well as network resources at each layer. The data stores also provide the

repository for storage of various rules and policies relating to the services deployed.

• CORBA based platform to provide an ubiquitous distributed computing platform.

•The idea of Service Management Layer (SML) is particularly useful in VPN where one Operation System Function (OSF) may be responsible for management of QoS and another for management of communications resources. Both OSFs need to communicate with each other and the NML. At the Service Management Layer (SML) - Network Management Layer (NML) interface, the concept of a Cross Domain Management is introduced. The XDM logically consolidates the multiple interfaces that a customer-facing system must contend with into a single well-defined CORBA IDL interface. This offers substantial insulation from the inevitable changes that would be required to these multiple interfaces as network systems adapt to new requirements. In effect, an SML system has only one interface to deal with and this interface's definition is likely to remain more stable by at least an order of magnitude. In practice, a changed network requirement (e.g. the induction of say, a new generation of ATM switches) is reflected by "snapping out" an old XDM component and "snapping back in" its updated version. Effectively, the architecture minimises the systems impact of altered business requirements and the introduction of new equipment or vendor domains.

•**Selection of Domains:** From a telco's or service provider's perspective, and current industry initiatives in the form of pilot project involving the SONET Interoperability Forum (SIF) [sif97] and the CATALYST project (involving TMF), the cross-domain management solution divides the network space along technology boundaries so that a coordinating XDM deals with technology specific domain managers. Within the IP-VPN management context, the following technology domains are proposed: IP Server Domain, IP Network Domain and the Layer 2 Domain. Details of these domains are discussed in the configuration management section.

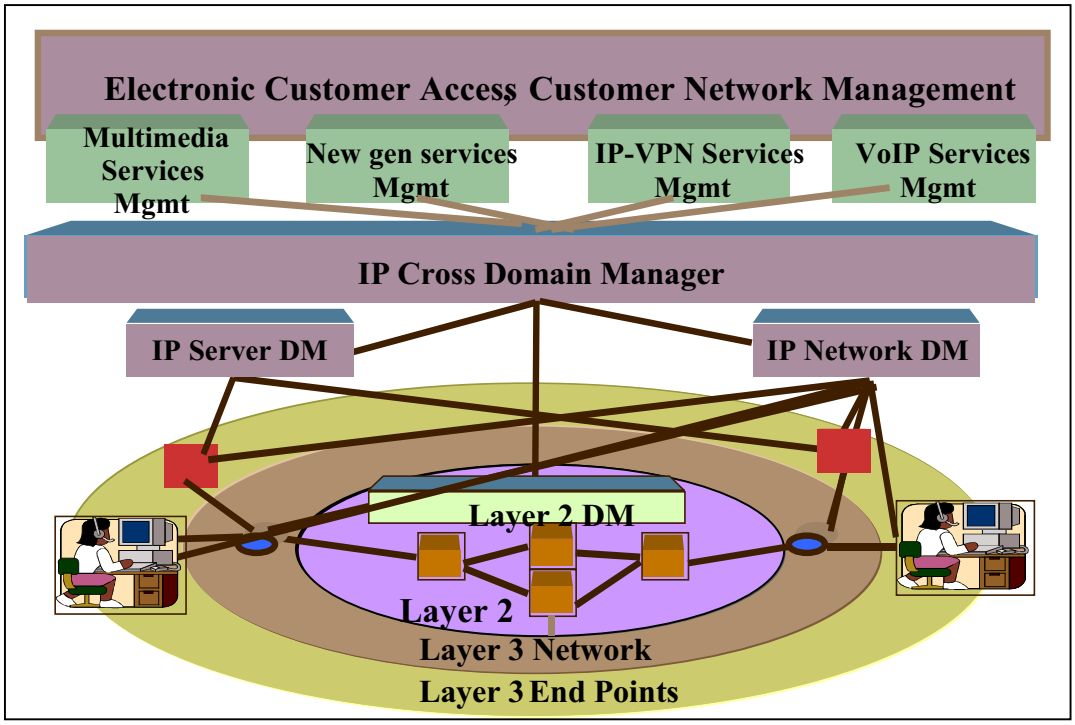

Figure 2 IP VPN Management Architecture

5. TMF BPM as basis of NML Modelling

The Network Management Layer (NML) for IP-VPNs needs to be highly flexible and adaptive to incorporate the ever changing business requirements of emerging new services as well as to deal with the complexity of implementing these services.

The TMF Business Process Model (BPM) depicts a sequence of activities related to specific business events (figure 3). Within the NML, the BPM is an ideal way to

model process workflows relating to a dynamic and highly interactive environment.

Implementation of the TMF Model: The TMF model does not lend itself to straight forward implementation. Two models are explored for the implementation, and a proposal is made in the paper to combine the function and data areas into a business object model and to model process workflows in terms of a intelligent agents suitable for implementation of processes.

Business Object Model: By integrating function, data and process, a business object model can provide the base for construction of a suitable application architecture. In such a schema, business objects correspond to detail at the level of subsystem or component definition.

The current industry trend is to model processes and process activities as objects thereby accruing all the benefits of object technology as compared to more traditional approaches.

Workflow Modelling: An alternative approach, and the one recommended in this paper, would be to tie the NML business objects together via a process workflow engine and to use high level process workflow systems to represent and code the business and technology rules within the NML. In this case, the objects would not need to encapsulate as much of the business process and would focus more on just encapsulating function and data. Recent advances in the usage of artificial intelligence in the modelling of process and workflows also lend themselves ideally to this approach. Adacel's Agentis set of process modelling toolset [wru99], and Hewlett Packard's ChangeEngine [hpc99] are some of the products which have been announced within the last few years and which can be used to effectively implement workflows within the NML layer.

It is desirable to the use a workflow engine as the process integration mechanism on the basis of its relative simplification of cross-organisational issues associated with management layer boundaries. Also the development of a workflow engine architecture has a more conservative learning curve than the implementation of a fully object oriented paradigm.

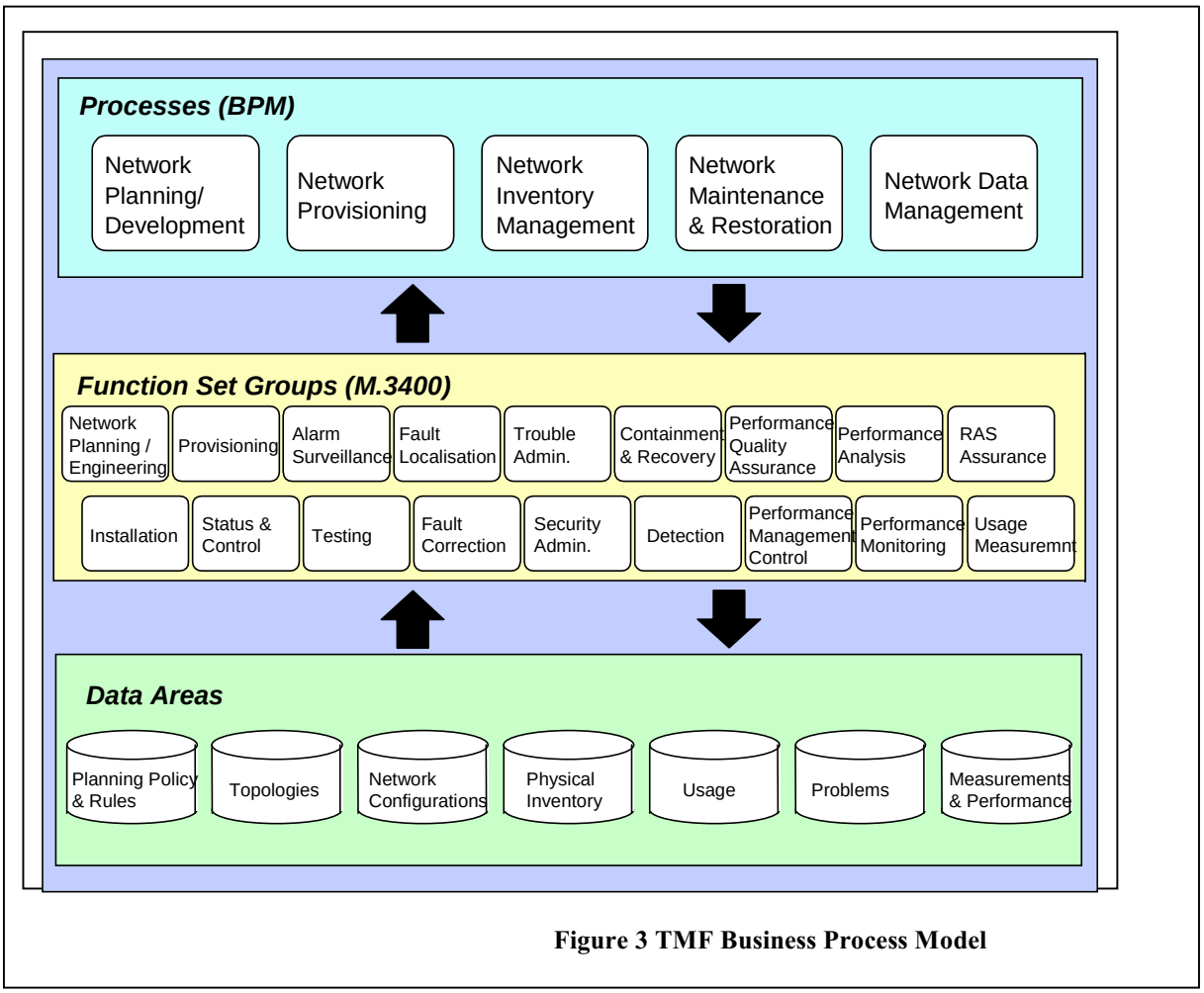

Figure 3 TMF Business Process Model

6. NML Network Data Inventory

This section covers the architecture framework relating to the diverse data inventories which are required for the policy based and rules based implementation of complex IP services such as IP-VPNs.

Network data as defined in the TMF model provides a good starting point. The TMF data stores needs to be augmented by other data inventories required for the management of IP-VPN, in particular, to incorporate policy based access and resources allocation.

Figure 4 shows the network data inventory system. There is a distinct requirement to implement the data stores in a directory environment. By virtue of being implemented in a directory, the data becomes ubiquitously accessible. Ubiquitous access to data is a prerequisite for the implementation of a substantial part of the network data inventories. Examples include network element configuration, network topology, network products, network rules, user profiles and preferences etc. Such a model for decomposition is also in alignment with the direction being adopted by the Directory Enabled Networking (DEN) initiative.

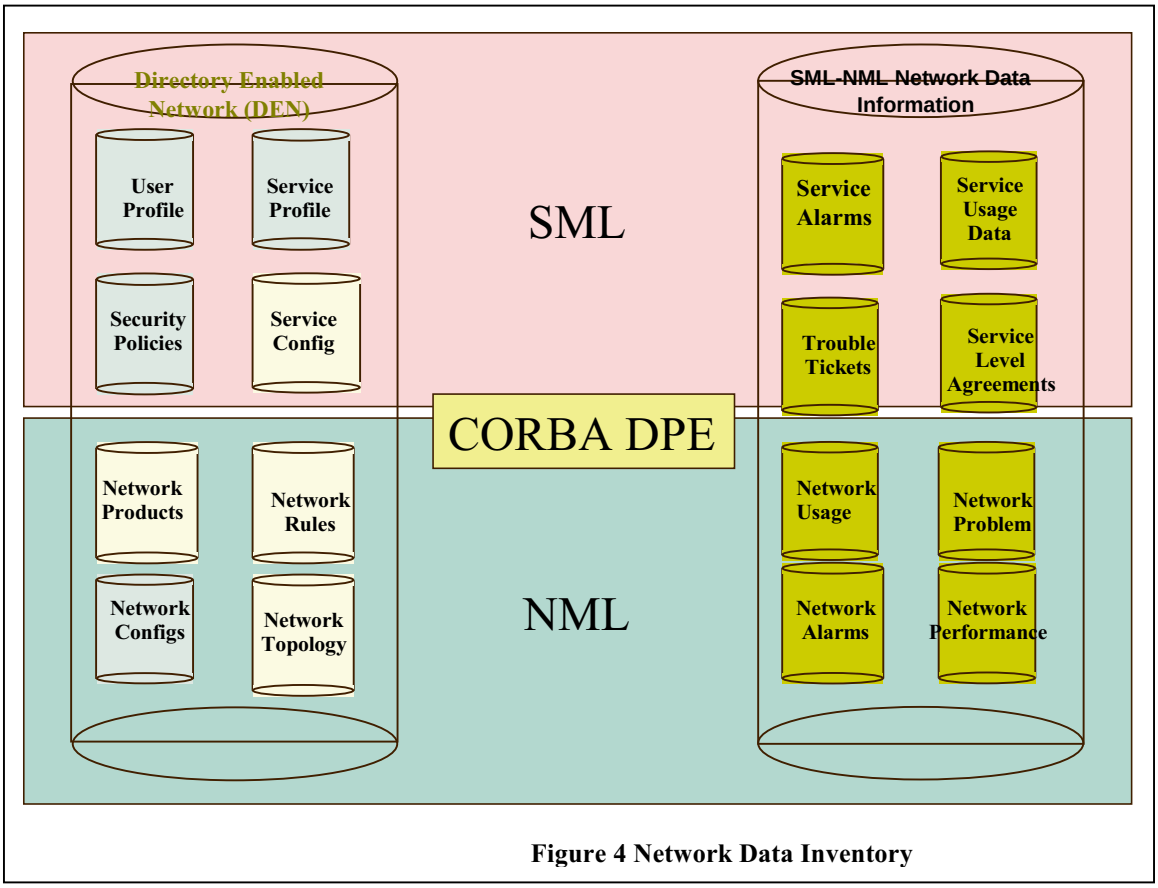

Figure 4 Network Data Inventory

In the longer term it is recommended that the Network Data Inventory (NDI) be migrated to the DEN schema. However, till such time as a schema covering all the network objects is available, the NDI may follow the most appropriate schema suitable for the definition of the object. These standards include X.805[itu95n], ETSI GOM[ets96], BME[nmf95], and SIF[sif97].

Examples of network data suitable for implementation in a directory environment include:

•User profiles, preferences, rules, policies
•Service configurations, rules, policies
•Product configurations, rules
•Network configurations, topology and rules
•Examples of network data suitable for implementation in data bases optimised for updates include:
•Network alarms, problems, usage, performance
•Service usage, performance, SLAs

A note of caution, directories are optimised for fairly static data (frequent reads and infrequent writes) and ubiquitous access. Not all of the NDI data is suitable for implementation within a directory (e.g. network performance - which has frequent writes and infrequent reads and requires very limited replication). As such, NDI needs to be flexible in terms of implementation. Further, the interface to the NDI must include other open standards such as SQL, ODBC and JDBC.

7. SML - NML Interface

The SML-NML interface is the single logical point where the customer facing systems interact with the network. As

such the SML-NML interface needs to be simple, straight forward, open and standards based. The SML - NML interface processes are described in some detail in the TMF Operations Map. The process groupings identified in the TMF are ideal for a high level understanding as well as providing a starting point for deriving a lower level definition of the interface. From an implementation viewpoint the interface exposed by the NML to the SML therefore needs to be expressed in CORBA IDL.

A representative list of functions exposed by the NML is given below.

Service Configuration:

•**config_service:** Provision and configure a service within the NML. Configuration of a service is different from the actual activation of the service.

•**activate_service:** Activate a service which has been configured previously.

•**Service Problem Resolution:**

•**diagnose_service:** Test the service and identify the location of the problem affecting the service. Also return the alarm history associated with the service

•**clear_alarm:** Clear an alarm associated with a service or a network element

•**Service Quality Management:**

•**get_service_SLA:** Return the SLA associated with a service

•A number of objects are passed at the SML-NML interface. There is a requirement to ensure that the object classes conform to a common model and schema. However, at this stage this may not always be possible, for example a definition of the Service or IP-VPN class is currently not available. A number of enhancements are therefore called for, mainly in the nature of definition of classes relating specifically to IP-VPNs. The IP-VPN abstract class (from which specific IP-VPN classes may be specialised) is described below:

•***IP-VPN Object inherits from Service***

•**Attributes:**

type, class, routing_rules, terminations, QoS, SLA, services.

Functions:

current_terminations, add termination, delete termination

8. TINA SA and IP VPN Session Realisation

Service Architecture as defined in TINA is ideally suited to the realisation of access IP-VPNs including aspects related to authentication, authorisation, service selection, resources allocation, and enforcement of rules and policies. TINA-SA is therefore chosen as the template for the architecture relating to IP-VPN session realisation and session usage.

Dedicated IP_VPNs by their very nature provide a dedicated environment where access and service selection are pre-assigned.

Access IP-VPNs follow the service paradigm

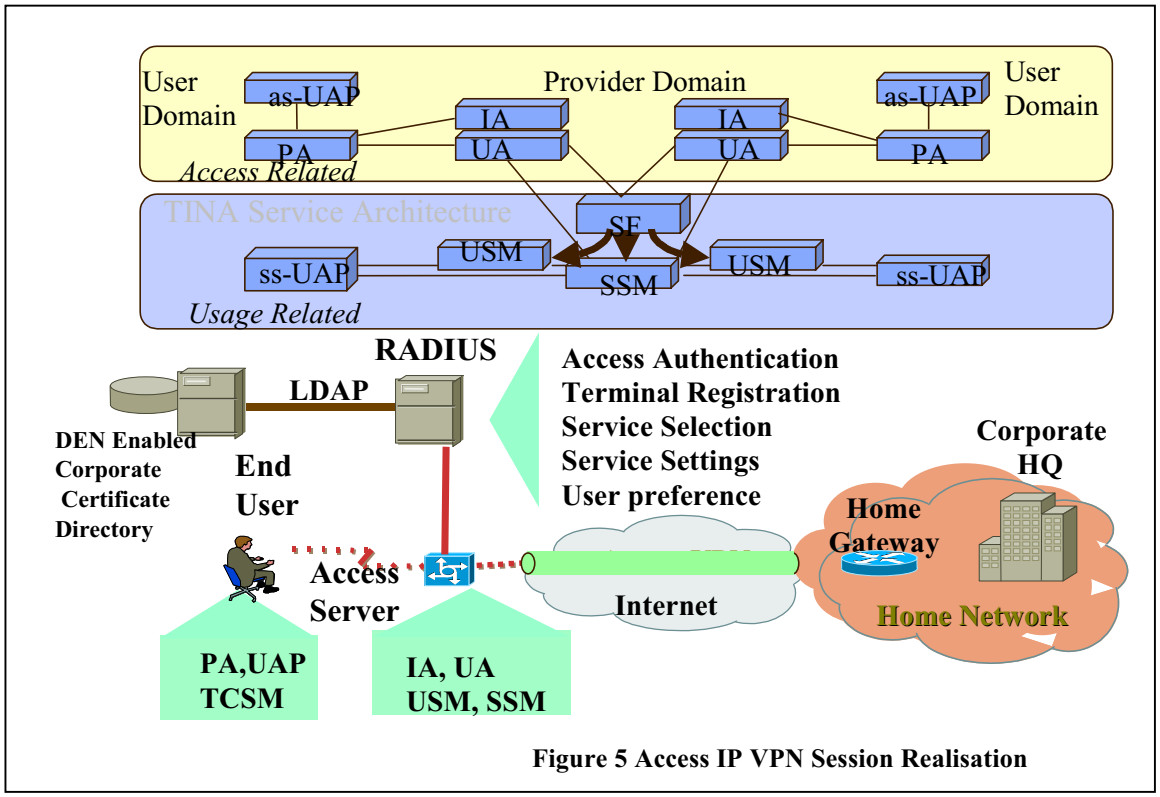

Figure 5 Access IP VPN Session Realisation

described in TINA Service Architecture. Taking the case of an ADSL or dial access IP-VPN, the implementation of the various TINA components is shown in the figure5.

From the above figure, the placement of the components of the TINA Service Architecture in what would be considered network elements may at first seem a bit odd,

but on a closer look, the functionality of the Access Server closely matches the functionality recommended by the TINA-SA. The Access Server provides the functionality to:

•provide terminal and end user authentication,

9. TINA NRA and IP VPN Configuration Management

IP-VPNs require connectivity and configuration across multiple technology domains as well as configuration of

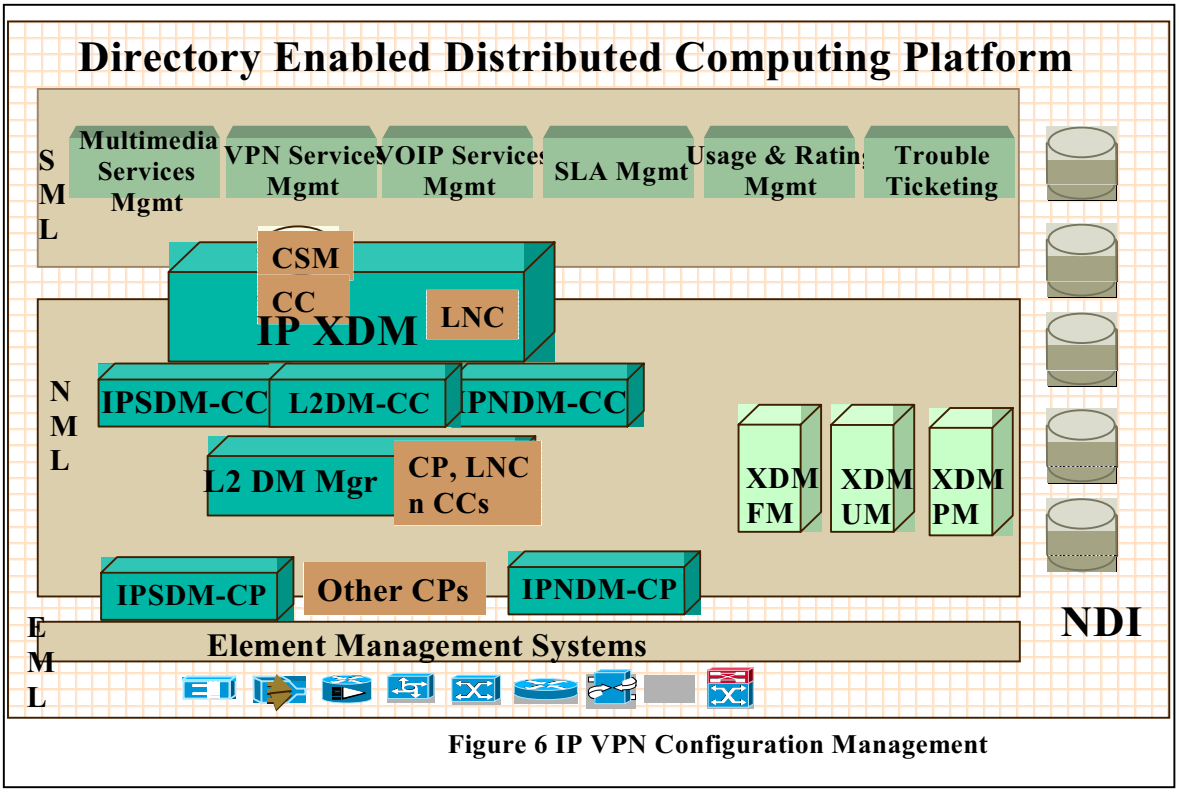

Figure 6 IP VPN Configuration Management

•service selection and validation, and

•session usage and coordination.

•The RADIUS server [cri95] works in close co-operation with the Access Server and provides services to the Access Server for Authentication, Authorisation and Accounting (AAA). It is also proposed that the users profile including such details as default service, preferences, and service settings also be stored in the RADIUS server.

•The RADIUS server could act as a proxy RADIUS and pass on the requests to the AAA RADIUS server in the home network from which the actual services are selected.

•A more recent development involves the usage of digital certificates for access permissions. The figure shows a scenario adapted from DEN policy management [sju99, mso98] . The figure shows the Access Server fulfilling the role of the Policy Enforcer, the RADIUS fulfilling the role of the Policy Server and the Certificate Database fulfilling the role of the Information Store.

multiple systems (e.g.. RADIUS, DHCP, Webhosting). The TINA Network Resources Architecture's Connection Management Architecture (CMA) provides an architecture for the realisation of connectivity across transport networks. This concept has been extended in this paper to provide configuration management across the IP domain. The Connection Coordinator and the Connection Provider are substituted by the Configuration Coordinator and the Configuration Provider i.e.. equivalent components in the IP domain. The figure 6 shows the placement of various TINA Network Resources Architecture (NRA) components within the IP management framework.

IP XDM: The IP Cross Domain Manager implements the Layer Network Coordinator (LNC) for the IP layer for the provisioning of IP-VPNs, the Connection Services Manager (CSM) for interfacing to the SML, the Configuration Coordinators (CCs) for the IP Server Domain and the IP Network Domain and Connection Coordinator (CC) for the Layer 2 Domain. As mentioned earlier, the XDM implements a workflow engine for handling of the requests received from the SML layer and fulfils each request via interactions with the various Configuration Coordinators and Connection Coordinators.

L2 DM: The L2 DM is in effect a Cross Domain Manager for the entire Layer 2 fabric which may comprise an ATM

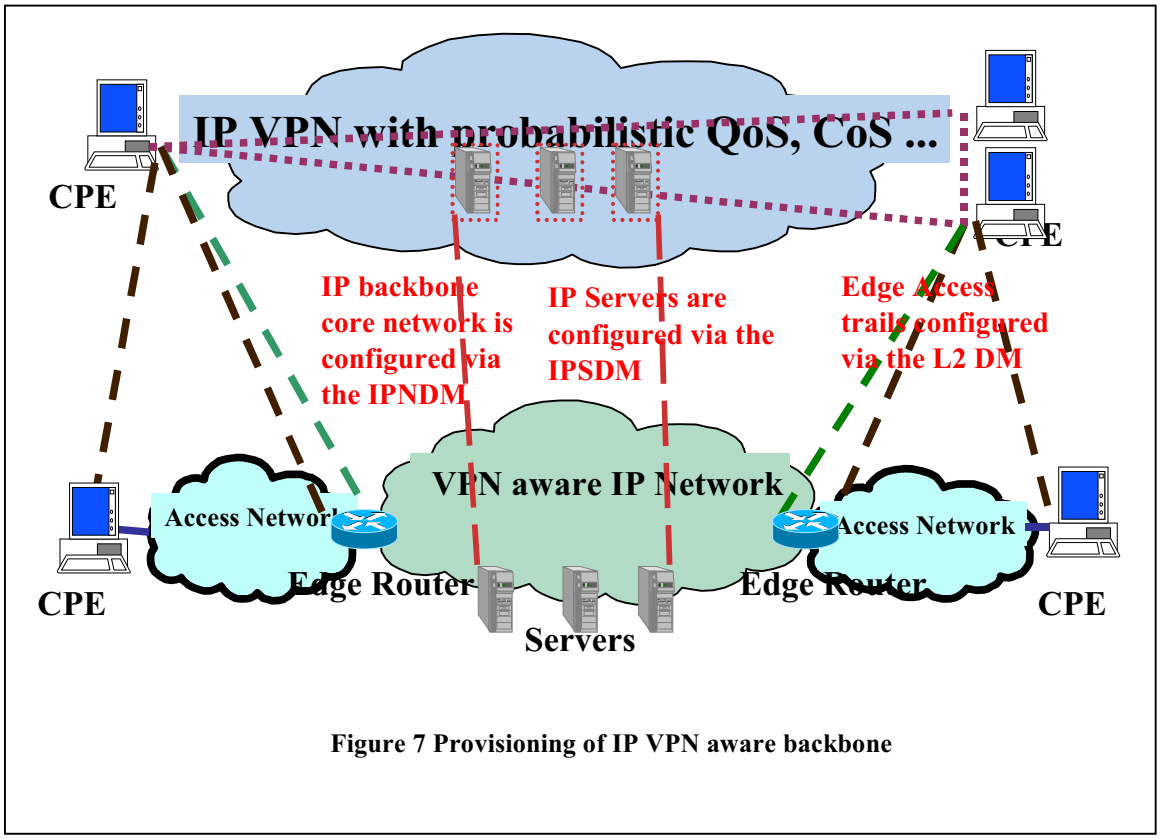

Figure 7 Provisioning of IP VPN aware backbone

backbone and a diverse set of access technologies including leased lines, FR, or ADSL. The L2 DM comprises the Connection Provider (CP) for layer 2 (which functions as the Communications Services Manager and may in its own right receive requests directly from the SML), the L2 Network Coordinator, the Connection Coordinators for the ATM DM and the other L2 networks. Like the IP XDM, L2 DM incorporates a workflow engine for the handling of requests received from the IP XDM or the SML.

IP Network DM: The IP Network Domain Manager handles the provisioning across the IP domain. It comprises the Configuration Provider for the IP Network Domain as well as zero or more Configuration Coordinators for specific router domains.

IP Server DM: The IP Server Domain Manager handles the provisioning across Servers in the IP domain. It comprises the Configuration Provider for the IP Server Domain as well as the Configuration Coordinators for specific servers such as Mail, DNS, RADIUS, H.323 GateKeeper.

10. Service Provisioning

The figure 7 illustrates the realisation of an IP-VPN service on a VPN aware IP network.

When the request is received at the CSM, the workflow process designated to handle the specific service event will be initiated. In essence, the LNC functionality is implemented via intelligent agent based adaptable process workflows. Based on the input parameters passed from the SML (eg.type of QoS, bandwidth commitments at end points, inter endpoint bandwidth commitments, topology, routing constraints, etc), the IP XDM, may decide on the infrastructure and the domains which are required to implement the IP-VPN service.

This specific example illustrates the implementation of an IP-VPN using a VPN aware IP network:

•The IP XDM LNC coordinates the interactions with the IP Server DM CC (to configure the servers via the IP Server DM CP). Services could include DNS, Mail Server, Web Hosting facilities for the IP-VPN. In an infrastructure supporting IP-VPNs, a single set of servers would need to have the capability to support multiple virtual instances of a specific service. In other words servers in a VPN aware network will need to be VPN aware.

• The IP XDM LNC coordinates the interactions with the IP Network DM CC to configure the edge routers via the IP Network DM CP. Configuration includes configuring the VPN termination (IP addresses, protocols, routing information, etc.), QoS characteristics (committed rates, excess rates, probabilistic percentage), enabling charging & billing instrumentation, enabling performance collection instrumentation.

• The IP XDM LNC coordinates the interactions with the IP Network DM CC to configure the Customer Premises Equipment (CPE).

•The IP XDM LNC coordinates via the L2 DM CC which interacts with the Layer 2 DM CP to request layer 2 services required (eg. the access paths between the CPE and the edge router). The layer 2 services provisioned need to be compatible with the QoS commitments requested at the specific IP-VPN endpoints.
•The IP XDM LNC coordinates the storage of service and configuration information into the relevant Network Data Inventories.

11. Fault Management

There is a distinct need for event and alarms to be service centric and to reflect an end to end view of the service. In the case of IP-VPNs, the correlation of events and alarms to services presents additional challenges for the following reason:

Network Element support for the implementation of service related alarms and event traps is either limited or non existent.

Not all services map seamlessly or otherwise to lower level entities. For example while PVC based IP-VPNs contain direct mappings, other IP-VPNs (using *best effort*) cannot be effectively correlated.

Network Element Support

There is a mandatory requirement for the next generation of network elements to encapsulate objects which are service centric. For example, the next generation of elements within an VPN aware network will need to include the VPN Id within the events generated and policy enforcers within the elements will need to include service details for events and alarms generated by them.

In the absence of network elements with in built instrumentation or service concepts, event correlation at the NML (or the EML) cannot by itself deliver a full correlation between the raw alarms raised and the service which they affect. Besides, any such correlation is bound to be constrained by scalability issues in looking up NDI configuration databases for the low level configuration of each node.

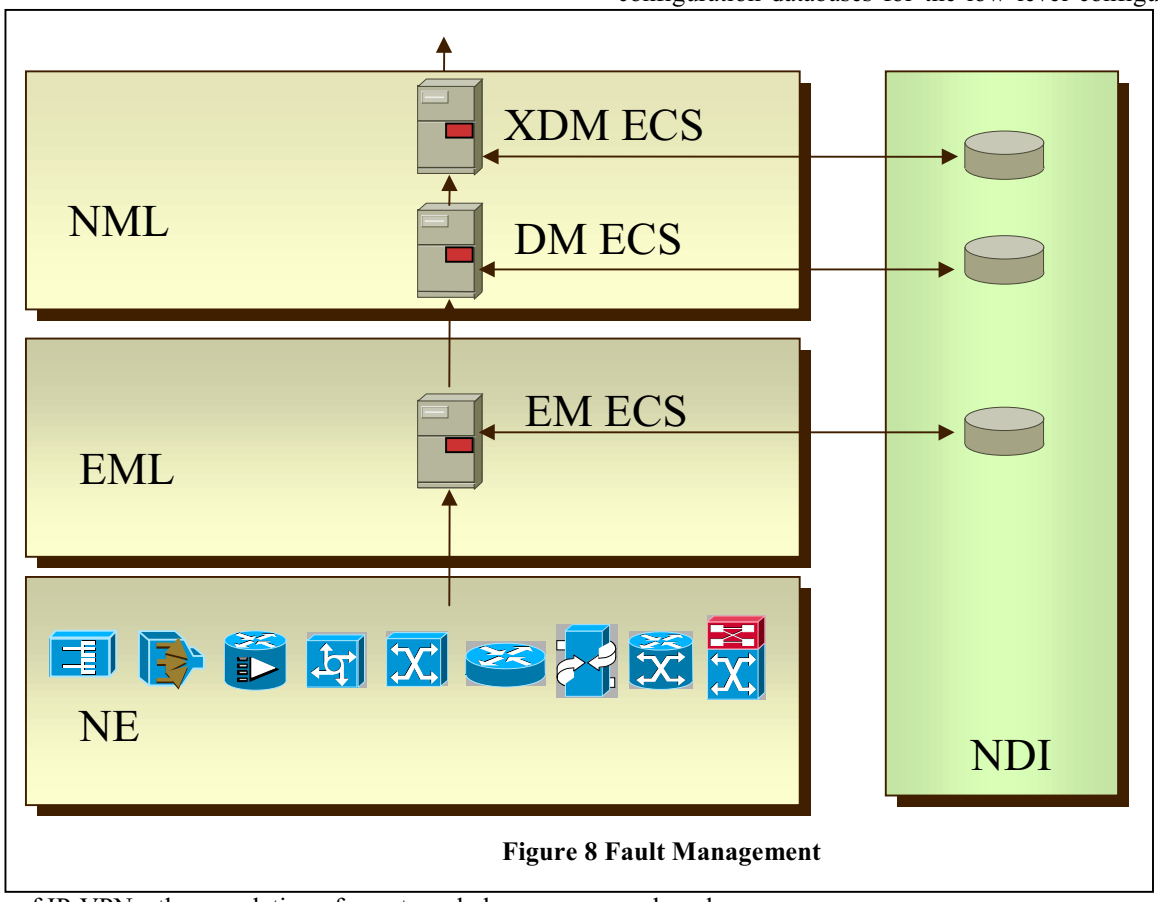

Figure 8 Fault Management

Event Correlation Engine

The proposed architecture includes an event correlation engine at each management layer as per figure 8 to correlate events in the immediately preceding lower layer. The correlation engine correlates alarms with reference to NDI (network topology, network configuration, and network rules) at each of these layers to filter out unwanted and superfluous events from reaching higher levels and to map physical events to services in a progressive manner.

The mechanism proposed in this paper includes the usage of rule based correlation engines, where the administrators will be able to maintain the rules in the NDI and capture

accurately the business requirements for the analysis and forwarding of alarms.

12. Performance Management

In generic terms, a Service Level Agreement (SLA) is a contract between a service provider and a customer that guarantees specific levels of performance and reliability at a certain cost.

SLAs in the past have mainly been related to metrics such as system availability, mean time to failure, mean time to repair, etc.. However, customers today expect metrics of a entirely different nature. These new metrics include attributes such as QoS violations, packet delay and loss, response times, throughput, etc. In the IP-VPN context, SLA metrics include:

•performance of bandwidth committed at each endpoint (CIR, CAR, EBR, etc.),

•packet delay and packet loss in the IP-VPN, and

•Service Level Objectives (SLOs) of IP-VPN services subscribed to e.g. DNS, SMTP, Webhosting, etc.

•In the majority of cases metrics may relate to characteristics which are common across the whole network and applicable to all or most services. Rather than enabling measurements at each CPE and edge router for each and every service, an alternative approach is to measure the common metrics on a network wide basis and to apply these to all customer SLAs. This effectively reduces the workload and aids scalability.

•Active Measurement Systems simulate a typical user within the network and periodically evaluate the various attributes based on simulated scenarios. As such the metrics evaluated by active measurements are typical of what a customer might experience but not what the customer actually experiences. Consequently, the utility of these metrics is limited to service quality assessment. Examples of such metrics for IP-VPNs include network packet loss, network packet delay, server SLOs (DNS, Webhosting, SMTP, News, etc.).

•The main reason for using active measurements is to overcome the lack of inbuilt instrumentation in various CPEs and network elements. Also active measurements may be done externally, thereby removing the need for configuring each and every service or element or CPE.

•Passive measurements utilise the instrumentation built into the network elements. Since they do not require the explicit simulation of traffic, these measurements have a minimal impact on the network. Also as they are obtained from elements which track real traffic, they are more accurate in reflecting the QoS perceived by the customers. Figure 9 shows examples of passive metrics for IP-VPNs such as access bandwidth performance, packet delay and loss, QoS, CoS compliance and call setup delay, call drop rate, etc.

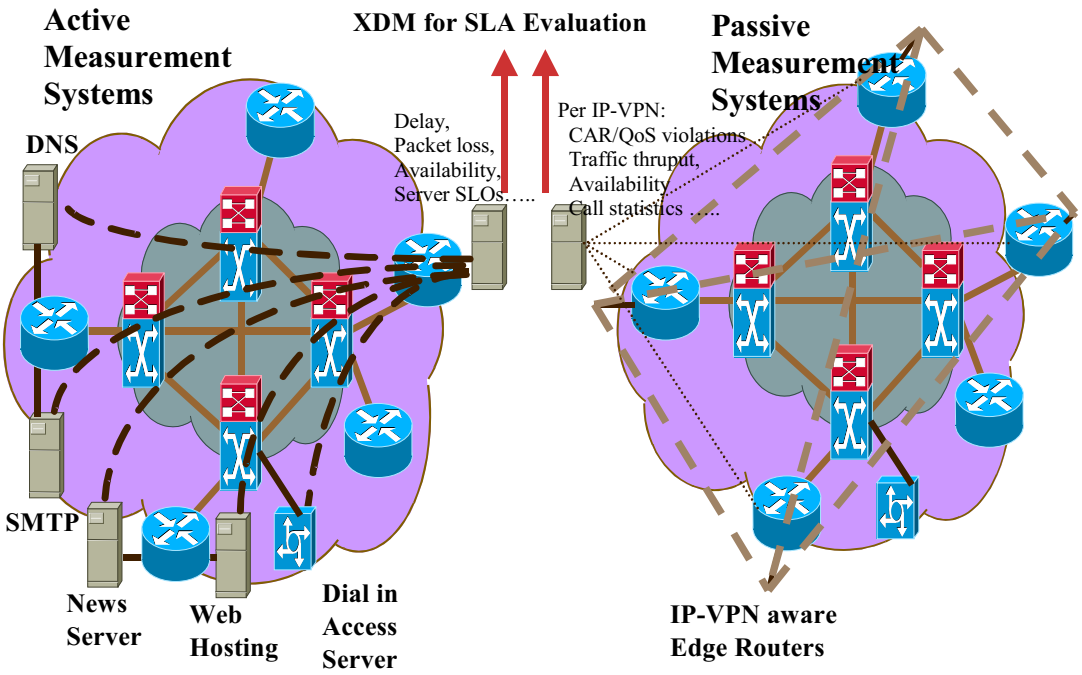

Figure 9 Performance Management

13. Conclusions and future work

This paper assesses the issues and requirements related to the management of IP-VPNs, explores the various

standards and their applicability to the realisation of IP-VPN management systems. The use of TMN as the architectural framework provides a solid ground for development of IP-VPN Management system. At the SML-NML interface, concept of a Cross Domain Manager is introduce with the aim of simplifying and consolidating the interface. CORBA-IDL is recommended for SML-NML interface for use by service planning, service configuration, service problem resolution etc. The TMF Business Process Model is recommended to be used to meet the ever changing business requirements of emerging new services as well as to deal with the complexity of these services. Workflow modelling is recommended as an alternative to the Business Object Model to tie the business objects together via a workflow engine.

Extension of Network Data Inventory defined by TMF Model is recommended in order to include inventories required for IP-VPN policy based access and resource management. It is also recommended that NDI be migrated to Directory Enabled Network (DEN) schema. Suitability of TINA - Service Architecture is described for session realisation and session usage. Also TINA - Network Resource Architecture's Configuration Management Architecture is used for connectivity across transport network. Further, scenarios for fault management, performance management and SLA reporting are also described.
This paper has attempted to bring together components of various standards and framework to crate an architecture for management of IP-VPNs. Future work will develop a proof of concept implementation of the proposed architecture.

Acknowledgments

This paper is based on the work done in the thesis on the management of IP-VPNs [aso99] submitted to the School of Computing Sciences, University of Technology, Sydney.
The permission of the Executive Director, Customer Process & Information, Telstra Corporation Limited, to publish this paper is hereby acknowledged.

References

[aso99] Anil Sood, An Architectural Framework for the Management of IP-VPNs, thesis submitted for the part completion of Master of Science, School of Computing Science, University of Technology, Sydney, 1999.
[bjer97] L H Bjerring, et al, A Virtual Private Network Service for an Open Service Market, XVI World Telecommunications Congress ISS 1997.
[bjer98] L H Bjerring, et al, Experiences in Developing Multi-technology TMN Systems, NOMS, 98 Conference, New Orleans, 1998.
[cri95] C Rigney, et al, Remote Access Dial In User Service, draft-ietf-radius-v2-00, February 1995.
[Ets96] ETSI-DTR/NA43315 ,Managed Object Modelling Guidelines, Version 0.1E, July 1996.
[ferg98] P. Ferguson and G. Huston, What is a VPN?, White Paper, Cisco, April 1998
[hein98] J. Heinman, E. Rosen, VPN Support for MPLS, draft-heinanen-mpls-vpn-01.txt, March 1998
[hpc99] Hewlett Packard, ChangeEngine Executive Overview, http://www.ice.hp.com, 1999.
[itu95n] ITU-T G.805, Generic Functional Architecture of Transport Networks, November 1995.
[itu95j] ITU-T-M.3100, Generic Network Management Information Model, July 1995.
[kent98] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, draft-ietf-ipsec-arch-sec-04.txt, March 1998
[lewi96] D. Lewis, et al, An inter-domain virtual private network management service, IEEE Network Operations and Management Symposium, pp 115 - 123, vol.1, April 1996
[mso98] Microsoft, Active Directory Technical Summary - White Paper, http://www.microsoft.com/ntserver, 1998.
[neil98o] R. Neilson, CA*net II Differentiated Services Bandwidth Broker Specification, October, 1998
[nmf95] NMF 028, Bandwidth Management Ensemble, issue 1, October 1995.
[nmf98m] NMF-GB 908, Network Management Detailed Operations Map, Draft Issue 0.9, March 1998.
[nmf98o] NMF-GB 910, SMART TMN Telecom Operations Map, Evaluation Version, release 1, Oct 1998.
[rfc2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, An Architecture for Differentiated Services, IETF RFC 2475, December, 1998
[sif97] SIF-014-1997, Information Model for Connection Management and Fault Management at the EMS/NMS interface, June 1997.
[sju99] Steve Judd, John Strassner, Directory Enabled Networks, Information Model and Base Schema, Draft Version 3.0c1, 1999.
[tina97f] TINA-C, Network Resource Architecture, Version 3.0, February 1997.
[tina97n] TINA-C, Network Resource Information Model Specification, Version 2.2, November 1997.
[tina97j] TINA-C Service Architecture , Version 5.0, June 1997.
[wru99] Wayne Rudland, Adacel Corp, Agentis Product Description, Adacel Corp, http://www.agentis.com.au/solution.htm, 1999

Sanjay Jha is a senior lecturer at the School of Computer Science and Engineering at the University of New South Wales, Sydney. He has Ph.D. degree in Computer Science from the University of Technology (UTS). Prior to this he was a lecturer at UTS. He was also a visiting scholar at the Transmission Systems Development Department, Fujitsu Australia Limited, Sydney in 1998 and Distributed Computer and Communications Laboratory at Columbia University in 1995. His research interests include Quality of Service Management, Network Management, Communications Protocols and Multimedia communications over the Internet.

Anil Sood is a Senior Architect, Network Systems Architecture, Customer Solutions, NTG, with Telstra, Australia. He has M.Sc (Computing) degree from the University of Technology (UTS), Sydney.