This PDF file contains a chapter of:

INTEGRATED COMMUNICATIONS MANAGEMENT OF BROADBAND NETWORKS

Crete University Press, Heraklio, Greece
ISBN 960 524 006 8

Edited by David Griffin

First published in 1996 by
CRETE UNIVERSITY PRESS
Foundation for Research and Technology
P.O. Box 1527, Heraklio, Crete, Greece 711 10
Tel: +30 81 394235, Fax: +30 81 394236
email: pek@iesl.forth.gr

The ICM consortium consists of the following companies:

Alcatel ISR, France
Alpha SAI, Greece
Ascom Monetel, France
Ascom Tech, Switzerland
Centro de Estudos de Telecommunicações, Portugal
Cray Communications Ltd., United Kingdom (Prime contractor)
Danish Electronics, Light & Acoustics, Denmark
De Nouvelles Architectures pour les Communications, France
Foundation for Research and Technology - Hellas, Institute of Computer Science, Greece
GN Nettest AS, Denmark
National Technical University of Athens, Greece
Nokia Corporation, Finland
Queen Mary and Westfield College, United Kingdom
Unipro Ltd., United Kingdom
University College London, United Kingdom
University of Durham, United Kingdom
VTT - Technical Research Centre of Finland

Chapter 6

VPN management

Editors: James Reilly, Richard Lewis
Authors: James Reilly, Konstantina Mourelatou, Panos Georgatsos,
David Griffin, George Mykoniatis, Valia Demestiha,
Petri Niska, George Pavlou, Peter Baxendale

This chapter presents an overview of the management and use of two generations of ATM Virtual Private Networks - intermediate and target VPN. The required Management Services are analysed, specified and mapped onto the TMN [6.1] architecture. The architectural components and their operational dependencies and information exchanges are described.

6.1 Introduction

The competitiveness of modern national and multi-national corporations is increasingly affected by how well they utilise telecommunications services. A service being increasingly demanded is called Virtual Private Network (VPN). VPNs allow the corporate customer to create *logical* private networks using public network resources. In the future, as the use of more advanced applications and services grows, there will be a need to extend VPN services to integrate many different types of corporate telecommunications traffic including voice, data, video and multi-media. ATM provides a suitable VPN infrastructure offering the high bandwidth and flexibility required by different types of services. ATM technology is becoming an increasingly important part of the

Wide Area Network (WAN) infrastructure and will be used by public network operators to offer advanced telecommunications services such as future VPN services. The provisioning of VPN services will require the deployment of advanced Management Services.

This chapter presents an overview of the management of two distinct types of ATM VPN service. The first service, called *intermediate-VPN* (iVPN) provides a generic service for provisioning of ATM leased-line VPCs in a multinational, multi-operator environment. Management Services for iVPN were specified, designed, implemented and tested by ICM on simulated and real ATM networks during 1995. The second service, called *target-VPN* (tVPN), concentrates on using the full statistical multiplexing power of ATM technology required for future ATM VPNs. This terminology is in keeping with previous RACE work in this area [6.5][6.6][6.7].

6.2 An overview of VPN services

6.2.1 Background information

A good overview of the requirements for efficient and flexible provisioning and usage of ATM VPNs (AVPNs) is presented in [6.8][6.9][6.10]. Recent ETSI work on the requirements for Broadband VPNs can be found in [6.11].

The ATM Forum is also an important driving force in many related areas such as ATM signalling [6.12], LAN emulation [6.13], and multi-carrier, multi-domain provision and management of ATM services [6.14][6.15][6.16][6.17]. Particularly relevant is the ATM Forum's management model. This is compared to ICM's work on the management of VPNs later in this chapter.

The Internet IETF has specified a rudimentary Management Information Base (MIB) for the management of ATM nodes [6.18].

A closely related area of interest is the provisioning and usage of VLANs. These are simple extensions of the traditional LAN model, that allow for the use of resources from a public network operator. Some vendors are seeking the use of the IEEE 802.10, for a VLAN identification mechanism that allows frames to be "tagged" for delivery to certain VLAN subnetworks [6.4]. This would allow for creation of VLANs based on protocol subtypes and subnetwork addresses. Larger issues, such as uniform management of multi-vendor equipment implementing this (or other proposed) VLAN standards, have not been addressed yet.

6.2.2 The market

Asynchronous Transfer Mode (ATM) technology combines the advantages of both packet switched data networks (flexible bandwidth) and circuit-switched, channel-oriented synchronous networks (high bandwidth and low delay that remain constant). ATM technology is an important base for all future Broadband ISDN (B-ISDN) networks and services. ATM aims to unify (or integrate) the many currently separate types of networks (telephony, CATV, data, audio, video) that exist today. As it is basically a packet-oriented technology, current commercial ATM offerings mostly support data

services (such as LAN-LAN or LAN-WAN interconnection, LAN backbones), but ATM is also intended as a base for modernising and integrating networks used for more profitable revenue generating services.

ATM can also flexibly handle different Quality of Service (QoS) types, and its statistical multiplexing features allow better use of network resources, while providing additional features such as bandwidth on demand. All of these facets make ATM an ideal infrastructure for future advanced services.

On the demand side, customer organisations would like full integration of all of their traffic needs, with the flexibility to adapt to changes in these needs. Figure 6.1 shows an example.

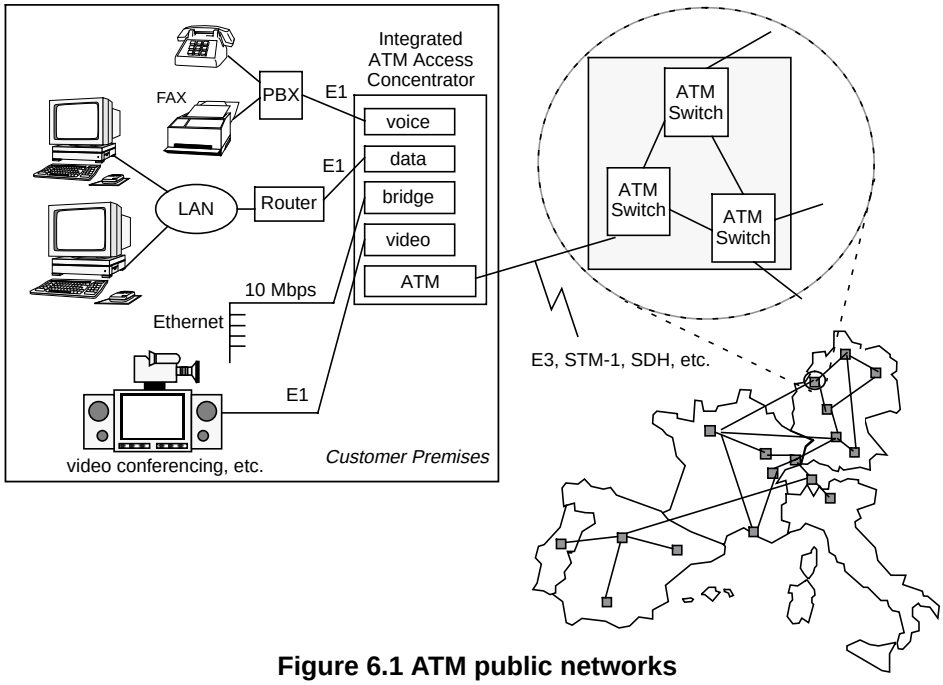


Figure 6.1 ATM public networks

In current telephony based VPN offerings, an organisation's CPN could be a large corporation's local PBX network. The most basic goal of a VPN service in this case is to lower the price of telephone calls within the company, when compared to using the public network.

This is accomplished by use of two more basic VPN services called: *private numbering plan* (PNP) and *closed user group* (CUG). A PNP provides groups of users within a customer organisation with the capability of placing calls within the organisation, by using a digit sequence having different structures and meanings than those provided in the public numbering plan. Within a CUG the named users can only call other members of the same CUG. Incoming calls from outside the CUG can be prohibited. Only authorised users with appropriate access rights can modify the contents of the CUG. A simplistic view of a CUG is that it allows creation of "sub-VPNs" within an

organisation's overall potential VPN. Use of CUGs allow an organisation to create, delete or modify subgroups of users within a PNP.

Most current commercial VPN offerings, such as Concert, Phoenix, Uniworld, and WorldPartners, target telephony/voice-based markets [6.2]. In addition, standardised data-based virtual LAN (VLAN) services are also on the horizon [6.3][6.4]. In the future, it seems certain that integrated VPN services will carry a rich mix of traffic: voice, data, video, audio and multimedia.

Regarding the basic technology, several integrated ATM access concentrators/multiplexers are already on the market, and many service providers are already planning next generation VPN services over an ATM based WAN infrastructure [6.23][6.24]. In Europe, liberalisation of the telecommunications market should increase competition in this area, the most important remaining problems are more political than technical [6.25].

6.2.3 VPN concepts and terminology

There is no single commonly agreed definition of a VPN. For our purposes, a VPN is defined as:

> *"a set of logical closed user groups implemented over public switched network that provides a number of special features which enhance service. This means that to a VPN customer the VPN appears as a physical private network"*
>
> *RACE Common Functional Specification D721*

A VPN bearer service is shown in Figure 6.2. In this example, a public network operator is providing two separate VPNs for two separate customers. Each customer's VPN uses resources from the public network to interconnect individual customer premises networks (CPNs). Each customer can only use, monitor and modify its own VPN.

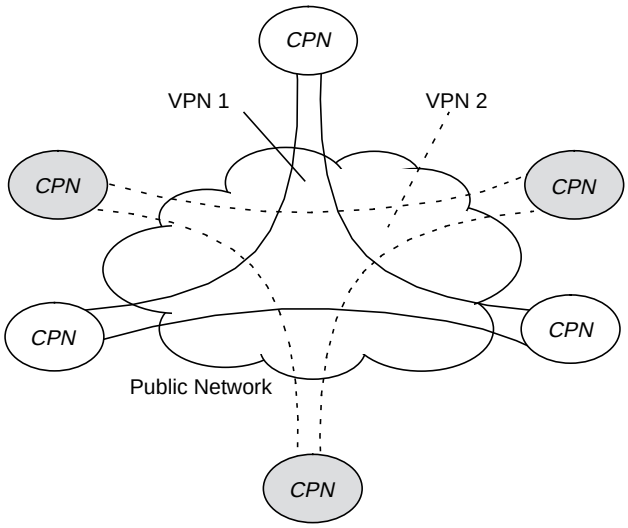


Figure 6.2 The VPN bearer service

Within a VPN, the CPNs appear to be connected together by purchasing additional private network resources. For the customer, VPN brings lower costs for network installation, operation, maintenance, capital equipment and staff; with the benefit of increased flexibility and additional features. The public network operator reaps economies of scale by selling similar VPN services to a variety of customers.

A simple VPN example is illustrated in Figure 6.3. In this case, a large multinational company connects all its regional office PBX-based telephone networks using a VPN service. One benefit of this is the establishment of a uniform numbering plan for all telephone extensions used in the company. Another is that when employees call

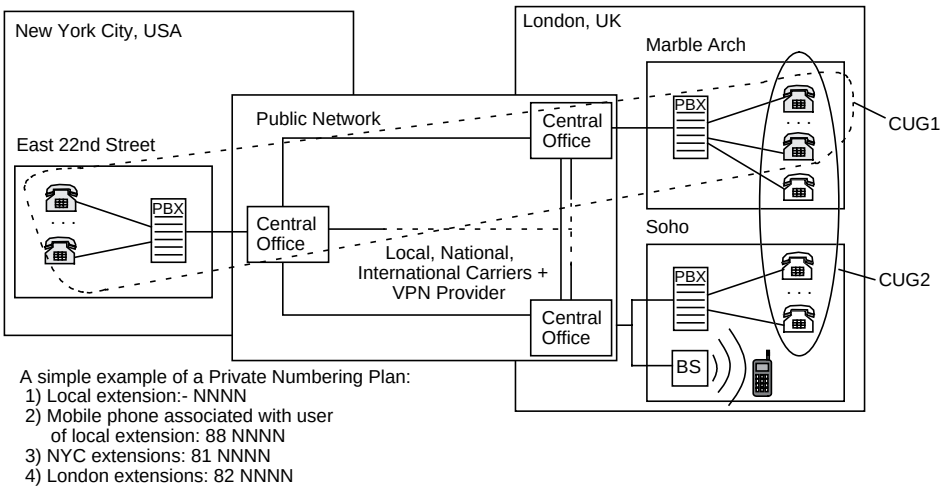


Figure 6.3 Traditional VPNs: use of PNP and CUG

their counterparts in other international offices of the company using the PNP, the calls are less expensive compared to similar calls placed through the international Public Switched Telecommunications Network (PSTN). A subscriber may belong to one or more CUGs.

Figure 6.4 illustrates the conceptual similarities and differences involved. The public network uses a public numbering plan and pricing scheme. VPNs are built using separate PNPs and CUGs.

6.2.4 VPN terminology from the RACE programme

The ICM project based its definition on previous work done in the RACE community [6.6][6.7]. The work defined three phases of VPN evolution:

- The *short-term VPN* (sVPN) phase is concerned with the current status of installed VPNs, and planning for future phases (iVPN, tVPN). Most VPN services available today are based on the conventional public switched telephone network (PSTN), or on the public switched packet data networks (PSDN).

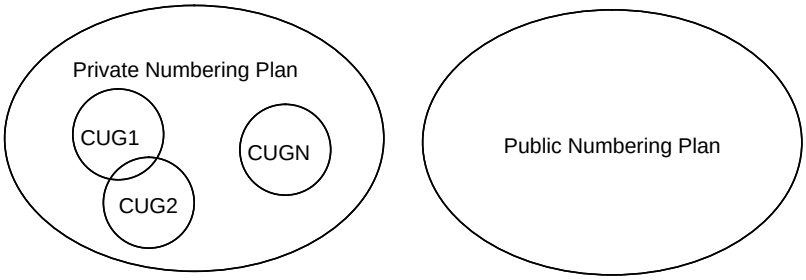


Figure 6.4 Public vs. private numbering plans, and CUGs

- The *intermediate VPN* (iVPN) phase maps the evolution of VPN management from the current s-VPN situation to the target integrated Broadband communications (IBC) environment. It is based on restrictions of ATM technology available in the current to near term.
- The *target VPN* (tVPN) phase is the ultimate goal for future VPN services in an IBC environment, which maximise the utilisation of underlying network resources, with reduced cost and increased flexibility.

sVPN and iVPN are implemented by interconnection of Customer Premises Networks (CPNs) over leased-lines, where the leased-lines are either dedicated or are provided by means of cross-connect equipment in the public domain. In the case of ATM networks, this leads to inefficient use of the underlying network resources, since the iVPN network resources are dedicated to individual leased-lines that may be under-utilised by their customers.

tVPN services should provide AVPNs at a reduced cost, with increased efficiency and flexibility to public network operators (PNOs), through increased multiplexing of traffic.

6.2.5 VPN actors, relationships and roles

Previous RACE work in the area of VPN services has also established the concept of a *Value Added Service Provider* (VASP). A VASP is an organisation that provides and sells added-value services such as VPN on top of the basic network providers' bearer services. The VASP can itself be a PNO, a consortium of PNOs, or a completely independent organisation. It provides "*one-stop-shopping*" for the planning, installation and maintenance of a VPN. The VASP rents network resources and connectivity from a suitable set of PNOs, and provides value added services by making use of these resources. In addition, the VASP provides uniform network Management Services such as accounting, billing, configuration and status monitoring to its customers.

A contractual relationship exists between the VASP and a customer organisation. The contract requires the VASP to provide the desired VPN service between specified customer end-points (e.g. CPNs) that are geographically distributed. The contract includes, but is not limited to, issues such as the location and types of sites to be interconnected, and the customer performance requirements (e.g. Bandwidth and Quality of Service parameters).

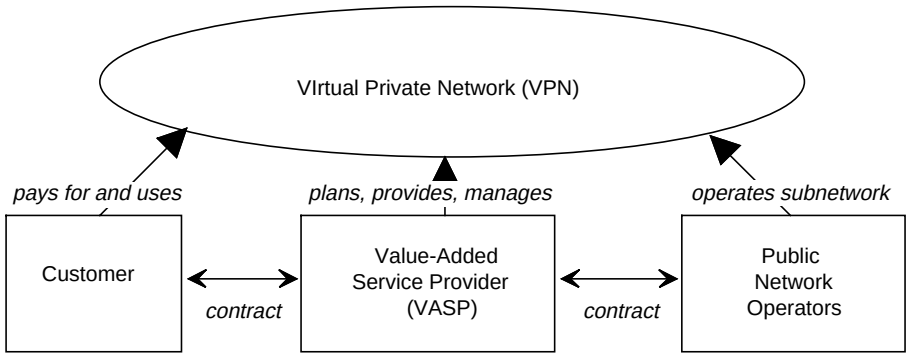


Figure 6.5 Actors and their relationships to VPN

The VASP will provide different VPNs to different customers, over the same set of public network resources available from a common set of many different possible PNOs. Figure 6.6 illustrates this.

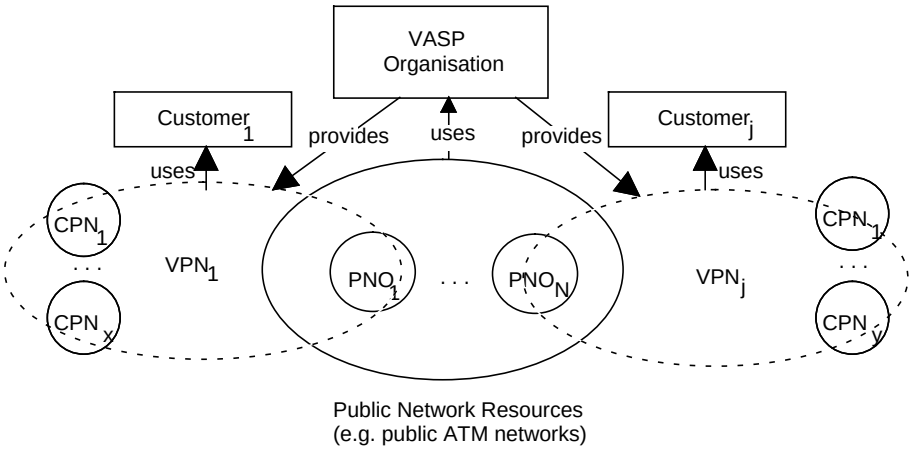
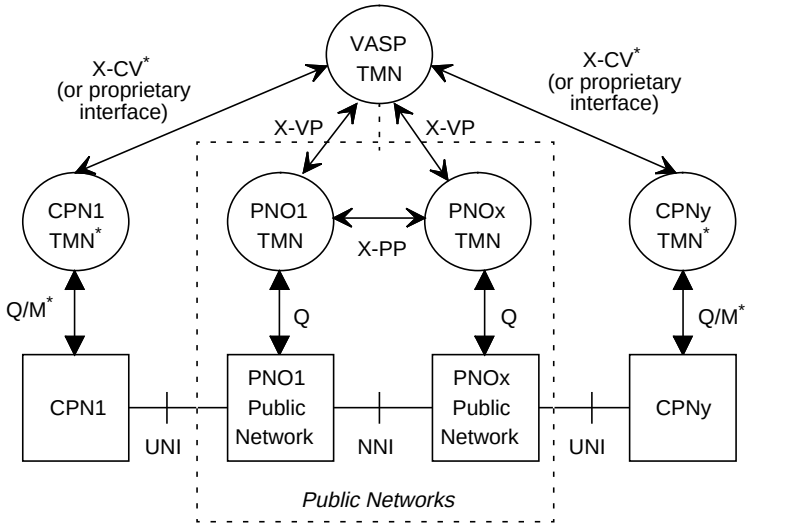


Figure 6.6 The VASP and multiple customers' VPNs

6.2.6 VPN management domains

The various actors involved in the provision, operation, maintenance and use of the VPN give rise to different VPN management domains. Figure 6.7 illustrates the management domains involved, their relation to physical public and private networks, and various interfaces involved (both network and management related). A one-to-one mapping exists between the terms “TMN” and “management domain.” Interfaces between different TMN domains require use of the secure TMN X-interface. Interfaces to the real networks can use the TMN Q_3/Q_x or M interfaces. Appropriate mediation devices or Q-adapters (QAFs) are needed in the latter case.



X-CV*: X interface between a customer TMN and a VASP TMN.
X-PP: X interface between two PNO TMNs.
X-VP: X interface between a VASP TMN and a PNO TMN.

* The CPN management system may be proprietary.
It does not have to be TMN compliant.

Figure 6.7 Management domains and interfaces for VPN services

6.3 The iVPN Management Service for provisioning ATM leased-lines

6.3.1 Introduction

Provision of multi-domain, multi-operator services is complex. In TMN based Management Services, use of the security features of the TMN X-interface is required. The iVPN Management Service presented here was implemented using a prototype TMN X-interface [6.19], that conforms to appropriate TMN security requirements for such services [6.20][6.21].

Within the ICM case studies, some basic assumptions were made regarding the iVPN Management Services. It was assumed that End-to-End VPCs (EEVPCs) would be used to interconnect customer sites, and that these EEVPCs are created by management operations as opposed to user signalling procedures. Therefore only VP cross-connects would be used by the iVPN Management Service to create semi-permanent ATM leased-lines. It was further assumed, for simplicity in the ICM work, that the End-to-End VPCs (EEVPCs) would be of fixed bandwidth. Creation and signalling issues related to the use of VCCs on the created EEVPCs is assumed to be the customer's responsibility and will take place in the VC switches of the CPNs.

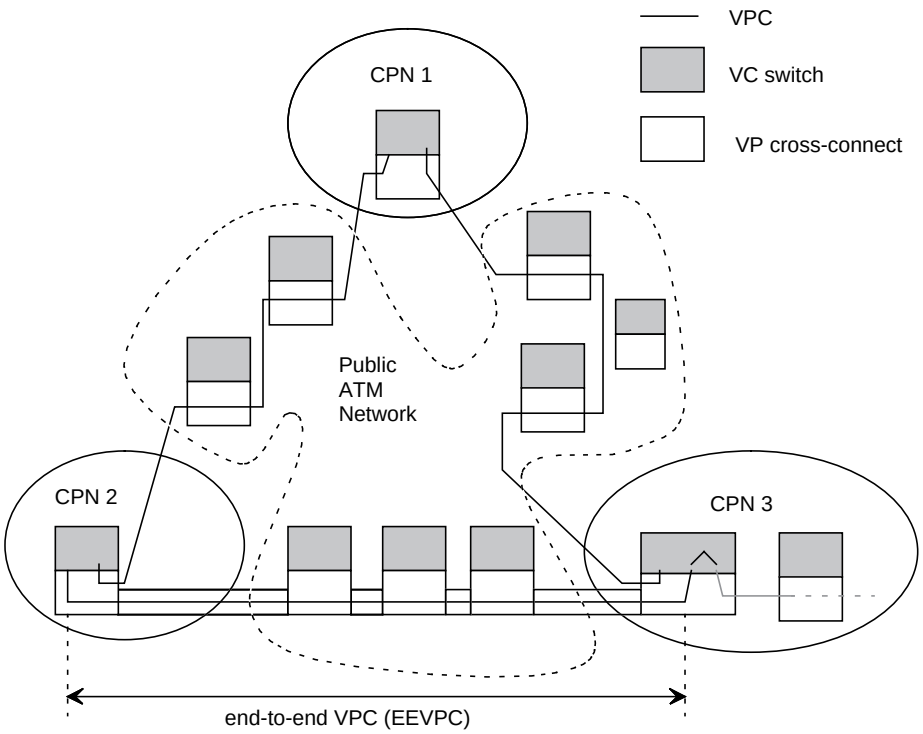


Figure 6.8 ATM leased-lines using end-to-end VPCs.

Figure 6.8 helps to illustrate the use of EEVPCs in a VPN Management Service. Only VP cross-connects and VC switches are shown. The VP links (VPL) used are only shown on the EEVPC between CPN2 and CPN3. The final ATM hosts, and terminal equipment are omitted for clarity. One needs to fully connect (mesh) the three CPNs below using EEVPCs to get a Virtual Private Network. The EEVPCs can be created/deleted using the iVPN Management Service described later. No VC switching takes place in any of the intermediate segments of the EEVPC. VC switching only takes place after the EEVPC has terminated (shown in CPN3). Although the figure only shows a single PNO, an EEVPC may span more than one PNO domain.

Because fixed bandwidth EEVPCs are used, when an EEVPC's capacity is fully utilised, no more VCCs can be switched onto it until enough capacity becomes freed (e.g. VCC deleted). Even if other VC/VP equipment and paths exist to the other CPN, they cannot be used for new VCs as the EEVPC is semi-permanent. Thus ATM network resources in the public network may be poorly utilised in some cases.

As discussed above, the iVPN is a Management Service provided by a VASP to automatically provision ATM leased-line end-to-end PVCs (EEVPCs) in an environment with multiple operators, customers and management domains. This conceptually simple service allowed the ICM project to study the issues arising from the provision of multi-domain TMN Management Services.

This section builds on ICM's previous work in the area of managing VPC bandwidth and load-balancing within a single operator's management domain (Chapter 5). The iVPN Management Service was designed, specified, implemented and tested on real and simulated Pan-European ATM networks. An important objective was a prototype TMN X-interface enabling inter-management domain security to be investigated.

In this section, the proposed Management Service is broken down according to established TMN design methodologies [6.26] into its constituent components which are described in some detail.

6.3.2 The iVPN case study

The iVPN case study, system design and architecture work [6.27][6.28][6.29][6.30] was a relatively straightforward addition to ICM's previous work on VPCM.

ICM's implementation of the iVPN service provided geographically distributed organisations with a leased-line service, used to interconnect a number of CPNs that are located at different geographic sites of an international organisation. The leased-line service is implemented on Broadband ATM networks, using EEVPCs. The leased-line service is used interconnect their CPNs and devices located at various sites to meet their organisation's business objectives. The EEVPCs are basically simple fixed-bandwidth VPC pipes. Another way of looking at EEVPCs, is that they are simply permanent virtual connections (PVCs) that can be automatically extended by the ATM Leased-line Management Service across multiple PNOs, even into the CPNs.

This type of leased-line service would normally be set up by a customer using a completely manual process, involving negotiations with the necessary PNOs and contractually arranging for the appropriate EEVPCs through each PNO-PNO and from PNO-CPN - for all the PNOs, CPNs and EEVPCs used. Configuration of VPIs used on the VPLs spanning management boundaries would be manually negotiated at each PNO-PNO and PNO-CPN boundary. The entire process is very labour-intensive, error-prone, time-consuming, difficult to change or modify (e.g. add new EEVPCs or delete existing ones) and varies from customer to customer. The objective of the ATM Leased-line Management Service is to completely automate this process, by providing a unified Management Service that spans all the relevant management domains. This is achieved through the VASP, which generates revenue by providing this generically useful service (and others) to many different corporate customers.

It is assumed that the VASP has available to it a set of ATM-based VP services that it buys or rents from suitable PNOs, based on its overall customer requirements. From the total set of potential EEVPCs available, it can then provide leased lines to various customers depending on their performance requirements (e.g. bandwidth, total end-to-end delay, maximum jitter, cost, operator preferences, etc.) and also the location of the CPN end-points to be interconnected. The VASP is not at all concerned with the type of traffic (multimedia, file transfer, etc.) that the customer puts onto the EEVPCs. The customer sets up individual calls (VCCs) on the EEVPCs in the signalling plane.

For the purposes of ICM, the main task of the iVPN Management Service therefore is to design and provision a set of EEVPCs that best meet the needs of individual customers. This is based on the customers' needs and on the available set of VP resources the VASP has available or can obtain. Figure 6.9 shows the relationship between the

iVPN Management Service with the PNOs, CPNs, human managers (TMN users), customer organisations, VASP, and other management functions.

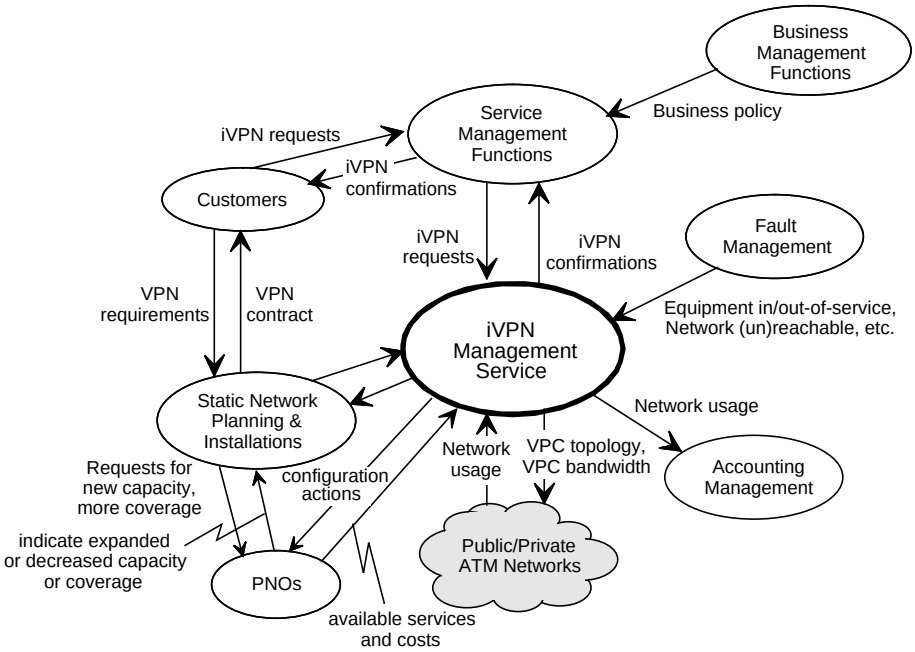


Figure 6.9 Enterprise view of the ATM Leased-line Management Service

6.3.3 Functional decomposition of iVPN

The iVPN Management Service was decomposed using the ICM methodology described in Chapter 3. It was decomposed into several Management Service Components (MSCs).

The *VASP Topology Information MSC* manages the logical and physical information about the underlying networks, links and possible routes through the underlying sub-networks of the VASP. It is decomposed into two MFCs: the *High Level Routing* and *Topology Information MFCs*. The *VASP Information MSC*[1] is used by the VASP TMN to provide useful information for interacting with customers (e.g. accounting, events/alarms, monitoring and performance information). It contains the following MFCs: *Configuration Status and Monitoring*, *Performance Monitoring*, and *Billing and Accounting Information MFCs*.

The *PNO VPN Services MSC* is needed to enable a PNO to provide a restricted high-level view of its underlying Management Services to VASPs. This is needed to present in a single high-level service, a minimal view of underlying PNO MIBs and

1. Not implemented in ICM due to time and effort constraints.

services. A PNO is unlikely to provide services that allow even monitoring or status information about their underlying networks and network elements, as this gives a good idea of the size and scope of an operator's networks (and thus is very sensitive and confidential). Besides the security and access control features provided by an interface like the TMN X-interface, the functionality of the high level Management Services of a PNO must themselves limit the types of services provided and visibility to the utilised lower management levels. The MSC is decomposed into a single corresponding MFC. Likewise, a *CPN VPN Configuration MSC* provides restricted management capabilities of the end-user's CPN.

Each of the MSCs has been mapped onto Operations Systems Functions (OSFs) which in turn have been mapped onto Operations Systems (OSs) residing in different TMN management domains. Communications within a TMN takes place using Q_3 or Q_x interfaces. Communications between OSFs of different TMN domains takes place using the X-interface. The X-interface provides security and access control features, and apart from the fact that the information model presented is different, it is otherwise similar to the Q_3 interface. A more detailed mapping onto the TMN system architecture used in ICM is shown in Figure 6.10.

Several generic security requirements were identified for iVPN:

- The VASP-TMN only has access to PNO-TMN information which is relevant to a VASP activity.
- A PNO-TMN management system will never have access to information from other PNO-TMNs via the VASP.
- The VASP must comply with security constraints of each PNO TMN and CPN TMN.
- The PNO-TMN and CPN-TMN domains are responsible for restricting domain accessibility to the VASP, and vice-versa.

The impact of security policies is generally in this order: from PNOs to VASP, and then from VASP to Customers, i.e. the VASP must obey the security policies provided by the PNOs, and the Customers must obey the security policy agreed upon with the VASP. This is reflected at the enterprise level in the contractual agreements between these parties.

6.3.4 iVPN functions and interactions

The most basic operation of an iVPN Management Service can be summarised in the following interactions:

1 *Initialise topology model*
The VASP-CM-OS obtains appropriate information from PNO and CPN TMNs to create physical and logical topology maps in its MIB. (Topology changes should also be handled.)

2 *Request creation of ATM leased line (EEVPC)*
The human manager requests the creation of an ATM leased-line (EEVPC) between two specified end-points available from the VASP-CM-OS's topology model, using appropriate input criteria (bandwidth, end-to-end cell delay, total cell delay variation, cost, etc.)

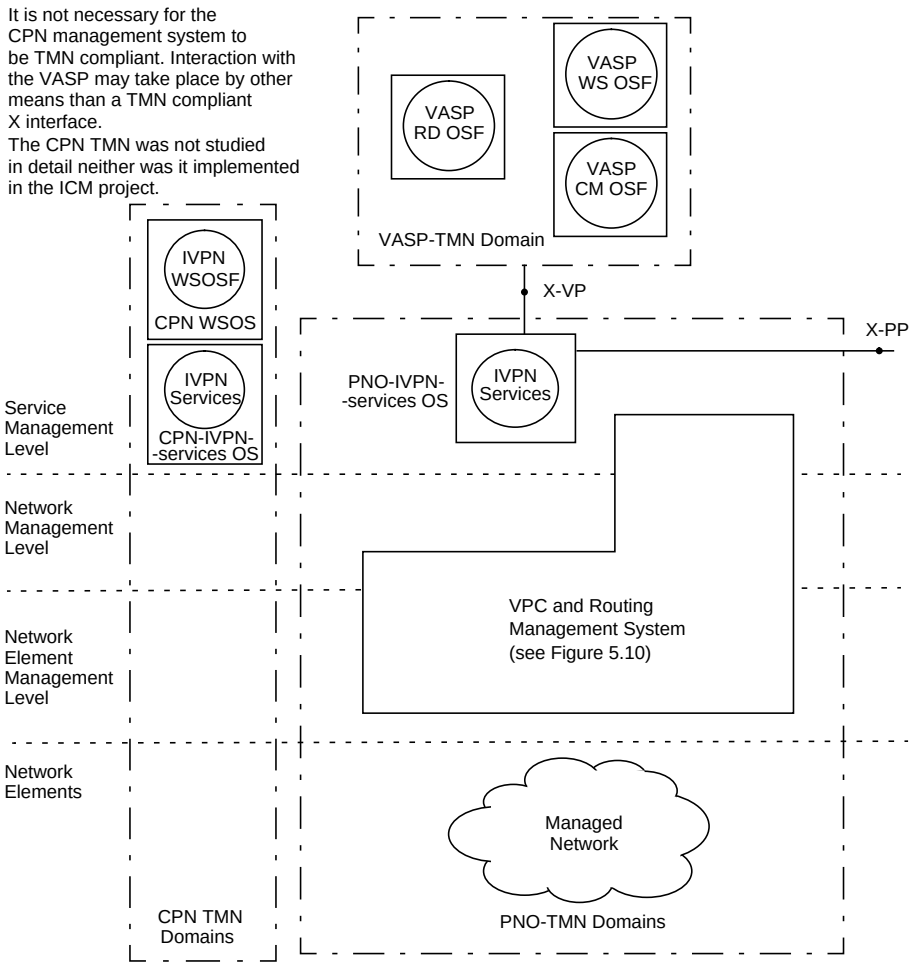


Figure 6.10 iVPN physical architecture (on top of VPCM)

3 *Determine best set of appropriate high-level routes*
The VASP-RD-OS determines a set of high level routes (i.e. which PNOs should be used), based on information it obtains from VASP-CM-OS; and returns an appropriate set of possible choices to the VASP-WS-OS for selection by the user. The VASP-RD-OS can also be easily modified to choose a best possible route for the requester.

4 *Choose best high-level route*
The human manager receives the indication of possible high-level routes from the VASP-RD-OS, and selects one of them for an instantiation of the desired EEVPC

5 *Create appropriate VP connections*
The instantiation is performed using the services of the VASP-CM-OS. It attempts to set up the appropriate underlying VP connections in the desired

PNOs and CPNs, using the services of one or more PNO-IVPN-Services-OSs and CPN-IVPN-Configuration-OSs respectively. This process will either completely succeed (and the VASP-WS-OS will be notified), or may fail. In the latter case, all the intermediate connections are torn down, and the VASP-WS-OS is notified of the reason for failure (e.g. Error: VPC create failed, Insufficient bandwidth in PNOnn). The human manager is notified of the success or failure of their request by the VASP-WS-OS.

6 *Modify or Delete existing EEVPCs*
The human manager may perform other types of activities, e.g. add, modify, delete managed objects residing in the MIB of the VASP-CM-OS.

7 *Fault Notification (not implemented in ICM)*
If an underlying segment or connection used to create the EEVPC should fail, the appropriate PNO-IVPN-Services-OS or CPN-IVPN-Configuration-OS should notify the VASP-CM-OS. This should in turn notify the VASP-WS-OS, which should in turn notify the appropriate human manager.

8 *Configuration and status monitoring (not implemented in ICM)*
Appropriate information should be monitored.

9 *Performance monitoring and accounting (not implemented in ICM)*
Appropriate usage information should be gathered for appropriate billing of the services involved

6.3.5 VASP-RD-OS

The task of the VASP-RD-OS in iVPN is to identify a set of interconnectable PNOs that satisfies the customer's usage requirements, given the constraints of the physical networks involved. This involves mapping the customer's requirements onto the available network resources that the VASP has available in its virtual ATM network and links/capacity available between PNOs. A further requirement could be to provide the leased-line VPCs in the most cost effective manner possible, assuming that multiple route possibilities are involved, each having a different cost.

The VASP-RD-OS will take requests from the customer to create an end-to-end VPC between VASP end-points, and propose (if possible) one or more possible routes that satisfy the customer's requirements. The VASP-RD-OS will use the services of the VASP-CM-OS to access any necessary information about the underlying PNO networks. If no route is possible, because of limitations in the underlying network (e.g. not enough links or bandwidth available), it will notify the network planning functions to purchase additional network resource or bring existing but unused ones into service. Figure 6.11 shows a case where the VASP-RD-OS may propose three possible routes using different PNOs. The VASP-WS-OS can select one of these routes and instantiate an actual VPC using the VASP-CM-OS (see Figure 6.13). The VASP-RD-OS uses information from the VASP-CM-OS to determine which possible routes that match the criteria for the desired EEVPC.

The containment schema of the VASP-RD-OS information model is shown in Figure 6.12. The MOs shown are all derived from the X.721:top MO class. The vaspRouteRequest MO identifies a particular request for the VASP-RD function to iden-

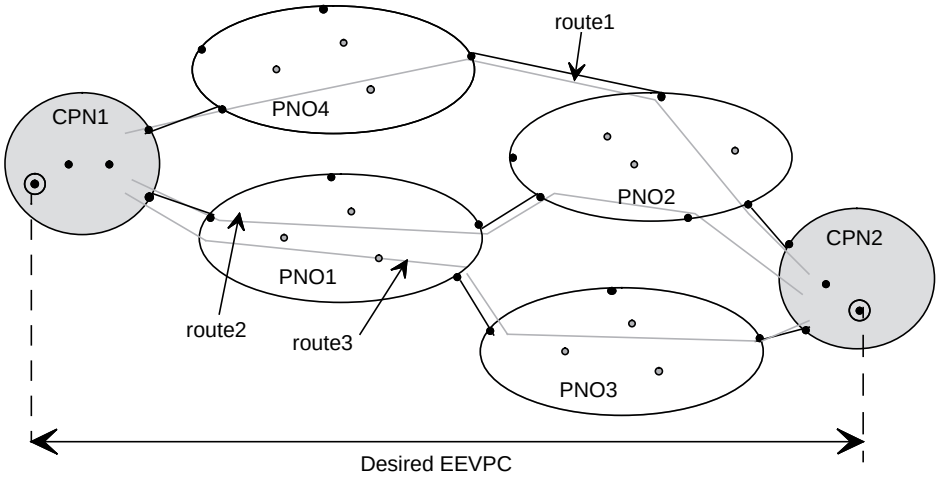


Figure 6.11 VASP-RD-OS proposes high-level routes (through appropriate PNOs)

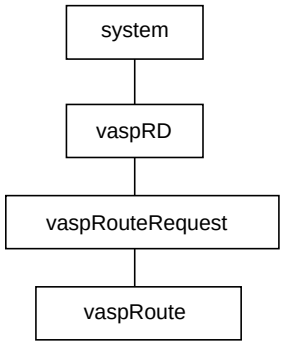
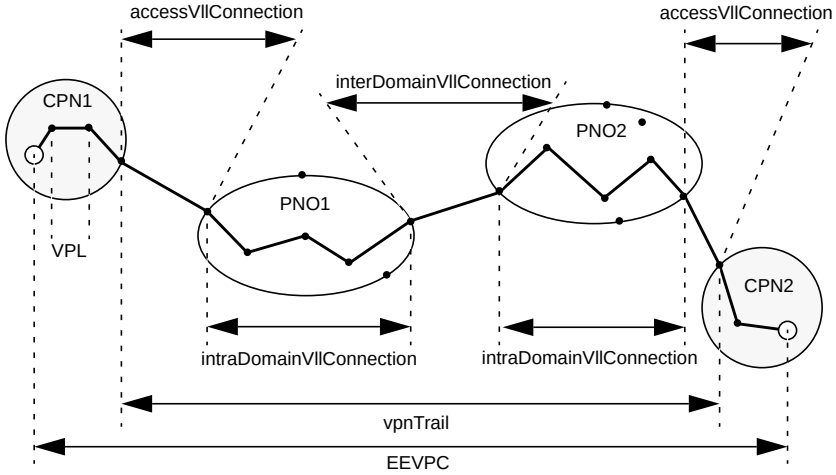


Figure 6.12 Containment schema of VASP-RD information model

tify possible routes for building a vpnTrail. It is created by the request of the VASP-WS-OS. Its attributes specify the desired source and destination for the trail and the desired class of service. The vaspRoute MO represents a possible route through the set of available PNOs, as identified by the VASP-RD function, to satisfy a particular route request. Its attributes specify the cost, available bandwidth, and a list of vllConnections needed to instantiate an instance of the route through the subnetworks. It can be used by the VASP-WS-OS to request creation of a vpnTrail using the services of the VASP-CM-OS.

6.3.6 VASP-CM-OS

The VASP Configuration Manager maintains a model of the connection resources made available to it by the various PNOs with which it has contracts, together with administrative details concerning the PNOs and CPNs. It passes topological information to the high level route design function. It also maintains the logical view of the VASP's network (PNOs, PNO-endpoints, inter-domain links, VPCs, VPNs, etc.). The logical view of the network for one EEVPC is shown in Figure 6.13 [6.31]. The VASP-



Note: The VASP Configuration Manager does not see the actual topology of intraDomainVllConnections. These are an internal matter for the PNOs. The VASP-CM-OS sees only the endpoints and the capabilities (bandwidth and performance) of the intraDomainVllConnections.

Figure 6.13 Logical resource component view of VASP-CM-OS

RD-OS is used to propose a set of possible PNO routes through the VASP's underlying virtual ATM network. The VASP-WS-OS operator can then request that an EEVPC is created using one of the proposed routes. The operator could also request the deletion of an existing VPC. Both these requests are handled by the VASP-CM-OS.

The VASP-CM-OS contains the information about the EEVPCs that have been created, or are in the process of being created. The VASP-CM-OS uses the services of the PNO-IVPN-Services-OS to obtain information about the underlying PNO networks, and inter-domain links, needed to create a physical and logical model of the VASP topology. The EEVPCs used for the ATM leased-lines are fixed-bandwidth (they are tagged as class 1 by the VPCM system, see Section 5.6.1). The PNO guarantees that their bandwidth will not be modified by other activities in the PNO that may perform load balancing of other PNO VPCs. This was accomplished in ICM, by the concept of different classes of VPCs within a PNO.

The inheritance hierarchy and containment schema of the information model used by the VASP-CM (corresponding to Figure 6.13) are shown in Figure 6.14 and Figure 6.15.

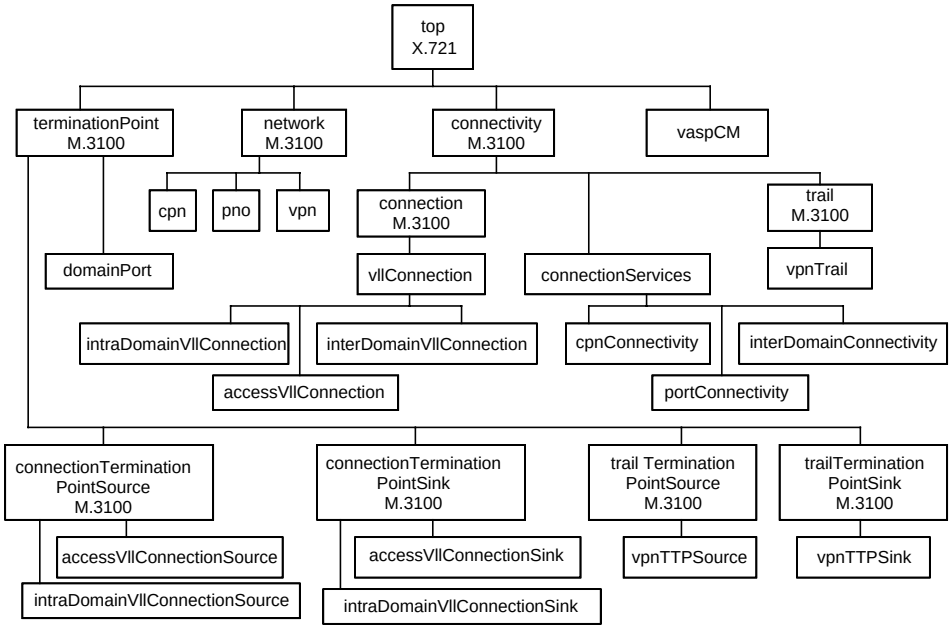


Figure 6.14 Inheritance hierarchy of VASP-CM information model

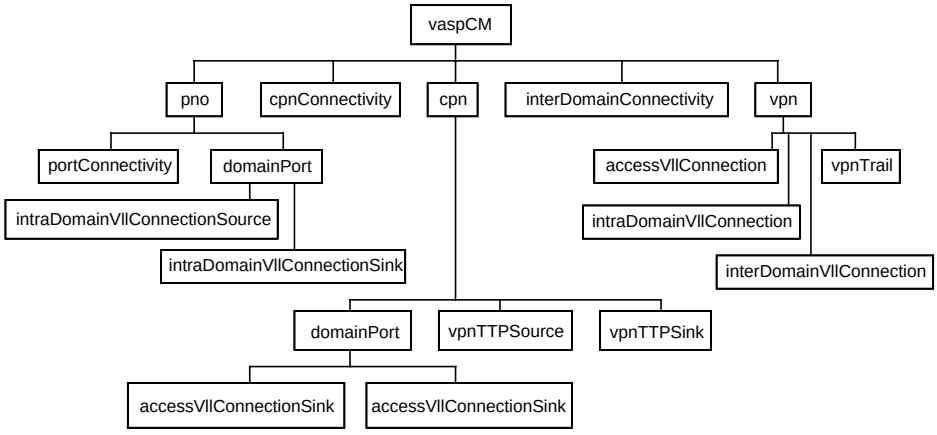


Figure 6.15 Containment schema for VASP-CM information model

6.3.7 PNO-IVPN-Services-OS

The PNO-IVPN-Services-OS contained within each PNO TMN management domain is the high level interface to the underlying VPCM OSs (see Chapter 5 and Figure 6.10). Its design restricts the types of Management Services and information that the PNO provides to the VASP.

This OS is responsible for providing the X interfaces of the PNO. Two types of X interface are supported: X-VP between the VASP and the PNO, and X-PP between itself and peer PNOs involved in providing the EEVPC.

Over the X-VP interface, it provides the VASP-CM-OS with appropriate topology information for it to model the end-points that may be used to create interDomainVll-Connections or accessVllConnections (see Figure 6.13). The latter are access end-points on the boundary of the PNO TMN, where segments of the EEVPC can be made to terminate inside each PNO TMN. The OS is responsible for choosing, creating, and maintaining an internal transit route between access end-points, when the VASP-CM-OS requests creation of an intraDomainVllConnection between two access endpoints. It also informs the VPCM Management Service that the appropriate VPC resources are *fixed bandwidth* as described in the previous section.

Over the X-PP interface, this OS is also responsible for interactions with peer PNO-IVPN-Service-OSs in other PNO TMN domains to negotiate, for example, the VPI used on a Virtual Path Link (VPL) connecting two PNOs.

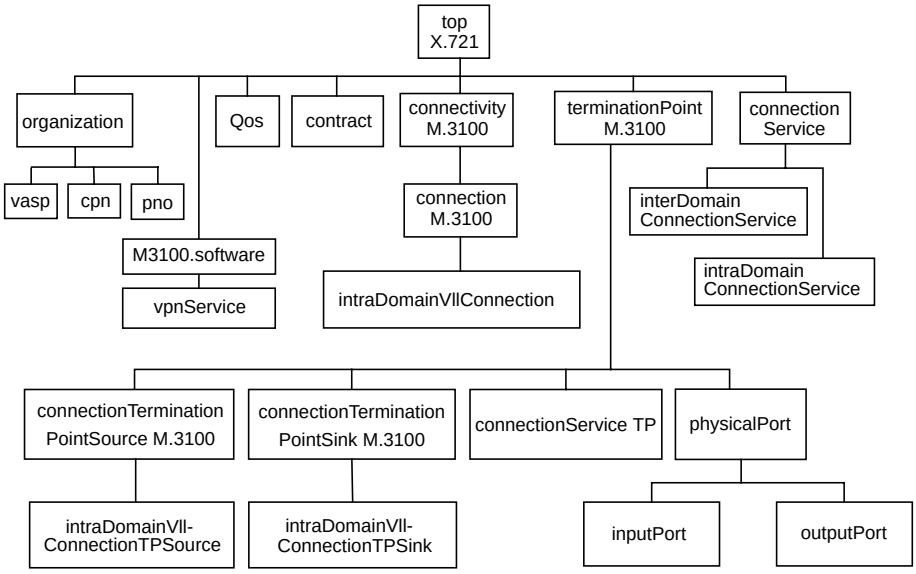


Figure 6.16 IVPN-services OS inheritance hierarchy

Figure 6.16 depicts the inheritance hierarchy, while Figure 6.17 shows the containment schema of the PNO-IVPN-Services-OS MIB. The agent part of the PNO-IVPN-Services-OS supports three types of interface: An internal Q_3 interface to provide

information to the PNO WS-OS, and two external X interfaces - X-VP and X-PP. The same agent supports all three interfaces, security mechanisms ensure that the managers accessing the MIB only see the subtree(s) to which they have access (see Figure 6.17).

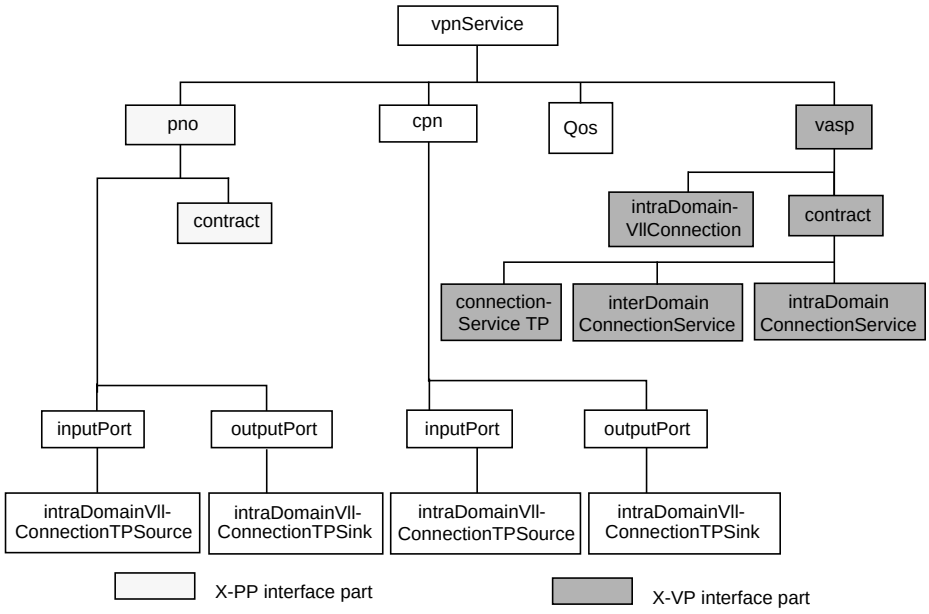


Figure 6.17 IVPN-services OS containment schema

6.3.8 CPN-IVPN-Configuration-OS

This management OS is responsible for configuring the remaining VPLs within the CPN TMN domain, and to automatically negotiate the VPI used on each access link to PNO. The CPN-IVPN-Configuration-OS was not implemented in ICM.

6.3.9 VASP-WS-OS

The VASP workstation OS (VASP-WS-OS) is the human computer interface (HCI) used by maintenance personnel working for the VASP operator. The VASP-WS-OS can be used for naming the customer-sites (CPNs) to be connected via VPCs (identified as endpoints residing on PNOs), describing the desired VPC performance requirements (e.g. bandwidth, end-to-end cell delay, jitter, cost, etc.) for an EEVPC. The VASP operator is allowed to invoke requests for proposed routes between CPNs using the services of the VASP-RD-OS. The operator may then select the most appropriate route that meets their requirements, and use the services of the VASP-CM-OS to instantiate it. The VASP-WS-OS presents a graphical interface used to add, delete, modify and view information about customers, PNOs, VPNs, EEVPCs (and underlying components).

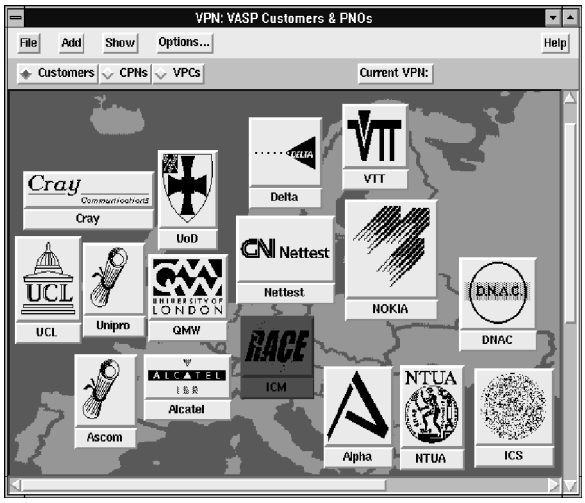


Figure 6.18 Customer view

Figure 6.18, displays all the potential customers. Figure 6.19 shows the VASP operator information about a particular customer - their CPNs, available PNOs to serve them, and existing access links between their CPNs and PNOs. Figure 6.20 shows the existing EEVPCs in use for the customer's VPN. Figure 6.21 shows a request for a new EEVPC. Figure 6.22 shows a choice of two possible routes proposed by the VASP-RD that fulfil the request for a new route. By clicking on one of these, the VASP operator will attempt to instantiate a new EEVPC using the selected route. If successful it will be reflected in the VPC view (Figure 6.20) of the customer's VPN, otherwise appropriate errors will be reported to the VASP operator.

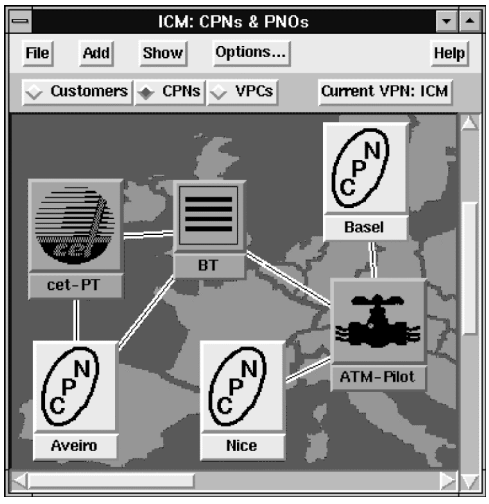


Figure 6.19 CPN view

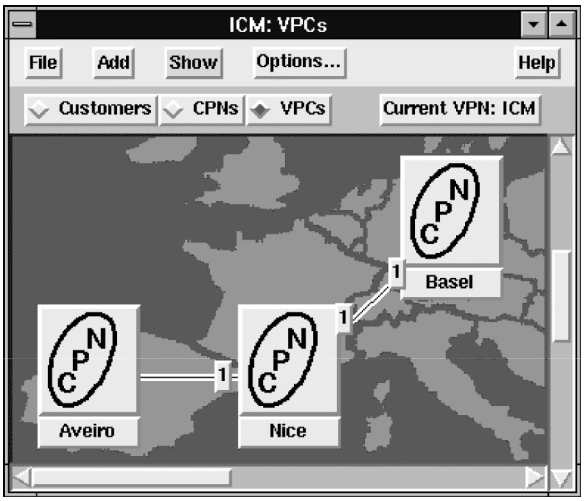


Figure 6.20 VPC view

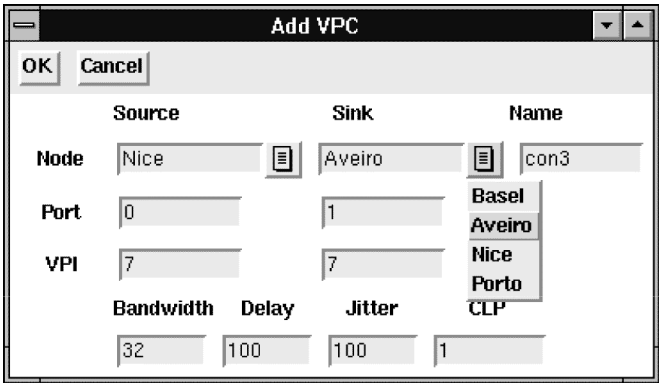


Figure 6.21 Adding a new VPC

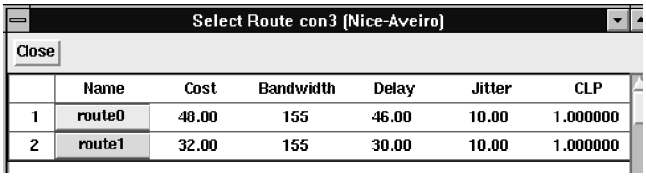


Figure 6.22 Choosing a route suggested by VASP-RD-OS

6.4 The tVPN Management Service: harnessing the true power of ATM

6.4.1 Overview

As introduced in Section 6.2.4, iVPN is implemented by interconnecting CPN equipment over leased lines, where the leased lines are either dedicated or they are provided by means of cross-connect equipment in the public domain. The dedication of network resources to connect the customer equipment results in increased cost for leased line provisioning and requires extended customer capabilities to manage their leased resources. It is very likely that the utilisation of network resources is not optimum due to the dedication of resources to individual customers, and, in general, there is no multiplexing of VPN traffic and ordinary network traffic. It is even possible for the call blocking probability in the underlying network to be higher than necessary due to lack of capacity while the resources dedicated to the leased line customers are lightly utilised. The cost therefore associated with private networks is high due to the dedication of resources to the end-to-end connections.

tVPN will allow network resources to be used more flexibly and more efficiently by adjusting to the changing traffic requirements of the customers. The gains in efficiency imply that tVPN will allow value-added services to be provided at a relative low cost compared to those in the sVPN and iVPN environments.

Within the t-VPN framework, this section elaborates on VPN service provisioning in a multi-operator, multi-provider environment.

Utilising the advantages of the ATM technology, ICM has proposed the notion of the *Broadband Switched VPN* (BX-VPN) as an efficient means for realising the VPN concept, in the tVPN context. According to this approach, the VPN is not a collection of leased lines but a network in its own right, offering multiplexing of different customers and hence the opportunity for increased VPN utilisation.

This section focuses on the definition of the fundamental BX-VPN concepts and ideas. The issues involved with BX-VPN provisioning and operation are discussed from the viewpoints of the PNOs and the VASPs, with particular emphasis on the management issues. It is shown how the BX-VPN concept increases the manageability of VPNs, therefore increasing the flexibility in provisioning, reducing redundancy and inefficiency inherent in static configurations. The operational and maintenance aspects are discussed and the functionality required for managing the BX-VPN is identified and described in terms of Management Services. Furthermore, the issues and policies for multiplexing VPN and other traffic at the public network domain are identified. The required enhancements in the PNO management functionality for guaranteeing the coexistence of the VPN services and network services are identified. A management system architecture for realising the proposed concepts and ideas is also proposed.

6.4.2 The BX-VPN concept

In leased line based networks, customers are provided with (semi-) permanent end-to-end connections interconnecting their sites. In this scenario, the customer is responsi-

ble for routing its traffic over the correct leased lines in order to arrive at the required destination, by configuring routing tables within its CPN equipment.

Multiplexing and switching are the fundamental techniques employed by ATM for implementing an integrated access and transport network. Taking into account the advantages of the multiplexing technique [6.39], ICM tried to exploit the features of ATM technology in the provision of tVPNs. In this direction, the notion of BX-VPN is proposed as an efficient means for realising tVPNs.

The prime motivation behind the BX-VPN concept is to optimise the resources rented from the underlying networks. The main objective of the BX-VPN concept is to permit the multiplexing of different customers to optimise VPN utilisation.

Driven by the above objective, the BX-VPN is not a collection of leased lines offering end-to-end connectivity between the individual sites of a customer as the current VPNs [6.40][6.41], but a network in its own right. In this respect, BX-VPN focuses on developing an architecture that will enable the multiplexing of the traffic of the individual BX-VPN customers in an attempt to achieve the best possible utilisation of the rented resources. The BX-VPN concept offers several degrees of freedom in achieving this kind of coexistence, which if managed properly by efficient resource management and routing algorithms will allow optimum utilisation of the network resources.

A BX-VPN is virtually built by *reserving* the required resources from the underlying network(s). However, the BX-VPN has all the elementary components constituting a real network:

- *BX-VPN links* which are defined to be the transmission means of the BX-VPN over which the BX-VPN user traffic is multiplexed. The BX-VPN links represent an amount of bandwidth and are characterised by their performance (in terms of cell loss, delay, etc.).
- *BX-VPN switches* which provide the switching capability of the BX-VPN necessary for routing and multiplexing the BX-VPN customers traffic. BX-VPN switches maintain appropriate routing tables which facilitate the proper routing of the BX-VPN calls over the BX-VPN links. The routing decisions taken by the VASP are reflected in terms of route selection entry updates in the routing tables of the BX-VPN switches.

BX-VPN links and BX-VPN switches are virtual resources which have been introduced in order to allow the VASP to operate and manage its own virtual network. However, they correspond to physical counterparts in the PN(s) domain(s). The following mappings have been considered (Figure 6.23):

- A BX-VPN link corresponds to one or more VPCs in the underlying PN.

  The BX-VPN links are assigned an amount of bandwidth to enable the transport of the BX-VPN customer information. This amount of bandwidth is reserved in the underlying PN(s) in terms of VPCs. There need not be an one-to-one mapping between BX-VPN links and VPCs. A BX-VPN link may be mapped to a network of VPCs where the minimum cut (capacity) of the VPC network equals the capacity of the BX-VPN link.
- The BX-VPN switches are subsets of the VC switches in the public network which interconnect the VPCs corresponding to the BX-VPN links.

  The switching capability reserved in the PN is in terms of entries in the route selection tables to enable the routing of BX-VPN traffic over the BX-VPN

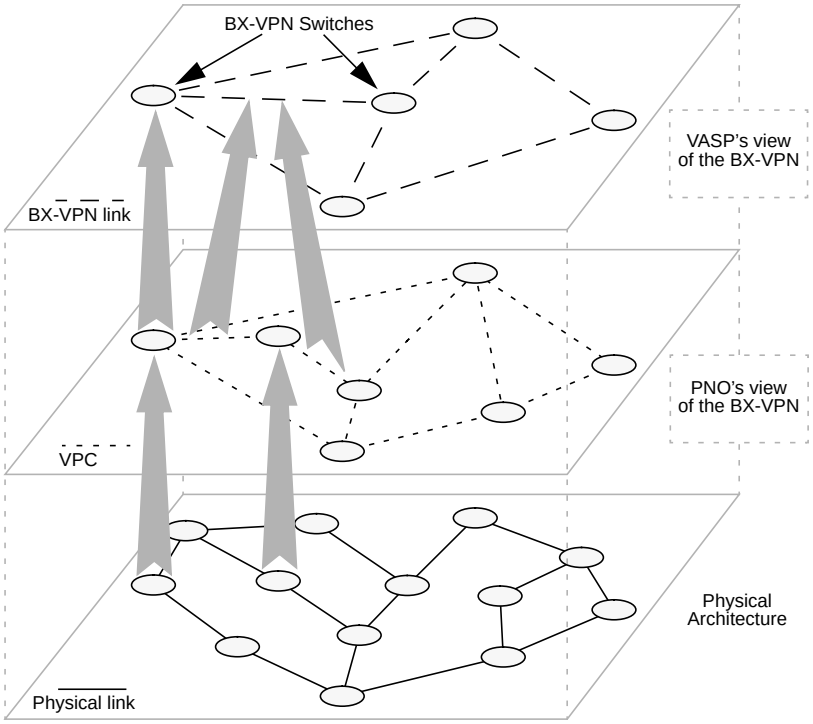


Figure 6.23 BX-VPN concept

links. At connection set-up time the public network's control and signalling procedures identify BX-VPN calls and use the BX-VPN entries of the route selection tables (as opposed to those entries used for the public switched traffic) to route the BX-VPN calls.

In order to rent resources from the underlying PN(s) to build its own network, the VASP must estimate the traffic to be generated by the BX-VPN customers. These estimates are based on the contracts between the VASP and its customers and on statistical traffic measurements once the VPN is operational. Appropriate configuration policies should be exercised by the VASP to meet varying traffic conditions and to optimise the utilisation of the rented network resources. In particular, traffic conditions change as the BX-VPN users needs change and as customers are added or deleted from the BX-VPN customer list. Hence, the VASP must be aware of the BX-VPN state to be able to estimate the additional resources required to support the requirements of new customers. This is illustrated in Figures 6.24 and 6.25

In Figures 6.24 and 6.25, the dark coloured nodes are the public network resources which, or part of which, form the BX-VPN resources. The light-coloured nodes are the PN resources which are used solely for the PNOs purposes and are not of concern to the BX-VPN. As illustrated in Figure 6.24, customer A1 owns three sites to be interconnected by using the BX-VPN resources. Traffic from site A1 to site A2 may be multiplexed with traffic from site A3 to site A2.

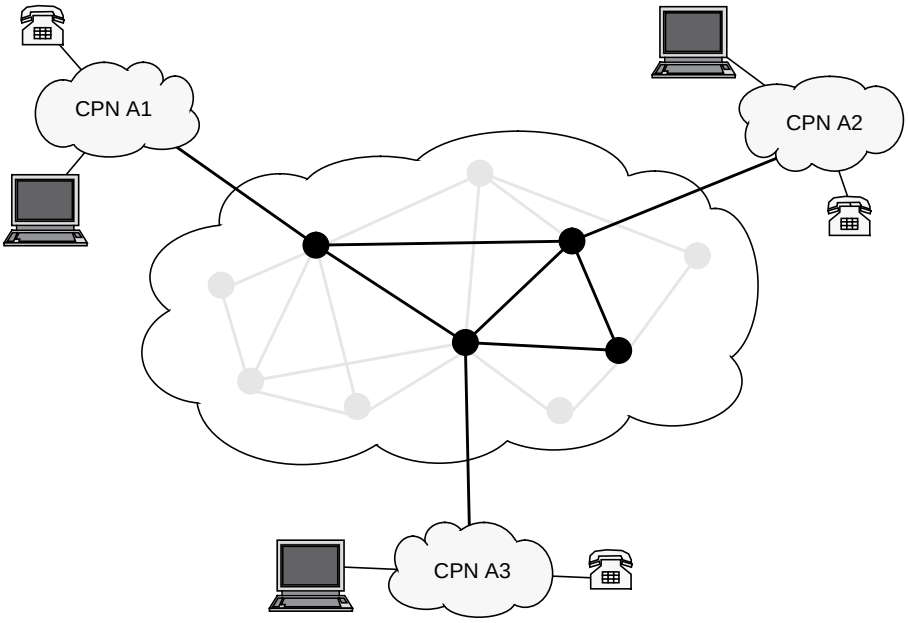


Figure 6.24 BX-VPN configuration - example 1

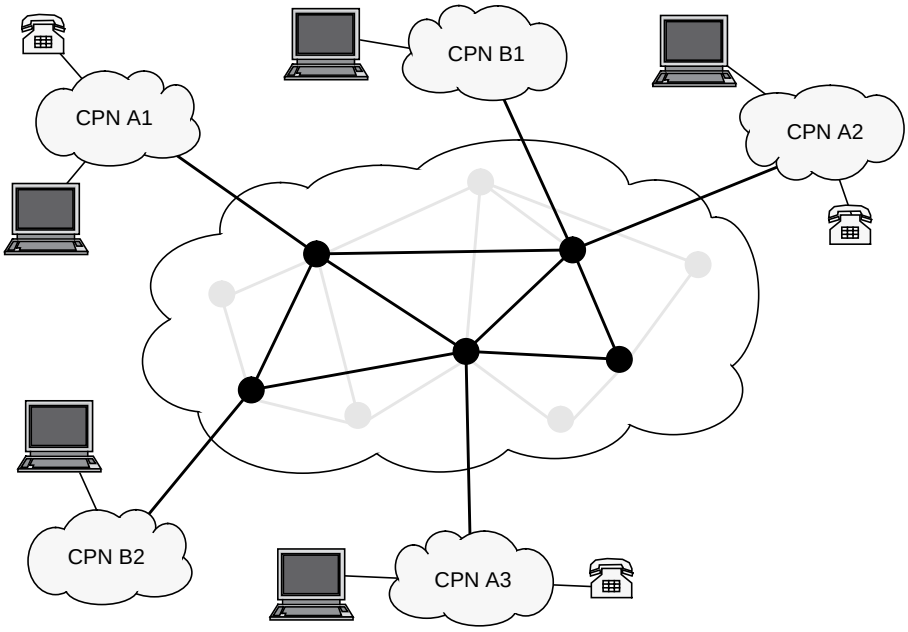


Figure 6.25 BX-VPN configuration - example 2

When a new customer is added (Figure 6.25), the VASP may need to rent additional resources; i.e. BX-VPN switches and BX-VPN links. The additional requirements may be met by: renting new resources from the PNs; by increasing the capacity of existing resources; or it may be possible to utilise existing resources with the same capacity in the case where the existing resources were under-utilised.

Once the infrastructure of a BX-VPN has been established, the set-up and release of individual customer connections is achieved through the control and signalling mechanisms of the PN. In this respect, the appropriate switching capability is reserved in the PN in order to realise the call control procedures. The control and signalling mechanisms of the public network must be properly updated to handle the BX-VPN calls in addition to the ordinary network calls. It is worth examining the call set-up procedure of the BX-VPN connections.

In Figure 6.26, a typical system configuration is depicted. The CPNs are connected to the core network via BX-VPN links. Where necessary (for example, when the CPN technology is not ATM), an interworking unit exists between the access node of the network and the CPN equipment. When a user (e.g. user X) wants to communicate with the user Y who resides in a remote site, a call request is created and is passed to the IWU of the CPN at the calling site. The IWU is responsible for generating ATM consistent call requests via the UNI signalling procedures of the public network. The requests are passed to the access node of the public network via a signalling protocol over the VPL connecting the CPN to the core network. The access node identifies that a request is for a BX-VPN call (by the use of a specific prefix in the called party number, for example) and therefore uses the route selection tables of the BX-VPN as opposed to those it would normally use for public switched traffic. In the case where a closed user group uses a private numbering plan, the mapping of the called number to the actual destination address is handled by the existing Intelligent Network (IN) facilities of the public network (in which case the IN resources would be pre-configured and subsequently managed by the VASP) or possibly by a direct mapping in the IWU.

All the network switches corresponding to BX-VPN switches store routing information for BX-VPN calls[1]. This information associates a particular BX-VPN service class and network destination with an outgoing VPC corresponding to a BX-VPN link. Using the PN signalling facilities, the BX-VPN call request is passed from BX-VPN switch to BX-VPN switch until it reaches its destination.

The provisioning and operation of BX-VPNs requires basic control and management functionality in the underlying PNs, and additionally requires management functionality in the VASP to specifically manage the BX-VPN operation. In the following section the management issues at both the VASP and the PNO levels will be discussed.

6.4.3 BX-VPN management issues

Management functionality needs to exist at both the VASP and PNO levels to support the BX-VPN concept. In the PNO domain, enhancements to existing management functionality are required, while the VASP must deploy management functionality to

1. The BX-VPN routing table entries are defined by the VASP management system. They are deployed by the PNO on the request of the VASP.

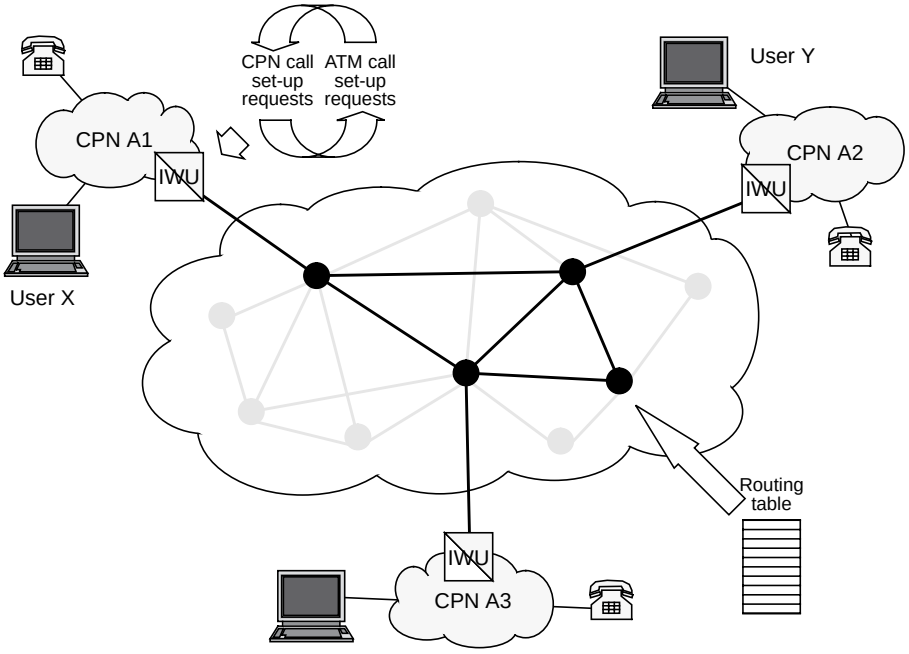


Figure 6.26 A typical system configuration

cover the policies and decision making mechanisms that will guarantee the successful provisioning, maintenance and operation of the BX-VPN as a whole.

Table 6.1 introduces the overall management issues involved with the provisioning, operation and maintenance of BX-VPNs in both the VASP and PNO domains.

Management Issues	At the VASP level	At the PNO level
BX-VPN Configuration	Concerned with building the BX-VPN by determining the type and quantity of resources to be rented from the PN(s). It involves routing at a high level (to identify the PNs) and resource management (see below).	Concerned with the provision of the requested BX-VPN resources. The PN provider must determine whether the resources requested by the VASP are available to meet the VASP's requests. Dynamic BX-VPN re-configuration guarantees the employment of efficient resource policies in the PN (see below).
BX-VPN Customer Traffic Characterisation	This is the process for estimating the expected traffic of BX-VPN customers in order to determine the required capacity of the BX-VPN.	

Table 6.1 BX-VPN management issues

Management Issues	At the VASP level	At the PNO level
BX-VPN Usage Predictions	Based on measurements of the BX-VPN customer traffic, VASP makes predictions on future BX-VPN customer requests.	PNO predicts BX-VPN needs in resources based on actual BX-VPN traffic measurements. These predictions are useful in exercising resource reservation strategies.
BX-VPN Resource Management	Concerned with the management of the logical resources constituting the BX-VPN. Efficient resource management guarantees better utilisation of the BX-VPN resources. BX-VPN configuration results in exercising resource management.	Policies are employed by the PN in order to optimise the utilisation of the network resources that have been rented to BX-VPN.
Routing	Determines how the traffic of the individual BX-VPN customers will be routed over the BX-VPN links. The BX-VPN routing plan is passed to the PN for the routing tables of the rented portions of the PN switches to be configured.	PN must be able to realise the decisions made at BX-VPN level. These decisions are passed to the PN to update the routing tables.
Monitoring	Enables the BX-VPN provider to monitor the usage of the BX-VPN resources. These results are a necessary input to the resource management policies.	Permits the PNO to estimate both the ordinary PN traffic and the BX-VPN load in order to exercise the appropriate resource management policy. The PNO also provides the required measurements according to the BX-VPN monitoring requirements.
QoS Monitoring	Enables the VASP to assess the performance of the BX-VPN and the quality of the offered BX-VPN services. In the case of QoS degradation the VASP reconfigures the BX-VPN or makes complaints to the PNO if the PN performance is low.	PNO needs to assess that the performance of the rented resources meet the performance targets negotiated with the VASP. This activity quantifies the efficiency of the employed resource management schemes and is used for analysing BX-VPN complaints.
Security Aspects	Concerned with the employment of proper authorisation and access control mechanisms to protect the BX-VPN user against unauthorised use.	Concerned with the protection of the BX-VPN traffic so that ordinary PN traffic and BX-VPN traffic will not interfere.

Table 6.1 BX-VPN management issues

Management Issues	At the VASP level	At the PNO level
Accounting/Billing	Used to calculate the charges for each BX-VPN customer. It is based on information about the utilisation of the BX-VPN resources. The accounting policies employed determine the profit of VASP.	Exercised by the PNO in order to charge the VASP for hiring the PN resources. The PNO also provides the VASP information on the utilisation of the rented PN resources in order to facilitate accounting at the BX-VPN level.
Customer Administration	Concerned with the maintenance of information pertinent to the BX-VPN customers and services. The BX-VPN customers provide the VASP with the topological aspects for interconnection of their sites and negotiate the service(s) available. This information is used by the VASP in order to configure his own network and to guarantee that the contract with the customers is preserved.	The characteristics of the services are negotiated with the VASP. Moreover, PNO maintains records of the VASPs he is working with.
Complaints Analysis	Concerned with the collection of customer complaints. The complaints analysis in combination with the BX-VPN performance monitoring facilitates the identification of potential problem occurred to either the BX-VPN of the underlying network that has caused the degradation of the offered QoS.	Analysis of complaints at the VPN level results in either further negotiations with the PNO or expression of complaints to the PNO regarding low performance of the PN. In the latter case, the PNO needs to be able to analyse the complaints and provide satisfactory answers.
Service Creation and Provision	Design and provision of new services to accommodate the specific needs of the BX-VPN customers. The VASP gathers information about the needs and complaints of the customers. Based on this information, the VASP negotiates with the PN for the creation of new services.	Creation of new services in order to meet the BX-VPN requirements. The VASP provides the PNO with the expected characteristics of the new services. The PNO performs the necessary actions to result in the provision of the new services.

Table 6.1 BX-VPN management issues

The following sections discuss resource management and routing management in more detail as these issues are particularly relevant to BX-VPN. These two management areas distinguish the BX-VPN concept, providing flexibility in configuration and potential gains in efficiency benefiting the customer and both the VASP and the PNO organisations.

6.4.3.1 Resource management at the VASP level

In general, resource management involves actions to ensure efficient utilisation of network resources. Specifically, in the BX-VPN environment, resource management is concerned with managing the resources rented from the PN(s).

It should be stressed that although the VASP manages its own virtual resources, it does not manage directly their physical counterparts, these are managed by the PNO(s) according to the decisions by the VASP. For instance, the VASP may know that the transmission capability it has rented between two BX-VPN switches has a capacity of 50 Mbit/s but it does not care how this transmission capability is physically realised in the underlying network. When the VASP decides to increase the capacity of a BX-VPN link to, say, 80 Mbit/s, this management decision is passed down to the PNO TMN which is then responsible for its implementation.

The main target of Resource Management in the VASP domain is the estimation of the resources to be rented from the PN(s) in order to meet the demands of the BX-VPN customers. Based on information retrieved from its customers and through the procedure of BX-VPN Customer Traffic Characterisation, the VASP determines the type and the amount of resources to rent from the PN(s). Through the interaction with the operators of the underlying networks the VASP rents the required resources in terms of BX-VPN links and BX-VPN switches.

When new customers are to be accommodated by the BX-VPN or the requirements of the existing customers change, the scope of resource management is to adapt the BX-VPN capabilities to the new requirements. The resource management actions may result in the re-configuration of the BX-VPN topology in the following ways:

- the amount of bandwidth corresponding to the BX-VPN links is increased or decreased,
- new BX-VPN resources are added, or,
- existing BX-VPN resources are deleted.

Resource management activities are triggered:

- at customer request epochs, at which the VASP gets new requests for customer connectivity changes (i.e. add, delete sites, modify connectivity characteristics of existing connections), and,
- dynamically, according to the current performance of the BX-VPN.

Figures 6.24 and 6.25 provide an example. Initially, customer A, with three sites, is inter-connected by the BX-VPN. When customer B is introduced the BX-VPN configuration is changed to meet the requirements (Figure 6.25). The figure shows that new resources were rented, furthermore the capacity of the existing resources supporting customer A may have been increased.

After the management decisions have been taken, the VASP negotiates with the PNO for the reservation of the required resources. The PNO in its turn provides the agreed resources to the VASP.

6.4.3.2 Routing management at the VASP level

As described previously, the VASP rents switching as well as transmission capabilities from the underlying PNO(s). The switching capability allows the VASP to multiplex traffic over the BX-VPN resources according to an appropriate routing plan (i.e. set of routes between customer sites).

The logical BX-VPN switches exhibit the principal characteristics of the underlying physical switches residing in the public network. That is, a BX-VPN switch maintains a Route Selection Algorithm (RSA) and an associated route selection table to choose an appropriate route for incoming BX-VPN call requests.

In connection oriented networks, such as ATM, routing decisions are made at call establishment time, by the control plane. However, an associated management activity is concerned with ensuring that the correct information is available in the network switches to enable suitable routing decisions to be made.

Based on the topology of the BX-VPN network and the service classes offered, the VASP determines an appropriate routing plan. This involves defining the route selection table entries to be down-loaded to the BX-VPN switches. Each route selection entry associates a particular destination and a given service class with the appropriate outgoing BX-VPN link.

The VASP routing plan may change dynamically in order to meet varying traffic conditions in the BX-VPN. In particular the routing plan may change when:

- the BX-VPN traffic load changes significantly,
- the BX-VPN customers requirements change, e.g. new customers are added or new service classes are introduced,
- the performance of the BX-VPN deteriorates.

6.4.3.3 Resource and routing management at the PNO level

Chapter 5 dealt with the details of the PNO management issues with respect to resource and routing management for the provision of public switched services. The support of BX-VPN services requires extensions to this management functionality.

It is the PNO who provides the physical resources for BX-VPNs following negotiations with the VASP. In this respect, the management functionality employed by the PNO must be enhanced to enable the coexistence of both public switched traffic and BX-VPN traffic on the same physical network infrastructure. This section will examine how PNO resource management and routing policies are influenced by the existence of BX-VPN.

The VASP rents transmission capability from the PNO in terms of BX-VPN links. The PNO in turn, reserves the requested resources in terms of VPCs. A key objective is that the PNO should be able to exercise flexible resource management and routing policies so that the public and BX-VPN services coexist without adversely affecting one other.

As illustrated in Figure 6.27, a network of VPCs may be used to implement a BX-VPN link. For instance, the BX-VPN link depicted in the figure corresponds to the VPCs: {ab1, bc1, cg1}, {ad1, de1, ef1, fg1}, and {ad2, df1, fg2}. The sum of the capacities of the set of VPCs supporting the BX-VPN link must always be equal to or

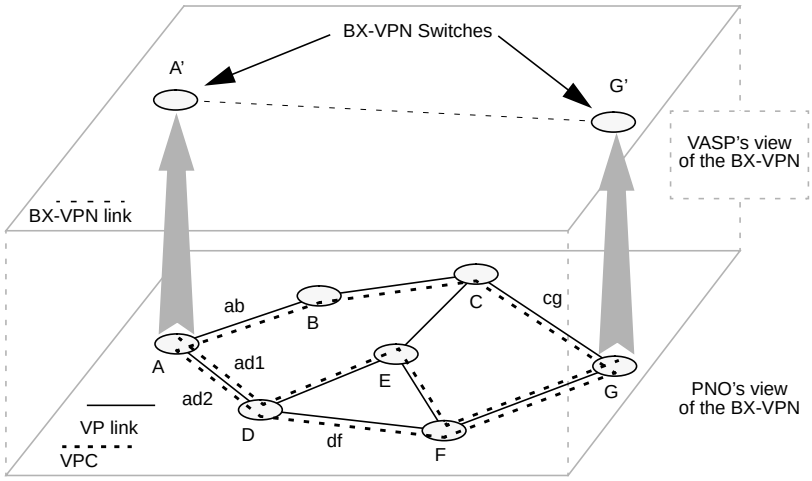


Figure 6.27 BX-VPN link handling in the PNO domain

greater than the negotiated capacity of the BX-VPN link. (It is assumed that all VPLs in a VPC are assigned the same amount of bandwidth).

This scheme allows the PNO to adopt flexible resource reservation policies. For example, there may not be enough capacity available along a single sequence of links to reserve the full bandwidth requested by the VASP for a BX-VPN link. Alternatively, a PNO may not wish to allocate a significant proportion of link capacity to the VASP as this may restrict the PNO's own resource and routing management options for managing the ordinary public switched traffic.

The VASP does not see how the PNO has implemented the BX-VPN link, it has an abstract view of the total capacity of the BX-VPN link and its end points.

As far as the BX-VPN routing plan is concerned, the VASP passes its defined routing plan to the PNO. The PNO will use this information so that the BX-VPN customers traffic will be properly routed over the VPCs reserved for the BX-VPN needs. The PNO's own routing plan for its ordinary switched services must guarantee that the performance requirements of the BX-VPN services will be preserved while the PN ordinary traffic will not be affected by the BX-VPN traffic.

6.4.4 Decomposition and mapping to the TMN architecture

The previous two sections have presented the concept of BX-VPN for provisioning VPNs in the tVPN framework together with the operational and management issues involved. This section elaborates on an architecture supporting BX-VPN management.

The enterprise view presented for the iVPN Management Service in Section 6.3.2 (see Figure 6.9) reflects also the BX-VPN Management Service.

The TMN architectural framework recommended by the ITU-T [6.1] is adopted. Following the methodology of the ITU-T Recommendation M.3020 [6.26], Management Services are decomposed into Management Service Components (MSCs) which

are in turn are decomposed into Management Functional Components (MFCs). The derived MFCs are mapped to the hierarchical layers of the TMN and to the TMN function blocks (OSFs, MFs etc.) of the TMN functional architecture.

6.4.4.1 MSCs and MFCs

The BX-VPN Management Service is decomposed into MSCs and MFCs as follows:

- A *Customer Information Service* MSC, responsible for carrying out all the necessary interactions and operations related with the VPN customers. It is further decomposed into the following MFCs:
  - A *Customer Interaction* MFC, responsible for carrying out the interactions with the VPN customers e.g. receiving requests and complaints, sending responses etc. The interactions with the VPN customers can be achieved through proprietary means or over standardised interfaces.
  - A *Customer Traffic Characterisation* MFC, with the purpose of monitoring and subsequently characterising customer traffic.
  - A *Customer Administration* MFC, responsible for storing all customer related information, e.g. location, services used etc.
- A *VASP Configuration Manager* MSC, responsible for maintaining a model of BX-VPN resources and implementing the required configuration changes. It is further decomposed into the following MFCs:
  - A *VPN Resource Configuration* MFC, responsible for maintaining a model of the BX-VPN resources and for implementing configuration changes through appropriate communication with the PNs.
  - A *PN Information Service* MFC, responsible for maintaining a repository of the PNs with which the VASP is associated, their connectivity and their offered services.
- A *VASP Route Design MSC*, responsible for exercising appropriate resource management and routing management policies so that the BX-VPN performs within contractual levels. The scope of BX-VPN resource management and routing has outlined in the previous sections. This MSC is further decomposed into the following MFCs:
  - A *BX-VPN Usage Predictions* MFC, with the purpose of predicting future BX-VPN customer requests per offered VPN service class.
  - A *VPN Resource Monitoring* MFC, responsible for monitoring the actual usage of the VPN resources. The measurements are taken from the underlying PNs, through the interaction of the VPN Resource Configuration MFC, and are forwarded to the management functions responsible for resource and routing management (see below).
  - A *VPN Design* MFC, concerned with the construction of the BX-VPN by determining the type and quantity of resources to be rented from the underlying PNs. This MFC also defines the routing plan according to which the different VPN customer classes will be routed through the BX-VPN.

    This MFC is triggered by VPN customer requests and by degraded BX-VPN performance. The inputs to this MFC are the VPN customer usage predictions from the BX-VPN Usage Predictions MFC and the alarms emitted

from the lower level MFCs. The actions from this MFC concern: creation/ deletion of VPN switches and links and allocation of bandwidth to the VPN links. Elements of the functionality of this MFC resemble the network topology planning functions of public networks as well as the Route Design component introduced for the VPCM management system (see Section 5.5).

    - A *VPN Link Bandwidth Management* MFC, responsible for the management of the bandwidth of the BX-VPN links. This MFC, based on measures on actual VPN resource usage, received through the VPN Resource Monitoring MFC, aims at warning the VPN Design MFC of undesirable trends on VPN link usage, emitting lightly loaded or heavily loaded link utilisation alarms. These alarms are further consolidated with the VPN customer usage predictions in the VPN Design MFC, where the final actions for VPN link bandwidth modifications are taken.
    - A *VPN Routing* MFC, carrying out routing management. This MFC taking into account the BX-VPN configuration and the current load on the BX-VPN modifies appropriately the routes offered per VPN service class.
- A *VPN QoS Verification* MSC, responsible for asserting that the performance of the BX-VPN is within the contractual levels. It is further decomposed into:
    - A *VPN Connection Performance Monitoring* MFC, responsible for undertaking all necessary measurements activities required for asserting the performance of the BX-VPN through interaction with the underlying PNs, through the VPN Resource Configuration MFC.
    - A *VPN Performance Analysis* MFC, responsible for analysing the performance measures to verify that the performance of the BX-VPN is within acceptable levels. Should BX-VPN performance be found to be unacceptable, Quality of Service alarms are emitted.
    - A *VPN Customer Complaint Analysis* MFC, responsible for analysing the received customer complaints to assert whether they are justified.
- A *VPN Services* MSC, responsible for creating and maintaining the VPN services offered to the customers. It is further decomposed into the following MFCs:
    - A *VPN Service Model* MFC, a repository of the offered VPN services.
    - A *VPN Service Creation and Advertisement* MFC, responsible for creating new VPN services and advertising them to the customers.
- An *Accounting and Billing* MSC, responsible for carrying out all necessary functions for charging and billing the VPN customers.

6.4.4.2 System architecture

Figure 6.28 shows the allocation of the identified MFCs to OSFs and also places the OSFs into the TMN architectural layers.

6.4.5 Conclusions on the BX-VPN work

The second half of this chapter presented the concept of BX-VPNs - VPNs supporting switched traffic in a broadband ATM network environment, as a means for provisioning VPN services in the tVPN framework.

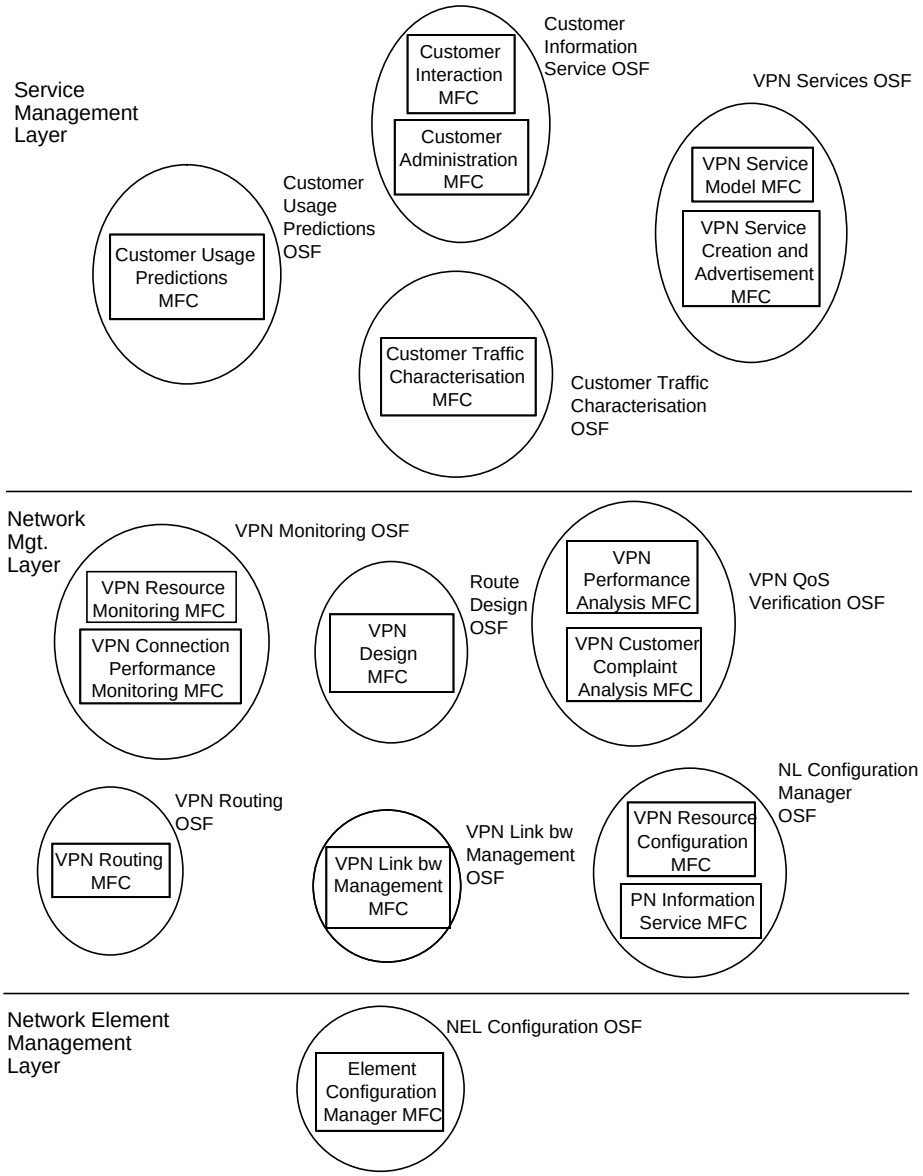


Figure 6.28 Functional architecture of the VASP TMN for BX-VPN

BX-VPNs are created, operated and managed through the co-operation of the Public Network Operators and the Value Added Service Providers. The management issues involved in provisioning and operating a BX-VPN were discussed and it was shown that the BX-VPN concept actually increases the opportunity for management, particularly in the areas of resource management and routing management. These two management areas are not considered in the provision of VPN services in today's context of iVPN. Improved manageability means more flexibility in provisioning at both the PNO

and VASP levels. There is an opportunity for decision making at each of these levels, but with different concerns. The VASP is concerned with the creation and operation of a logical network, while the PNO is concerned with operating and managing the physical counterpart.

Behind BX-VPN is the concept of multiplexing different customers' traffic over the same resources. This multiplexing is achieved under the control of the VASP, who shares out the rented resources between its customers. This allows the VASP to take advantage of statistical multiplexing at the call level and ensure higher levels of utilisation thereby increasing the revenue on its rented resources and thereby lowering the cost of VPNs. Because the BX-VPN is switched, the VASP can take further advantage of multiplexing through routing. Customers no longer have to be connected end-to-end, instead the VASP may reproduce the equivalents of access links and core transmission networks in the BX-VPN, where full advantage may be taken of the increased number of connections in the "core network" where sharing of resources may be fully exploited.

The advantages of the BX-VPN approach, in terms of enhanced flexibility, enhanced manageability, reductions in redundancy, increased efficiency in multiplexing, all have the tendency to reduce the costs for VPN services, and benefit all parties: the public networks, the VASPs and the customers.

The work to-date has defined the Management Service and the management system architecture for BX-VPN. Future work includes the validation of the proposed concepts and ideas through implementation of the proposed management system architecture; specifically it involves:

- system design and information modelling, based on the proposed architecture,
- derivation of specific algorithms for the management components at both the VASP and PNO levels.
- implementation of prototypes, experimentation and demonstration,
- a techno-economic study to further investigate and quantify the cost savings associated with the BX-VPN approach.

6.5 Security issues for VPN Management Services

The use of the TMN X-interface in the iVPN case study was described previously. A key issue behind the TMN X-interface is security of management interactions as these cross the boundaries of administrations or domains. General security requirements and services are described in [6.20] while [6.1] presents the TMN-specific security requirements. TMN security may be needed both intra-domain (Q) as well as inter-domain (X), depending on the environment in which a TMN operates. In the case of the ICM VPN, given the fact that the Internet was used as the TMN Data Communication Network (DCN), some security mechanisms were also applied within a TMN domain.

The TMN security requirements are the following:

- *authentication*, which is used to authenticate peer entities at association establishment, providing confidence that an entity is not attempting to masquerade as a legitimate one;

- *data integrity,* which counters active threats such as the modification or replay of information in transit;
- *confidentiality,* which guarantees that observed data by a third party in an information flow would be meaningless to the observer;
- *access control*, which provides different levels of access to management information (managed objects) by authenticated peer entities.

While access control is specific to OSI management and is fairly well advanced by ISO/ITU-T [6.21], authentication, integrity and confidentiality will be eventually catered for in a generic fashion, encompassing all upper layer protocols and applications [6.22]. The state of the relevant standards is still not stable enough and, as such, lightweight secret-key based mechanisms were designed and implemented in ICM. The detailed issues behind the ICM security mechanisms are described in Chapter 10, as they constitute an integral part of the OSIMIS ICM TMN platform.

Figure 6.29 describes the context in which security services were applied and illustrates from a very high level, the interactions between different OSs involved in a complex management service such as VPN. The arrows show the direction of manager to agent relationships between the various TMN physical blocks. The internal structure of the PNO TMNs is simplified for clarity. The use of TMN Q and X-interfaces is clearly depicted. Authenticated secure interactions can take place with appropriate access control restrictions across the TMN X-interface. The full range of security services, including integrity and confidentiality have been used across the various X interfaces. Within each TMN domain, interactions between TMN physical blocks use TMN Q-

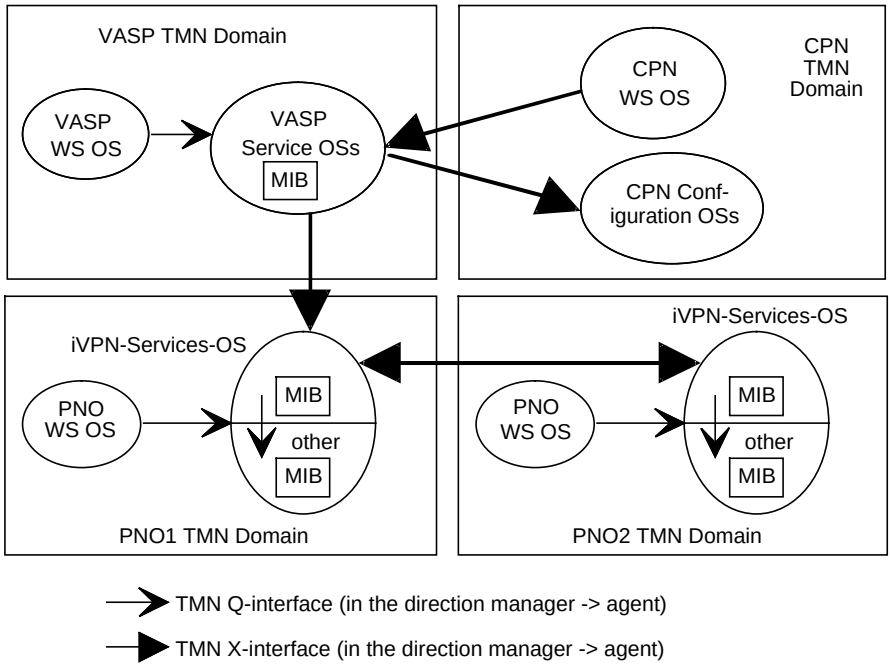


Figure 6.29 Security in a multi-domain VPN Management Service

interfaces. In the context of ICM, authentication has been chosen as the only security service within a domain. This prevents unauthorised associations but there is no need for integrity, confidentiality and access control: integrity and confidentiality are not an issue since management traffic stays intra-domain while access control requirements can be relaxed given the fact that trusted "well-behaved" applications are used.

Access control has been solely used for access to the Management Information Tree (MIT) of the PNO-IVPN-Services-OS. This has been crucial as the latter provides the X-VP (to VASPs) and X-PP (to other PNOs) interfaces. Different VASPs and neighbouring PNOs should "see" different parts of the MIT. The access control model implemented in ICM provides object-level restrictions (class or instance based) as opposed to restrictions on individual attributes, actions, event reports and their values. Object-level access control according to the model in [6.21] has been found very powerful and has served very well the needs of the ICM VPN.

Summarising, in order to ensure that no accidental, deliberate or malicious misuse in the interaction between OSs residing in different TMN domains will occur, the following steps must be taken:

- Design Specific

  The first line of defence is always in the design of the allowed functionality of the services provided by the OSs (MIBs and MOs) themselves. Especially important are any restrictions imposed in the design at the service layer.
- Generic

  Authentication, integrity, confidentiality and access control may be essentially "inherited" by every TMN X-interface, being available by the infrastructure or platform that is used to realise the relevant OSs.

Finally, it should be stated that through experimentation it has been demonstrated that the ICM lightweight security mechanisms do not impose a significant overhead to management interactions, justifying the use of some security mechanisms even on an intra-domain basis, to prevent mainly accidental damage.

6.6 Conclusions

The competitiveness of modern national and multinational corporations is increasingly affected by how well they utilise telecommunications services. In the future, as the use of more advanced applications and services grows, there will be a need to extend VPN services to integrate many different types of corporate telecommunications traffic including voice, data, video and multimedia. ATM networks are well suited as a network infrastructure for this. Advanced types of VPN Management Services are needed for ATM networks.

This chapter presented two diverse approaches to the problem of managing ATM VPNs. The first, iVPN, is an evolution of current leased-line services. Practical implementation experience was gained by the ICM project, and the service has been implemented and used on both real and simulated ATM networks. The project experimented in practice with solutions to the problems of security involved with services that span multiple management domains.

The second approach, tVPN, addresses the limitations of iVPN aiming to optimise the ATM network resources used, and to multiplex different VPN customers over these resources to improve VPN utilisation. The system design and architecture was presented but future work is needed in the areas of implementation and experimentation.

Valuable experience was gained in the area of network management security and in the implementation of ATM VPNs in general.

6.7 Acknowledgements

Many people contributed to the successful design, implementation and testing of the iVPN work in ICM. Sarah Cowell assisted in the detailed design of the VASP-CM OS. Babul Miah made the detailed design for the VASP-RD OS. Paul Thomas implemented both of those VASP TMN OSs. Pekka Jussila did the detailed design and much of the implementation of the VASP WS OS. Bruno Rossi is responsible for the detailed design and implementation of the IVPN-Services-OS. The previous work of the RACE PREPARE project in the area of IBC VPN was very useful as input for ICM's iVPN work.

6.8 References

[6.1] ITU-T Recommendation M.3010 - Principles for a telecommunications management network

[6.2] P. Heywood, The Dawn of the New VPN Era, Data Communications International, September 1995

[6.3] V. McCarthy, Are Virtual LANs still a Virtual Reality? Datamation, July 1995

[6.4] J. Duffy, Cisco plan just piece of the VLAN puzzle, Network World, June 26 1995

[6.5] Management of Virtual Private Network Services in the IBC Environment, IBC Common Functional Specification RACE H412, RACE Common Functional Specifications and Common Practice Recommendations, Document 19, CFS Addendum to Issue D, D1, August 1994

[6.6] VPN Service Management Evolution, IBC Common Functional Specification RACE M221, RACE Common Functional Specifications and Common Practice Recommendations, Document 19, CFS Addendum to Issue D, D1, August 1994

[6.7] Virtual Private Networks, Vol.II, IBC VPN Services, Editor: M. Louis, RACE 2004 Project PREPARE Deliverable 16, CEC Deliverable: R2004/MAR/WP6/DS/R/016/b1

[6.8] S. Fotedar, M. Gerla, P. Crocetti, L. Fratta, ATM Virtual Private Networks, Communications of the ACM, Feb. 1995/Vol.38, No.2

[6.9] P.Crocetti, S.Fotedar, et al., ATM Virtual Private Network Design Alternatives, Computer Communications, Vol. 18, No.1, Jan. 1995

[6.10] S. Fotedar, ATM Virtual Private Networks, PhD Thesis, Dept. of Computer Science, University of California, Los Angeles, USA, May 1995

[6.11] B-ISDN requirements for the support of Broadband Virtual Private Network, Work Item No: DRT/NA-53001 (Version 1, Draft 06.10.95), Final Version Due: 12/96.
[6.12] ATM User-Network Interface Specification, Version 4.1, ATM Forum, 1995
[6.13] LAN Emulation Over ATM, Draft Specification Revision 5, ATM Forum, AF-94-0035R5, Aug. 1994
[6.14] Public Network-Network Interface (PNNI), Draft Specification Revision 5, ATM Forum, AF-94-0471R5, 1995
[6.15] Broadband Inter Carrier Interface (BICI), Draft Specification, ATM Forum, 1995
[6.16] Customer Network Management (CNM) for ATM Public Network Service (M3 Specification), Revision 1.04, ATM Forum, 5 October 1994
[6.17] M4 Interface Requirements and Logical MIB: ATM Network Element View, Version 1.0 (Draft), ATM Forum, 1994
[6.18] M. Ahmed, K. Tesink, Definitions of Managed Objects for ATM Management using SMIv2, Internet IETF, RFC 1695, 1995
[6.19] G. Pavlou, T. Tin, K. McCarthy, OSIMIS4.1 Security and Access Control: Configuration and Utilisation, ICM Internal Document, Dept. of Computer Science, University College of London
[6.20] ITU-T Recommendation X.800, Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications, Security Architecture for Open Systems Interconnection for CCITT Applications, Geneva 1991
[6.21] ISO/IEC IS 10164-9, Information Technology - Open Systems Interconnection - Systems Management - Part 9: Objects and Attributes for Access Control, 1994 [X.741]
[6.22] ISO/IEC DIS 11586-1, Information Technology - Open Systems Interconnection - Generic Upper Layer Security - Part 1: Overview, Models and Notation, 1993 [X.830]
[6.23] Voice Enters Infobahn's Fast Lane: MFS Datanet Offers Customers User-friendly voice over ATM, Phillips Business Information's Broadband Networking News, September 5 1995
[6.24] K. Taylor, Channel Surfing Comes to ATM, Data Communications, September 21 1995
[6.25] P. Heywood, T.C. Eng, Big Pipes, Big Promises... and One Big Problem, Data Communications, September 21 1995
[6.26] ITU-T Recommendation M.3020, TMN Interface Specification Methodology, October 1992
[6.27] J. Reilly, P. Jussila, K. Salo, IVPN Case Study, RACE ICM Internal Design Document: /R2059/ICM/WP1/NRC/STL/VPNCS
[6.28] J. Reilly, P. Jussila, B. Miah, Intermediate Virtual Private Network (ATM Leased-line) System Design and Architecture, RACE ICM Document: / R2059/ICM/WP1/NOK/STL/9422110001
[6.29] RACE R2059 ICM Deliverable 14, "ICM Case Studies," R2059/QMW/BM1/ DS/P/014/b1, Babul Miah, editor, September 1994

[6.30] RACE R2059 ICM Deliverable 19, “Final TMN Architecture, Functions and Case Studies,” R2059/QMW/BM2/DS/P/019/b1, Babul Miah, editor, July 1995
[6.31] P. Baxendale, S. Cowell, VASP Configuration Manager Detailed Design, version 1.3, ICM Internal Document, University of Durham, 9 May 1995
[6.32] P.Jussila, P.Niska, J.Reilly, Intermediate Virtual Private Network (IVPN) Value-Added Service Provider (VASP) Workstation Operations System (WS-OS) Design, ICM Internal Document: ICM/WP6/NOK/STL/140395v1, 31 March 1995
[6.33] J.K. Ousterhout, Tcl and the Tk Toolkit, Addison-Wesley Publishers, 1994
[6.34] T. Tin, The Remote MIB Manager Support in OSIMIS, ICM Internal Document, February 1994
[6.35] Recommendation I.150, “B-ISDN Asynchronous Transfer Mode Functional Characteristics,” Study Group XVIII, Geneva, June 1992.
[6.36] Recommendation I.361, “B-ISDN ATM Layer Specification,” Study Group XVIII, Geneva, June 1992.
[6.37] Recommendation I.362, “B-ISDN ATM Adaptation Layer (AAL) Functional Description,” Study Group XVIII, Geneva, June 1992.
[6.38] Recommendation I.363, “B-ISDN ATM Adaptation Layer (AAL) Specification,” Study Group XVIII, Geneva, June 1992.
[6.39] T. Aoyama et. Al., “Introduction Strategy and Technology for ATM VP-Based Broadband Networks,” IEEE Journal on Selected Areas in Communications, Vol. 10, No. 9, December 1992.
[6.40] CFS D721-C, “Virtual Private Networks,” Issue C3, RACE, January 92.
[6.41] PREPARE Deliverable 6.4A, “Virtual Private Networks,” August 1994.
[6.42] PRISM D2, “Service and Network Management,” RACE R2041 PRISM, September 1992.
[6.43] PRISM D3, “VPN and UPT Service Management,” RACE R2041 PRISM, March 1993.
[6.44] ETSI SRC5, “Strategic Review Committee on Corporate Telecommunications Networks,” Final Report, ETSI, 02/08/93.
[6.45] ETSI Draft ETS, “Virtual Private Network (VPN) Service Description,” Version 0.2, ETSI-NA, 09/93.
[6.46] K.E. Mourelatou, D. Griffin, P. Georgatsos, G. Mykoniatis, “ATM VPN Services: Provisioning, Operational and Management Aspects,” IFIP TC6, 3rd Workshop on Performance Modelling and Evaluation of ATM Networks,” UK, July 1995.
[6.47] K. Mourelatou, G. Mykoniatis, V. Demestiha, “Target VPN: Case Study Description,” ICM Internal Report, /icm/wp1/alpha/144, V.2, Jan.1995