ATM VPN services: Provisioning, operational and management aspects

Konstantina Mourelatou[1], David Griffin[2], Panos Georgatsos[3], George Mykoniatis[4]

Abstract

Virtual Private Networks (VPNs) have been recognised as a vital means for providing value added services over future ATM-based IBC networks. The multi-operator, multi-provider nature of the deregulated telecommunications market imposes requirements for one-stop shopping, complaining and accounting. The VPN concept aims at meeting these requirements and, moreover, advancing the current telecommunication environment by offering value-added services at a relative low cost and at an enhanced quality compared to the basic services offered by the network operators. In general VPN services are considered as an application of Intelligent Networks (IN).

In this paper we introduce the concept of the Broadband Switched VPN (BX-VPN) as a means for provisioning VPNs on ATM based networks. We present the issues involved with BX-VPN provisioning and operation from the viewpoints of the network operators and the value added service providers (VASPs), with particular emphasis on the management issues. We show how the BX-VPN concept increases the manageability of VPNs, therefore increasing the flexibility in provisioning, reducing redundancy and inefficiency inherent in static configurations. We define the management services necessary for resource management and routing management at both the network operator and the VASP levels.

1. Introduction

The VPN concept permits private networks to be built by using public network resources. Communication over a VPN is accomplished in terms of “closed-user groups”. That is, the members composing a closed user group can communicate with each other by accessing the VPN and using the provided VPN services.

According to [9] VPNs have been evolved through the following three phases:

- The short-term VPN (s-VPN) phase concerning the current status of installations for VPNs and the planning for the next phase. Most of the VPN services available today are based on conventional Public Switched Telephone Network (PSTN) or on Public Switched Packet Data Networks (PSPDN),
- The intermediate VPN (i-VPN) phase covering the evolution of VPN Management from the current situation to the target Integrated Broadband Communications (IBC) environment,
- The target VPN (t-VPN). It will allow an efficient and flexible use of the provisioned resources so that can be easily adjusted to the changing traffic requirements of the customers in the IBC environment.

I-VPN is implemented by interconnecting Customer Premises Network (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 lines 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

[1] Alpha Systems, Athens, Greece, Tel.: +30.1.4826014-16, Email: kmour@alpha.ath.forthnet.gr

[2] FORTH-ICS, Heraklion, Greece, Tel: +30.81.391722, Email: david@ics.forth.gr

[3] Alpha Systems, Athens, Greece, Tel: +30.1.4826014-16, Email: panos@alpha.ath.forthnet.gr

[4] NTUA, Athens, Greece, Tel.: +30.1.7721479, Email: mykoniat@ektor.ntua.gr

ordinary network traffic. It is even possible for the call blocking probability in the underlying network to be higher than necessary due to a lack of capacity while the resources dedicated to the leased line customers are lightly utilised. The cost associated with the provision of Private Networks is high due to the dedication of resources to the end-to-end connections.

T-VPN 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 t-VPN will allow value-added services to be provided at a relative low cost compared to those in the s-VPN and i-VPN environments.

Within the t-VPN framework, the paper concentrates on the concepts as well as the operational and management issues involved with VPN service provisioning in a multi-operator, multi-provider environment. The paper elaborates on optimum and efficient ways for VPN service provisioning, operation and maintenance in a broadband ATM environment.

Utilising the advantages of the ATM technology, the paper proposes the notion of the "Broadband Switched VPN" (BX-VPN) as an efficient means for realising the VPN concept. 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.

The paper focuses on the definition of the fundamental BX-VPN concepts and ideas. The operational and maintenance aspects are discussed and the functionality required for managing the BX-VPN is identified and described in terms of management service components. 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.

Section 2 introduces the BX-VPN concept applied in the broadband environment. The management functionality required for operating VPNs is described in section 3, while section 4 concentrates in more detail on the specific management issues of Resource Management and Routing Management in BX-VPNs. Finally, section 5 presents our conclusions and identifies the scope of future work in this area.

2. The BX-VPN concept

Asynchronous Transfer Mode (ATM) has been adopted by the ITU as a basis for B-ISDN [1-4] which is designed to support and accommodate a wide variety of different services. Multiplexing and switching are the fundamental techniques employed by ATM for implementing an integrated access and transport network.

Multiplexing is a powerful technique which enables the efficient utilisation of the network resources by statistically multiplexing the network traffic. User information is organised into fixed-length packets, called "cells", prefixed with a header containing a label that uniquely identifies the virtual path (VP) and virtual channel (VC) over which user information is routed. VPs and VCs are the basic virtual connections standardised by the ITU with respect to the ATM network. In particular Virtual Path Connections (VPC) are semi-permanently allocated (by management actions) between two switching points and, as such, they do not require end-user signalling. VPCs provide end-to-end broadband ATM connectivity between the VPC end-points. Virtual Channel Connections (VCCs) are routed over previously established VPCs, therefore VPCs can be considered as aggregates of VCCs. VCCs are allocated on the demand of the users and thus require broadband end-user signalling.

Taking into account the advantages of the multiplexing technique [5], we try to exploit the above mentioned features of ATM technology in the provision of Virtual Private Networks (VPN). In this direction the notion of BX-VPN as an efficient means for realising the VPN concept is proposed. 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 [6-8] but a network in its own right. The primary objective of the BX-VPN concept is to permit the multiplexing of different customers to optimise VPN utilisation.

Current VPNs are implemented as leased line based private data networks. The leased lines providing end-to-end connectivity between customer sites are implemented by either dedicated links or semi-permanent VPCs rented from the public network. This approach succeeds in providing connectivity but is likely to

result in inefficient utilisation of the public network resources. The leased lines are used solely by one customer and it is very likely that the rented resources may be lightly utilised by the customer while the underlying network has insufficient resources to accommodate the ordinary public network calls.

The BX-VPN is built not by investing in new physical resources but by renting the appropriate resources from the underlying PNOs. An important characteristic of the BX-VPN concept is the optimisation of the rented resources. 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 better possible utilisation of the rented resources.

The provisioning and operation of BX-VPN requires the employment of the basic control and management functionality of the underlying Public Network Operator(s)' (PNOs) network(s), and additionally requires management functionality to specifically manage the BX-VPN issues.

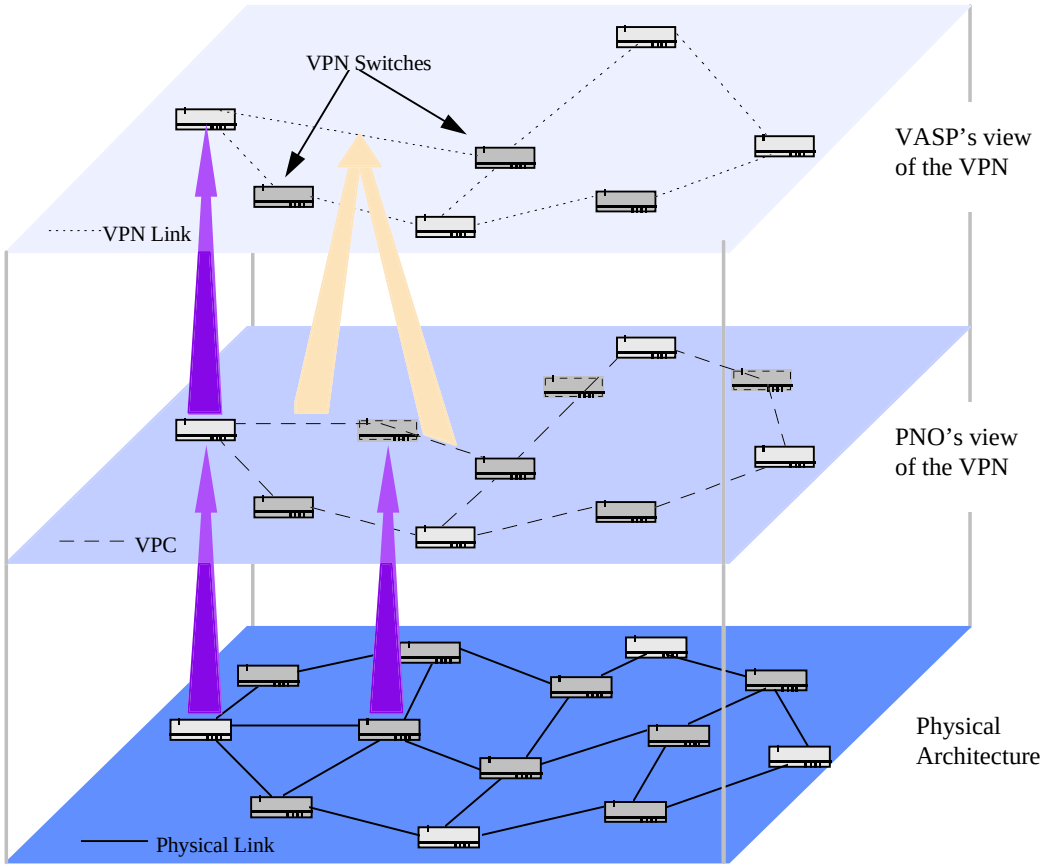

Figure 1. BX-VPN concept

Since the BX-VPN is a "virtual" network, it consists of logical resources. The following resources are rented from the Public Network(s) (Figure 1):

- ✓ VPN links which are defined to be the transmission means of the BX-VPN over which the VPN user traffic is multiplexed. The transmission capability is rented in terms of the bandwidth and the required performance of the links. In the Public Network, each VPN link may be implemented by one or more VPCs (Figure 1)
- ✓ VPN switches providing the switching capability of the BX-VPN necessary for routing and multiplexing the VPN customers traffic. The rented switching capability is in terms of routing table entries and subsequently VP/VC tables which reside in the public network. The engagement of certain parts of the routing tables enables the routing of the VPN calls.

The transmission capability enables the transport of customers information while the switching capability supports routing through the BX-VPN and the simultaneous accommodation of many customers by multiplexing their traffic over the VPN links.

The BX-VPN provider or Value Added Service Provider (VASP) rents resources from one or more Public Networks in order to build his own network. The rented network resources are used by the individual BX-VPN customers, on demand. These resources are dimensioned in order to accommodate the estimated traffic of the BX-VPN customers. If new customers are added to the BX-VPN customer list, the VASP has to estimate the additional resources required to support the requirements of the new customers. This is illustrated in figures 2 and 3.

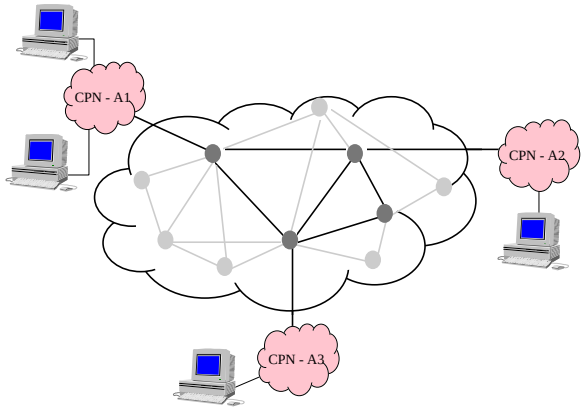

Figure 2.

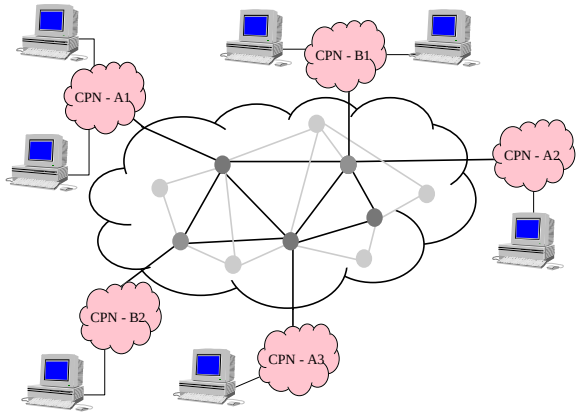

Figure 3.

In figures 2 and 3, 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 2, customer A1 owns three sites to be interconnected by using the VPN resources. Traffic from site A1 to site A2 may be multiplexed with traffic from site A2 to site A3. When a new customer is added (Figure 3), the VASP rents additional resources; i.e. VPN switches and 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.

In leased line based networks, customers are provided with (semi-)permanent end-to-end connections interconnecting their sites. In this scenario, the customer is responsible for routing its traffic over the correct leased lines in order to arrive at the required destination, by configuring routing tables within CPN. In the BX-VPN concept, the existing control functionality of the public network is used, that is, the connectivity of the individual customer sites is achieved through the control and signalling mechanisms of the public network.

It is worth examining the call set up procedure of the VPN connections.

In figure 4, the system configuration is depicted. The Customer Premises Networks (CPN) are connected to the core network via VPN Links. Where necessary, an interworking unit exists between the access node of the network and the CPN.

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 the ATM consistent call request. The request is 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 the request is a VPN call request. 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 IN facilities of the public network.

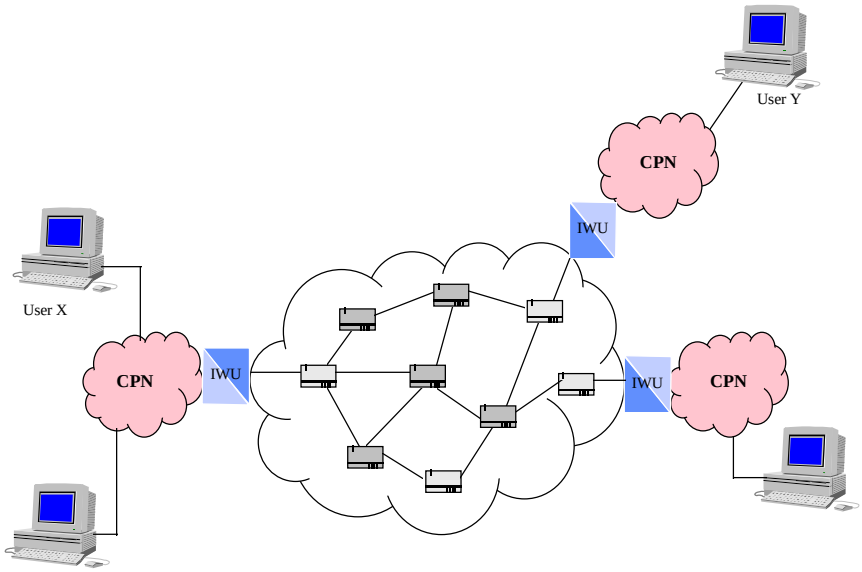

Figure 4. System configuration

3. VPN Management issues

Management functionality needs to exist at both BX-VPN and PN levels for supporting the BX-VPN concept. In the PN domain enhancements in existing management functionality are required to support the VPN operation. On the other hand, the management functionality at the BX-VPN level covers the crucial policies and decision making mechanisms that will guarantee the successful provisioning, maintenance and operation of the BX-VPN as a whole.

The following table 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 BX-VPN level**	**At the PN level**
VPN Configuration	Concerned with the building of the VPN by determining the type and amount of resources needed to be rented from the PN(s). VPN configuration is based on the VPN customers traffic characterisation and topological aspects. It involves routing in high level and resource management (see below). The configuration procedure is repeated during the VPN lifetime in order to accommodate varying customer requirements .	Concerned with the provision of the requested VPN resources. The PN provider must guarantee that the resources requested by the VASP are available to accommodate the VPN traffic. Dynamic VPN re-configuration necessitates the employment of efficient resource policies in the PN.
VPN Customer Traffic Characterisation	This is the process for estimating the expected traffic of VPN customers in order to determine the required resources needed to be rented from the PN	
VPN Resource Management	Concerned with the management of the logical resources constituting the VPN. Efficient resource management guarantees better utilisation of the VPN resources. 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 VPN.
Routing	Determines how the traffic of the individual VPN customers will be routed over the VPN links. The 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 VPN level. These decisions are passed to the PN to update the routing tables.

Monitoring	Enables the VPN provider to monitor the usage of the 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 VPN load in order to exercise the appropriate resource management policy. The PNO also provides the required measurements according to the VPN monitoring requirements.
QoS Monitoring	Enables the VASP to assess the performance of the VPN and the quality of the offered VPN services. In the case of QoS degradation the VASP reconfigures the VPN or makes complaints to the PNO if the PN performance is low.	PNO needs to assess that the performance of the rented resources rmeet the performance targets negotiated with the VASP.
Security Aspects	Concerned with the employment of proper authorisation and access control mechanisms to protect the VPN user against unauthorised use.	Concerned with the protection of the VPN traffic so that ordinary PN traffic and VPN traffic will not interfere.
Accounting	Used to calculate the charges for each VPN customer. It is based on information about the utilisation of the 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 VPN level.
Customer Administration	Concerned with the maintenance of information pertinent to the VPN customers and services. The 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 VPN performance monitoring facilitates the identification of potential problem occurred to either the VPN of the underlying network and has caused the degradation of the offered QoS.	Analysis 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 exercises appropriate actions to guarantee the negotiated services with the VASP.
Service Creation and Provision	Design and provision of new services to accommodate the specific needs of the VPN customers. The VASP gathers information about the needs and complaints of the customers. Based on this information, either the VPN is re-configured or the VASP negotiates with the PN for the creation of new services.	Creation of new services in order to meet the 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.

In the following sections we will 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 the efficiency gains benefiting the customer and both the VASP and the PNO organisations.

4. Resource Management and Routing principles

4.1. Resource Management in BX-VPN

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).

As stated in section 2, the BX-VPN consists of “VPN resources”, i.e. “VPN links” and “VPN switches”. The VPN links and VPN switches represent the transmission and switching capability respectively, rented from the underlying PN(s). The concept of the VPN resources permits the VASP to have the notion of a “network”; i.e. the BX-VPN network. The VPN resources are mapped to the PN(s) resources. However, the VASP has an abstract view of the underlying resources, only being aware of those aspects necessary to exercise its management policy. For instance, the VASP knows that the transmission capability it has rented between two VPN switches has a capacity of 50 Mbits/s but it does not care how this transmission capability is physically realised in the underlying network (see also Resource Management in PN level).

The main target of Resource Management in VPN domain is the estimation of the resources to be rented from the PN(s) in order to meet the demands of the VPN customers. Based on information retrieved from its customers and through the procedure of 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 VPN links and VPN switches.

When new customers are to be accommodated by the BX-VPN or the requirements of the existing customers change, the VASP exercises appropriate resource management actions in order to adapt the BX-VPN capabilities to the new requirements. In this process the current topology of the BX-VPN is taken into account. These actions may results in the re-configuration of the BX-VPN topology in the following ways:

- ✓ the amount of bandwidth corresponding to the VPN links is changed (increased or decreased)
- ✓ new VPN resources are added
- ✓ existing VPN resources are deleted

Figures 2 and 3 provide an example. Initially, customer A, with three sites, is accommodated by the BX-VPN (Figure 2). As depicted in the figure, the BX-VPN is constituted of a number of VPN links and switches. When customer B is added to the VPN customers list, the BX-VPN configuration is changed to meet the requirements (Figure 3). The figure shows that new resources were rented, furthermore the capacity of the existing resources supporting customer A may have been increased.

The resource management decisions taken at the VPN level are passed to the PN level. After the decisions have been taken, the VASP has to negotiate with the PNO the reservation of the required PN resources. The PNO in its turn will provide the negotiated resources to the VASP.

It should be noted that the VASP does not have direct access to the VPN resources. VASP decisions are passed as requests to the PNO who is responsible to realise them if it is possible. In the following sections, the way the VASP decisions are accomplished in the PN level will be studied.

4.2. Routing in BX-VPN

Routing in BX-VPN is concerned with the efficient delivery of the VPN users information over the VPN resources. It should be noted that in connection orientated networks, such as ATM, routing decisions are made at call establishment time, by the control plane. The management of routing is not a control plane activity, routing management is concerned with ensuring that the correct information is available in the network switches to enable suitable routing decisions to be made. Routing management is not an on-line activity to be performed at call establishment.

As it has been already stated, the prime objective of the BX-VPN idea is to multiplex the VPN customers traffic on the resources rented by the PN(s). This is the point where the BX-VPN idea is mainly differentiated from the typical VPN concept where each customer is assigned an amount of bandwidth in terms of personal links or VPCs and no multiplexing is achieved.

To achieve multiplexing of the customers traffic, the VPN provider rents from the underlying PN(s) switching capability besides to the transmission capability. The rented switching capability permits VASP multiplexing the VPN customers traffic over the VPN resources according to the plan set by the VASP. The VASP perceives the rented switching capability as the VPN switches constituting the BX-VPN network (see also section 2). The VPN switches “present” the principal characteristics of the physical switches residing in the PN(s). That is, a VPN switch maintains a “routing table” to influence the procedure of setting up the new VPN call requests. It should be noted that the VPN switches are not physical components but they logically “represent” the potion of the PN(s) switches dedicated to the provision of the BX-VPN network.

As the VASP has the notion of a “self-contained” network it must be involved with corresponding activities to those performed by operators of ordinary physical networks. Regarding the routing of the VPN customers traffic over the VPN links, the VASP exercises his own routing policy. Based on the topology of the BX-VPN network (i.e. VPN links) and the services classes offered by it (i.e. the traffic characteristics and the performance requirements of each service class), the VASP determines his routing plan. This involves determining the routing table entries of the VPN switches; i.e., for a particular destination which VPN links are going to accommodate the various service classes.

The VASP routing plan may change dynamically in order to meet the varying traffic conditions of the BX-VPN. In particular, the procedure of changing the VPN routing plan may be triggered by:

- ✓ the modification of the VPN traffic load
- ✓ the modification of the VPN customers requirements; e.g. new customers are added, new service classes are created.
- ✓ the degradation of the VPN performance.

The VASP rents resources from the underlying PN(s) but he can not have direct access to these resources. That is, all the decisions taken by the VASP are passed to the PN, and the PNO takes them into account when he exercises his policies. Hence, when the PNO exercises his routing policy, he considers the decisions of the VASP and the routing tables that have been partially hired to the VPN are updated properly. This aspect is further discussed in the following section.

4.3. Resource Management and Routing in PN

In this section, the PN management issues pertinent to BX-VPN concept are examined.

The PN employs appropriate management functionality to smooth the operation of the network and to increase its efficiency. The provision of BX-VPN over the PN, implies further management requirements in the PN. Actually, it is the PN who provides the BX-VPN under the negotiations taken place between the PN operator and the VASP. In this respect, the management functionality employed by the PN must be enhanced to enable the coexistence of PN and BX-VPN. Section 2 gave a brief reference to the BX-VPN related management issues at the PN level, this section will examine in detail how resource management and routing policies are influence by the existence of BX-VPN.

The VASP rents transmission capability from the PN in terms of VPN links. The PNO in his turn, reserves the requested capability in terms of VPCs. The key objective is that the PNO has to exercise flexible resource management and routing policies so that the PN and BX-VPN coexist in harmony and the operation of one does not adversely affect the operation of the other.

As illustrated in figure 5, the VPN links are mapped to a network of VPCs in the underlying PN(s). This means that there is not one-to-one mapping between the VPN links of the BX-VPN and the VPCs of the PN; i.e. one VPN links corresponds to one. On the contrary, a network of VPCs can be defined to correspond to a simple VPN link. The capacity (Minimum cut) should equal the capacity of the VPN link negotiated with the VASP.

For instance, the VPN link depicted in figure 5 corresponds to the VPCs[5]:

- ✓ {ab1, bc1, cg1}, {ad1, de1, ef1, fg1}, {ad2, df1, fg2} and {ab2, bc2, ce1, ef2, fg3}

If the negotiated bandwidth of the VPN link is 50 Mbits/s, then the following equation must be valid:

$$\Sigma\, BW_{VPCi} = 50 \text{ for } i = 1 \text{ to } n \qquad \text{(Eq. 1)}$$

where VPC_i is each sequence of VPCs between the end nodes of the VPN link.

[5] Note that:

- ✓ the network switches are marked by capital letters; (i.e. A, B, …),
- ✓ the VPCs between two switches are denoted by the sequence of constituting VP links
- ✓ the VP Link existing between two switches is denoted by the switches letters in small, and the sequential number of VP on the specific link (i.e. the VP link between switches A and B is denoted as VPLink ab1)

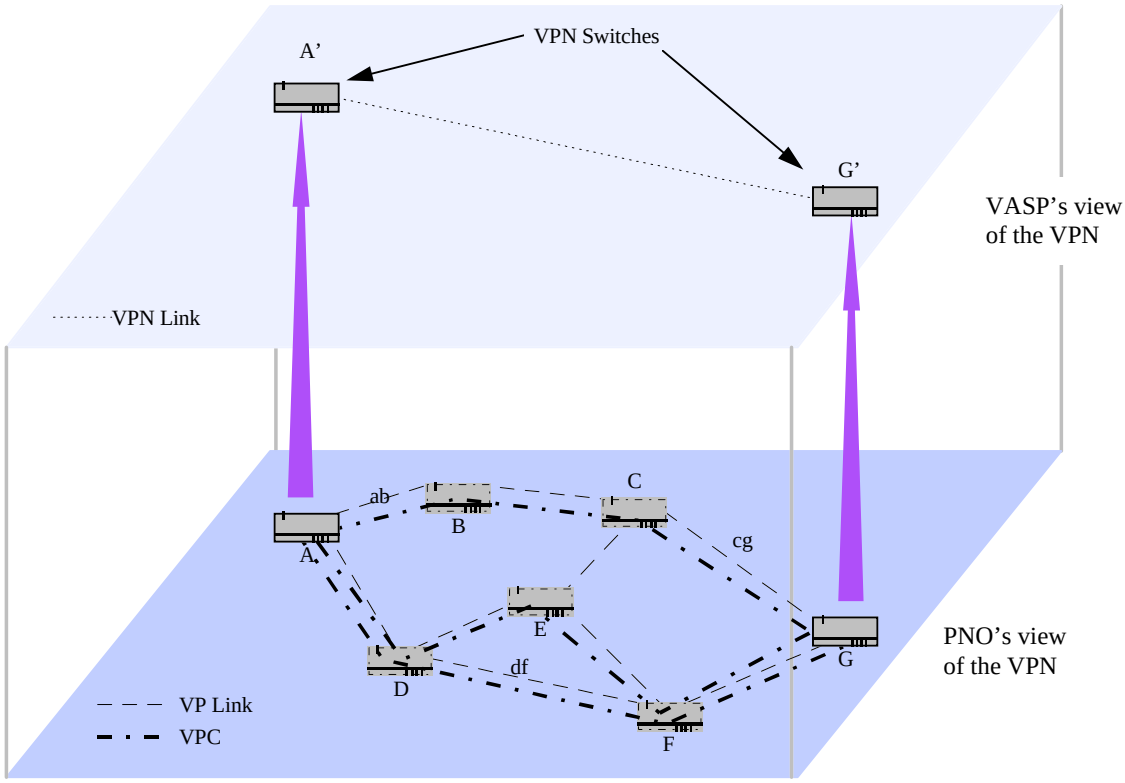

Figure 5.

This scheme allows the PNO to be very flexible as far as the reservation of network resources is concerned. That is, the PNO may change the VPC network corresponding to a certain VPN link while this VPN link is active if the traffic conditions of the network demand. In the simplest case, the bandwidth corresponding to the individual VPCs may be changed (increased or decreased)[6] while in the worst case new VPCs may be added or those not carrying traffic may be deleted.

When the VASP requests additional transmission capability, the PNO has to reserve the requested amount of bandwidth. Either the bandwidth allocated to existing VPCs will be increased or appropriate new VPCs are created and assigned the requested amount of bandwidth. The VASP does not see how the PNO has implemented the VPN Link in the PN, it has only an abstract view of the total capacity of the VPN Link and its end points. Whenever, the VASP wants to request any modification to the VPN links, he refers to the PNO by using the VPN link name. The PNO keeps the mapping between the VPN link and the associated VPC network and according to the VASP requests, he proceeds to the appropriate modifications.

As far as the VPN routing plan is concerned, the VASP passes his routing plan to the PNO. The latter will take into account this plan while setting up the routing tables of the switches of the PN. The VASP provides PNO with an association between VPN links and VPN supported Class of Services. The PNO will use this information so that the VPN customers traffic will be properly routed over the VPCs reserved for the VPN needs. The PNO routing plan has to guarantee that the performance requirements of the VPN services will be preserved while the PN ordinary traffic will not be affected by the VPN traffic. On the other hand, the PN routing plan focuses on the maximisation of the PN resources.

[6] Please note that all the VPCs of a VPC sequence between the end nodes of a VPN link, are assigned the same amount of bandwidth.

5. Summary, Conclusions and Future Work

The paper has presented the concept of BX-VPN, i.e. VPNs supporting switched traffic in a broadband ATM environment. VPNs are provisioned through the co-operation of the public network operators and the value added service providers. We have discussed the management issues involved in provisioning and operating a BX-VPN and 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 today. This gain in 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 a 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. At the PNO level, there is an increased flexibility in configuring VASP requests to provide VPN services, this enables flexible routing policies to be adopted by the PNO domain.

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.

Our work to date has defined the Management Services involved with resource and routing management. Future work includes:

- definition of a management architecture as a framework for the system design.
- derivation of specific algorithms for the management components at both the VASP and PNO levels.
- implementation of prototypes, experimentation and demonstration.
- a techo-economic study to further investigate and quantify the cost savings associated with the BX-VPN approach.

Acknowledgements

The work described in this paper has been carried out by the authors in the course of the Integrated Communications Management (ICM) project (R2059), in the framework of the RACE II programme. The RACE II programme is partially funded by the Commission of the European Union.

References

[1] Recommendation I.150, "B-ISDN Asynchronous Transfer Mode Functional Characteristics", Study Group XVIII, Geneva, June 1992.

[2] Recommendation I.361, "B-ISDN ATM Layer Specification", Study Group XVIII, Geneva, June 1992.

[3] Recommendation I.362, "B-ISDN ATM Adaptation Layer (AAL) Functional Description", Study Group XVIII, Geneva, June 1992.

[4] Recommendation I.363, "B-ISDN ATM Adaptation Layer (AAL) Specification", Study Group XVIII, Geneva, June 1992.

[5] 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] CFS D721-C, “Virtual Private Networks”, Issue C3, RACE, January 92.

[7] RACE CFS M221, “VPN Management Evolution”

[8] PREPARE Deliverable 6.4A, “Virtual Private Networks”, August 1994.

[9] PRISM D2, “Service and Network Management”, RACE R2041 PRISM, September 1992.

[10] PRISM D3, “VPN and UPT Service Management”, RACE R2041 PRISM, March 1993.