On Managing Virtual Private Networks

1.0 Introduction

Virtual Private Network (VPN) is one of the major trends in the integrated broadband communications environment. There is a myriad of definitions of a VPN used in the networking community to describe a broad set of problems and solutions. In [1], Ferguson et al. define a VPN as a communications environment in which access is controlled to permit peer connections only within a defined community of interest. A VPN is constructed through some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a non-exclusive basis".

A VPN service is primarily useful for organizations that wish to use public networks to connect their various LAN's for private purposes. This is typically the case of large corporations that need to connect a set of geographically separated offices while preserving the private character of their communications. Therefore, the VPN concept has to respond to two conflicting requirements:

1. Allow for a cost-effective communications infrastructure through resource sharing. Compared to the dedicated leased circuit approach, organizations reduce the cost of connecting geographically dispersed sites by establishing VPNs across a shared public network.
2. Allow for communications privacy. Although several organizations share a common communications infrastructure (public backbone network), they want their communications services to be within one closed environment isolated from all other environments that share the common underlying communication infrastructure.

VPN services are commonly offered by a value added service provider to a number of service subscribers referred to as the VPN customers. The VPN provider sets up the VPN connectivity for a customer using the services of multiple Public Network Operators (PNOs). The VPN provider may be a separate organization or it may be part of one of the PNOs. The advantage of the VPN provider as an intermediate level between the customer and the involved PNO(s) is that of one-stop shopping which provides a single interface to the customer for accepting requests, queries and complaints, and also to provide a single bill to the customer.

The initial target of the VPN concept was to successfully replace the leased lines-based private data networks and PBX interconnection. The evolution of VPN is motivated by the reduction of the high cost due to the dedication of equipment. Most of existing VPN services are based on conventional Public Switched Telephone Networks (PSTN) or on Public Switched Packet data Networks (PSPDN). Second generation VPNs use technologies such as ATM cross connect, and support semi-permanent pipes such as ATM end-to-end Virtual Path Connections (VPCs).

In such VPNs, management services include configuration and static bandwidth management, in which bandwidth is not altered after VPC set up. Similar VPNs are implemented using Frame Relay (FR) networks. New generation VPNs are evolving to support full open network provisioning. They use B-ISDN based on switched ATM and IP routing capabilities as well as encryption techniques. There is a powerful logic to the shift towards Internet VPNs. *Economic of communications* is the most predominant factor: a corporation's expenses are only the cost of the short loop between its offices and the Point Of Presence (POP) of the local ISP. *Flexibility* in setting up a VPN using the public Internet is another factor. This can be as simple as adding a gateway and the necessary software for establishing a secure VPN connection. The Internet provides *worldwide connectivity*. Indeed, a VPN node can be added wherever there is an Internet POP, which are available worldwide. Last but not the least worldwide availability of cheap Internet access increases *mobile workforce productivity* through remote access. In turn Internet VPN face significant challenges such as security, quality of service and reliability. These issues are currently subject to large research and development efforts.

This article starts with a comprehensive analysis of existing VPN models. Then, it describes current VPN operation and management practices. Finally, it discusses future trends in VPN management.

by *Raouf Boutaba*
Computer Science Dept., University of Waterloo, ON

Abstract

Network operators and value added service provider offer VPN services to corporations that wish to tie together their geographically dispersed offices and to provide their mobile workforce with access to the company resources. Currently, the management of the VPN resources is mainly ensured by the provider of the bearer telecommunication services, while the VPN customers have no direct control over these resources. The increasing importance of the broadband communication infrastructure in corporate operations and transactions is stressing the requirement for a customizable design, operation and management of VPN services. This article discusses the trend towards customer management of VPNs.

Sommaire

Le réseau privé virtuel (RPV) est un service offert par les opérateurs de réseaux et les fournisseurs de services à valeur ajoutée. Il est utilisé par les corporations qui ont besoin de relier ensemble leurs bureaux géographiquement répartis et pour fournir à leurs employés mobiles un accès à distance aux ressources. Actuellement, la gestion des ressources du RPV est assurée par l'opérateur du service de télécommunication de base, alors que les clients du service RPV n'ont aucun contrôle directe sur ces ressources. L'importance grandissante de l'infrastructure réseau pour les activités et les transactions des corporations suscite de plus en plus le besoin d'une conception et une gestion personalisées du service RPV. Cet article analyse la tendance vers une gestion client des RPVs.

2.0 VPN Models

The models to construct VPNs can be categorized into two main models: "peer" and "overlay" VPN models [1]. In the peer VPN model, the network layer forwarding path computation is done on a hop-by-hop basis. Traditional routed networks are examples of peer models, where each router in the network path is a peer with its next hop adjacencies. In the overlay VPN model, the intermediate link layer network is used as a "cut-through" to another edge node on the other side of a large cloud. Examples of overlay VPN models are ATM, Frame Relay, and tunneling implementations. Orthogonal to the previous models is the security requirement in a VPN, including confidentiality, data integrity, authentication, and access control. Encryption is what makes VPNs private. It is a key component used to respond to most of these requirements.

In general, the VPN architecture depends on the layer of the protocol suite that is used to implement the VPN service. Also, the complexity of implementation and maintenance of the VPN depend on the type of VPN as well as on scalability and security requirements. The remaining of this section overviews the different types of VPNs and presents their respective features.

2.1 Overlay VPN Models

Overlay VPN models are more naturally implemented at the link-layer of the protocol stack. A link-layer VPN attempts to provide a functionality similar to conventional private data networks while achieving economies of scale and operation through multiplexing (using virtual circuits instead of dedicated transmission paths). In this scenario, VPNs share a common switched public network infrastructure for connectivity (i.e., the same switching elements within the public network), while the VPNs have no visibility of one another. Usually, such infrastructure consists of Frame Relay or ATM networks. The major advantage of utilizing virtual circuits in the public switched network is their flexibility

and cost-effectiveness. However, the disadvantage is the scaling limitation and the complexity of configuration management.

Multi Protocol Over ATM [2] (*MPOA*) is an "overlay" model of constructing VPNs similar to the "cut-through" mechanisms where the switched ATM network enables egress nodes to be one "Layer-3" hop away from one another, using dynamically controlled edge-to-edge ATM Virtual Connections (VC's). However, MPOA approach assumes a homogeneous ATM environment, and relies on external address resolution servers to support the Address Resolution Protocol (ARP).

Tunneling is one increasingly popular method of constructing VPNs by sending specific portions of network traffic across tunnels. It is considered as an overlay model. The most common mechanisms are GRE (Generic Routing Encapsulation) [3] tunneling between a source and destination router, router-to-router or host-to-host tunneling protocols such as L2TP [4] (Layer 2 Tunneling Protocol) and PPTP [5] (Point-to-Point Tunneling Protocol), and DVMRP [6] (Distance Vector Multicast Routing Protocol) tunnels.

2.2 Peer VPN Models

Controlled Route Leaking is one implementation of the peer VPN model. It consists of controlling route propagation to the point that only certain client networks receive routes for other networks which are within their own community of interest. The routes associated with a set of clients are filtered such that they are not announced to any other set of connected clients, and that all other non-VPN routes are not announced to the clients of the VPN. The controlled route leaking technique is considered to be prone to administrative errors, and admit an undue level of insecurity and network inflexibility. In addition, this technique does not possess the scaling properties desirable to allow the number of VPNs to grow beyond the bounds of a few hundreds, using today's routing technologies. An alternative technique uses *BGP community attribute* [7, 8] to control route propagation. This method is less prone to human misconfiguration and allows for a better scalability. It allows a VPN provider to "tag" BGP NLRI's (Network Layer Reachability Information) with a community attribute, such that configuration control allows route information to be propagated in accordance with a community profile. The BGP communities technique allows flexible construction of network layer VPNs by preventing VPN service subscribers to detect the fact that there are other subscribers to the service. However, it does not guarantee data privacy in the core of the service provider's network (i.e., the portion of the network where traffic from multiple communities of interest share the infrastructure).

Multi-Protocol Label Switching [9] (*MPLS*) is a hybrid architecture which combines the use of network layer routing structures and per-packet switching, and the use of link-layer circuits and per-flow switching. In the case of IP over ATM, each ATM bearer link becomes visible as an IP link, and the ATM switches are augmented with IP routing functionality. The latter is used to select a transit path across the network, and those transit paths are marked with a sequence of locally defined forwarding path indicators or labels. A generic MPLS architecture for the support of VPN structures is that of a label switched common host network and a collection of VPN environments that use label-defined virtual circuits on an edge-to-edge basis across the MPLS domain. The label applied to a packet on ingress to the MPLS environment effectively determines the selection of the egress router, as the sequence of label switches defines an edge-to-edge virtual path. MPLS itself and MPLS-based VPNs are still under active research and present great potential particularly for supporting VPNs with Quality-of-Service (QoS) over the Internet.

2.3 Encryption-based VPNs

Encryption technologies are effective in providing the virtualization required for VPN connectivity, and can be deployed at almost any layer of the protocol stack. The implementation of VPNs at the transport and application layers is mostly based on the use of encryption services. Application layer encryption, for example, is the most pervasive method of constructing VPNs in multiprotocol networks. Transport layer encryption aims at providing privacy and data integrity between two communicating applications. For this purpose the Transport Layer Security Protocol or TLS [10] is being defined within the Internet Engineering Task Force (IETF). Network layer encryption is implemented according to two modes: the end-to-end mode where encryption is performed between participating hosts; and the tunnel mode where encryption is performed between intermediate routers. The first mode allows for a higher level of security and implements VPN granularity at the level of the individual end system. The second mode is less secure in that it leaves the tunnel ingress and egress points vulnerable, since these points are logically part of the host network as well as being part of the unencrypted VPN network. In the Internet, the network layer encryption standard being defined within the IETF is IPSec (IP Security) [11]. Encryption at the link layer is supported by special encryption hardware generally vendor specific and hence poses interoperability problems in multi-vendor environments. It is worth noting that as one moves down through the protocol stack, the implementation of VPN tunnels become easier, while securing them becomes more challenging.

3.0 VPN Operation and Management

3.1 Current Practice

The VPN is mainly viewed from two distinct viewpoints: the VPN customer and the VPN provider. The VPN customer represents the closed user group of the VPN. It is responsible for negotiating the VPN services with the VPN provider. The negotiation includes the type of services required, the offered quality and the price. If the VPN fails to provide the contracted quality of service, the customer complains to the VPN provider. The VPN provider is the party offering the VPN service to the VPN customer. Commonly, each VPN has one provider, which can be either a private company or a public network operator. The most important task of the VPN provider is to coordinate the various sub-networks over which the VPN is built and to make this inter-working transparent to the VPN customer and user. The VPN provider predicts the traffic generated by its customers and plans the capacity of its network resources. In case the VPN service provider is the public network operator, then the VPN provider is also responsible for operating the network over which the VPN is implemented.

VPN provisioning may involve several levels of providers and customers. The visibility of network resources is not the same in these distinct administrative domains and the operation and management functions are not applied the same way. Efficient operation of the network necessitates the management of the available resources in order to maximize their utilization and to ensure the expected QoS. The provision of VPN imposes further requirements on the management of network resources (physical and logical) which has to be performed in a cooperative way between VPN providers and VPN customers. The configuration of the VPN commonly leads to the reservation of a set of resources in order to accommodate the VPN traffic.

3.2 Operation and Management Functions

The estimation of traffic expected to be generated by VPN users (traffic matrix) is a prerequisite to determine the transmission and switching capabilities needed to support the VPN operation. This estimation, referred to as user traffic characterization, is initially used by the VPN customer to select which VPN service to subscribe to. It is then continuously adjusted to reflect the real utilization of the subscribed services (e.g., frequency and duration of service utilization) possibly leading to service re-negotiation. The VPN provider has also to continuously estimate the expected traffic to accommodate changing VPN customers needs. The provision of the VPN service consists of network resources reservation according to the specified performance and bandwidth requirements. The service may be of the following types:

- Fixed bandwidth is provided for the lifetime of a VPN;
- Pre-booked bandwidth variations where the customer may specify in advance how the bandwidth reserved on a VPN should vary over time (throughout the working day for example);
- Bandwidth on demand where the customer may change the bandwidth reserved on an already existing VPN.

To configure a VPN, the VPN provider takes into account the location of the VPN customer sites and the associated traffic needs as estimated in the traffic characterization phase. The VPN customers provide the VPN provider with a private addressing scheme (if applicable), an estimate of traffic requirements and the requested QoS. Based on the previous information, the VPN provider plans his network by determining the type and amount of transmission and switching resources. The objective of the VPN provider is usually to minimize the amount of network resources in order to reduce the cost and hence maximize the revenue while satisfying the QoS contracted to VPN customers. VPN reconfigurations may also occur during the VPN lifetime to take into account changes of user-traffic requirements (e.g., service upgrade);

faults occurrence at the network level; QoS degradation; customer's complaints; and others.

A continuous monitoring of the VPN customer traffic and the underlying network is performed by the VPN provider to ensure that service is provided to customers according to the contracted QoS. The VPN customer computes statistics on the VPN service performance (e.g., the number of (un)successful accesses). The measured and the expected VPN performance are then compared which may lead, in case the VPN users are not satisfied with the experienced QoS, to issuing complaints to the VPN provider or to a re-negotiation of QoS parameters.

The VPN service can be used by VPN customers only. Therefore, access control mechanisms are required to protect VPN users/services from unauthorized access. Encryption mechanisms are used to guarantee privacy and data integrity. These mechanisms are usually defined on a per closed user group (i.e. customer) basis. Accounting management uses the information collected by the VPN provider monitoring function to establish the service usage bills and charge the VPN customer.

3.3 Inter-domain VPN Management

The provision of a VPN service may involve several network providers. For example, setting up an Internet VPN between a company's headquarters and its branch offices abroad typically requires services from several local Internet Service Providers (ISPs) and backbone network providers. The management of such VPN involves several administrative domains (the customer domain and the various providers' domains).

VPN end-to-end management requires interactions between VPN customer and VPN provider(s) management domains. These interactions are based on a client/server model, and mainly correspond to negotiating the VPN configuration and the VPN service provision according to the agreed contract. Contracts specify equipment rental and service-level agreements (SLA). During the lifetime of the VPN, the management domains interact to ensure proper operation of the VPN or to renegotiate their contracts. The customer is responsible for identifying the end points, the performance (delay, jitter, packet loss ratio), and the bandwidth (peak bandwidth and variations in bandwidth over time) requirements. According to traffic characteristics and QoS parameters agreed with the customer, the VPN Provider establishes the VPN with the negotiated QoS. In addition to the regular VPN, the customer may require exceptional traffic demands such as setting up high bandwidth calls at given times or changing backup schedule leading to changes in bandwidth requirements. The customer complaints to the provider whenever the offered QoS is below the negotiated one. The customer may also request for re-configuration of the VPN. Ultimately, VPN Provider management is required to provide a single interface to the customer for accepting requests, queries and complaints and also to provide a single bill to the customer. In case the VPN provider is a value added service provider distinct from the public network operator, the VPN provider determines which public network operators should be involved in the provision of the VPN. The VPN provider identifies the end points in each public network domain, the performance and bandwidth requirements, and rents network resources from the involved public network operators. In turn network operators interact with each other, most likely in a peer-to-peer fashion, to negotiate which network resources between their gateway nodes will be used for the VPN.

Service level agreement (SLA) or service contract, mainly consisting of the *traffic contract*, is the basis for the peer-to-peer negotiations involved in a VPN service provision. A traffic contract can be defined for every connection. It consists of connection traffic descriptors and QoS parameters. Each customer is expected to generate traffic that conforms to these parameters. The VPN service provider monitors the offered load and enforces the traffic contract. The VPN service provider is committed to meet the requested QoS, as long as the customer complies with the traffic contract. In addition to the traffic contract, a service contract, for example between the customer and the VPN provider, may include time intervals information for the connections (e.g., days of the week, times during the day, duration etc.) and which customer sites should be connected.

4.0 Future trends

In traditional VPN environments, the customer has the view of the configuration of its CPN (Customer Premises Network) and a view of the VPN resources dedicated to interconnect its sites. The customer is also aware of the capacity of these connections. The VPN provider has a view of the access and transit nodes (VPN switching/routing nodes in the public network domain) and the interconnection between them. If the VPN service provider is also the public network provider then it has also an explicit view of the physical and logical configuration of its own network including the transit and access nodes constituting the public network as well as the links interconnecting these nodes.

In this scenario, the VPN provider hides the network topology as far as the customer was not interested in the way the connections between the customer sites are realized. The main reason for that is the assumption that customers do not have the appropriate skills to control and manage the public network resources that are rented to them. In this case, the customer only controls its CPN including the equipment used to access the public network. The customer also performs the modifications in the CPN when requested (e.g., updates the route selection tables or the private addressing scheme, etc.). The VPN service provider, as a value added service provider, plays an intermediate role between the customers and the involved providers of bearer communication services. It operates the network links rented from the network providers and allocates the contracted bandwidth to customers. In this case, the VPN service provider has a limited access to the network infrastructure and performs management such as the reconfiguration of the links indirectly by requesting the appropriate network provider.

Customers ranging from large to small enterprises are relying more than ever on the networks to conduct their businesses. For that reason, they are either acquiring the appropriate management tools and qualified personnel to administrate and maintain their growing customer premises networks or outsourcing the management of their network resources to third parties. Moreover, customers are seeking to control and manage the VPN services they are subscribing to. There are several reasons for that. Above all is the possibility for customers to control and manage their VPNs according to their own policies reflecting their business goals. A VPN service provider cannot easily accommodate a large variety of service requirements of the various customers. Customers may have different traffic requirements (data, voice, and video) with different priority schemes and performance characteristics. They often require different levels of security. Another important reason for customers to control and manage their VPN is to perform the necessary partitioning of the VPN resources among the different end-users and applications they support, and to implement their own policing mechanisms. Last but not the least is the ability of customers to introduce new communication services if they have full control over the resources allocated to them in the internal network nodes and hence the possibility to introduce their proper resource control algorithms. This trend has been recently strengthened by the emergence and wide acceptance of network programmability as the networking paradigm of the future.

Indeed, effort is currently spend in both academia and industry to open the core network infrastructure and facilitate its programmability by providing the appropriate *network programming interfaces.* Among the undergoing works in this area, there are: the definition of open switching architectures [12], the specification of open signaling protocols [13], the development of programmable and active networks [14]. This trend will bring new challenges to the control and management of network resources. One of the most critical problems that need to be addressed is the shared control and management of the network resources between several domains, which may lead to conflicts. In general, the functions of each domain and the interactions between the different domains have to be re-engineered.

These advances will ultimately enable customer management of VPNs and thereby customizable configuration and goal-driven management of these VPNs. A demonstration of such capabilities is presented in [15].

5.0 References

[1]. Paul Ferguson and Geoff Huston, *What is a VPN?*, White paper, http://www.employees.org/~ferguson/, April 1998.

[2]. ATM Forum, *Multi-Protocol Over ATM*, Specification v1.0, af-mpoa-0087.000, July 1997.

[3]. Hanks, T. Li, D. Farinacci, P. Traina, *Generic Routing Encapsulation*, RFC1701, October 1994.

[4]. A. Valencia, K. Hamzeh, A. Rubens, T. Kolar, M. Littlewood, W. M. Townsley, J. Taarud, G. S. Pall, B. Palter, W. Verthein,, *Layer Two Tunneling Protocol 'L2TP'*, draft-ietf-pppext-l2tp-10.txt, March 1998.

[5]. K. Hamzeh, G. Singh Pall, W. Verthein, J. Taarud, W. A. Little, *Point-to-Point Tunneling Protocol – PPTP*, draft-ietf-pppext-pptp-02.txt, July 1997.

[6]. D. Waitzman, C. Partridge, S. Deering, *Distance Vector Multicast Routing Protocol*, RFC1075, November 1988.

[7]. R. Chandra, P. Traina, T, Li, *BGP Communities Attribute*, RFC1997, August 1996.

[8]. E. Chen, T. Bates, *An Application of the BGP Community Attribute in Multi-home Routing*, RFC1998, August 1996.

[9]. Callon, P. Doolan, N. Feldman, A. Fredette, G. Swallow, A. Viswanathan, *A Framework for Multiprotocol Label Switching*, draft-ietf-mpls-framework-02.txt, November 1997.

[10]. T. Dierks, C. Allen, *The TLS Protocol – Version 1.0*, draft-ietf-tls-protocol-05.txt, November 1997.

[11]. S. Kent, R. Atkinson, *Security Architecture for the Internet Protocol*, draft-ietf-ipsec-arch-sec-04.txt, March 1998.

[12]. Proceedings of OPENARCH'99, N.Y., March 1999.

[13]. Proceedings of OPENSIG'98, Toronto, October 1998.

[14]. D. Tennenhouse, J. Smith, W. Sincoskie, D. Wetherall, and G. Minden, *A Survey of Active Network Research*, IEEE Communications Magazine, January 1997.

[15]. R. Boutaba, W. Ng., A. Leon-Garcia, *Web-based Customer Management of VPNs*, Journal of Network and Systems Management, Vol. 9, No. 1, 2001.

6.0 List of Acronyms

ARP	- Address Resolution Protocol
ATM	- Asynchrous Transfer Mode
BGP	- Boarder Gateway Protocol
CPN	- Customer Premises Network
DVMRP	- Distance Vector Milticast Routing Protocol
FR	- Frame Relay
GRE	- Generic Routing Encapsulation
IETF	- Internet Engineering Task Force
ISP	- Internet Service Provider
LAN	- Local Area Network
L2TP	- Layer 2 Tunneling Protocol
MPLS	- Multi-Protocol Label Switching
MPOA	- Multi Protocol Over ATM
NLRI	- Network Layer Reachability Information
PBX	- Private Branch Exchange
PNO	- Public Network Operators
POP	- Point of Presence
PSPDN	- Public Switched Packet Data Networks
PSTN	- Public Switched Telephone Networks
QoS	- Quality-of-Service
SLA	- Service Level Agreement
TLS	- Transport Layer Security
VC	- Virtual Connection
VPC	- Virtual Path Connections
VPN	- Virtual Private Network

About the author

Prof. Raouf Boutaba teaches networks and distributed systems in the Department of Computer Science of the University of Waterloo and conducts research in integrated network and systems management, wired and wireless multimedia networks, and quality of service control in the Internet. He is the program chair of the technical committee on information infrastructure of the IEEE Communications Society and the chairman of the IFIP working group on network and distributed systems management Dr. Boutaba is a member of the advisory editorial board of the International Journal on Networks and Systems Management. He is the recipient of the Province of Ontario Premier's Research Excellence Award in 2000.

Newly Elected IEEE Fellows 2002

Majid Ahmadi
University of Windsor
Windsor, ON
For contributions to the design of digital filters, and to pattern recognition and image restoration.

Jens Bornemann
University of Victoria
Victoria, BC
For contributions to the modeling of design of waveguide components and planar structures.

Terrence Michael Caelli
University of Alberta
Edmonton, AB
For contributions to machine vision and pattern recognition.

James Kennedy Cavers
Simon Fraser University
Burnaby, BC
For contributions to the theory and practice of digital transmission over wireless channels.

Henrietta L. Galiana
McGill University
Montreal, QC
For leadership in understanding biological control systems and for the development of transient identification methods in the modeling of ocular reflexes.

Wayne Davy Grover
University of Alberta
Edmonton, AB
For contributions to survivable and self-organizing broadband transport networks.

James W. Haslett
University of Calgary
Calgary, AB
For contributions to high temperature instrumentation and noise in solid-state electronics.

Praveen K. Jain
Queen's University
Kingston, ON
For contributions to efficient high frequency power converter systems.

Wenyuan Li
BC Hydro
Burnaby, BC
For contributions to power system reliability theory, calculation methods and algorithms, and applications.

Jose Ramon Marti
University of British Columbia
Vancouver, BC
For contributions to the development of electromagnetic transients programs for transmission line modeling and real-time simulation.

Andrew Ng
University of British Columbia
Vancouver, BC
For contributions to plasma science concerning warm dense matter, femtosecond-laser matter interactions, and laser-driven shock waves.

Graham John Rogers
Cherry Tree Scientific Software
Colbourne, ON
For contributions to the modelling, analysis and control of dynamic phenomena in power systems.

Magdy M.A. Salama
University of Waterloo
Waterloo, ON
For contributions to the advancement of distribution system performance.

Kon Max Wong
McMaster University
Hamilton, ON
For contributions to sensor array and multi-channel signal processing.