行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　※
※　下一代虛擬私有網路彈性資源管理與代輸服務品　※
※　質保證方法之研究　　　　　　　　　　　　　※
※　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※

計畫類別：□個別型計畫　　■整合型計畫

計畫編號：NSC 90-2213-E-002-079

執行期間：90 年 8 月 1 日至 91 年 7 月 31 日

計畫主持人：國立台灣大學資訊管理學系　孫雅麗教授

計畫參與人員：謝明甫 張　　纁鄭霈群 陳佩文 杜勇正

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份

□赴大陸地區出差或研習心得報告一份

□出席國際學術會議心得報告及發表之論文各一份

□國際合作研究計畫國外研究報告書一份

執行單位：國立台灣大學資訊管理學系

中　華　民　國　91　年　5　月　24　日

下一代虛擬私有網路核心技術之研究(子計劃一)：
下一代虛擬私有網路彈性資源管理與代輸服務品質保證方法之研究
Flexible Resource Management and QoS Assurance for Next Generation Virtual Private Networks(VPNs)

計劃類別：整合型計劃
計劃編號：NSC 90-2213-E-002-079
執行期限：2001.08.01 至 2002.07.31

整合型計劃：總計劃主持人：蔡志宏教授
子計畫主持人：孫雅麗教授
子計畫參與人員: 謝明甫 張 繼鄭霈群 陳佩文 杜勇正
執行單位：國立台灣大學資訊管理學系

一. 中文摘要

基於網路經濟及防範駭客入侵的需求，架設於Internet 的虛擬私有網路(IP-VPN, Virtual Private Network)服務提供正快速成長中。第一代 IP 虛擬私有網路則是在公眾網際網路中建立加密的資料通道，技術發展集中在第二層(Layer 2)的通道建立機制(例如 PPTP, L2TP)以及遠端存取的安全性(如 RADIUS 與以 IPsec 為基礎的加密)。目前這個階段的技術已相當完備，我們預期每個虛擬私有網路的端點(endpoint)將會迅速成長。

在現今多變的企業連網環境裡，端點之間可靠而動態的通訊需求將日益增加，然而通訊型態卻愈來愈難以預測。在許多狀況下，使用者無法描述虛擬私有網路端點間的流量負載，更遑論點對點(point-to-point)的服務品質(QoS)需求。此外，傳統私有網路的使用者即使在專線沒有被使用時也必須對全部頻寬支付全額費用。架設以 IP 為基礎的虛擬私有網路上的新議題是：a) 網路管理者需要更積極地依據流量負載與服務協定(service level agreement)介入虛擬私有網路的頻寬分配與管理, 在這個新模式下，使用者不必再為沒有使用到的頻寬付費，網路提供者也可以更妥善地規劃網路資源及利用頻寬; b) 可擴充性(scalability) - 在有著成千上萬各有不同服務品質需求的資料流(flow)的高速骨幹網路上; c) QoS support。傳統上固定速率(constant bit rate)的頻寬管道(即虛擬租用專線)已經不能符合動態、多變的通訊型態及應付使用者多元化的內容，以及在端點間建立安全且有服務品質保證連線的要求。本計畫研究在下一代以 IP 為基礎的虛擬私有網路，彈性的容量管理及資源分配確保每個 VPN 通道的服務品質。

關鍵詞：虛擬私有網路、傳輸服務品質保證、資源管理、封包排程，容量規劃與管理、整合服務，差別性服務、寬頻網際網路

Abstract

Driven by fear of hackers and the economics of the Internet, the subject of Virtual Private Network (VPN) over the Internet (i.e. IP-based VPN) has received considerable attention from the industry and recently ever-growing interest from the research community. The service support and provisioning of VPN are going into an age of dramatic growth. In the meantime, the transfer requirements of VPN will as well have drastic changes. The first generation VPN was built mainly using private leased line service. The second generation VPN is to create encrypted data tunnels through the Internet. The technology focuses Layer 2 tunneling techniques such as PPTP, L2P and L2TP, and remote access security such as RADIUS and IPsec-based encryption.

While the current VPN technology reaches a state of readiness, we expect the number of endpoints per VPN will grow rapidly. In today's *dynamic* business environments, demand for dependable, dynamic communication between endpoints increases and the communication patterns become difficult to forecast. In many cases, users are unable to clearly specify loads between endpoints of VPN sets. Let alone the QoS requirements on a point-to-point basis. Moreover, in traditional private networks users have to pay for the full bandwidth *at all times* even the line is not being used. The new issue in IP-based VPN implementation is that the network managers need to play a more active role in allocating and managing bandwidth allocated to individual VPNs in accordance with the traffic load and the service level agreement. In this new model, users will no longer need to pay for the bandwidth they do not use. Network providers can better plan network resources and utilize bandwidth.

This project focuses on the design and implementation of VPN resource management mechanisms to support effective and flexible VPN configuration and billing at the boundary router. Specifically, we address the problems of *a*) how to

manage and allocate bandwidth in order to support effective and flexible VPN configuration and billing at the boundary router; *b*) how to assure service quality and performance between individual VPN tunnels; and *c*) how to guarantee performance to different classes of applications within a tunnel for all time scales.

Keywords: Virtual Private Network, VPN, Quality of Service, resource management, packet scheduling, capacity planning and management, Integrated Services, Differentiated Services, Broadband Internet.

二. 研究緣由、目的與成果

Ⅰ緣由

下一代的虛擬私有網路是在共享的網路上透過建立通道的技術提供點對點或是多點的連結服務，因為傳統的私有網路有其限制，首先，使用者即使沒有使用頻寬仍需付費，第二，私有網路只提供點對點連線，多點連線的需求是必要的，同時能夠提供群體通訊，第三，私有網路並沒有提供行動通訊或是遠端存取服務，為了解決上述在傳統私有網路的限制，虛擬私有網路需要滿足幾個需求：有彈性的分配資源、有效的使用頻寬、使用才付費的機制、提供多點連結的服務、達到服務品質的保證、確保存取的安全性等。

Figure 1 顯示了兩個虛擬私有網路，VPN1 有三個地點，VPN2 有兩有個地點，這兩個 VPNs 在路由器 R1 和 R2 之間共享頻寬，在此共享的連線裡有兩個 Pipes 可以區隔不同的 VPN 流量，每個 Pipe 又有三個 sessions，所以虛擬私有網路可以在通道裡提供品質服務的保證。

Ⅱ目的

In the first part, we studied and surveyed works related to the following issues: *a*) how to manage and allocate bandwidth in order to support effective and flexible VPN configuration and billing at the boundary router (see Figure 2 and Figure 3); *b*) how to assure service quality and performance between individual VPN tunnels; and *c*) how to guarantee performance to different classes of applications within a tunnel for all time scales. The goal is to address the two basic needs – performance and accounting - for carriers to offer VPN services

In the second part of the project, we have set up a VPN router prototype based on Linux. We are currently working on the implementation of dynamic VPN configuration and provisioning, and resource management. These management/control modules will integrate with the pricing system developed by subproject 2 and mobile VPN systems by subproject 3.

Ⅲ成果

A. Design Goals

To address the needs of today's *dynamic* business environments the next generation VPN must be able to quickly respond to *corporate growth*. In summary, the requirements of the next generation VPN are as follows:

- Flexibility – on-demand resource allocation to accommodate the pace and unpredictability of business and traffic demands;
- Affordability – dynamic resource allocation to provide flexible accounting/billing instead of flat-rate, static pricing;
- Efficiency - efficient resource utilization;
- Connectivity – dynamic configuration of point-to-point and multipoint connectivity to meet the demands of a growing community of *remote users, customers and partners;*
- Communications – ability to manage *VPN connectivity both end-to-end unicast and multicast* communications**;**
- Scalability – to meet the quality of service requirements of traffic transfer;
- Security - to provide access to networked resources, including legacy systems and enterprise protocols, without compromising security.

VPN services have recently received considerable attention within the IP, frame-relay, MPLS, and ATM networking communities[2]. The next generation VPN is a "*virtual*" connectivity, point-to-point and multipoint, unicast and multicast communication, over a shared network via "*tunneling*"- Traffic from many sources to travel via *separate tunnels* across the *same* infrastructure.

B. 文獻探討

IETF has specified four general VPN requirements: Opaque Packet Transport, Data Security, Tunneling Mechanism and Quality of Service Guarantees [1]. Data Security and Tunneling Mechanism are the basic mechanism to construct a VPN. The first three issues have been the focus of research in the Internet community in the last couple of years. The goal is to provide security of the VPN service. Much less attention has been paid to resource management issues related to VPNs, but it is necessary for VPN service to offer comparable performance assurance [2].

In [3], the authors propose a new service interface, termed a *hose*, to provide the appropriate performance abstraction. A Hose is characterized by the aggregate traffic to and from one endpoint in the VPN to the set of other endpoints in the VPN, and by an associated performance guarantee. The connectivity of endpoints to the network is specified by a hose model, comprising:

- the capacity required for aggregate outgoing traffic from the endpoint into the network (to the other end points of the VPN)
- the capacity required for aggregate incoming traffic out of the network to the endpoint (from the other endpoints of the VPN);

- the performance guarantee for the hose, conditioned only on the aggregate traffic seen at the hose interface.

The *Hose* Model implements the link-sharing concept and provides customers simpler, more flexible Service Level Agreements (SLAs). The *Hose* model appears to present the provider with a more challenging problem in resource management. In [3] the authors also propose two basic mechanisms to manage network resources which can be applied on both access links and network internal links:

- Statistical Multiplexing: Multiplexing can be applied to a hose or a set of hoses.
- Resizing: The provider can make a worst case initial allocation, and then resize that allocation based on online measurements.

The dynamic resizing algorithm is shown to result significant statistical multiplexing gain (factor 1.5 to 3), but the issue of fairness and isolation has not been discussed. 然而，施行 hose model 對於虛擬私有網路服務供應者(VSP)來說會使得原本已經困難的資源管理的任務更加複雜。

Based on the hose model, [4] 提出以一個單一樹狀結構連接一個 VPN 端點的想法 to maximize 頻寬保留的共享. 亦即在某一 link 上所保留的頻寬可由兩個 VPN 端點集合所共享。這是由於在樹狀結構上，任兩端點的傳輸路徑(transmission path)是唯一的(unique)，故樹狀結構上任一條 link 會將 VPN 上的端點分成兩個集合。In this paper, they consider four cases with respect to two dimensions: symmetric and asymmetric bandwidth requirement at a VPN interface, and finite and infinite link capacity. 作者對於在 symmetric traffic and infinite capacity case 導出一個時間複雜度是 O(mn)的最佳演算法，可以找出總保留頻寬最小的樹狀結構。其中 m 是 Network graph 上的邊數，n 則是點數。For finite capacity cases，找出總保留頻寬最小樹狀結構的問題本身就是 NP-hard，而且此問題的近似演算法也是 NP-hard。

In [5], they consider the reconstruction of a tree-based VPN topology in the presence of a link failure. They consider one single link failure. Their approach is that since 事前無法預知那一條 link 會損壞，所以事先 setup 一組備份路徑(backup paths)，以便於當樹狀結構中任一條 link 損壞時可以立刻找到一條 path，將之加入斷掉的樹狀結構中以形成一顆完整的樹。Moreover, VSP 必須事先在這一組 setup 起來的備份路徑上保留足夠的頻寬，以符合 hose model 所指定的進入速率及離開速率。Basically，為樹上的所有 link 都保留一條以上的替代路徑其實有很多種選擇，希望選出一組替代路徑儘可能保留最少的總頻寬。The first problem is a NP-Complete problem，因為它是 optimal augmentation problem 的一種變型，而後者也是 NP-Complete。為了節省計算時間，作為提出了一個 approximation ratio 是 16 的近似演算法來找出一個近似最佳解。

In [6], they 對於 VPN 的自動化的建構，提出一個 simple 的架構(architecture)。首先，將 user-level VPN requirements 用 VANDAL 語言翻譯成 a specification of system-level requirements。Then,根據 specification and 目前網路資源的可用情形、construct VPN topology 找出一個符合顧客所要求、VSP 所訂定的政策的 VPN topology，並且在 VPN topology 上會配置足夠的資源。

[5] proposed a heuristic algorithm to 找出最小成本的 tunnel 安排方式(layout)。

In [8], a scheme called Stochastic Fair Sharing (SFS) is proposed. The SFS scheme implements fair sharing among Virtual Leased Links (VLLs) by dynamically modifying their capacities as sessions arrive and depart. The SFS is an admission control algorithm used to decide which sessions to accept and which to reject depending upon the current utilizations and provisioned capacities of the classes. The simulations exhibit that SFS achieves isolation (low session arrival rate low blocking probability), Statistical Multiplexing (more multiplexing gain than static partitioning), Fairness (higher max-min fairness index (0.97) in virtual link), efficiency (low signal overhead).

C. VPN Service Model

We propose a new *VPN service model* to capture users' and providers' requirements. We consider a network with N VPN users; each forms a VPN group. There are several possible service models. An edge link has M VPN users. The user-level QoS requirements per VPN endpoint follows the Hose model[3]. The bandwidth allocation is transformed into a pool of tokens that could be flexibly assigned to traffic going towards any destination from the endpoint within the VPN. Figure 2 depicts the key resource management components in a router: resource reservation, admission control, QoS routing, traffic control, queue Management and packet scheduling. Data transmission operations proceeds as follows:

- When sender wants to send data, it initiates a QoS request. The request will pass to "Resource Reservation" mechanism, to reserve adequate resources.
- During the resource reservation phase, "QoS Routing" component discovers the feasible path; "Admission Control" mechanism decides whether there is adequate free capacity to accept the reservation request.
- If the request is accepted, the "Traffic Control" mechanism will monitor the traffic and force it to conform to sender's traffic specification. The "Queue Management" mechanism will monitor the queue length to avoid congestion. The "packet scheduling" mechanism will determine the sequence the packet will be transmitted.

We are currently working on a) the link sharing scheme between tunnels of a VPN and between VPNs;

and b) admission control. The objectives of our link-sharing scheme must possess the following features: [9][10][11]

- Isolation - Every VPN flow will not be suffered from rogue source, such as ill-behaved users, network load fluctuation, and best-effort users.
- Fairness - The available network resources must be shared among the flows in a fair manner.
- Flexibility - Flexibility means elasticity. For example, users could modify SLAs dynamically.
- Utilization - The network resources must utilize efficiently. The idle resources may be shared within the same service class or among different service classes.
- Efficiency - Efficiency means lower overhead or more end-to-end performance guarantee.

To achieve efficient resource usage, we propose to build *VPN membership tree*. The multicasting tree concepts can be used to build *VPN membership tree* [12][13][14][15][16]. But we need to consider the difference between them, VPN packets need higher security control and multicasting tree is more dynamic than VPN membership Tree. Note that in this approach they consider the bandwidth allocation for the worst-case. In reality, at any time instant, it is likely that bandwidth allocated to a VPN will not be fully used. Therefore, how to make use of the characteristics of statistical multiplexing gain between flows of VPNs sharing a common link and be able to dynamically allocate bandwidth subject to the QoS constraints becomes a challenge.

D. 實作

虛擬私有網路的技術發展集中在第二層的通道建立機制和遠端存取的安全性，我們在通道建立的機制上使用 L2TP，在遠端存取安全性上使用 RADIUS 和以 IPSec 為基礎的加密技術，此虛擬私有網路的系統已建置完成，架構圖如 Figure 3 所示。

使用者透過區域網路連上 LAC，經過 RADIUS 伺服器認證使用者帳號/密碼無誤後，建立 L2TP 通道至 LNS，LNS 可視為私人企業的 Gateway，為通道的結束端點，進而存取企業內部的資訊，另一種方式是使用者可以直接利用 IPSec，將送出的資料加密，資料的接收者將此資料解密得到原來的資料，資料送收雙方需事先協調參數，例如加密演算法、認證演算法等。

整個虛擬私有網路系統在 Linux 上執行，kernel 版本 2.4，我們所採用的軟體如下：

- L2TP 使用 l2tpd，版本 0.64。
- RADIUS 使用 FreeRadius，版本 0.4。
- IPSec 使用 Frees/WAN，版本 1.94。

除了系統的安裝，我們也深入程式碼，希望了解運作方式。在實際架設虛擬私有網路系統時，為了讓這些 Components 能夠緊密結合，而不只是一個個獨立的軟體，我們花了很多時間追蹤程式碼，了解其中運作的流程與原理，以便在將來有必要時能夠自行修改程式碼，達到計畫預期的目標。

四、參考文獻

[1] B. Gleeson, A. Lin, J. Heinanen, G.Armitage and A. Malis, “Framework for IP Based Virtual Private Networks,” IETF RFC 2764, February 2000.

[2] D. Mcdysan, “VPN application guide,” Wiley Computer Publishing, 2000.

[3] N. G. Duffield, P. Goyal, A. Greenberg, P. Mishra, K.K. Ramakrishnan, and Jacobus E. van der Merwe, “A Flexible Model for Resource Management in Virtual Private Networks,” Proceedings of SIGCOMM, pp. 95-108, August 1999.

[4] Amit Kumar, Rajeev Rastogi, Avi Siberschatz and Bülent Yener “Algorithms for Provisioning Virtual Private Networks in the Hose Model,” SIGCOMM 2001.

[5] Giuseppe F. Italiano, Rajeev Rastogi and Bülent Yener, “Restoration Algorithms for Virtual Private Networks in the Hose Model,” INFOCOM 2002.

[6] Rebecca Isaacs and Ian Leslie, “Support for Resource-Assured and Dynamic Virtual private Networks,” IEEE Journal of Selected Areas in Communications, Vol. 19, No. 3, March 2001.

[7] Reuven Cohen and Gideon Kaempfer, “On the Cost of Virtual Private Networks,” IEEE/ACM Transactions on Networking, Vol. 8, No. 6, December 2000.

[8] S. Deering, D. L. Estrin, D. Farinacci, V. Jacobson, C. G. Liu and L. Wei, “The PIM Architecture for Wide-area Multicast Routing,” IEEE/ACM Transactions on networking, Vol. 4, No. 2, pp. 153-162, April 1996.

[9] H. Zhang, “Service Disciplines for Guaranteed Performance Service in Packet-Switching Networks,” Proceedings of IEEE, Vol. 83, No. 10, pp. 1374-1396, October 1995.

[10] M. H. Hou and C. Chen, “Service Disciplines for Guaranteed Performance,” IEEE Fourth International Workshop on Real-Time Computing Systems and Applications, pp. 244 –250, October 27-29, 1997.

[11] J. Liebeherr, D. E. Wrege and D. Ferrari, “Exact Admission Control for Networks with a Bounded Delay Service,” IEEE/ACM Transactions On Networking, Vol. 4, No. 6, pp. 885 –901, December 1996.

[12] K. C. Almeroth, “The Evolution of Multicast: From the MBone to Interdomain Multicast to lntemet2 Deployment”, IEEE Network, pp. 10-20, January/February 2000.

[13] B. Wang and J. C. Hou, “Multicast Routing and Its QoS Extension: Problems, Algorithms, and Protocols,” IEEE Network, pp. 22-36, January/February 2000.

[14] C. Diot, B. N. Levine, B. Lyles, H. Kassem and D. Balensiefen, “Deployment Issues for the IP Multicast Service and Architecture,” IEEE Network, pp. 78-88, January/February 2000.

[15] T. Ballardie, P. Francis and J. Cowcroft, “Core Based Trees (CBT): An Architecture for scalable Inter-Domain Multicasting Routing,” Proceeding of ACM Sigcomm, pp. 85-95, September 1995.

[16] S. Floyd and V. Jacobson, “Link sharing and resource management models for packet networks,” IEEE/ACM Transactions on networking, vol. 3, no. 4, August 1995, pp. 365-386.

[17] R. Garg and H. Saran, “Fair Bandwidth Sharing Among Virtual Networks: A Capacity Resizing Approach,” Proceedings of INFOCOM, Tel Aviv-Jaffa, Israel, March 2000.

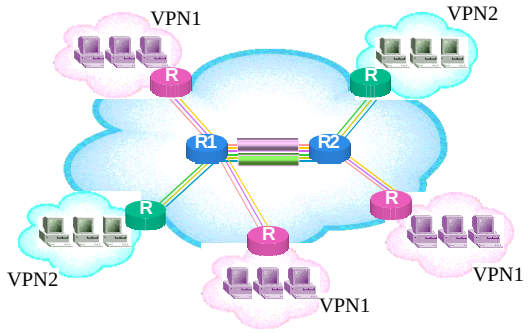

Figure 1. The QoS-assured VPN service - per-tunnel and per-session within the tunnel

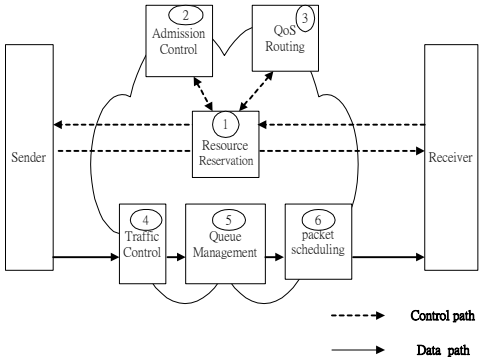

Figure 2. Resource management components of a QoS router

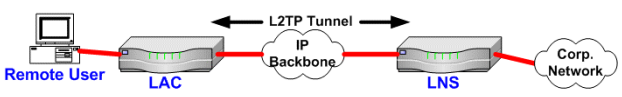

Figure 3. 系統架構圖