

※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※

※

※ 下一代虛擬私有網路核心技術之研究(1/2)－總計畫 ※

※

※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※※

執行期間： 90 年 8 月 1 日至 91 年 7 月 31 日

計畫主持人：國立台灣大學電信工程研究所 蔡志宏教授
共同主持人：國立台灣大學電機工程學系 張時中教授
國立台灣大學資訊管理學系 孫雅麗副教授

☒ 九十一年度預核清單影本一份
☐ 變更經費對照表一份(欲變更經費者才檢附)
☐ 欲參加九十一年度傑出研究獎遴選者應備資料

執行單位：國立台灣大學電信工程研究所
國立台灣大學電機工程學系
國立台灣大學計算機及資訊網路中心

中 華 民 國 91 年 5 月 24 日

行政院國家科學委員會專題研究計畫執行進度報告

下一代虛擬私有網路核心技術之研究(1/2)－總計畫

Enabling Technology for The Next Generation Virtual Private Networks

計畫編號：NSC 90-2213-E-002-077

執行期間：90年8月1日至91年7月31日

計畫主持人：國立台灣大學電信工程研究所 蔡志宏教授

共同主持人：國立台灣大學電機工程學系 張時中教授

國立台灣大學資訊管理學系 孫雅麗副教授

一、中英文摘要

近年來虛擬私有網路之技術及應用，隨著網際網路的成長已迅速發展並引人注意。然而，現有虛擬私有網路雖然技術及標準推陳出新，在數據資料的安全性，服務品質(QoS)保障，計價機制的引進，多元化多媒體服務，以及在有線及無線寬頻接取網路上提供虛擬私有網路的能力上，均仍有極大的發展空間。因此，最近在工業界及學術界均已掀起探討下一代虛擬私有網路關鍵技術之研究風潮。本研究群乃預計以兩年時間投入下一代VPN之研究，其中並特別強調、在服務品質、計價機制、以及無線接取這三個領域之關鍵技術。本計畫第一年先分別以三個子計畫進行測試，在一方面先各自規劃出可行之架構，第二年將逐步地相互整合，最後提出一個下一代虛擬私有網路之具體雛形。

關鍵詞：虛擬私有網路、服務品質、計價、無線

Abstract

Following the rapid growth of Internet, the technology and applications of Virtual Private Networks (VPN) have made significant progress and have attracted much attention. Although different technologies and standards for realizing VPN have been

proposed and promoted in areas such as data security, QoS guarantee, pricing mechanism, streaming data and multimedia services, and wired/wireless broadband access, there is still much room to grow. Therefore, both the industry and the academic researchers have started the discussion about the research of the next generation VPN. This research team shall dedicate 2 years to the research of key technologies for the next generation VPN, and shall focus on 3 major areas: QoS, pricing, and wireless. In the first year, three subprojects have proposed novel architectures for these areas, and then we will gradually integrate these architectures and finish their implementations. Next year, we will finish a prototype for the next generation VPN.

Keywords: Virtual Private Networks, Quality of Service, Pricing, Wireless

二、計畫緣由與目的

基於網路經濟及防範駭客入侵的需求，架設於網際網路之上的虛擬私有網路(VPN, Virtual Private Network)(亦即以IP為基礎的虛擬私有網路)已經獲得工業界高度重視，同時最近也在學術界掀起一陣研究的熱潮。虛擬私有網路服務的提供正快速成長中，同時虛擬私有網路的需求也將有重大改變，第一代虛擬私有網路多半以私有專線佈建，第二代虛擬私有網路則是

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)。

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。

在這個計畫裡，我們將會探討在虛擬私有網路在資源管理所遇到的問題，並提出解決之道，雖然目前有很多的虛擬私有網路產品，但是要廣泛的使用還有困難，因為目前對於虛擬私有網路的定義與範疇缺乏一致的協議，所以當我們開始深入這些相關的議題時，一個已知的架構是必需的，我們將會建構虛擬私有網路的參考模式，這個架構可以符合現行的技術又允許未來的擴充性，同時，我們將會找出此模式的基本成員，像是安全控制、品質控制和存取控制等。

本計劃的 VPN Gateway 研究工作分為以下二部分：

在第一部分，我們結合差別服務(DiffServ)架構與網路安全協定，設計了品質服務虛擬私人網路路由器。

在第二部分，我們持續校園宿舍網路差別服務計價收費實驗之研究，設計了利用尖峰計價(Peak Load Pricing)的方式去做網路交通流量的管制，並保證使用者合理需求的滿足及提供相對的服務品質(Quality of Service)。

後續研究中我們將結合以上二部份所建立之基礎，來達成具有服務品質之下一代虛擬私人網路計價收費機制之研究，並將在台大宿舍網路進行實驗。

此外，隨著 VPN 技術的快速發展和世

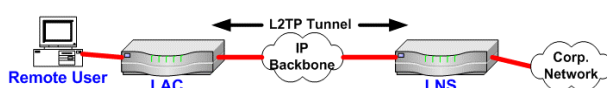
界 VPN 服務市場的成長，該如何以正確、安全和可信的方式對 VPN 服務計價與收費，對經營具有競爭力 ISP 而言，不僅有經濟上的重要性，技術上也極具挑戰性。在這個計畫裡，我們的研究可以了解下一代 VPN 的服務模式、技術趨勢和營運經濟，以及設計和發展出促成下一代 VPN 具競爭力運作的計價收費相關核心技術。

最後，在本計畫我們著重 Wireless VPN 技術，將包含兩個部分。第一，可在固定式無線網路或區域網路支援多個對 QoS 敏感的多媒體即時串流及一般 TCP/IP 交通流的封包排程器及空中存取介面。第二，對於在無線存取節點及無線終端使用者之間的自動調整組態機制，IP VPN gateway 功能及 VPN tunneling 協定。這些技術所要達成的目標是在相同的無線接取網路上同時的提供多重 VPN 服務，但是不同的 VPN 服務所需的 QoS 都相異，而且對不同的使用族群也需不同的安全等級。此外，無線 VPN 終端設備必須要能夠提供自動組態設定機制使得無線 VPN 使用者能以無縫式的接取意欲的 VPN 與應用。

三、研究方法、結果與討論

3.1 子計畫一——下一代虛擬私有網路彈性資源管理與傳輸服務品質保證方法之研究

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，架構圖如圖一所示。



圖一 系統架構圖

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：

1. L2TP 使用 l2tpd，版本 0.64。
2. RADIUS 使用 FreeRadius，版本 0.4。
3. IPSec 使用 FreeS/WAN，版本 0.5。

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。

3.2 子計畫二—下一代虛擬私有網路計價收費技術之研究

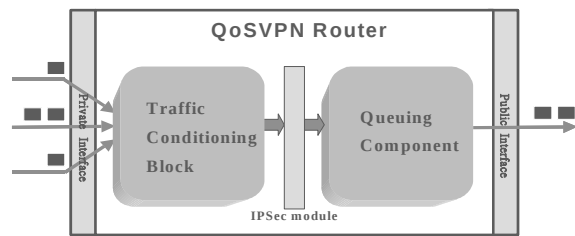
3.2-1 品質服務虛擬私人網路系統之設計與實作

1. 設計目的

- 1) 保障私人網路之通訊安全
- 2) 研究路由器之資源管理
- 3) 整合路由器之虛擬私人網路與品質服務功能
- 4) 滿足不同型態的虛擬私人網路需求
- 5) 提供動態的頻寬設定服務

2. 整合型品質服務虛擬私人網路路由器

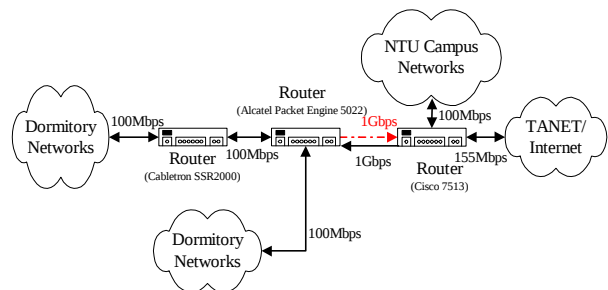
根據設計目的，我們提出了以下的路由器系統設計軟體架構圖與系統方塊圖(圖一)。此設計主要由以下三個模組構成：(1) 網路交通調節器(Traffic Conditioning Block, TCB)。(2) 網路安全協定模組(IPSec module)。(3) 佇列元件(Queuing Component)。其達成 QoS 功能之原理為藉由封包分類規則將封包分類，再經過標記器替每一個網路流(per flow) 的封包標記不同的 DSCP 而把不同的網路流歸成一個服務等級。其後使用網路安全協定替屬於各虛擬私人網路的封包作加密，在封包離開路由器之前使用 WRR 的方式，根據 DSCP 替不同的服務等級分配不同比例的網路資源。我們也設計了服務代理人(Service Broker)提供使用者動態的頻寬設定服務，藉由上述的設計我們實作了具有服務品質的虛擬私人網路實驗環境。



圖一 整合型品質服務虛擬私人網路路由器

3.2-2 校園宿舍網路差別服務計價收費之研究

鑒於校園網路存在著大用戶使用者濫用與不公平的情形，所以我們利用尖峰計價的方式去達到網路交通流量的管制，並保證使用者合理的需求提供相對的服務品質(Quality of Service)。除了計價策略，在此研究中我們根據校園網路實際量測所得數據建構了相關的使用者行為模型、網路交通流量模型及網路效能模型，並將應用在校園宿舍網路實驗平台(圖二)。



圖二 台大宿舍網路虛擬計價實驗架構圖

本計畫之進度與原本的目標非常地接近，我們已順利建立了具 QoS 功能之下一代 VPN 實驗環境，並推導出收費計價之策略與分析模型，並已規劃整合進我們之前於台大宿舍網路所進行之虛擬網際網路計價(VIP)實驗之中，以進行完整之下一代虛擬私人網路之計價研究。

3.3 子計畫三—以無線網路提供下一代 VPN 服務關鍵技術之研究

本研究中，為提供 Wireless VPN 的開道器，我們使用 Linux 路由器，並且開啟它的 CBQ 功能，因為它是目前業界最常用的 Wireless VPN 開道器設計。

我們使用 Chariot 中內建的 IPTVv.scr 檔

來模擬產生兩個 UDP 交通流，這兩個交通流皆由主機 C 的 x.y.3.1 流到主機 D 的 x.y.1.1；再使用內建的 Throughput.scr 檔來模擬產生一個 TCP 交通流，而它是由主機 C 的 x.y.4.1 流到主機 D 的 x.y.1.1。

CBQ(Class-Based Queuing)是目前常見的排程器之一。它的作法是將交通分成數種不同的 class，每個 class 有自己的 queue 與設定的頻寬。一般在頻寬充裕的情況下每個 class 可以按照比例分配可用的頻寬，一旦發現有 class 因為頻寬不足而無法完全使用設給它的頻寬時，則會開始限制某些超過設定頻寬的 class，讓它不再超過。CBQ 特別的地方在於 class 的分類是有階層性的，當 parent class 有多餘的頻寬時，能讓它的 children 優先享用，而不會均分給所有的 class。不過在本實驗裡我們並不打算測試頻寬分享的功能，而是著重在 CBQ 估算各 class 使用的頻寬與限制頻寬的能力上。

由於本實驗是要驗證 Linux 路由器的 CBQ 性能。此外，我們也探討在有小封包出現時，對 CBQ 的效能有何影響。實驗的結果見表一。

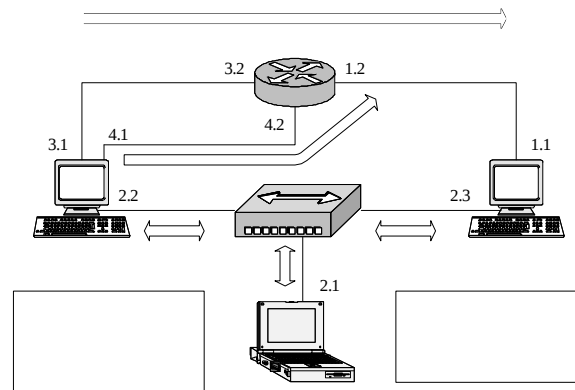
表一 實驗結果列表

Allocated bandwidth (Mbps)			Chariot 量得的 throughput (Mbps)		
UDP1	UDP2	TCP	UDP1	UDP2	TCP
0.1	0.1	1	0.103	0.103	1.041
0.1	0.1	1	0.073	0.103	1.041
0.5	0.5	5	0.545	0.545	5.413
0.5	0.5	5	0.384	0.544	5.439
1	1	10	1.183	1.182	11.571
1	1	10	0.830	1.176	11.526
2	2	20	2.480	2.485	21.153
2	2	20	1.282	2.492	22.047
3	3	30	3.857	3.864	30.652
3	3	30	1.622	3.812	30.602
4	4	40	4.548	4.554	48.374
4	4	40	1.808	4.404	46.733
Packet Style			UDP1	UDP2	TCP

本研究中，我們可以看到 Linux 的 CBQ 效能，在處理小封包交通流時的表現遠遜於處理大封包交通流，這可能是因為 Linux 路由器的 CPU 在某段時間內相對於以大封包傳送的交通流接收到太多的中斷訊號，而來不及處理所造成，所以導致小封包的遺失率很高，因而使得 throughput 下降。

而且就所得的數據來看，最壞的情況可以跟 allocated bandwidth 有 28% 的誤差，最好的情況也有 3% 的誤差，所以 CBQ 的效果似乎不是那麼地準確，只能提供一個大概的機制來限定頻寬而已。

因此目前我們已可藉由 Linux 路由器頻寬管理功能的測試，對 Wireless 交通流提供粗略的 QoS 保證。



圖三 Wireless VPN 開道器測試

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. 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.
3. D. Mcdysan, "VPN application guide," Wiley Computer Publishing, 2000.
4. S. Shenker, C. Partridge, R. Guerin, "Specification of Guaranteed Quality of Service," IETF RFC 2212, September 1997.
5. John Gilmore, Henry Spencer, Richard Guy Briggs, Hugh Redelmeier, Eric Young, "Linux Frees/WAN Project", February 2001, <http://www.freeswan.org>
6. Rob Neilson, BCIT Jeff Wheeler, Francis Reichmeyer, Susan Hares, Merit, "A Discussion of Bandwidth Broker Requirements for Internet2 Qbone Deployment", 1999

http://www.merit.edu/working.groups/i2-qbone-bb/doc/BB_Req7.doc

7. M. Günter, T. Braun, I. Khalil, “ An architecture for Managing QoS-enabled VPNs over the Internet”, Proceedings of the 24th Conference on local Computer Networks LCN’99, pages p.122-131. IEEE Computer Society, October 1999
8. A.K. Parekh, R.G. Gallager, “A Generalized Processor Sharing Approach to Flow Control in Integrated Services Networks: the Single-node Case,” *IEEE/ACM Transactions on Networking*, vol. 1, no. 3, pp. 344 –357, Jun. 1993.
9. S. Lu, V. Bharghavan, R. Srikant, “Fair Scheduling in Wireless Packet Networks,” *IEEE/ACM Transactions on Networking*, vol. 7, no.4, pp. 473 –489, Aug. 1999.
10. S. Floyd, and V. Jacobson, “Link-Sharing and Resource Management Models for Packet Networks, *IEEE/ACM Trans. Networking*, vol. 3, no. 4, pp. 365-386, Aug. 1995.
11. “Linux Advanced Routing and Traffic Control” (<http://lartc.org/>)