下一代虛擬私有網路核心技術之研究－總計畫(2/2)

計畫類別：整合型計畫
計畫編號：NSC 91-2219-E-002-031
執行期限：2002.08.01 至 2003.12.31

總計畫主持人：台大電信工程學研究所 蔡志宏教授
共同主持人：台大資訊管理學系 孫雅麗教授
台大電機工程學系 張時中教授
執行單位：國立台灣大學電信工程學研究所

一.中文摘要

現行企業網路節點散佈各地，提供安全並隱密地連結各節點網路的需求變成極為重要。除了成本昂貴的私有網路（private network）外，虛擬私有網路（Virtual Private Network，VPN）形成一種新興的服務架構，已經廣泛的被採用來解決這樣的需求。過去虛擬私有網路的相關技術多半著重在安全性的存取，如何提供一個具有服務品質（Quality of Service, QoS）保證的虛擬私有網路並未受到重視。

在現今多變的企業連網環境裡，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；b) 可擴充性(scalability) – 可支援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；c) QoS support。本計畫研究下一代以 IP 為基礎的虛擬私有網路，強調彈性的容量管理及資源分配確保每個 VPN 通道的服務品質。

本計畫中，我們首先提出一個新的服務模型（service model），它包含一個三層的重疊網路（3-layered overlay network）架構以及頻寬交易的機制，以提供每一個虛擬私有網路具有傳輸品質保證的服務。其中頻寬交易的機制可以彈性地一旦某個虛擬私有網路的頻寬不敷使用，它可以向其它的虛擬私有網路挪借部份頻寬，藉由暫時增加虛擬私有網路的頻寬以減少它的阻塞率，並且提高網路頻寬資源的使用率。

本計畫第二部分，第二年是研究有頻寬保證的虛擬私人網路服務計價之研究與實做，我們探討ISP如何經由有頻寬保證的虛擬私人網路和盡力傳送的公眾網路服務間的費率來影響購買和使用服務的機率，進而決定頻寬的分配策略與期望的總營業額大小。我們針對所設計的虛擬私人網路計價策略，進行了一個具體而微的計價實驗平台實作，來驗證其可行性並掌握了基本技術。

最後，我們提出一套以私有虛擬網路 VPN (Virtual Private Network)為基礎的解決方案，同時考慮公司內部使用與公司外來訪客的上網需求，且同時滿足兩者網路安全上的不同考量。對公司外來訪客，本計畫提供公司的內部網路 VPN 通道使其經認證機制及政策性路由之保護下，供其連上 Internet 上網。經由適當的系統設定與網路規劃，我們的 VPN (Virtual Private Network)技術可以解決外來的訪客上網需求，並且也能同時保護公司內部網路的安全與服務品質。

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

二. 研究緣由、目的與成果

2.1 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提供點對點或是多點連結服務的技術。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，而多點連線的需求是必要的，例如提供群體通訊，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：有彈性的資源分配、有效的頻寬使用、使用才付費的機制、多點連結的服務提供、達到服務品質的保證、確保存取的安全性等。

過去，雖然虛擬私有網路相關的議題已經被廣泛的討論，但是如何提供具有服務品質保證的議題卻不如安全性議題受到重視。即使我

們能夠給所有在操作網路上的流量給予固定的頻寬保證，但由於網路流量有 bursty 的特性，因此還是會有問題產生。考慮下列的情形：給定一個兩 VPN sites 間的通訊連結，假如我們能為所有這樣通訊連結給予保證固定的頻寬，雖然每個虛擬私有網路都能在 QoS 保證的情形下傳輸，但是我們為這些通訊所保留的頻寬卻不一定會全用到。因為在不知所有流量形態（traffic flows' pattern）的條件下，我們無法預先得知這通訊連結的頻寬需求。如此一來，不僅造成頻寬資源的浪費，在保留特定的頻寬給特定的虛擬私有網路後，勢必也會增加其它人的 blocking rate。除了頻寬浪費外，亦有可能發生頻寬不足的情形。另一方面，也因為對未來需求的不確定性，所以亦有可能會發生頻寬不足的情形。例如像是緊急的視訊會議召開等，在這樣臨時的頻寬需求下，如果能夠暫時增加該虛擬私有網路的頻寬，頻寬的管理上則更有彈性，並提高網路頻寬資源的使用。

在頻寬不足的情況下對該流量的負面影響遠大於頻寬保留過剩的情況，然而同時間對於其它的流量來說，它們所保留的頻寬可能大於它們自己需要的頻寬大小。如果有一個彈性調整保留頻寬的方式，則不僅可以減少每個使用者的 blocking rate，也可以為減少保留過多頻寬而造成浪費的情形。換句話說，藉由動態保留適當的頻寬，我們可以提高整體網路的使用率。這裡我們將使用率定義為已使用頻寬和保留頻寬之比。

虛擬私人網路（VPN）因此提供了一種讓網際網路服務提供者(ISP)跳脫日常網路傳輸量販的方式，而能提供加值服務給公司型客戶。VPN 的基本動機是來自於通訊經濟的考量，它可把多個通訊服務結合在一個高承載容量的通訊平台，使得高固定成本得以讓為數眾多的用戶群共同分擔。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。

2.2 目的

針對一個網際網路服務提供者（ISP）的骨幹網路，我們提出一個全新的虛擬私有網路服務模型，它包含一個三層的重疊網路（3-layered overlay network）架構以及頻寬交易的機制，讓不同的虛擬私有網路能夠在這個重疊網路上交易和管理它們所多餘或是不足的頻寬，動態地、彈性地滿足每一個虛擬私有網路傳輸品質保證的服務。此外。也可以讓網路管理者能夠透過此架構有效率並且有組織的管理所有的虛擬私有網路。

在三層的 overlay network，由於現行 Internet 的發展，以 IP 通訊協定為基礎的實體網路已經是完善的開發和維護，所以 IP 基礎實體網路層是 overlay network 的最底層。第二層是由選擇支援封包交換技術的網路節點後，再併以網路管理者的特殊目的篩選過後而得。在這一層，所有節點之間的流量都是具有頻寬保證的服務，以支援上層應用的需求。最上層則是建構各個虛擬私人網路，每一個虛擬私人網路是從 overlay network 的第二層中選擇數個節點而形成一個樹狀的拓樸。每一個虛擬私人網路下，任兩個 VPN sites 間的流量都是具頻寬保證的。為了有效率達到快速遞送封包、支援頻寬管理、以及為上層虛擬私有網路建立樹狀的拓樸，第二層網路的建構我們假設可以利用像是 Multi-Protocol Label Switching（MPLS）[RFC3031] 的封包交換技術來達到。

近年來由於對於網路安全的重視以及成本上之考慮，使 VPN 的應用愈來愈普遍。VPN 在一般企業上是應用在 Internet 的兩端，如兩家不同的分公司需要作資料傳輸時，先由 VPN gateway 將資料加密後，再經由 ISP 所提供的網路服務透過 Internet，傳到另一家分公司，由於資料經過加密，所以 Internet 上的其他人並無法取得該資料，換言之，就是在 Internet 上以特殊的形式建立一條類似專屬的通道(tunnel)，就像是私人網路一樣；但是在本篇將在 VPN IPSec 的 tunnel 技術做另一型態的應用。

對公司外來的訪客，基於網路安全上的考量，無法提供公司的內部網路使其連上 Internet，常常必需透過使用客戶自己的行動電話才能上網。經由適當的系統設定與網路規劃，我們希望能使用 VPN（Virtual Private Network）的技術來解決這方面的問題，可使外來的訪客能夠連上 Internet，並且也能同時保護公司內部網路的安全。

進一步保障私人網路之通訊安全，研究整合路由器之資源管理、虛擬私人網路、與品質服務功能、、滿足不同型態的虛擬私人網路需求，並且提供動態的頻寬設定服務，則是本計畫的研究方向主軸。

2.3 計畫成果

2.3.1 Q-Overlay 網路架構

服務模型

網路管理者扮演頻寬交易經紀人(broker)的角色藉著維持虛擬私有網路間的借貸關係(credit & debt)提供不同虛擬私有網路間頻寬交易的服務。一旦有頻寬借用的需求產生，頻寬交易經紀人必須從現有的虛擬私有網路中選擇合適的貸方，挪用它的部份多餘頻寬給借方使用。至於如何選擇合適的貸方，我們提出一套計算方法。另一方面，網路管理者也必須紀錄每一個虛擬私有網路貸給其它虛擬私有網路的頻寬量以及它向其它虛擬私有網路借用的頻寬量。這些交易的頻寬數量都會影響該虛擬私有網路對全體網路的貢獻度、該虛擬私有網路的信用度以及急需時可借用的頻寬量。當一個虛擬私有網路的頻寬有剩餘時，它可以將其使用率不高的線路的頻寬分享給其它人使用。一旦其它的虛擬私有網路有緊急的頻寬需求時，就可以使用這些分享且未使用的頻寬。

Q-overlay 從最下層至上層分別稱之為：IP infrastructure network 、 Q-network 以及 Q-VPN。圖 1 是一個 Q-overlay 網路的架構示意圖。最底層的 IP infrastructure network 是一個以 IP 作為通訊協定的基礎架構網路。中間層是一個標記交換網路，稱為 Q-network。為了建構 Q-network，網路管理者需要從最底層的 IP infrastructure network 中選定幾個 core routers，稱之為 Q-node，形成一個抽象虛擬的 overlay network，目的是提供上層虛擬私有網路 QoS 的保證。這些構成 Q-network 的 Q-nodes，都是能夠支援標記交換的路由器，除了可以讓封包快速的儲存和傳送(store and forward)外，亦可以讓網路管理者明確的指定封包繞送的路徑。換句話說，為了能夠提供最上層 Q-VPN 的需求，Q-network 具有標記交換的技術，能讓封包在指定的路徑上快速的被傳送。

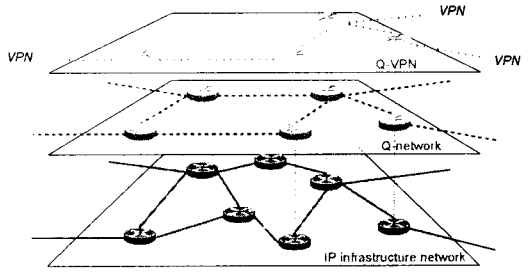

圖 1.Q-overlay 網路架構

Q-VPN 位於 Q-overlay 網路的最上層，每一個虛擬私有網路都有自己的一層 Q-VPN 網路。所謂的一個虛擬私有網路是由許多的 VPN sites 所連結構成。這些 VPN sites 分佈在網路的不同點，它們有可能是企業各處的辦公室、分公司或是事業上的夥伴。這些 VPN sites 彼此之間都想要除了安全可靠的連結來傳送資料外，還要有服務品質的保證。我們假設每一層 Q-VPN 都由一棵樹來連結所有該虛擬私有網路的 sites。Q-VPN 如同 Q-network 一樣，也是抽象的一層虛擬網路，藉由在 Q-network 中選取數個 Q-node 來形成一個虛擬私有網路的拓撲樹。

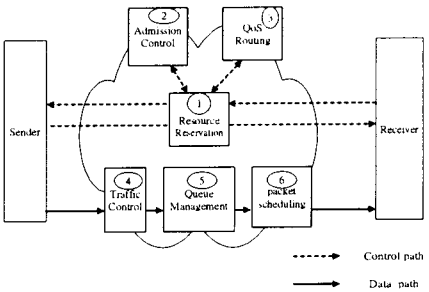

圖 2. 路由器內部架構

實作方法

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。

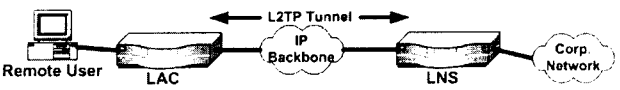

圖 3. 系統架構圖

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。

2.3.2 品質服務虛擬私人網路系統及計價實驗

服務模型 1

為了提供動態的品質服務虛擬私人網路設定服務，我們設計了一個以規則為基礎之服務代理人(Service Broker)，由四個功能方塊所組成：使用者介面、設定規則資料庫、控制信號產生器、以及跨網域通訊介面。

實作方法

在品質服務虛擬私人網路系統的實作(如圖 4)中，我們利用有限的實驗設備，將整個差別服務環境做了如下的簡化：網路資料從伺服器到服務使用者的途中依序經過兩個品質服務虛擬私人網路路由器(QoS VPN Router) B 與 A，我們在 B 點根據來源位址或目的地位址對網路資料進行分類與標記的動作，並且在加密之前，將內層 IP 的標記複製到封裝之後的 IP 服務種類欄位(Type of Service，TOS)，最後根據標記的結果來作網路資源的分配，對流出 B 的資料做合理的控管。而當網路資料抵達 A 時，它會對封包解密與解封裝，並且再次的根據標記資訊作資源的分配。因此在我們的差別服務虛擬私人網路架構中，B 與 A 分別相當於整合了虛擬私人網路功能的入口路由器(Ingress Router)與出口路由器(Egress Router)。

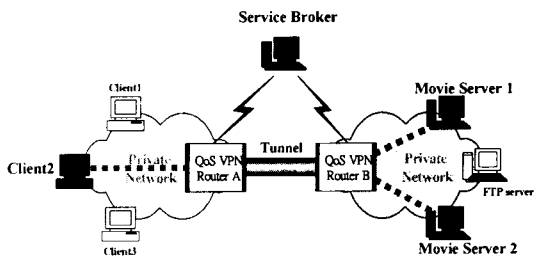

圖 4 品質服務虛擬私人網路系統架構圖

服務模型 2

本研究考慮虛擬私人網路屬於網路類型的虛擬私人網路，由 ISP 直接提供網路管理的功能，建構在 IP 的協定上，利用差別服務(DiffServ)達到品質保證。本研究考慮 ISP 提供「有頻寬保證的網路類型虛擬私人網路」與「以盡力傳送資料的公眾網路」，兩種不同類型的服務，主要目的是為了獲得營業額的成長，規劃一個滿足兩種不同需求的網路環境，提供一個可以獲得最大營業額的計價模型，讓 ISP 能在虛擬私人網路與公眾網路間，尋找最佳的費率與頻寬分配策略。

實作方法

計價研究的重點考慮設固定費率的方式下根據使用時間收費，討論費率與營業額之間的關係。首先建構一個模型，將所有使用者視為一個整體的使用者，在已知訂購者對價錢的需求函數、實際使用的需求頻寬與服務請求的機率條件下，分配頻寬會影響請求服務後願意使用服務的機率，即為使用者的行為，在把這種行為列入計價考慮後，ISP 可以決定在一個時間周期內虛擬私人網路與公眾網路的價格，讓獲得的營業額最大化。這個計價問題在求解上採用窮舉法(Exhaustive Search)，逐一評估所有符合頻寬分配策略的解，找出能產生最大營業額的費率組合，此即為 ISP 最佳的定價決策。

經由觀察用窮舉法尋找的到結果，在有限頻寬改變的情況下，虛擬私人網路的費率會維持在一段有限頻寬中不改變，只改變公眾網路的費率，讓營業額的損失由公眾網路承受(圖 5)。且因為公眾網路訂購需求容易受到價錢的影響，所以當資源不足時，費率會比虛擬私人網路先調升，誘導使用者減少網路訂購的意願，增加個別使用者的願意使用網路的機率。

根據對虛擬私人網路的網路系統設計與計價策略，進行一個具體而微的實驗環境實作(圖 6)，驗證網路架構的可行性，提供一個計價的實驗平台。建構服務代理人與兩個整合型虛擬私人網路路由器。其中，服務代理人是一個介於使用者與 ISP 之間的角色，設計使用 MySQL 的資料庫，儲存網路連線設定與計價收費的相關資料，提供有頻寬保證的 IP VPN。在整合型虛擬私人網路路由器端，以 SSH 與 PPP 實現虛擬私人網路，且以 iproute2 區分服務等級與切割服務的頻寬，並利用 Ntop 作流量分析做為記帳收費的依據，顯示一個可以配合計價策略的環境，同時提供「有頻寬保證的網路類型虛擬私人網路」與「以盡力傳送資料的公眾網路」。

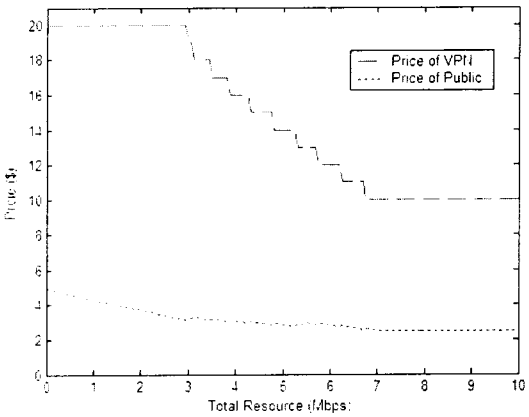

圖 5. 案例三的最佳定價決策

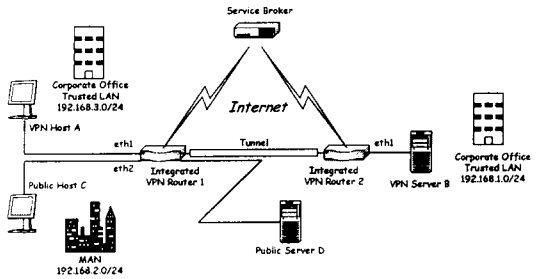

圖 6. 虛擬私人網路計價實作系統架構圖

2.3.3 企業 VPN 分組及分流

服務模型

在這個環境中，我們運用網頁認證的方式，將無線網路使用者分成公司內部使用者和外來訪客兩大類，且分別擁有不同的權限，內部使用者可以任意的存取公司內部網路的資料；外部訪客只能經由 VPN gateway 包裝後以特定的通道連上 Internet。

接下來在第二節的部份，會簡介我們將如何利用 VPN 之 IPSec 技術來實現整個系統以達成我們的目標，在第三節裡，會列出實驗的系統所使之設備以及實驗架構圖，然後，在第四節中，將列出實作步驟及結果，最後的部份則是結論及未來需要再改進的地方。

實作方法

首先，先定義實作之系統主要目的：希望能利用 VPN，將外來的訪客上網的封包作加密並包裝起來，然後直接送到公司的防火牆外之 Internet，以保護內部網路，同時也保護外來的訪客。

接著，我們將外來使用者規劃為使用 Wireless LAN (IEEE 802.11b)上網，並希望使用者能經由以下之流程上網：首先，使用者先設定好 Wireless LAN 之設定。

然後，建置之 DHCP Server 會先給予一個暫時性的 IP 位址給使用者開啟認證網頁。在確認過身份後，DHCP Server 將會收回之前所分配之暫時的 IP 位址，並根據使用者的身份給予新的 IP 位址，而使用者便可使用此新的 IP 位址上網了。

在完成認證之後，因為外來的使用者的封包必被加密包裝，所以 Layer 3 Switch 必須依所給予之新的 IP 位址將封包做分類以及 policy route，如果是外來之使用者，則將之繞送到 VPN Gateway 做封裝並 tunnel 到 Firewall 外，反之，若是本地的使用者則不需要做封裝，並且可以任意存取內部之網路。

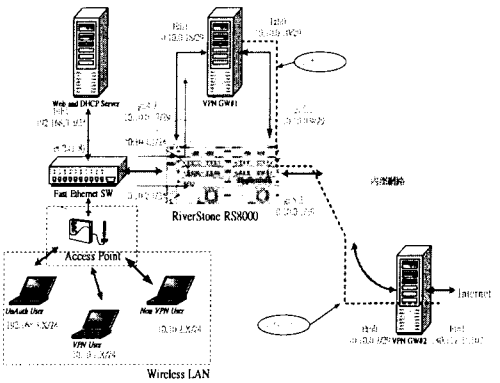

圖 7. 企業分流實驗架構圖

實作步驟與結果如下：VLAN 分割及 Traffic 分流 (policy route)方向，我們先把 Wireless LAN 上的使用者及其 IP Address 分為 3 類：未認證過之使用者 (192.168.3.X/24)、已認證過之內部使用者 (10.10.1.X/24)和已認證過之外來使用者 (10.10.2.X/24)。其中 10.10.1.X/24 之使用者以 10.10.1.1 作為 Gateway 上網。同理，10.10.2.X/24 之使用者以 10.10.2.1 作為 Gateway 上網。

認証服務登入畫面如下：

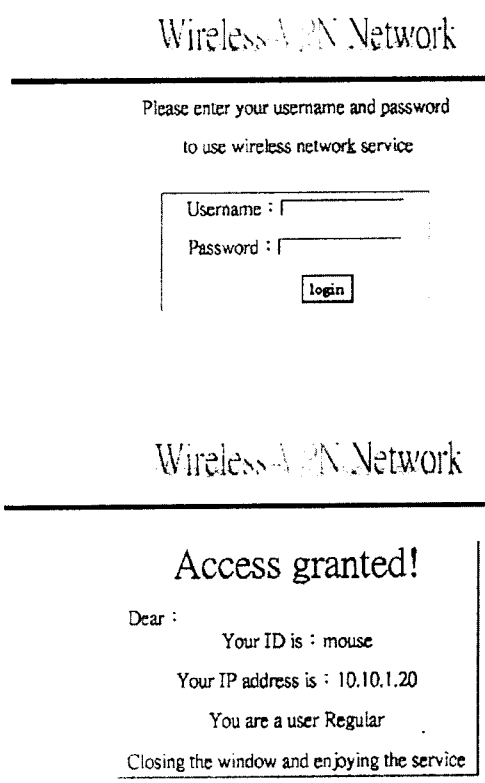

圖 8. 登入畫面

三. 結果與討論

本計畫之研究群同時探討了下一代虛擬私有網路的各項核心技術，包含建立了重疊網路架構，頻寬交易及服務計價機制，以及在企業內部實施用戶分級分流之方法。此三項技術，使得未來虛擬私有網路服務除了可以提昇其服務品質及可擴充性外，更因為建立了寬頻交易計畫機制，以及企業內部分級分流的方案，使此一技術所能提供之服務型態更加多元，並且得到服務概念上之突破。

四. 成果自評

本計畫在執行最後階段，為使自製 VPN 路器能與商業等級之 VPN 路由器測試互連功能，而延長期限，為美中不足之處。

五、參考文獻

[1]Y. C. Lee, "Design and Implementation of QoS VPN Experimental Environment in DiffServ Network," *Master thesis*, Dept. of Electrical Engineering, Nation Taiwan University, Taipei, June 2002.

[2] Y.-C., Dai "Research on Pricing Virtual Private Network with Bandwidth Guarantee and Its Implementation," *Master thesis*, Dept. of Electrical Engineering, Nation Taiwan University, Taipei, July 2003.

[3]T. Braun, M. Guenter, I. Khalil, "Management of Quality of Service Enabled VPNs," *IEEE Communications Magazine*, May 2001.

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

[5] D. Mcdysan, "VPN application guide," Wiley Computer Publishing, 2000.

[6] 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.

[7] Amit Kumar, Rajeev Rastogi, Avi Siberschatz and B ülent Yener "Algorithms for Provisioning Virtual Private Networks in the Hose Model," SIGCOMM 2001.

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

[9] 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.

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

[11] 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.

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

[13] 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.

[14] 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.

[15] K. C. Almeroth, "The Evolution of Multicast: From the MBone to Interdomain Multicast to Internet2 Deployment", IEEE Network, pp. 10-20, January/February 2000.

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

[17] 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.

[18] 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.

[19] 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.

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