行政院國家科學委員會專題研究計畫　成果報告

子計畫二:下一代虛擬私有網路計價收費技術之研究(2/2)

計畫類別： 整合型計畫
計畫編號： NSC91-2219-E-002-033-
執行期間： 91 年 08 月 01 日至 92 年 07 月 31 日
執行單位： 國立臺灣大學電機工程學系暨研究所

計畫主持人： 張時中

計畫參與人員： 林宗慶 朱紹儀 李育全 戴奕驥 陳建志 趙圻軒 李豐凡

報告類型： 完整報告

處理方式： 本計畫可公開查詢

中　華　民　國 93 年 3 月 9 日

下一代虛擬私有網路核心技術之研究-子計畫二：下一代虛擬私有網路計價收費技術之研究(2/2)

計劃類別：整合型計劃
計劃編號：NSC91-2219-E-002-033
執行期限： 91 年 8 月 1 日至 92 年 7 月 31 日

整合型計劃：總計劃主持人：蔡志宏教授
子計畫主持人：張時中教授
子計畫參與人員:林宗慶 朱紹儀 李育全 戴奕驥 陳建志 趙圻軒 李豐凡
執行單位：國立台灣大學電機工程學系

一. 中文摘要

本計畫兩年的研究工作分為三部分，(一) 虛擬私人網路之技術研究，(二)計價收費之機制，(三)正交分頻多工(OFDM)偏移估測。第一年在虛擬私人網路之技術研究上，我們整合 DiffServ 架構中分類、塑流(traffic shaping)、封包排序與虛擬私人網路架構中網路安全協定對封包加密、驗證、建立通道的功能，在 Linux 環境中設計並實作了品質服務(QoS)虛擬私人網路路由器和服務代理人(Service Broker)。進而據以建構品質服務虛擬私人網路實驗環境，來對每一個網路流(per flow)作資源保留，提供各虛擬私人網路使用者一個動態的頻寬設定服務，在安全通道上提供虛擬私人網路與服務品質。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，研究中考慮 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」，而營運目標主要為了獲得最大營業額。「有頻寬保證的網路類型虛擬私人網路」的服務，以企業為訴求，企業內的個人使用者並不直接負擔費用。「盡力傳送資料的公眾網路服務」，是一個沒有頻寬保證的服務，所以服務的費率影只響訂購服務的總人數，但不直接影響訂購後的使用行為。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，在第一年品質服務(QoS)虛擬私人網路路由器和服務代理人外，加入流量量測與記帳收費的模組，成為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。此外，我們也研究了正交分頻多工系統時序和頻率的偏移造成符元(Symbol)與符元、子頻道(Subchannel)與子頻道間互相干擾的問題。我們提出了一個混合式頻率偏移估測演算法，該方法在訊雜比(SNR)低以及循環字首短的時候，估測效能有相大的改善。

關鍵詞：虛擬私人網路、差別服務、計價、品質服務、實驗平台實作、正交多頻分工、偏移估測

Abstract

This two year research included three tasks: (1) research on QoS-based virtual private network (VPN) technology, (2) the design of pricing scheme for VPN service, and (3) research on the synchronization problem of OFDM system

In the first year, we adopted differentiated service (DiffServ) architecture to design and implement a QoS VPN experimental environment. We designed a QoS VPN router and a service broker by combining packet classification, traffic shaping and packet scheduling of DiffServ routing with encryption, authentication and tunneling of VPN. They were implemented into a Linux-based experimental network, where a VPN service with per flow-based QoS can then be provided.

In the second year, a decision model was developed for ISP pricing between two types of Internet services: bandwidth guaranteed VPN and best effort public network (BEPN). The VPN users are corporates and their employees, where a corporate subscribes and pays for the VPN service while its employees are the actual users. Each VPN user is guaranteed a minimum bandwidth. The BEPN users are the general public and have no QoS guarantee. Under this setting, our study found that the price level affects the number of subscribers. The usage behavior of a VPN user is insensitive to the pricing policy and the probability that a BEPN subscriber will actually use the service depends on the bandwidth level to share among BEPN subscribers. Bandwidth is shared between VPN and BEPN but the ISP puts the bandwidth guarantee to VPN users in a high priority. We also implemented the pricing scheme and added a NTOP™-based network traffic metering and accounting module to the QoS VPN experiment environment.

In addition, we studied the synchronization problem of OFDM system, including carrier offsets caused by both frequency and time. We designed a hybrid frequency offset correction method that significantly improved for the OFDM system with low signal-to-noise ratio and short cyclic prefix.

Keywords: Virtual Private Network , DiffServ, Quality of Service, Pricing, OFDM, offset estimation

二. 研究緣由，目的與成果

虛擬私人網路（VPN）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。而針對建立下一代具 QoS 之 VPN 及收費計價機制，我們完成了以下成果:

I. 品質服務虛擬私人網路系統之設計與實作

I.1 品質服務虛擬私人網路環境設計

I.1.1 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

I.1.2 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(圖一)與系統方塊圖(圖二)。此設計主要由三個模組構成：(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)。

網路交通調節器

包含分類器(Classifier)、量測器(Meter)、標記器(Marker)、重塑器/丟棄器(Shaper/Dropper)。

我們採用多欄位分類器(Multi-field Classifier)，根據來源位址、協定名稱(Protocol ID)、與差別服務欄位(DS Field)等作為分類的依據。使用標記器替封包的 IP 標頭 TOS 欄位作標記。

網路安全協定模組

網路安全協定模組主要的功能就是在網路層提供每一個封包的加密與驗證功能，並同時肩負起建立通道的責任。我們用這個模組來提供建立通道、加密、與驗證的功能。

服務代理人

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，並將之設置在網際網路上，如系統服務架構圖。(圖三)

我們設計的服務代理人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。使用者的請求信號會先透過使用者介面下達，再交給控制信號產生器產生更改服務所須的控制命令，所產生的控制命令最後再經由跨網域通訊介面傳送到品質服務虛擬私人網路路由器更改頻寬的配置並做安全參數的調整。

使用者介面 (User Interface)

為了接受使用者的服務請求，我們提供了一個命令模式(Command mode)介面作為和使用者溝通的橋樑，使用者可以透過這個介面送出服務請求，比如：建立安全通道、服務等級規格變更、查詢服務等級、監控網路狀態、接受服務代理人回覆的訊息、終止服務等。

設定規則資料庫 (Configuration rule DB)

在使用者與服務代理人建立起服務連結後，我們提供給使用者多重的服務規格選擇性，這些服務規格被儲存在「設定規則資料庫」中，使用者的服務請求必須符合資料庫的格式。

控制信號產生器 (Control Signal Assembler)

在選定適當的服務規格後，控制信號產生器會根據這個選擇，產生適當的路由器設定信號，並透過安全的連線將控制命令下達給品質服務虛擬私人網路路由器。

I.2 品質服務虛擬私人網路系統的實作成果

在差別服務環境中主要由三種元件構成：(1)邊界路由器 (2)核心路由器 (3)服務代理人。為了提供一個端點對端點的服務品質，必須在資料流所經之路徑上的每一個節點作資源分配，但在有限的實驗設備環境中，我們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)。

II. 品質服務虛擬私人網路系統之設計與實作

I.1 設計目的

在第二年研究中討論的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。

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。

這個計價問題在資源足夠時，可以不考慮頻寬的限制，直接對訂購服務的需求函數求解，能很容易決定出一組最佳的定價策略。但資源不足時，由於使用者在請求服務後願意使用服務的機率是一個非線性的函數，為了解決這個問題，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。

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，驗證網路架構的可行性，提供一個計價的實驗平台(圖五)。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」。

實驗成果:

ISP 提供服務的建立流程，當一個總公司的使用者 A，需要透過虛擬私人網路，與分公司的使用者 B 交換資料，由 A 提出服務的請求，到實際把封包傳送到遠端的 B，一共需要經過七的步驟。

1. A 對 SB 提出服務請求。
2. SB 在確定使用者的權限後，設定網路上的設備，並通知使用者可以使用虛擬私人網路的服務。
3. 在收到連線建立完成的訊息後，使用者傳送封包到入口端的 CE。
4. 封包在入口端的 CE 進行資料加密後，傳送到入口端的 PE。
5. 入口端的 PE 為封包加上新的 IP 標頭後，傳送到網際網路上，網路經由新的 IP 標頭傳送到出口端的 PE。
6. 出口端的 PE 進行復原封包標頭的工作後，把風包傳送到出口端的 CE。
7. 出口端的 CE 把封包解密，最後傳送給遠端的使用者 B，完成虛擬私人網路的封包傳遞動作。

不過在現實的環境中，ISP 除了虛擬私人網路外，還有公眾網路的部分，提供三種不同對象服務，包過了企業、虛擬私人網路使用者、公眾網路使用者，因此必須設計提供兩種服務與三個不同對象的代理人。由於公眾網路的使用者在購買服務後，本身就是實際的網路使用者，所以在描述設計規格時，考慮以虛擬私人網路的部分來做說明，因為公眾網路的使用者當要購買服務時，即如同企業的角色，而當要使用網路時，就如同虛擬私人網路的使用者，只是使用的網路沒有安全與頻寬保證，所以在服務代理人的設計上，只在使啟動服務時的設定部分有所不同。

接下來對於服務代理人的設計說明，服務代理人必須包含幾個功能:允許連線控制(Connection Admission Control)、契約協商與收費(Contract Negotiation & Charging)、啟動服務(Service Activation)、量測記帳與收帳(Metering, Accounting & Billing)、收費與服務設定資料庫(Charging & Service Configuration Repository)、計價與頻寬分配策略(Pricing & Resource Allocation Policy)，如(圖四)所示。

對目標函數 J 求解，首先我們要討論的是價錢與簽約人數之間的關係，最基本的性質是，當價錢增高，會減低購買服務的意願，使 ISP 需要服務的人數減少；當價錢減低，增加購買服務的意願，使 ISP 需要服務的人數增加，而且在不收費時，會有最大的購買服務的總人數，$n_{V,MAX}$、$n_{P,MAX}$。所以我們首先考慮的需求函數，擁有單調的下降特性(monotonic decreasing)，且 $f_V(p_V)$、$f_P(p_P)$ 是一個大於等於零的函數，如下所示，考慮的是一個線性的需求函數，來探討達成目標函數 J 下，各種參數的分析。

$$f_V(p_V) = n_{V,MAX} - \alpha_V p_V \geq 0;$$
$$f_P(p_P) = n_{P,MAX} - \alpha_P p_P \geq 0$$

我們的參數設計如下:

$$f_V(p_V) = 20 - 1p_V \geq 0;$$
$$f_P(p_P) = 160 - 32\,p_P \geq 0.$$

輸入變數：$d_V = 512Kbps$，$d_P = 64Kbps$，$P_{RV} = 0.8$，$P_{RP} = 0.4$。

預期結果:

1. 在資源充分時，$J_V = p_V{}^* \cdot n_V{}^* \cdot P_{RV} = 80$，$J_P = p_P{}^* \cdot n_P{}^* \cdot P_{RP} = 80$。
2. 虛擬私人網路的頻寬需求較高，在頻寬足夠下會分得較多的頻寬。

數值模擬結果:

1. 在資源充分時，$J_V = J_P = 80$ 符合預期。
2. (圖六)中 p_V 是以階梯的形式向上攀升，而每上升一階代表 n_{SV} 減少一人，所以對於中(圖六) J_V 的影響，也是下降減少了一個服務人次可以獲得的營業額，但同時會增加 J_P，而在 p_V 沒有上升一階前，因為資源下降而減少的營業額，由 J_P 反應。
3. 發生 p_V 改變的頻率，當 R 越來越小，頻率越快。
4. 因為 $d_V = 8d_P$，因此我們可以概略知道減少一個 n_{SV} 可以解決頻寬競爭的狀況，因此每當 p_V 是以階梯的形式向上攀升一階，代表多出 d_V 的頻寬給公眾網路使用，而當總頻寬 R 減少的量沒有大於 d_V 時，(圖七)中的 P_{AP} 會因此上升。
5. 當 $n_{SV} = 0$ 以後，P_{AP} 會快速下降。
6. 圖八公眾網路使用者會使用服務的機率。

III. 正交分頻多工系統中使用最大可能估測法之頻率與時序同步問題之研究

由於正交分頻多工系統(OFDM System)本身的特性，能夠減輕通過不理想通道所造成的損害，所以被人們廣泛的使用在有限以及無線通訊系統中。然而，正交分頻多工系統卻存在一個問題，就是對於時序和頻率的偏移非常的敏感，只要頻率與時序稍微不同步，就會造成正交分頻多工系統每個符元(Symbol)與符元、子頻道(Subchannel)與子頻道之間的互相干擾，因而對系統傳輸效能造成嚴重的傷害。所以，如何有效的估測正交分頻多工系統中時序與頻率的偏移，是一個重要的問題，也是本部分研究的重點所在。

交互逼近(iterative approaching)演算法

我們提出了一個交互逼近演算法以期能夠從最大可能(Maximum Likelihood)估測函數中找到最大可能的頻率與時序偏移估測值，經由這樣的逼近法，可以正確的找到最大可能估測函數中的全域最大值(global maximum)，搜尋時的計算複雜度也能成功的降低。

同步演算法

我們對一個既有的同步演算法做討論。這個方法原本是設計來改善 Rayleigh 衰弱(fading)通道之上的估測效能。雖然它在 Rayleigh 衰弱通道上有所改善，但在 AWGN(Additive White Gaussian Noise)通道的估測效能上，表現卻不甚理想。我們明確指出這個問題發生原因，是由於一個函數值被過分簡化成常數，進而提出一個動態修正法，使其在 AWGN 通道上的估測效能有所改進。

混合式頻率偏移估測演算法

我們提出了一個混合式頻率偏移估測演算法，該方法同時利用循環字首(Cyclic Prefix)以及指標子頻道(Pilot Subcarriers)兩種存在於正交分頻多工系統符元中的特徵來估測頻率偏移。因同時利用傳輸端所提供的兩種資訊，與單單使用循環字首或指標子頻道的演算法比較，在訊雜比(SNR)低以及循環字首短的時候，估測效能有相大的改善。(圖九)

三、計劃成果自評

本計劃成果完成原本的目標，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，完成下一代虛擬私人網路計價模問題之模擬研究。已發表論文如下:

[1] T.-C. Lin, Y. S. Sun, S.-C. Chang, S.-I Chu, Y.-T. Chou, M.-W. Li, "Management of Abusive and Unfair Internet Access by Quota-based Priority Control," *Computer Networks*, 2004

[2] S.-I Chu, S.-C. Chang, "Design of Integrated Pricing and Bandwidth Allocation over Differentiated Services," *submitted to IEICE Transactions*, 2003.

[3] T.C. Lin, Y. S. Sun, S.-C. Chang, S.-I Chu, Y.-T. Chou, M.-W. Li, "Priority-Based Internet Access Control for Fairness Improvement and Abuse Reduction," *Proceedings of QoS_IP2003*, Milan, Italy, Feb 2003.

[4] 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.

[5] 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.

[6] C. C. Chen, "Hybrid Offset Estimation Method for Synchronization of OFDM System," Master thesis, Dept. of Electrical Engineering, Nation Taiwan University, Taipei, July 2003.

四、參考文獻

[1] D. Kosiur, *Building and Managing Virtual Private Networks*, Wiley Computer Press, 1998.

[2] S. Blake, D. Black, M. Carlson, and etc., "An Architecture for Differentiated Services," *IETF RFC 2475*, December 1998.

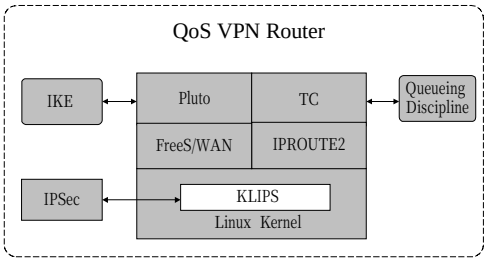
[3] E. Rosen, A. Viswanathan, R. Callon, "Multiprotocol Label Switching Architecture," *IETF RFC 2475*, January 2001.

[4] TeleChoice, Inc., "Expanding the IP VPN Value Proposition: An Introduction and Analysis of Network-Based Service Delivery," TeleChoice White Papers, March 2002.

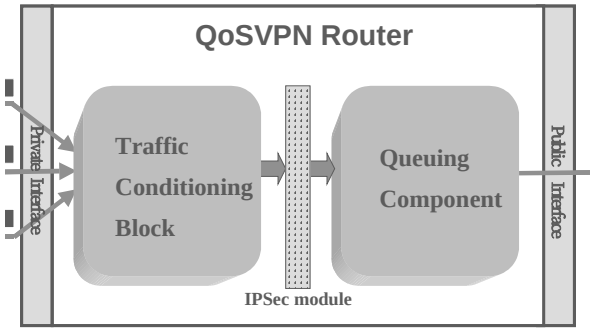
[5] J. D. Clercq, O. Paridaens, "Scalability Implications of Virtual Private Networks," *IEEE Communications Magazine*, May, 2002.

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

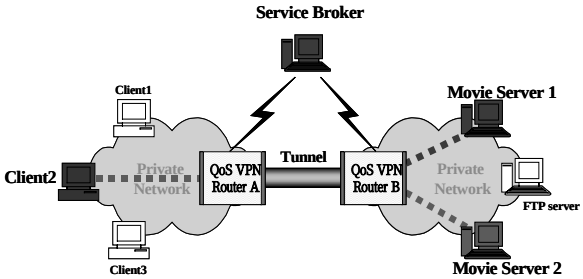
[7] U. Tureil, H. Liu, and M. D. Zoltowski, " OFDM blind carrier offset estimation：ESPRIT, " *Personal, Indoor and Mobile Radio Communication*, vol.2, pp.816-820, 1998.



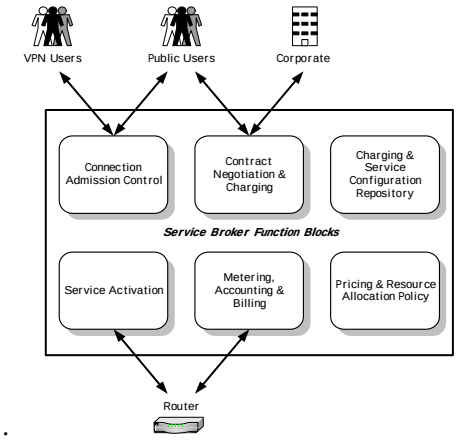
圖一 整合型品質服務虛擬私人網路路由器軟體架構圖



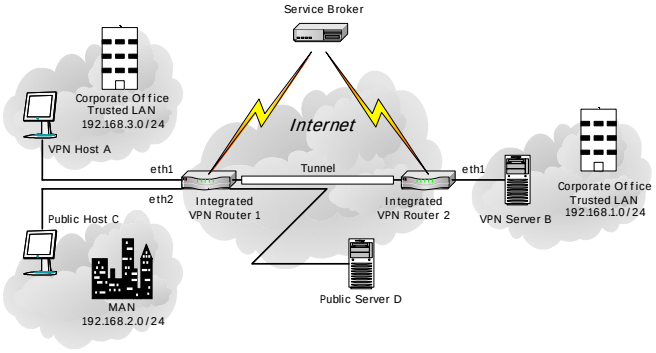
圖二 整合型品質服務虛擬私人網路路由器



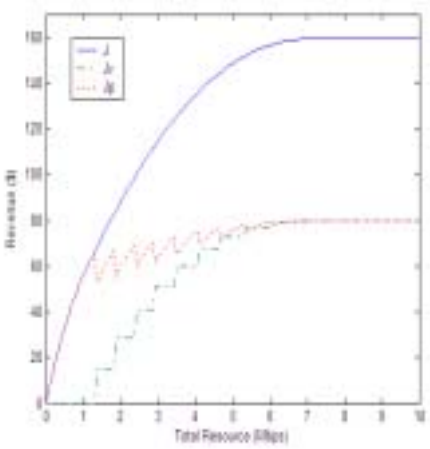
圖三 系統服務架構圖



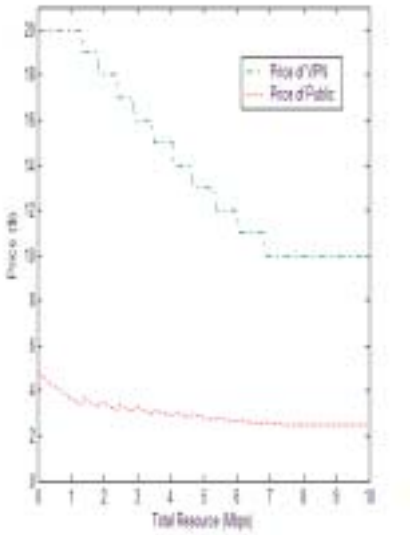
圖四．服務代理人功能方塊圖



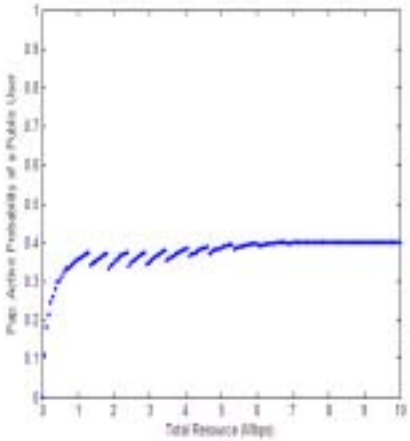
圖五．虛擬私人網路計價實作系統架構圖



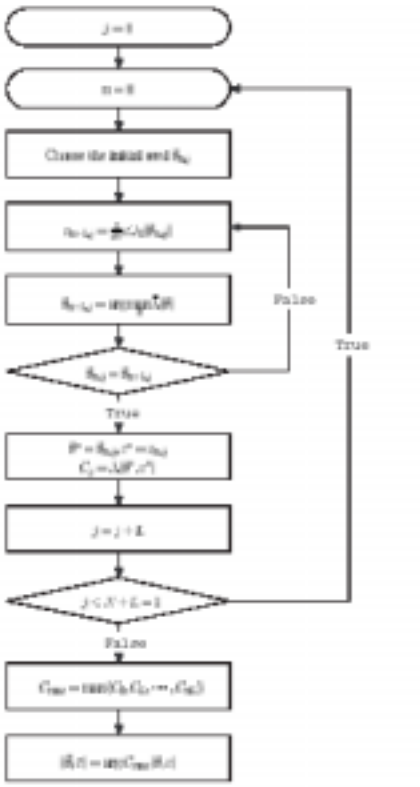
圖六．有限資源與營業額關係



圖七．最佳定價決策



圖八． 公眾網路使用者會使用服務的機率



圖`九. 互動式演算法