行政院國家科學委員會補助專題研究計畫成果報告

網際網路服務品質保證之促成工具(Ⅲ)

計畫類別：□個別型計畫　■整合型計畫

計畫編號：NSC 89－2213－E－002－167

執行期間：89 年 8 月 1 日至 90 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　雷欽隆教授

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　孫雅麗教授

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：國立台灣大學電信工程研究所

中　華　民　國　90　年　9　月　28　日

行政院國家科學委員會專題研究計劃成果報告

網際網路服務品質保證之促成工具(Ⅲ)

Internet Quality of Service Enablers (Ⅲ)

計劃編號：NSC 89-2213-E-002-167
執行期限：89 年 8 月 1 日至 90 年 7 月 31 日

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

一、中文摘要

本計劃研究並實作一整套提供網際網路服務品質保證所需之機制與促成工具，其功能涵蓋點對點即時傳輸，多向性傳輸，費率訂定及收費，網路安全，及服務品質與用量量測。本計劃所完成之各項機制及促成工具將以一共用之實驗網路環境完成測試與整合。最終之目標，則是將整合之網際網路服務品質保證促成工具，直接提供使用者之網路應用在與具服務品質保證特性之網路介接時，所需之完整配套功能。

各子計劃所探討之研究課題及促成工具包括：

1. 服務品質保證之網際網路多向式傳輸促成工具
2. 網際網路服上高效率之安全促成工具
3. 差別服務架構下的網際網路費率策略及促成工具
4. 網際網路服務品質查詢量測及分配之促成工具
5. 寬頻網際網路邊緣路由器支援差別性服務品質保證封包排程與緩衝區管理之設計與實作

關鍵詞：網際網路、服務品質、促成工具

Abstract

This project designed and implemented a complete set of mechanisms and enablers for Internet Quality of Service(QoS) guarantee and investigate related issues. The functions of these enablers include real-time Internet protocols, multicast, pricing and accounting, network security, and QoS measurement. The completed enablers and mechanisms of this project are tested and integrated over a shared testing network environment. The final goal of this project is to directly provide the users or their network applications the necessary integrated functions via these enablers, when an end system is connected to a network with QoS guarantee.

The investigated issues and targeted enablers of various subprojects include:

1. QoS-based Multicast Enablers for the Internet
2. Efficient IP-based Security Enablers for Internet
3. Pricing Policy and Enablers for Differentiated Services in Internet.
4. Enablers for Internet QoS Query, Measurement and Allocation.
5. Design and Implementation of Packet Scheduler and Buffer Management for Broadband Internet QoS Router Supporting Differentiated Service.

Keywords: Internet ,QoS, Enabler

二、計畫緣由與目的

在早期的網際網路發展中，網路安全並未受到太大的重視。然而，隨著電子商務的快速發展，越來越多的商業應用軟體及商業交易使用網際網路為媒介，網路安全已成為一亟待解決的問題。然而，現有的網路安全解決方案大多將安全機制設計於應用層，因此針對各個不同的應用程式，必須做個別修改，方能達到保密及認證的功能，十分不便。有鑑於此，本子計畫提出網際網路安全促成工具的概念，作為一有效的網際網路安全解決方案。

網際網路安全促成工具的概念，在於提供一個可彈性運用，擴充性高的網路安全介面，讓所有網路應用程式，毋須做任何修改，即可使用，並立即享有認證，保密，使用權控制等網路安全服務，且使用者可視其需要隨時加入新的安全功能。由於網路應用程式必須透過 IP 層發送封包來傳送資料，而所接收的資料也必須經由 IP 層方能往上送達位於應用層的網路程式。因此，我們在網路層做適當的修改，以達成網際網路促成工具的功能。我們並且融入了網際網路安全協定(IP Security)、Public Key Kerberos 及入侵偵測(Intrusion Detection)的概念到我們所設計的網際網路安全促成工具之中。

另外，對目前相當熱門的電子商務，在本計畫中，我們也加入了 SET Enabler。我們認為現有的網路付款系統，在使用的方便性與不可否認性等方面，及保障消費者付款資料的保密性及私密性上，仍有改進的空間。所以我們提出了架構在 SSL 層上的 Secure Information Layer (SIL)，作為提供安全付款的機制。

在差別服務等級環境下，網路服務提供者間計價協議問題之研究是在相互網接但卻各自擁有管理權與所有權的網路間所會發生的一個重要商業問題。網路傳輸服務提供者要向使用者收取網路服務使用費並且要付網路服務使用費給相互網接的網路傳輸服務提供者。本研究主要是探討『相對品質網路服務』(Qualitative Service)的網路架構下比較基礎的關於 ISP 雙邊拆帳的模型(如圖五)。我們的研究考慮由服務供應者定價的方式，找出使用者對於不完全替代的服務品質之需求函數，並根據網路的使用情形來決定拆帳費率的大小以及網際間的頻寬買賣的多寡。

在國內的校園網路環境裡，由於是免費的使用且常缺乏適當的流量控管機制，因此存在著不合理與不公平的網路使用情形，也造成了不良的網路使用品質。以台灣大學宿舍網路為例，少數的網路使用佔用了網路資源，造成了大多數使用者要忍受不好的網路品質，如何結合網路技術發展趨勢進行有效的網路管理，使得網路被合理與公平的使用，是重要而具挑戰性的研究課題。

三、計畫執行成果與討論

A. 網路單向延遲之量測

網路延遲(Network Delay)是一個變動非常大的變數，要對這種變數找到一種數學模型來預測是一件非常困難的事，所以我們將改對其網路延遲抖動(Network Delay Jitter)進行統計分析以進行預測。本計畫使用的方法為採用 Chernoff Bound 來找出網路延遲機率上限。

本計畫採用之 Chernoff Bound 公式如下

$$P[\delta X(\tau) > X_B] < e^{-\lambda X_B} E[e^{-\lambda \delta X(\tau)}]$$

$$\lambda \geq 0$$

其中 $\delta X(\tau)$ 為 τ 時間間隔之後的網路延遲抖動。在公式中 X_B 則為網路延遲抖動的目標臨界值。由於在公式 我們將 λ 以任一值帶入，並且一直比較其錯誤機率直到找到最小的錯誤機率，即為預測的錯誤機率。

如果當我們得到 τ 時間間隔之後的網路延遲抖動，再加上目前的網路延遲觀察值，這樣就可以得到 τ 時間間隔後的網路延遲。

網路單向延遲預測與網際網路服務品質查詢系統之整合

由於既有之網際網路服務品質查詢系統缺乏網路單向延遲之預測功能，故本文將前述之預測方法加以整合。整合後之服

務品質查詢伺服器[1]中，資訊交換模組與效能評估及解釋模組經過修改並且增加歷史資料查詢模組，圖一為服務品質查詢伺服器之內部模組，歷史資料查詢模組主要的功能是可以讓網路管理者得知過去網路的好壞，資訊交換模組整合前述之網路單向延遲之交換，而效能評估及解釋模組則整合之前所述之網路單向延遲預測功能。

實作與驗證結果

與既有之服務品質查詢系統整合後，本文在國家實驗網路與台灣學術網路上進行實際的測試，以驗證整合後之服務品質查詢系統之可行性。架構如圖一。本計畫利用三台電腦主機進行量測實作，並各連接一 GPS 接收器以做為時間同步之參考時鐘。圖二為 3 月 20 號量測從台灣大學 IP 位置 140.112.21.103 到台灣大學 211.73.64.200 的 IP 位置的網路單向延遲進行 1000 秒以後網路延遲預測的結果。

B. 網際網路服上高效率之安全促成工具

本計劃經過三年的執行與研究，我們已設計並實作出幾種基本的網際網路安全促成工具(包含認證、加密、密鑰管理等安全策略促成工具)，我們另外完成了數種先進的安全促成工具，一為安全通道促成工具(Tunnel Enabler)，其設計目的在提供無法安裝網際網路安全促成工具的使用者，可以經由一個安裝網際網路安全促成工具的閘道器或路由器，間接得到網際網路安全促成工具之保護。另一為公開密鑰促成工具(Public-Key Enabler)，其設計目的在引入公開密鑰的機制，以加強本促成工具之認證功能，同時能夠讓系統的擴充性能夠更加的良好。其次為入侵偵測促成工具，其設計目的在引入代理人的機制，以加強系統對病毒及各種入侵攻擊之辨識、追蹤及反擊之能力。

我們所提出的網際網路安全促成工具的系統架構設計分為三個主要的部分：認證及密鑰管理部分、網路層協定加密部分以及安全策略部分。在實作方面，我們的實作平台為 FreeBSD 2.2.8 作業系統。網際網路安全促成工具的網路架構如圖(三)所示。其系統架構如圖(四)所示。

C. 在差別服務等級下，網路服務提供者間計價協議問題之研究

在差別式服務網路架構下，本研究提出了一個重覆協議的拆帳費率協議模型(Repeated Settlement Rate Negotiation Model)。每一個 ISP 都是要將個別的利潤最大化，如何協議使得雙方都能更有效地利用自己的資源，是本論文的研究主題。我們的研究步驟如下：

1) 回顧差別式服務網路架構以及定義出『使用者與 ISP 之間』的交易模式和『ISP 之間』的交易模式。
2) 描述兩個相互網接的差別式服務網路之間互動關係。這中間包含了描述使用者對於不同服務品質的連線時間與價格結構之間的關係、對方設定的拆帳費率對於我設定本地費率的關係和我方所設定的拆帳費率對於我整體利潤的影響關係。
3) 設計 ISP 的談判策略以及分析費率結構與『使用者的需求彈性大小』、『平均連線要求到達率』、『網際間頻寬需求大小』和『拆帳週期大小』之間的關係。

目前考慮的是提供傳輸服務上的計價問題(ISP 本身是擁有網路線路資源)而暫不考慮資訊內容的計價問題。

為了解決如何設定拆帳費率的問題，我們必須在差別式服務網路架構下提出合適的交易模式，以及訂出三個管理單元：1）政策管理者、2）資源管理者和 3）服務管理者去控管這個網路並且和相互網接的網路做必要的通訊。有了這些基本的交易市場環境後，我們利用加州柏克萊大學『網路需求實驗計畫』中所提出的結果：使用不同傳輸速度的連線時間和價格結構的關係來描述使用者的需求行為，利用不同傳輸速度的連線時間來估計使用者會選用哪一種傳輸速度的機率，並假設 ISP 可以估測約有多少比例的網路頻寬需求是網際間頻寬需求；利用這些分析將使用者的行為受到價格結構影響的關係描述出來。將這

1 分鐘，就網路使用者可能超額使用的時間則為 1 分 14 秒。

最後，就擴充性問題來分析此系統的效能，發現當網路使用者日趨增多時，討論在一個 Class B 的網路使用者的環境裡，如果考慮 Netflow 計算流量的機制，計價系統的統計週期為 3 分鐘。在服務品質路由器之效能方面，CPU 的負載與記憶體的使用也是可以勝任的。

E. 寬頻網際網路邊緣路由器支援差別性服務品質保證封包排程與緩衝區管理之設計與實作

許多的網路服務需要有封包分類(Packet Classification)的功能，像防火牆、提供不同品質的服務(Quality of Service)，網路計價(Internet Pricing).....等，都需要路由器決定進來的封包屬於那一個服務等級、並且決定如何去處理它。傳統的封包分類器有下列的缺點如無法支援彈性的規則，規則優先權的設定，以及不良規則管理效率(例如規則之新增、刪除或是更改等問題)。綜合高速網路高效能封包分類的需求以及過去文獻的探討，我們認為一個好的封包分類器應該具備下列的條件： (1)有效率的記憶體使用：在理想狀況下，當設定 N 條規則，每個規則有 d 個欄位，所花費的記憶體呈 O(dN)成長；(2)快速搜尋；(3)有效率的規則管理與更新；(4)可支援大量的規則設定; (5)支援彈性的規則設定。

在本研究中，我們針對這些缺點提出了一個新的封包分類器的架構叫做索引搜尋樹我們提出了 interval tree 和 group threaded binary search tree 這二種資料結構(見圖七、八)，這二種資料結構可以處理區間的比對和可支援彈性擴充至多個欄位的問題，並允許使用者可以設定彈性的規則－包括各個欄位區間的設定、規則之間的優先權、not 運算子的使用。另外我們針對規則管理提出一些解決方式，包括偵測規則衝突、如何解決規則衝突，規則更新時的 lock 機制。一個好的規則管理方式有助於網路管理者訂定出符合期望的網路政策。我們也實作所提出的架構與方法在過去兩年所開發的 QoS router 上，其效能測試結果顯兩種方法在大部分情況下都可以表現良好，其中 interval tree 的方法在特別的設定可以表現地更好。我們另外用上萬的規則測試我們的架構，在規則數目很多時仍然很有效率。

在規則管理上，我們提出規則衝突的定義和解決規則衝突的原則，管理者可以應用不同解決規則衝突的方法提供不同的彈性。

四、計畫成果自評

由於多媒體應用等對網路單向延遲敏感之交通在網際網路上所佔之比重日益增加，然而目前網路服務品質提供者並無法提供一套可以預測多媒體應用的服務，本計畫開發網路預測技巧與整合既有的量測系統，完成了一個有理論基礎的網路延遲預測工具。

此外，本計畫提出一個在網際網路上高效率的安全促成工具，做為一個有效的網際網路安全解決方案。網際網路安全促成工具提供使用者一個具彈性且擴充性高的安全機制與介面，讓使用者在毋須修改應用
程式的情況下，即可達成其所要求的安全功能。使用者可視其需要隨時加入新的安全功能。另外，本促成工具對於網際網路應用程式而言是透通的(Transparent)。我們所設計的網際網路安全促成工具提供使用者包含身份認證、加密、資料完整性、密鑰管理、存取控制等基本安全功能。我們另外公開密鑰促成工具以加強本促成工具之認證功能，同時讓系統的擴充性能夠更加的提升。在實作方面，我們已在 FreeBSD 作業系統上完成多種網際網路安全促成工具的實作及其相關之安裝及管理工具軟體，經測試使用及評估，符合當初計畫之目標。

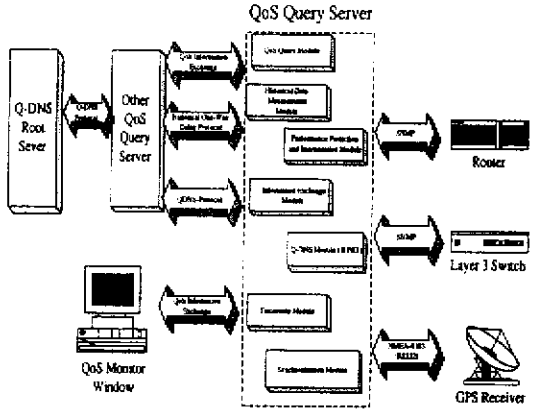
最後，我們建構了多個 ISP 之間計價拆帳模型與市場機制且提出演算法解決問題.。此外在台大校園網路上，我們實作一虛擬計價系統且與其他子計劃的促成工具

〈服務品質路由器〉作整合去進行網路交通控制的實驗，並已有初步的實驗結果及分析。

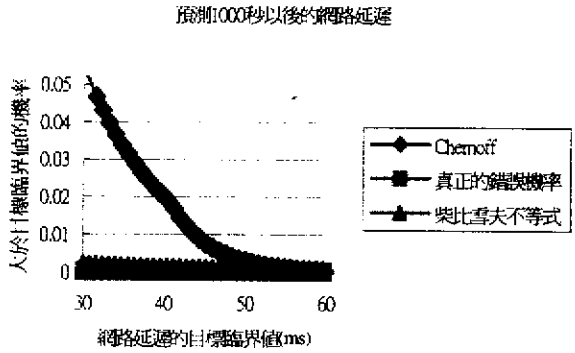
五、參考文獻

1. 吳潮銘，蔡建良，黃金維，蔡志宏，"網際網路服務品質查詢系統之設計與實作", TANET'99, October 1999.
2. Qiong Li, David L. Mills, "Jitt Based Delay Boundary Prediction of Wide-Area Networks," *http://www.ee.udel.edu/~qli/paper/delay_pred.html.*
3. 張譽鐘，網際網路安全促成工具之設計與實作，台大電機所碩士論文，八十八年六月。
4. 陳立峰，分散式免疫型自我學習入侵偵測系統，台大電機所碩士論文，九十年六月。
5. P. C. Cheng, J. A. Garay, A. Herzberg, H. Krawczyk, "A Security Architecture for the Internet Protocol," IBM Systems Journal, Vol. 37, No.1, 1998.
6. D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, Nov. 1998.
7. S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, Nov. 1998.
8. S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402, Nov. 1998.
9. S. Kent and R. Atkinson , "IP Encapsulating Security Payload (ESP)," RFC 2406, Nov. 1998.
10. J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)," RFC 1510, Sep. 1993.
11. W. Stallings, Cryptography and Network Security, 2nd Edition, Prentice-Hall, 1999.
12. 周怡廷, "校園網路虛擬計價系統之設計與實作", 碩士論文, 台灣大學, 2001.
13. 錢膺仁, "相對品質網路服務雙邊拆帳模型之研究", 碩士論文, 台灣大學, 2001.

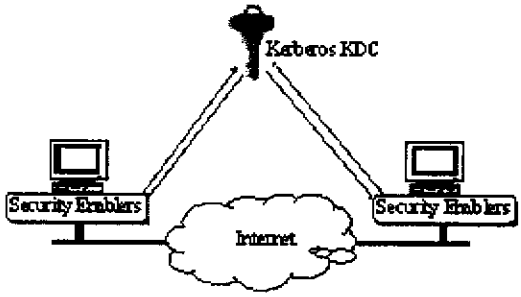
六、圖表



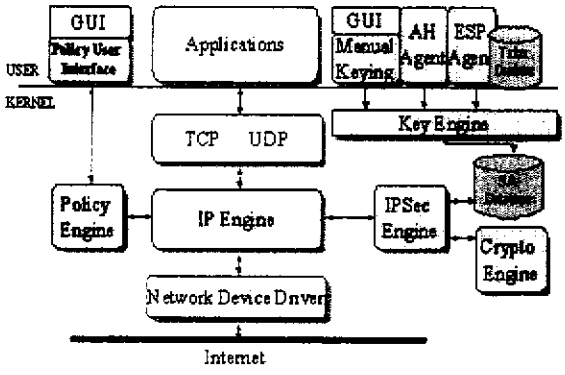
圖一：整合後之服務品質查詢伺服器內部



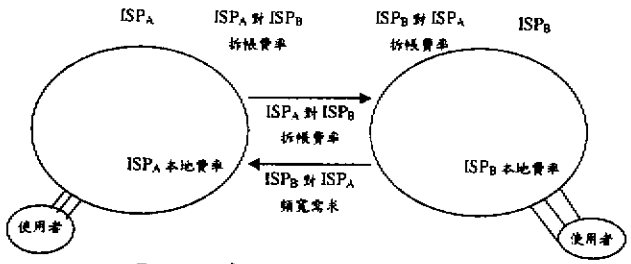
圖二：由台灣大學量測到國家實驗網路的網路單向延遲進行預測



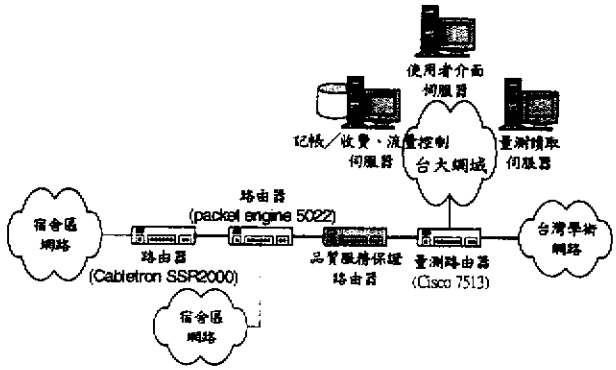
圖三：安全促成工具之網路架構



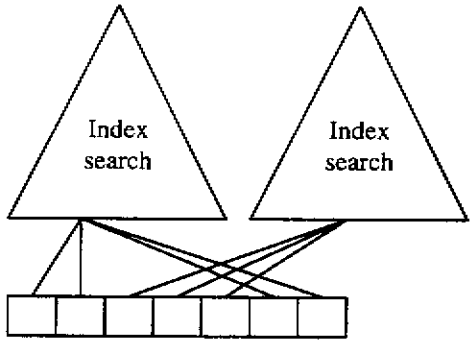
圖四：安全促成工具之系統架構



圖五：多 ISP 之拆帳模型

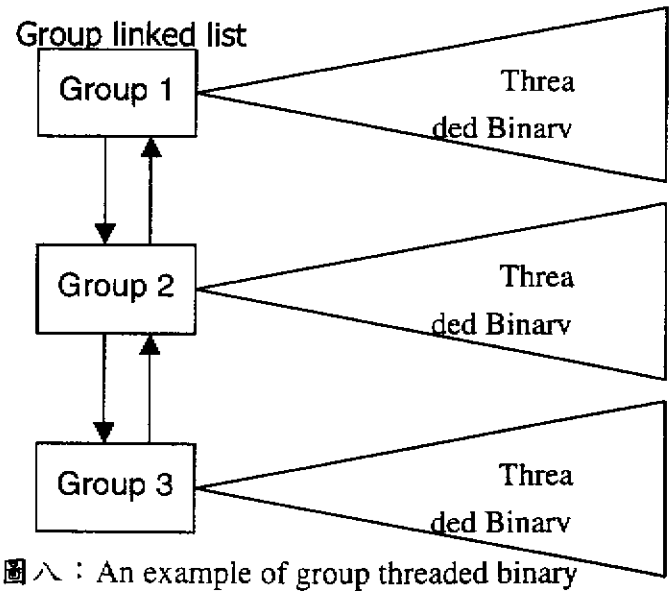


圖六：實驗環境的拓樸圖



規則表格

圖七：Index search 系統架構圖



圖八：An example of group threaded binary search tree