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(II)　　　※
※　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：☐個別型計畫　■整合型計畫

計畫編號：NSC 89－2213－E－002－077

執行期間：88 年 8 月 1 日至 89 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　顏嗣均教授

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　89 年 10 月 30 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(Ⅱ)
Internet Quality of Service Enablers (Ⅱ)

計劃編號：NSC 89-2213-E-002-077
執行期限：88 年 8 月 1 日至 89 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： 顏嗣均 國立台灣大學電機工程學系教授
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. 服務品質導向的網際網路費率策略及促成工具
4. 網際網路服務品質量測及用量統計之促成工具
5. 支援網際網路服務品質保證的封包排程與服務分流之設計與實作

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. QoS-based Pricing Policy and Enablers for Interne
4. Enablers and Infrastructure for QoS Measurement and Usage Summarizatior.
5. Design and Implementation of Packet Scheduler and Service Classifier for Broadband Internet QoS Router

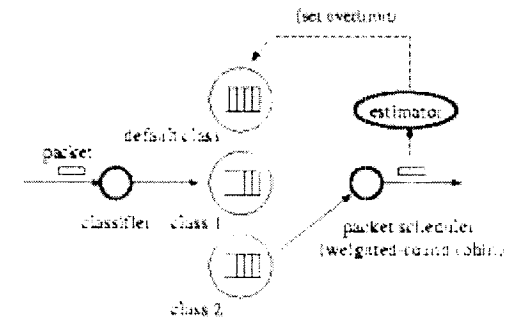
Keywords: Internet, QoS, Enabler

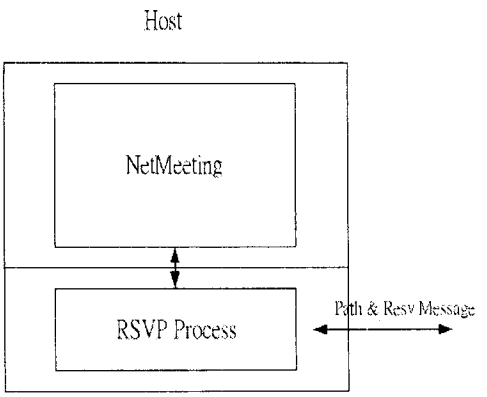
二、計畫執行成果

子計畫一考慮網路技術在處理即時互動及影像和聲音應用程式時，必須要考慮服務品質。多元傳播的方法也不例外。當使用多元傳播的方式時，允許將資訊同時傳送到一些目的地，對每個目的地以多元傳播的方式達到適當的服務品質是非常重要的。如果由於網路的壅塞，會致使一些目的地接收到低品質的多元傳播。服務品質在多元傳播中扮演了一個重要的因素。所以，支援多元傳播傳輸的服務品質已經成為最近網路的研究焦點。子計畫一架設了一個可以支援多向式傳輸的小型區域網路，利用資源頻寬保留和可選擇的排隊方法建立一個有服務品質的網路。在此，並成功的建立了一對一的服務品質供證的測試環境。

首先測試的是一對一的服務品質保證，所採用的 Host 端的作業系統是 Windows 2000 Professional 版本，Router 端的作業系統則為 FreeBSD 3.4 Release 的版本。當子計畫一把 RSVP 和 ALTQ 安裝好了之後，首先先測試傳送端、Router 和接收端之間的 RSVP 協定的訊息傳遞狀況，根據 RFC2205 來觀察 RSVP 訊息是否在這個網路上面有正確的訊息傳遞，以確保傳送端和接受端之間作正確的溝通。

接下來開始去測試影音軟體，透過 Windows 2000 中的 NetMeeting 軟體來測試，架構如圖一。並開始測試保留頻寬的效果，我們可以從路由器中藉由 ALTQ 的分析器來觀察到頻寬動態保留的情形，因為子計畫一採用 queueing 的方法是 CBQ，故可以看到路由器中各個 queue 所配置的情形，並且可以看到 ALTQ 幫 RSVP 協定建立的 queue，故當建立一個 session 時，ALTQ 就動態的為這個 session 建立一個 queue，並且這個 queue 的頻寬配置是根據保留訊息所建構的。





圖一　子計畫一實作系統架構圖

子計畫二所提出的網際網路安全促成工具之系統架構設計分為三大部分：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。子計畫二已將此系統實作於 FreeBSD 2.2.8 作業系統上。

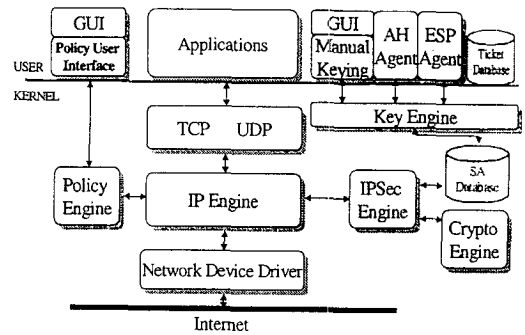
子計畫二所提出之網路安全促成工具，提供使用者一個強健的網路安全架構，以及多種的網路安全服務，並具有系統設定容易，適用於區域網路及企業內部網路，且可適用於低計算能力的行動計算裝置等優點。

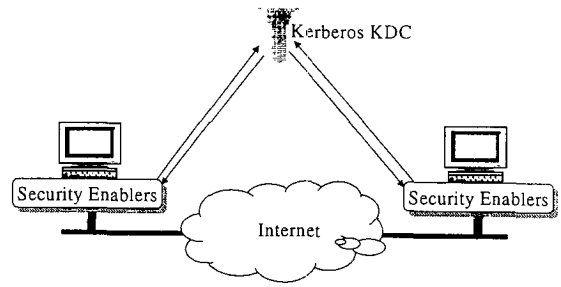
此外，子計畫二的系統亦將 Public Key Kerberos 的觀念整合進來，使得系統具有相當良好的擴充性。對於近來日漸受到重視的電子商務，本計畫亦提出 SET Enabler 的安全服務，讓使用者在網路上進行電子交易時，能有一個既安全又方便的電子付款解決方案。

子計劃二經過一年的執行與研究，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、密鑰管理及安全策略促成工具），另外並提出了兩種安全促成工具之設計，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。

子計畫二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。在認證及密鑰管理部分，子計畫二自行設計出了一個基於 Public Key Kerberos 認證服務的密鑰管理協定，稱為通行票式密鑰管理協定。在網路層協定加密部分，子計畫二採用網際網路安全協定（IP Security），用來做 IP 封包的加密。在安全策略部分，子計畫二利用過濾封包的輸出及輸入做分析，將之歸納成四種安全策略。

未來，子計畫二將繼續完成安全通道促成工具之實作，設計新的促成工具以擴充網際網路安全促成工具的功能，並加強整個系統安全性與執行效能。





圖二　子計畫二實作系統架構圖

子計畫三在執行期間,進行下列三項研究：

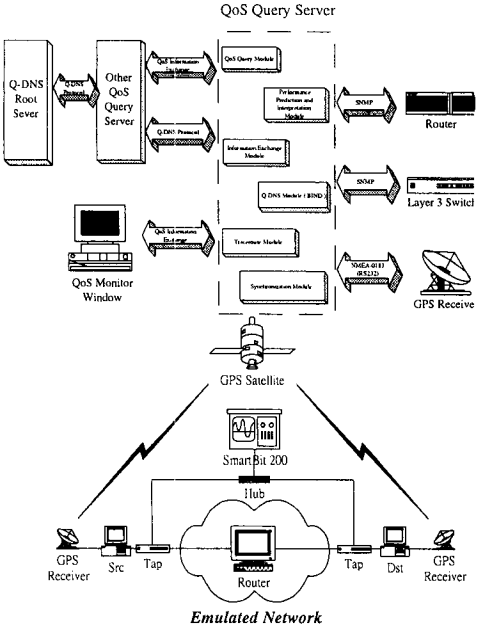
1. 差別服務架構中相對品質服務(Qualitative Service)之拍賣競價機制設計。

此研究，子計畫三設計一套配合 DiffServ 架構的競價機制，讓使用者的競價行為自然反映了他們的需求且同時把市場帶到一個穩定的運作點。子計畫三的分析證明市場在這一點上，沒有任何使用者會

步之參考時鐘。子計畫四使用 Linux 做為路由器，加重其 CPU 負載用以模彷網路延遲，並以 SmartBit 所量測之數據做為子計畫四量測系統之驗證，如圖四所示。

與既有之服務品質查詢系統整合後，子計畫四在台大校園網路進行實測，以驗證整合後之服務品質查詢系統之可行性。下一階段之測試則將在國家實驗網路上與其他大學進行互連測試。

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，然而過去網際網路量測工具之開發過度著重於對封包遺失率敏感之交通，故子計畫四同時開發網路單向延遲之量測技巧以及整合既有的量測系統，目的在於以減少量測封包造成網路資源的浪費的前提下，開發一套簡單、低成本、高精準度且具有即時量測功能之網路單向延遲量測工具。由實作結果顯示，子計畫四所設計之網際網路單向延遲量測系統之精準度可達數十個微秒（Microseconds），如此高之精準度足以滿足網路多媒體應用之要求，並且可以達到子計畫四所要求之目標。

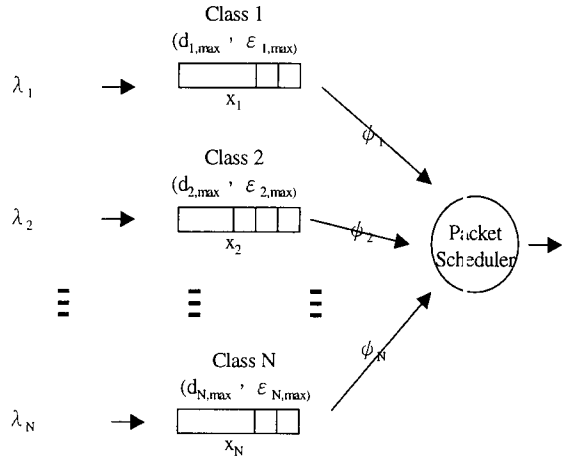


圖四 服務品質查詢伺服器及單向延遲量測之架構圖

在子計畫五研究中定義在差異化服務網路(Differentiated Services Networks) 的一種新的服務模式叫“ Statistical Expedited Forwarding Service ”，該服務可以保障封包延遲和封包遺失率不超過某個上限。子計畫五針對此一新服務模式提出一個新的動態頻寬及緩衝區資源分配的方法與機制。子計畫五的設計理念是希望能在連接提供差異化服務的骨幹網路的邊際路由器(edge router)上提供使用者整合性服務般的效能保證，卻不需在網路的核心路由器(core router)維持 per-flow 的資訊。目標應用是同時對封包延遲和封包遺失兩項服務品質敏感的應用，如網路電話、即時影像傳輸和線上電子商務等等提供 QoS 的保證。

為了保障封包延遲和封包遺失不超過上限值，子計畫五根據給定的 QoS 要求，來替每個類別保留“ effective resource ”（包括頻寬和緩衝區大小）。除此之外，子計畫五更進一步探討在同一個類別中所有資料流的公平性。數個聲音和影像應用的實驗顯現出子計畫五提出機制的適用性。

故子計畫五提出一個以應用為導向的服務模式，整合不同應用（具有不同服務品質保證要求），想法是將差異化網路架構下的路由器排程分成多個佇列，每個佇列代表一種服務品質保證要求的應用，不同佇列之間則以 WFQ（weighted fair queueing）來排程以達到分配頻寬和緩衝區大小的目的。



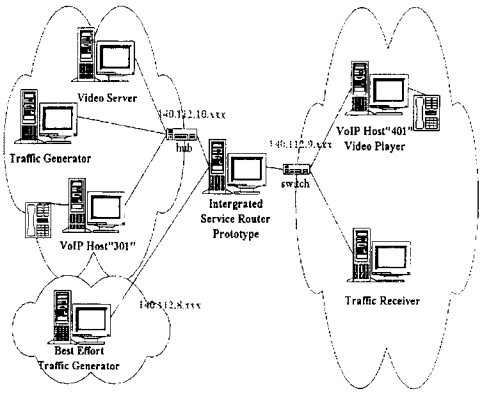
圖五 子計畫五 QoS 服務架構圖

整個架構可以用圖五來表示，不同 Class 表示不同的應用，經過 Classifier 後，被分配到不同的佇列，然後我們會分配頻寬 R 和緩衝區 B 兩項資源給各個佇列。

在子計畫五的研究主要探討了：一、使用 " Summed Tspec " 來為要求封包遺失率為 0 的應用保留資源。二、使用 " Equivalent Capacity " 來為可以忍受一定封包遺失的網路聲音、影像應用保留資源。並且在保障封包遺失率不超過要求值的同時，封包的最大延遲也不能超過要求值。由以上的實驗結果可以得知，子計畫五提出的以應用為導向的服務模式，的確可以在差異化網路架構下，提供明確的量化服務品質保證。針對同時滿足兩項服務品質保證指標是本研究的特點。

子計畫五的架構適用環境在：一、骨幹網路上。二、企業網路，管理者可以決定想要保障其服務品質的應用，並為其保留資源，不屬於這些應用的其他網路資料流就歸到 Best-Effort 佇列。而應用導向的緣故，也適合企業拿來支援某些特定應用。例如在企業內推動視訊會議、分公司間以網路電話聯繫等等。

為驗證整個系統的效能，子計畫五設計了一系列實驗，實驗環境如圖六所示



圖六 子計畫五實驗環境圖

在子計畫五的實驗中，由 " Policy Manager " 建立了階層式的政策，觀察 QoS Router 是否能夠根據這些政策正確地被設定和啟動。同時並使用 Video 和 VoIP 等應用來測試 QoS Router 對服務品質保證的效能。

三、計畫成果自評

本計畫群在過去近二年之執行期間內，雖然常受到經費及人力的限制，無法進行大規模測試及整合；但多項計畫已有實作成果，並正在校內或以跨校方式進行推廣擴散，希望下一年度能夠結合更多資源，擴大計畫成果。

四、參考文獻

[1] K. Cho, "A framework for alternate queueing: towards traffic management by PC-UNIX based router", Sony Computer Science Laboratory, Inc.

[2] R.A. Guerin, S. Kamat and S.Herzog, QoS Path management with RSVP, Performance, Computing and Communications, 1998. IPCCC '98., IEEE International , 1998 , Page(s): 291 –297

[3] I. Mahadevan and K. M. Sivalingam,

Architecture and experimental results for quality of service in mobile networks using RSVP and CBQ, *Wireless Networks* 6, 3 (Jul. 2000), Pages 221 – 234

[4] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, Nov. 1998.

[5] S. Kent and R. Atkinson , "IP Encapsulating Security Payload (ESP)," RFC 2406, Nov. 1998.

[6] J. Kohl and C. Neuman, "The Kerberos Network Authentication Service (V5)," RFC 1510, Sep. 1993.

[7] W. Stallings, Cryptography and Network Security, 2nd Edition, Prentice-Hall, 1999.

[8] C.-C. Liu, S.-C. Chang, H.-H Cheng, "Pricing and Fee Sharing for Point to Multipoint Multicast Services with Quality Guaranteed," *Proceedings of the Seventh International Conference on Parallel and Distributed Systems:Workshops 2000,* Iwate, Japan, July 4-7, 2000, pp.255~260.

[9] H.-I. Wu, S.-C. Chang, "Design of Resource Management at IP Router," *Proceedings of ICOIN-14,* Hsin-Chu, Jan. 26-28., 2000, pp. IC-4.1~ IC-4.8.

[10]鄭新禾,"Design for Auctioning Qualitative Service in DiffServ Network", Master thesis, National Taiwan University, 2000.

[11]朱紹儀,"Design of Integrated Pricing and Bandwidth Allocation Scheme", Master thesis, National Taiwan University, 2000.

[12]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.

[13] GARMIN Corporation, *GPS 25—LVS Technical Specification*, 1998.

[14] G. Almes, S. Kalidindi, M. Zekauskas, "A One-way Delay Metric for IPPM," RFC 2679, September 1999.

[15] D. Mills, "A Kernel Model for Precision Timekeeping," RFC 1589, March 1994.

[16] J. Mogul, D. Mills, J. Brittenson, J. Stone, U. Windl, "Pulse-Per-Second API for UNIX-like Operating Systems, Version 1.0," RFC 2783, March 2000.

[17] [Guerin 1991] R. Guerin, H. Ahmadi, and M. Naghshineh, "Equivalent capacity and its application to bandwidth allocation in high-speed networks," IEEE J. Select. Areas Commun., vol. 9, pp. 968-981, 1991.

[18] [Sriram 1990] K. Sriram, "Dynamic bandwidth allocation and congestion control schemes for voice and data multiplexing in wideband packet technology", IEEE International Conference on Communication, 1990 , Page(s): 1003 -1009 vol.3

[19] [Lee 1996] C. B. Lee, Ha, K.B., and Park, R.-H. "Computation of effective bandwidth of aggregated VBR MPEG video traffic in ATM networks using the modified equivalent capacity" , ICC '96, Volume: 2 , 1996 , Page(s): 627 -631 vol.2

[20] Kenjiro Cho, "*A Framework for Alternate Queueing: Towards Traffic Management by PC-UNIX-Based Routers*", Proceedings of USENIX 1998 Annual Technical Conference, New Orleans LA, June 1998

[21] Parekh, A., Gallager, R., "*A generalized processor sharing approach to flow control – the single node case*", IEEE/ACM Transactions on Networking, Vol. 1, No.3, pp.344-357, June 1993