嵌入式 PPTP VPN 伺服器系統之設計和實作

The Design and Implementation of Embedded PPTP VPN Server System

曾建豪、李逸元、鮑立國
資訊技術處/網路通訊實驗室
財團法人資訊工業策進會
{arthur, iyylee, pert}@iii.org.tw

摘要：網際網路(Internet)近年來風行全世界，我國也已經達成三百萬人上網的目標，顯而易見的是無限廣泛的商機。對於企業內的網路而言，如何利用網際網路來達成『虛擬私有網路』(Virtual Private Network，VPN) 的需求，越來越重要。有鑑於此，本會實做了目前市場佔有率最高的VPN解決方案－『點對點隧道協定』(Point-to-Point Tunneling Protocol，簡稱PPTP）。PPTP的標準已由Internet Engineering Task Force (IETF) 於七月底頒佈，目的在提供使用者能夠應用此種隧道化的通訊協定，安全並私密地存取企業網路。本文詳盡討論了PPTP的協定，探討本會應用此系統在嵌入式系統時之設計及實作，以及如何應用PPP提供之安全機制及其它種身分驗證系統來加強PPTP系統的安全保障。另外，對於實務應用上，結合了隧道化通訊協定與NetBIOS over TCP/IP技術，讓使用者能透過「網路芳鄰」功能，雙向存取彼此資料。

關鍵詞：Virtual Private Network (VPN)，Microsoft Point-To-Point Encryption (MPPE)，Point-to-Point Protocol (PPP)，Point-to-Point Tunneling Protocol (PPTP)，NetBIOS over TCP/IP，Microsoft PPP CHAP Extensions (MS-CHAP)，Server Message Block(SMB)，Windows Internet Naming Service(WINS)，NetBEUI。

一、前言

『點對點隧道協定』(Point-to-Point Tunneling Protocol，以下簡稱 PPTP）主要是由 Microsoft、3Com、U.S. Robotics、Ascend Communications、ECI/Telematics 五家企業所組成之 PPTP Forum 聯合發展，前不久才正式成為 Internet RFC（RFC 2637，July 1999)。 PPTP 最大的優點就是 Microsoft 的全力支援：一方面 PPTP client 內建於 Windows 95、Windows 98、Windows NT 中，而另一方面 Windows NT 可以擔任 PPTP server 端的角色，預計在未來所推出的 Microsoft 作業系統(Windows 2000)也都會內建 PPTP。由於 Windows 系列產品的暢銷，其作業系統在全世界有著龐大市場佔有率，所以對於撥接方面的市場會有很大的影響力，進而使 PPTP 成為業界標準。另外，PPTP 不像『網際網路層安全架構協定』(Security Architecture for the Internet Protocol，簡稱 IPSec) [RFC 2401]只支援 IP， PPTP 對於撥接客戶端(透過 PPP encapsulation)支援 multiprotocol， 也就是說除了 IP 外還可以支援 IPX、NetBEUI、AppleTalk 等等不同的網路層協定。 這也是 PPTP 一個很大的優點。

顧名思義，PPTP 是 PPP (Point-to-Point Protocol) 協定[RFC 1661]的擴充，PPTP 隧道(PPTP tunnel)中所裝載的封包，皆為 PPP 的資料封包。基本上，PPTP 利用 Generic Routing Encapsulation Protocol (以下簡稱 GRE) 協定[RFC 1701，1702]來封裝 PPP 資料封包；但其中的 PPP 資料封包並不包含一些控制字元以及循環重復檢查(CRC)的資訊。tunneling 的建立方式是把 IP、IPX、NetBEUI、AppleTalk 等等網路協定封裝在 PPP [Ethertype for PPP]封包內當做 GRE 封包的資料(Payload)， 再由 IP 封包負責傳送 GRE 封包。

『遠端撥接 tunneling』的方式可以進一步區分為『遠端用戶起始』(client-initiated)及『ISP 起始』(ISP-initiated)兩種模式；前者是由客戶端撥接到 ISP，和 ISP 建立 PPP 連線後再由客戶端來起始 PPTP 的 session，和所欲連線另一端的 PPTP server 之間建立 tunnel，這樣就可以不需要 ISP 的支援就完成 PPTP 連結，所以稱為 client-PPTP-enable；後者則剛好相反，客戶端在和 ISP 的 access server 建立 PPP 連線後， 再由 access server (ISP) 和位於目地的 PPTP server 建立 tunnel， 客戶端不需要安裝任何特殊的 PPTP client 軟體，是屬於『ISP-PPTP-enable』。PPTP 除了支援『遠端撥接 tunneling』，亦可進一步擴充網路功能成為『LAN to LAN tunneling』。『LAN to LAN tunneling』的方式是在 PPTP Server 的兩端之間建立 PPTP tunnel，譬如安裝有 Microsoft 的 Routing and Remote Access Service（R&RAS）的 NT server 。 透過這樣的連結再加上一些保護措施後便可讓雙方的私有網路形成一個安全的 VPN。

以上討論的三種 tunneling 建立的方式，各有市場間隔。『ISP-PPTP-enable tunneling』需要 ISP 的 access server (Remote Access Switch) 支援 PPTP 功能，並由使用者向 ISP 提出使用 PPTP Service 的申請；『LAN to LAN tunneling』需用特定的網路軟體支援且不同軟體之間無法相容；再考慮 Microsoft 提供完整客戶端撥接軟體的因素，因此我們的系統架構範圍定位在支援遠端撥接『client-PPTP-enable』Service 的 PPTP Server。

PPTP 本身並沒有提供 Security 的能力；目前 PPTP RFC [RFC 2637]說明 PPTP Security 的機制仍由 PPP 負責驗證協定確保網路的安全。 Microsoft NT Remote Access Server （RAS）利用 MPPE 協定，搭載了 RC4 加密演算法來保護資料的私密性，在美國境內使用的 key 長度是 128 位元，國外使用則是 40 位元[RC4]。一般 PPP 使用者身分驗證用 Password Authentication Protocol [RFC 1344]與 Challenge Handshake Access Protocol [RFC1994]；Microsoft 本身增

加了 Microsoft PPP CHAP Extensions [RFC 2433]。在 PPTP RFC 中，提到新的 PPP 使用者身分驗證協定 PPP Extensible Authentication Protocol (EAP) [RFC2284]。

在下一節裡，我們將對 PPTP 通訊協定之兩個平行機制做概括性介紹。關於 PPTP 的兩種隧道模式與其封包格式，我們在第三節中介紹。在第四節裡，我們將會詳細分析本會在嵌入式系統實做的 PPTP 系統架構。最後，我們在第五節中討論 PPTP Server 的一個應用實例，並在第六節裡對本文做一個結論。

二、PPTP 協定

PPTP 協定主要由兩個平行的機制所組成：控制連結(Control Connection)機制與 IP 隧道(IP Tunneling)機制。

控制連結(control connection)機制

PPTP 系統由 PPTP 連結的兩個端點 PAC (PPTP Access Concentrator) 與 PNS (PPTP Network Server)， 利用 TCP port 1723 相互傳送『隧道（Tunnel）控制訊息』。

其主要目的在：

1. 隧道的建立、維護與刪除：一組 PAC – PNS 之間只有一個隧道。要等隧道建立後，才能在隧道內建立 User Sessions。
2. User Sessions 的建立、維護與刪除。

IP隧道(IP tunneling)機制

對隧道內的每個 User Sessions 要傳送的資料， 利用 GRE 協定封裝傳送。 IP 隧道中的封包結構如圖 1：

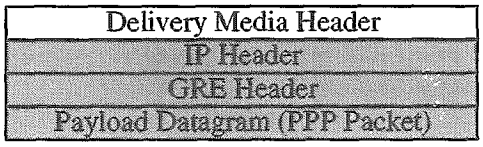

圖 1. IP 隧道封包結構

基本上 IP、GRE、Ethertype PPP 之間的關係如下：

1. IP 指定 GRE：GRE 封包被包裹 (be encapsulated) 在 IP 封包內；IP header 的 protocol type 欄位定值 47 (GRE)。
2. GRE 指定 Ethertype PPP：Ethertype PPP 封包被包裹在 GRE 封包內； GRE header 的 Protocol type 欄位定值 0x880B (Ethertype PPP)。
3. Ethertype PPP 支援 Multi-protocol：PPP 的 NCP (Network Control Protocol) 可以支援 IP、IPX、NetBEUI 等通訊協定。

GRE 像是 PPTP 一個對外的窗口。當封包由遠端網路來的時候，經由 GRE 的解讀，再將封包丟給更上層的 PPP 去處理；當己端要送封包至遠端時， GRE 將此一資料封包打包送至網路遠端。更詳盡地說，以前者而言，其流程為：首先，收進網路封包；接下來判讀封包標頭：是否為 GRE 封包，是否夾帶確認數字，是否帶有資料；第三步，若帶有資料封包則將之交由上層協定處理。

而送出 GRE 封包的流程剛好對稱：首先收到上層協定封包；接著，依封包特性（是否為空封包）製作 GRE 標頭；最後將資料加上 GRE 標頭再經由網路送到遠端。

由於普通的 PPP 封包內都含有一些 HDLC (High-Level Data Link Control)的控制字元，若要經由 GRE，則必須將這些控制字元移除，再送到網際網路上；反過來說，若是從遠端網路收到的封包，也不該含有任何這類控制字元，因為那對 GRE 來說是不需要的。

PPTP協定的特性

PPTP 協定主要的特性，包含下列五點：

1. 多重通訊協定：利用 PPP 支援 Multi-Protocol 的特性，間接使 PPP 支援多重通訊協定功能。包含：IP、IPX、NetBEUI．．．等。
2. Media Independence：PPTP 的傳輸介面為 IP 封包，與下層傳輸介面無關。任何傳輸網路(Physical Layer) 的改變，只要不影響 IP 封包傳輸，則不會影響 PPTP 封包的運送。
3. 彈性設定 client IP 位址：透過 PPTP 啟動之 PPP 協定中 NCP 協調 （Negotiation）動作，可依使用者需求，設定成私有網路節點位址，或區域網路內特定節點位址。
4. 多工隧道(Multiplex Tunnel)：兩端點間之同一隧道(Tunnel)，可供多人使用者共同使用(User Sessions)，而彼此間以不同 Call ID 區別。
5. 低通訊成本：透過網際網路來傳遞 PPP 封包，以取代傳統電話線路長途撥接成本的高額成本。換言之，運用 PPTP 通訊協定，即可使 PPP 封包透過網際網路傳輸，而取代傳統電話線路（PSTN）高額的連接

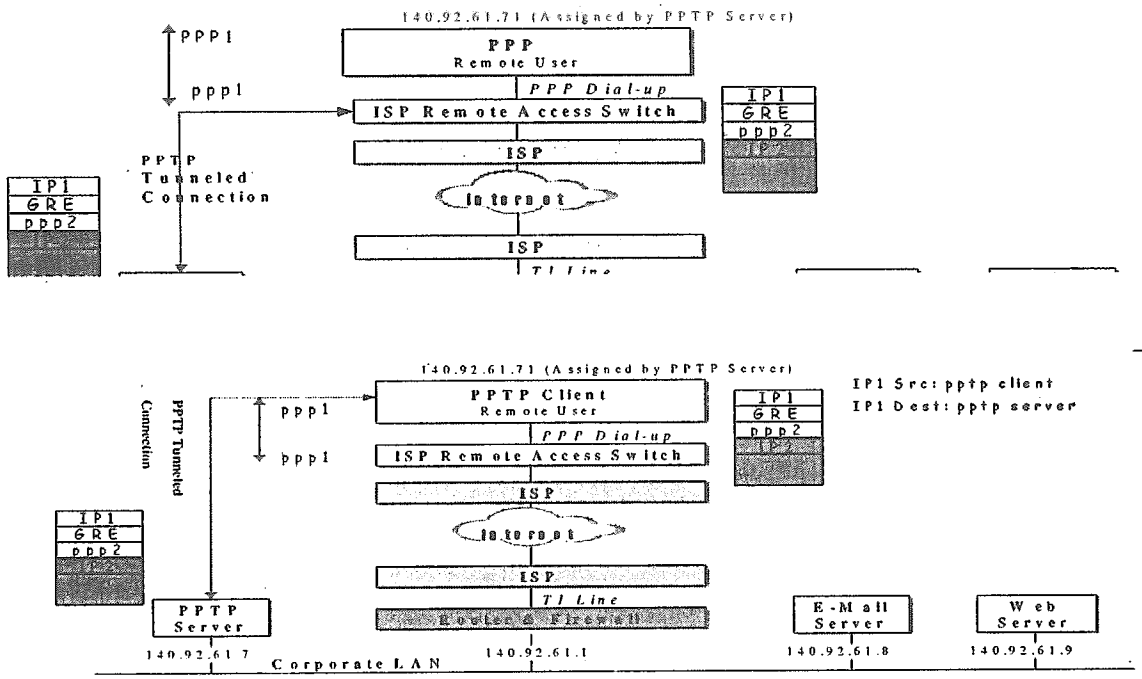

圖 2. Client-PPTP-enable的 PPTP隧 道 示 意 圖

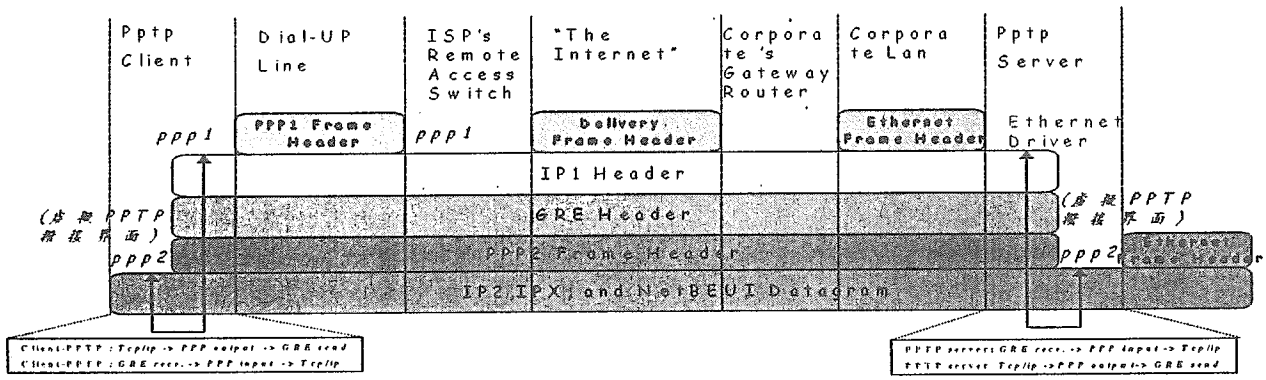

圖 3. Client-PPTP-enable隧 道 的 標 頭 轉 換 機 制

圖 2 為 Client-PPTP-enable 隧道建構圖； 圖 3 說明 PPTP 標頭轉換機制。圖例假設公司網路使用 IP 通訊協定，圖例說明封包到達 PPTP Server 前之狀況；其中，PPP1 表示遠端使用者與 ISP 端通訊所使用之標頭；PPP2 表示 PPTP 啟動 PPP 協定之所附加的新標頭。IP1 表示傳輸於 ISP 與 PPTP 伺服端間使用之合法 IP 位址(IP1 的 Source IP Address 由 ISP 指定)；IP2 的 Source IP Address 表示建構隧道後，PPTP 伺服端指定給遠端使用者之公司網路內部 IP 位址（可為 Private 位址）。透過節點位址彈性化的設定，使 PPTP 封包可以合法傳輸於網際網路(IP1)，亦可以自由取用區域網路內部資源(IP2)。

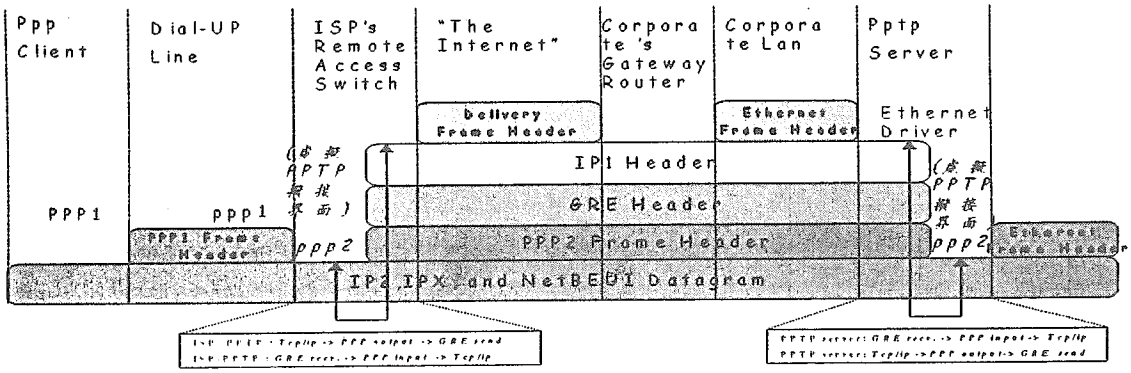

圖 5. ISP-PPTP-enable隧 道 PPTP標 頭 轉 換 機 制

圖例說明封包到達 PPTP Server 前之狀況；其中，PPP1 表示遠端使用者與 ISP 端通訊所使用之標頭；PPP2 表示 PPTP 啟動 PPP 協定之所附加的新標頭。IP1 表示傳輸於 ISP 與 PPTP 伺服端間使用之合法 IP 位址（IP1 的 Source IP address 由 ISP 指定）；IP2 的 Source IP Address 表示建構隧道後，PPTP 伺服端指定給遠端使用者之公司網路內部 IP 位址（可為 Private 位址）。透過節點位址彈性化的設定，使 PPTP 封包可以合法傳輸於網際網路(IP1)，亦可以自由取用區域網路內部資源(IP2)。

PPTP的安全機制

網際網路是一個公開的環境，無法限制使用者的連接，為避免區域網路內部資料傳輸過程中，被第三者非法截聽與竊取，因而造成機密資料外洩，相當程度的安全機制是必需的。

在 Internet 上建立一個安全的 VPN，主要是確保資料在 Internet 傳輸過程中的安全。為避免重要的機密資料或文件在網路中被有心人士竊取或竄改，所以對於傳輸內容的私密性（privacy）和完整性（integrity）就必須有相對應的保護措施。對於 PPTP 通訊協定而言，單純隧道化的觀念是不足以提供資料安全的保障，仍需配合 PPP 協定支援資料加密的特性或採用 IPSec 通訊協定，才能完整確保資料安全性。在本系統中，我們採取了 MPPE (Microsoft Point-To-Point Encryption) [MPPE draft-1] 協定與 MS-CHAP（Microsoft PPP CHAP Extensions）[RFC 2433] 協定來提供的封包加密及驗證等保護機制。

以下分成三部份說明 PPTP 通訊協定的安全機制。

1. 封包過濾(Packet Filter)：藉由預先設定的封包過濾條件，PPTP 會要求防火牆（Firewall）開放 TCP 1723 埠號（Port number）給 PPTP Server。另外 PPTP 利用 GRE 協定來傳送 user sessions 的資料，故 PPTP 也要求防火牆對 PPTP Server 開放 GRE 協定（此時 IP header 的 protocol type 欄位為 47）。

2. 身分驗證(Authentication)：PPTP 通訊協定針對於身分驗證部份，由 PPP 協定負責，PPTP 不做額外處理。

一般 PPP 協定提供之身分驗證：包括 PAP [RFC1344]、CHAP [RFC1994]．．．等，隨著撥接雙方支援種類不同，於 PPP 協定中 LCP 協調時決定採用之身分驗證方式；而 PPP 系統支援之 Hash 演算法，包括 MD4 與 MD5。驗證目的用以確認撥接使用者。在我們的 PPTP 系統中，增加 MS-CHAP 這個演算法。

3. 資料加密(Encryption)：PPTP 通訊協定針對於資料加密部份，由 PPP 協定負責，PPTP 不做額外處理。

在我們的 PPTP 系統中，乃利用 PPP 通訊協定中 MPPE 加解密協定，提供 PPTP 封包中 PPP 資料欄之加解密，其加密演算法採用 40 bit 的 RC4。一般做 MPPE 的先決條件是 PPP 身份驗證時採取 MS-CHAP。

四、PPTP Server 系統設計

本節描述本系統『PPTP Server 系統』之預定目標、架構、原理及設計考量。

系統目標

傳統之遠端撥接網路，遠端使用者（個人或 LAN）必須透過長途電話撥接至目的端，如此雖然可以直接利用目的端內部網路的資源，但必須花費長途電話費，成本頗高。藉由本系統之開發，預計達成目標如下：

1. 利用 Internet 建構 Virtual Private Network，遠端使用者通訊傳輸資料的費用也由長途性降為區域性通訊傳輸資料的費用。
2. 建構 PPTP Tunneling，並藉由 GRE 封裝 Multi-Protocol 的特性，間接支援 IP、IPX...等多種通訊協定。
3. 系統操作者可以由 PPTP Server 取得企業網路內的 IP Address，這種 IP Address 可以是合法 IP Address 或私有 IP Address。透過本系統所做的網路位址分配，可以使 IP Address 的使用更為彈性。
4. 凡 Internet 上支援 IP 協定的各種通訊網路，皆可適用本系統。
5. 可藉由安全驗證及資料加密等機制，使得傳輸於 Internet 上之各種封包都無法被竄改及竊聽。

PPTP 系統利用隧道化（tunneling）及資料加密（encryption）方式所建立虛擬私有網路，可使系統兩端的使用者相互做私密的資料傳輸，而如同在公司內部般地安全存取私有資料。

本系統之目標在建構安全穩定的虛擬私有網路-PPTP 系統，遠端使用者得以利用 Client-PPTP-enable 軟體（如

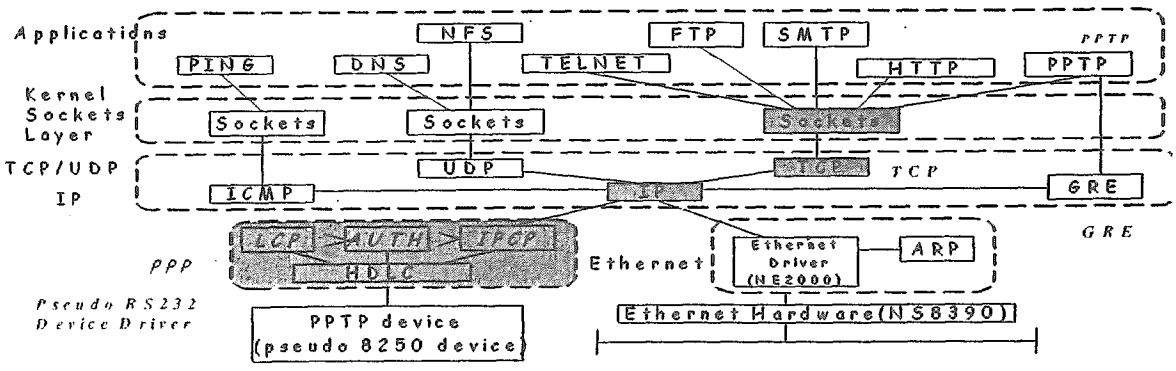

圖 6. PPTP 系統建置架構圖

Windows 95/98 或 NT4.0 內建之 PPTP Client 軟體) 撥接上企業網路內之 PPTP Server (本系統)，存取企業內部網路資源。

系統架構

本系統由即時作業系統、TCP/IP Stack 及針對此 RTOS 所開發的 PPTP 系統軟體所構成，系統建置架構如圖 6。PPTP 系統主要利用現成的網路通訊協定與 device driver (如 TCP Protocol、PPP protocol、GRE Protocol、Pseudo RS232 device driver 等等) 來建構 PPTP 系統，而非制定新的通訊協定。

系統範圍

本 PPTP Server 系統應用 IETF PPTP 協定所提供的虛擬私有隧道(Tunneling) 觀念，並支援加解密及身分驗證特性，可提供使用者低成本、低風險、資源運用及更彈性化的解決方案。

與PPTP相關的系統軟體概述

我們前面曾說明，基本上 PPTP 本身未制定新的 Protocol，只規定如何利用現成的 Protocol 來實作 PPTP；同時基於模組化與未來平台轉換的難易度的考量，本 PPTP Server 系統原則上是應用層的軟體，故在實作上它需系統軟體支援。以下我們將描述與 PPTP 相關的各系統軟體意義及用途，請同時參閱圖 6 (PPTP 系統建置架構圖)。

1. TCP Protocol

PPTP 本身由「隧道控制」與「User Sessions 傳送」兩大部分構成。前者屬於控制命令的傳送，憑藉

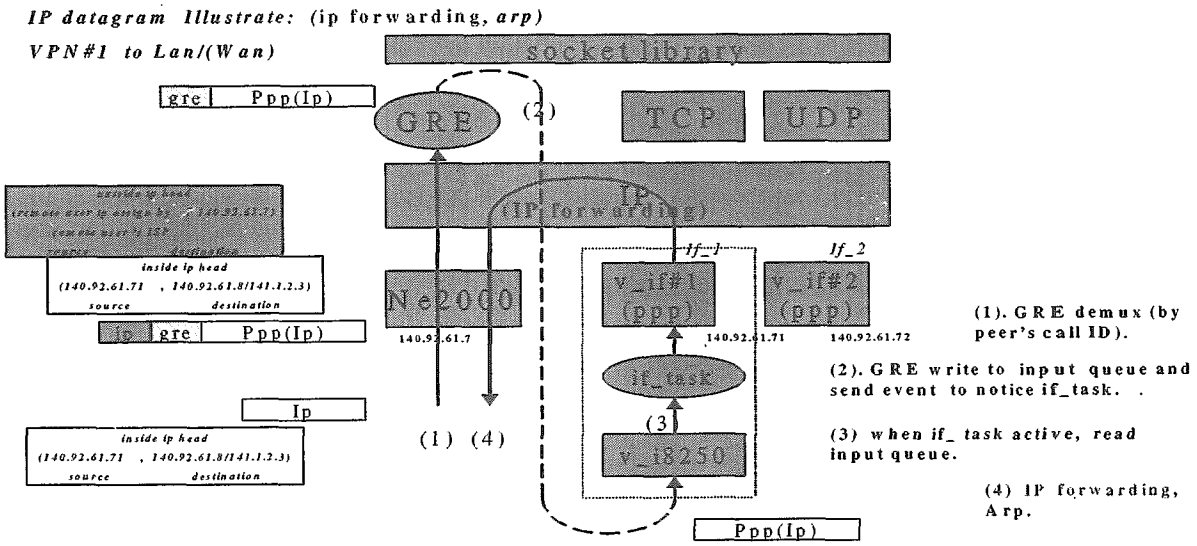

圖 7. 遠端使用者的IP封包傳回至PPTP Server端LAN內之機制

的方式是 TCP 通訊協定，這方面 PPTP 有專用的 TCP Port；其 port 的定義值是 1723。而後者負責資料的傳送，這部份 PPTP 由 GRE 來負責。

2. Enhanced GRE Header

請參見圖 1. IP 隧道封包結構；PPTP 有專屬的 GRE header 定義，稱之 Enhanced GRE header；GRE 與 Enhanced GRE 的差別如下：

- Enhanced GRE Header 定義了一個新的 Flag 欄位; 稱之為 Acknowledgement Number Field。
- Enhanced GRE Header 的 version 欄位規定為 1。
- Enhanced GRE Header 的 protocol type 欄位規定為 0x880B； 而 0x880B 定義了 Ethertype PPP。換言之，PPTP 採用了 GRE over (Ethertype) PPP 的通訊協定。

3. PPP Protocol

雖然 PPP 與 PPTP 的關係密切，但 PPTP 不會更改 PPP 協定本身。對 PPTP 而言，每一個撥接 User Session (Call) 都在 PPTP Server 佔用一個 PPP 網路界面(Interface)；其運作機制類似使用者由 Modem 撥接至 Terminal Server 的情形。

4. IP Forwarding 與 Proxy Arp

為使 PPP encapsulated 的 IP 封包可以正確地在 LAN 內正確傳送，TCP/IP 需支援 IP Forwarding 與 Proxy Arp。我們用圖例說明使用的時機。圖 7 描述遠端使用者的 IP 封包傳回至 PPTP Server 端 LAN 內之機制；圖 8 則說明 PPTP 端 LAN 上的 IP 封包透過 PPTP Server 到 WAN 之機制。

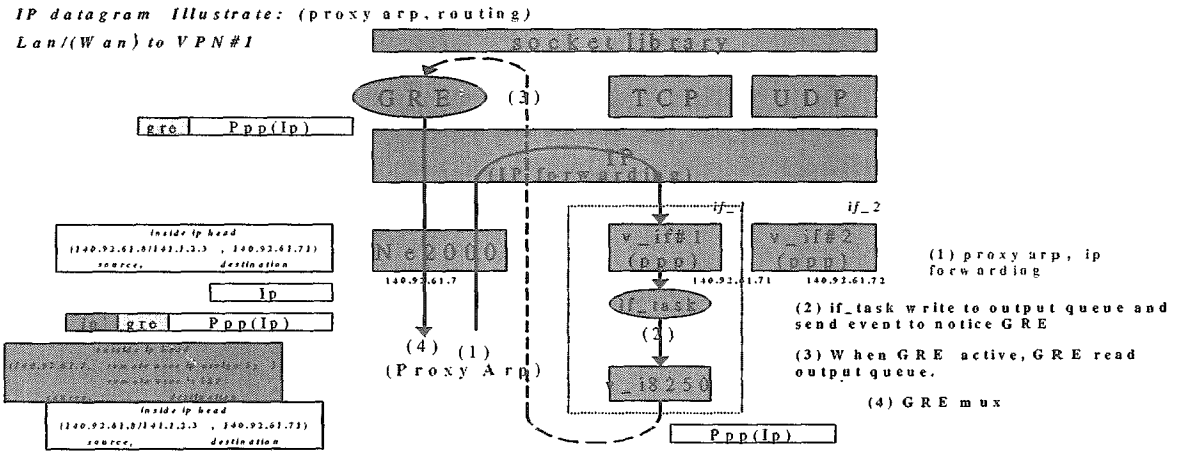

圖 8. PPTP端 LAN 上 的 IP封 包 透 過 PPTP Server到 WAN 之 機 制

五、實例應用

本節將說明整合『PPTP Server 系統』與 NetBIOS over TCP/IP [RFC1001, RFC1002]技術之相關課題，包括：NetBIOS-Based 網路、NetBIOS over TCP/IP 技術概述、系統整合與應用系統架構。將 VPN 安全性的網路服務，實際應用於一般常見的「網路芳鄰」(Network Neighborhood)檔案分享。透過本系統功能，讓使用者雖然身在家中卻如同坐在辦公室一般，共享彼此資源。

NetBIOS-Based網路

傳統 NetBIOS-Based 網路架構下，NetBIOS 的功能是提供上層應用程式存取 NetBIOS 相容網路資源的界面。配合上層統一的檔案資源分享協定 Server Message Block Protocol(SMB) [SMB]與下層網路層通訊協定，達到網路資源共享。比照 OSI 網路模型來看(如圖 9 所示)，NetBIOS 所扮演的角色，是介於 Transport Layer 與 Session Layer 間，並提供 Transport Layer 與 Session Layer 相關訊息溝通的傳遞機制。

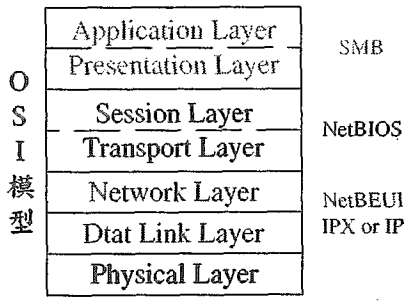

圖 9. NetBIOS-Based 網路架構比照 OSI 模型

儘管 NetBIOS 的設計上，底層的網路層通訊協定可以是 NetBEUI、IPX 或 IP，但由於前兩者的設計是適用於區域網路，甚至 NetBEUI 協定並無封包繞徑(routing)功能，須藉由網路廣播機制以達到封包傳遞，如此會造成內部網路嚴重負載，減低網路頻寬的使用效率。

依據 RFC1001、RFC1002 網路標準制定文件的定義，本系統採用 NetBIOS over TCP/IP 的架構，不但使得傳統區域網路 NetBIOS 相容設備彼此資源共享外，更能透過廣域網路存取遠端個人電腦或不同的區域網路。

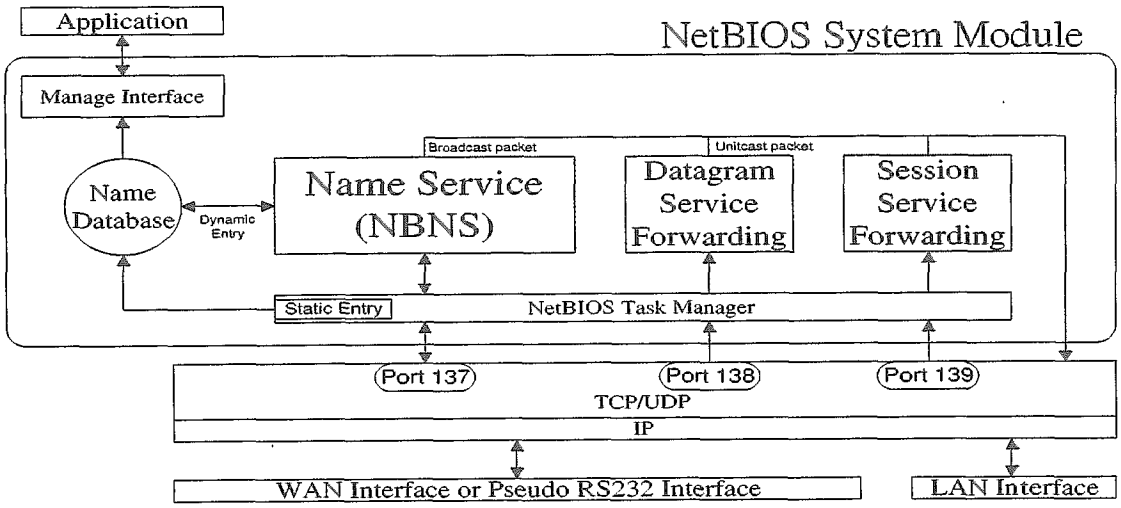

圖 10. NetBIOS 模組架構

NetBIOS over TCP/IP模組架構與系統整合

本系統 NetBIOS 模組使用標準 Socket 介面，透過 TCP/UDP port 137、138、139 三個通道，分別提供網路名稱服務(Name Service)、資料封包服務(Datagram Service)與會議服務(Session Service)。詳細模組架構參考圖 10。

如圖 10 所示，由 WAN Interface 接收之名稱服務封包，除了對區域網路 NetBIOS 相容設備，做名稱註冊的廣播封包外，其他將由本系統名稱代理伺服器(NetBIOS Name Server, NBNS)代為回覆與查尋，以提升名稱服務的效率。其次，對於資料封包服務的群組廣播封包，由於目前使用狀況並不普遍，本系統僅對單點傳送封包做處理。

在系統整合上，NetBIOS 系統模組是接收通過 PPTP 系統認證與解密後的明碼封包(置放於 WAN Interface 的 Input Queue 中)，經過 NetBIOS 模組處理後，選擇性的轉送給區域網路(LAN Interface)內部設備。如此處理的目的，除了之前提到的提升名稱服務的效率外，更可以增加內部網路的安全性，與減少大量不必要的廣播封包轉送，造成內部網路的壅塞。

系統應用實例

PPTP 系統應用架構主要分為兩大部分，其一為放至於區域網路內部的 PPTP 伺服器系統，負責接收與轉送外來 PPTP 服務的封包；其二為遠端撥接使用者，使用支援 PPTP 撥接服務的客戶端程式。本實例測試採用本會自行開發的 PPTP 伺服器，搭配 Windows 作業系統上 PPTP Client 介面，透過電話撥接功能，連接本會內部網路系統並分享內部網路資源，詳細架構圖如圖 11 所示。

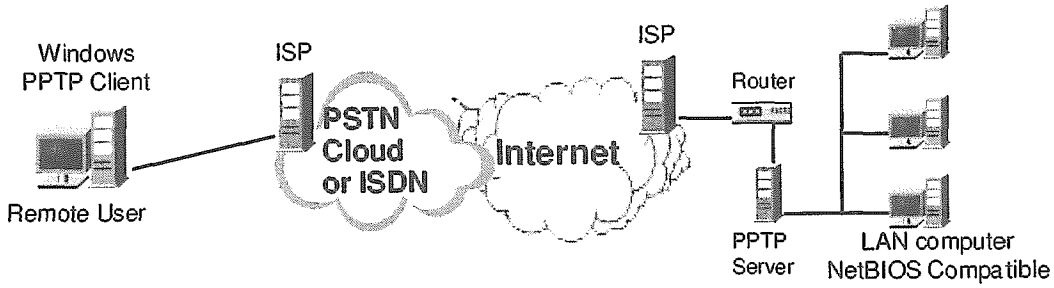

圖 11. 實例應用架構

經過實際測試，遠端使用者應用「網路芳鄰」(Network Neighborhood)分享公司內部網路資源部分，比較本系統採用名稱服務代理伺服器(NBNS)與單純名稱服務封包的轉送，執行效率上確實以代理名稱服務的方式較快。

六、結論

在 VPN 日漸風行的今日，本會選用目前市場佔有率最高的 PPTP 通訊協定做為實際實做的 VPN 的 solution。而也因為 PPTP 此種通訊協定的先天上的安全性不足，我們引進了 MPPE 安全機制與 PPTP 通訊協定相結合，將 PPTP 封包內的 PPP 內容做加密動作。除此之外，我們也提出了利用傳統的 PPP 身份驗證功能中的 PAP、CHAP 與 MS-CHAP 驗證任何使用此 VPN 服務的使用者。利用 PPTP 系統提供的隧道化（tunneling）及資料加密（encryption）方式所建立虛擬私有網路，可使系統兩端的使用者相互做私密的資料傳輸，達到如同在公司內部般地安全存取私有資料。

本會利用嵌入式系統實做了 PPTP 此種通訊協定的目的，是希望對國內網路設備製造廠商提供一種更合乎市場

需求的選擇。目前 VPN 的服務日漸成長及成熟，希望我們的經驗能夠提供各廠商一些的觀念及方向。

七、參考文獻

[RFC 883] P. Mockapetris, "*Domain Names - Implementation and Specification*", RFC883, November 1983

[RFC 1001] NetBIOS Working Group, "*Protocol Standard For A NetBIOS Service On A TCP/UDP Transport : Concepts And Methods*", RFC1001, March 1987

[RFC 1002] NetBIOS Working Group, "*Protocol Standard For A NetBIOS Service On A TCP/UDP Transport : Detailed Specifications*", RFC1002, March 1987

[RFC 1321] R. Rivest, and S. Dusse, "*The MD5 Message-Digest Algorithm*", MIT Laboratory for Computer Science and RSA Data Security, Inc., RFC 1321, April 1992

[RFC 1344] B. Lloyd and W. Simpson，"*PPP Authentication Protocols (PAP)*"， RFC 1344，October 1992

[RFC 1661] W. Simpson，"*The Point-to-Point Protocol (PPP)*"， RFC 1661，July 1994

[RFC 1701] S. Hanks、T. Li、D. Farinacci、"*Generic Routing Encapsulation (GRE)*"， and P. Traina，RFC 1701，October 1994

[RFC 1702] S. Hanks、T. Li、D. Farinacci、and P. Traina，"*Generic Routing Encapsulation over IPv4 networks*"， RFC 1702，October 1994

[RFC 1825] R. Atkinson, "*Security Architecture for the Internet Protocol*", IETF RFC 1825, August 1995

[RFC 1994] W. Simpson，"*PPP Challenge Handshake Authentication Protocol (CHAP)*"， RFC 1994，August 1996

[RFC 2097] G.Pall, "*The PPP NetBIOS Frames Control Protocol*", Microsoft Corp., RFC2097, January 1997

[RFC 2284] Blunk, L., Vollbrecht, J., "*PPP Extensible Authentication Protocol (EAP)*"，RFC 2284，March 1988

[RFC 2341] A. Valencia、M. Littelwood、T. Kolar，"*Cisco Layer Two Forwarding Protocol (L2F)*"，RFC 2341，May 1998

[RFC 2401] S. Kent and R. Atkinson, "*Security Architecture for the Internet Protocol*"，IETF RFC 2401, November 1998

[RFC 2433] G. Zorn, and S. Cobb. ,"*Microsoft PPP CHAP Extensions*", IETF RFC 2433, October 1998. (Format: TXT=34502 bytes) (Status: INFORMATIONAL)

[RFC 2637] Kory Hamzeh、Gurdeep Singh Pall、William Verthein、Jeff Taarud、and W. Andrew Little，"*Point-to-Point Tunneling Protocol (PPTP)*"，IETF RFC 2637，July 1999。

[MPPE draft-3] G. S. Pall and G. Zorn，"*Microsoft Point-To-Point Encryption Protocol (MPPE)*"，draft-ietf-pppext-mppe-03.txt，May 1999

[Ethertype for PPP] Reserved with Xerox Corporation.

[RC4] RC4 is an encryption standard available from RSA Data Security Inc.

[SMB] "*Microsoft Networks SMB Files Sharing Protocol v6.0p*", Microsoft Corp., January 1996

[WINS] "*Microsoft Windows NT Server WINS White Paper*", Microsoft Corp., 1996