

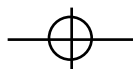
第五章

規劃與測試 Layer 2 連線

本章內容：

- * Windows NT RAS 伺服器的 PPTP 安裝與設定
- * 在 Windows NT 用戶端設定 PPTP 撥號網路
- * 設定 Windows 95/98 用戶端的 PPTP 撥號網路
- * 啟動遠端存取轉接器上的 PPTP
- * 進行撥號
- * 故障排除
- * PPTP 與其它安全機制的運作考量

在第四章，我們已介紹了「點對點包容通道協定」(Point-to-Point Tunneling Protocol, PPTP)，它可以在遠端使用者與網路間建立一條安全的通訊管道。PPTP 主要是 Windows NT 「遠端存取服務」(Remote Access Services, RAS) 的一項延伸功能，它把 RAS 伺服器當作閘道器，在 Internet 使用者與目的地網路間建立一個 VPN。Microsoft 附加在 Windows NT Server 上的 "Routing and Remote Access" 功能，甚至可以建立 LAN-to-LAN 的 PPTP 連線。本章為想要設定自己的 PPTP 連線的讀者提供了所需的基本資源；我們首先會談到如何在你的 Windows NT Server 上設定 PPTP，並只討論 RAS 與 PPTP 互動的細節（如果你沒有玩過 RAS，最容易得手的資料就是 NT 的 Help 檔，不然，市面上有不少論及這方面議題的好書，你可以參考歐萊禮出版的“Windows NT 系統管理”）。在設定 RAS 的時候，你必須決定要提供多少 port 給 VPN 撥號存取。雖然大部分的網路管理者將 RAS 伺服器設為“只能撥入”(dial-in only)，但其實你也可以讓伺服器建立對外的 PPTP 連線。





90 / 第五章

RAS 也允許你設定 Windows NT Server 可供撥接用戶使用的通訊協定，讓你能進一步掌握撥接使用者所能存取的範圍。例如，如果只允許 IP 協定，則使用者便只能存取到使用 TCP/IP 的電子郵件伺服器，而無法存取到使用 IPX 協定的 Novell NetWare 伺服器。同樣的，如果你的內部伺服器完全不使用 IP 協定，你也可以取消 IP 協定，而啟用其它的協定。在後文“5.1.2.1 挑選可包容的協定”會告訴你如何設定。

RAS 伺服器也支援過濾 PPTP 的功能，讓它幫你篩選可以跟系統網路卡建立連線的機器。遠端使用者必須能夠通過 NT 網域的驗證機制才能建立連線，在一台「多寄主」(multi-homed)【譯註】的 Windows NT Server 上，你可以利用 PPTP 的過濾功能來限制對 LAN 或 Internet 的存取；使用固定的 IP 位址，並開啟 IP 過濾功能，你可以把 RAS 伺服器當成防火牆來用。如果你偏向較彈性的做法，不打算使用固定的 IP 位址，你也可以用 DHCP (Dynamic Host Configuration Protocol) 來動態分配 IP 位址。本章將深入討論過濾與 DHCP 的設定。

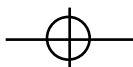
我們在第四章曾經提到過，目前有些 ISP 的設備可以支援 PPTP，有些則否，本章將會告訴你如何處理這兩種情況。我們也會告訴你，如何在兩種常用的路由器上設定 PPTP。ISP 可以透過 PPTP 讓客戶們能夠更容易地建立 VPN 連線，而網路管理者則可以藉此降低 RAS 伺服器處理要求建立連線的負擔。

在本章的最後，我們將介紹一連串的測試程序，檢測你初次安裝 PPTP 連線是否能正常運作，同時也會談到 PPTP 如何搭配其它的網路保全產品。

5.1 Windows NT RAS 伺服器的 PPTP 安裝與設定

在 Windows NT Server 4.0 上安裝設定 PPTP 的方式非常簡單，跟安裝其它元件沒有兩樣。包括了三個基本步驟：安裝通訊協定，建構設定 RAS，與設定撥號使用者的組態。

譯註 有兩片網路卡的機器，由於每片網路卡都可以分屬於不同的網路，所以稱為 multi-homed computer，通常這類機器可以兼任路由器的任務。





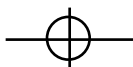
5.1.1 安裝 PPTP

一般來說，初次安裝 Windows NT Server 4.0 時，並不會順便幫你安裝 PPTP，你得自己動手把它加到系統中。此外，對於 Windows NT 而言，所有額外的安裝設定動作，都會需要原始的安裝光碟，這是一件很麻煩的事，所以一般都會將光碟片根目錄下的 \i386 複製到硬碟中，如果你用的不是 Intel-based 的電腦(例如 DEC Alpha)就應該複製 \Alpha 或其它對應的目錄到硬碟。由於本章有許多的安裝過程都會需要用到 NT 光碟片，所以你最好先把需要的目錄複製到你的硬碟。回到正題，安裝 PPTP 的過程很簡單：

1. 在“開始”功能表上，選擇“設定”，再選擇“控制台”。
2. 點選 (double-click) 控制台視窗中的“網路”圖示。
3. 在“網路”對話方塊中，選擇“通訊協定”這個設定頁。
4. 在“網路通訊協定”清單中，你會看到目前已安裝的協定。除非你已經安裝了 PPTP，否則應該不會出現。請按清單下方的“新增”按鈕。
5. 這時會出現“選擇網路通訊協定”的對話方塊，列出可以選擇的協定。選擇“Point To Point Tunneling 通訊協定”，然後按下“確定”按鈕。
6. 這時會出現另一個對話方塊，標題是“PPTP 設定”，可讓你選擇想支援的“虛擬私人網路個數”(就是 RAS 伺服器所能同時接受的 PPTP 連線數目)，當然，最好不要同時讓太多使用者建立連線以拖累系統的速度。可以選擇範圍是從 1 到 256，我們選擇 8，然後按下“確定”按鈕。安裝程式會掃描 NT 光碟片以搜尋需要的檔案，或是詢問你這些檔案的位置。

5.1.2 設定 RAS

在安裝 PPTP 協定之後，會出現一個標題為“安裝訊息”的視窗，告訴你系統要啟動遠端存取服務，並提醒你要設定 PPTP 連接埠；請在該視窗按下“確定”以便開始安裝程序。以下是設定 RAS 來提供 VPN 服務的程序：





92 / 第五章

1. 首先會出現“遠端存取設定”對話方塊，該視窗會列出目前所有的 RAS 連接埠和裝置，如果你已經為 RAS 設定了數據機，則該數據機也會出現在這個視窗裡，如果要設定 RAS 來使用 PPTP 的裝置，請按下“新增”按鈕。
2. 接著“新增 RAS 裝置”的對話方塊會出現，你可以利用下拉式選單挑選 RAS 裝置，除了系統的序列埠之外，你應該還會看到一串有埠號的 VPN 裝置，埠號會從 1 開始，最大值是你當初在安裝 PPTP 協定時的設定值。請參考圖 5-1，我們會看到同一個裝置（RASPTPM）已對應到八個連接埠（VPN1 - VPN8），這是一個貼心方便的設計，讓我們從清單中一次挑選一個連接埠。當你選擇好所要新增的連接埠，按下“確定”按鈕便可完成新增的動作。如果還想增加新的連接埠，可以在“遠端存取設定”對話方塊中按下“新增”按鈕重覆同樣的程序。



圖 5-1：設定一個 PPTP RAS 裝置





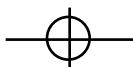
3. 新增的 VPN 連接埠只能允許“接收”(dial-in)，如果你想讓該連接埠也能“撥出”(dial-out)(我們會在稍後的「在 Windows NT 用戶端設定 PPTP 撥號網路」一節再詳加介紹)，請在“遠端存取設定”對話方塊中按下“設定”按鈕。
4. 如果你按下“遠端存取設定”對話方塊中的“網路”按鈕，便會出現“網路設定”對話方塊，你可以在這個對話方塊中設定該連接埠的網路組態。我們會在接下來的章節中詳細介紹“網路設定”對話方塊裡的參數與意義。然而，你將會發現到，因為我們不能強迫某個特定的使用者撥號進入某個特定的 VPN 連接埠，所以只好讓所有的連接埠都使用相同的設定，有經驗的 RAS 管理者將會發現，此對話方塊與設定一般 RAS 連線的對話方塊很相似。

5.1.2.1 選擇通道所用的協定

請參考圖 5-2；從“網路設定”對話方塊中，我們發現一個 VPN 連接埠只能接受三種協定：TCP/IP、IPX、NetBEUI。以我們的案例來說，我們必須啟用 TCP/IP 才能讓 Bill 可以存取 Internet 郵件伺服器，此外，他也需要 NetBEUI，才能存取他桌上型電腦的分享磁碟機 (shared disk)，因為沒用到 Novell NetWare 伺服器，所以我們把不必要的 IPX 關閉。

你可以在同樣的對話方塊中，將 VPN 使用者的使用範圍限制在該 RAS 伺服器裡，而不讓他存取整個網路。以我們的案例來說，Bill 必須要能存取整個網路。我們並不建議你做太多的限制，理由如下：

- 首先，這樣就沒意義了。因為 VPN 最令人驚訝的功能，就是它讓使用者能安全地進行遠端存取的動作，就好像他們直接連線到 LAN 一般。如果你限制了使用者只能存取 RAS 伺服器上的資源，也就是，你限制了使用者只能使用 RAS 伺服器原本在網路上所提供的服務。
- 如果你限制遠端使用者只能存取 RAS 伺服器，也就是，你必須在 RAS 伺服器上執行其它的服務，例如電子郵件或列印服務，甚至把 RAS 伺服器當成應用程式伺服器來使用。除非你的網路只有少數幾個用戶端（四個以下），不然我們並不建議你在 RAS 伺服器上執行其它的服務，同一部機器同時兼負多項任務不是一件好事，不但拖累效率，有時候還可能造成安全漏洞。





94 / 第五章



5-2 : RAS 的網路設定對話方塊

- 在本質上，一台 PPTP RAS 伺服器至少要能讓 Internet 做部份的存取，因此它也相當容易遭受到來自 Internet 的攻擊，如果讓 RAS 伺服器兼任其它任務，或執行特殊的應用程式，一旦它遭受攻擊，甚至崩潰，則你的應用程式也會跟著毀於一旦。

5.1.2.2 挑選驗證方法

在第四章，我們介紹過幾種 RAS 可用的驗證方式：“需要編碼確認”(CHAP)、“需要 Microsoft 編碼確認”(MS-CHAP) 以及“允許任何確認，包括一般文字”(PAP)。你可以使用 CHAP 或 MS-CHAP，或者是同時使用這兩種方式再加上 PAP；你可以在“網路設定”對話方塊依你自己的需要自行決定。





假設你的用戶端都支援上述的三種驗證方法（如果他們都是使用 Windows 用戶端，或 Mac 上的 TunnelBuilder），我們建議你使用 MS-CHAP。因為只有它能允許你把資料加密，讓 PPTP 達到真正的安全。若你的用戶端並不支援 MS-CHAP，當然也可以使用其它的驗證方式，但你就必須承受在 Internet 上傳輸未加密的資料以及密碼的風險（在使用 PAP 的狀況下）。

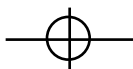
5.1.2.3 用 DHCP 配發 IP 位址

用 DHCP (Dynamic Host Configuration Protocol) 動態配發 IP 位址給連線進入的 PPTP 用戶是相當理想的方式。與 PPTP 一樣，初次安裝 Windows NT Server 4.0 的時候，並不會自動幫你安裝 DHCP，所以你必須自己透過“控制台”的“網路”來安裝 DHCP 服務【註】，安裝 DHCP 的過程與 RAS 很像，在安裝完畢後，你可以在“開始”功能表的“系統管理工具(公用)”找到“DHCP 管理員”。

要規劃 DHCP，請依照下列設定步驟：

1. 從【開始 -> 程式集 -> 系統管理工具(公用)】的清單中啟動“DHCP 管理員”。
2. 在“DHCP 伺服器”的欄位下選擇“*本地機器*”，到“領域”選單中選擇“建立分割”。
3. 會出現如圖 5-3 的“建立領域-(區域)”對話方塊，你必須輸入“起點位址”與“終點位址”，以我們的案例，起點位址是 2.1.1.129，終點位址是 2.1.1.136。
4. 輸入“子網路遮罩”。由於我們指定的位址範圍是 2.1.1.0 的一部份 Class C 網路，所以輸入 255.255.255.0。

註 如果 NT Server 4.0 RAS 系統上有兩片網路卡，而其中任何一片啟動了 PPTP 過濾功能的話，DHCP 將無法運作，Microsoft 已經發現了這個問題，並且在 Service Pack 2 中把它加以解決。如果你想在 RAS 上使用 DHCP，我們建議你安裝 Service Pack 3 或更新的版本。在稍後【過濾的注意事項】小節中，將會提到一些 DHCP 與 PPTP 之間的其它問題。





96 / 第五章

5. 我們目前把“排除範圍”的部份留白，因為我們不想排除這個範圍內的任何位址。
6. 將此領域命名為“撥接範圍”，然後按“確定”。當對話視窗詢問你是否要啟動此領域，請按“確定”。



圖 5-3 : Windows NT Server 的 DHCP 管理員

如果你有好幾個 RAS 伺服器，建議你使用“DHCP Relay 代理人”服務，其安裝方式也是透過在“控制台”裡的“網路”。因為我們通常不會架設太多 DHCP 伺服器，甚至好幾個不同的網路會共用一台 DHCP 伺服器，所以，為了避免在每個 RAS 伺服器所在的網路都架設一部 DHCP 伺服器，我們會需要有個“代理人”幫 RAS 伺服器代為處理用戶端申請配發 IP 位址的要求。至於到底該向哪一部 DHCP 請求配發 IP 位址，可以在“DHCP Relay 代理人”的“內容”中加以設定；如此一來，就算所有的 RAS 伺服器都不在同一個網路下，也可以由同一部 DHCP 伺服器來統籌控管所有的 IP 位址配發工作。





5.1.3 PPTP 過濾

我們在本章一開頭就介紹了 PPTP 的過濾功能，設定 PPTP 過濾的方式很簡單；請打開“控制台”裡的“網路”，在“內容”鍵上按一下，並選擇“TCP/IP”，然後按下“內容”按鈕，最後按下在 TCP/IP 設定對話方塊裡的“進階”按鈕，並點選在“進階 IP 位址”方塊裡最底下的“啟動 PPTP 過濾功能”核取方塊。

5.1.3.1 利用 PPTP 過濾進行對外流量的驗證

在 multihomed 的主機上，只要對連接到 LAN 的網路卡啟用 PPTP 過濾，就可以把它當作為一種對外交通的防火牆。在內部網路的使用者可以用類似 PPP 連線的方式，把 RAS 伺服器的 IP 位址當作電話號碼，撥入 PPTP 伺服器。他們會被迫一定要經過驗證，才能透過伺服器的選徑功能進入外界的 Internet。如此讓網路管理人員能控制對外的 Internet 交通，監控誰正在存取 Internet、存取的時間長短，並限制同時可以存取 Internet 的人數。

5.1.3.2 過濾的注意事項

如果你的 NT Server 4.0 Server 只有一片網路卡，啟動 PPTP 的過濾功能會使得非 PPTP 的使用者無法存取其它的網路服務（例如：DHCP、FTP ... 等等）。網路卡會要求所有的網路交通都必須通過 PPTP 驗證。有個辦法可以讓封包直接抵達 RAS 伺服器本身，而不須再經由網路，但你必須先安裝 NT Server 4.0 Service Pack 3 或更新的版本，以及在 Registry（登錄檔）中加上一筆特殊的記錄。



編輯 NT 的 Registry 是一件非常危險的事情，錯誤的資料可能會毀掉 Registry 並造成許多的（很有可能是無法回復的）系統問題，甚至你還需要重新安裝整個系統，所以請時時作好系統的備份工作。





98 / 第五章

要執行“登錄編輯器”，請在“開始”功能表的“執行”之檔案名稱欄位中輸入“REGEDIT.EXE”。所需要加入參數是在下列的機碼（Registry key）上：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RASPPPTPE\Parameters\Configuration
```

加入一筆資料型態為 REG_DWORD 的新資料，然後將資料名稱取名為“AllowPacketsForLocalMachine”，值設定為 1，然後結束編輯程式。你需要重新開機，才能讓修改發揮作用。

我們先前曾提過，我們不建議你在 RAS 伺服器上執行可能會造成系統安全漏洞的服務（例如：匿名 FTP），或是會干擾你內部網路作業的服務（像是 DHCP）。

5.1.4 過濾 IP 位址

另一種增進安全性的方式，就是讓 RAS 伺服器只允許某些特定的 IP 才能連建立 PPTP 連線。但這種方式有一個前提，就是遠端使用者必須擁有 ISP 所指定的固定 IP 位址，這樣子伺服器才有準則可以判斷對方來自何處。如果再搭配 PPTP 過濾功能，不但可以避免未經驗證授權的連線，也可以避免不明主機的入侵，這種做法可確保相當的安全性，但比較麻煩的是，這些動作無法透過簡單的使用者圖形界面來做到，你還是必須修改 NT 系統裡的 Registry：

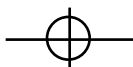
再次執行登錄編輯器，並找到以下的機碼：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RASPPPTPE\Parameters\Configuration
```

在該機碼下，你必須建立一筆資料型態為 REG_DWORD 的資料，名稱為“AuthenticateIncomingCalls”，定為十進位的數值，其值為 1。在同樣的機碼下，再建立一個型態為 REG_MULTI_SZ 的資料，名稱為“PeerClientIPAddresses”，請你在此輸入 RAS 伺服器所允許的 PPTP 連線用戶端的 IP 位址。所有的位址中間都必須以一個空格隔開。

5.1.5 設定撥接用戶

新增 Windows NT RAS 的用戶帳號，跟新增一位 NT 網域使用者的帳號沒有兩樣。



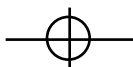


1. 從【開始 ->程式集 -> 系統管理工具 (公用)】的清單中啟動“網域使用者管理員”。
2. 編輯或新增使用者時，按下對話方塊右下方的“撥入”鈕。
3. 此時會出現如圖 5-4 的“撥號資訊”對話方塊。如果是 PPTP 使用者，請勾選“授與使用者撥入的使用權限”，並設定為“不回撥”。
4. 按下“確定”鈕，離開該對話方塊與“使用者內容”的視窗。

5.2 在 Windows NT 用戶端設定 PPTP 撥號網路

如果用戶端機器也是 Windows NT (Server 版或 Workstation 版)，要撥號進入支援 PPTP 的 ISP，其設定程序跟一般撥號網路幾乎一樣，只要再設定驗證與編碼選項就行了。在本節中，我們會著重於如何在你的 ISP 並不支援 PPTP 的狀況下，設定 NT 用戶端來使用 PPTP 協定。我們先把設定的步驟條列出來，在此之前，我們假設你已經會建立撥號網路，並與你的 ISP 建立 PPP 連線，這應該難不倒你，不是嗎？

1. 先依照在【5.1.1】一節中所指示的方法，依照在 RAS 伺服器上建構 PPTP 協定的步驟，來建立 PPTP 協定。
2. RAS 的組態設定與【5.1.2】一節中所介紹的非常類似。但在步驟 3 中，你必須按下“遠端存取”對話方塊中的“設定”鈕，並點選“只限撥出”，因為這是用戶端，我們需要撥號到 ISP 或 RAS 伺服器，而不是撥入。
3. 點選在“我的電腦”中的“撥號網路”。當出現撥號網路對話方塊時，按下“新增”，然後輸入你想撥入的 VPN 連線名稱，而我們輸入的是“總公司 VPN”，在“電話號碼”欄位中，輸入你想連線的 RAS 伺服器之 IP 位址，以我們的案例而言，這是 2.1.1.60。在“撥號使用”欄位中，選一個安裝 PPTP 及 RAS 時所建立的 VPN 連接埠，名稱是 RASPPTM (VPNn)，n 代表連接埠的編號，請參考圖 5-5。





100 / 第五章



圖 5-4 : 設定一個遠端存取的使用者

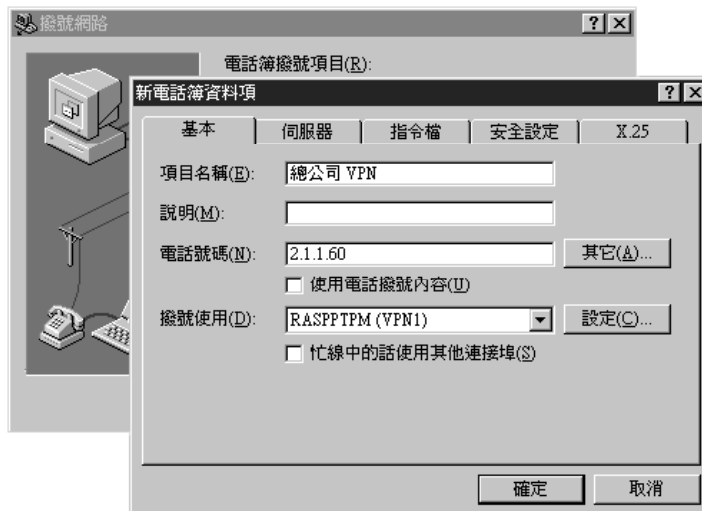


圖 5-5 : 設定一個使用 PPTP 裝置的撥號網路





- 你也可以指定要使用哪一種驗證機制，並決定用戶端資料是否需要加密。也是在同一樣的電話簿對話方塊中，按下“安全設定”標籤，此時你應該會看到如圖 5-6 的視窗，對一個最安全的 VPN 來說，你必須選擇“只接受 Microsoft 編碼確認”，並點選“需要資料編碼”。不管你撥號進入的 ISP 有無支援 PPTP，如果你的用戶端支援的話，你最好使用 MS-CHAP 及其加密機制。



圖 5-6：撥號網路的安全設定

5.3 設定 Windows 95/98 用戶端的 PPTP 撥號網路

我們曾經說過，Windows 95 並沒有內附 PPTP，你必須從 Microsoft 的網站 (www.microsoft.com) 下載「撥號網路更新版 1.3」(Dial-Up Networking Update 1.3)。因為更新版與 service packs 時常都會推出新版，所以你必須時常到 Microsoft 的網站上去看看，並把所需要的程式下載回來。撥號網路程式 (Dial-Up Networking，簡稱 DUN) 的更新很簡單，不用輸入任何參數，Microsoft 也有完整有用的文件，所以我們不會逐步教你安裝。我們之前已提到，Windows 98 本身已具備 VPN 的存取能力，所以不用外加任何軟體。





102 / 第五章

為了要設定 Windows 95/98 的 PPTP 的組態，你需要設定兩個撥號網路：一個連接到 ISP，另一個連接 PPTP 伺服器。因為大部分人都已經相當熟悉 DUN 連接到 ISP 的設定，所以我省略這個步驟。若你真的從沒做過，你可以在 DUN 更新版所附的說明文件中找到相關說明。

為了要建構你的 VPN DUN 設定檔，你必須照著以下的步驟做：

1. 點選【我的電腦->撥號網路】。
2. 當“撥號網路”視窗出現時，按下“建立新的連線”。
3. 這時“建立新的連線”精靈會出現，在“請輸入對方電腦的名稱”欄位中填入“總公司 VPN”(如圖 5-7 所示)，並選擇裝置為“Microsoft VPN adapter”，然後按“下一步”。



圖 5-7：使用“建立新的連線”精靈新增 VPN 設定檔

4. 接下來會出現一個對話方塊，要求你輸入 VPN 伺服器的名稱或位址，以我們的案例，在此輸入 2.1.1.60 (如圖 5-8)。
5. 依序按“下一步”、“完成”之後，在撥號網路視窗中會多一個名為“總公司 VPN”的圖示。





圖 5-8：輸入VPN伺服器的 IP 位址

6. 接著點選該圖示，並按下滑鼠右鍵，選擇“內容”，便會出現如圖 5-9 的對話方塊，顯示你剛剛所輸入的資訊；此時請點選“伺服器類型”標籤。
7. 在如圖 5-10的對話方塊中，若你要登入 Windows NT 或是 Novell NetWare 網路，請勾選“登入網路”與“啟動軟體壓縮”。但是不要勾選“需要加密的密碼”，稍後會說明理由。
8. 在“可用的網路通訊協定”中，選擇你在遠端網路上所需要使用的協定。請視情況需要自行選擇，必要的話，可勾選“TCP/IP”，按下“TCP/IP 設定值”，然後輸入固定的 IP 位址（要先點選“指定 IP 位置”）、指定名稱伺服器的位址（就是 DNS 伺服器的 IP 位址）、決定是否要使用遠端網路的預設通訊閘，最後按下“確定”以儲存你所輸入的設定。

5.4 啟動遠端存取轉接器上的 PPTP

有了伺服器端，也有了用戶端，我們還少了什麼？沒錯，ISP 的「遠端存取轉接器」（Remote Access Switch）。本節將討論 ISP 業者或者是網管人員如何在他們的轉接器上設定 PPTP 服務；ISP 會想如此做，是為了要提供更多的加值服務給其客戶；



104 / 第五章



圖 5-9：總公司 VPN 設定檔的“一般”選項

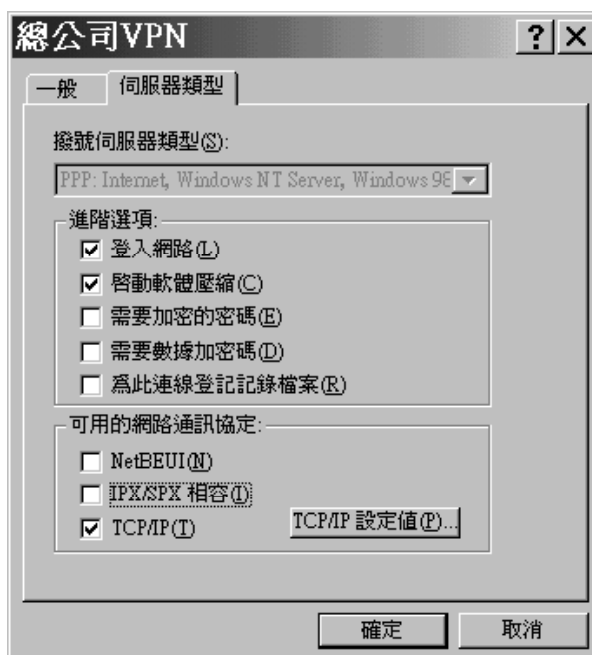
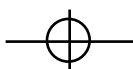


圖 5-10：總公司 VPN 設定檔的“伺服器類型”選項





網管人員則是為了減輕 RAS 伺服器的網路負載，或者只是為了增加網路頻寬。例如，Ascend 的 MAX 4004 可以處理 48 個類比數據機的連線，事實上，要 NT 來處理這樣數目的連線，其表現可能會非常地差。在這裡，我們會介紹兩種最常見的遠端存取轉接器：3Com/U.S. Robotics 的 Total Control Enterprise Network Hub（後文簡稱 USR switch）和 Ascend 的 MAX 4004。

5.4.1 在 Total Control Enterprise Network Hub 設定 PPTP

典型的 USR switch 配備有一張 NETServer 卡、一張有雙埠的 ISDN PRI 卡（共提供 23 個 64-Kbps 頻道），以及 48 部數位數據機。自 NETServer 3.2 版之後的韌體開始支援 PPTP 的功能。USR switch 提供三種方案來支援 PPTP：只開放某個 port 支援 PPTP（稱為「通訊埠模式」）、只讓某些特定使用者可以使用 PPTP（稱為「用戶模式」）、來者不拒（不管是來自哪一個 port，也不管使用者是何方神聖，我們稱此為「全域模式」）。

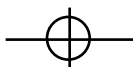
5.4.1.1 設定全域模式

你最多可為 USR switch 的 NETServer 卡設定 8 個全域 PPTP RAS 主機。假如有某個 port 或使用者需要 PPTP 服務，但沒有指定特定的 RAS 伺服器，NETServer 卡將會使用這些主機，首先會嘗試連線到第一順位的主機，若不行，則依序向後找尋可連線的主機。如果你使用 USR switch 來提供單一的 Windows NT 網域的撥接服務（就像是公司內部的網路），我們建議使用「全域參數」（global parameter）；但此方案則不適用於 ISP 業者，因為使用者可能來自不同的公司，而每個公司分別有自己的 RAS 伺服器。

以下是設定全域參數的步驟：

1. 用 Telnet 或是透過串列界面以 “!root”（管理者帳號）登入 NETServer 卡。
2. 使用以下的命令去建立 PPTP 主機。

```
set pptphost number hostname | ipaddress
```





106 / 第五章

其中的 number 代表的是 PPTP 主機的編號 (由 1 到 8), 若沒有指定, 則預設值為 1; 你可以使用 IP 位址 (ipadress) 或主機的「完整網域名稱」 (Full Qualified Doman Name, FQDN) (hostname) 來設定 RAS 伺服器。我們建議使用 IP 位址, 以避免 FQDN hostname 無法被解譯時的麻煩。

3. 使用 "Save All" 指令將設定寫入 USR Switch 的記憶體內。

5.4.1.2 設定通訊埠模式

NETServer 卡有許多的通訊埠, 每個埠都連接到它所支援到的各個撥接設備, 從 "S0" 開始編號到 "S64", 如果你有專屬的頻道 (例如: 租用專線), 你可能會想把只用某個特定通訊埠的來支援 PPTP, 其步驟如下。

1. 在命令提示符號下, 輸入以下命令以設定 PPTP 所用的通訊埠。

```
set port network hardwired
```

其中的 port 指的是通訊埠編號 (S1, S24, S48等), 如果要讓所有的通訊埠都支援 PPTP, 可以使用 "all" 來表示所有的通訊埠。

2. 輸入下列命令, 讓先前所挑選的通訊埠能支援 PPTP 協定。

```
set port protocol pptp
```

3. 然後指定一部 PPTP 主機給指定的通訊埠:

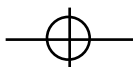
```
set port ppiphost number hostname | ipaddress
```

如果省略這個指令, 就會使用全域的 PPTP 主機。

4. 最後, 重新啟動該通訊埠, 讓剛剛的命令生效。

```
reset port
```

5. 使用 "Save All" 指令將設定寫入 USR switch 的記憶體內。





5.4.1.3 設定用戶模式

對 ISP 業者來說，最理想的方式，就是讓遠端存取轉接器為各別的使用者設定 PPTP；此種模式將可允許個別的使用者連接到不同的 PPTP 主機。每個使用者可以設定 7 部 RAS 主機來用作嘗試連線之用。

以下是在 USR switch 上為個別使用者設定 PPTP 服務的步驟：

1. 使用以下的命令加入新的 PPTP 使用者：

```
add netuser username password clear-text_password protocol pptp
```

其中的 `username` 是 8 個字元長度的使用者登入名稱，`password` 是密碼參數（可有可無），`clear-text_password` 則是 8 個字元長度的登入密碼【註】。在本案例中，我們輸入：

```
add netuser bill password CrAzY*MX protocol pptp
```

你可以把擔任使用者驗證工作的 RAS 主機加入，如果省略此參數，則會使用全域的 PPTP 主機。此指令跟指定通訊埠給 PPTP 主機相當類似，除了多了一個 `netuser` 參數：

```
set netuser username pptphost number hostname | ipaddress
```

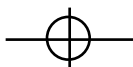
在我們的案例中，我們輸入：

```
set netuser saran pptphost 1 2.1.1.60
```

2. 使用 "Save All" 指令將設定寫入 hub 的記憶體內。同時使用 `show netuser` 指令將會顯示相關資訊，例如：

```
Command> show netuser bill
Username: bill                               Type: Dial-in Network User
Protocol: PPTP                               Options:
PPTP hosts: 2.1.1.60
2.1.1.33
```

註 所謂的 `clear-text`，是說輸入此命令時，密碼是以明文的狀態呈現而已，不是說會將密碼以明文形態使用或儲存。





5.4.2 在 Ascend MAX 4004 設定 PPTP

在 Ascend MAX 4000 系列中，4.6Bi12 之後版本的韌體開始支援 PPTP。最典型的 Ascend MAX 4004 支援了4條 T1 或 PRI 線路、和 48 部數位數據機。它不像 USR switch 那樣支援三種模式，它只能依據個別的線路來設定 PPTP 伺服器，而且其每條線路都是 WAN 界面。在 MAX 1800，所能連接的線路為 BRI ISDN，而在 MAX 4004 上，線路則為 T1 或 PRI；這會對想要提供 PPTP 服務的 ISP 造成困擾，因為不同的客戶所使用的 RAS 伺服器也不同。我們期待 Ascend 在不久的將來可以改進這個問題。然而，若只是應付單一 Windows NT 網域撥號服務的，這倒是個可行的方案。請注意，MAX 會將所有驗證的資料經由 PPP 連線傳送給 RAS 伺服器，所以 MAX 上不須存有任何使用者或是 RADIUS 的設定檔。

以下是在 Ascend MAX 4004 上設定 PPTP 的步驟：

1. 從主要 Edit 視窗選單，選擇【Ethernet -> Mod Config -> PPTP】選項。
2. 在 PPTP option 選單下，讓 PPTP Enabled=YES，然後按下 Enter 鍵。

每條 Route line 至少都要對應到一台 PPTP 主機，如果你只想讓某些線路可以接收 PPTP call，只要為該線路輸入 IP 位址就可以了，而其它未輸入位址的線路會使用預設值 0.0.0.0，表示以一般的方式來處理 call。然而，若你已經啟用 PPTP 功能，但沒有指定任何線路（所有線路都設為 0.0.0.0），則 MAX 會把所有的 call 都當成是 PPTP call，而且不再接受其它的撥入的 call，並同時關閉選徑的功能。以我們的案例來說，我們讓 4 條 PRI 線路使用同樣的 PPTP 主機 1.1.1.60，如圖 5-11 所示。

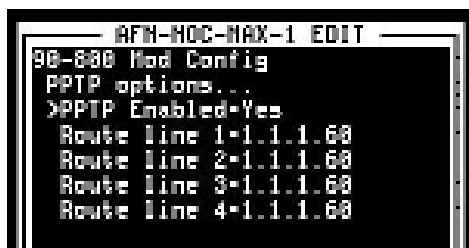
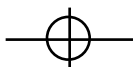


圖 5-11 Ascend MAX 4004 的 PPTP 線路設定畫面





3. 按下 Escape 鍵，並接受所有的變更，然後離開設定畫面，以便把新的 PPTP 資訊儲存在 MAX 的常態記憶體中。

5.5 進行撥號

當撥號進入支援 PPTP 的 ISP 時，所有 VPN 所需要的連線工作，都由 ISP 的遠端存取轉接器幫你搞定；你只要像設定直接撥入 RAS 伺服器一樣，把用戶端的設定弄好就行；至於身份驗證的資訊，ISP 的遠端存取轉接器會幫你轉送給 RAS 伺服器。

若撥號進入不支援 PPTP 的 ISP 時，你必須先利用撥號網路與 ISP 建立 PPP 連線，然後再點選 PPTP 連線（以我們的案例來說，就是“總公司VPN”），再按下“連線”，這將會透過你剛剛的 PPP 連線啟始一個 PPTP 呼叫連到 RAS 伺服器。

5.6 故障排除

如果你的系統沒辦法連線上線時，該怎麼辦？問題是出在哪裡？是遠端使用者的 ISP 嗎？還是總公司的 ISP？是 RAS 伺服器嗎？或用戶端？還是 Internet 掛了？有嫌疑的對象太多了，所以，要排除 VPN 的故障也特別困難。

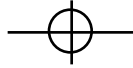
5.6.1 登入問題

對撥接到 RAS 的使用者來說，最常發生的問題，大概首推數據機的連線不穩定，像這樣的問題就可在用戶端解決；而驗證問題（不正確的使用者名稱、密碼、錯誤的驗證方法）則需要有人去查閱 RAS 伺服器上的日誌檔才可解決。Windows NT 的「事件檢視器」（Event Viewer）以及「撥號網路監視器」（Dial-Up Networking Monitor）則可幫助你解決這類的問題。

5.6.1.2 事件檢視器

事件檢視器是 Windows NT 通用的日誌系統，從【開始->程式集->系統管理工具（公用）->事件檢視器】就可以啟動它來查閱系統上發生了哪些事件。現在假設





110 / 第五章

Sara 沒辦法撥號進入，她認為似乎是協商的問題，但不能確定原因；這時你可藉著事件檢視器，依照她嘗試進入的時間，把任何的 RemoteAccess 訊息找出來，而在左邊的欄位，有圖示來標明資訊型訊息（一個字母 "i" 外有藍色圈），警告訊息（一個用黃色圓圈圈住的驚歎號），錯誤訊息（紅色的停止符號）。你看到在 Sara 試圖登入的時間的 RemoteAccess 訊息旁有一個紅色的錯誤訊息，在上頭按兩下，你便可以看到詳細的錯誤訊息（圖 5-12），由錯誤訊息得知，是 DHCP 的協商問題，問題排解的下一步是確定 Sara 是否已經被正確地設定了使用 DHCP 所配發的 IP 位址，並且確認你的 DHCP 伺服器可以正常運作。

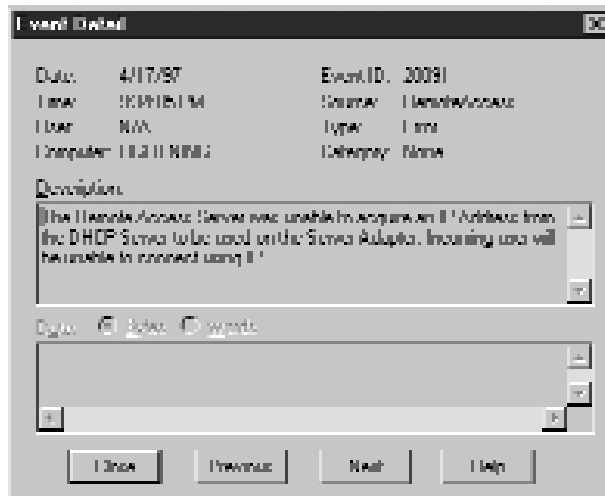


圖 5-12：一個失敗的 VPN 連線

事件檢視器也可用來查看成功登入的資訊，包括了使用者名稱、連接埠編號、連線時間，連線速度、輸出及輸入的總位元數。圖 5-13 即為一個成功登入的詳細資訊。

5.6.1.3 撥號監視器

你可以在“控制台”找到“撥號監視器”。它可用來監控目前的連線狀態，你不只可以在此察覺驗證問題，你還可以看到封包的進出狀況，以及連線設備的狀態（如圖 5-14）。



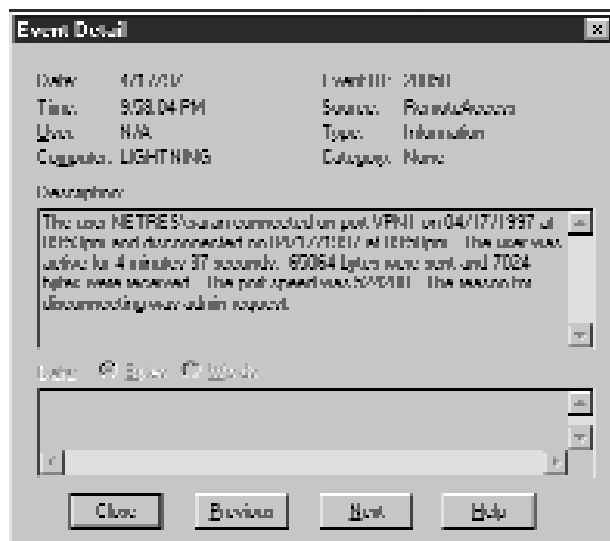
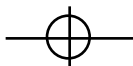


圖 5-13：一個成功登入 VPN 的連線資訊

5.6.2 連線測試

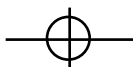
如果你的 PPTP 用戶端有無法撥入的問題，第一步要做的就是連線測試；這包括了用戶端與 ISP 之間的 PPP 連線，以及 ISP 與 RAS 伺服器之間的連線問題。請注意，連線測試只適用於與未提供 PPTP 服務的 ISP 連線，因為當你撥號到有提供 PPTP 服務的 ISP 時，你得通過 RAS 伺服器之後，才算真正連線成功。你可以用以下的方法，看看問題是不是真的出現在連線上。

5.6.2.1 ping 和 traceroute

對於 TCP/IP 網路而言，ping 是最適用來測試連線狀況的指令。在你連上 ISP 之後，你可以開一個 DOS 視窗，然後依照下列的指令格式用 ping 來測試你與 RAS 伺服器之間的連線狀況：

```
ping IP address of RAS server
```

在我們的案例中，你可以 ping 2.1.1.60，若你得到了成功的回應，表示你的連線狀況一切正常，不然，你可以再試著 ping 其它的機器，老練的工程師通常會 ping 所





112 / 第五章



圖 5-14：撥號監視器

連線的 ISP 的 DNS 伺服器，如果可能的話，還可以 ping 用戶端的另一路連線。如果最後的結果，是你能 ping 到另一路的連線（當地的區域網路），但是 ping 不到 RAS 伺服器，則問題可能有以下幾種狀況：

- 你已經離線了！有時候用數據機連線常常會有這樣的問題，莫名其妙就突然斷線了，但撥號網路卻還是顯示連線中的狀態。如果你有外接式的數據機，你可以檢視數據機上的「載波偵測」(carrier detect，通常標示為 CD) 燈號是否有亮，以判斷你是不是在連線狀態。請注意，這不一定真的是數據機的問題，一些外來的因素，像是插撥、電話線不良、閃電、電話線旁的大哥大、太陽黑子、這些都可能干擾到電話線，造成突然斷線。
- 你的 PPP 連線沒有設定正確，請把 ISP 給你的 PPP 與 TCP/IP 設定資訊，和你自身的設定值做個比較，除非你有固定的位址，不然，你的 IP 位址和閘道器應該由 ISP 的 PPP 伺服器所配發的；同時，請確定 DNS 的設定正確無誤。





- Internet 核心網路壅塞、或主幹的選徑問題，也可能造成你無法存取公司的網路（不要懷疑，這種狀況時常發生！），要知道是不是 Internet 壅塞造成無法連線，最好的測試方法就是 ping 你公司 Internet 閘道器。若一切正常，就表示封包可以順利到達公司的網路，所以你可以假設問題可能來自 RAS 伺服器，有可能是 RAS 的設定不正確，再不然就是被關機了，或因為其它原因沒有連上線。

另外一個測試連線狀況的工具是 Traceroute。UNIX 的使用者對 traceroute 這支程式應該都相當熟悉，它會追蹤封包從起點到終點之間所走過的路徑，並把途中所經過的 "hops"（其它的閘道路由器）都列出來。在 Windows 95/98 和 Windows NT 系統裡，Traceroute 程式是稱作 TRACERT。Traceroute 並非完美無缺，由於它會透過一個特殊的 port【譯註】送出一個特殊的 UDP 封包，但是有些 ISP 會因為安全考量而擋下這類的封包（因為使用到了違法的 port），所以，若是你的 Traceroute 告訴你無法到達目的地，並不一定表示你的連線或機器有問題。

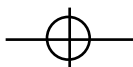
5.7 PPTP 與其它安全機制的運作考量

到目前為止，我們都是教你如何使用 PPTP 來建立 VPN；但是你的 VPN 能否順暢地運作下去，還要看你公司的區域網路安全措施是否夠健全；就像其它的協定一樣，PPTP 必須要能夠穿越防火牆，或是讓 proxy 伺服器放行（bypass），才能正常運作。

5.7.1 PPTP 穿越防火牆的考量

跟其他以 IP 為基礎的通道協定一樣，PPTP 使用了一個特定的 TCP port：1723。你必須讓你的防火牆或過濾器放行這類封包，才能讓 PPTP 進出，並與你的 RAS 伺服器溝通。若你的防火牆以通訊協定的種類來過濾封包，你也必須讓 GRE（IP protocol 47）可以穿過防火牆；把 RAS 伺服器上的其它 port 擋掉是個不錯的主

譯註 它會用到一個高於 1023 的 port，如果沒有特別設定，大多數的防火牆都會擋掉這類的封包，所以你要注意目的網路是否有防火牆的設置。





114 / 第五章

意，尤其是聲名狼籍的 NetBIOS name service、datagram 以及 session ports (137、138 和 139)。這些 port 可用來瀏覽你私有網路上各個機器的 NetBIOS 名稱，與網路上的資源分享狀況。

5.7.1.1 固定 IP 位址

因為遠端 PPTP 使用者會透過 ISP 連上線，他們不見得每次都會有相同的 IP 位址，所以不可能依據 IP 位址來過濾封包，更何況，PPTP VPN 應該依據使用者的身份來設定驗證系統才對，你不可能要求出差人員一定要在某處以某特定的電腦來上線，幾乎使用固定 IP 位址的政策都會遇到這類問題。此外，雖然有些 ISP 業者願意提供每次都配發相同 IP 位址的服務，但是多半得額外收費。無論如何，假設你不會有這樣的問題，使用固定的 IP 位址倒是一個不錯的選擇，你可以讓防火牆只允許特定 IP 位址的主機使用 port 1723 連接到 RAS 伺服器，而不必對所有的 IP 位址都開放讓 port 1723 可以通過防火牆。

5.7.2 如何讓 PPTP 越過 Proxy 伺服器

Proxy 伺服器的作用，就像是內部主機與 Internet 上目的主機之間的單幫客。一般來說，從外界看來，proxy 伺服器就像是內部網路上的唯一機器，它通常架設在需要穿越防火牆的 Internet 服務伺服器（像是 SMTP 郵件伺服器）之外側，網管人員可控制誰可以在防火牆之外存取何種 Internet 服務，雖然這看起來還蠻相配的，但 PPTP 的確會無法與某些 proxy 伺服器配合（唯一的例外是 Microsoft Proxy Server 2.0），因為 proxy 伺服器沒有提供適當的 socket 讓 PPTP 用戶端與伺服器端可以溝通。這意味著，你不能在 proxy 伺服器之後架設 PPTP 伺服器，因為用戶端無法越過 proxy 伺服器看到 PPTP 伺服器。在這種情況下，還是需要讓防火牆為 RAS 伺服器開一道門，然後讓 RAS 伺服器與 proxy 伺服器在路由器與區域網路之間腳踏兩條船（也就是兩種伺服器都成為 Multi-homed 伺服器）；Multi-homed 伺服器就是用兩片網路卡分別連接兩個分離的網路「區段」(segment)；然後還需要對每片網路卡都「啟用 IP 轉送」(IP Forwarding)【譯註】。

譯註 透過「控制台 -> 網路 -> 通訊協定 -> TCP/IP 通訊協定 -> 內容 -> 路由」，這樣一來，兩片網路卡之間就可以互相傳遞 IP 封包。

