前言

你坐在螢幕前盯著電腦，正疑惑為什麼連網速度越來越慢，希望從 ISP 業者一貫的閃爍其辭中獲得夠多的訊息。或者，你是任職於一家小公司的孤獨 IT 管理人員，之所以得到這份工作，僅僅是因為你知道交換器和集線器的差異而已，現在你卻被別人認為已經掌握了所有問題的答案。或者，你確實對於網路技術頗感興趣，想要學習更多知識，並立志以此作為職業。或者，你已經具備了豐富的知識，只是需要彌補某些知識漏洞。但是你發現，網路這一門學科，雖有大量參考資料，但這些資料通常不是那麼容易看懂，往往閱讀大量資料只是為了明白該按哪個按鈕。

為了把事情變得更有趣，你可能需要將 Linux 和 Windows 的主機整合起來。如果你想要挑選一本書，可以描述如何完成特定任務的詳細步驟，清晰闡釋所需的命令和配置，而且不會用那些雜亂無章，漫無邊際的理論和晦澀難懂的 RFC（Request For Comments）來考驗你的耐心，那麼你需要的就是這本書。

適合對象

理想情況下，你應該具備一些 Linux 的經驗，應該知道如何安裝和移除程式，瀏覽檔案系統，管理檔案權限，以及建立使用者和群組。你應該瞭解一些 TCP/IP 協議和乙太網路的基礎知識，與 IPv4、IPv6、區域網路、廣域網路、子網路、路由器、防火牆、閘道器、交換器、集線器，以及網路佈線等。如果你完全是從頭開始，那麼有一大堆介紹性的入門書可以加速你的基礎知識學習。

如果你還沒有具備基本的 Linux 的經驗，我建議先去讀《Linux Cookbook》（O'Reilly 出版）。《Linux Cookbook》（我是該書作者）是本書的姐妹篇。它涵蓋了安裝和移除軟體，使用者帳號管理，跨平台文件和印表機共用，跨平台用戶驗證，伺服服務程式（例如，郵件、網頁、DNS）中，備份和復原，系統急救和修復、配置 X 視窗、遠端管理，還有更多實用的主題。

家庭辦公（SOHO）的使用者還能在本書中發現一些有用的章節，而且任何想要學習 Linux 的網路的人都能透過兩台一般的 PC 和一些廉價的網路硬體，實踐本書中介紹的所有內容。

本書內容

本書共分為 19 章和三個附錄：

第 1 章，Linux 網路概述

本章是關於電腦網路的高層次概覽，涵蓋佈線、路由與交換、網卡、不同類型的網際網路服務，以及網路架構和性能的基礎知識。

第 2 章，透過單板電腦建立 Linux 閘道

在本章中，我們被引入令人著迷而且能適應各種環境的 Linux 路由器世界，例如，基於 Soekris 和 PC Engines 機板的產品，還有，較之那些貴出數倍的商業產品，本章介紹了如何基於此類機板的 Linux 作業系統，為你提供更強的功能和更佳的靈活性。

第 3 章，建立 Linux 防火牆

學習使用 Linux 的強大的 *iptables* 的封包過濾器來保護你的網路。本章案例全面介紹了邊界防火牆、單機防火牆、讓伺服服務穿越 NAT（網路地址轉換），阻止對內部網路存取的外部服務，穿過防火牆進行安全之遠端存取，以及如何在正式部署之前安全地測試新的防火牆等內容。

第 4 章，建立 Linux 無線存取點（AP）

你可以使用 Linux 和一塊路由板（或者任何一般的 PC 主機），定制一個符合需求且安全、強大、功能完整的無線 AP，包括先進的驗證和加密、名稱服務、路由和橋接等各項功能。

第 5 章，建立基於 Asterisk 的 VoIP 伺服器

本章深入剖析了革命性的網路電話（VoIP）最知名的 Asterisk 伺服器的相關內部細節。當然，近來出現的每個產品都有了漂亮，且以圖形介面點擊管理的 iPBX 系

統，不過你還是需要理解其內涵。本章將告訴你如何從頭開始安裝和配置 Asterisk：怎樣建立用戶分機和語音郵件、自訂歡迎語和訊息、發出廣播語音郵件、規劃電話、安裝數位總機、與 PSTN 的（公共交換電話網路）整合、純網路電話、管理用戶等等。

第 6 章，使用 Linux 路由

Linux 上的網路功能簡直就是一個發電廠，它包含了高級路由能力。這裡介紹的案例有，透過 Linux 建立路由器、計算網路遮罩（準確而且無痛苦）、阻擋不受歡迎的訪問者、使用靜態和動態路由，以及監控那些繁忙的小路由器等。

第 7 章，使用 SSH 進行安全的遠端管理

OpenSSH 的是一種非常安全的 SSH 協議之實現，令人驚奇而且極為有用。它支援傳統的基於密碼之方式登入，無需密碼之公鑰登入，以及支援經由不信任的網路進行安全的數據傳輸。你會學到如何完成上述所有工作，以及如何妥善地記錄。

第 8 章，使用跨平台遠端圖形桌面

OpenSSH 執行平滑流暢，可提供文字模式和安全的 X 視窗通道，用以執行許多圖形化的程式。還有多種優秀的程式（FreeNX、rdesktop 和 VNC）可作為功能上的補強，比如遠端幫助服務、遠端桌面，以及作為視窗終端服務器的使用者端。你可以透過一個鍵盤和一台顯示器控制多台電腦，甚至還能透過讓多個使用者觀看或參與同一個遠端會話，進行班級教學。

第 9 章，使用 OpenVPN 建立安全跨平台的虛擬私人網路

每個人似乎都想要一個安全，且擁有友善使用者介面的 VPN 網路（虛擬私人網路），但是關於 VPN 究竟是什麼，尚存有一些疑惑，很多商業化的產品並非真正的虛擬私人網路，而僅是透過 SSL 介面登入並提供有限服務而已。OpenVPN 是一個真正基於 SSL 的 VPN 產品，需要所有節點皆受信任，而且利用先進方法進行資料保護及連線加密。OpenVPN 其使用者端包含 Linux、Solaris、OpenBSD、FreeBSD 和 NetBSD 等多種使用者端，所以它是你綜合性的 VPN 解決方案。你將學會如何建立和管理自己的 PKI（公鑰基礎設施），這對於輕鬆管理的 OpenVPN 非常重要。而且，你還能學會如何安全地測試 OpenVPN，如何設定伺服器，以及如何連接使用者端等。

第 10 章，建立 Linux PPTP VPN 伺服器

本章涵蓋為 Windows 和 Linux 的使用者端建立並配置 Linux 上的 PPTP VPN 伺服器；如何替 Windows 使用者端進行修補，使它們支援 VPN 所需的加密功能；如何與 Mircosoft AD（Active Directory）整合，以及如何讓 PPTP 穿透 *iptables* 防火牆等相關內容。

第 11 章，在混合 Linux/Windows 的區域網路中使用 Samba 進行單一登入

使用 Samba 作為 Windows NT4 類型的領網域控制器，提供一個靈活、可靠、廉價的網路使用者端驗證機制。你將學會如何從 Windows 領域制器移轉到 Linux 上的 Samba，如何將 Windows 使用者帳號整合至 Samda，將 Linux 使用者帳號與 AD 整合，以及如何連及使用者端等。

第 12 章，使用 OpenLDAP 提供集中式網路目錄服務

LDAP 目錄是一種優秀的機制，可用它來構建網路目錄服務。本章告訴你如何從頭開始建立一個 OpenLDAP 的目錄，如何進行測試、如何變更、如何尋找內容、如何透過聰明索引（smart indexing）加速查詢，以及如何進行效能最佳化調校。

第 13 章，使用 Nagios 監控網路

Nagios 是一個極佳的網路監控系統，它利用標準 Linux 命令來監控服務和主機，而且還能在發現問題時即刻警示。狀態報告以漂亮的彩色圖形之 HTML 頁面顯示，可在網頁瀏覽器中直接查看。學習監控基本的系統健康狀況，以及通用服務如 DNS、WEB 和郵件伺服器，還有如何進行安全的遠端 Nagios 管理等。

第 14 章，使用 MRTG 監控網路

MRTG 是一個基於 SNMP 的網路監控程式，所以理論上它可適用於監控任何支援 SNMP 的設備或服務。學習如何監控硬體和服務，以及如何尋找所需的 SNMP 的資訊以建立監控點。

第 15 章，認識 IPv6

無論是否已做好準備，IPv6 的時代已經來臨，而且它終將取代 IPv4。藉由在區域網路和網際網路執行 IPv6 來趕上潮流，瞭解為何那些很長的 IPv6 的位址實際上比 IPv4 位址更容易管理，學習如何使用基於 IPv6 的 SSH，以及如何自動配置非 DHCP 的使用者端。

第 16 章，建立新系統自動網路安裝服務

Fedora Linux 及其所有同類發行版（Red Hat、CentOS、Mandriva、PC Linux OS 等等），還有 Debian Linux 與其衍生發行版本（Ubuntu、Mepis、Knoppix 等等）都包括了建立和複製自訂安裝，以及透過網路部署新系統的相關實用程式。所以，你可以準備一台電腦，然後在若干分鐘內就能將其重新安裝，並開始使用。本章描述了如何使用原有之安裝 ISO 影像檔進行 Fedora 的網路安裝，還有如何建立和維護本地區域端之 Debian 鏡像站。

第 17 章，透過 Serial Console 管理 Linux 伺服器

當乙太失效時，Serial Console 將會拯救這個世界，無論透過本地端還是遠端方式。此外，路由器和交換機常常透過 Serial Console 進行管理。學習如何設置一台 Linux 設備，使其接受 Serial Console 連接，以及如何使用 Linux、Mac OS X、或 Windows 個人電腦作為 Serial 終端機。你還將學會如何管理撥號伺服器，以及如何透過 Serial 連線上傳檔案。

第 18 章，運作 Linux 撥號伺服器

儘管已是現代社會，撥號網路還是很重要，我們離全球普及寬頻還很遙遠。本章介紹了建立基於撥號的網際網路連接共用，視需要撥號（Dail-on-Demand），使用 *cron* 安排定期撥號，以及建立多個撥號帳戶等相關內容。

第 19 章，網路故障診斷

Linux 包含種類豐富、功能強大的網路問題診斷和修復工具。你將會學到 *ping* 的深層奧秘，如何使用 *tcpdump* 和 Wireshark 竊聽，如何診斷名稱和郵件服務器的問題，如何發現網路上所有的主機，如何追蹤問題的根源，以及如何建立一台中央日誌伺服器。你還會學到大量不為人知但卻非常強大的實用工具，比如 *fping*、*httping*、*arping* 和 *mtr*，以及如何將一台一般的舊筆記型電腦改造成為必備且便於攜帶之網路診斷和修復工具。

附錄 A，參考文獻

電腦網路是一個廣泛而又複雜的主題，所以這裡提供了一份圖書和其他參考資料列表，它們告訴你哪些知識是需要知道的。

附錄 B，網路術語詞彙表

不知道這些術語是什麼意思？可在此查閱。

附錄 C，Linux 核心編譯參考

隨著 Linux 核心（Kernel）持續擴張檔案大小和功能，編譯 kernel 時將所有不需要的模組排除在外，是非常有用的。學習如何以 Fedora 方式、Debian 方式，以及源碼方式編譯自訂核心。

本書包含主題

本書同時涵蓋舊式和新奇的技術。舊時代的內容包括透過 Serial Console 進行系統管理、撥號網路、建立網際網路閘道器、虛擬區域網路、多種方式的遠端安全存取、路由與流量控制。新奇技術包括建立自己的 Asterisk iPBX、無線連接、跨平台遠端圖形桌面、自動化網路安裝新系統、混合 Linux 和 Windows 區域網路的單一登入，以及 IPv6 的基礎等。還有關於監控、警示和故障診斷的相關章節。

第一章

Linux 網路概述

1.0 介紹

電腦網路整體而言就是讓電腦之間相互對話的技術。說起來很簡單，實現起來卻很難。在這篇介紹中，我們將會鳥瞰 Linux 乙太網絡，還要看看支持其運作的諸多要素：路由器、防火牆、交換器、網路線、網路卡，以及不同類型的廣域網路和網際網路服務。

一個網路，無論它是 LAN（區域網路）還是 WAN（廣域網路），都可以認為具有兩個部分：電腦，以及與電腦間相互往來的所有東西。本書主要著重於網路連接相關部分：防火牆、無線存取點、遠端安全管理、遠端幫助、遠端用戶存取，虛擬私人網路、驗證、系統和網路監控，以及快速增長的 IP 語音服務（VoIP）。

我們將要說明以下工作任務，Linux 和 Unix 機器的連網、整合 Windows 主機、路由、使用者身份和驗證、共用網際網路連線、連接分支機構、名稱服務、有線和無線連接、安全、監控以及故障診斷等。

連接至網際網路

網路管理員所面臨的最大問題之一，就是如何安全地連接至網際網路。你需要怎樣的保護？你是否需要昂貴的商用路由器和防火牆產品？你如何實際的將區域網路連結至網際網路？

這裡是前兩個問題的答案：你至少需要一個防火牆和一個路由器，但是，你並不需要昂貴的商業設備。在一般個人電腦上執行的 Linux 系統，可以針對多數家庭和商業用戶之需求特性，為你提供所需的強大功能和靈活性。

選擇一家 ISP 業者

謹慎購買 ISP 業者的連線服務。這並不是個可以節省金錢的地方，因為一家好的服務商會賺取比其成本高出很多的錢。而一家較差的業者則會耗費你的金錢。你不得不依賴於他們，以獲取優良的服務和建議，還能讓他們為你而去跟電信公司和其他相關機構交涉。從瀏覽 DSL Reports（*http://dslreports.com*）開始，該網站包含了服務商的評價和大量的技術資訊。託管主機是一種可考量的替代方式，它在商業數據中心租用機架空間 — 你將在頻寬成本方面節省不少費用，而且無需為提供備份電源和設備之物理安全擔心。

最後那個問題的答案取決於網際網路服務之類型。Cable（有線電纜）和 DSL（數位用戶連線）比較簡單 — Cable 或 DSL 線路連接至一個廉價的頻寬數據機（Modem），然後連接至你的 Linux 防火牆/閘道器，再連接至你的區域網路交換器，如圖 1-1 所示。

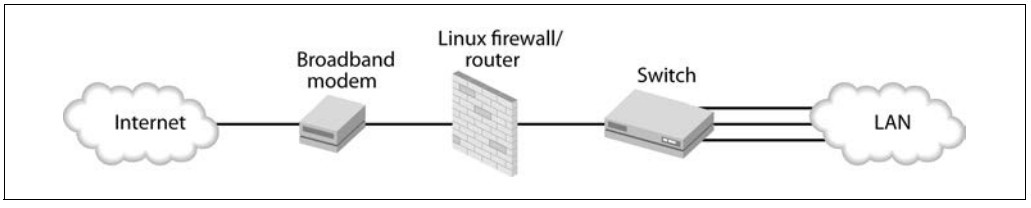

圖 1-1：寬頻的網際網路連線連接至一個小型的區域網路

在這篇介紹中，我將要提及位於區域網路和外部網絡之間的介面，也就是閘道器。從最小意義上說，這個閘道器就是一個路由器。它也許是一個不做其他任何額外事情的專用路由器。你可以在上面添加一個防火牆。你可能還想要其他服務，如領域名稱服務（DNS）、虛擬私人網路介面、無線存取點，或者遠端管理等。頗具吸引力的是，只要你想，它就可以掛載各種形式的服務，但基於安全和便於管理等方面考量，你最好保持網際網路閘道器儘可能的簡單。不要額外增加 Web、郵件、FTP 等或是驗證伺服服務。保持簡潔、平衡，並且儘可能不改變。

如果你想要將頻寬升級到專用線路，T1 線路就是下個選擇，其價格可與商用的 DSL 相比，但你將要用到一個特別的介面硬體，你需要在 Linux 閘道器中安裝一塊 PCI T1 的網卡（它比 DSL 數據機貴出許多），如此可以獲得更多的靈活性和操控性。為了精確地符合你的需求，你可能需要很多的準備及配置工作，例如：多個網路埠，以及支援數據和語音協定。

如果你喜歡商用路由器產品，可從你的 ISP 業者那裡找找是否有包含了一個免費路由器的連線服務可供選擇。如果你找不到提供較好路由器設備的免費服務，還可以看看市場上種類繁多的二手路由器，去尋找一台具有 T1 介面和能處理通道服務單元/數據

服務單元（CSU / DSU）的路由器，但不要對一個低階路由器有太多的期望 — 你的 Linux 機器一旦配上 T1 網卡，就會擁有更好的性能和更強的自訂能力。

一個典型的 T1 佈建如圖 1-2。

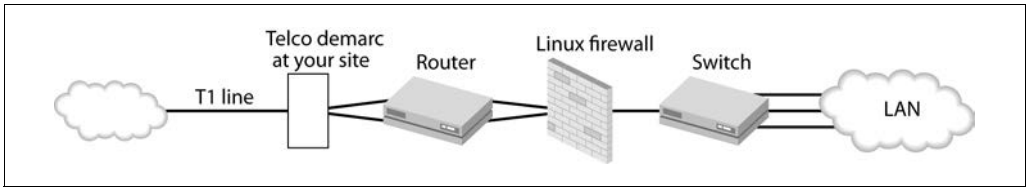

圖 1-2：連接至一條 T1 線路

T1 以上的電路，按服務等級和價格分級。高階服務可能要求不同類型的區域網路網卡硬體。一家好的 ISP 會告訴你什麼是你所需要的，並且提供相對應的服務。切勿自以為是而不求幫助 — 要知道電信技術一半是工程，一半是巫術，尤其當我們開始在語音線路上發送資料封包時。

網際網路服務選項概覽

如果你的安裝地點處於正確位置，勤勞的網路管理員就會列出很多關於優化連接之選項。一個聰明的技巧（儘管沒有被充分利用）是在租賃辦公場所前，先調查該場所現有的語音和數據服務狀況。搬遷到一個預先佈有線路的地方，你就可以節省金錢，免除煩惱。否則，你會發現自己會被撥號網絡或 ISDN、不穩定或價格高、超越實際需求的服務，搞得困窘不堪。

Cable、DSL 和撥號網路

Cable（電纜）、DSL 和撥號網路都是未受管制的服務。這些服務費用低，而且到處都有。

Cable

Cable 的網際網路服務通常與電視服務捆綁，儘管某些供應商只提供網際網路服務。Cable 的主要吸引力是可以提供比 DSL 更高頻寬的下載速度。很多 ISP 不允許使用者架設公開服務，甚至關閉通用 port（連接埠）如 22、25、80 和 110 等。某些 ISP 頻繁斷線，長時間當機，因為其不可靠的服務而臭名遠揚。儘管如此，某些 Cable ISP 還是好的，他們會全心全意為你服務，所以貨比三家不吃虧。要瞭解服務限制條款；某些 ISP 企圖針對每個客戶端區域網路收取費用，這就像自來水公司要按人頭收費一樣愚蠢。

第三章

建立 Linux 防火牆

3.0 介紹

在本章中，你將學到如何從頭開始建立一個 Linux *iptables* 防火牆。儘管相關各章節針對目標讀者是 DSL 和 Cable 用戶，所描述內容對於 T1/E1 客戶也同樣有效。實際上，具有 T1 網卡的 Linux 機器，是昂貴商用路由器的極佳替代品。如果你是普通的商業用戶，而是不那些需要透過巨型路由器來處理百萬條路由表的 ISP，在優質的 x86 機器上執行 Linux 也能滿足你的需求。

Linux 邊界防火牆（border firewall）可以提供安全保護，並為整個區域網路提供 Internet 連接共用，區域網路可以包括 Linux、Windows、Mac 及其他 PC 在內。單機防火牆可以保護單台 PC。還有許多種硬體可以作為防火牆伺服器，從小的單板電腦，到廢物利用的舊式 PC，再到機架式伺服器均可。任何 Linux 版本都包含了建立先進、可設定、可信賴的防火牆所需要的一切。

iptables 防火牆可同時用來進行封包過濾和路由指向，其角色和定義都會比較模糊。你不妨稱之為封包過濾路由器（filtering router）。

iptables 是讓一切成為可能的關鍵。只要具備關於 *iptables* 如何運作，以及如何制定政策（policy）的紮實基礎，你就能得到網路大師級水準的強大力量。請學習 Oskar Andreasson 的《Iptables 教學》（*http://iptables-tutorial.frozentux.net/*），以及 Craig Hunt 的《TCP/IP 網路管理》（O'Reilly）一書，深入理解 *iptables* 和 TCP/IP 是如何運作的。另一個優秀的資源是 Netfilter FAQ（*http://www.iptables.org/documentation/index.html*）。至少，你應該知道 IP、TCP、UDP 和 ICMP 封包都包含了哪些表頭（headers）資訊，而《Iptables 教學》中的 "Traversing Of Tables and Chains" 章節，則尤其有助於理解封包在 *iptables* 中的移動過程。如果你不知道這些，*iptables* 就會永遠保持其神秘性。

防火牆和路由器經常結合在一個設備中，通常稱之為網際網路閘道（Internet gateway）。嚴格地說，是一個在不同協定的網路之間進行數據移動的閘道，比如在我們不常見的 NetBEUI 和 TCP/IP 網路之間傳輸數據。近年來，它可以視為任何可連網的網路設備。

路由器在眾多網路之間轉發流量。你總是需要一個位於區域網路和其他網路之間的路由器。你還可以加上入侵偵測、流量控制、代理（proxy）、安全遠端存取、DNS/DHCP，以及任何其他想要的服務。儘管在我看來，最好是把你的防火牆功能限制在路由、防火牆和流量控制這三種功能範圍之內。其他服務應該位於防火牆後面單獨的機器上，當然，這完全取決於你的決定。在小型企業，用一台單獨的機器來運作多種服務也不算奇怪。其風險是任何成功入侵者都會享受一場可以滿溢出服務的盛宴，或者可能會讓該機器超過負載，從而導致效能受影響。

任何暴露給非信任網路的電腦或網路設備，都被稱為**堡壘主機**（bastion host）。顯然，堡壘主機有特殊的要求 — 它們必須是堅固的，與區域網路中的其他主機不共用驗證服務，而且必須有嚴格的存取控制。

私有和公用區隔

如果你準備運作網際網路可存取服務，就需要將你的公用（public）伺服器從私有區域網路中分離出來。如果你正在共用一條單獨的網際網路連線，最簡單的辦法就是建立一個具有三個介面（三片網卡）的 Linux 路由器，而第三片網卡就與你的非軍事區（DMZ）連線。**非軍事區**是一個敏感的區域，位於兩個相敵對的群組之間。在電腦術語中，這是一個單獨的子網路，用於將公用伺服器從私有區域網路主機中分離出來，而你的 DMZ 主機被視為僅次於網際網路上眾多邪惡勢力外的低可信任主機。

只要把你的公用伺服器放到一個不同的子網路中，就能增加一層有效的保護。DMZ 主機不能初始化反向的連線，無法連到私有網路，除非被明確允許。如果一台 DMZ 伺服器被攻陷，攻擊者應該不會找到通向私有網路的路徑。

如果你的 DMZ 主機擁有公用或者私有的 IP 地址也沒關係。千萬不要在區域網路內部的主機上運作公用服務。這實際上就是把整個網際網路黑洞引入了你的區域網路。

如果你的伺服器有公開可路由的 IP 位址（public IP），那麼不妨選擇直接將它們連線至網際網路或者一條單獨的網際網路連線。主機防火牆對於限制進入伺服器的流量，以及阻擋數以萬億計的網際網路自動攻擊非常有效。在你的公用伺服器前放一台獨立的防火牆，在不受歡迎的流量到達伺服器之前過濾掉它們，是一件很好的事。

Windows 安全

儘管防火牆很有用，還是要記得充分保證你的應用層和 OS 安全。某些管理員推薦將伺服器配置成如同沒有防火牆，那是一種不錯的策略。Linux 和 Unix 伺服器可以強化到那個水準，它們真的不需要防火牆。Windows 系統卻不可能強化到這個程度。防火牆也不可能解決所有問題。強大的 *iptables* 防火牆是 Windows 主機的最佳保護傘，但是防火牆無法防堵電子郵件惡意程式、被感染的網站，或者與日俱增的間諜軟體、廣告軟體、木馬和後門等等，也無法像商業的安全產品一樣偵測所有惡意行為的問題。

Iptables 和 NAT、SNAT，以及 DNAT

我們建置於 Linux 的 *iptables* 防火牆將要完成多項任務：

- 封包過濾
- 路由指向
- 網路位址轉換（NAT）

封包過濾是一種非常強大而富有彈性的機制，可以讓我們實現各種魔法，甚至在加密的傳輸上也能奏效，因為 TCP/IP 封包表頭是不加密的。*iptables* 規則可基於位址、協定、埠號（port number）和 TCP/IP 封包表頭的每一個部分進行過濾，它不會對任何類型的數據資料進行檢查和過濾。

擁有路由功能帶來了極大的便利，可以讓你將多種功能打包塞進一個單獨的設備，只要數行 *iptables* 規則即可。

NAT 是讓你可以在整個私有子網路中共用一個單獨的公用 IP 位址的神奇功能，還可以用私有不可路由的位址運作公用伺服器。假設你有一個典型的廉價 DSL 網際網路帳號，你只有一個單獨的公用 IP 位址，以及一個有著 25 台工作站、筆記型電腦和伺服器的區域網路，以 *iptables* NAT 防火牆作為保護。你的整個網路在外界看來如同單台電腦一樣（精明的網路專家可以滲透 NAT 防火牆，但這並不容易）。來源 NAT（SNAT）重寫所有流出（outgoing）封包的來源位址，將其改為防火牆的位址。

採用其他方式也同樣有效。儘管擁有公用可路由 IP 位址是 Web 和郵件之類的公用服務所必需的，你還是可以採用廉價的方式來實現，也就是在私有位址上運作公用伺服器。目標 NAT（DNAT）會重寫目的地位址，將防火牆位址改為真實的伺服器位址，然後 *iptables* 將流入（incoming）流量轉發到這些伺服器上。

某天，當 IPv6 廣泛實施的時候，我們才可以告別 NAT，而現在我們真的很需要它。它對於延伸有限可用的 IPv4 位址非常有用，還提供了一些潛在的安全特性。但是，它也帶來了一些路由問題。需要穿越 NAT 的協定，如 FTP、IRC、SMTP 和 HTTP 都內

嵌了很多天才般聰明的技術，使通訊變成為可能。點對點協定如 BitTorrent、即時傳訊（IM）和會話發起協定（SIP）尤其完美地實現了 NAT 穿越。

iptables 和 TCP/IP 表頭

iptables 讀取封包表頭的相關部分，但不包含資料欄位（data payload），所以它並不擅長內容過濾。

當你正在研究不同的協定時，你將遇到術語上的衝突。嚴格來說，IP 和 UDP 移動資料訊息（datagrams）、TCP 交換 segmemt 和 ICMP 封包都是訊息。在 *iptables* 的語境中，多數管理員只說 "封包"，儘管這樣要冒著惹惱那些學者般的網路工程師的風險。重要的是必須理解每次數據傳輸，都會分割為一系列的封包，獨立地在網路上旅行，常常要經過不同的路由。然後，當它們到達目的地時，TCP 協定會將它們以正確的順序重新組裝。每個封包都在其表頭中含有路由器所需的全部資訊，可以據此將其轉發到最終目的地。IP 和 UDP 是不可靠的協定，因為它們並不傳遞確認訊息，也因此它們傳輸速度很快。TCP 關注傳遞確認訊息、序列號和錯誤檢查，所以它會帶來一定的開銷，但是由此獲得了可靠性。TCP/IP 一起合作會帶來很高的可靠性。

如果你有任何關於連線網際網路或網路硬體基礎知識的問題，可以閱讀本書的介紹部分。

什麼時候需要防火牆？

你真的需要一個防火牆嗎？較短的答案是：如果你連線到其他網路，是的。Ubuntu Linux，是個著名的例子，在安裝過程中並不包括防火牆設定工具，因為它不會安裝對外運作的服務。沒有服務意味著沒有可以攻擊的目標。但是，我認為這樣就忽略了很重要的一點：當發生變化，錯誤產生時，分層防禦就是標準、最佳練習。儘管你的主機和網路是微不足道的，為何要讓它們受到外界攻擊的影響呢？當然應該把所有的垃圾都擋在你的防火牆之外，甚至公用服務也會受益於防火牆防護，例如，沒有必要讓你的 web 伺服器接受無止盡的 SSH 攻擊，還有橫行於網際網路的 MSSQL Server 蠕蟲的干擾，你完全可以把除了 TCP 80 port（埠）之外的所有東西都擋掉。對於你所有的主機也一樣：透過轉移非正常流量來降低負載，並在到達主機之前消除潛在的攻擊。

你可以想得更遠一點，按來源細分允許進入的流量。SSH 是一個範例 — 如果你不想允許來自外界無窮的連線嘗試，就得編寫規則只允許某些位址範圍或者特定的合法位址，而丟棄其他連線。