序

對網域名稱系統（**Domain Name System**，簡稱 **DNS**）你可能所知不多，但只要你用過 Internet（網際網路），你就用過 DNS。你能夠送出電子郵件、瀏覽全球資訊網（World Wide Web，簡稱 WWW），這都得靠 DNS 的幫忙。

身為人類的我們寧可記憶電腦的「名稱」，而電腦之間卻喜歡以「數字」相稱。在 internet（使用 TCP/IP 協定的網路）上，對 IPv4 而言，此數字有 32 位元長，其值域為零到四十億左右（2^{32}=4,294,967,296）。【註】電腦要記憶這種數字，簡直是小事一樁，因為它具有許多適合儲存數字的記憶體；但這對慣用邏輯思維的人類而言可就吃力了。不信邪？找來一本電話簿，隨便挑出十組電話號碼背背看，不容易吧！而記憶任意十組 internet 位址的難度，差不多就是這樣！

這只是我們需要 DNS 的原因之一。DNS 負責處理「主機名稱」與「internet 位址」間的對映關係；前者是為了方便人類記憶，而後者則是供電腦實際運作時所需。事實上，DNS 是 Internet 上傳佈和存取主機相關資訊的標準機制，其所提供的資訊並非只有位址而已。幾乎所有與網路相關的軟體，都會直接或間接用到 DNS，包括電子郵件、遠端終端機模擬程式（像是 *ssh*）、檔案傳送程式（像是 *ftp*）、網頁瀏覽器（像是 Microsoft 的 Internet Explorer）。

DNS 另一個重要的特性，是讓主機資訊得以散佈到 Internet 上每個角落。將主機資訊以檔案的形式放在某部電腦上，只有該電腦的使用者能夠受益。有了 DNS 卻能讓網路上位於任何地點的使用者，能夠從遠端取得資訊。

註　對 IPv6 而言，此數字有 128 位元長，其值域為零到 39 位數的十進制數字。

不僅如此，DNS 還能讓你將主機資訊的管理工作分配給多個網點（site）和組織。有了 DNS，你不必再把自己的資料往上提交到某個中央網點，也不必定期擷取主資料庫的副本。你只需要確定你的名稱伺服器（nameservers）所控管的部分 — 稱為轄區（**zone**）— 符合實際的狀況即可。而你的名稱伺服器會將你的轄區的資料提供給網路上所有其他的名稱伺服器。

因為資料庫分散各地，所以系統還需具備能力，遍尋各個可能的地點，以找到你想詢問的資料。有了 DNS，名稱伺服器便具備這樣的能力，可以在分散於各地的資料庫中，找出位於任一轄區的資料。

當然，DNS 並非完美無缺，它也有些問題存在。例如，為了相互備援，系統允許同一個轄區內，可以有超過一部以上的名稱伺服器儲存該轄區的資料。在這種情況下，轄區的最新資料就有可能跟舊副本之間發生不一致的狀況。

不過，DNS 最糟糕的問題是，儘管它在 Internet 上被如此廣泛地使用著，但是提及管理與維護 DNS 系統的文件卻是少之又少。Internet 上絕大多數的管理者，都必須跟廠商打交道，看看他們能提供哪些有用的資訊，要不就是利用相關主題的郵遞論壇（mailing list）或 Usenet 新聞群組互相討論交換心得。

缺乏文件的背後意義是，今日 Internet 上最龐大、最重要、最關鍵之服務的知識，竟然像祖傳秘笈一般，在管理者之間傳承著，或是不斷由獨立的程式設計者和工程師反覆學習著。而新進的轄區管理者只得嘗試無數的人已經犯過的錯誤。

這本書正是為了避免這種狀況而寫的。當然我們也理解到，並非所有讀者都有成為 DNS 專家的意願（或時間）。購買本書的讀者，除了管理自己的轄區和名稱伺服器，想必還有很多事要做：管理系統、規劃網路或開發軟體。因此，我們不會建議你把整本書重頭讀到尾，然後成為 DNS 專家。然而，我們將試著給你足夠的資訊，讓你能夠完成自己的任務：不管你控管的是個小轄區、或是個大型的跨國怪物，不管你只負責維護一部名稱伺服器、或同時要駕馭幾百部伺服器。閱讀本書你將可以找到你所需要知道的知識。

DNS 是一個大題目 — 大到需要兩位作者 — 但無論如何，我們會盡可能讓本書的內容易讀易懂，並同時兼顧實際與理論。我們將在前兩章，為讀者打好 DNS 的理論基礎，並提供足夠的實際資訊。隨後各章將逐一填補各項細節。稍後看到本書的閱讀指南時，你就會知道，要完成你想做的工作，應該要看哪幾章的內容。

當我們談論實際的 DNS 軟體時，幾乎都是指 BIND（Berkeley Internet Name Domain）這套最通行（就我們所知，它同時也是最好的）而且符合 DNS 規範的實作。我們嘗試匯整了自己用 BIND 管理與維護轄區的經驗，去蕪存菁後寫入本書。（附帶一提，我們所管理的轄區，曾是 Internet 上最大的網域之一，這不是為了自誇，而是希望讀者能信任我們所提供的資訊。）在必要時，也會提及我們實際用於管理工作的程式，為了速度與效率，這些程式多半都用 Perl 改寫過。

如果你才剛起步，我們希望這本書能幫你征服 DNS 與 BIND；如果你已經熟悉它們，我們希望這本書能讓你溫故知新。

版本說明

本書第五版涵蓋了 BIND 的新版本 9.3.2 與 8.4.7，以及 BIND 8 和 9 較舊的版本。寫作本書當時，BIND 9.3.2 與 8.4.7 是最新的版本，許多 Unix 版本的廠商並沒有將它們應用在自己的作業系統上，有部分原因是，這兩個版本才剛出爐，許多廠商對新發行的軟體通常都會比較謹慎。此外，我們偶爾也會提及 BIND 的其他版本，因為仍有許多 Unix 廠商在其所運交的產品中，納入了使用這些較舊版本的程式碼。當我們遇到版本 8.4.7 或 9.3.2 中特有的功能，或者版本的行為比較特立獨行時，我們都會嘗試加以解釋。

本書的範例中，我們常會用到名稱伺服器公用程式 *nslookup* 。我們所用的是 BIND 9.3.2 程式碼所隨附的版本。較舊版（但並非所有的版本）的 *nslookup*，其所提供的功能比 9.3.2 版的 *nslookup* 為多。在我們的範例中，我們會盡量使用多數 *nslookup* 版本通用的命令；實在沒辦法的話，我們會加以說明。

第五版新增了哪些內容？

除了更新本書的內容讓它涵蓋 BIND 最新的版本，第五版還加入了相當多的新資料：

- 在第 5 章加入 Sender Policy Framework（送信者政策框架，簡稱 SPF）的內容
- 在第 10 章更廣泛地加入 dynamic update（動態更新）與 NOTIFY 的資料，包括經簽章的動態更新，以及 BIND 9 的新 *update-policy* 機制
- 在第 10 章介紹 incremental zone transfer（遞增式轄區資訊傳送）機制
- 在第 10 章介紹支援條件式轉送功能的 forward zone（轉送轄區）機制
- 在第 10 章最後一節介紹如何使用 AAAA 紀錄和 ip6.arpa 分別進行 IPv6 的正向和反向對映
- 在第 11 章介紹 transaction signature（交易簽章），也就是所謂的 TSIG，這是 DNS 用來驗證交易的新機制
- 第 11 章中，名稱伺服器安全防護的內容被擴充成一節的篇幅
- 第 11 章中，Internet 防火牆的內容被擴充成一節的篇幅
- 在第 11 章介紹經修訂之 DNS Security Extensions（或 DNSSECbis）的內容，這是一個用數位簽章來簽署轄區資料的新機制
- 新增一章（第 16 章）介紹如何為一個組織設計一個完整的 DNS 架構

- 在第 17 章介紹 ENUM，說明如何將 E.164 電話號碼對映至 URI
- 在第 17 章介紹 Internationalized Domain Names（國際化網域名稱，簡稱 IDN），這是一個在網域名稱的標籤中編碼 Unicode 字符的標準
- 在第 17 章最後一節加入 Active Directory 的內容

本書結構

基本上本書結構係採取循序漸進的方式。第 1 和 2 章，討論網域名稱系統的原理。第 3 到 6 章，協助你判斷是否應該設置自己的轄區、從何處著手、應該如何選擇。第 7 到 11 等中間章次，討論如何維護你的轄區、如何設定主機以便使用你的名稱伺服器、如何做好擴充轄區的規劃、如何建構子網域以及如何防護你的名稱伺服器。第 12 到 15 章是關於除錯工具和常見問題的探討，以及使用 resolver 程式庫常式撰寫程式時一些不為人知的技巧。第 16 章則將這一切整合成一個端對端架構。

本書的章節編排如下：

第一章，背景介紹

以簡短的歷史透視 DNS 的全貌，以及 DNS 發展的緣由，然後概要說明 DNS 的工作原理。

第二章，DNS 的運作細節

深入討論 DNS 的工作原理，包括 DNS 命名空間（namespace）的結構、網域、轄區以及名稱伺服器。同時還會介紹一些重要的概念，像是名稱解析（name resolution）以及快取（caching）。

第三章，從何處著手？

說明如何取得 BIND 軟體（如果你尚未擁有的話）、一旦取得之後該怎麼辦、如何選用你的網域名稱，以及如何跟可以委派（delegate）轄區給你的主管單位聯繫。

第四章，設置 BIND

詳細地說明如何設置你的頭兩部 BIND 名稱伺服器，包括建立你自己的名稱伺服器資料庫、啟動你的名稱伺服器以及檢視它們是否運作正常。

第五章，DNS 與電子郵件

討論與 DNS 之 MX 紀錄有關的議題，管理者可以透過 MX 紀錄指定代理主機，以便處理特定目的地的郵件。這章將會說明廣泛應用在網路與主機上的郵件選徑（mail routing）策略，包括使用防火牆的網路以及無法直接連通 Internet 的主機。本章還會說明 Sender Policy Framework（送信者政策框架），此機制會透過 DNS 授權郵件伺服器從特定電子郵件地址傳送郵件。

第六章，設定主機

解釋如何設定 BIND resolver（解析器）。本章還會特別指出 Windows resolver 的設定方式。

第七章，BIND 的維護與管理

定期的維護是 DNS 能夠順利運作的保證，本章會說明如何檢查名稱伺服器的健康狀態以及權威資料檔。

第八章，當網域成長時

說明擴展轄區的因應計劃，包括如何擴大，以及主機遷移、停電和斷線的因應計畫。

第九章，子網域的分割與管理

探索成為父網域的樂趣。本章會解釋何時應該變為父網域（建立子網域）、如何為子網域命名、如何建立子網域以及如何看管它們。

第十章，進階功能

介紹一些較不常用的名稱伺服器組態設定項，透過這些設定項的協助，你可以調校名稱伺服器的運作狀況以及簡化管理的工作。

第十一章，安全防護

說明如何防護你的名稱伺服器的安全、如何設定你的名稱伺服器讓它因應 Internet 防火牆的需要，同時還會介紹 DNS 的安全性做哪些強化工作：DNS Security Extension 以及 Transaction Signature。

第十二章，nslookup 與 dig

展示以工具程式 nslookup 與 dig 實施 DNS 除錯作業時的輸入與輸出，包括如何解讀遠端名稱伺服器所提供之不明確資訊的技巧。

第十三章，解讀 BIND 的除錯訊息

這章是 BIND 除錯資訊的羅塞達石（Rosetta stone）【譯註】。本章應該可以協助你理解 BIND 所送出的除錯資訊，進而讓你對名稱伺服器有更深入的了解。

第十四章，排除 DNS 與 BIND 的問題

先介紹許多常見的問題以及解決方案，然後說明數種不常見的、難以診斷的狀況。

譯註　羅塞達石（Rosetta stone）是解釋古埃及象形文字的線索。

第十五章，DNS 程式設計

示範如何展寫 C 程式，透過 BIND 的 resolver 常式，詢問名稱伺服器以及擷取資料；同時也會介紹 Perl 命令稿的做法。我們還提供了一支有用的程式（希望如此！）可用來檢查自己名稱伺服器的健康狀況，以及權威資料的設定是否正確。

第十六章，架構

呈現 DNS 基礎結構的端對端設計，包括外部名稱伺服器、代詢伺服器以及內部名稱伺服器。

第十七章，雜項

將一些尚未探究的議題納入本章討論。本章會介紹 DNS 的通配符、透過撥接暫時連通 Internet 的主機與網路、網路名稱的編碼、其他的紀錄型態、ENUM、IDN 以及 Active Directory。

附錄 A，DNS 訊息的格式與資源紀錄

逐位元組（byte-by-byte）地剖析 DNS 之詢問與回應封包中的訊息格式，同時還廣泛地列示了目前有定義的資源紀錄型態。

附錄 B，BIND 各版本的相容性對照表

將 BIND 各個最主要版本的最重要特性製成對照表，供讀者參考。

附錄 C，如何在 Linux 機器上編譯與安裝 BIND 軟體

提供如何在 Linux 機器上編譯與安裝 BIND 9.3.2 的逐步指引。

附錄 D，頂層網域

列示 Internet 網域命名空間中，目前的頂層網域。

附錄 E，BIND 名稱伺服器及解析器的組態

摘要說明名稱伺服器以及解析器之組態設定項的語法和語義。

閱讀指南

本書主要是為負責管理轄區以及一或多個名稱伺服器的系統和網路管理者而寫的，不過它也提供網路工程師、郵件管理者以及其他人所需要的資訊。雖然全書章節的安排是循序漸進的，但並非每個人都需要逐一閱讀完所有章節。想當然，你也不願意從頭看到最後一章才找到所需要的資訊。我們希望這篇指南能協助你閱讀本書。

初次設置轄區的系統管理者

應該閱讀第 1、2 章對 DNS 原理的解說，參考第 3 章對如何著手規劃、挑選網域名稱的建議，看第 4、5 章來瞭解初次設置轄區有哪些工作要做，看第 6 章來瞭解如何設定主機以便使用新的名稱伺服器。完成以上這些工作後，你的轄區應該可以

順利運作了，但是建議你還應該看看第 7 章，學習如何設置多部名稱伺服器，以及如何新增轄區資料。然後跳到第 12、13、14 章，學習排除故障的工具與技術。

有經驗的管理者

可以從第 6 章開始，學習如何在不同的主機上設定 DNS resolver；第 7 章可以學到如何維護轄區；第 8 章則提供了如何為轄區的成長與變遷預作規劃的建議，對於控管大型轄區的管理者們，這一章應該特別有價值。第 9 章說明了子網域的分割與管理，打算進行此大動作的管理者，應該看看這一章的建議。第 10 章涵蓋了 BIND 9.3.2 和 8.4.7 名稱伺服器中許多新的以及進階的功能，有經驗的管理者可能會對這些資訊特別感興趣。第 12 到 14 章所介紹的問題排除工具與技術，即使是進階的管理者也值得一讀。第 16 章可以協助管理者以大藍圖來理解 DNS 的架構。

所管理的網路並非全天候與 Internet 連線之系統管理者

應該閱讀第 5 章，看看如何在這類網路上規劃郵件服務，以及第 11 和 17 章，學習設置獨立之 DNS 基礎結構的方法。

程式設計人員

應該閱讀第 1、2 章對 DNS 原理的解說，然後參考 15 章對如何以 BIND resolver 程式庫常式進行程式設計的詳細說明。

不直接參與任何轄區管理工作的網路管理者

仍然應該看看第 1、2 章對 DNS 原理的解說，然後學習第 12 章所提供之 *nslookup* 與 *dig* 的使用技巧，以及第 14 章的問題排除技巧。

郵件系統的管理者

應該閱讀第 1、2 章對 DNS 原理的解說，然後到第 5 章看看 DNS 與電子郵件如何共存。此外，瞭解第 12 章所介紹的工具程式 *nslookup* 與 *dig* ，應該能協助你從網域命名空間中擷取出郵件選徑資訊。

對 DNS 有興趣的讀者

可以看看第 1、2 章所介紹的 DNS 工作原理，然後隨興閱讀你認為有用的章節。

請注意，本書假設讀者已經熟悉基本的 Unix 系統管理、TCP/IP 網路架構，並能使用 Perl 與 shell 命令稿來設計簡單的程式。當我們介紹新術語或觀念時，我們會盡量給你一個明確而清楚的定義與解釋。如果可能，我們將從 Unix （以及實際的世界）舉例說明，以幫助你釐清觀念。

建議和問題

歐萊禮公司是世界性的電腦資訊出版公司。我們永遠樂意聽到讀者對出版品的意見，包括如何讓本書可以更好的建議、指正本書的錯誤、或是讀者建議本書往後改版時，應該再加進來的其它主題。以下是本公司的聯絡資料：

美商歐萊禮股份有限公司台灣分公司

電話：（02）2709-9669 傳真：（02）2703-8802

網頁：*http://www.oreilly.com.tw*

電子郵件：*mail@oreilly.com.tw*

與本書有關的線上資訊（可能包括勘誤、範例程式、相關連結）：

原文書

http://www.oreilly.com/catalog/dns5/

中文書

http://www.oreilly.com.tw/product2_network.php?id=a225

本書的慣例

本書採用下列字型與格式印刷 Unix 命令、工具程式以及系統呼叫：

- 組態檔或命令稿的內容以定寬字印刷：

```
if test -x /usr/sbin/named -a -f /etc/named.conf
then
    /usr/sbin/named
fi
```

- 在人機互動的範例中，一樣以定寬字印刷命令列的輸入以及相應的輸出，但是會把使用者動手鍵入的內容加粗印刷：

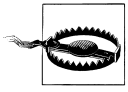
```
%  cat /var/run/named.pid
78
```

- 對於需要擁有超級使用者（root）權限才能執行的命令，我們會以井字號（#）來表示：

```
# /usr/sbin/named
```

- 程式碼中可供代換的部分（例如變數）會以定寬斜體字印刷。
- 內文中若出現網域名稱、檔名、函式、命令、Unix 的線上說明文件（manpage），以及從程式碼中所取出的片段，會以斜體字印刷。

此符號代表「訣竅」、「建議」或「一般注意事項」。



此符號代表「警告」。

使用範例程式

本書的宗旨是協助你搞定工作。一般而言，你可以將本書的程式碼用在你的程式裡，或是在文件裡提及，而無須要求我們的同意，除非你想大幅度引用。舉例來說，使用本書範例裡的幾個程式片段，無須經過我們的同意；但如果打算將 O'Reilly 書籍裡的範例程式燒錄成光碟來銷售或散佈，則需要授權。引用本書內文或程式片段來回答問題，不需要授權；但如果大量引用本書範例到你的產品說明書裡，則需要知會我們。

如果你引用本書（內文或範例程式），我們會感謝你註明出處，但沒要求你必須得這麼做。如果你願意，請註明書名、作者、出版公司以及 ISBN。例如："DNS and BIND, Fifth Edition, by Cricket Liu and Paul Albitz. Copyright 2006 O'Reilly Media, Inc., 0-596-10057-4."

每一章的引文

本書每一章開頭所引用的文句係來自 Lewis Carroll（路易士・卡洛爾）的著作《Alice's Adventures in Wonderland》（愛麗絲夢遊仙境）和《Through the Looking-Glass》（愛麗絲鏡中奇遇），而《Alice's Adventures in Wonderland》所採用的是 Project Gutenberg（古登堡計畫）的 Millennium Fulcrum 2.9 版，《Through the Looking-Glass》所採用的是 Millennium Fulcrum 1.7 版。第 1、2、5、6、8 和 14 章的開頭文句引用自《Alice's Adventures in Wonderland》，而 3、4、7、9-13 和 15-17 等章次的開頭文句則引用自《Through the Looking-Glass》。

致謝

我們想要感謝 Ken Stone、Jerry McCollom、Peter Jeffe、Hal Stern、Christopher Durham、Bill Wisner、Dave Curry、Jeff Okamoto、Brad Knowles、K. Robert Elz 與 Paul Vixie 等人對本書無價的貢獻。我們還想要感謝本書的審閱者 Eric Pearce、Jack Repenning、Andrew Cherenson、Dan Trinkle、Bill LeFebvre 與 John Sechrest 等人的批評與建議，沒有他們的協助，這本書的內容不可能會如此地豐富。

對於第二版的技術審閱，我們要感謝這個表現超水準的團隊：Dave Barr、Nigel Campbell、Bill LeFebvre、Mike Milligan 與 Dan Trinkle.

對於第三版的技術審閱，我們要向這個夢幻團隊致敬：Bob Halley、Barry Margolin 與 Paul Vixie。

對於第四版的技術審閱，我們欠這個頂呱呱的團隊一份人情： Kevin Dunlap、Edward Lewis 與 Brian Wellington。

對於第五版的技術審閱，我們想要感謝這個令人讚賞的團隊：Joao Damas, Matt Larson 和 Paul Vixie，以及感謝 Silvia Hagen 對 IPv6 的緊急協助。

Cricket 要特別謝謝：他以前的經理 Rick Nordensten，他是現代 HP 經理人的典範，本書的第一版就是在他的關心之下寫成的；他的左鄰右舍，忍受這數月來他偶而亂發的脾氣；當然還有他的老婆 Paige 無怨無悔的支持，以及在她小睡片刻時忍受連綿不絕於耳的鍵盤聲。對於第二版，Cricket 還要感謝另兩位他以前的經理，Regina Kershner 與 Paul Klouda，支持他從事 Internet 的工作。對於第三版，Cricket 要感謝他在 Acme Razor 的工作夥伴 Matt Larson。對於第四版，Cricket 要感謝 Walter B. 以及 Dakota 與 Annie 等人，為他紓解心中的壓力。對於第五版，Cricket 要感謝 Baby G. 和他的朋友，以及他在 Infoblox 努力工作的同事，慷慨的支持和陪伴。

Paul 想要謝謝他的太太 Katherine，忍受他時常參加審閱會議的冷落，以及證明了她在空閒時間做一床被子的速度，比她的先生寫半本書的速度還快多了。