

第三章

本章內容：

- * 取得 BIND
- * 選用網域名稱

從何處著手？

目前你對 DNS 身後的理論應該有一定程度的瞭解，現在或許是我們多瞭解一下實際狀況的好時機。在開始設置網域之前，你必須先取得 BIND 這套軟體。大部分的 UNIX 系統都已經內附 BIND 套裝程式，但有些時候，你可能會想找到能夠安裝在特殊作業系統的版本，或是想要取得剛出爐的版本，以便使用 BIND 的最新功能。

一旦取得了 BIND 軟體後，你必須決定網域名稱——這可就沒那麼簡單了，因為你必須先在 Internet 的命名空間中找一個合適的上層（parent）網域。一旦決定好網域名稱的 parent 網域之後，你還需要和這個 parent 網域的管理者聯繫。

讓我們按部就班地著手！從如何取得 BIND 開始談起。

3.1 取得 BIND

假如你打算設置自己的網域，並在這個網域上執行名稱伺服器，你將需要 BIND 這套軟體。即使你打算讓別人管理你的網域，最好還是要備有 BIND 套裝程式。舉例來說，你可以先利用自己當地的名稱伺服器來測試資料檔，然後再把資料檔提供給遠端的網域管理者。

大多數商用版本的 UNIX 廠商都已將 BIND 附加在他們的標準 TCP/IP 軟體之上，並且這些網路軟體也都附在作業系統之中。所以就算使用商用版本的 UNIX 系統，你仍然可以免費使用 BIND 套裝程式。就算網路軟體與作業系統的價錢分開計算，你可能也已經買了，因為想要正常地使用網路，必須具備 DNS 的功能，不是嗎？

假如你手上沒有支援目前所用 UNIX 廠牌的 BIND 版本，或是想取得最新版的 BIND，你可以轉而取得 BIND 的原始程式碼。這非常容易，因為它是免費而自由流通的。最新版的 BIND 原始程式碼都可以透過網路免費取得。在本書英文版撰寫期間，BIND 已經發展到 8.1.2 版【譯註】。你可以從 ISC (Internet Software Consortium) 組織的網站 (<http://www.isc.org>) 取得，或透過匿名 ftp 直接到 <ftp.isc.org> 網站的 `/isc/bind/src/cur/bind-8/bind-src.tar.gz` 檔案路徑取得。在一般常用的 UNIX 平台底下，直接編譯這個原始碼應該非常簡單。ISC 組織在 Makefile 中附了一些常用 UNIX 版本的定義範例，包括 HP-UX、Irix、AIX、Solaris 與 SunOS 等。而本書的附錄 B 則提供在 Solaris 2.x 上編譯 BIND 最新版的步驟說明。

既然作業系統已經內附某個版本的 BIND，你可能會質疑還有必要取得最新版的 BIND 嗎？最新版的 BIND 有哪些功能是之前版本所沒有提供的呢？以下做了一些概略性的整理：

譯註 在編譯本書的當時 BIND 8 已經發行到 8.2.2-P5 的版本，而 BIND 9 也正在發展中。BIND 9 將著重在：提高 DNS 規模的擴充性（對 Thread safety、多元處理器、大型轄區等功能的支援）；加強安管功能（對 DNSSEC 以及 Firewall 等功能的支援）對 IPV6 的支援、等等。

對安全性的補強

最常見的例子就是，新版的 BIND 會補強一些在安全上易受到攻擊的弱點。BIND 8.1.2 擁有非常強固的安全防護特性【譯註】，BIND 4.9.7 也具備了部分的功能。在更早期的 BIND 則有許多眾所週知的弱點。如果你的名稱伺服器有連上 Internet，那麼我們將強烈建議你採用最新版的 BIND。

安管功能

BIND 8.1.2 支援了存取清單 (access list) 的管制功能，可以針對查詢、轄區資料傳輸、以及動態更新等服務，執行安全管制的作業。而使用 BIND 4.9 版本的伺服器則只支援查詢以及轄區資料傳輸的安管作業。更早期的版本就完全沒有 access list 的功能了。對於某些特定的名稱伺服器而言（特別是那些在防火牆的屏障主機上，或是其它安全性要求較高的主機上，執行的名稱伺服器），這些安全管制的功能是不可或缺的。

我們會在第十章中詳加討論安管功能。

DNS UPDATE 功能

BIND 8.1.2 支援 RFC 2136 所定義的動態更新標準 (Dynamic Update Standard)。它允許經授權的代理程式 (agent) 傳入特殊的更新訊息，以新增或刪除資源記錄的方式，更新轄區資料。若採用 BIND 4 版本的伺服器，則不支援動態更新的功能。

我們會在第十章中詳加討論這個功能。

DNS NOTIFY 功能

BIND 8.1.2 支援轄區資料的變更通知。也就是說當序號增加時，轄區的 primary master 名稱伺服器會對 slave 發出變更通知。BIND 4 並不支援這樣的功能。

關於 NOTIFY 的細節將在第十章討論。

譯註 其實 BIND 8.1.2 已被發現存在有 Denial of service (癱瘓服務) 的安全漏洞，期間歷經 8.2、8.2-P1、8.2.1、8.2.2、8.2.2-P1 一直到目前的 8.2.2-P5 版本。

組態的設定語法

BIND 8 的組態設定語法和 BIND 4 完全不同。雖然新的語法功能較為強大且彈性更佳，但是你必須重新學習這套新的設定系統。請不用擔心，這正是本書的重點。

我們將會在第四章介紹 BIND 8 組態的設定語法，並在整本書之上都使用這套語法。

看過了以上所列的清單之後，如果你仍然十分確定需要 BIND 8 的功能，並且你所使用的作業系統尚未提供 BIND 8 的伺服器，那麼你必須自行下載 BIND 原始程式碼，並重新編譯與安裝。

3.1.1 便利的郵遞論壇 (Mailing List) 和 USENET 網路新聞群組 (newsgroup)

若要指導你如何將 BIND 移植到各個版本的 UNIX 去，則幾乎可以再寫成另一本書了，因此我們建議各位加入與 BIND 有關的郵遞論壇 (bind@uunet.uu.net)，或是 USENET 網路新聞群組 (comp.protocol.s.dns.bind)，以便能隨時取得援助【註】。此外還有一個稱為 bind-workers 的郵遞論壇 (bind-workers@vix.com)，是一群測試新版 BIND 8 程式碼的人士們彼此討論問題的地方，這也是個提問題的絕佳場所。這些在 BIND 論壇上閱讀並提供資訊的人士們，將對你的移植工作提供莫大的幫助。在你要移植 BIND 之前，記得要諮詢這些人，看看是否已經有前例可循了。同時也請瀏覽一下 <http://www.isc.org/products/BIND/bind8.html> 網頁對 BIND 8 最新版本的介紹，你還可以透過內文中 security vulnerabilities 的超鏈結，瞭解 BIND 各種版本的安全漏洞。若你想知道目前有哪些預先編譯好之 BIND 軟體二元碼可用，則查閱 Andras Salamon 所提供的網頁 (<http://www.dns.net/dnsrd/bind.html>)，便能一目瞭然。

註 若想在 Internet 的郵遞論壇中發問，則你必須訂閱這份論壇。假如你想要加入這個論壇，那麼你得送出一個訂閱訊息給論壇的管理者，請他將你的電子郵件地址加到郵寄名單之中。千萬不要將這個訂閱訊息直接寄到論壇的地址去，這是很不禮貌的行為。根據 Internet 的慣例，你可以透過 list-request@domain 的通信模式與郵遞論壇的管理者聯繫：其中 list@domain 是該郵遞論壇的地址；但是，只要在收信者名稱欄中附加上 -request 之後，則就成為了論壇管理者的地址。譬如，你可以經由 bind-request@uunet.uu.net 與 BIND 郵遞論壇的管理者聯繫。

此外，你可能會對另一個稱為 `namedroppers` 的郵遞論壇感到興趣。`namedroppers` 的訂閱者通常只討論 DNS 的相關議題，而非 BIND 方面的問題。例如，關於 DNS 協定的功能擴充、或對 DNS 記錄型態的建議、等等的討論都會在這裡出現。應避免將相同的信息寄到每個郵遞論壇去，因為大多數人都會同時訂閱這些郵遞論壇。

`namedroppers` 郵遞論壇的地址是 `namedroppers@internic.net`，它常會與名為 `comp.protocols.tcp-ip.domains` 的網路新聞群組交換信息。若想加入 `namedroppers` 的郵遞論壇，請先寄出一封要求訂閱的電子郵件給 `majordomo@internic.net`，並請在信件的本文中請寫上 `subscribe namedroppers` 的訂閱要求。

3.1.2 找出 IP 位址

你應該已經注意到了，我們提供了一堆主機的網域名稱，便於你可以利用 `ftp` 程式到該處取得軟體。而且我們所提到的郵遞論壇地址，也包含了網域名稱。DNS 的重要性可見一般：你可以透過 DNS 的協助取得有價值的軟體和建議，不是嗎？但問題在於，這也是個「雞蛋相生的問題」。在你尚未設置好 DNS 之前，你根本無法直接送出電子郵件給對方，所以你要如何請教那些在郵遞論壇上活動的人，協助你完成 DNS 的設定？

雖然我們也可以告訴你這些主機的 IP 位址，但問題是 IP 位址的異動性實在太大了（至少以出版書的時程來看，是這樣子沒錯）。因此我們將教你如何臨機應變地透過其它的名稱伺服器，來尋找到所需要的資訊。只要你的主機有連上 Internet，而且你可以執行 `nslookup` 程式，那麼你便可以從 Internet 的命名空間中取得一些資訊。例如，若你想取得 `ftp.isc.org` 的 IP 位址，則你可以這麼做：

```
% nslookup ftp.isc.org 207.69.188.185
```

`nslookup` 會自動向位於 `207.69.188.185` 的名稱伺服器發出查詢要求，以找出 `ftp.isc.org` 的 IP 位址，而且應該會產生如下的訊息：

```
Server: ns1.mindspring.com
Address: 207.69.188.185

Name:    publ.pa.vix.com
Address: 204.152.184.33
Aliases: ftp.isc.org
```

此時，你可以 `ftp` 到 `ftp.isc.org` 的 IP 位址（`204.152.184.33`）去。

但是，我們怎麼知道在 207.69.188.185 位址上的主機，是否有提供名稱伺服器的服務呢？其實這是服務我們的 ISP 廠商，Mindspring，通知的。如果 ISP 有提供名稱伺服器的服務給客戶（大部分的 ISP 都會這樣做），那麼身為客戶的我們當然可以直接拿來使用。假如你的 ISP 不提供這樣的服務（這樣的 ISP 未免就太遜了吧！），那麼你可以暫時使用書中所列的 IP 位址。反正你只是臨時要查詢幾個 IP 位址或其它的資料而已，他們應該不會太介意才對。但是，如果你把自己的 resolver 指到別人的名稱伺服器去，並打算長久使用別人的資源的話，那就未免太過分了。

當然，假如你已經可以透過 Internet 連線到設置有 DNS 的主機，那麼你就能以 ftp 的方式取得任何你想要的資料。

當你取得了新版的 BIND 之後，也正是你認真思考網域名稱選用問題的開始？

3.2 選用網域名稱

網域名稱的選用並非易事，因為你必須選出名稱以及找到可以依附的 parent 網域。換句話說，你必須先找出適合自己的 Internet 網域命名空間，再針對你可以決定的部份選取自己想要的名稱。

選用網域名稱的第一步就是先找尋現存的網域命名空間，看看你應該歸屬於哪一個網域。最簡單的方法就是由上往下找：先找出你所屬的頂層（top-level）網域，接著再查自己合適哪一個子網域。

為了找出 Internet 網域命名空間的概況，你必須透過 ISP 連線到 Internet 去。當然你不一定要連線到已經設置有名稱伺服器的主機去，不過這樣會比較方便一點。假如你無法就近連線到已經設置有 DNS 的主機，那麼你可能要向其它的 ISP “借用” 名稱伺服器（正如前面所舉的 ftp.isc.org 範例），以便能繼續下面的步驟。

3.2.1 廣闊的世界中何處才是安身的地方？

假如你的機構從美國以外的地方連上 Internet，那麼你首先要做的決定是：要依附在 gTLDs 底下（譬如 com 或 edu 等的通用頂層網域），或是加入到你自己國家的 ccTLD（國名代碼頂層網域）底下（譬如 tw）。雖然 gTLDs 底下大部份都是美國的機構，但是 gTLDs 並非美國機構專屬的網域。因此，如果你的公司是個跨國經營的大型機構，那麼你可能會希望申請加入某個 gTLD；或者，不管怎樣你就是比較喜歡某個 gTLD 的話，那麼你也可以去申請加入它。假如 gTLDs 就是你的選擇，那麼你可以直接跳到本章的 3.2.2.2 節去。

如果你選擇的是加入 ccTLD 底下的子網域，那麼請先檢查該 ccTLD 是否已經被註冊過了，若有的話，請查看一下它的架構。假如你不確定自己國家的 ccTLD 名稱，那麼請參閱附錄 C 所提供之目前的 top-level 網域清單。

有些國家的 ccTLD，譬如：紐西蘭（New Zealand）的 nz、澳洲（Australia）的 au、英國（United Kingdom）的 uk，等 ccTLDs 都依組織的特性畫分了第二層（second-level）網域。所以這些第二層網域的名稱，可以真實反映出組織的特性，像是 co 或 com 便是提供給商業機構使用的。其它如：法國（France）的 fr 網域以及加拿大（Canada）的 ca 網域，也被分成多個不同的子網域，並由所屬的教育機構或公司獨自負責管理，譬如：St. Etienne 大學的網域為 univ-st-etienne.fr 以及 Bell Northern Research 公司的網域為 bnr.ca。你必須使用類似 nslookup 的工具程式，才能探索並找出 top-level 網域的架構。（關於 nslookup 的用法，請參考第十一章。）下面便是使用 nslookup 列出所有 au 網域之子網域的方法：

```
% nslookup - 207.69.188.185 -- 透過位於 207.69.188.185 的名稱伺服器查詢
Default Server: ns1.mindspring.com
Address: 207.69.188.185

> set type=ns -- 找出名稱伺服器 (ns) 的資料
> au. -- 搜尋 au 網域
Server: ns1.mindspring.com
Address: 207.69.188.185

au nameserver = MUNNARI.OZ.AU
au nameserver = MULGA.CS.MU.OZ.AU
au nameserver = JATZ.AARNET.EDU.AU
```

```
au      nameserver = NS.UU.NET
au      nameserver = NS.EU.NET
au      nameserver = NS1.BERKELEY.EDU
au      nameserver = NS2.BERKELEY.EDU
au      nameserver = VANGOGH.CS.BERKELEY.EDU
MUNNARI.OZ.AU      internet address = 128.250.1.21
MUNNARI.OZ.AU      internet address = 128.250.22.2
MULGA.CS.MU.OZ.AU      internet address = 128.250.1.22
MULGA.CS.MU.OZ.AU      internet address = 128.250.37.150
JATZ.AARNET.EDU.AU      internet address = 139.130.204.4
NS.UU.NET      internet address = 137.39.1.3
NS.EU.NET      internet address = 192.16.202.11
NS1.BERKELEY.EDU      internet address = 128.32.136.9
NS1.BERKELEY.EDU      internet address = 128.32.206.9
NS2.BERKELEY.EDU      internet address = 128.32.136.12
NS2.BERKELEY.EDU      internet address = 128.32.206.12
```

```
> server ns1.berkeley.edu.      -- 現在詢問其中一部名稱伺服器 (盡量利用最近的伺服器)
Default Server: ns1.berkeley.edu
Addresses: 128.32.136.9, 128.32.206.9
```

```
> ls au. --列出 au 的轄區資料
--轄區的 NS 記錄標示了委任的子網域並會提供你子網域的名稱
--但基於安全的顧慮,並非所有的名稱伺服器都會允許你列出轄區資料
```

```
[ns1.berkeley.edu]
      3D IN SOA      munnari.OZ hostmaster.munnari.OZ (
          1998051400      ; serial
          6H              ; refresh
          1H              ; retry
          23w5d16h        ; expire
          3D )            ; minimum

      3D IN NS      munnari.OZ
      3D IN NS      mulga.cs.mu.OZ
      3D IN NS      vangogh.CS.Berkeley.EDU.
      3D IN NS      ns1.Berkeley.EDU.
      3D IN NS      ns2.Berkeley.EDU.
      3D IN NS      ns.UU.NET.
```

	3D IN NS		ns.eu.NET.
ORG	1D IN NS		yalumba.connect.COM
yalumba.connect.COM		1D IN A	203.8.183.1
ORG	1D IN NS		mulga.cs.mu.OZ
mulga.cs.mu.OZ		1D IN A	128.250.1.22
	1D IN A		128.250.37.150
ORG	1D IN NS		rip.psg.COM.
	1D IN NS		munhari.OZ
munhari.OZ		1D IN A	128.250.1.21
	1D IN A		128.250.22.2
info	1D IN NS		ns.telstra.net.
	1D IN NS		ns1.telstra.net.
	1D IN NS		munhari.oz
munhari.oz		1D IN A	128.250.1.21
	1D IN A		128.250.22.2
info		1D IN NS	svc01.apnic.net.
a	3D IN A		139.130.23.2
otc	4H IN NS		ns.telstra.com
ns.telstra.com		4H IN A	192.148.160.10
otc	4H IN NS		ns2.telstra.com
ns2.telstra.com		4H IN A	192.148.160.11
otc	4H IN NS		munhari.oz
munhari.oz		1D IN A	128.250.1.21
	1D IN A		128.250.22.2
CSIRO		1D IN NS	steps.its.CSIRO
steps.its.CSIRO		1D IN A	152.83.8.3
CSIRO		1D IN NS	munhari.OZ
munhari.OZ		1D IN A	128.250.1.21
		1D IN A	128.250.22.2
CSIRO		1D IN NS	manta.vic.cmis.CSIRO
manta.vic.cmis.CSIRO		1D IN A	144.110.16.100
CSIRO		1D IN NS	dmssyd.nsw.cmis.CSIRO
dmssyd.nsw.cmis.CSIRO		1D IN A	130.155.16.1
CSIRO		1D IN NS	zoiks.per.its.CSIRO
zoiks.per.its.CSIRO		1D IN A	192.245.210.1

[]

> ^D

此處，我們所到用的基本技術，其實都非常的簡單明瞭：首先查出所有 top-level 網域的權威名稱伺服器清單——因為在相對的轄區中，這些名稱伺服器是唯一擁有完整資訊的地方——然後再連到其中的一台名稱伺服器，並列出 second-level 網域的名稱伺服器。

假如你無法從子網域的名稱中，分辨出自己所隸屬的子網域，那麼你可以查看相對轄區的聯絡資訊，並透過電子郵件詢問技術連絡人（technical contact）以取得建議。同樣地，若你自認為應該隸屬某個現存的子網域，但不是很有把握，則為了慎重起見，你可以直接詢問這個子網域的管理者。

要找到可以詢問子網域問題的人，你必須查看相對轄區的 SOA 記錄。在每個轄區的 SOA（Start Of Authority）記錄中，都會有一個欄位記載著技術聯絡人的電子郵件地址【註】。（SOA 記錄中的其它欄位還提供了轄區的一般訊息，稍後會再討論到。）你也可以利用 nslookup 來查看某個轄區的 SOA 記錄。

如果你對 csiro 子網域的用途感到好奇，那麼可以找出 csiro.au 的 SOA 記錄，看看是誰在負責管理 csiro 子網域：

```
% nslookup - 207.69.188.185
Default Server:  ns1.mindspring.com
Address:  207.69.188.185

> set type=soa      -- 找出 start of authority 的資料
> csiro.au.         -- 搜尋 csiro.au 網域
Server:  ns1.mindspring.com
Address: 207.69.188.185

csiro.au
  origin = steps.its.csiro.au
  mail addr = hostmaster.csiro.au
  serial = 1997122201
  refresh = 10800 (3 hours)
  retry  = 3600 (1 hour)
  expire  = 3600000 (41 days 16 hours)
  minimum ttl = 86400 (1 day)
```

註 雖然子網域和轄區擁有同樣的網域名稱，但實際上 SOA 記錄只歸屬轄區所有，與子網域無關。雖然轄區的技術聯絡人不見得會管轄整個子網域，但是他一定知道轄下子網域的用途為何。

mail addr 欄位紀錄著 csiro.au 聯絡人的電子郵件地址。當然，實際上的地址必須將第一個“.”換成“@”，所以 hostmaster.csiro.au 會變成 hostmaster@csiro.au。【註】

3.2.1.1 whois

你可以透過 whois 服務來瞭解某個網域的實際狀況。很多廠商都提供了簡單的 whois 用戶端程式，可藉以查詢 InterNIC 之服務主機（或是其它你所指定之主機）所提供的資料庫，來取得其中有關的網域、網路以及管理者的資訊。譬如：

```
% whois bob
```

會傳回資料庫中所有與 bob 字串相符之管理者、網路以及網域的資訊。如果想將搜尋的範圍限制在網域或網路之上，那麼你可以分別使用 dom 或 net 等的關鍵字，譬如：

```
whois "dom foo" # 列出所有與 foo 字串相符的網域資訊
whois -h whois.arin.net. "net 17" # 列出與 17 相符的網路資訊【譯註】
```

如果你的 whois 比較舊，它可能會向舊的主機（譬如 sri-nic.arpa 或 nic.ddn.mil）詢問 InterNIC 的資料庫。此時就要看運氣了：不是出現服務主機的歡迎訊息，就是會看到如下的錯誤訊息：

```
sri-nic.arpa: Unknown host
```

如果真的發生這樣的問題，那麼你必須取回原始程式碼，並將 whois 程式更改為向 whois.internic.net 詢問，然後再重新編譯。若你沒有 whois 的原始程式碼，則你還是可以在命令列中，以 -h 選項直接要求 whois 程式向 whois.internic.net 詢問。譬如：

```
whois -h whois.internic.net "dom au"
```

如果你沒有 whois 的用戶端程式，或想要透過較友善的介面，那麼你可以利用 InterNIC 所提供的 whois 網頁（<http://rs.internic.net/whois.html>）。你可以透過這個 HTML 式的表單介面，來詢問 InterNIC 的資料庫。

註 此形式的電子郵件地包含了兩種早期 DNS 記錄的遺跡：MB 與 MG。MB (Mailbox) 和 MG (Mail group) 都是 DNS 所使用的記錄，可將 Internet 上的電子郵件信箱以及電子郵件群組（即郵遞論壇）指定為某個網域的子網域。雖然 MB 和 MG 不會被廢止掉，但是這樣的地址格式也只被用在 SOA 記錄中而已，或許是懷舊的因素吧。

譯註 有些版本的 whois 必須這麼使用：whois "net 17"@ whois.arin.net。

不過，在 InterNIC 的資料庫中，只列出了 ccTLDs 之網域以及 gTLDs 之子網域的聯絡資訊，所以妳將找不到像 csiro.au 這類的子網域，但妳至少可以找出 au 網域的聯絡人。

圖 3-1 是 InterNIC 所提供之 whois 網頁介面，在輸入詢問條件並按下 Search 鈕之後，妳將會看到如圖 3-2 的畫面【註】。

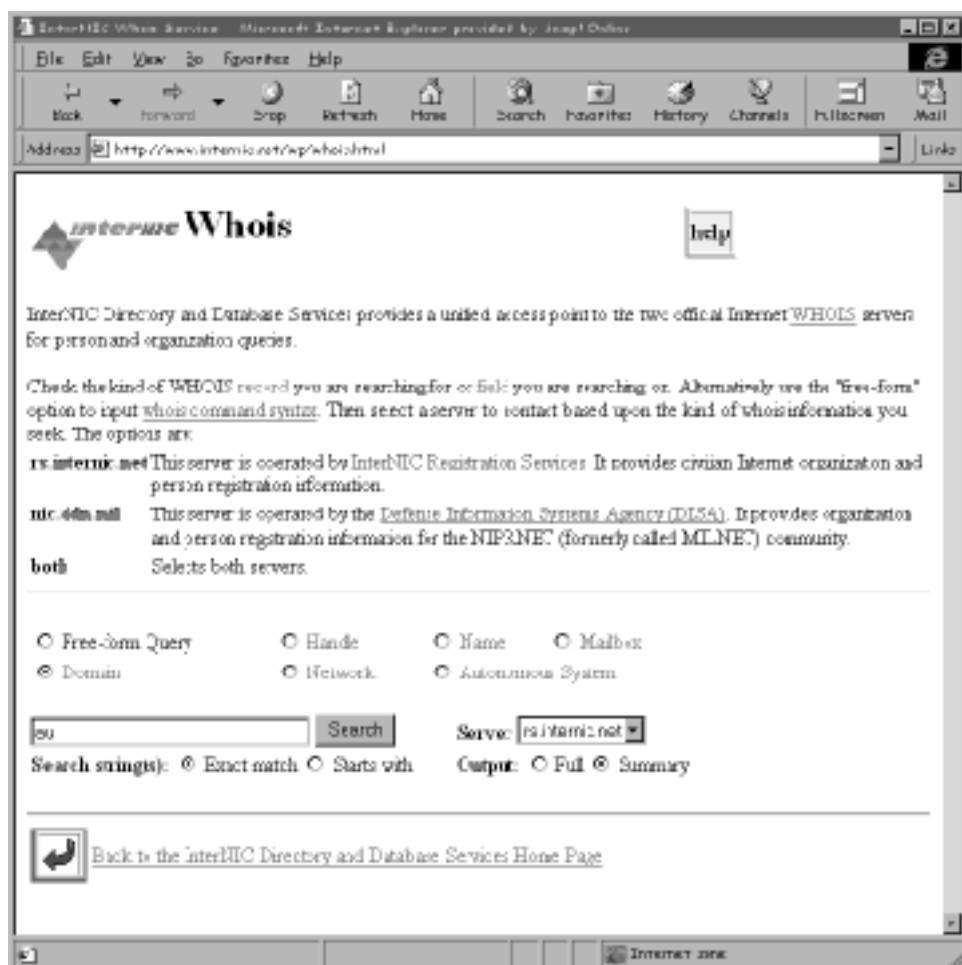


圖 3-1 InterNIC 所提供之 whois 網頁介面

註 信不信由你，同樣的查詢條件，在本書第一版的時候，符合的結果只有一個！

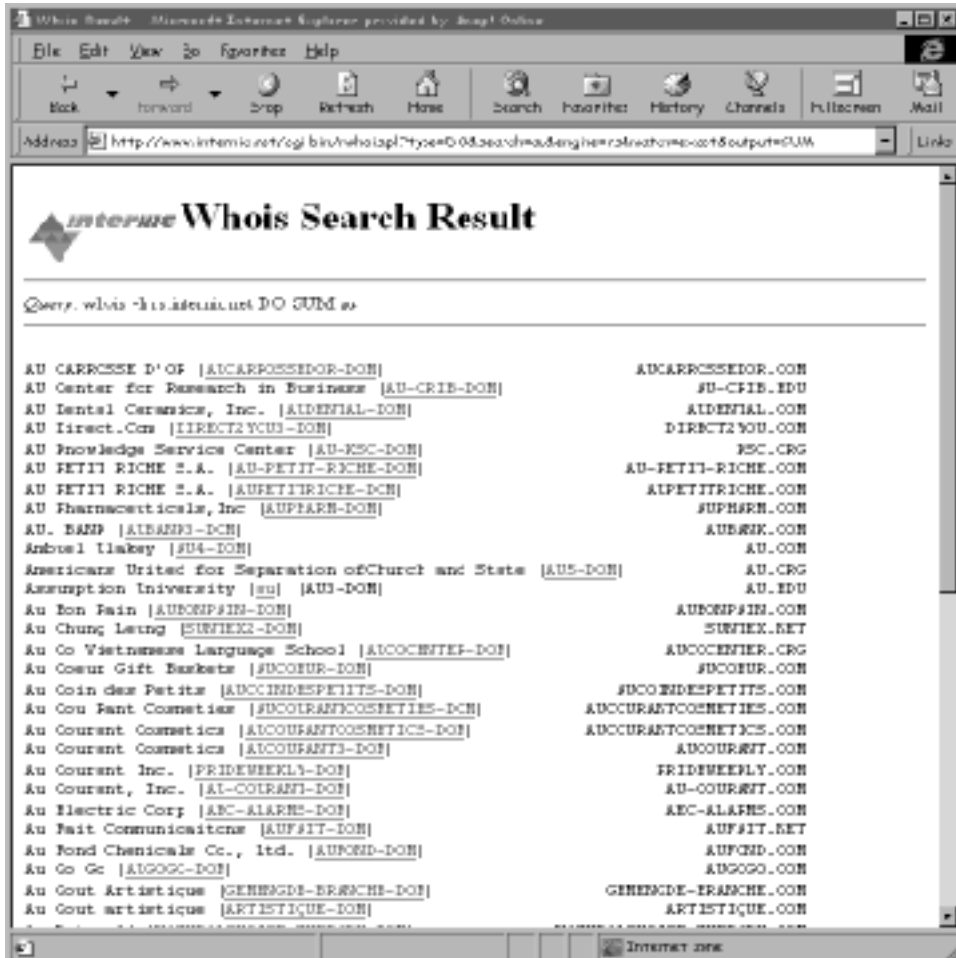


圖 3-2 InterNIC 之 whois 服務所搜尋到的結果

若再往下捲動一點，則我們將發現“Australia top-level domain”的訊息，這就是我們稍後要找的資訊。當你按下同一行標示有“AU-DOM”字樣的超鏈結 (hyperlink) 之後，你將會看到如圖 3-3 的畫面。我們因此而瞭解到 Robert Elz 便是 au 這個 ccTLD 的聯絡人。

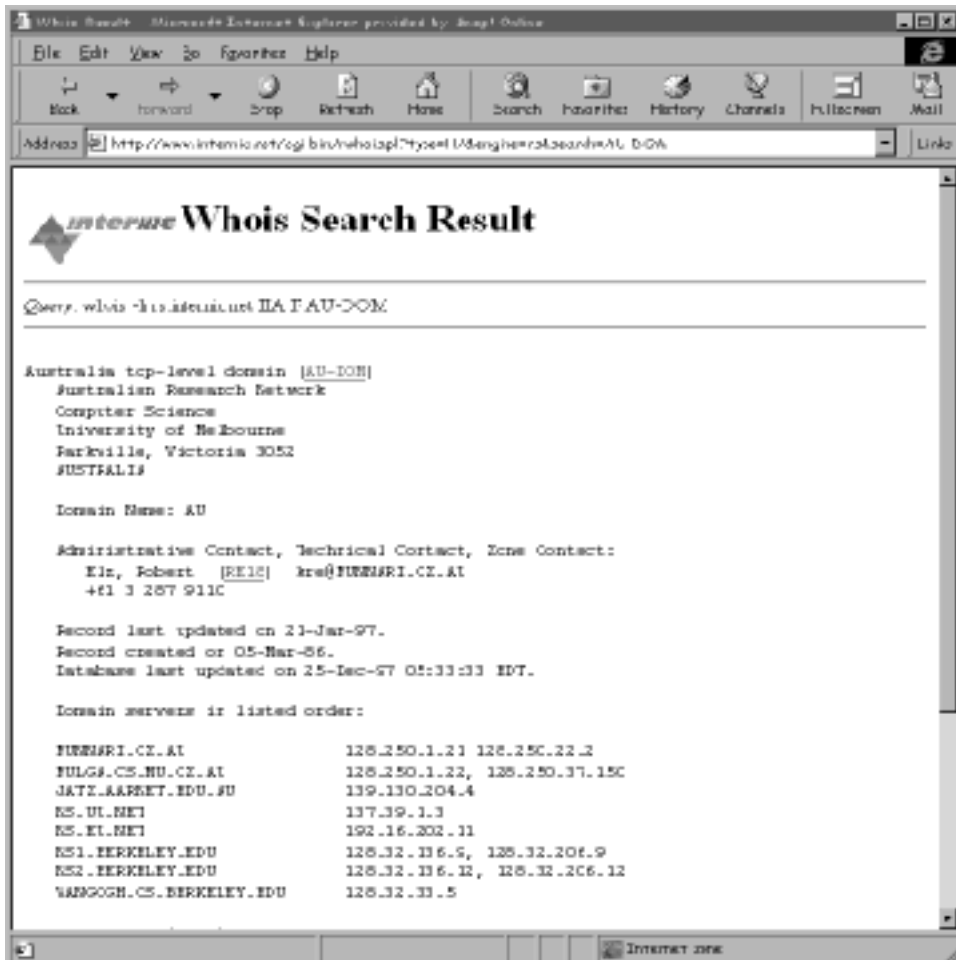


圖 3-3 InterNIC 之 whois 服務所搜尋到的詳細結果

若要透過網頁取得 [csiro.au](http://www.csiro.au) 的聯絡人資訊，則你必須詢問澳洲的 NIC。但是真的這樣一個機構嗎？你可以連到 <http://www.allwhois.com/> 網頁上試看看。按下左手邊之 frame 中，Australia 這個超鏈結，你將會看到如圖 3-4 的畫面。



圖 3-4 www.allwhois.com

當你按下標有 Whois 字樣的超鏈結之後，將會出現一個表格式的前端界面，讓你可以查詢 AUNIC (即 Australian NIC) 的資料庫。

如果你所尋找的網域在美國之外，那麼 www.allwhois.com 將會是個非常有用的網站。

3.2.2 就在這世界的某處

我們將秉持世界性的精神，以國際性的眼光來說明網域。好！讓我們從美國的 us 網域開始討論起，如何？【譯註】

假如你人在美國，將會根據你所擁有的主機數目，來決定你所隸屬的子網域。假如你只有一兩台或為數不多的主機相要在 Internet 的網域命名空間中註冊，那麼你可以加入 us 網域。us 網域會將個別的主機登記在第三層子網域之下（即第四層），第三層大部分是根據城市來命名的；而第二層子網域則會對應到美國郵政服務所使用之（兩個英文字母的）州名縮寫（這在第二章曾經提到過）。舉例來說，如果你家住 Colorado 州的 Colorado Springs，而你想為地下室所放置的兩台互連主機註冊，那麼你可以將它們加到 `cospsgs.co.us` 網域中即可。

你甚至可以取得管理自己網域的權利，這都要感謝當局對 us 網域管理者的開放政策。原本 us 網域只純粹根據地理的特性來畫分子網域。當時 us 網域的管理員可以為申請者的主機登記地址以及處理郵件的資訊（先不要急著知道這是如何設定的，我們將在下兩章為各位細說分明），但卻不包含名稱伺服器的資訊。換句話說，它們無法委任部份的網域給你管理。不過現在情況大反轉，他們鼓勵美國的學校、政府、以及公司來參與 us 網域的管理工作。假如你對相關的細節有興趣，請參閱 RFC 1480，你可以到 <ftp://ftp.sinica.edu.tw/pub/doc/rfc/rfc1480.txt> 取得這份文件，或是到 ISI 網站（<http://www.isi.edu/in-notes/usdnrl/>）查看 us 網域的相關資訊。

你也可以申請加入 gTLDs 的子網域（譬如 edu 或 com）。只要你不要申請太長的子網域名稱（NIC 建議應少於 12 個英文字母），或是已被使用的子網域名稱，通常你都可以取得你想要使用的名稱。稍後我們會詳細介紹 gTLDs 的每個成員。

譯註 美國的英文字縮寫是 U.S.A 也可以說成是 U.S. of A.。作者語帶幽默的說：按照英文字母的先後次序，也應該是美國的 us 網域先說明。

3.2.2.1 us 網域

為了讓大家能夠體認到，如何在 us 網域的命名空間上尋找到理想的網域名稱，我們還要舉一個例子來說明。假定你住在 Maryland 州的 Rockville，你才剛從一輛卡車的後車廂買回了一台 UNIX 工作站（喂，別說這是不可能的！），而你想替這台機器註冊名字。雖然你無法直接連上 Internet，不過你有一條 UUCP 線路可以連上 College Park 的 UMD（University of Maryland）。

既然你只要登記一台主機就夠了，所以你大可不必自己管理網域。你只需要將主機登記在 Internet 網域命名空間中的某處就行了。而 us 這個 ccTLD 便是一個理想的地方。讓別人來為你管理名稱伺服器 and 網域，將可免除你許多的管理工作。

利用你在 UMD 就讀時期某部主機上的帳號，你就可以查看 Maryland 的網域是否存在。（如果你沒有帳號，但是你可以連上 Internet，那麼你也可以利用 nslookup 來查詢已知的名稱伺服器。）

```
nslookup
Default Server:  noc.umd.edu
Address: 128.8.5.2

> set type=ns          -- 查詢名稱伺服器
> md.us.              -- 從 md.us 的網域開始
Server:  noc.umd.edu
Address: 128.8.5.2

md.us  nameserver = NS.UU.NET
md.us  nameserver = ADMII.ARL.MIL
md.us  nameserver = EXCALIBUR.USC.EDU
md.us  nameserver = VGR.ARL.MIL
md.us  nameserver = TRANTOR.UMD.EDU
md.us  nameserver = MX.NSI.NASA.GOV
md.us  nameserver = VENERA.ISI.EDU
md.us  nameserver = NS.ISI.EDU
md.us  nameserver = RS0.INTERNIC.NET
```

沒錯，的確存在有給 Maryland 州使用的網域。現在變更伺服器的設定，讓它指向一台 md.us 的名稱伺服器，例如 venera.isi.edu，並檢查是否有其它的子網域存在（此時你尚未離開 nslookup 程式）：

```
> server venera.isi.edu. -- 將名稱伺服器設為 venera.isi.edu
Default Server:  venera.isi.edu
Address:  128.9.0.32

> ls md.us. -- 列出 md.us 轄區資料以尋找 NS 記錄【譯註】
[venera.isi.edu]
      1D IN SOA      VENERA.ISI.EDU. us-domain.ISI.EDU. (
                980112          ; serial
                12H             ; refresh
                1H              ; retry
                2W              ; expire
                1D )            ; minimum

      1W IN NS      RS0.INTERNIC.NET.
      1W IN NS      NS.UU.NET.
      1W IN NS      ADMII.ARL.MIL.
      1W IN NS      EXCALIBUR.USC.EDU.
      1W IN NS      VGR.ARL.MIL.
      1W IN NS      TRANTOR.UMD.EDU.
      1W IN NS      MX.NSI.NASA.GOV.
      1W IN NS      VENERA.ISI.EDU.
      1W IN N       NS.ISI.EDU.

north-laurel.md.us.  1D IN NS      top2.domainregistry.net.
                    1D IN NS      top.domainregistry.net.
                    1D IN NS      primary.southern-domains.com.
fruitland.md.us.    1D IN NS      top2.domainregistry.net.
                    1D IN NS      top.domainregistry.net.
                    1D IN NS      primary.southern-domains.com.
frostburg.md.us.    1D IN NS      winnt.i-theta.com.
                    1D IN NS      ns2.us-domains.com.
                    1D IN NS      ns.manchester.mo.us.
creativdesign.college.md.us.  1W IN NS      ns.webindonesia.com.
                    1W IN NS      ns2.webindonesia.com.
```

譯註 或許是基於安全的理由吧，目前已經看不到書中的結果了。

```
carroll.md.us.          1W IN NS      auth00.ns.uu.net.  
                        1W IN NS      auth50.ns.uu.net.  
oxon-hill.md.us.       1D IN NS      winnt.i-theta.com.  
                        1D IN NS      ns2.us-domains.com.  
                        1D IN NS      ns.manchester.mo.us.
```

[...]

列出了許多的子網域名稱，但似乎沒有給 Rockville 使用的網域。也許你是 Rockville 這個小城中第一台想在 md.us 登記的主機，亦或許是 Maryland 州的下一層是根據郡（county）來命名的，而在郡底下才可能是 Rockville。不管怎樣，md.us 的管理者都會幫你找到一個適合的地方。因為你的網域名稱只是 md.us 轄區的一部份而已，所以這件事不會耗費他們多少時間的——不需要額外設置另一部伺服器。

要如何為全新的子網域命名呢？是 rockville.md.us？還是 rock.md.us？事實上 us 網域有個命名習慣：城市層級的網域將仿照 Western Union “City Mnemonic” 的方式命名。（不用擔心，us 管理者會有一份文件副本）另一種方式便是採用完整的城市名稱。

實際上，有些（位於上層之）parent 網域的管理者對（位於下層之）child 網域的命名方式，有著非常強烈的主觀意識（就像父母為你取名字一樣）。他們或許會希望維持所管轄網域之命名空間的一致性。我們建議你在命名之前，先詢問一下 parent 網域的管理者，是否介意子網域的命名方式——否則他們可以拒絕你加入該網域。在這個前提之下，你仍然擁有為你的主機命名的權利。

要如何跟 parent 網域的管理者聯繫呢？你可以嘗試使用 whois 程式，但因為 md.us 並不是個 ccTLD，也不隸屬於 gTLD，所以你可能找不到多少資訊。最保險的方法還是透過 nslookup 將 md.us 轄區的 SOA 記錄找出來，就如同先前找到 csiro.us 的連絡資訊一樣。你可以將信寄到 SOA 記錄所列的地址，不過讀取這封信的人不見得會處理登記的作業（該轄區之技術性和管理性的工作，可能分別由兩個不同的人來處理），但他們應該知道誰負責實際登記作業，並把你的資料轉送給這些實際負責的人。

下面這個例子便是利用 nslookup 來讀取 md.us 轄區的 SOA 記錄：

```
nslookup
Default Server:  noc.umd.edu
Address: 128.8.5.2

> set type=soa    --查詢 SOA 記錄
> md.us.         --針對 md.us 網域
Server:  noc.umd.edu
Address: 128.8.5.2

md.us
    origin = VENERA.ISI.EDU
    mail addr = us-domain.ISI.EDU
    serial = 971109
    refresh = 43200 (12 hours)
    retry   = 3600 (1 hour)
    expire  = 1209600 (14 days)
    minimum ttl = 86400 (1 day)
```

和 csiro.au 的例子一樣，你必需將 mail addr 那欄設定中，第一個“.”換成“@”。因此，us-domain.ISI.EDU 會變成 us-domain@ISI.EDU。

3.2.2.2 通用頂層網域

正如前面所說的，有許多因素會促使你在 edu、com 或 org 等 gTLDs（通用頂層網域）底下，申請一個子網域：你的公司可能屬於跨國的大企業，或是你覺得這些網域比較有名氣，或者你覺得公司的網域名稱之後能有個 com 會比較好！讓我們舉幾個在 gTLD 下選擇網域名稱的簡短例子。

假設你是個學生，目前負責管理 Minnesota 州位於 Hopkins 之小型的大學網路。你剛獲准透過地區網路，MRNet，連上 Internet。但是你所就讀的大學，除了目前這一條新設立的 UUCP 連線之外，以往未曾有過任何對外的連線，所以你目前並未 Internet 的命名空間上有任何名稱的登記。

由於你目前人在美國境內，因此你可以選擇加入到 us 或 edu 的網域之下。但在你的區域網路中，已經設置了超過一打以上的電腦，而且你預期將來還會繼續增加，因此顯然不適合使用 us 的子網域。此時選用 edu 的子網域可能會比較好。

因為你所就讀的學校稱為 Gizmonics 學院，所以你決定將網域命名為 gizmo.edu。現在你必須檢查這個網域名稱是否已經被別人登記走了，因此你利用在 UMN 的帳號來查詢：

```
nslookup
Default Server: ns.unet.umn.edu

Address: 128.101.101.101

> set type=any    -- 查詢任何的記錄
> gizmo.edu.      -- 針對 gizmo.edu
Server: ns.unet.umn.edu
Address: 128.101.101.101

*** ns.unet.umn.edu can't find gizmo.edu.: Non-existent domain
```

看起來好像不存在 gizmo.edu 這個網域（這倒沒什麼好驚訝的！），因此你可以繼續下一個步驟：利用 whois 找出到底是誰在管理該 parent 網域：

```
whois "dom edu"
Education top-level domain (EDU-DOM)
Network Solutions, Inc.
505 Huntmar Park Dr.
Herndon, VA 22070

Domain Name: EDU

Administrative Contact, Technical Contact, Zone Contact:
Network Solutions, Inc. (HOSTMASTER) HOSTMASTER@INTERNIC.NET
(703) 742-4777 (FAX) (703) 742-9552

Record last updated on 17-Jan-97.
Record created on 01-Jan-85.
Database last updated on 25-Dec-97 05:33:33 EDT.

.

Domain servers in listed order:

[...]
```

3.2.3 檢查你的網路編號是否已經被登記

在你繼續以下的動作之前，請先檢查你的 IP 位址的網路（編號）是否已經被登記好了。【譯註1】許多 parent 網域不會將子網域的管轄權，隨便委任給設置在尚未登記網路之上的名稱伺服器，而且接受註冊的機構也不會隨便將 in-addr.arpa 子網域委任給未正式登記的網路。

IP 位址的網路（編號）定義了某個範圍的 IP 位址。例如，網路 15/8 是由 15.0.0.0 到 15.255.255.255 的 IP 位址所組成的。而 199.10.25/24 的範圍則是由 199.10.25.0 到 199.10.25.255 的 IP 位址所組成的。（以上的表示法請見關於 CIDR）

關於 CIDR

在撰寫本書第一版的當時（1992 年 10 月之前），Internet 的 32 位元位址空間，將網路的大小分為三種主要的等級：A 級、B 級和 C 級。A 級網路會把這 32 位元的 IP 位址中，第一個 octet（最前面 8 個位元）看成是整個網路的編號，剩下的 24 個位元則可再次細分網路編號，以便區分不同子網路上的主機。大部分擁有 A 級網路的機構，都會使用另一個層級的定址法，把整個網路繼續細分為子網路。B 級網路會把這 32 位元的 IP 位址中，前面 2 個 octets 視為整個網路的編號，而所剩下的 2 個 octets 則分配給主機；C 級網路會將前面 3 個 octets 視為整個網路的編號，而最後的 1 個 octet 則分配給主機。

然而，這種將網路分成大中小三種規模的作法並不適用於每個人。有許多機構大到需要申請好幾個 C 級網路才夠用，一個 C 級網路的 IP 位址只能分配給 254 台主機；但這些機構的規模又不夠格去申請 B 級網路，一個 B 級網路的 IP 位址可分配給高達 65,534 台主機。無論如何，B 級網路已經快要不敷使用了！

為了解決這個問題以及建立具有彈性的網路規模，可供各種機構使用，CIDR (Classless Inter-Domain Routing, 唸為 cider) 應運而生。顧名思義，CIDR 拋棄了傳統的位址定義方式，不再限定必須以 8 個位元（octet）為單位來作為網路編號，而是可以用任何連續的位元來代表網路編號。舉例來說，如果一家公司需要的位址空間大約是 B 級網路的 4 倍，那麼你可以分配給它 14 個位元用來指定網路編號，剩下來的 18 個位元【譯註2】則分配給主機使用。

譯註1 你可以透過這個方式來檢查：譬如，`whois -h whois.arin.net. "net 15"`、`whois -h whois.arin.net. "net 199.10.25"`。

譯註2 $2^{18} = 2^2 * 2^{16} = 4 * 65536$ ，這個剛好是 B 級網路所能提供之位址空間的四倍。

可想而知，CIDR 的崛起使得分級 (classful) 這個名詞走入歷史，只是偶而還會有人提到。要表示一個 CIDR 網路時，我們會先指定分配給這個機構的高效位元 (high-order bits) 值 (以點和十進位數字表示)，以及用了多少個位元來表示這個網路。兩者之間用一個斜線分開。例如，15/8 代表一個傳統的 A 級規模的網路，其高效位元值是 00001111。傳統的 B 級規模的網路 128.32.0.0 現在則以 128.32/16 來表示。而 192.168.0.128/25 則包含了從 192.168.0.128 到 192.168.0.255 之中的 128 個 IP 位址。

在過去，InterNIC 是所有 IP 網路 (編號) 的正式發放單位；所有連線到 Internet 的網路，都必須由 InterNIC 來指定其 IP 網路 (編號)，以保證不會出現重疊的問題。現在，傳統 InterNIC 的角色已漸漸被 ISPs (Internet Service Providers) 所取代。ISPs 會將自己網路的位址空間分配給它們的客戶使用。如果你知道你的網路 (編號) 來自於 ISP，那麼你的網路就是從 ISP 的網路中分割出的，而 ISP 的網路 (編號) 應該是已經登記好的 (你的網路編號因此也算登記好了)。你可以向你的 ISP 確認，是否他們已經登記好自己的網路 (編號)，但是你不必 (或許不能) 自己動手，你能做的也只是向 ISP 抱怨網路 (編號) 為什麼沒有登記。一旦你確定 ISP 的網路 (編號) 已經登記好了，你可以跳過本節再繼續讀下去。

如果你的網路 (編號) 是 InterNIC 很久以前指定給你的，或你本身就是 ISP，你應該查詢你的網路 (編號) 是否已有正式的登記。那麼要向誰查詢呢？當然是跟為你登記資料的機構呀，這還用說。這些機構又稱為登記資料管理處 (registry)，分別負責全球各地區的網路編號登記事務。在西半球的主管單位是 ARIN (American Registry of Internet Numbers)，網址為 <http://www.arin.net/>，負責發放 IP 位址空間以及登記網路 (編號)。主管亞太地區的單位是 APNIC (Asia Pacific Network Information Center)，網址為 <http://www.apnic.net/>，也是提供相同的服務。在歐洲的主管單位是 RIPE Network Coordination Centre，網址為 <http://www.ripe.net/>。每個負責登記的機構也可以將登記權委任給地區內的專責單位：譬如，ARIN 會將登記權分別委任給墨西哥和巴西境內的專責單位。請洽詢你自己國家境內的主管單位。

如果你不確定你的網路（編號）是否已經登記，最好的方法便是利用 whois 來查詢。底下是各個單位的 whois 網頁：

ARIN

<http://www.arin.net/whois/arinwhois.html>

APNIC

<http://www.apnic.net/reg.html>

RIPE

<http://www.ripe.net/db/whois.htm>

假如你發現自己的網路（編號）尚未正式登記，你必須在設置 in-addr.arpa 轄區之前先完成正式的登記手續。每個負責登記的機構都有不同的登記程序，但多半會牽涉到一些金錢往來（很不幸的，是從你的手上轉到他們手上）。

你可能會發現到，你自己的網路（編號）已經指定給你的 ISP 了。這時候你就不需要再自己去申請了。

一旦你連上 Internet 之所有主機的網路（編號）都已經正式登記好了，你便可以通知你的 parent 網域。

3.2.4 向你的上一層登記

其實你的上一層只需要你提供 dns 伺服器的名稱和 IP 位址等基本資料。假如你還未連上 Internet，那麼請把將會作為你名稱伺服器之 Internet 主機的 IP 位址提供給他們。某些 parent 網域還會要求，必須在你自己的網域上設置有名稱伺服器才算數。若是這樣的話，請直接跳到第四章，先設置好你的名稱伺服器，然後再聯絡你的上一層。

假如是由 InterNIC 來負責管理你的 parent 網域，他們也會詢問一些關於你的機構以及網域的聯絡人的資訊（兩者可能是同一個）。假如你機構的聯絡人並沒有登記在 InterNIC 上的 whois 資料庫裡面，你就必須提供一些資訊好讓他們在 whois 資料庫中登記。這些資訊包括：他們的姓名、地址、電話以及電子郵件地址。假如他們在 whois 資料庫中已有登記，那麼你只需要在資料中指定他們的 whois 代碼（一個獨特的文數字編號）即可。

向 InterNIC 登記一個新的網域時，還有一件事需要注意：那就是費用問題。InterNIC 的管理承包商，NSI 公司 (Network Solutions, Inc.)，對於登記新的 top-level 網域（目前是指 ccTLD），以及將網域名稱登記在 com、net 和 org 等 gTLDs 底下的使用者訂定有如下的收費標準：以網域為單位，首次登記費用為 \$70 美金（含兩年的年費），而後每年繳費 \$35 美金的年費。然而，自從美國商務部與 NSI 公司的合約期滿之後一切都改觀了。美國商務部授權 ICANN【譯註】所執行的 SRS (Shared Registration System) 計畫，開啟了多家網域名稱註冊機構相互競爭的局面，不僅提高了服務的品質，也同時促成了註冊費用的削價競爭。若想知道目前提供服務的註冊機構有那些，則請參考附錄 D。

SRS是什麼？ (Shared Registration System)

1998 年 10 月，美國商務部 (Department of Commerce, DoC) 與 NSI 公司 (Network Solutions, Inc) 修正合約的內容。在舊有合約的保障之下，由 NSI 公司獨享 .com、.net 和 .org 等 gTLDs 之第二層網域的登記權（即 registrar 的身份）與登記資料庫的管理權（即 registry 的身份）。根據第 11 號修正案的規定，計畫建立一套共享的註冊系統 (Shared Registration System, SRS)。在此系統中，將不限制登記權擁有者 (registrars) 的家數，如此可形成一個具競爭性的網域名稱註冊市場，以便於提升註冊服務的品質；但是這些 registrars 必須使用並共享同一個登記資料庫 (registry) (由 NSI 繼續充當 registry 的管理機構)。同年 11 月，DoC 授權 ICANN 這個剛成立的非營利的民間組織，監督 SRS 計畫的執行。ICANN 的部份任務是建立與設置一套 registrar 核定程序，以確保從現有的系統過渡到具競爭性之網域名稱註冊系統時，能繼續維持 Internet 的穩定性以及網域名稱的耐久性。請參閱網頁 <http://www.icann.org/registrars/accreditation.htm> 的說明。

譯註 ICANN (Internet Corporation for Assigned Names and Numbers; 在 Internet 上負責分配名稱與編號的機構) 是個非營利的機構，成立時預設的職掌為：IP 位址空間的配置、協定參數的指派、網域名稱系統的管理、以及 root 伺服器系統的管理。也就是根據美國政府合約的規定，原本由 IANA 以及其它機構所執行的業務。

假如你是直接連線到 Internet 的用戶，應該還有一個與 IP 位址相對應的 in-addr.arpa 網域會委任給你。例如，如果你的公司被分配到 192.201.44/24 這個範圍的位址，那麼你就能夠管理 44.201.192.in-addr.arpa 這個網域。透過這個反向網域將可以讓你輕易控制 IP 位址與主機名稱的對映關係。在第四章中會討論到如何設定你的 in-addr.arpa 網域。

在 3.2.3 節我們曾經向你提出了幾個問題：你的網路屬於你的 ISP 網路的一部分嗎？你的網路或是 ISP 網路中你所使用的那部分是否有正式登記？要向哪個單位登記？你必須先能夠回答這些問題，才有辦法取得 in-addr.arpa 網域的授權。

假如你的網路（編號）來自於你的 ISP，那麼你可以直接要求 ISP 將 in-addr.arpa 中屬於你的子網域委任給你。每家 ISP 處理 in-addr.arpa 網域的委任程序各有不同，你可以自行查閱他們的網頁。若找不到的話，你可以檢查與你 ISP 的網路編號相對映之 in-addr.arpa 網域的 SOA 記錄。例如，假設你的網路（編號）屬於 UUnet 網路（編號）153.35/16 的一部分，那麼你可以檢查 35.153.in-addr.arpa 的 SOA 記錄，以便找出該轄區之技術聯絡人的 email 地址。

如果你的網路（編號）必須向地區性的 registry 註冊，那麼請直接與他們聯絡，以便登記你的 in-addr.arpa 網域。每個 registry 都會把他們委任 in-addr.arpa 網域的作業程序公佈在自己的網站上。請參考附錄 E，ARIN 所提供之 in-addr.arpa 申請表格。你也可以線上取得這份文件，<http://rs.arin.net/templates/inaddrtemplate.txt>。

目前你已經送出了註冊信息給你想要加入之 parent 網域的聯絡人，現在該是花些時間整理一下自己思緒的時候。如果你已經取得了網域的授權，請接著看下一章，我們將教你設置網域的方法。