第十三章 網域名稱系統

13-1 DNS 系統簡介

『網域名稱系統』(Domain Name System, DNS) 是由 RFC 1034 和 1035 制定的標準規範，為目前 Internet 網路不可或缺的應用系統，不論使用者瀏覽網頁、傳遞電子郵件、或使用各種應用系統等都必須仰賴 DNS 系統，來將網域名稱轉譯成 IP 位址，才能連結到資源所在的網站。我們在第十二章討論過，以有意義的網域名稱來記憶資源所在位置，總比沒有意義數字 (IP 位址) 來得容易。況且 IP 位址可能會受限於地理環境的因素，而被侷限於某一網路範圍下，而網域名稱的命名可以不受任何地區限制，近年來，國內許多廠商將網域名稱 (網路在國內) 註冊於國外網域名稱之下，就是一個明顯的例子。目前 Internet 網路上絕大部份的資源都以網域名稱來命名，譬如，網頁名稱(www.nsysu.edu.tw)、FTP 資源(ftp.nsysu.edu.tw)、Telnet 伺服器(bbs.nsysu.edu.tw) 或電子郵遞信箱 (tsnien@pchome.com.tw)。又當您在瀏覽網頁時，可以發現絕大部份時間都在作超連結動作，這些超連結也都是以網域名稱來表示。因此，任何一部電腦雖然網路狀況良好，如果沒有指定某一部 DNS Server，來負責解譯 IP 位址的工作，也無法連結到 Internet 網路上，譬如，在 Windows 98 電腦上必需指定 DNS 伺服器位址，才可順利瀏覽網頁或收發郵件。

然而，全世界至少有上億的網域名稱需要解譯，以得到它的 IP 位址，如此龐大的紀錄資料如何來登錄和解譯呢？這的確是個非常繁重的工作，但事實上並沒有那麼複雜。DNS 是一套分散式系統，解譯與登錄工作是由全球的 DNS 系統共同來達成，每一部 DNS 伺服器只負責該管轄地區的網域名稱，如果客戶查詢的名稱不在自己管轄範圍，便將其轉送到其它 DNS 伺服器上。DNS 系統的運作模式有點類似路徑選擇協定一樣，都是由 Internet 網路上所有端點共同來達成，也就是說，它的組織管理是鬆散的，並沒有一套嚴謹的專屬系統來負責，如此便增加了 Internet 的成長速度。

本章首先介紹 DNS 系統的運作原理，以及它的通訊協定，再以目前 Internet 網路上使用最普遍的 BIND 系統為範例，介紹 DNS 系統的設定與管理。

13-2 DNS 系統功能

如果僅將 DNS 的功能定位為『將網域名稱解譯成 IP 位址』，那就太小看 DNS 系統了，其實 DNS 不僅扮演名稱解譯成 IP 位址的工作，還具有將 IP 位址反向解譯為網域名稱、以及郵件解譯的功能，這些功能在 Internet 網路上都扮演非常重要的角色，以下分別介紹之。

13-2-1 正向解譯功能

『正向解譯』(Forward Resolve)是 DNS 系統最基本的應用，功能是將網域名稱解譯成 IP 位址。當客戶端使用網域名稱連結時，首先會到 DNS 伺服器上查詢該名稱的 IP 位址，再以查詢出來的 IP 位址連結到資源所在的地方。如圖 13-1 所示，在電腦 A 上執行 telnet linux-1.cu.edu.tw，電腦 A 首先會到所指定的 DNS 伺服器上，查詢 linux-1.cu.edu.tw 的相對 IP 位址(163.15.2.62)，再依此位址連結到目的地 (動作順序如圖中編號次序)。但此動作如要能順利進行，DNS 伺服器必需事先登錄有關 linux-1 的資料。

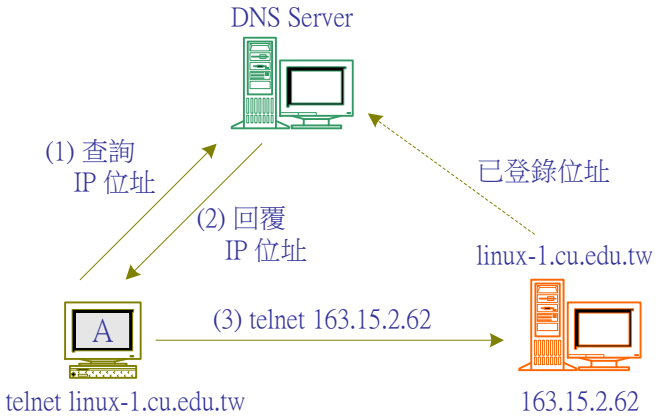

圖 13-1 DNS 正向解譯功能

13-2-2 反向解譯功能

『反向解譯』(Reverse Resolve) 是由 IP 位址解譯成網域名稱的功能。它的查詢動作大多是發生在被連結端，如圖 13-2 所示，電腦 A 以 Telnet 連結到 163.15.2.62 主機上，主機便可向來源端的 DNS Server 查詢電腦 A (163.15.2.34) 是屬於哪一個網域管轄之內，同時更進一步可查閱該網域下的電腦是否允許連結到本機 (如，TCP-wrapper 功能)。由於非法進行存取者為了隱瞞身份，大多不會進行 DNS 登錄，所以反向解譯就可以達到防止非法存取的效果。但話說回來，這種防禦功能也無法達到百分之一百的功能，如果使用者是動態 IP 位址，也只好向 ISP 查詢連線的人。另一方面的應用，透過反向解譯可統計分析要求連線的個人或單位。

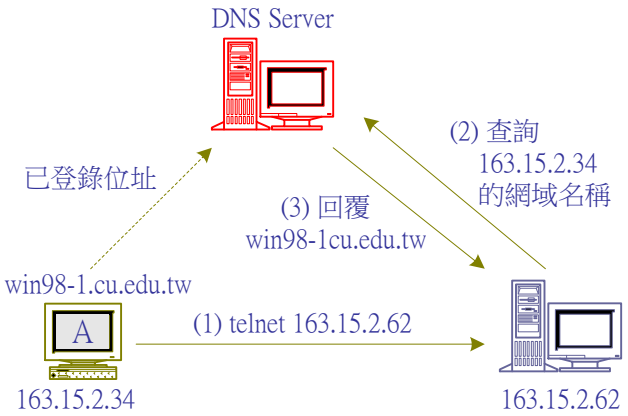

圖 13-2 DNS 反向解譯功能

13-2-3 郵件解譯功能

DNS 系統的另一個重要應用是郵件解譯功能，用於郵件伺服器查閱目的郵件位址。一般傳送郵件時，大多僅指定網域名稱，而並未指定郵件伺服器位址，譬如，傳送一個郵件到 tsnien@pchome.com.tw，此時就必須透過 DNS 伺服器來查詢該網域的郵件伺服器位址，此動作和一般利用網域名稱查詢 IP 位址的應用有所不同。如圖 13-3 中，使用者在電腦 A 上發送一封郵件到 tsnien@pchome.com.tw 的動作（如圖中訊號編號）如下：首先到 DNS Server 上查詢本網域之郵件伺服器（SMTP Server）位址(編號 1, 2)，再將信件傳送給郵件伺服器(編號 3)，郵件伺服器收到該信件後，再依照郵件上之目的位址（pchome.com.tw）向 DNS Server 查詢該信件的郵件伺服器（POP Server）位址，並得到該伺服器的 IP 位址(編號 4, 5)，接下來，來源端的郵件伺服器再將信件，轉送該信件的郵件伺服器（POP Server）(編號 6)。由此可見，在 DNS Server 上登錄郵件轉送功能，並不像一般解譯 IP 位址那麼簡單，尤其在設定管理上更為複雜。

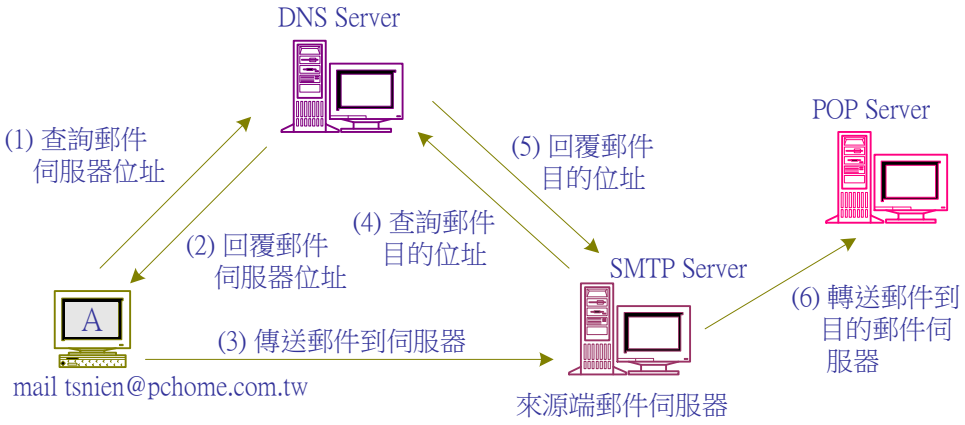

圖 13-3 郵件解譯功能

透過郵件解譯功能，我們可以瞭解 DNS 伺服器除了登錄網域名稱 (或電腦名稱) 和 IP 位址的對應外，也記錄了許多有關 Internet 網路上的資訊以供查詢，網域名稱僅是功能之一，如此更能突顯 DNS 系統在 Internet 的上扮演極重要性。

13-3 DNS 命名方式

在第十二章曾簡單介紹網域名稱的命名方式，但只列出正向解譯的名稱排列方式。至於所有正反向解譯的名稱命名方式則列於圖 13-4。因此，整個 DNS 系統裡包含三種網域名稱系列：

(1) 反向網域：作為登錄由 IP 位址解譯到網域名稱使用。

(2) 通用網域：大多以三個英文字母表示某一組織單位的網域名稱，此網域名稱都以美國本土單位為主，如 adsl.support.cisco.com。

(3) 國家網域：大多以兩個字母來表示某一國家的網域名稱 (ISO 3166 規範)，或者表示某一地理區域的網域，如 cis.cu.edu.tw。

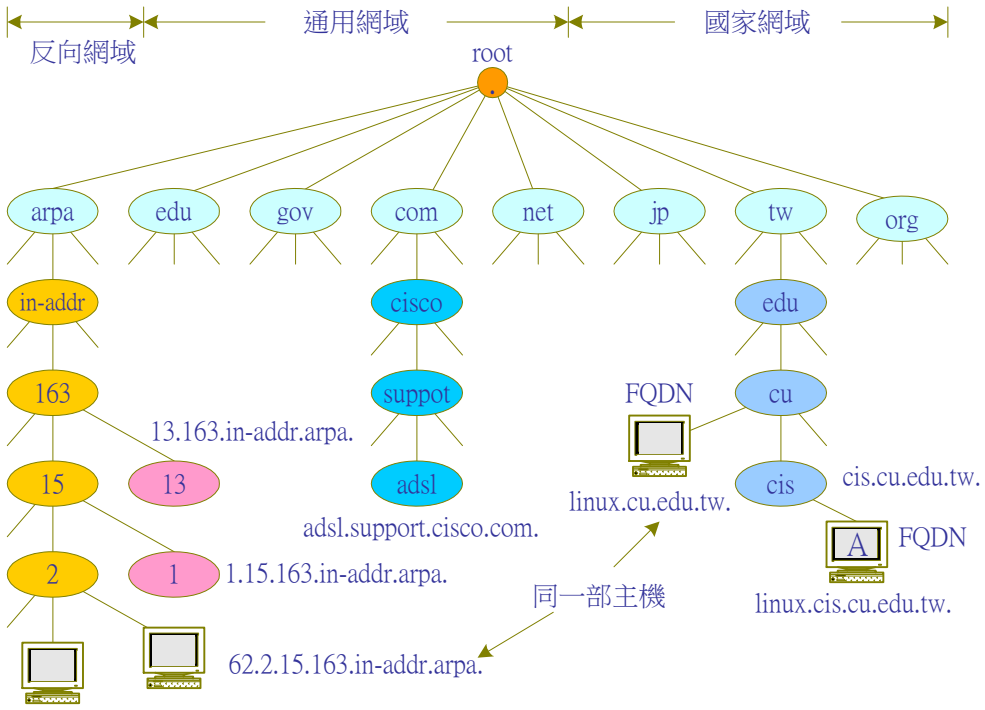

圖 13-4 DNS 網域名稱階層

13-3-1 網域區域

網域名稱是以樹狀階層式方式建構，最上層的根網域『.』包含三種系列網域名稱：反向網域、通用網域和國家網域。在根網域之下的網域稱之為『頂層網域』(Top Level Domain)，譬如，com、

edu、tw、jp 等。每一頂層網域管轄它所屬的第二層網域，也就是說，它必須負責登錄與管理第二層網域名稱的解譯，如要查詢頂層網域底下的哪一次網域，便可直接詢問該頂層網域。然而，第二層網域也必須負責登錄及管理它所管轄的第三層網域。當然，每一網域（不論哪一層次）都必須有專屬名稱伺服器（Name Server）來負責登錄及管理，簡單的說，上層名稱伺服器必須登錄下層名稱伺服器的位址，當客戶端查詢某一網域時（如 edu.tw），則上層名稱伺服器（tw），必須回應該網域（edu.tw）所管轄的名稱伺服器位址，同理，edu.tw 網域的伺服器必須登錄 cu.edu.tw 名稱伺服器位址，然而 cu.edu.tw 的名稱伺服器，再登錄 linux.cu.edu.tw 的主機位址（IP 位址）。

因此，所謂**『網域區域』（Domain Zone）**表示某一網域所管轄的範圍，如圖 13-4 中，橢圓形都表示一個網域區域。任一網域至少要有一部名稱伺服器負責該網域下的子網域和主機登錄。譬如，圖中 edu.tw. 網域不但要管理該網域下的次網域（如 cu 等），可能該網域也有主機名稱（如 linux.cu.tw.），而必須登錄以備查詢。然而，如果網域區域（如 com.）過大時，也許會由許多名稱伺服器來服務查詢工作，而另一方面，網域區域較小時（一般企業網域），一部名稱伺服器也可以管理若干個區域。

任何查詢動作非常有可能由上層名稱伺服器來得到下層名稱伺服器的位址，由此可見，查詢最上層根網域的機率將是非常大，並非一部伺服器可以承載的負荷，目前全世界有 A 到 M 共 15 部根伺服器分散各地(如 13-10-4 節範例)，各個根伺服器都有其管轄範圍，以處理各地區的查詢。甚至其他網域（如 com.）也需要好幾部伺服器分散全球各地以備查詢，才足以承擔負荷。

13-3-2 完整網域名稱

所謂**『完整網域名稱』（Full Qualified Domain Name, FQDN）**，就是能完整表現出某一主機的名稱。然而，網域名稱是以樹狀的反向排列方式，上下層之間都以一個**『.』**來區分，因此，FQDN 的表示必須由**『主機名稱』** + **『網域名稱』** + **『.』**。譬如，圖 13-4 中 linux 主機的 FQDN 為**『linux.cu.edu.tw.』**，其中**『linux』**為主機名稱、**『cu.edu.tw』**為網域名稱、又**『.』**為根網域。但一般習慣性並未將根網域填入，而一般電腦系統也都會自動將**『.』**填入。這是因為 DNS 系統的查詢，都以 FQDN 名稱來查詢，正是我們設定 DNS 伺服器時（登錄時）必須注意的事項。

13-3-3 反向網域名稱

DNS 系統除了可以由網域名稱解譯到 IP 位址外，還必須提供由 IP 位址來查詢出網域名稱，這稱為反向查詢。亦即 DNS 伺服器必須登錄有關 IP 位址解譯到網域名稱，然而 IP 位址是一組

數字的組合，使用什麼方法來登錄最為方便呢？可讓查詢動作會最方便。早期 ARPANET 網路就想出一個便捷的方法，讓 IP 登錄的方法和網域名稱相同，而它的格式編寫如同網域名稱一樣，如下：(圖 13-4)

62.2.15.163.in-addr.arpa.

其中，in-addr.arpa. 為『**反向網域**』管轄有關 IP 位址對網域名稱的登錄，在這網域區域下的 163.in-addr.arpa 網域管轄有關 IP 位址為 163.×.×.×；又 15.163.in-addr.arpa 管轄 163.15.×.×；又 2.15.163.in-addr.arpa 管轄 163.15.2.×，而 62.2.15.163.addr-arpa 便登錄主機的網域名稱 (linux.cu.edu.tw)。由此可見，反向網域也是用反向的命名方式，這可和正向網域相同，因此，不但可以方便登錄次序，也可以用相同的演譯法來查詢。

從另方面來看，任何一部主機在 DNS 伺服器除了必需登錄網域名稱外，也必須登錄反向網域以供查詢。如圖 13-4 中，linux.cu.edu.tw 和 62.2.15.163.in-addr.arpa. 是表示同一部主機，但這兩份資料也不一定非得存放在同一部 DNS 伺服器上，可分別登錄不同的 DNS 伺服器上以供查詢。

13-4 DNS 伺服器種類

我們瞭解 DNS 查詢動作是非常繁雜的工作，上網連結時，隨時隨地都需要向 DNS 伺服器查詢相關的 IP 位址，尤其在瀏覽器上瀏覽網站時，只要用到超連結就必須求助於 DNS 來查詢網路位址。因此，隨著不同環境需求，而有不同的 DNS 伺服器種類，以下分別說明之。

13-4-1 本地快取資料庫

一般客戶端主機裡都備有『**本地快取檔**』**(Local Cache)**，來登錄已查詢過的資料。任何向 DNS 伺服器查詢過的資料，都會登錄在快取擋內，因此稱之為『**本地快取資料庫**』**(Local Cache Database)**，當下一次查詢同一網域名稱 (FQDN) 時，便可直接由快取檔回覆即可，而不用到 DNS 伺服器上查詢，這可以節省許多查詢的時間。

13-4-2 主機檔案

這是早期 Unix 系統上的 DNS 查詢方法，它將一些常用的主機名稱登錄在 主機檔案 (/etc/hosts) 內，當有查詢動作時，再到這個檔案內搜尋相對應的 IP 位址。目前這種搜尋法已漸漸不符所需，也很少人會再維護 /etc/hosts 檔案，但一般電腦系統還是會去搜尋它。

13-4-3 主要伺服器

表示負責某一網域區域(Domain Zone)的 DNS 伺服器，又稱為『主要伺服器』(Master Server)。有關本區域內的次網域名稱或主機名稱（FQDN），都必須向主伺服器登錄。而在主要伺服器上登錄的動作，稱之為『授權』(Authority)，也就是說，除非向主要伺服器（或次要伺服器）查詢到它所管轄的資料，稱之為『授權答案』(Authoritative Answer)；否則皆稱為『非授權答案』（Non-authoritative Answer)。

13-4-4 次要伺服器

一部主伺服器維護一個網域區域，如果負荷很重時，無法由一部伺服器承擔負荷，此時便需另外建構一部以上的『次要伺服器』(Slave Server) 來分擔負荷。基本上，次要伺服器並不負責登錄網域名稱的工作，它的資料是週期性的（一般都是 30 分鐘），由主伺服器轉移過來，這種由主伺服器轉送到次要伺服器的動作稱之為『區域轉送』(Zone Transfer)。次要伺服器除了負責客戶端的查詢動作外，另一重要的目的是作為主要伺服器資料的備份，萬一壞損時，可由次要伺服器上索取所有完整的資料。目前在 Internet 網路上有許多名稱伺服器，都有許多次要伺服器分散各地區以供查詢。

13-4-5 快取伺服器

『快取伺服器』(Cache Server) 是紀錄 DNS 伺服器所查詢過的資料，並不同於『本地快取資料庫』，後者是在客戶端主機上；而前者是在 DNS 伺服器上。當 DNS 伺服器的查詢資料量很大時，與其相對應的快取伺服器的資料也會成長很快，因此，一般較小的系統環境可將 DNS 伺服器和快取伺服器，由同一部主機來負責，然而針對較大的系統環境，快取伺服器可與 DNS 伺服器分開安裝，由不同的主機來分別處理。也就是說，快取伺服器可以是獨立的系統，但它的資料來源仍是由該區域的 DNS 伺服器供應。快取伺服器所登錄的資料非常具有時效性，管理人員必須設定更新時間，如果某一筆資料儲存太久，其正確性就值得懷疑，必須刪除。

客戶端查詢某一筆資料時，有可能由上述伺服器中的任何一部來服務，它們之間的優先順序為何？圖 13-5 表示客戶端提出某一查詢要求時，可能經過伺服器處理的優先順序，和各伺服器之間的關聯。一般客戶端主機上都有一只『解譯者』(Resolver) 程式，來負責查詢的工作。當主機上任何應用程式需要查詢時（反向或正向查詢），便呼叫 Resolver 程式，再由 Resolver 程式負責查

詢的工作。當 Reslover 接收到查詢命令時，首先查詢本機電腦內的快取資料庫（如圖 13-5 (1)），看看是否曾經查詢過相同的資料，如果有則回應資料給應用程式；否則再查詢主機檔案內是否有登錄該筆資料（如圖 13-5 (2)）；如果還是沒有，則 Resolver 程式就依照主機內所指定的 DNS Server（/etc/resolv.conf），發出查詢訊號（依照 DNS 通訊協定）（如圖 13-5 (3)）。此時，DNS Server 收到查詢訊號後，便直接查詢該筆資料是否有登錄，如果沒有登錄，再查詢快取伺服器上是否有該筆資料，如果有便可直接回應訊息，如果沒有也必須通知客戶端的 Resolver 向其他伺服器查詢，至於如何再向其他伺服器查詢的動作，將會在下一節介紹。在這個過程中，所指定的 DNS Server 並不一定是原客戶端所管轄的網域伺服器，有可能指定到次要伺服器（Slave Server）或者一部獨立的快取伺服器（Cache Server）上。

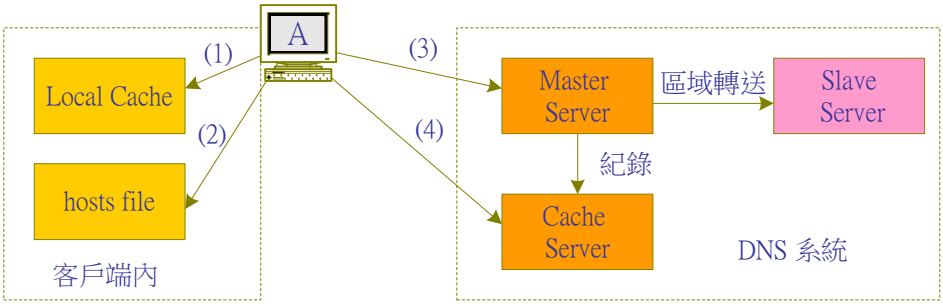

圖 13-5 DNS 伺服器種類與查詢順序

13-5 DNS 協定運作

當 DNS 伺服器收到某一筆查詢要求卻無法提供服務時，或者客戶端向伺服器查詢卻得不到正確回應時，應該如何向其它伺服器查詢呢？這就是 DNS 系統的協定運作。記得我們談過，DNS 是一種分散處理系統，所有 DNS 系統上的資料是由全球的 DNS 伺服器共同所構成，每一網域區域（Domain Zone）（如 cu.edu.tw）都有一部專屬伺服器（如 linux-2.cu.edu.tw），來負責紀錄該區域內的名稱資料（反向或正向查詢資料），同時負責被查詢的工作（但也可能一部專屬伺服器負責多個網域區域）。由此可見，除非查詢到該資料所登錄的伺服器，否則將會得不到正確的答案（這也不一定）。因此，DNS 系統的查詢動作就顯得非常困難與複雜，但首先我們來看兩個基本的查詢動作，再來看伺服器之間如何運作。

13-4-1 遞迴查詢與反覆查詢

『遞迴查詢』（Recursive Query）是當某一 DNS 伺服器收到查詢訊息後，而該筆資料並未登錄在伺服器上，這表示該伺服器必須向其它伺服器查詢。DNS 伺服器經由其它伺服器得知另一查

詢地方，該伺服器再向另一部伺服器查詢，如此反覆而得到查詢資料的動作，稱之為遞迴查詢。另一方面，被此伺服器查詢到，而回應它到另一伺服器查詢的動作，稱之為『反覆查詢』(Iterative Query)。簡單的說，反覆查詢的動作就是伺服器回應：『資料不在我這裡，請到另一地方查詢吧！』，如果經過多個伺服器都是同樣的回應，就如同一來一往的反覆動作一樣。

13-5-2 搜尋順序

瞭解遞迴查詢和反覆查詢動作之後，我們用圖 13-6 來探討當一伺服器接收到客戶端 Resolver 的查詢要求時，它如何來搜尋出應該到哪一個伺服器上查詢(資料所登錄位置)的動作。譬如 DNS 客戶端要求查詢 FQDN 名稱為 www.cu.edu.tw. 的 IP 位址，而將該查詢要求傳送到特定的 DNS 伺服器上 (DNS_A)，所搜尋的次序如圖中的編號順序。首先，DNS_A 搜尋本身紀錄是否有該筆資料 (包含 Cache Server)，如果沒有便直接向根 (『.』) 伺服器查詢，根伺服器回應網域為 tw. 的伺服器位址(IP 位址)給 DNS_A，然後 DNS_A 再向 tw. 網域伺服器查詢，而得到網域為 edu.tw. 的伺服器位址。如此以下類推，DNS_A 得到 cu.edu.tw. 網域的專屬伺服器位址，便向它查詢而得到 www.cu.edu.tw 網域名稱的 IP 位址，再回應給 DNS 客戶端。

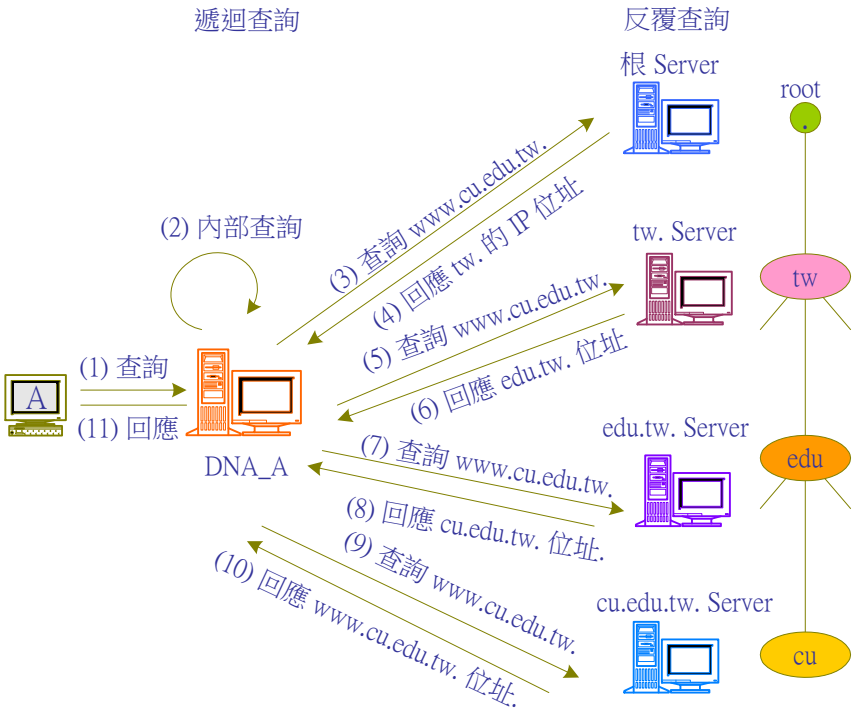

圖 13-6 查詢順序

由這個搜尋次序我們可以看出，所指定的 DNS 伺服器 (DNS_A) 每發送一個查詢後，得到下一個網域的伺服器位址，再往下一個網域伺服器查詢，直到得到答案為止，因此，DNS_A 正扮

演著『遞迴查詢』的動作。另外，其它伺服器只回應：『資料不在我這裡，請到另一地方查詢吧！』，而是共同扮演著『反覆查詢』的動作。

13-5-3 快取查詢

如果每一查詢都如同圖 13-6 的查詢順序，這將是一種耗時又耗力的動作，而 DNS 系統幾乎無法應用，還好每個 DNS 伺服器上都有快取伺服器，可以解決大部份的問題。我們可以發現原伺服器發出查詢的訊號都是『查詢 www.cu.edu.tw.』，在查詢當中，如果有某部伺服器的快取伺服器上有登錄該筆資料，便可直接回應，而不用再搜尋下去。甚至在搜尋當中也有可能是跳躍的。譬如，詢問到 tw. 伺服器時，就可以得到 cu.edu.tw. 伺服器的位址，便可直接向 cu.edu.tw. 伺服器查詢，而不必再經由 edu.tw. 伺服器查詢。另一方面，DNS_A 由 tw. 伺服器中得到 edu.tw. 伺服器位址後，便會記錄到快取伺服器上，下一次其它主機需要查詢 www.nsysu.edu.tw.的 IP 位址時，便直接向 edu.tw. 伺服器查詢即可，而不用到根伺服器查詢。

由此可見，快取伺服器扮演極重要的角色，我們絕大部份的查詢資料都是經由它得到的。當然，快取伺服器上的資料是經過查詢後所紀錄的，因此，當客戶查詢一個名不經傳的名稱，或者是第一次查詢該名稱，那可能真的要像圖 13-6 所示的搜尋順序了。但話又說回來，如果有一個 DNS 伺服器被許多客戶端指定，它的查詢機會非常的多，而它的快取伺服器上的紀錄也非常多，相對應的回應速度也非常快。當然這部名稱伺服器主機必須承擔非常重的工作負荷，因此，一般 ISP 公司都會指定一些特殊伺服器讓客戶使用，而 Internet 網路上也常會出現一些較有名氣的名稱伺服器，上面標明其查詢動作最快，任何客戶都可以指定它。

13-5-4 轉送服務

除了快取伺服器可以解決大部份的查詢問題，有一些名稱伺服系統也提供『轉送服務』『Forwarder』功能（如 Microsoft 系統）。在有轉送服務的系統下，當資料不在原伺服器（指定伺服器）時，它並不直接向根伺服器查詢，而是向所指定轉送的伺服器查詢，如果在指定時間內沒有得到適當的回應時，再到根伺服器查詢。另外在 Unix/Linux 系統下，主機都可指定多部名稱伺服器（如 /etc/resolv.conf 設定）（Windows 系列也可以），當一部名稱伺服器無法提供資料時，便會轉向其它伺服器查詢，並按照優先次序搜尋，說實在的，要能真的查詢到根網域也是不簡單。

13-6 DNS 訊息格式

由上述 DNS 運作程序，我們可以瞭解 DNS 系統中的訊息傳遞不但會出現在客戶端和伺服器之間，在伺服器和伺服器之間傳遞也非常頻繁，因此，DNS 的查詢動作就不像 Telnet 和 FTP 系統那麼簡單。在 Telnet 和 FTP 系統中，我們將客戶端和伺服端都模擬成網路終端機，而以 NVT ASCII 方式來互相通訊，雙方都用直譯程式來編譯傳遞命令。而 DNS 系統雖然也是以終端機模式來通訊，但雙方命令並非由使用者直接下達，而是 Resolver 程式執行查詢動作，因此沒有提供直譯命令的功能。如果需要由直譯命令來測試 DNS 伺服器功能，必須有特殊應用程式，譬如 nslookup 程式。

圖 13-7 (a) 為 DNS 訊息封包格式，它如同一般協定一樣，都是以 IP 封包傳送，並且採用 UDP 傳輸方式，連接在著名埠口 53 (53/udp)。不論 DNS 客戶端和伺服器之間，或伺服器和伺服器之間都採用此封包格式，它可區分為四大部份，以下分別介紹之。

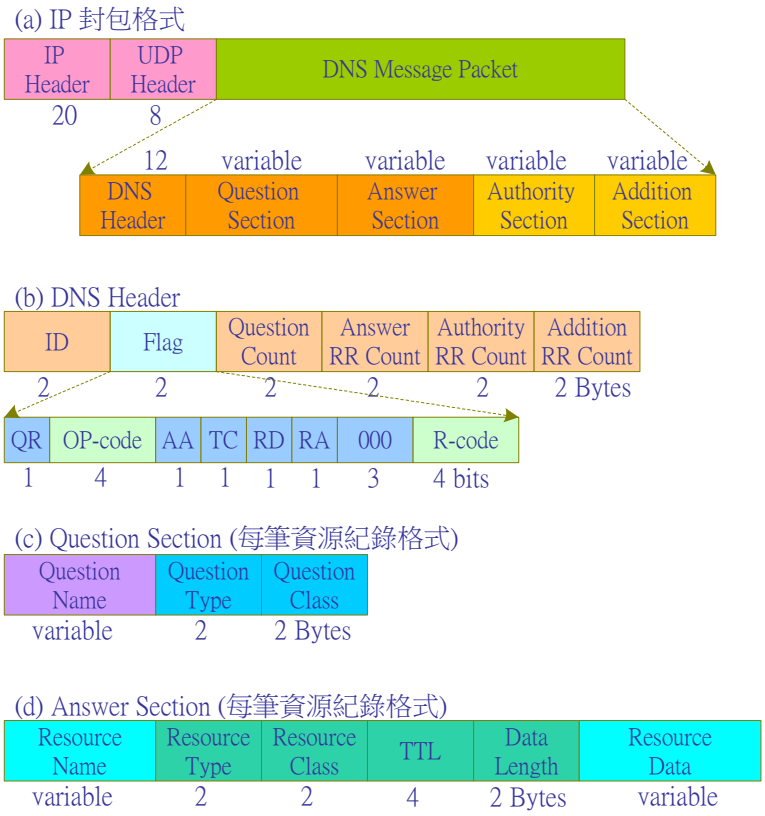

圖 13-7 DNS 訊息封包格式

13-6-1 訊息標頭

圖 13-7 (b) 為 DNS 訊息標頭格式，由此標頭可以分辨查詢或回覆型態，各欄位功能如下：

- **識別碼（Identifier, ID）：**此 16 位元識別碼的內容是由客戶端所設定，標示所詢問訊息的號碼，伺服端也按照這識別碼回應所詢問的訊息，客戶端再依照這個號碼比對是否為自己所發出的詢問訊息。

- **旗標（Flag）：**這 16 位元旗標示用來描述此 DNS 訊息封包的功能，各欄位功能如下：

  - ▲ **QR（Question/Response）：**本欄位為 0 表示此訊息是查詢；1 為回應訊息封包。

  - ▲ **OP-code(Operating Code)：**表示此封包的工作模式。0 表示標準查詢(正向查詢)；1 表示反向查詢；2 為伺服器狀態查詢；3 ~ 15 保留未用。

  - ▲ **AA（Authoritative Answer）：**1 表示所回應的查詢答案（答案區段中的資料）是具有授權的資料。這也表示該資料是由管轄的名稱伺服器得來的。

  - ▲ **TC（Truncated）：**TC = 1 表示原來資料長度過長，超過 UDP 封包所能承載（512 Bytes），而被截短了。

  - ▲ **RD（Recursive Desired）：**遞迴期待。RD = 1 表示此為『遞迴式查詢』；RD = 0 表示此封包為**『反覆式查詢』**。此位元大多由查詢封包設定，而回應封包也以相同內容設定。

  - ▲ **RA（Recursive Available）：**遞迴可獲得。一般都由回應的伺服器設定，RA = 1 表示支援遞迴。

  - ▲ **R-code（Response Code）：**回應碼。在回應封包裡表示處理查詢的結果，0 表示沒有錯誤發生；1 表示封包格式錯誤（Format Error）；2 為伺服器錯誤（Server Error），無法處理這個查詢；3 表示名稱錯誤（Name Error）；4 表示不支援此查詢類型（OP-code）（No Implemented）；5 為拒絕處理此查詢封包（Refused）。

- **問題計數（Question Count）：**表示後面緊接著問題區段的數量，圖 13-7 (c) 表示本查詢問題為一筆。

- **答案 RR 計數(Answer RR Count)：**表示後面緊接著答案區段中資源紀錄(Resource Record, RR) 的數量，如圖 13-7 (d) 為一筆答案的格式。

- **權威計數（Authority Count）：**權威區段的紀錄數量。

- **增加紀錄計數（Addition Records Count）：**此欄位為增加權威區段中紀錄的數量。

13-6-2 問題區段

『問題區段』（Question Section）是客戶端（或伺服器）向名稱伺服器查詢時，所攜帶 FQDN 名稱所儲存的位置。一般來講，客戶端每次向名稱伺服器查詢一個 FQDN 名稱（Question Count = 1），其問題區段格式如圖 13-7 (c)所示。然而客戶端並非每次都只查詢一筆資料，如需要詢問多筆資料時，則會在問題計數欄位中指明後面緊接著有幾個問題區段。如圖 13-7 (c)，問題區段的功能如下：

- **問題名稱（Question Name）：**此欄位存放所欲查詢的 FQDN 名稱，每一名稱長度不定，因此，此欄位的長度也不定。網域名稱的存放是以 ASCII 字元表示，最長限制在 64 個字元之內，名稱中的『.』（dot），並不表示出來，而以字元計數取代。譬如，查詢名稱為 www.cu.edu.tw，則填入問題名稱的格式如圖 13-8 所示。

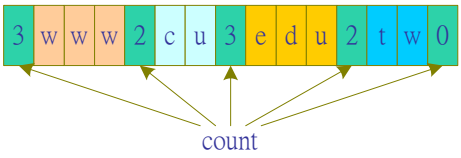

圖 13-8 問題名稱填入方式

圖 13-8 中，每個名稱的最前面欄位表示該名稱的長度，以 0 表示名稱的結束，也表示根網域名稱『.』。

- **問題型態（Question Type）：**長度為 16 位元，表示要查詢該名稱的資源紀錄（Resource Record, RR）型態，常用之紀錄型態如下：（各紀錄功能將於 13-7 節說明）

數值	資源紀錄（RR）名稱	功能
1	A	查詢 IP 位址
2	NS	查詢名稱伺服器
5	CNAME	查詢主機別名
12	PTR	反向查詢網域名稱
13	NINFO	查詢主機訊息
15	MX	查詢郵件交換紀錄

- **問題類別（Question Class）：**通常都為 1（IN），表示 Internet 通訊協定的位址，如果不是 1，則表示其他網路型態（非 IP 位址格式）。

13-6-3 答案區段

『答案區段』（Answer Section）裡所存放的是被查詢之名稱伺服器所回應資料，一般查詢都只是一筆資料（Answer RR Count = 1），其格式如圖 13-7 (d) 所示，如有多筆資料回應，則會在答案計數欄位中指明有幾筆資源紀錄（RR）。答案區段中各欄位功能如下

- ▲ **資源名稱（Resource Name）：**表示回答詢問的資源名稱，也就是要求詢問訊息封包內問題區段之問題名稱欄位的內容。也表示針對哪一個問題名稱作回答，存放格式也如同圖 13-8 所示。
- ▲ **資源型態（Resource Type）：**資源紀錄（Resource Record, RR）型態，也是如同問題區段中的問題型態一樣。
- ▲ **資源類別（Resource Class）：**如同問題類別，一般都為 1（IN），表示 Internet 網路。
- ▲ **存活時間(Time-To-Live, TTL):** 長度為 32 位元的正整數，以秒為單位，表示該筆 RR 紀錄可以存活的時間(也就是，可儲存於 Cache 的時間)，如超過此時間(一般都是 2 天)，則表示該筆資料已失去時效，必須將其刪除。如果 TTL = 0，表示該筆記錄為變動性，而接收端（客戶端或伺服器）不必再儲存於快取伺服器（或快取資料庫）上。
- ▲ **資源資料長度（Resource Data Length）：**16 位元長度，表示後面資源資料的長度，以位元組計算。
- ▲ **資源資料（Resource Data）：**不定長度。表示所回應的資源紀錄（RR）的答案，譬如，RR = A（詢問主機位址），則資料資料欄位回應該主機的 IP 位址（163.15.2.30）。

13-6-4 授權區段

DNS 查詢中所得到的並非直接的答案，而是被查詢之伺服器回應可查詢到的其它伺服器資訊（如圖 13-6 中遞迴查詢），此時，便將該資訊儲存於**『授權區段』（Authority Section）**內。授權區段所儲存的格式也如同答案區段一樣，只不過資源資料欄位所存放的是所指明的 DNS 伺服器的網域名稱，而不是它的 IP 位址。另外**『增加紀錄區段』（Addition Records Section）**是當授權區

段有存放資料時才會加入，也是六個欄位，但是資源名稱和資源型態兩個欄位並不存放查詢的網域名稱（FQDN），而是存放授權區段中所紀錄的 DNS 伺服器名稱及其 IP 位址。

13-7 資源紀錄

『資源紀錄』（Resource Record, RR）表示存放在 DNS 伺服器上，提供一般客戶端查詢的資料。我們在前面談過，DNS 系統是整個 Internet 網路的核心，它不但提供網域名稱和主機位址（IP）之間的轉換查詢，還提供許多有關 Internet 網路上許多資訊，這些資訊便是 DNS 系統上所紀錄的資源紀錄。當然，一個 DNS 系統所能提供的資源紀錄愈完整，對它所能提供的服務也愈完善，在 RFC 1035 上有許多資源紀錄的規範，但並不是所有 DNS 伺服器都提供這些服務，這需要管理人員耐心設定才可達成。以下介紹較常用的資源紀錄（RR）。

（A）紀錄 A – IPv4 主機位址

主機位址（Address, A）資源紀錄，是紀錄 FQDN 名稱到 IP 位址（32 位元）之間的轉換，此為 DNS 資料庫最常見的 RR。

（B）紀錄 CNAME – 主機別名

主機別名（Canonical NAME, CNAME）資源紀錄是提供主機設定另一個別名紀錄。CNAME 是非常重要的資源紀錄，提供不同的網域名稱轉譯到同一個 IP 位址，較常用的是將 www、ftp、mail 名稱轉譯到同一主機位址，譬如，www.cu.edu.tw、ftp.cu.edu.tw、mail.cu.edu.tw 都是 linux-2.cu.edu.tw 的別名，也表示同一主機位址。設定時，每一主機只能設定一個 A 紀錄，而其它別名紀錄（CNAME）便設定到此 A 紀錄的主機上，同一主機可以設定多個 CNAME 紀錄。

（C）紀錄 NINFO – 主機資訊

主機資訊（Host INFOrmation, HINFO）資源紀錄是登錄主機使用的硬體和作業系統訊息，以供查詢使用。

（D）紀錄 MX – 郵件交換

郵件交換（Mail Exchange, MX）是用來設定區域中擔任郵件伺服器的主機位址，以及多個郵件伺服器之間的優先次序。當區域中建立 MX 紀錄之後，便會依照所紀錄的郵件主機和其它區域的郵件主機交換信件，同時設定多個主機以防郵件主機當機，保持郵件傳遞順暢。在這麼多個郵件

主機之中，以數值大小來決定傳送優先次序，數值愈小者，優先權愈高，如『MX 10』表示優先數值為 10。

（E）紀錄 NS – 名稱伺服器

名稱伺服器（Name Server, NS）紀錄是用來指定管理網域區域（Domain Zone）的主機名稱。

（F）紀錄 PTR – 反向位址指標

指標（Pointer, PTR）紀錄是用來登錄由 IP 位址轉譯成 FQDN 名稱，其功能剛好和 A 紀錄相反。也就是說，使用 PTR 來建立 in-addr.arpa 的反向網域檔案。

（G）紀錄 SOA – 授權啟動

授權啟動(Start Of Authority, SOA)是在任何網域區域設定中的第一項紀錄，用來指定 DNS 伺服器或是目前區域上的主要伺服器名稱，以及有關伺服器的設定內容。在 SOA 紀錄上所設定的內容主要是伺服器版本和到期日期，以及區域授權伺服器之間 (主要和次要伺服器之間) 的區域傳送頻率。

（H）紀錄 TXT – 文字

文字（Text, TXT）紀錄是提供一些文字說明，用來說明主機或網環境的設定。

（I）紀錄 AAAA – IPv6 主機位址

AAAA 資源紀錄是將 DNS 網域名稱對應到 IPv6 的 128 位元位址。

（J）紀錄 AFSDB – Andrew 系統

Andrew 檔案系統資料庫（Andrew File System Database, AFSDB）資源紀錄的功能是將某一網域名稱對應到另一子類型網域名稱的主機，而子類型伺服器的主機名稱，可支援下列兩種型態：

- **數值 1**：表示伺服器儲存格式為 AFS 3.0 磁碟區位置伺服器。
- **數值 2**：表示伺服器儲存格式是已驗證之名稱伺服器的根目錄，且以 OSF（Open Software Foundation）的驗證命名儲存格式。

13-8 DNS 客戶端設定 – resolv.conf

一般 Unix/Linux 系統上，都有一只『解址器』(Resolver) 程式負責 DNS 查詢工作，而它是在 /etc/resolv.conf 檔案上設定的 (也可以由 netconf 或 linuxconf 來設定)。Resolver 並非一個獨立明確的處理程序，而是提供網路程式呼叫的程式庫。如果主機有設定 resolv.conf 檔案，網路程式每次開始使用 Resolver 時，都會讀取這個檔案。如果主機沒有 resolv.conf 檔案，則會企圖連接本地的 named 程式 (DNS 的守護程式)，雖然如此也可以達到查詢的目的，但除非本地主機也是名稱伺服器 (才會有 named)，才能連結得到。另一方面，某些系統的 named Daemon 設定方式不同，也許無法查詢到所需的資料。因此，無論一般主機或伺服器都必須安裝有 /etc/resolv.conf 檔。我們以 linux-2 主機上的 /etc/resolv.conf 為範例如下：

```
[root@linux-2 root]# cat /etc/resolv.conf
search cu.edu.tw
nameserver 163.15.2.30
nameserver 210.17.1.1
nameserver 202.145.138.200
```

上述範例中，cu.edu.tw 為本身網域名稱；163.15.2.30 是本書 DNS 伺服器範例的位址；210.17.1.1 和 202.145.138.200 兩者是由 linux-1 主機 (NAT 路由器) 上抄錄過來的。以下說明 /etc/resolv.conf 各欄位之功能：

(1) domain：domain 設定預設網域名稱。

(2) serach：search 紀錄用來記錄要搜尋的網域。例如紀錄是 cu.edu.tw，則關於 liunx-1 的搜尋會以 linux-1.cu.edu.tw 來進行。

(3) nameserver：nameserver 指定給 Resolver 詢問網域資料的伺服器 IP 位址。詢問的順序就按照名稱伺服器在設定檔裡排列的順序。如上檔案中，首先查詢 210.17.1.1，如查詢不到，再往 202.145.138.200 上查詢，依此類推。

(4) option：option 是用來設定 Resolver 的某些選項。Option:debug 用來啟動除錯功能；option ndots:n 用來設定主機名稱內的點號數目，以決定是否使用預設網域，預設值是 1。若指定 option ndots:2，包含一個點號的主機名稱就有預設網域，但包含兩個點號的位址則沒有。

範例檔案表示 linux-2 設定了三個預定名稱伺服器，最前面的伺服器（163.15.2.30）優先權最高，當 linux-2 主機以客戶端身分查詢網域資料時，首先到 163.15.2.30 查詢，如果失敗，再到 210.17.1.1 查詢，如再失敗，則到 202.148.138.200 伺服器上查詢，如果還是失敗，再由 163.15.2.30 向根網域查詢。

13-9 DNS 查詢命令 – nslookup

如果 DNS 伺服器依照上述製作主設檔與相關查詢檔之後，還是需要重新啟動 named 守護程式才會有效。或是有修改查詢檔案內容(增加或修改 RR 紀錄)，也是需要重新啟動 named 程式，重新啟動命令如下：

```
[root@linux-2 RPMS]# /etc/rc.d/init.d/named restart
Stopping named:      OK    ]
Starting named:      OK    ]
```

當 DNS 伺服器設定完成之後，我們可以利用 nslookup 命令來測試伺服器的查詢動作。自從 bind 8.0 版以後，該命令必須以 "nslookup –sil" (請參考 #man nslookup 說明) 方式下達。為了使讓讀者更清楚 nslookp 的動作，我們以 linux-1 主機 (如圖 9-1 所示)，來測試 linux-2 主機上的 DNS 伺服器，當然，也可以連結測試其它 Internet 上的 DNS 伺服器。首先我們來看 linux-1 主機的預設 DNS 伺服器，這可由 /etc/resolv.conf 檔案查出。因為 linux-1 是 NAT 路由器，它的 DNS 伺服器位址是經由 ADSL 的 ISP 廣播而來，檔案內容如下：

```
[root@linux-1 /root]# cat /etc/resolv.conf
search cu.edu.tw
nameserver 163.15.2.30
nameserver 210.17.1.1
nameserver 202.145.138.200
```

其中，163.15.2.30 是由管理設定的，另外 210.17.1.1 和 202.145.138.200 是經由 ISP 廣播而來。以下利用 nslookup 來測試伺服器的查詢動作。

(A) 啟動 nslookup，並查詢預定 DNS 伺服器

```
[root@linux-1 /root]# nslookup   –sil
```

```
Default Server:    linux-2.cu.edu.tw

Address:    163.15.2.30

> server

Default server: 163.15.2.30

Address: 163.15.2.30#53

Default server: 163.15.2.30

Address: 163.15.2.30#53

Default server: 210.17.1.1

Address: 210.17.1.1#53

Default server: 202.145.138.200

Address: 202.145.138.200#53
```

由此可看出，共計有三個預定伺服器，也如同 /etc/resolv.conf 檔案設定，並且都在傳輸埠口 53（53/udp）。

（B）查詢正向網域 – A

```
> linux-1.cu.edu.tw

Server:              163.15.2.30

Address:             163.15.2.30#53


Name:      linux-1.cu.edu.tw

Address: 163.15.2.62
```

我們可以看出，查詢 linux-1.cu.edu.tw 主機的 IP 位址為 163.15.2.62。

（C）查詢反向網域 – PTR

```
> 163.15.2.30

Server:              163.15.2.30

Address:             163.15.2.30#53


30.2.15.163.in-addr.arpa            name = linux-2.cu.edu.tw.
```

查詢 IP 位址為 163.15.2.30 的網域名稱（FQDN）為 "linux-2.cu.edu.tw."。

（D）查詢主機別名 – CNAME

```
> www.cu.edu.tw
Server:         163.15.2.30
Address:        163.15.2.30#53

www.cu.edu.tw   canonical name = linux-2.cu.edu.tw.
Name:   linux-2.cu.edu.tw
Address: 163.15.2.30
```

查詢 www.cu.edu.tw 的主機位址，回應是 linux-2.cu.edu.tw. 的別名，而 IP 位址是 163.15.2.30。

（E）查詢快取伺服器 – Catch Server

```
> server 210.17.1.1
Default Server:  210.17.1.1
Address:  210.17.1.1#53

> www.nsysu.edu.tw
Server:  210.17.1.1
Address:  210.17.1.1#53

Non-authoritative answer:
Name:   www.nsysu.edu.tw
Address:  140.117.11.112
```

利用外部 DNS 伺服器（210.17.1.1）來查詢 www.nsysu.edu.tw 的 IP 位址，所得到的是非授權資料 140.117.11.112。也就是說，它是由 210.17.1.1 的快取伺服器所得到資料，這也表現出快取伺服器的重要性。如果某部伺服器經由多人使用之後，所攫取的資料較多，一般來說就足以應付客戶的查詢。如果我們在客戶端主機上都有指定多部 DNS 伺服器以供查詢，而將轉送到根網域查詢的機率降到最低，才可提高 DNS 系統的效率。

（F）查詢名稱伺服器 – NS

```
> set type=ns
> cu.edu.tw
```

```
Server:         163.15.2.30
Address:        163.15.2.30#53


cu.edu.tw       nameserver = cu.edu.tw.
```

（G）查詢郵件交換紀錄 – MX

```
> set type=mx
> cu.edu.tw
Server:         163.15.2.30
Address:        163.15.2.30#53


cu.edu.tw       mail exchanger = 5 linux-1.cu.edu.tw.
cu.edu.tw       mail exchanger = 10 linux-2.cu.edu.tw.
```

如果還想要查詢其它 RR 紀錄，也同樣，首先設定查詢型態（set type=RR），其中 RR 為紀錄名稱，譬如：A、NS、SOA 等等。

習題

1. 請簡述 DNS 系統有哪三個基本功能。
2. 請敘述 DNS 系統在 Internet 網路上所扮演的角色，及其重要性。
3. 請說明 DNS 系統的正向解譯的運作方式。
4. 請說明 DNS 系統的反向解譯的運作方式。
5. 請說明 DNS 系統郵件解譯的運作方式。
6. 何謂反向網域？並請說明它的建構方式。
7. 何謂『完整網域名稱』（FQDN）？
8. 一般 DNS 伺服器有哪幾種類型？請分別說明其功能。
9. 何謂『網域區域』（Domain Zone）？
10. 何謂 DNS 系統的『主要伺服器』（Master Server）？何謂『次要伺服器』（Slave Server）？

11. 何謂『**區域傳輸**』(**Zone Transfer**)？如何規劃它發生的週期和有關參數？

12. 何謂『**遞迴查詢**』(**Recursive Query**)？何謂『**反覆查詢**』(**Iterative Query**)？兩者之間有何關聯？

13. 請用一個範例來說明 DNS 系統的搜尋順序，這和實務上 DNS 查詢有何差異？

14. 何謂『**快取伺服器**』(**Cache Server**)？它在 DNS 系統上扮演何等角色？

15. Unix/Linux 系統的客戶端如何來指定多個預定 DNS 伺服器？又 Windows 系統的客戶端如何指定多個預定 DNS 伺服器。

16. 請說明 DNS 系統中，資源紀錄(RR)型態為 A、CNAME、SOA、MX 和 PTR 的功能為何？

17. 請利用 nslookup 程式命令來查詢您的預定名稱伺服器上的 SOA 和 MX 紀錄，並說明查詢內容的功能。

18. 請利用封包擷取軟體(附錄 A)，擷取一個 DNS 查詢封包(主機上可執行 nslookup 命令)，來分析 IP 和 UDP 封包格式。

19. 同上題，擷取一個主機名稱查詢，並分析 DNS 查詢和回應的封包格式。

20. 同上題，擷取一個反向解譯查詢，並分析 DNS 查詢和回應的封包格式。

21. 同上題，擷取一個非權威性的資料(由 Cache Server 得到)，並分析 DNS 查詢和回應封包格式。