4

Ubuntu Linux 管理

4.1 帳號管理

4.1.1 Ubuntu Linux 上的使用者能做些什麼

Linux 主機若拿來擔任伺服器的工作，那麼帳號能用的功能，就會依主機所提供的服務而定。具體而言，「郵件」、「SSH」、「FTP」與 「SAMBA」這幾個服務，是與使用者帳號比較相關。意即，若網管人員在 Linux 架設了以上服務，原則上所有自建的使用者帳號皆能使用，不必再個別指定。

更具體一點來說，一旦網管人員使用「adduser」建立了一個使用者，而且上述服務皆已建立妥當，那麼他就可以收發郵件、使用終端機登入主機以及使用「FTP」或「SAMBA 網芳」存取家目錄上的檔案。

4.1.2 到底有多少類型的「帳號」

網管人員在初學 Ubuntu Linux 的時候，常被一大堆「帳號」給搞昏頭，為什麼 A 帳號可以收發郵件，卻又無法登入 XOOPS；又為什麼要分 MySQL 的 root 帳號與 Linux Root 帳號；為什麼改完 Linux 帳號的密碼，可以用新密碼收發郵件並登入 FTP，卻無法登入 SAMBA 網芳。「到底有多少帳號類型？要如何管理？」，便是一個重要的課題。

的確，很多網路服務都有自己的一套帳號管理系統，無法直接使用 Ubuntu Linux 上的帳號。如果您要求一定要統一帳號，目前通用的解決方案，是另外架 LDAP 認證伺服器，然後修改各服服器的設定檔，使其能經由單一的 LDAP 認證系統。

1. 各伺服器之帳號別

底下筆者把 Ubuntu Linux 常用的「帳號類型」做個分析整理：

- 使用 Ubuntu Linux 主機帳號密碼的服務：SSH、FTP、Mail（含 Webmail）

以上只是在預設狀態下才使用 Linux 帳號，其實各伺服器都可以設定成使用獨立的帳密管理系統，來因應特定要求。

- 使用 Ubuntu Linux 帳號，但有獨立密碼：SAMBA
- 獨自的帳密系統：MySQL、各種網頁內容管理器，如：XOOPS、WIKI、Moodle...etc

2. Ubuntu Linux 主機帳號類型

Ubuntu Linux 主機帳號密碼又分成「系統帳號」與「使用者帳號」兩類，系統帳號的意思是，「各系統伺服軟體因有檔案操作的需求，而建立的帳號」；使用者帳號是指「由網管 人員建立，供使用者登入存取主機服務用」。它們之間最大的差異是系統帳號是不可由終端機登入的，而使用者帳號沒問題。

常見的系統帳號，有 root、syslog、www-data、vsftpd... 等，一般而言，伺服軟體幾乎都有寫入檔案的需求，比如：postfix 要把收到的信件暫存於 /var/mail，又如 vsftpd 要把使用者登入存取的過程記錄在 /var/log 底下。這些檔案的寫入，都必須是要有檔案寫入權，也就是要先有帳號，才可賦予寫入權限。因此，每當安裝一個伺服軟體，就會多出一個系統帳號。

這些系統帳號不可隨意刪除或變動，而且每次重灌 Ubuntu 系統，各伺服軟體系統帳號之 UID 與 GID 不一定會與上次所安裝的一樣。這也是為什麼本書第十三章在說明 rSync 備份取回時，要求不得直接把帳號檔（/etc/passwd）直接從備份機蓋掉重建主機的 /etc/passwd，一旦做了這件事，那麼系統帳號的 UID 及 GID 會全亂了套，功能自然大亂。

4.1.3 Ubuntu Linux 主機帳號管理

1. 帳號管理暨其設定檔

- Ubuntu Linux 的使用者帳號管理核心四檔，以下四檔只有 root 權限才可瀏覽與修改。
  - 帳號基本資訊： /etc/passwd
  - 密碼： /etc/shadow

- 群組：/etc/group
- 群組密碼：/etc/gshadow（不常用）

/etc/passwd 內容初解

```
# 欄位解釋
# 帳號 : 密碼 : User ID : Group ID : 個人資料說明 : 家目錄位置 : SHELL 執行權
saned:x:112:121::/home/saned:/bin/false
yh:x:1000:1000:yh,,,:/home/yh:/bin/bash
sshd:x:113:65534::/var/run/sshd:/usr/sbin/nologin
```

- 密碼：已獨立在 /etc/shadow，所以一律以「x」來代替。
- 使用者帳號會從 1000 開始編號，而且 UID 與 GID 一致。

  由此可知，上面範例中的「saned」及「sshd」皆是屬於系統帳號，「yh」是使用者帳號。
- /bin/false：該帳號不能使用 SHELL

  若以 SSH 登入，輸入完密碼，就直接被主機跳離。
- /bin/nologin：該帳號可以用 SHELL 但不可登入

  若以 SSH 登入，它還是會跳出密碼供使用者 Key IN，只是不管密碼正確與否，都會出現「Access Denied」訊息。
- /bin/bash：該帳號可登入並使用 SHELL。

2. 帳號管理指令

先切換成 root 身份

```
user@dns:~# sudo -i
```

新增帳號，以 yhtest 帳號為例：

```
root@dns:~# adduser yhtest
增加使用者 `yhtest' ...
增加新群組 `yhtest' (1001) ...
增加新的使用者 `yhtest' (1001) with group `yhtest' ...
```

```
Creating home directory `/home/yhtest' ...
Copying files from `/etc/skel' ...
輸入新的 UNIX 密碼：
再次輸入新的 UNIX 密碼：
passwd：密碼已成功地變更
正在改變 yhtest 的使用者訊息
請輸入新值，或直接按 ENTER 鍵以使用預設值
        全名 []:
        房間號碼 []:
        工作電話 []:
        住家電話 []:
        其它 []:
以上輸入的資料正確嗎？[是／否] y
```

- 刪除帳號，一樣以 yhtest 為例

```
root@dns:~# userdel -r yhtest
```

「-r」意思是連同 /home/yhtest 也一併刪除。

3. 大量建帳號工具

若您有大量建立帳號的需求，可以使用筆者提供的 yhtools/maccount 工具來協助。本工具會要求您自行準備好「帳號：密碼」列表，再依該檔案內容新增。

- 下載並解壓 yhtools
  - root@dns:~# wget http://myip.tw/download/yhtools.tar.gz
  - root@dns:~# tar xzvf yhtools.tar.gz
- 進入 /root/yhtools/maccount 目錄
  - root@dns:~# cd yhtools/maccount
  - root@dns:~/yhtools/maccount#

5

網路概念暨 Ubuntu 網路服務概說

- 5.1 InterNet 網際網路
- 5.2 網路基本概念
- 5.3 IP Address 基本概念
- 5.4 IPv4 網段分割
- 5.5 網路硬體
- 5.6 網路服務管理

網路（Network）是利用傳輸線（或無線電波），把四散的電腦／印表機／網路儲存設備等連結起來，使得彼此間的資料可以互通的一種技術。在早期，台灣網路尚未發達之前，電腦與電腦間的文件交換，要不使用磁碟片來做為媒介，要不就得使用 LL3 線材連結，再搭配特定軟體，把兩台電串接起來交換檔案。可是這樣的架構，就只能串接兩台電腦，而網路的出現，不只家裡的電腦間彼此串連了起來，並實現了在家能知天下事的夢想。

一般人說到「網路」，第一聯想到的就是上網（surf the internet），而這個網路世界，可以讓人玩游戲、看新聞、購物...等等。在這樣的概念之下，電腦與電腦之間就會變成一種主客關係：主人是網站服務主機（Server），如 http://tw.yahoo.com，它可以提供新聞、購物、拍賣、字典等等的服務來等客人上門。而另一個端卻是客人（Client），它只負責讓使用者在網址列上輸入網址，按個「Enter」，便把伺服器所提供的網頁秀在螢幕上。而且重要的是，這兩者之間地理上的距離，可以是近在咫尺，也可能是遠在天邊。為達成此目的，其中的 原理非常深奧，筆者也懂的不多，只能就我個人淺見，以本章來簡要介紹。

5.1 InterNet 網際網路

我們知道，網路叫「Net」，以學校而例，整個學校的電腦用網路線接起來，便會形成「校園網路」。依此理論，兩所學校互連，便是「校園網路」與「校園網路」之間互連。而英文字：「inter-net」便是代表了這個狀況：「網路與網路之間」互連，簡言之，InterNet 就是全世界串在一起的網路系統，讓我們可以在學校連到自己學校的官方網站，也可以連到美國 amazon 買書，或是到中國大陸的淘寶網購物。

5.2 網路基本概念

5.2.1 什麼是 TCP/IP

我們知道郵差送信，一定要依地址才可。那麼在全球巨大的網路系統內，電腦與電腦間要溝通，第一件事就是要有「電腦地址」，而這個電腦地址就是 IP Address。另外，當郵局送信或包裹時，必須要確保物品的完整性，不然我們是

可以拒收的。在電腦網路，負責物品（封包）完整性的控制工作，就是由傳送控制協定（TCP：Transmission Control Protocol）來幫忙。

全球網路的相連，中間會間隔很多各種不同的設備；簡單如家中的 Cat5 網路線加集線器，複雜如偏遠山區的微波基地台或國與國之間的海底電纜等。這些設備運作方式差異度很大，想要讓它們彼此間能互通溝通，就必須遵循相同的語言（通訊協定），否則你講你的，他講他的，誰也上不了網。基於這個構想，國際標準組織（ISO）就制定一組開放系統互連（OSI）參考模型。TCP/IP 網路架構也是基於這個理念所發展而成，而且，它在美國強力的推廣之下，已然取得全球的認可，成為全球互連的主要標準，下面「表 5-1」顯示出 OSI 參考模 型與 TCP/IP 間的關係。

對於網管／使用者而言，對這些通訊協定其實只要具備基本觀念就好，因為其理念的具體實作是網路設備商的事情。比如：集線器一定得符合 OSI Layer1～Layer2 規定，無線 AP 路由器則至少要符合 Layer1～Layer4 的規定，不然若造成電腦無法成功連線，這些網路商品也賣不出去。

5.2.2 OSI 七層次架構與 TCP/IP 四層次架構

表 5-1 TCP/IP 與 OSI 七層對照表

	OSI 七層	TCP/IP 四層 通訊協定	簡要說明
Layer 7	表達層	應用層	• 功能：應用程式，如 IE、Firefox、FTP... 等。 • 相關設備：電腦、網路電話、入侵防禦系統（IPS）等。
Layer 6	對談層		
Layer 5	傳送層		
Layer 4	傳送層	TCP / UDP	• 功能：控制資料傳輸之正確性；為應用程式開設服務窗口（Port）。 • TCP：強調資料正確；多用 於 HTTP、FTP 等注重資料完整性的網路服務。 • UDP：強調資料傳送順暢；多用於多媒體資料或網路電話語音傳送。 • 相關設備：防火牆等。

實務上，若只給您一個 IP 值，再告訴您網路遮罩，您要如何算出此網段之代表號及廣播，並以另一型式寫出該網段。範例：163.26.119.131 / 255.255.255.192

```
10100011.00011010.01110111.10000011/11111111.11111111.11111111.11000000
```

- 分析一：前面共有 26 個數字不能變化
- 分析二：所以 10100011. 00011010. 01110111. 10（163.26.119.128 是不會變化的）
- 分析三，最小值（代表號）便是：10100011. 00011010. 01110111. 10000000 (163.26.119.128)
- 分析四，最大值（廣播）便是：10100011. 00011010. 01110111. 10111111 (163.26.119.191)
- 因此，網段另一種寫法是：163.26.119.128/26

作業：163.26.62.90 / 255.255.255.192

請自行把上述兩個值轉成二進位值，再進行分析，便可得解。

5.4.4 IPv6 網段分割

IPv6 的網段分割與 IPv4 完全一樣，只是其網址表示法以 16 進位來表示而已，若各位把其網址完全二進位化，再來執行 AND 運算，一樣可以得到相同的結論。

5.5 網路硬體

在講完軟體的通訊協定暨其簡易的運作原理後，再來要談談實現這些運作的硬體設備有那些，並簡單交代一下其歷史，以方便讀者了解一些名稱之命名由來。

5.5.1 各種網路拓樸

網路拓樸可以是兩種意義：

1. 依理論上電子訊號在設備間交換所走的路徑及其原理而定
2. 依實際上網路設備安裝位置及佈線型式來看

目前，在各大市面上所販賣的設備，無論是有線或無線，幾乎都是採用乙太網路（ethernet）之通訊協定（802.3）產品，而這也是各國中小學所採用的硬體設備。所以在下文，筆者只針對乙太網路做詳細的介紹。其餘，請自行參考相書籍。

5.5.2 乙太網路（ethernet）簡介

1. 資料傳遞原理

乙太網路訊號傳送的拓樸是採用【匯流排式(BUS)＋廣播】式，也就是，大家都是必須經由同一條公共走道送出訊息。而且，甲電腦要送資料給乙電腦時，是由 甲把資料經由匯流排（BUS）廣播到所有節點。每個節點接到封包後，發現不是他的，便直接丟棄。只有乙電腦拆封後，看一下收件人是自己，才會把它接收起來。

因為此一特性，所以在 BUS 上，一次只允許一台傳送資料，若兩台同時傳送，就會發生碰撞（Collision）。為了解決此問題，它採用了載波感應多重存取／碰撞偵測（Carrier Sense Multiple Access / Collision Detection; CSMA/CD）基頻技術。也就是說，一台設備要送訊號之前，要先聽一下（listen），道路是否正在使用中，若沒人用，才送出資料。若有人用，就再等。但即使如此，仍 可能因兩台同時偵測到沒人用，同時送出封包而發生碰撞。一碰撞，此節點會立即發出擁塞（jam）訊息到 BUS 上。此一 BUS 上的設備接到 jam 訊息後，便會中止動作，進入等待狀態，過一段時間，才又隨機啟動傾聽／傳送的動作。

搭配早期的乙太網路設備圖（請參考下圖），就很容易理解上述的原理。依圖示，我們發現電腦間利用 RG58 線材（類似電視第四台的訊號線），所建構成的 BUS 來溝通訊息。

另外要注意的是，「網域名稱的有無」與郵件服務可是息息相關的，若沒有正當的網域名稱，家中郵件伺服器所寄出的信件，大多都會被判定為垃圾郵件而退件，由此便知本服務的重要性。

筆者以自己所申請的泛英網域（myip.tw）為例，圖解上述這樣的階層關係，以及自己 DNS Server 可做的事情：（一）.自由新增「主機名－IP」對照；（二）.再分配其子網域出去給別台 DNS Server，比如說 yhlab.myip.tw。

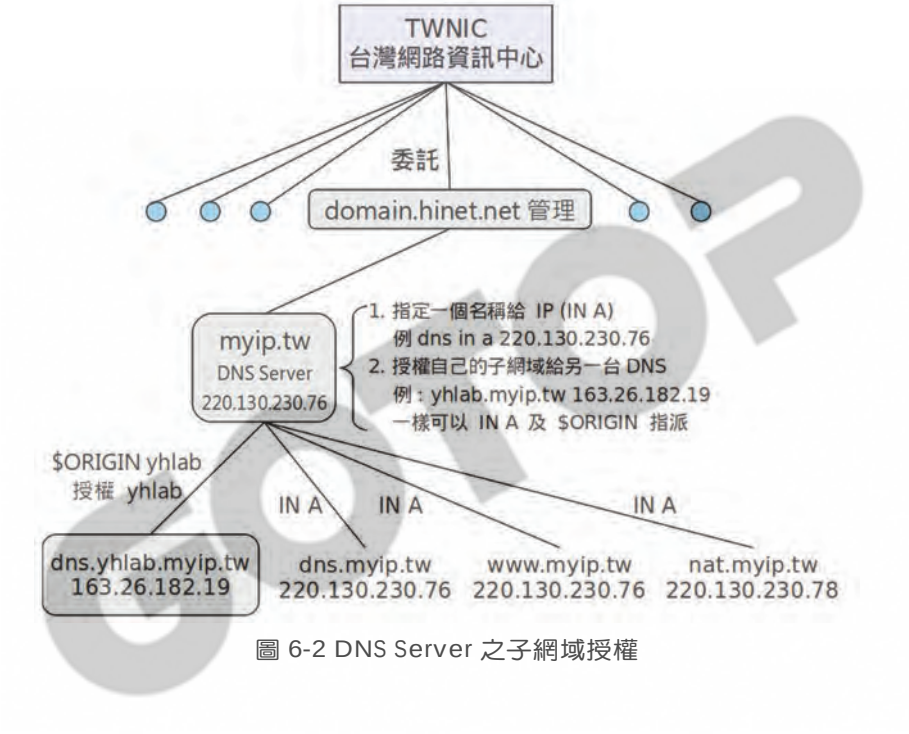

圖 6-2 DNS Server 之子網域授權

由上面範例得知網域正解之 IP 指定（IN A）或子網域授權，並不限於同一 IP 網段；反解才會受限。

6.1.3 Client 端上網查詢 IP 位址過程

由於 DNS 的管理是一種分散式的管理，查詢時是由頂層（/etc/bind/db.root 內所記錄的根查詢區）而下的「層層下問」，因此，為加快反應速度，好不容 易問

來的答案會被暫存 86400 秒（24HR），這種機制稱之為 DNS Cache(快取)，下圖呈現了 Client 端向 dns server 查詢「英文網址－IP 位址」的過程，請參考。

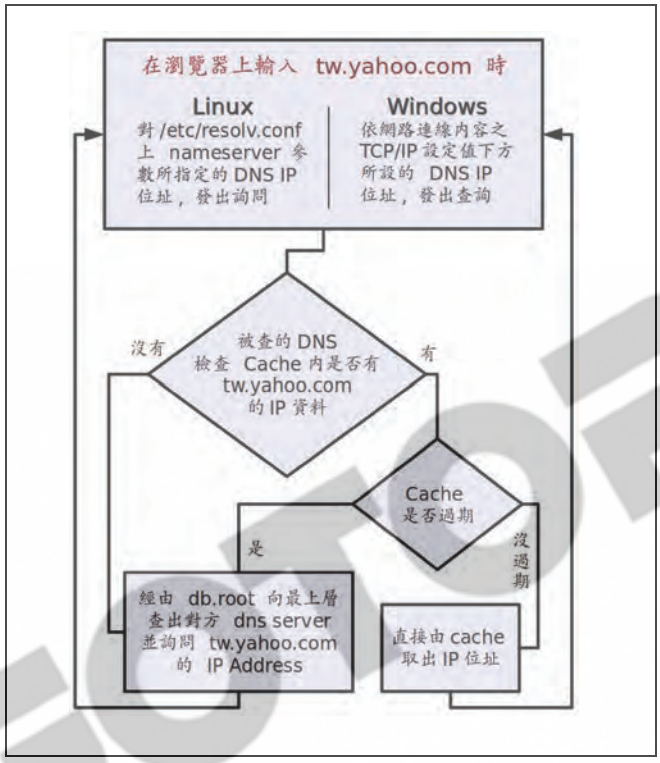

圖 6-3 DNS Client 查詢 IP 位址流程圖

6.2 DNS 伺服器安裝與初步設定

有了上述幾個概念之後，實際的安裝與設定工作，就不太困難了。安裝設定的步驟簡述如後：

1. 使用 apt-get 指令安裝 bind9 套件。
2. 下載並執行筆者提供的 dns 設定檔產生器，以完成初步的設定工作。
3. 若要指定額外的網址，可以直接修改正反解檔。