第九章 伺服器管理

9-1 網路伺服器簡介

9-1-1 前置作業 - 伺服器系統

安裝伺服器之前，需考慮該平台的安全性如何。亦是，期望 CentOS Linux 的安全能力到甚麼程度，以及以甚麼方式安裝。吾人以一般 **SOHO** (Small Office/Home Office) 所需環境歸納如下：(大企業網站則須另行考量)

1. **關閉 Selinux**：Security Enhanced Linux (SELinux) 係針對帳戶登入後使用資源的管制。目前 CentOS Linux 大多使用於 Client/Server 架構，甚至禁止帳戶登入系統，僅允許透過網路存取，因此甚少使用到此功能而將它關閉。(**請參考 2-6-5 節操作方法**)

2. **啟動 Firewalld**：防火牆是網路伺服器最重要的防護系統之一，一定要將它開啟。(**請參考 6-6 節操作方法**)

3. **YUM/DNF** 線上安裝工具：有了 yum/dnf 工具之後，擴充軟體方便許多了，它會自動到 CentOS mirror 網站上搜尋及下載所要的軟體套件，不需要去找套件在哪裡。(**請參考 8-5-3/4 節操作方法**)

9-1-2 網路伺服器架構

基本上，網路服務系統都是屬於『主從式架構』(Client/Server Achitecture)，包含伺服端與客戶端兩種角色。客戶端(Client)扮演著主動式角色，主動向伺服端(Sever)提出要求服務的需求；至於伺服端則扮演被動角色為主，隨時等待客戶端提出服務要求。所以一個網路應用系統必定包含兩個專屬程式，一者為安裝於伺服端的網路伺服器(Network Server)，另一者為安裝於客戶端的客戶程式。圖 9-1 顯示較常見的三種網路應用系統，其中網頁伺服系統包含的 httpd（伺服端）與 IE（客戶端）兩程式，它們之間透過某一種標準協議（http）的運作，達成了網頁儲存與瀏覽的任務，另外檔案傳輸系統與遠端登入系統，也是分別透過某一種協定（ftp）的運作，達成檔案傳輸與遠端登入的工作。

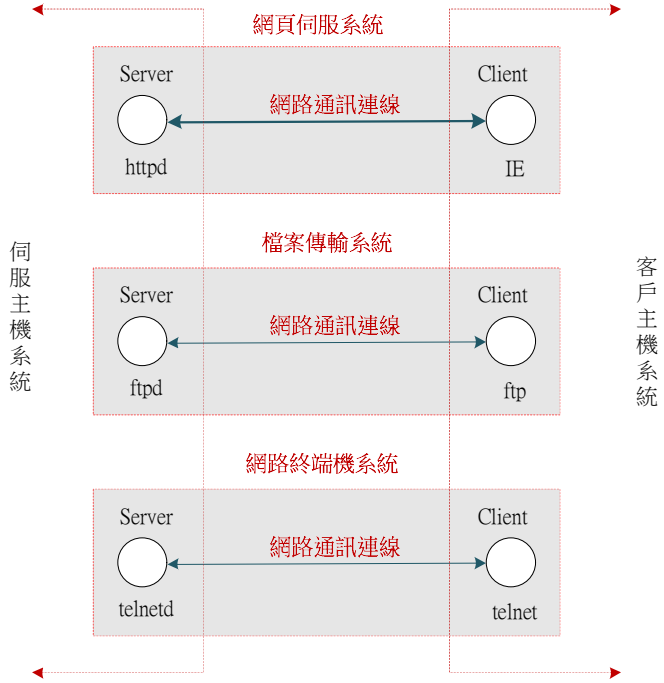


圖 9-1 主從式架構

當然這些網路服務程式都必須安裝於某一系統主機，安裝伺服器的主機，稱為伺服器系統(Server System)，如 Linux 或 Windows Server。安裝客戶程式的主機，則稱為工作站系統(Workstation System)，如 Windows 7、10。但若某一主機同時安裝伺服程式與客戶程式，則該主機可同時扮演雙重角色(伺服端與客戶端)，大部分的 Unix/Linux 與 Windows Server 系統皆是如此。

9-1-3 網路伺服器與 TCP 埠口

網路伺服器即是透過網路提供服務，客戶端也需透過網路索取服務。一部主機系統上大多允許提供多個網路服務，但它只有一個 IP 位址，如何產生多個服務的功能呢？即是透過 TCP 埠口(TCP Port) 的多工功能，如圖 9-2 所示。TCP 埠口就好像公司行號電話分機號碼的功能，公司的代表電號號碼就如同 IP 位址一般。網路服務就如同打專屬電話到公司後再轉接分支號碼一樣，亦是 IP 連結到主機後，再連結 TCP 埠口到相關伺服器上。

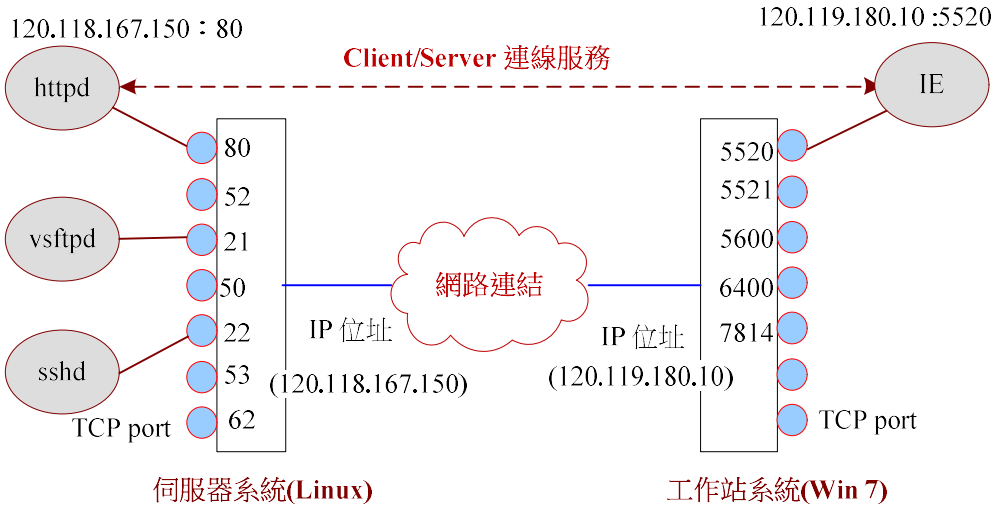


圖 9-2 伺服器與 TCP 埠口

主機(伺服器系統或工作站系統)的 TCP 埠口有 0～65535，哪一部伺服器連結到哪一個埠口上，這有標準規範。譬如 http 連結到 80 埠口、ftp 連結到 21 埠口、ssh 是 22 埠口，規範內 0～1023 是系統指定使用，1024～65535 可以讓使用者任意使用。埠口與系統服務之間對應關係，登錄於 /etc/services 檔案內，如下：(執行 **#cat /etc/services** 結果，擷取部分)

```
....
# service-name    port/protocol    [aliases ...]     [# comment]

tcpmux              1/tcp                                  # TCP port service multiplexer
tcpmux              1/udp                                  # TCP port service multiplexer
rje                 5/tcp                                  # Remote Job Entry
rje                 5/udp                                  # Remote Job Entry
echo                7/tcp
echo                7/udp
discard             9/tcp               sink null
discard             9/udp               sink null
systat              11/tcp              users
systat              11/udp              users
daytime             13/tcp
daytime             13/udp
....
```

以圖 9-2 為例，伺服器架設於 120.118.167.150:80 埠口上，前者為 IP 位址，後者為 TCP 埠口。工作站上的 IE 連結於 120.119.180.10:5520 埠口上。但一般 http 埠口都是 80，沒有特殊的話，自動會連結到 80 埠口。

9-1-4 TCP 埠口與防火牆

其實 TCP 埠口僅是一個虛擬代號，此代號的範圍是 0～65535 之間，但它是網路訊息進出的通路。任何程式產生一個不與其它服務的代號，就可以用來進出系統，這也是網路安全上很大的漏洞。一般系統對於 TCP 埠口的使用有所管制，此設施即為防火牆。防火牆管制訊息是否允許進出主機系統，但為了安全起見，一般都採用從嚴措施(Deny)，即是，預定是任何埠口皆部允許封包進入，當管理者開放了哪個埠口，那個埠口才允許封包進出。簡單來講，您安裝伺服器之後，沒有開啟該伺服器所連結的埠口，該伺服器是無法使用的。

吾人建議開啟防火牆功能，再依照企業網站需求開啟某些埠口，命令範例如下：

```
# systemctl  status|stop|start|restart|enable  firewalld.service
```

啟動防火牆操作如下：

```
[root@secureLab ~]# systemctl start firewalld    [啟動防火牆功能]
[root@secureLab ~]# systemctl enable firewalld     [開機時自動啟動防火牆]
[root@secureLab ~]# systemctl status firewalld      [顯示防火牆狀態]
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled;>
   Active: active (running) since Fri 2021-05-14 21:52:50 CST; 13h ago
     Docs: man:firewalld(1)
 Main PID: 33370 (firewalld)
    Tasks: 2 (limit: 11332)
   Memory: 24.3M
   CGroup: /system.slice/firewalld.service
           └─33370 /usr/libexec/platform-python -s /usr/sbin/firewalld>
Docs: man:firewalld(1)
....
```

開啟防火牆的服務部口命令如下：(以 httpd 80/tcp/udp 為例)

```
[root@secureLab ~]# firewall-cmd --add-port=80/tcp –permanent [開啟 80/tcp]
Success
[root@secureLab ~]# firewall-cmd --add-port=80/udp –permanent [開啟 80/udp]
success
[root@secureLab ~]# firewall-cmd –reload      [重新導入]
success
[root@secureLab ~]# firewall-cmd --list-all –permanent [查詢目前已開啟埠口]
public
  target: default
  icmp-block-inversion: no
```

```
  interfaces:
  sources:
  services: cockpit dhcpv6-client ssh
  ports: 80/tcp 80/udp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@secureLab ~]
```

9-2 終端機伺服器 – sshd

許多系統為了安全性考量，安裝系統時大多不會自動安裝網路終端機程式，待需要時再另外安裝也不遲。本書以 Telnet 與 SSH 伺服器作為範例，說明網路終端機的基本原理與安裝技巧。

9-7-1 網路終端機簡介

【A. 何謂終端機？】

在『多人/多工』(Multi-user/Multi-task) 系統下，一般使用者必須透過終端機連線，才可以使用到系統的資源，它的架構如圖 9-3 所示。主機電腦利用串列 (Series)『多工器』(Multiplexer) 的連線和終端機銜接，其連線方式依照各家廠商製作而有所不同，但大部份都是以 RS-232C 連線方式。一般來講，一部主機可連接數十部到數百部的終端機，它的連線架構如圖 9-3 (a) 所示。經過連線之後，使用者由終端機鍵盤輸入各種命令給主機，主機處理後再將結果顯示在終端機螢幕上。基本上，終端機只負責使用者和主機電腦之間的交談 (Interactive) 工作，並不負責其它相關資料的處理。圖 9-3 (b) 為一般 Unix/Linux 連線啟動程序，主機啟動後 (執行 Run Level 3)，便執行 gettty 程式來掃描監視多工器上是否提出連線要求，如有連線進來再啟動使用者 Shell Script，來處理使用者的登入工作 (Login Script)。使用者在終端機所下的命令，就宛如在主機的主控台所下命令一樣，所執行的命令也是在自己的 Login Script 下所產生的。

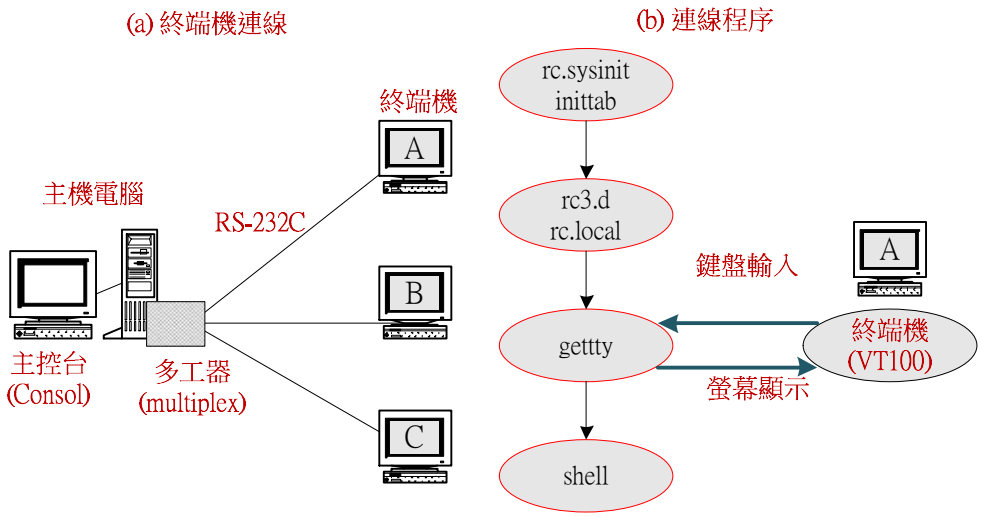


圖 9-3 終端機連線與處理程序

【B. 何謂網路終端機？】

主機和終端機之間採用固定連線（如 RS-232C），將某一終端機固定於特定主機上，如果希望再成為另一部主機的終端機，則必須再另外佈放一條連線到其它主機。隨著個人電腦愈來愈便宜，我們不希望再製作沒有處理計算能力的終端機，而希望能以有處理能力的個人電腦來取代終端機設備，因此漸漸地有終端機模擬程式的出現。簡單的說，我們可以依照連線需求將個人電腦模擬成各式各樣的終端機（如 IBM 3270、VT 100、VT220 等等），來連接不同主機系統。又早期模擬終端機的電腦與主機之間還是採用類似 RS-232C 的連線方法，而隨著網路應用的蓬勃發展，佈放網路連線愈來愈普遍，固定連線的 RS-232C 也漸漸由網路連線來取代，『網路終端機』(Network Terminal) 的雛形就因而成型，其連線架構如圖 9-4 所示。

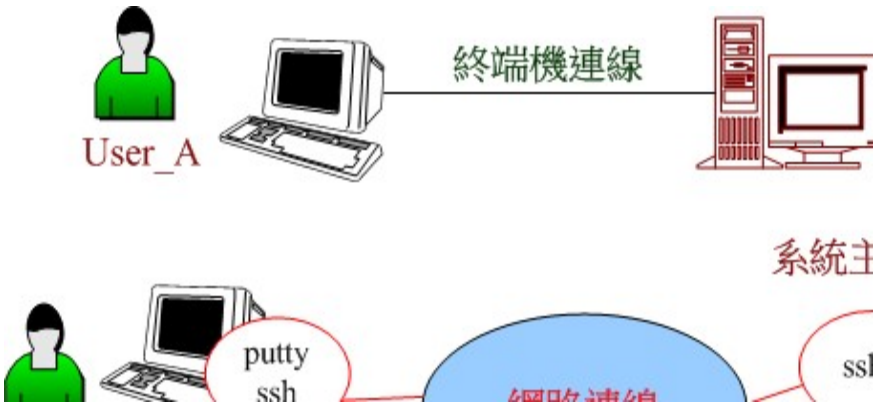


圖 9-4 網路終端機連線

圖 9-4 為網路終端機連線方式，客戶端電腦上執行終端機模擬程式（如 Putty 等），將電腦模擬成所需要的終端機型態（如 IBM 3270、VT100、VT220 等），再透過網路通訊協定

（如 Telnet 或 SSH 等等）和主機連線。此時就將客戶端電腦模擬成終端機，由客戶端鍵盤輸入各種命令給主機電腦，主機電腦執行後再將結果顯示在客戶端電腦的螢幕上。。

從另一個角度來看，我們只要知道對方主機的 IP 位址，以及帳戶名稱及密碼，就可以透過網路登入該主機，並由鍵盤輸入各種命令請求主機執行。如此一來，網路終端機將可能成為一套非常危險的系統，有心人士只要偷竊到帳號密碼（尤其是系統管理者密碼）。因此，大多使用 Putty 內的 SSH 連線，功能是連線之前終端機會與主機電腦協議出一支秘密鑰匙，通訊時就利用這支鑰匙來加密，傳輸中的密碼與訊息就比較不容易被盜取。

9-2-2 終端機伺服器安裝 - openssh

(A) 查閱 sshd 是否以啟動

操作如下：(一般安裝系統時，都會自動安裝)

```
[root@tsnien ~]# systemctl | grep sshd
  sshd.service              loaded active running     OpenSSH server daemon
[root@tsnien ~]# systemctl is-active sshd
active
```

(B) 安裝 openssh 套件

目前 sshd 使用最普遍的是 Openssh，如果系統沒有安裝的話，安裝操作如下：

```
[root@tsnien ~]# yum -y install openssh
Loaded plugins: fastestmirror, langpacks
base                                                    | 3.6 kB    00:00:00
extras                                                  | 3.4 kB    00:00:00
updates                                                 | 3.4 kB    00:00:00
Loading mirror speeds from cached hostfile
 * base: ftp.tc.edu.tw
 * extras: ftp.tc.edu.tw
 * updates: ftp.tc.edu.tw
…
```

(C) 啟動 sshd 服務

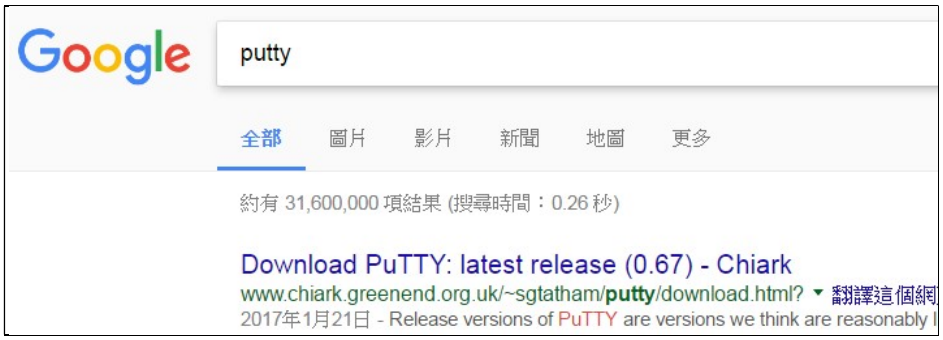
操作如下：(# systemctl start sshd)

```
[root@tsnien ~]# systemctl start sshd
[root@tsnien ~]# systemctl enable sshd [開機時自動啟動]
```

9-2-3 Putty 連線

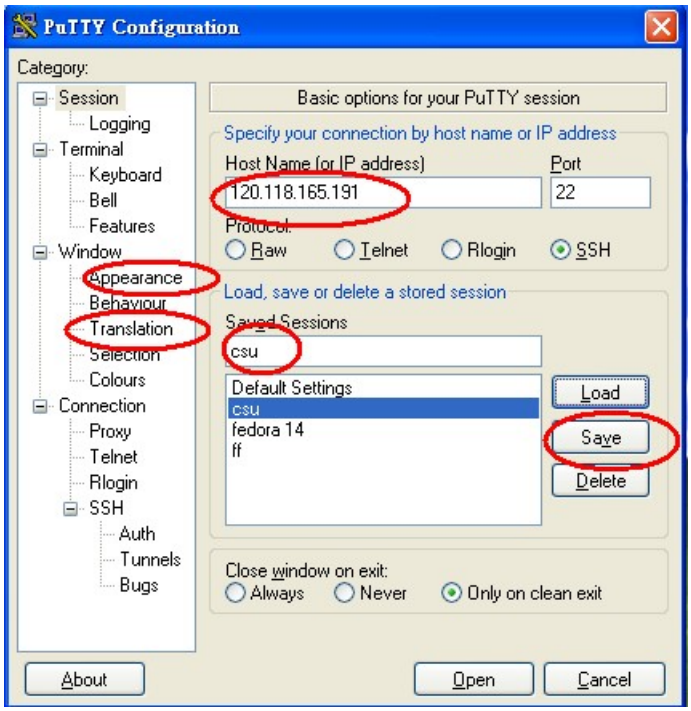
(A) 下載 Putty 軟體

利用 Goggle 搜尋下載，並不需要安裝，直接執行即可，如下：



執行後，請先設定如下：

- Appearance：設定字型 (Chinese Big-5)
- Translation：UTF-8



(B) 登入系統

設定好 Putty 參數之後，即可連線登入系統。輸入帳號名稱與密碼，但為了保護密碼不外洩，輸入時並不會顯示，如下：

9-3 檔案傳輸伺服器 - vsftpd

9-3-1 FTP 簡介

『檔案傳輸協定』(File Transfer Protocol, FTP) 主要應用於異質性電腦之間，檔案相互傳輸使用。各類型電腦的檔案儲存格式，多半不會相同，所以檔案如果沒有經過特殊處理，異質電腦之間的檔案將很困難相互共享。而共享的機制必須透過裝置將共享檔案以某一種標準格式儲存 (ASCII 或 Image 格式)，再利用某一種專屬協定 (FTP 協定) 讓共享檔案可以在不同電腦之間流通，此設備即是 FTP 系統。在 FTP 系統上，客戶端可透過網路由 FTP 伺服器下載或上傳檔案。上傳檔案時，FTP 伺服器會使用某一種標準格式儲存；下載時，檔案儲存到目的主機時，也會轉換成該主機的檔案格式，如圖 9-6 所示。

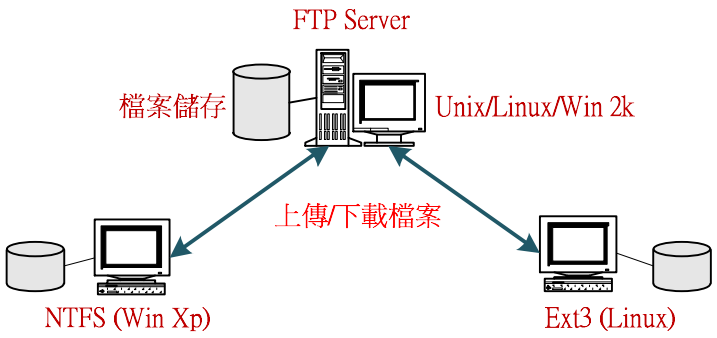


圖 9-7 FTP 系統架構

標準 Unix/Linux 版本上的 FTP 伺服器，使用者都必須具有系統帳戶名稱及密碼才可以登入。但目前 Internet 網路上共享資源愈來愈多，而且都是無條件讓使用者下載使用，如需要帳戶名稱及密碼的話，將會嚴重限制使用者的方便性，因此，就有『匿名 FTP』(Anonymous FTP) 的產生。在匿名 FTP 之下，使用者以 anonymous 為使用者名稱，再以電子郵遞帳號作為密碼便可登入，來從事檔案傳輸的工作，除非特殊網站，否則一般伺服器並不會真正去偵測帳號的真實性，只判斷是否有『@』便決定允許登入與否。許多廠商會將一般共享軟體或產品更新程式放置於匿名 FTP 網站，供客戶自由下載。

目前許多知名的 FTP 網站都使用 vsftpd (very secure FTP daemon) 套件，相對的，許

多 Linux Distributuion 也都將該套件列入所發行 Linux 系統的標準配備中。本書就以此套件來說明 FTP 伺服器的安裝與管理。

9-3-2 FTP 伺服器安裝

(A) 查詢 vsftpd 服務

查詢 vsftpd 服務是否以安裝，操作如下：

```
[root@tsnien ~]# rpm -qa | grep vsftpd
[root@tsnien ~]#                                    [沒訊息表示沒有安裝]
```

上述結果表示系統還未安裝 vsftpd 套件。

(B) 安裝 vsftpd 伺服器

只要網路設定正常，yum 可以線上直接安裝，操作方法如下：

```
[root@tsnien ~]# yum -y install vsftpd
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: ftp.tc.edu.tw
 * extras: ftp.tc.edu.tw
 * updates: ftp.tc.edu.tw
…

Complete!
```

安裝完成之後，可再查詢 vsftpd 是否，如下：

```
[root@tsnien ~]# rpm -qa |grep vsftpd   [查詢套件是否已安裝]
vsftpd-3.0.2-21.el7.x86_64                    [套件已安裝]
[root@tsnien ~]# systemctl | grep vsftpd    [雖已安裝，但還未被導入執行]
[root@tsnien ~]# systemctl start vsftpd      [啟動 vsftpd 套件]
[root@tsnien ~]# systemctl | grep vsftpd      [查詢 vsftpd 服務]
 vsftpd.service   loaded active running    Vsftpd ftp daemon   [vsftpd 執行中]
[root@secureLab ~]# systemctl enable vsftpd     [開機時啟動 vsftpd 服務]
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service →
/usr/lib/systemd/system/vsftpd.service.
```

```
[root@secureLab ~]# systemctl is-enable vsftpd      [查詢開機時是否啟動]
Unknown operation is-enable.
[root@secureLab ~]#
```

(C) 安裝客戶端工具

一般伺服器主機也允許當作 FTP 客戶端操作，因此，也需安裝 FTP 工具，操作如下：

```
[root@tsnien ~]# yum   -y   install   ftp
Loaded plugins: fastestmirror, langpacks
…
Installed:
   ftp.x86_64 0:0.17-67.el7
Complete!
```

(D) 組態設定

vsftpd 套件係利用 /etc/vsftpd/vsftpd.conf 設定檔來規劃其運作環境，主要的設定項目是：(1) 是否允許匿名登入(除 FTP 操作者外，不允許上傳檔案)、(2) 是否允許建立個人 FTP 網站、與(3) 個人 FTP 網站是否允許上傳檔案 (**內定值都是允許的，大多不需要修改**)。

操作命令：# **vi /etc/vsftpd/vsftpd.conf** (利用 vi 編輯，僅列出部分檔案)

```
Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
……
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES                          【將 # 號刪除允許匿名登入】
#
# Uncomment this to allow local users to log in.
local_enable=YES                              【允許建立個人網站】
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES                              【允許個人網站上傳檔案】
……
```

(E) 設定匿名 FTP 網站

匿名 FTP(Anonymous FTP)網站也是需要適當的限制，譬如是否允許使用者上傳檔案，或建立新目錄，都是由 **/etc/vsftpd/vsftpd.conf** 檔案設定，設定範例如下：(內定值大多是不允許的，僅列出部分檔案)

```
……
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES                    【前面是 # 號表示沒有開放】
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES               【前面是 # 號表示沒有開放】
……
```

另外，匿名網站所儲存的位置是在 **/var/ftp/pub** 目錄下， FTP 管理者或該目錄擁有者可上傳檔案供匿名使用者下載。

(F) 開啟防火牆 - ftp 埠口

開啟防火牆的 ftp 埠口，如下：

```
[root@localhost ~]# firewall-cmd --add-service=ftp --permanent
success
[root@localhost ~]# firewall-cmd --reload
success
```

(G) 重新啟動 vsftpd

更改組態檔案後，須重新啟動才有效，如下：

```
[root@tsnien ~]# systemctl   restart   vsftpd          [重新啟動 vsftpd]
```

(I) FTP 使用者管理

在 /etc/vsftpd/ 目錄下，有兩個管理 FTP 使用者的設定檔，如下：

- ✧ **ftpusers**：此檔案所記錄的帳戶名稱，將不允許登入 FTP 伺服器。
- ✧ **user_list**：如果系統變數 userlist_deny=no，表示允許此檔案內所記錄的帳戶可以登入 FTP 伺服器；相反的 userlist_deny=yes (內定值)，則表示不允許登入。

所謂允許登入 FTP 的意思是允許該帳戶名稱建立個人 FTP 網站，不允許登入，則不允許建立個人網站。譬如設定 root 可以使用 ftp 服務，如下：(# **vi /etc/vsftpd/ftpusers**) 或 (# **vi /etc/vsftpd/user_list**)

```
# Users that are not allowed to login via ftp
# root      [前面加 # 號表示沒有限制 root 帳戶]
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
```

9-3-3 Windows 客戶端操作

vsftpd 服務啟動後，每一個使用者的家目錄(Home directory)，即是該使用者的個人 FTP 網站位置。登入時，必須輸入使用者名稱與密碼；以 student01 使用者為例，其家目錄為 /home/student01，客戶端可利用下列兩種方法上傳或下載檔案。

(A) FileZilla Client 操作

目前免費 FTP 傳輸工具以 FileZilla 最為普遍使用，可利用 Google 搜尋並下載安裝，如下：

安裝後，即可啟動上傳或下載檔案：

(B) FTP 命令操作

在 Windows 工作站或 Unix/Linix 系統上，命令登入如下：

```
D:\>ftp                                    [鍵入 ftp 命令]
ftp> open 120.119.165.113                  [鍵入 open IP 位址]

Connected to 120.119.165.113.
220 (vsFTPd 2.3.4)
User (120.119.165.113:(none)): tsnien      [鍵入使用者名稱]
331 Please specify the password.
Password:********
230 Login successful.
ftp> ls                                    [鍵入 shell 命令]
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
Backup2013_04_15
…
ftp> pwd                                   [鍵入 pwd 命令]
257 "/home/tsnien"
257 "/home/tsnien"
ftp>
```

其中『?』命令是 Help 的功能，它會顯示出所有 FTP 命令，我們大略由上列命令名稱來知道它的功能為何，但是我們還是將較常用的命令條列如表 9-1。

表 9-1 常用的 FTP 命令

命令名稱	功 能 說 明
?	顯示命令（help）。
!	執行本機命令，如 !ls 表示執行本機上的 ls 命令。

ascii	設定 ASCII 模式傳輸，使用於文字檔案傳輸。
binary	設定二進位模式傳輸，一般使用於執行檔或影像檔傳輸。
bye	結束 FTP 連線。
cd	切換伺服器的工作目錄。
close	關閉 FTP 連線。
debug	進入偵錯模式。
delete	刪除遠端伺服器檔案。
dir	顯示遠端伺服器工作目錄下的檔案和目錄清單。
get	下載一個檔案
mdelete	刪除多個遠端檔案。
mget	下載多個檔案。
mkdir	在遠端伺服器建立目錄。
mput	上傳多個檔案到遠端伺服器。
open	開啟 FTP 連線。
put	上傳一個檔案到遠端伺服器。
pwd	顯示目前遠端伺服器的工作目錄。
rmdir	刪除遠端伺服器的目錄。
status	顯示目前連線狀態。
type	設定檔案傳輸模式。
user	登入 FTP 伺服器使用者名稱 (如 user tsnien)。

9-3-4 匿名 FTP 管理

匿名 FTP (Anonymous FTP) 允許使用者以 Anonymous 帳號登入，密碼僅有 "@" 記號的 E-mail 帳號即可(系統不會檢查真偽)。應用於公用檔案讓一般用戶下載，客戶端不需要在系統上建立帳號即可下載檔案，但吾人大多會限制其被上傳檔案的功能(如 9-2-3 敘述)。Anonymous FTP 公用檔案儲存於 /var/ftp/pub 目錄下，需具有 root 權限才可以上傳檔案，但 vsftpd 安裝後，自動限制 root 登入 FTP 功能，因此，需編輯 /etc/vsftpd/ftpusers 與 /etc/vsftpd/user_list 兩檔案。

(A) 開啟 root FTP 登入

編輯 /etc/vsftpd/ftpusers 與 /etc/vsftpd/user_list 兩檔案，以 **# vi /etc/vsftp/ftpusers** 為例，如下：

```
# Users that are not allowed to login via ftp
# root      (前面加入 # 號)
bin
daemon
adm
lp
sync
.....
```

(B) 上傳公用檔案 - root

開啟 FilleZilla 後，以 root 帳號登入，並上傳一個檔案到 /var/ftp/pub 目錄下。

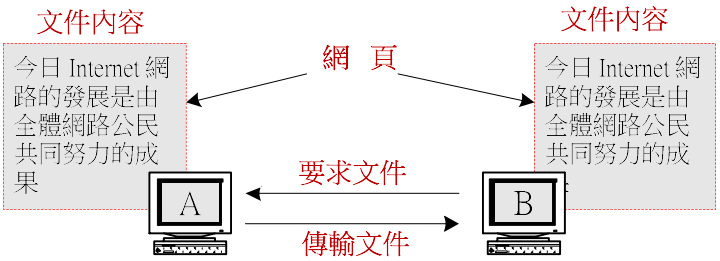
(C) Chrome 瀏覽器下載 - Windows

客戶端可利用瀏覽器直接下載公用檔案，如下：(**ftp://192.168.1.107**)

9-4 網頁伺服器 - httpd

9-4-1 全球資訊網系統

早期發展 Web 系統時，並沒有想到會有這麼大的發展空間，那時候只考慮到如何將文件可以在各種系統之間流通。因為當時各系統之間的文件格式並不相容（現在也一樣），譬如，在 Apple、Windows、Unix、或其它系統所製作的文件，並無法直接在另一系統上顯示或修改處理。當時只希望建立一套系統，方便顯示不同系統之間的文字，其基本構想就是建立一套顯示平台，並可以安裝於各種不同的系統上。另外，由於作業系統之間的檔案結構也不盡相同，無法將一個系統所製作的文件儲存於磁碟片，再由另一系統將它讀出來，因此，共通平台的文件必須利用網路以 ASCII 格式互相傳輸。上述構想就是網頁系統的基本原理就，如由電腦 A 所製作出來的文件，能夠透過網路傳輸給電腦 B，並可在電腦 B 能如身歷其境般的顯示出來。

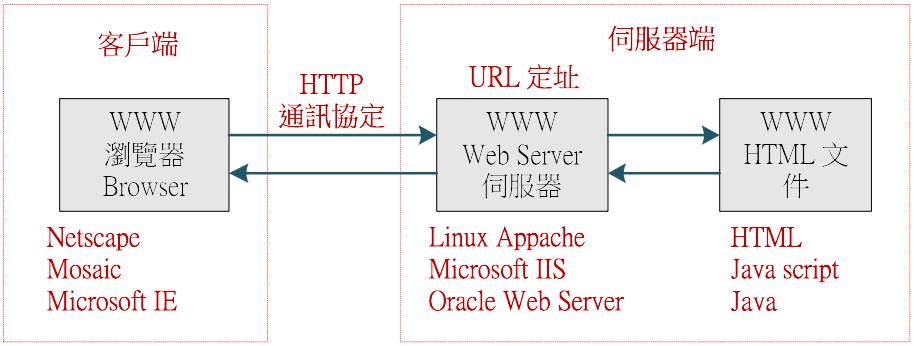


所謂示共通平台即是目前所稱的『瀏覽器』，而電腦之間就以 HTTP 協定來互相通訊。文件在瀏覽器上以一頁一頁為單位來顯示，所以瀏覽器上顯示的文件就稱為『網頁』（Web Page），又每一文件都有封面，其封面則稱為『首頁』（Home Page），而將提供網頁供瀏覽器下載的伺服器就稱為『網頁伺服器』（Web Server）。至於文件要如何製作才能在瀏覽器上

顯示出來？於是就制定了 HTML 標準，希望所有文件都能依此標準來製作，才能在不同系統上的瀏覽器顯示，網頁系統就是這麼簡單的概念之下產生。早期網頁只能顯示文字模式（如 Mosaic），萬萬沒想到數位訊號處理的技術，如火速般的發展，兩者一拍即合，很快地將影像及聲音的數位處理技術嵌入瀏覽器之中，多采多姿的全球資訊網世界就因此而誕生了。

(A) Web 系統架構

下圖為 Web 系統架構，是屬於主從式架構，伺服端（Web Server）提供資源（HTML 文件）供客戶端（瀏覽器）下載，它們之間是以 HTTP 通訊協定來傳輸。伺服端使用 URL 的定址方式，客戶端可以依照 URL 位址找到所要的網站，所以 URL 又稱為『網址』。



(B) 瀏覽器

客戶端就是瀏覽器(如 IE 或 Netscape)，它的功能是由伺服端上接收 HTML 程式後，再將其執行並顯示成文件，此文件型態就稱為網頁（Web Page）。所以，客戶端以顯示大量文件（或網頁）為主要工作。每一網頁上的文字或圖樣可以指向其它的相關頁來連結，頁和頁之間的連結可以無止境的延伸，此連結方法就稱為『超連結文件』（HyperText）。不僅可以連結網頁，還可以在網頁上任何文字或圖樣設定連結到其它網站，稱之為『超連結』（Hyperlink）。因此，客戶端就可以行走全世界任何一個網站，觀看網站上所有的網頁，所以稱為『瀏覽器』（Browser）。

(C) 一致性資源定址

基本上，瀏覽器可以接受多種協定的傳輸，也可以處理不同語言所編寫的程式，但它如何判斷應以何種模式來工作，這必須由使用者命令它處理。然而使用者又應以何種模式和瀏覽器溝通？這就是『一致性資源定址』（Uniform Resource Locators, URL）的制定目的。URL

包含以下三項資訊：(a) 連接該網站使用何種通訊協定（http 或 ftp）；(b) 網站位址在哪裡（主機的 DNS 名稱）；(c) 該網頁的檔案名稱（或檔案格式），例如：

http://www.tsnien.idv.tw/index.html

URL 的三個部分是：通訊協定（http）、主機位址（www.tsnien.idv.tw）、網頁的檔案名稱（index.html）。通訊協定有：http（超連結文件，HTML）、ftp（FTP 檔案傳輸協定）、file（本地檔案）、news（新聞文章）、gopher（Gopher 文件協定）、mailto（傳送郵件協定）。檔案名稱的副檔名（如，.html）是用來標示，該檔案是由何種程式語言編寫而成，以啟動相對應的直譯程式（如，HTML 直譯程式）。

(D) 網頁伺服器

『網頁伺服器』(Web Server) 是用來儲存 HTML 文件，讓瀏覽器下載執行的伺服器。它和客戶端之間是以 HTTP 通訊協定溝通，又稱為『HTTP 伺服器』(HTTP Server)，傳輸埠口大多架設在 80/tcp 位置。網頁伺服器是目前最炙手可熱的設備，它也是一套非常複雜的系統。隨著網站需求的大量增加，一部網頁伺服器只能架設一個網站已漸不符所需了，我們希望在同一部網頁伺服器上建構更多的網站，才能符合經濟價值。因此，它必須透過虛擬主機技術，來建構許多虛擬網站，乃至個人網站。

9-4-2 網頁伺服器安裝 - Apache

Apache 幾乎與全球資訊網 (World Wide Web, WWW) 劃上等號，也就是說，大部分的商業站都使用 Apache 網站伺服器套件。Apache 是由 The Apache Software Foundation (ASF) 所發展出來，也是免費自由軟體，官方網站是 http://www.apache.org；使用者不但可在官方網站上找到並下載最新版本，也可以找到其他系統上的 Apache 版本，如 Windows 版本。

(A) 套件查詢與安裝

Web Server 服務名稱為 httpd，可利用 # rpm –qa | grep httpd 命令查閱該套件是否已安裝，操作如下：

```
[root@tsnien ~]# rpm   -qa   | grep httpd
[root@tsnien ~]#
```

如果已安裝完成則會顯示所安裝套件的名稱與版本，如沒有安裝的話，可利用 # yum install httpd

命令來安裝，如下：

```
[root@tsnien ~]# yum -y install httpd [安裝 httpd 套件]
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: ftp.tc.edu.tw
 * extras: ftp.tc.edu.tw
 * updates: ftp.tc.edu.tw
....
Complete!
[root@tsnien ~]# rpm -qa |grep httpd [查詢 httpd 套件]
httpd-tools-2.4.6-45.el7.centos.x86_64
httpd-2.4.6-45.el7.centos.x86_64
[root@secureLab ~]# systemctl start httpd [啟動 httpd 服務]
[root@secureLab ~]# systemctl status httpd [查詢 httpd 服務狀態]
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor pres>
   Active: active (running) since Tue 2021-05-18 22:10:19 CST; 9s ago
     Docs: man:httpd.service(8)
 Main PID: 4982 (httpd)
....
[root@secureLab ~]# systemctl enable httpd [開機時自動啟動 httpd ]
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service →
/usr/lib/systemd/system/httpd.service.
```

(B) 組態設定項目

Httpd Server 組態管理檔案全部儲存於 /etc/httpd/ 目錄下，主要設定檔是 /etc/httpd/conf 檔，其中包含下列三個區段（Section 1 ~ Section 3）所組成：

- ✧ **全域環境設定(Global Environment):** 針對整個網頁伺服器的環境設定，譬如 ServerType、ServerRoot.....等等。
- ✧ **'主'伺服器設定（'Main' server configuration）:** 針對 Apache 預設（或主要）伺服器的環境設定，譬如 Port、User/Group、ServerName、DocumentRoot、UserDir.....等等。
- ✧ **虛擬主機設定(Virtual Hosts):** 除了允許預設伺服器存在外，也可以增加其他虛擬主機，可設定成 NameVirtualHost 或 VirtualHost 兩種虛擬主機模式。

除非有特殊變更或設定虛擬主機外，其他都採用預設值即可，讀者可以自行瀏覽看看。

(C) 設定主網站

可以由 /etc/httpd/conf/httpd.conf 設定檔指定預設網站的網頁文件之儲存位置，其變數項目為 DocumentRoot，預設位置是 /var/www/html 目錄，如下：(執行 **# vi /etc/httpd/conf/httpd.conf** 進入修改)

(1) 選用預定埠口 80

```
95 #
96 # If your host doesn't have a registered DNS name, enter
   here.
97 #
98 ServerName www.example.com:80      (移除 # 表示選定)
99
100 #
101 # Deny access to the entirety of your server's filesystem
102 # explicitly permit access to web content directories in
```

(2) 觀察主網頁文件儲存位置 (/var/www/html)，管理者只要將網頁文件上傳到該目錄下，就可以建立主要（Main）網站。

```
118 # DocumentRoot: The directory out of which you will serve
119 # documents. By default, all requests are taken from this
120 # symbolic links and aliases may be used to point to other
121 #
122 DocumentRoot "/var/www/html"
123
124 #
125 # Relax access to content within /var/www.
```

(3) 新增 index 網頁格式 (index.htm，index.php)

```
165 #                                          增加
166 <IfModule dir_module>
167     DirectoryIndex index.html index.php index.htm main.html
168 </IfModule>
169
170 #
171 # The following lines prevent .htaccess and .htpasswd files fro
```

(D) 設定個人網頁網站

系統的 httpd 服務程式啟動後，每一個帳戶（如 user01 帳戶）自動建立一個個人網頁網站，網站名稱為 IP/~login_name（如 http://120.118.165.191/~user01），該帳戶的網頁文件則儲存於家目錄上（/home/user01）。如要建立個人網頁網站，也是必須規劃 /etc/httpd/conf.d/userdir.conf 設定檔，由該檔案中尋找出 mod_userdir.c 設定段落，刪除掉

UserDir disable 功能(增加 # 記號)，並增加 UserDir public_html 選項功能(移除 # 記號)，其中也表示網頁文件是儲存於家目錄的 public_html 子目錄上(如 /home/tsnien/public_html，最好將該目錄權限設定成 $chmod 711 會比較安全)，本書範例如下：(執行 **#vi /etc/httpd/conf.d/userdir.conf** 進入修改)

```
# The path to the end user account `public_html` directory must be
# accessible to the webserver userid.  This usually means that ~userid
# must have permissions of 711, ~userid/public_html must have permissions
# of 755, and documents contained therein must be world-readable.
# Otherwise, the client will only receive a "403 Forbidden" message.
#
<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    # UserDir disabled        加入 # 表示允許建立個人網站

    #
    # To enable requests to /~user/ to serve the user's public_html
    # directory, remove the "UserDir disabled" line above, and uncomment
    # the following line instead:
    #
    UserDir public_html
</IfModule>                   移除 # 表示網站目錄位置
```

除此之外，管理者 (root) 必須將個人網站的家目錄設定成他人都可以讀取與寫入的權限 (輸入 # chmod 777 /home/student01)，操作如下：

```
[root@secureLab ~]# ls -l /home        [觀察目錄權限]
總計 4
drwx------. 15 user01 user01 4096  5 月  18 21:39 user01
drwx------.  3 user02 user02   78  5 月  14 21:13 user02
[root@secureLab ~]# chmod 777 /home/user01      [設定目錄權限]
[root@secureLab ~]# ls -l /home      [觀察目錄權限]
總計 4
drwxrwxrwx. 15 user01 user01 4096  5 月  18 21:39 user01
drwx------.  3 user02 user02   78  5 月  14 21:13 user02
```

(E) 開啟防火牆 - httpd 埠口

開啟防火牆的 ftp 埠口，如下：

```
[root@localhost ~]# firewall-cmd --add-service=http --permanent
success
```

```
[root@localhost ~]# firewall-cmd --reload
success
```

(E) 重新啟動 httpd

設定完之後，必須重新啟動才有效，如下：

```
[root@tsnien ~]# systemctl  restart  httpd
[root@tsnien ~]# systemctl  is-active  httpd
active
[root@tsnien ~]# systemctl  enable  httpd  [開機時自動啟動 httpd]
```

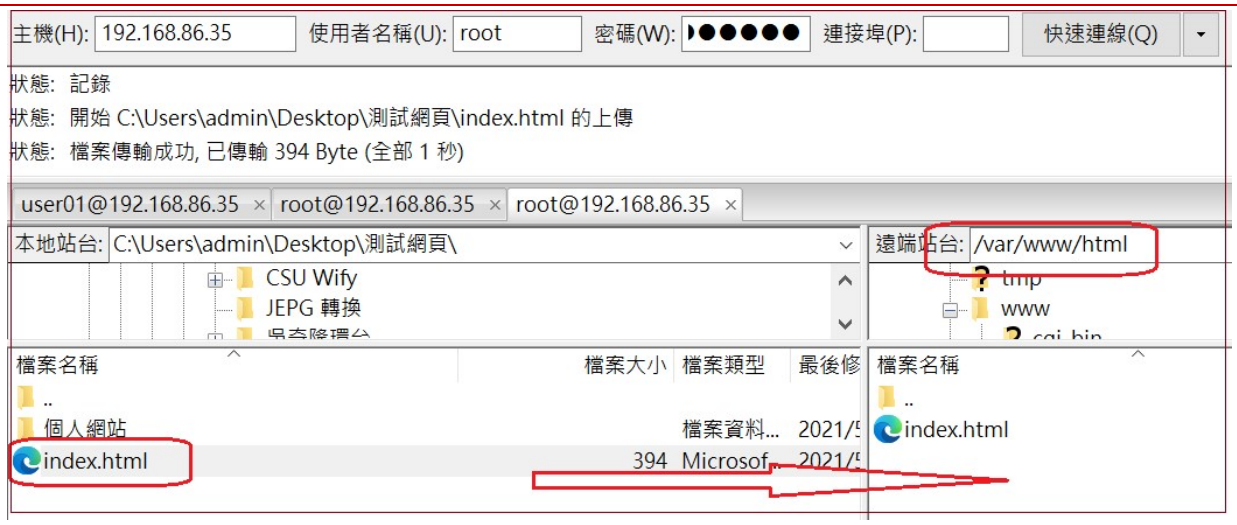
(G) 驗證網站啟動

當 Apache 主網站架設後，可利用瀏覽器驗證網站是否安裝成功，如下：(**http://192.168.86.35**)

9-4-3 上傳主網站網頁 - root

(A) 上傳主網頁 - /var/www/html

Apache 啟動後有兩類網站：主網站 (如 http://192.168.86.35)與個人網站。主網站的網頁儲存於 /var/www/html 目錄下，須由 root 帳戶上傳。吾人利用 root 帳號(須設定允許 **root 登入 FTP**，如：9-3-4 節介紹)上傳一個網頁如下：(請先建立一只 index.html 網頁)



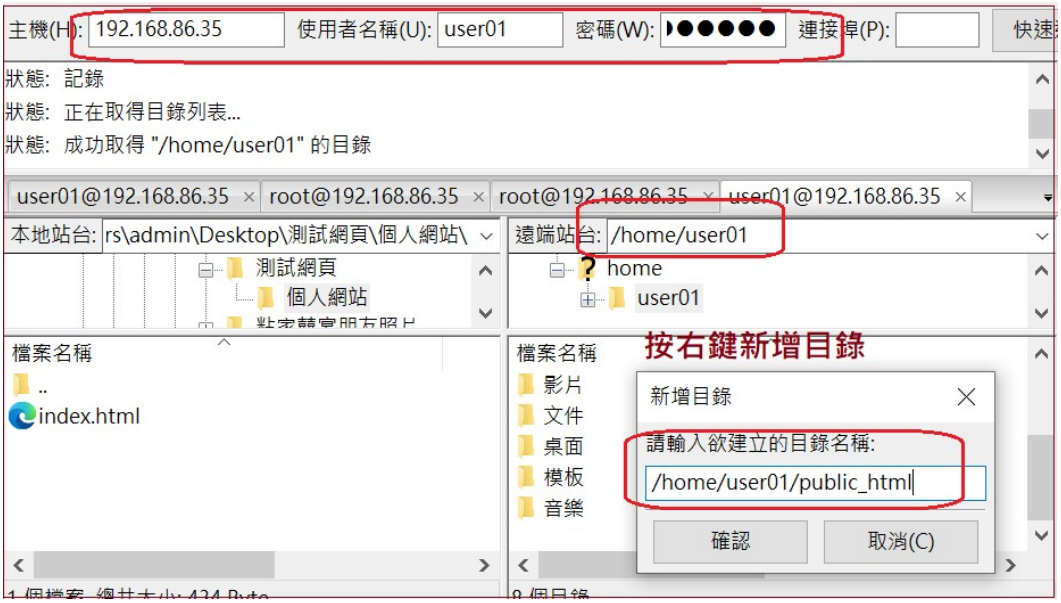
(B) 瀏覽主網頁

瀏覽主網站 (如 http://192.168.86.35) 如下：

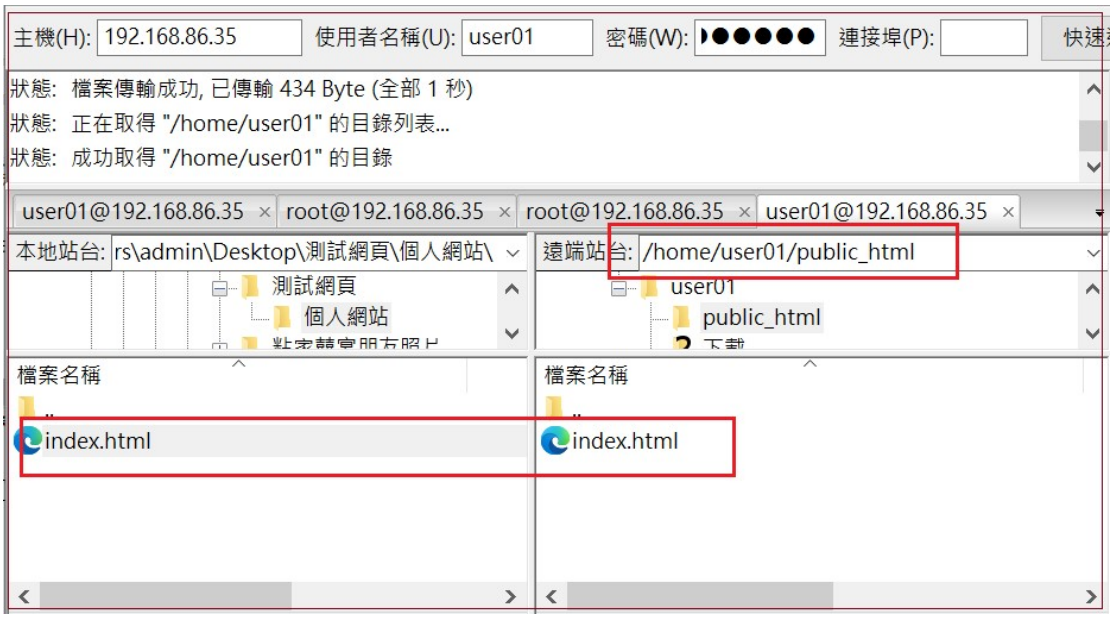
9-4-4 客戶端操作

(A) 上傳個人網站首頁

吾人建立一只個人網站 (http://192.168.86.35/~user01) 的首頁 (index.html) 並上傳該帳戶 (user01) 家目錄的 public_html 目錄下，首先在該帳戶家目錄下建立 public_html 子目錄如下：



再將所建立的首頁 (index.html) 上傳到 public_html 目錄下：



(B) 瀏覽個人網站首頁

瀏覽個人網站(http://120.118.165.191/~user01)，如下：