# 第五章 應用系統協定與分析

## 5-1 網頁伺服系統

### 5-1-1 網頁系統簡介

**『全球資訊網』( World Wide Web, WWW )** 是帶動整個網路發展中最重要系統，已漸漸成為網際網路的代名詞，也就是一般所謂的『網頁伺服系統』(Web Server System)。早期發展網頁系統時，並沒有想到會有這麼大的發展空間，僅考慮到如何將文件可以在各種系統之間流通。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 CERN 只希望建立一套系統，可以共通顯示不同系統之間的文字，它的做法是建構一套平台來顯示文件，而這個平台可以安裝在不同系統之上。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，共通平台的文件必需利用網路以 ASCII 格式來互相傳輸。圖 5-1 為網頁系統的基本原理，其目的是希望建構一個可以共通的顯示平台，例如，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。CERN 的想法是希望各研究單位的成果，利用網路傳輸到其它單位上，而用此共通平台來顯示，以解決不同系統之間，文件格式不相容的問題。

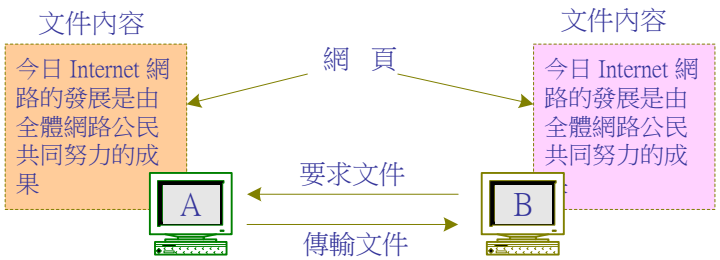



圖 5-1 網頁系統原理

這個共通平台就是目前所稱的**『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，因此，將瀏覽器上顯示的文件稱之為**『網頁』( Web**

**Page )**，又每一文件都有封面，就將文件的封面稱之為**『首頁』( Home Page )**，而將提供網頁讓瀏覽器下載的伺服器稱之為**『網頁伺服器』( Web Server )**。至於文件要如何製作呢？才能在瀏覽器上顯示出來，於是製定了 HTML (HyperText Makeup Language) 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了。因此，早期網頁只能顯示文字模式 ( 如 Mosaic )，真的沒有想到數位訊號處理技術，也正在同時如火如荼的發展中，兩者一觸即發地結合在一起，很快的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。

## 5-1-2 網頁系統架構

WWW 也是主從式架構，伺服器端 ( Web Server ) 提供資源 ( HTML 文件 ) 讓客戶端 ( 瀏覽器 ) 下載，它們之間是以 HTTP 通訊協定來傳輸。伺服器端使用 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』**。我們分別簡述其功能如下：

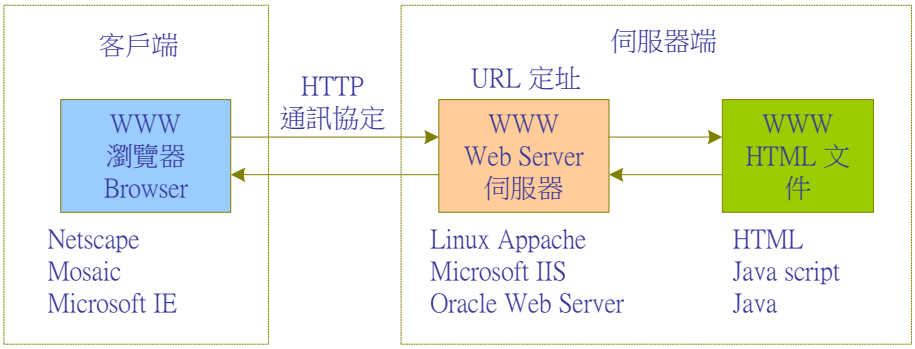



**圖 5-2 全球資訊網簡介**

### (A) HTML

**『超文字標記語言』( HyperText Makeup Language, HTML )** 定義文書處理的文件都有其資料表示方式，譬如：對於某一段文字的大小或粗細體 ( 如 14 號字及粗體 )，會在這一段文字的頭尾加入標記符號。當文件被開啟時，再依照標記符號將文字型態顯示在螢幕上，如圖 5-2-1 所示。

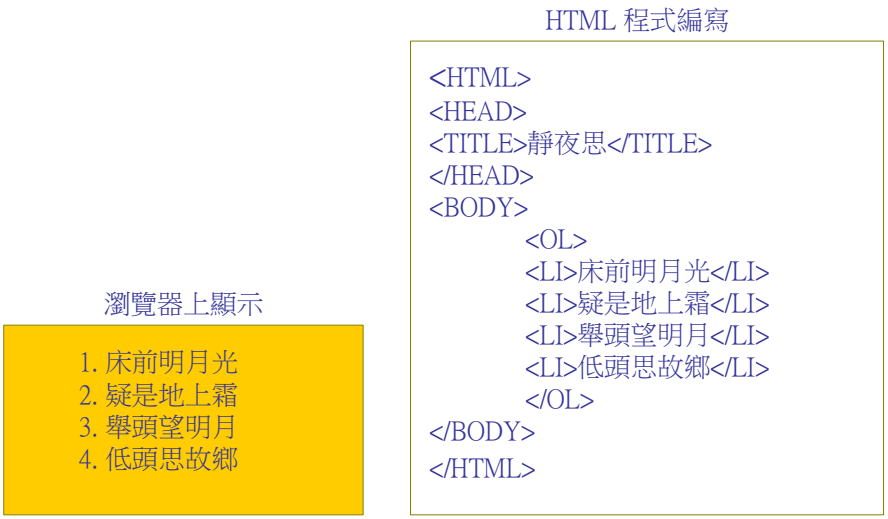



**圖 5-2-1 HTML 文件製作**

常用標記符號如下：

| 標　　記 | 描　　述 |
|---|---|
| <HTML> ….. </HTML> | 宣告網頁將以 HTML 編寫。 |
| <HEAD> …. </HEAD> | 定義網頁的檔頭。 |
| <TITLE> … </TITLE> | 定義標題（並不在網頁上顯示）。 |
| <BODY> … </BODY> | 框註內為網頁主體。 |
| <Hn> … </Hn> | n=1~6，框註內六個階層的標題字大小。 |
| <B> … </B> | 設定框註內文字為粗體。 |
| <I> …. </I> | 設定框註內文字為斜體字。 |
| <UL> … </UL> | 框註內為無序串列（註標式）。 |
| <OL> … </OL> | 框註內為編號串列。 |
| <MENU> … </MENU> | 框註內<LI>項目行成選單。 |
| <LI> | 串列項目的開始（並無 </LI>）。 |
| <BR> | 強迫分離。 |
| <P> | 區段開始。 |
| <HR> | 水平線。 |

| | |
|---|---|
| <PRE> … </PRE> | 已格式化文字。 |
| <IMG SRC= "…"> | 在此載入影像圖形。 |
| <A HREF="…"> … </A> | 定義超連結。 |

## (B) 瀏覽器

客戶端就是瀏覽器( 如 IE 或 Netscape )，它的功能是由伺服器端上接收 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**『超鏈結文件』( 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，在客戶端上可以行走全世界任何一個網站，觀看網站上的網頁，所以稱之為**『瀏覽器』( Browser )**。

基本上，瀏覽器是屬於直譯器( Interpreter )的功能，它由伺服器上下載網頁程式( HTML ) 將其翻譯並執行後，再將結果顯示到螢幕上。另一方面，它也是屬於 HTTP 伺服器的客戶端，負責和 HTTP 伺服器之間的通訊。但隨著瀏覽器應用的方便性，人們期望將不同的網路功能都附加到瀏覽器上，使它具有其它網路系統的功能，譬如，FTP，BBS，Mail 等功能。因此，再將其它網路系統的客戶端功能加到瀏覽器上，如圖 5-3 所示。

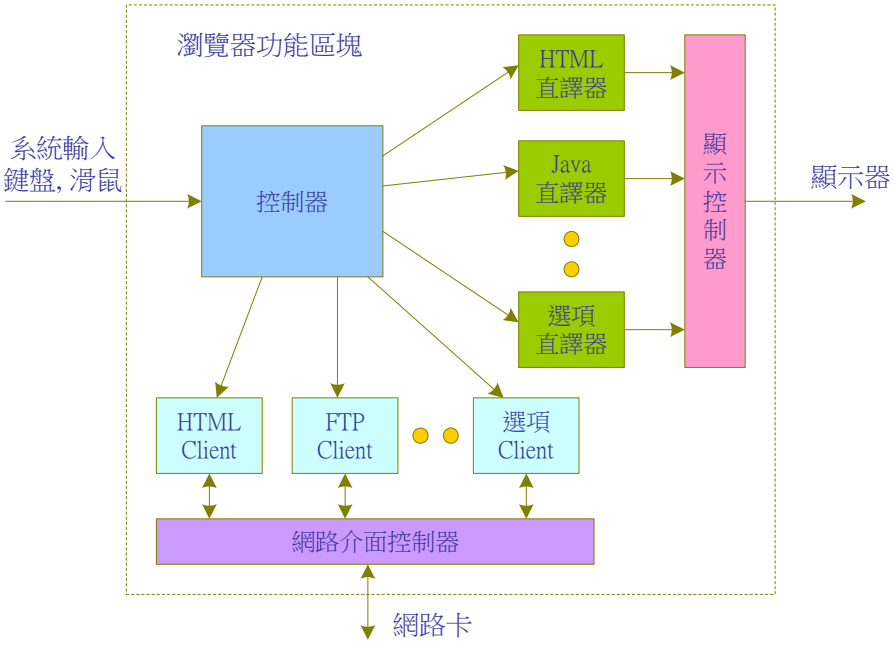



圖 5-3 瀏覽器的功能圖

由圖 5-3 可以發現瀏覽器不再僅是網頁系統的客戶端，也可當作 FTP、Mail、New 等系統的客戶端，甚至可以瀏覽本機上的檔案（File）內容。另一方面，如果僅有 HTML 直譯程式，那麼瀏覽器只能觀賞文字或圖形，如此並不能滿足使用者的需求，我們希望能隨使用者的喜好載入其它程式，來增加瀏覽器的功能。例如，插入 Java 直譯器後，瀏覽器就可以執行 Java 所開發的程式，不但可以整合多媒體（文字、聲音、影像），還可以表現動畫，提高網站的可看性。也就是說，我們可以將各種不同的直譯程式，崁入瀏覽器之中，使它能編譯執行不同的程式語言，來增強瀏覽器的功能。總而言之，瀏覽器不但必須具備有各種通訊協定的功能，也包含各式各樣的直譯程式，因此，可以將瀏覽器視為全球資訊網的工作平台並不為過，也促使瀏覽器成為最複雜的軟體套件，相對的，網路應用系統的最大安全漏洞，也出現在瀏覽器上。

### (C) 一致性資源定址

既然瀏覽器可以接受不同協定的傳輸，也可以處理不同語言所編寫的程式，但它如何判斷該以何種模式來工作，這必須由使用者命令它處理。然而使用者應該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，當使用者以 URL 通知瀏覽器工作時，必須標明以下三項資訊：(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、ftp://tsnien.idv.tw**

### (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。

## 5-1-3 HTTP 傳輸協定

**『超文件傳輸協定』( HyperText Transfer Protocol, HTTP )** 是針對 Web 設計的傳輸協定。目前使用的協定大多是 HTTP/1.0 ( RFC 1945 ) 以上的版本，而在 HTTP/1.1 ( RFC 2068、RFC 2616 ) 版中增加了虛擬主機的功能，相信會有更新版本陸續被發展出來。在 HTTP 協定下，伺服端和客戶端之間是屬於**『要求/回應』**的存取方式。也就是說，客戶端以 ASCII 文字的通訊命令，來要求伺服端執行，伺服端將執行結果以 ASCII 文字方式回應給客戶端，基本上，所有請求命令都由客戶端要求，而伺服端只是被動地接受命令來工作。

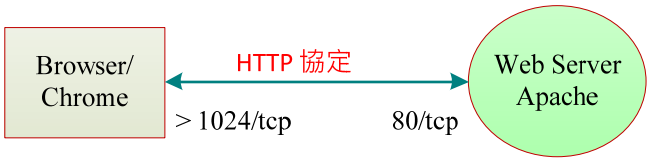



**圖 5-3-1 HTTP 傳輸協定**

## (A) HTTP 常用命令

HTTP 協定常用基本命令如下：

**(1) GET**：請求讀取網頁。瀏覽器以 GET 命令，請求伺服器送出網頁，以 MIME 方式編碼。

**(2) HEAD**：請求讀取網頁的檔頭 ( header )。客戶端僅請求訊息檔頭，而非實際網頁。這方法可取得網頁最後修改時間，可用在建立或測試 URL 的有效性。

**(3) PUT**：請求儲存網頁。客戶端寫入網頁，提供客戶端建立網頁的功能。

**(4) POST**：附加一個名稱資源。客戶端將資料附加到某一資源的資料之後。

**(5) DELETE**：刪除網頁。客戶端要求刪除某一網頁。

**(6) LINK**：建立超連結。客戶端要求加入超連結。

**(7) UNLINK**：刪除超連結。客戶端要求刪除超連結。

HTTP 伺服端也以 3 個數字來回應執行的結果，第一個數字表示回應種類，如下：

- **2××** 表示命令執行成功 ( Success )；

- **3 ××** 為命令執行轉向（Redirection）；
- **4××** 為客戶端錯誤（Client Error）；
- **5××** 為伺服端錯誤（Server Error）。

## 5-1-4 HTTP 協定運作

Http 協定係利用 TCP 封包承載，一般伺服器埠口大多是 80/tcp，包裝格式如圖 5-3-1 所示。

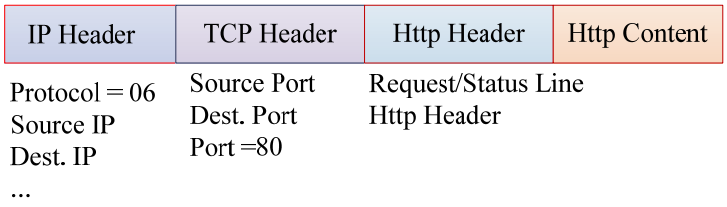



**圖 5-3-2 Http 封包包裝**

HTTP 命令格式並不像其他通訊協定有欄位可以填寫，而直接以文字方式要求、回應，像交談式對話方式，但還是有制定句型格式。Http 協定運作模式如下圖：

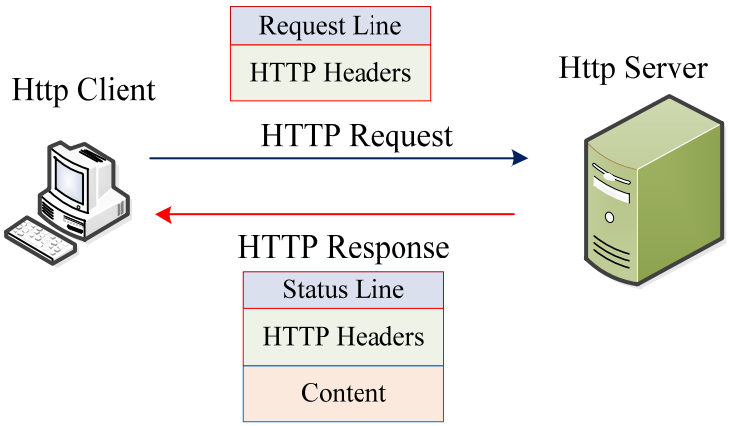



**圖 5-3-3 Http 協定運作模式**

客戶端發送 Http Request 向伺服端請求訊息，伺服端再以 Http Response 回應給客戶端。Http Request 包含 **Request Line** 與 **Http headers** 兩部分，Request Line 即是發送請求命令，包含：**Method (方法)**、**Path (路徑)**、**Protocol (協定)**等三項構成(至多四項)。Http Headers 包含若干個相關參數，每一參數是由： **Name: Value** 格式所構成。以 Get 命令的 Http Request 範例如下：

| GET /image/flag.img HTTP/1.1 **(Request Line)** |
|---|
| Host:tsnien.idv.tw **(Http Header)**<br>User-Agent:Mozilla/5.0<br>Accept:text/html<br>Accept-Language:en-us<br>… |

第一行是 Request Line 內容：GET 是 HTTP 命令，表示向伺服器要求檔案，檔案位於 /image 目錄下的 flag.img，HTTP/1.1 代表所使用的 HTTP 協定版本。其他相關參數有 Host、User-Agent、Accept 等等。第二行以下便是 Http Header，攜帶相關參數。

當伺服器收到 Http Request(Get 命令)後，回應 Http Response，如下：

| HTTP/1.1 200 OK **(Status Line)** |
|---|
| Transfer-Encoding：chunked **(Http Header)**<br>Date：Sun, 20, Nov 2018 08:20 GMT<br>Server:<br>… |
| 傳輸內容 **(Content)** |

第一行為 Status Line，包含傳輸協定 (HTTP/1.1) 與傳輸狀態 (200 OK)，接著是 Http Header 與傳輸內容。

## 5-1-5 系統規劃與建置

### (A) 網路規劃與建置

我們利用 Cisco Packet Tracer 規劃與建置網頁系統，來觀察它的運作模式。雖然它是模擬真實情況，但幾乎能與真實網路完全相符。吾人需選擇下列元件來建置：

(1) Server-PT：模擬伺服器主機。於該主機上可選擇開啟多種服務，譬如：HTTP、DHCP、DNS、FTP 等伺服器功能，本範例選擇開啟 HTTP 服務。

(2) PC-PT：模擬客戶端主機。該主機上提供多種客戶端套件，譬如：Terminal、Command Prompt、Web Browser、Email 等等。本範例選擇使用 Web Browser 套件。

(3) 2960-24TT。模擬 24 埠口 Layer 2 交換器。作為連結 Server-PT 與 PC-PT 的設備。

另外，吾人選擇 192.168.0.0/24 私有網路區段，並指定 192.168.0.254 為 Default Gateway 與 DNS = 168.95.1.1，雖然本範例沒有用到此功能，但還是依照標準作業程序完成它。主機的 IP 位址設定與連接埠口位置，如下表所示：**(請自行設定主機上網路參數)**

| 裝置 | IP 位址 | 連接埠口 |
|---|---|---|
| HTTP_Server | 192.168.0.250 | SW1(fa0/24) |
| PC0 | 192.168.0.1 | SW1(fa0/1) |
| Default gateway = 192.168.0.254、DNS = 168.95.1.1 | | |

依照上表所建置的網路圖，如下所示：**[請下載：Web Server 系統.pkt]**

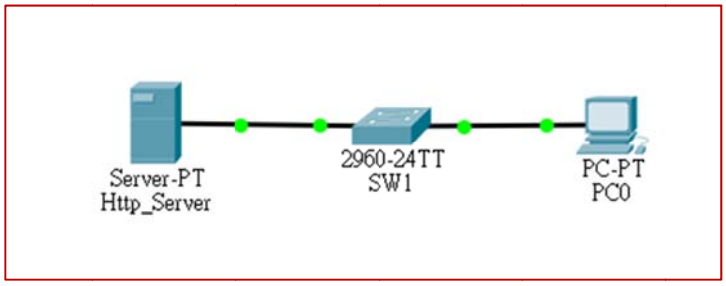
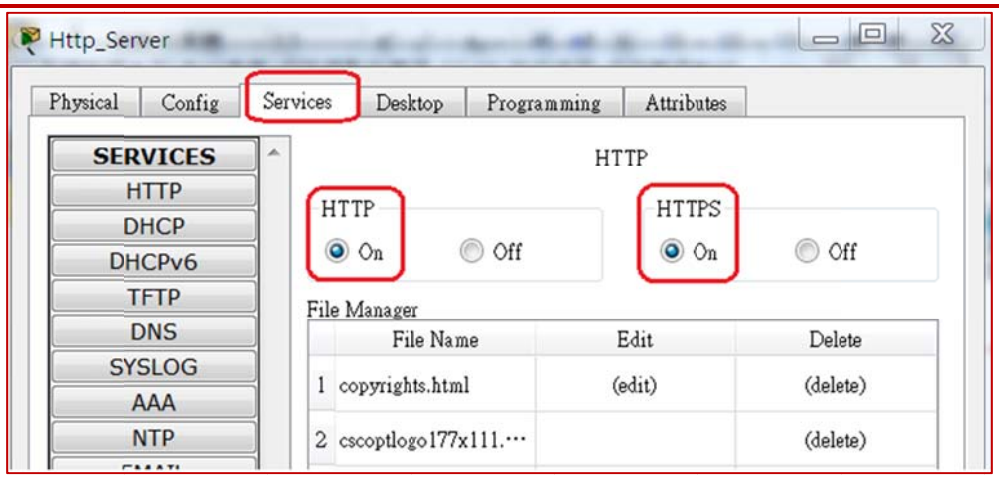



**圖 5-4 Web 網路系統**

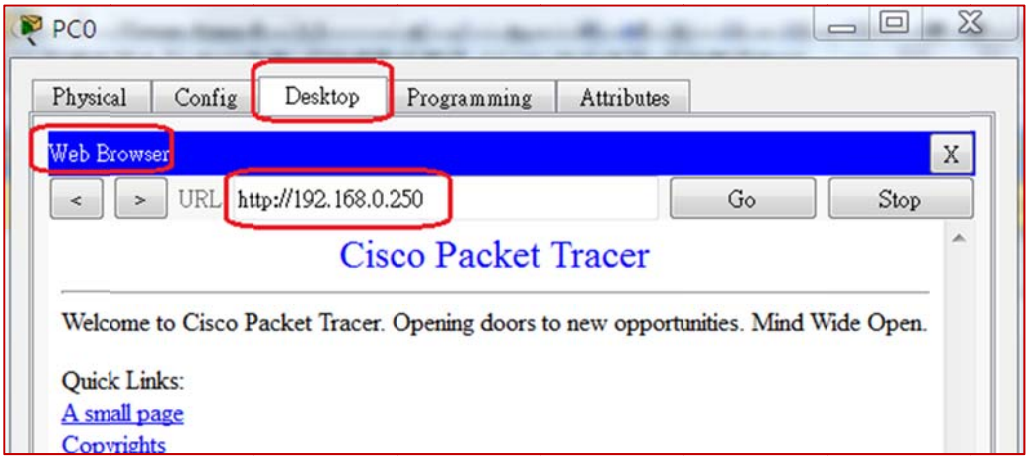
## (B) 伺服器設定與連線

連線完成之後，須開啟伺服器上的 HTTP 服務，再由 PC 上瀏覽該伺服器上網頁。

**(1) 步驟 1：**於 HTTP_Server 上開啟 HTTP 服務，如下：



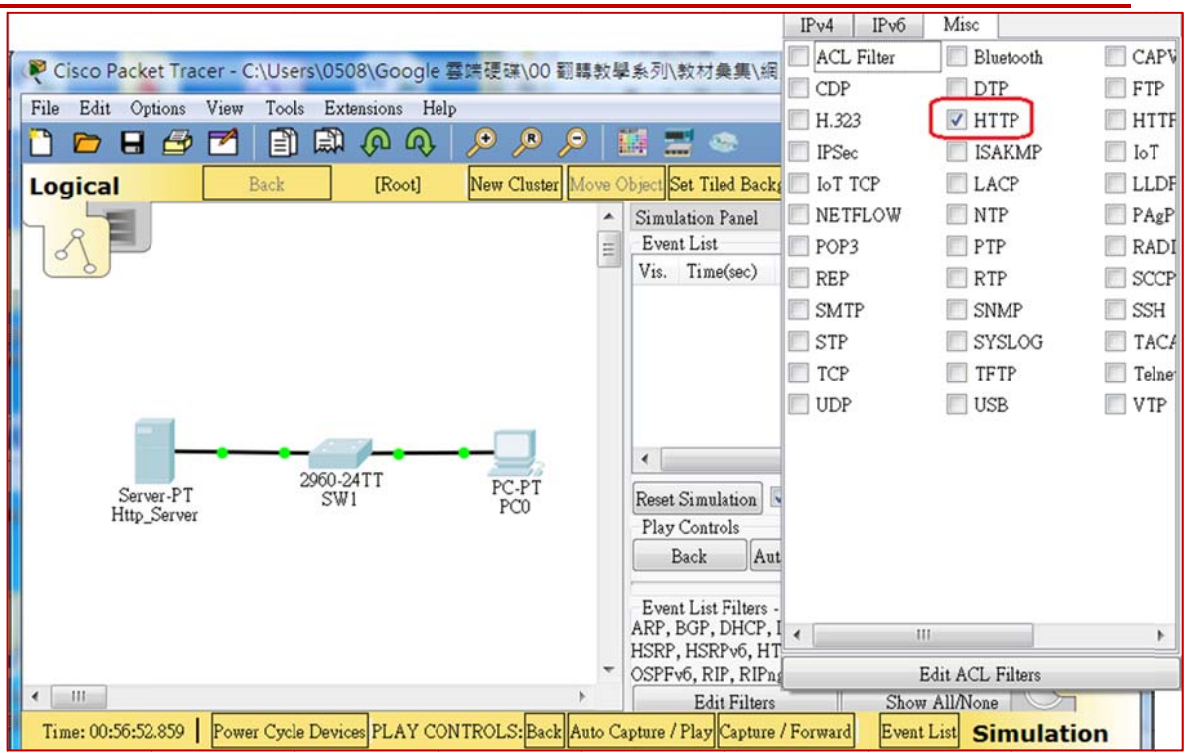

**(2) 步驟 2：**於 PC0 上開啟 Browser，並輸入 http://192.168.0.250，如果可以瀏覽到伺服器上網頁，則表示網頁系統建置成功，如下：




## 5-1-6 分析 HTTP 協定

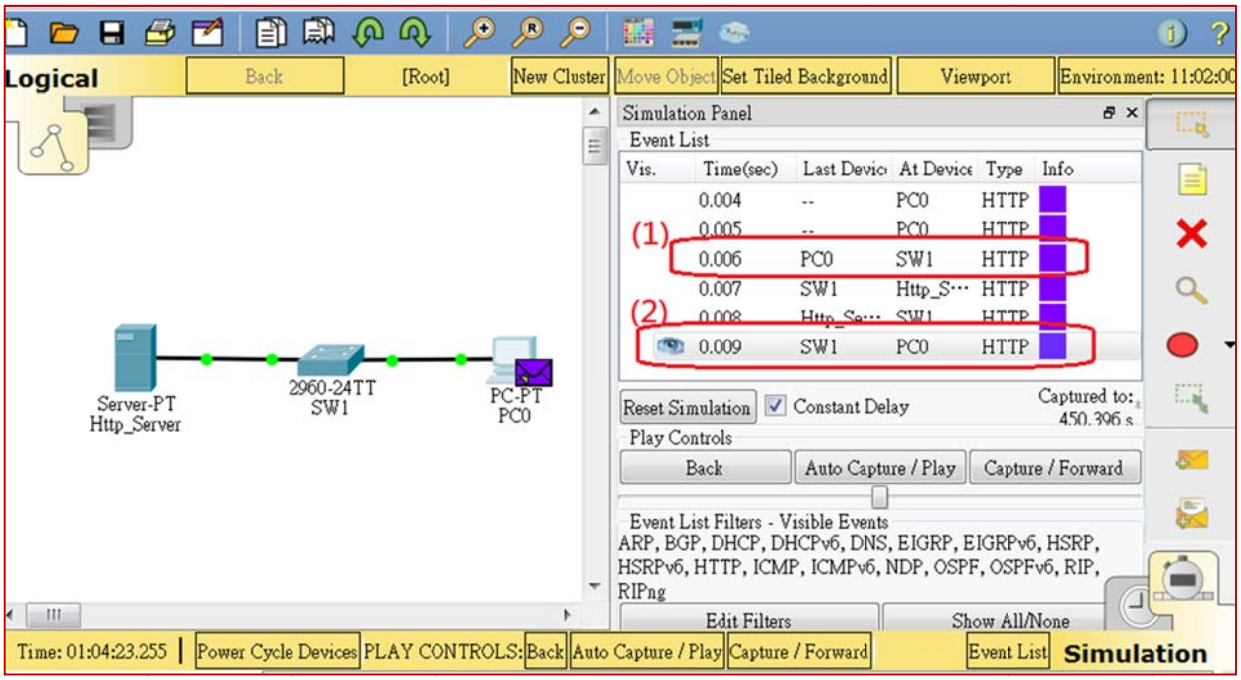
### (A) HTTP 封包擷取

**(1) 步驟 1：**擷取 HTTP 封包：將 Packet Tracer 設定成 Simulation Mode，並將過濾封包僅選擇 HTTP 封包，如下：




**(2) 步驟 2：**PC0 再選擇 desktop -> Browser -> 輸入 http://192.168.0.250 -> enter

**(3) 步驟 3：**Packet Tracer 上點選 Auto Capture/Play，之後觀察封包流動，並擷取封包，如下：

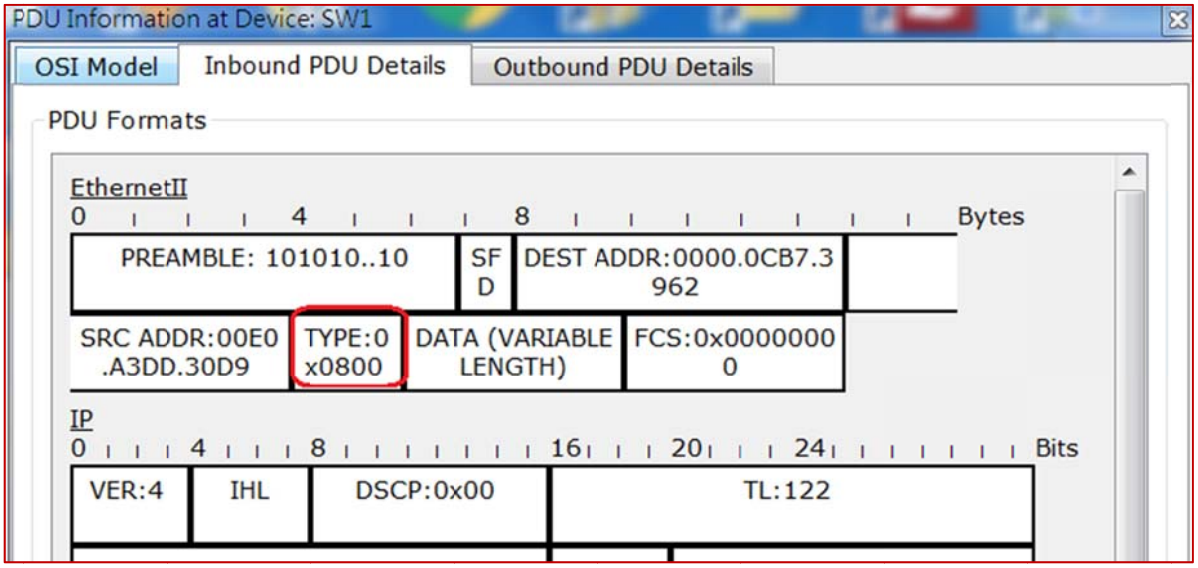



- 第一個封包是 PC0 => HTTP_Server 的 http request 封包。
- 第二個封包是 HTTP_Server 回應給 PC0 的 http response 封包。

## (B) HTTP 協定分析

**(1) 步驟 1：**觀察 HTTP Request 封包，得到下列結果：

- Ethernet II 標頭：Type = 0x0800。
- IP 標頭：PRO = 0x06(TCP 封包)、SRC IP = 192.168.0.1、DST IP = 192.168.0.250。
- TCP 標頭：Source Port = 1026、Dest Port = 80。
- HTTP Request。




**(2) 步驟 2：**觀察 HTTP Response 封包，得到下列結果：

- Ethernet II 標頭： Type = 0x0800。
- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.250、DES IP = 192.168.0.1。
- TCP 標頭：Source Port = 80、DES Port = 1026。
- HTTP Response。

## 5-1-7 分析 HTTP 協定 - Wireshark

請自行練習

# 5-2 檔案傳輸系統

## 5-2-1 檔案傳輸系統簡介

**『檔案傳輸協定』( File Transfer Protocol, FTP )** 也幾乎是和 TCP/IP 網路同時誕生，是 APARNET 網路上重要的應用系統之一。FTP 主要是應用於檔案傳輸使用，將共享檔案存放於 FTP 伺服器，讓一般使用者可以透過網路來下載或上傳。它的重點是在異質性電腦之間、以及遠距離的檔案共享使用，如圖 5-5-1 所示。

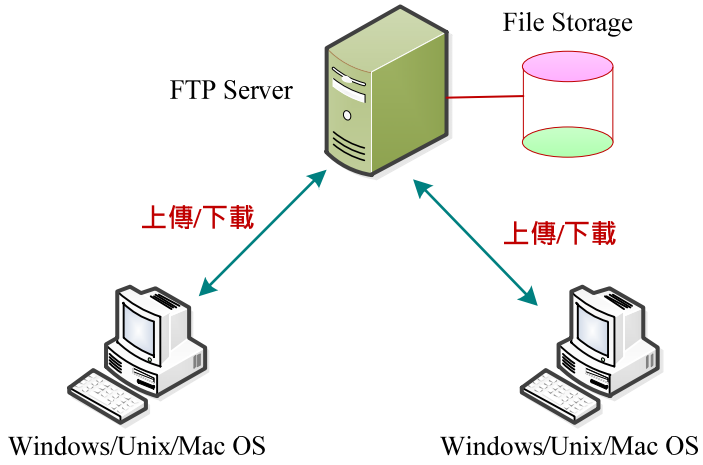



**圖 5-5-1 FTP 系統功能**

標準 Unix/Linux 版本上的 FTP 伺服器，使用者都必須具系統上的使用者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，並且都是無條件讓使用者下載使用，如需要完整系統上的使用者名稱及密碼，將會嚴重限制使用者的方便性，因此，就有**『匿名 FTP』( Anonymous FTP )** 的誕生。在匿名 FTP 之下，使用者以 anonymous 為使用者名稱，而以電子郵遞帳號作密碼便可登入，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真正去偵測帳號的真實性，而只判斷是否有**『@』**來決定是否允許登入。

FTP 使用兩個 TCP 連線來傳輸檔案，著名埠口 20 ( tcp/20 ) 做為傳輸資料使用，而另外埠口 21 ( tcp/21 ) 做為傳輸控制訊息使用，以下分別介紹這兩個連線的管理。

圖 5-5 為 FTP 建立連線方式，其中包含控制連線與資料連線，控制連線運作如下：

1. FTP 檔案傳輸系統採用主從式模式，FTP 伺服端隨時監視埠口 21 ( tcp/21 ) 是否有連線要求。FTP 客戶端需要連線時，便由著名埠口 21 連結到 FTP 伺服器。

2. 主從雙方都模擬成 NTV 終端機系統，可由使用者介面輸入 FTP 命令，並將該命令以直譯（Interpret）方式，編譯成 ASCII 命令，再傳送給對方。因此，主從雙方皆具有『使用者協定直譯器』（User Protocol Interpreter, User PI）和**『伺服端協定直譯器』（Server Protocol Interpreter, Server PI）**。

3. 伺服端同意連線後（驗證使用者名稱及密碼），便建立並保持著控制連線，以便隨時交換訊息，當需要傳輸檔案時，再建立資料連線，傳輸後立即釋放該資料連線，一般伺服端的資料連線都建立在埠口 20（20/tcp）。

4. 雙方透過資料連線來存取各自檔案系統（File System）中的檔案，此時會牽涉到系統檔案的讀取和寫入動作，而它是由主從式雙方各自呼叫系統函數來達成，該工作是由『使用者資料傳輸程序』（User Data Transfer Process, User DTP）和**『伺服端資料傳輸程序』（Server Data Transfer Process, Server DTR）**來完成。

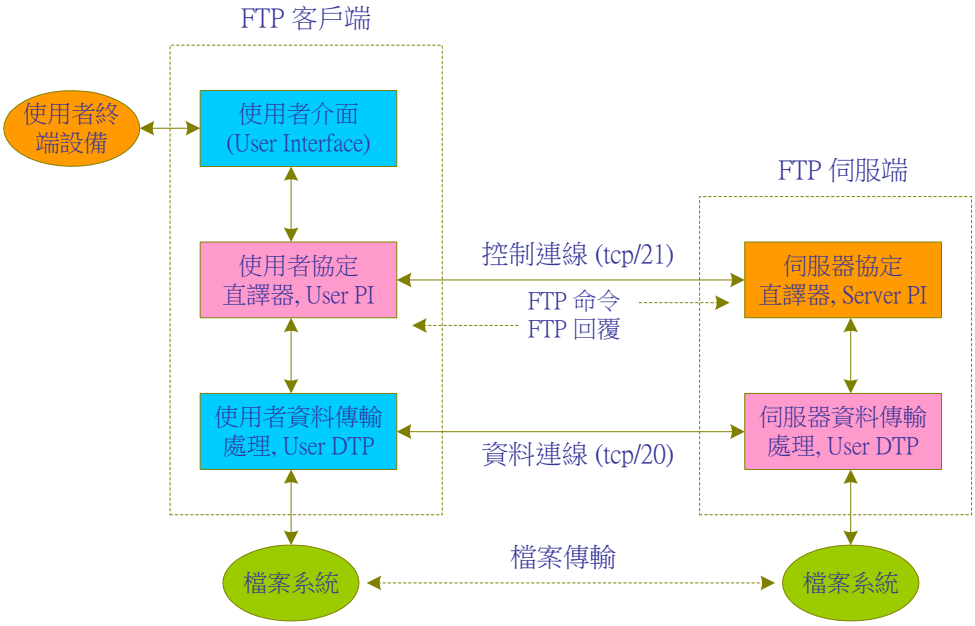



**圖 5-5 FTP 連線方式**

FTP 協定運作重點說明如下：

- **交談式溝通(Interactive)：**客戶端與伺服器之間以請求與回應方式，客戶端以 FTP 命令向伺服端要求服務，伺服端再以 FTP 回應，給予執行結果。
- **直譯式命令：**客戶端以 ASCII 格式傳送命令給伺服端，伺服端再以直譯式解釋命令，並給予服務。

- **沒有標準封裝格式：**在 FTP 封包標頭上，並不像 DNS 協定一樣有標準欄位可以填寫。

## 5-2-2 FTP 傳輸模式

FTP 有 Active Mode 與 Passive 兩種傳輸模式，最主要是決定如何建立資料連線。FTP 客戶端與伺服端都使用兩個埠口傳輸，基本上 FTP Server 上控制連線的埠口是 21/tcp，資料連線是 20/tcp 埠口。FTP Client 無論控制連線或資料連線都採用隨機埠口(> 1024/tcp)，但隨著傳輸模式不同，FTP Server 的資料連線也可能採用其他隨機埠口。

### (A) 伺服端主動 – Active Mode

一般在主從式的應用系統上，任一事件的發生，大多是由客戶端主動要求，而伺服端才會隨著客戶端需求做出適當的反應，因此是否需要建立的決定權在於客戶端，所以建立資料連線的運作程序如下：

1. 當 FTP Client 利用一個隨機埠口(>1024) 呼叫 FTP Server 的埠口 21/tcp 要求控制連線，並利用 Three-way Handshake 連線成功。
2. FTP Client 告訴 Server，Client 端欲利用哪一埠口做資料連線。
3. FTP Server 利用 20/tcp 埠口向 Client 所告知的埠口建立資料連線(採 Three-Way Handshake)。
4. 由雙方即可利用資料連線傳輸資料。
5. Active 的缺點：一般 FTP Server 主機都設有防火牆防護，伺服端不太可能允許發送 TCP SYN 向外要求連線的訊息，因此，一般 Internet 網路較少使用。

圖 5-6 為 FTP Server 主動要求建立資料連線的運作圖，FTP Client 以埠口 1073（1073/tcp）連結到 Server 端的埠口 21（21/tcp），此為控制連線。但當需要傳輸資料時，FTP Client 發出 PORT 163,15,2,62,4,50 來告訴 Server 端，欲傳輸資料的 IP 位址（163.15.2.62）和埠口位址（1074 = 4 *256 +50）。FTP Server 再由埠口 20（20/tcp）要求建立資料連線到 Client 端的 1074 埠口。

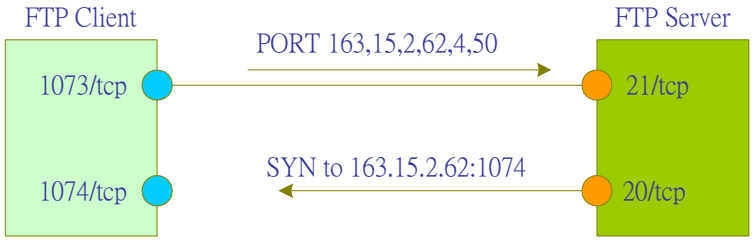



圖 5-6 伺服器主動之運作圖

## (B) 客戶端主動

在 FTP 協定的預設是伺服器主動狀態，但有些情況必須由客戶端主動連接，在這種情況下 FTP Client 可利用 PASV( Passive Mode )命令，要求 Server 端進入聆聽狀態等待連接。運作程序如下：

1. 當 FTP Client 利用一個隨機埠口(>1024) 呼叫 FTP Server 的埠口 21/tcp 要求控制連線，並利用 Three-way Handshake 連線成功。
2. FTP Client 發送 PASV Command 給 Server，要求進入 passive 傳輸模式。
3. FTP Server 隨機選擇 TCP 埠口(>1024)，利用控制連線告訴 Client 端。
4. TCP Client 呼叫 Server 告知的埠口，並利用 Three-Way handshake 建立資料連線。
5. 由雙方即可利用資料連線傳輸資料。

因此， FTP Server 的資料連線就不一定會建立在 20/tcp 埠口上，運作如圖 5-7 所示。(4 * 256 + 16 = 1040)

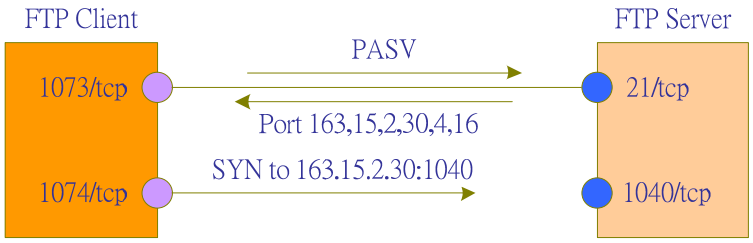



圖 5-7 客戶端主動之運作圖

# 5-2-3 FTP 服務命令

簡單來說， FTP 控制連線是 FTP Server 與 FTP Client 之間溝通的管道，**它們之間是利用交談式(Interactive) 方式溝通，由 FTP Client 下命令給 FTP Server 要求那些服務，當 FTP Server 同意服務之後，再利用資料連線傳送資料(可能 Up Load 或 Down Load)**。所以雙方傳送訊息便沒有像其他應用系統(如 DNS Systen)有一定的封裝格式。常用命令如下：

- **STOR**：FTP Client 儲存檔案於 Server 端，也就是 Client 端上傳一個檔案到 Server 端，如：『**STOR file1.dat**』。
- **RETR**：FTP Client 向 Server 複製一個檔案，也就是由 Server 端下載一個檔案到 Client 端，如：『**RETE file1.dat**』。
- **STOU**：（**Store Unique**）如同 STOR 一樣都是傳輸一個檔案到 Server 端，但 STOU 表示傳輸後在 Server 端必須是唯一的檔案名稱，也就是不可覆蓋同一檔名的檔案。
- **REST**：（**Restart**）要求重新啟動傳輸連線。
- **DELE**：（**Delete**）要求刪除 Server 上某一檔案。
- **RMD**：（**Remove Directory**）要求刪除某一檔案目錄。
- **MKD**：（**Make Directory**）要求建立一個目錄。
- **LIST**：顯示檔案目錄。
- **NOOP**：（**No Operation**）此為 dummy 命令，Server 並未執行任何工作，而回應一個執行正確的訊息。
- **ABOR**：中斷前一個 FTP 命令及任何資料傳輸。

## 5-2-4 FTP 系統規劃與建置

### (A) 網路規劃與建置

我們利用 Cisco Packet Tracer 規劃與建置網頁系統，來觀察它的運作模式。雖然如此建立的系統是模擬真實情況，但幾乎能與真實網路完全相符。吾人需選擇下列元件來建置：

(1) Server-PT：模擬伺服器主機。於該主機上可選擇開啟多種服務，譬如： HTTP、DHCP、DNS、FTP 等伺服器功能，本範例選擇開啟 FTP 服務。

(2) PC-PT：模擬客戶端主機。該主機上提供多種客戶端套件，譬如：Terminal、Command Prompt、Web Browser、Email 等等。本範例選擇使用 Command Prompt 介面。

(3) 2960-24TT。模擬 24 埠口 Layer 2 交換器。作為連結 Server-PT 與 PC-PT 的設備。

另外，吾人選擇 192.168.0.0/24 私有網路區段，並指定 192.168.0.254 為 Default Gateway 與 DNS = 168.95.1.1，雖然本範例沒有用到此功能，但還是依照標準作業程序完成它。主機的 IP 位址設定與連接埠口位置，如下表所示：**(主機上網路參數請自行設定)**

| 裝置 | IP 位址 | 連接埠口 |
|---|---|---|
| HTTP_Server | 192.168.0.250 | SW1(fa0/24) |
| FTP_Server | 192.168.0.251 | SW1(fa0/23) |
| PC0 | 192.168.0.1 | SW1(fa0/1) |
| Default gateway = 192.168.0.254、DNS = 168.95.1.1 | | |

依照上表所建置的網路圖，如下所示：**[請下載：FTP Server 系統.pkt]**

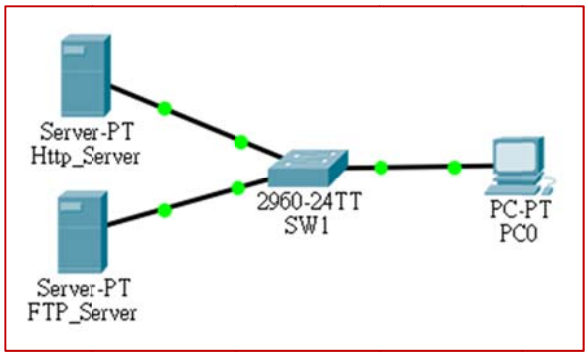
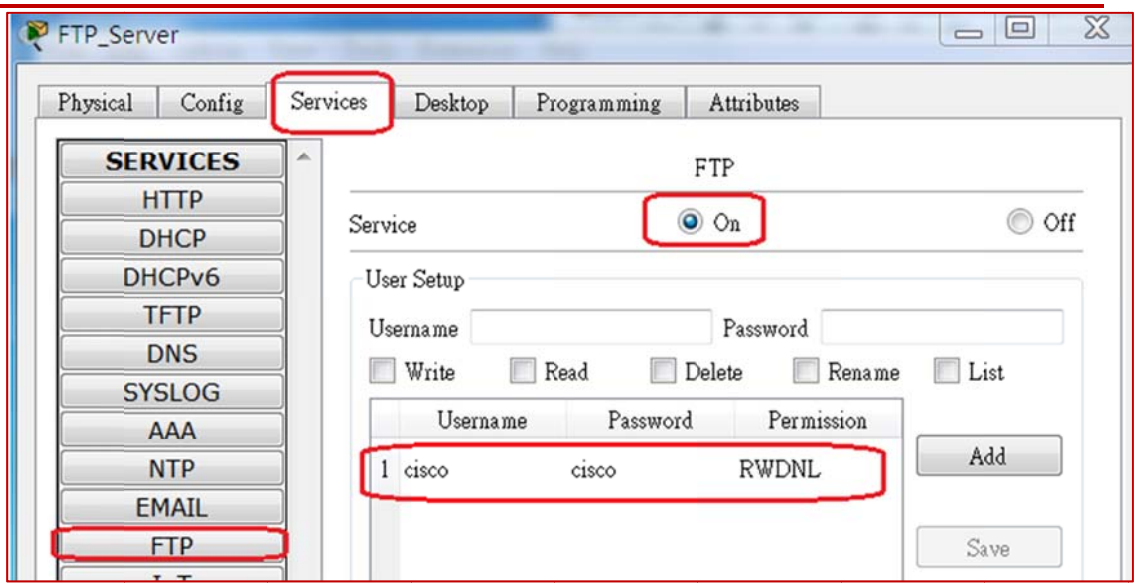


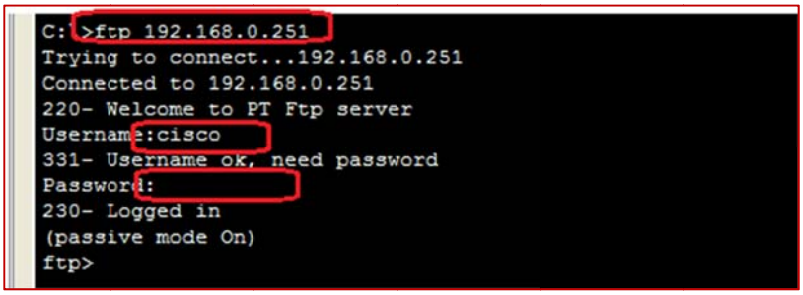

**圖 5-8 FTP 網路系統**

## (B) 伺服器設定與連線

**(1) 步驟 1：**於 FTP_Server 上開啟 FTP 服務，如下：(得知帳號： cisco、密碼：cisco)




**(2) 步驟 2：**於 PC0 上開啟 Desktop => Command Prompt，並輸入>ftp 192.168.0.250。輸入帳號與密碼後，可連結到 FTP 伺服器，表示建置成功。如下：




## 5-2-5 分析 FTP 連線封包

### (A) FTP 連線封包擷取

Packet Tracer 自動採用 FTP Passive Mode 傳輸模式，吾人先將它的運作程序歸納如下：

- FTP Server 開啟埠口 21/tcp，並等待客戶端要求連線。
- FTP Client 利用一個大於 1023 (如 1030) 埠口向 FTP Server 要求連線 (1030 => 21)。
- FTP Sever 回應同意連線。
- FTP Client 發送 PASV 要求客戶端主動，請給予埠口位置。
- FTP Server 發送 port 命令，並告知 Data Channel 為埠口 1040/tcp。

- FTP Client 利用 1050 埠口向 FTP Server 1040 要求連線。(Client 1050/tcp => Server 1040/tcp)。
- FTP Server 回應同意資料連線。(Server 1040/tcp => Client 1050/tcp)

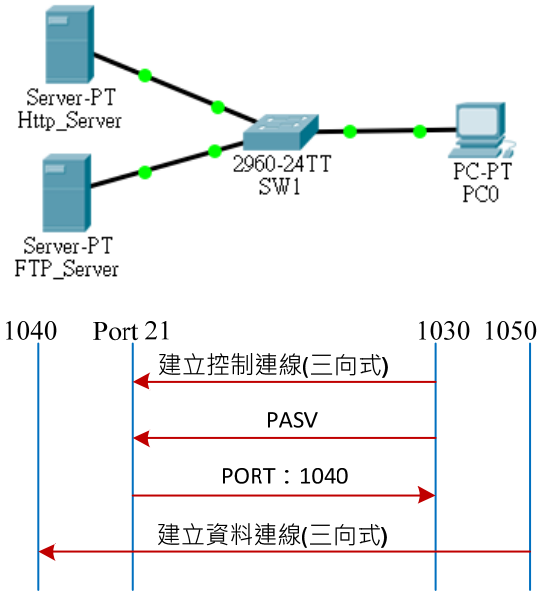
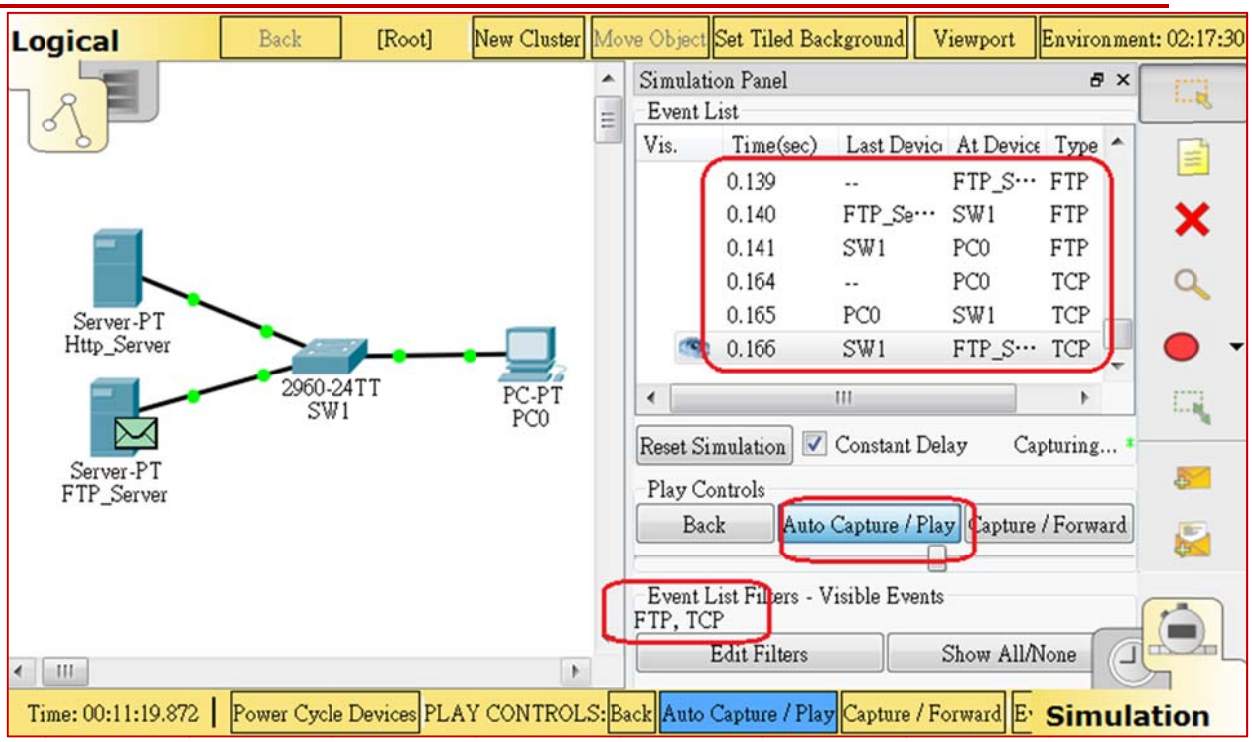



圖 5-9 FTP 訊號流程

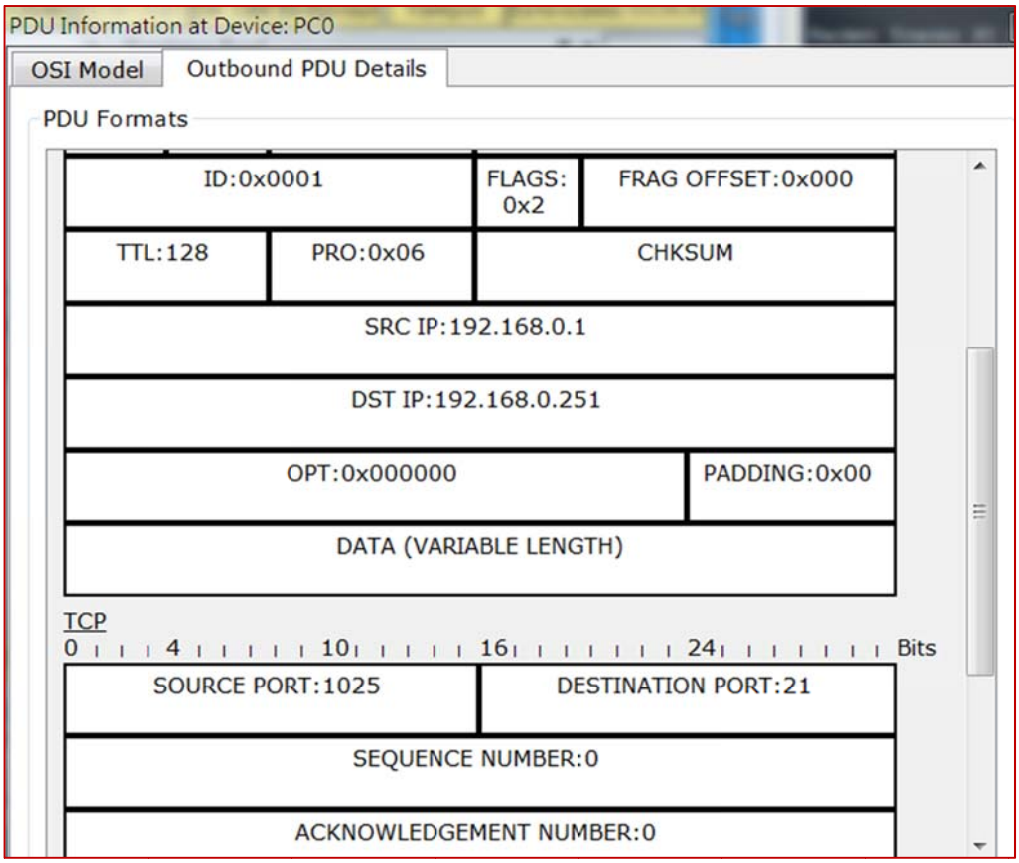
**(1) 步驟 1**：將 Packet Tracer 設定成 Simulation Mode，並將過濾封包僅選擇 **FTP** 與 **TCP** 封包。

**(2) 步驟 2**：將 PC0 進入 Command Prompt 模式，並輸入 > ftp 192.168.0.251 與執行。

**(3) 步驟 3**：將在 Packet Tracer 上按 Auto Capture/Play 擷取封包如下：




## (B) 分析 TCP Connect Request 封包

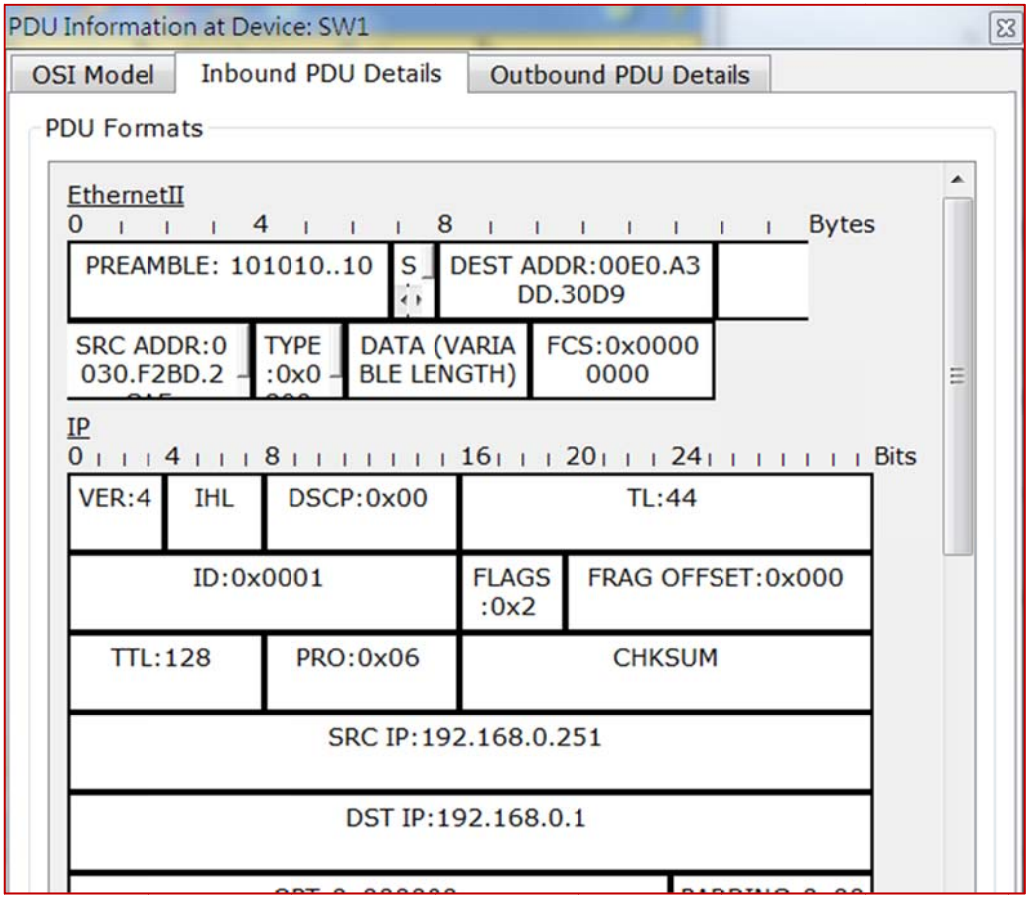



得到下列結果：

- Ethernet II 標頭： Type = 0x0800。
- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.1、DES IP = 192.168.0.251。

- TCP 標頭：Source Port = 1025、DES Port = **21**。

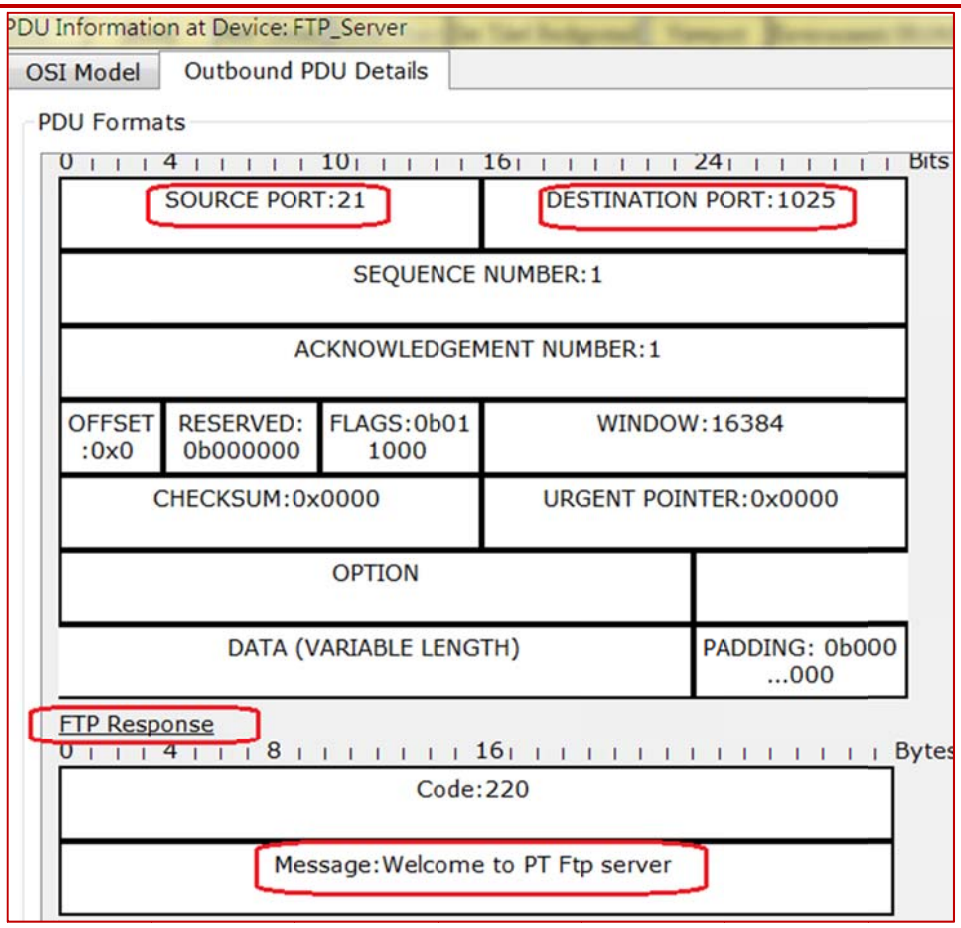
## (C) 分析 TCP Connect Response 封包




得到下列結果：

- Ethernet II 標頭： Type = 0x0800。
- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.251、DES IP = 192.168.0.1。
- TCP 標頭：Source Port = 21、DES Port = **1025**。

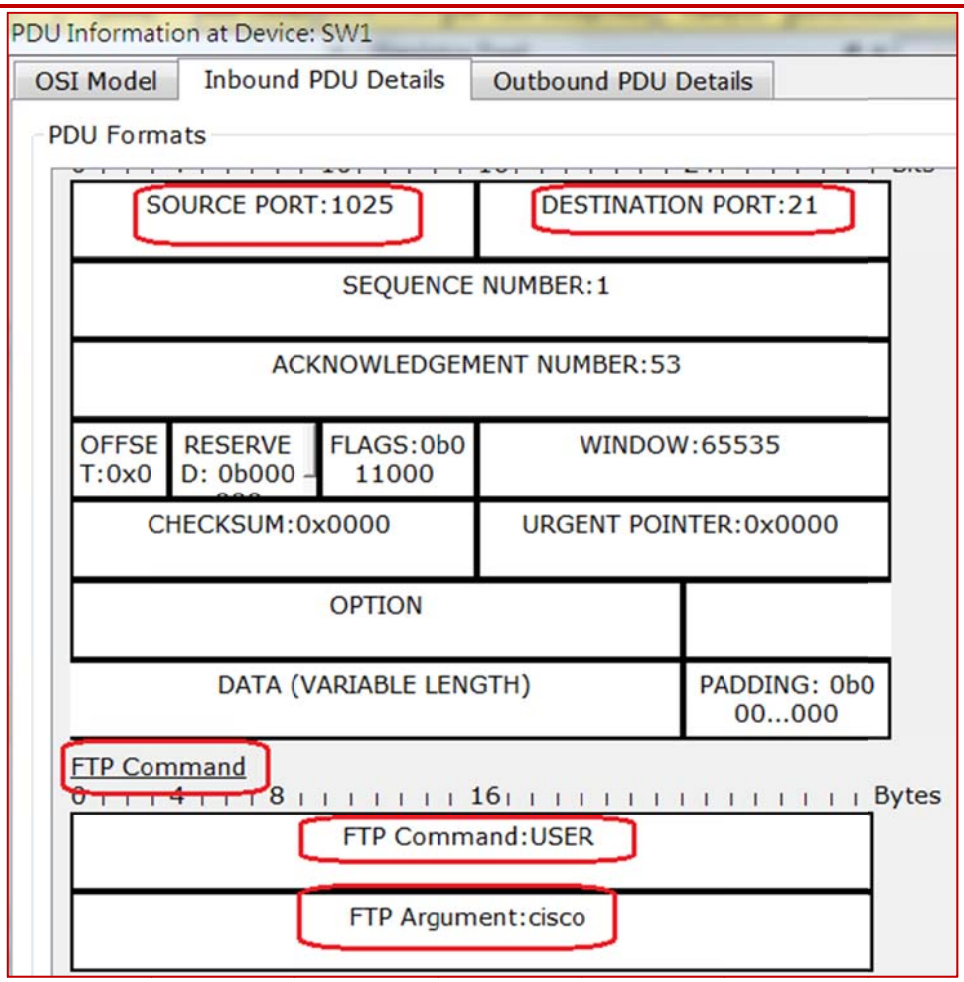
## (D) 分析 FTP Response 封包




得到下列結果：

- Ethernet II 標頭： Type = 0x0800。
- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.251、DES IP = 192.168.0.1。
- TCP 標頭：Source Port = 21、DES Port = **1025**。
- FTP 封包：code=220、Message = Welcome to PT FTP Server。

## (E) 分析 FTP Command 封包




得到下列結果：

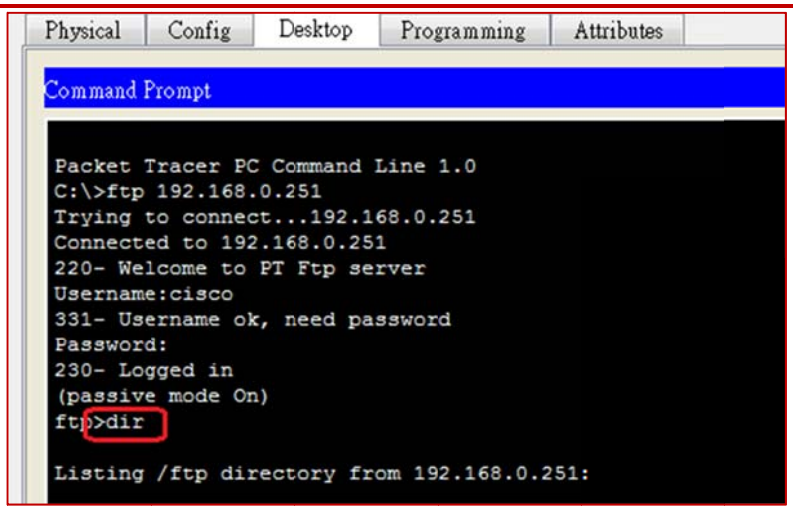
- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.1、DES IP = 192.168.0.251。
- TCP 標頭：Source Port = 1025、DES Port = **21**。
- FTP 封包：FTP Command:USER。

### (F) 其它 FTP Command 與 Response 封包

接著 FTP Server 要求 Client 端輸入帳號與密碼，會出現一連串的 FTP Command 與 FTP Response 封包交互傳遞，請自行觀察分析。

## 5-2-6 分析 FTP 資料封包

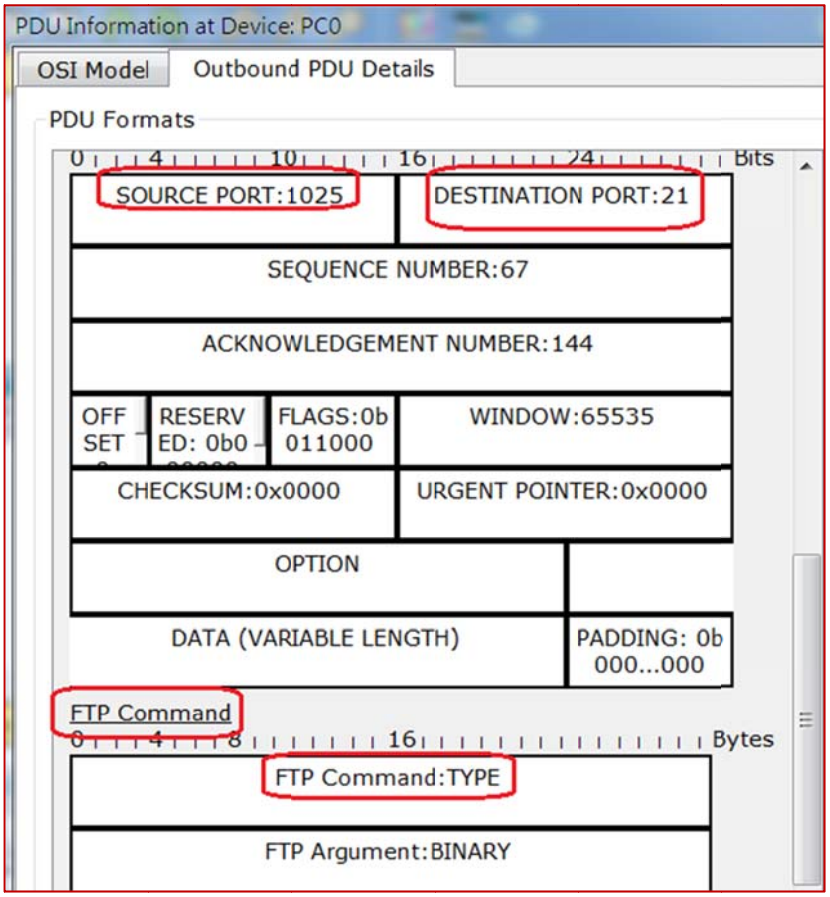
接著上述的實驗，PC0 上會出現等待命令的 Prompt，則輸入 dir，要求顯示伺服端命令，如下：




Packet Tracer 擷取到封包如下：

## (A) FTP Command：Type 封包

此封包為 FTP Client 要求是否同意制定 Data Channel 的型態？(PORT or PASV)



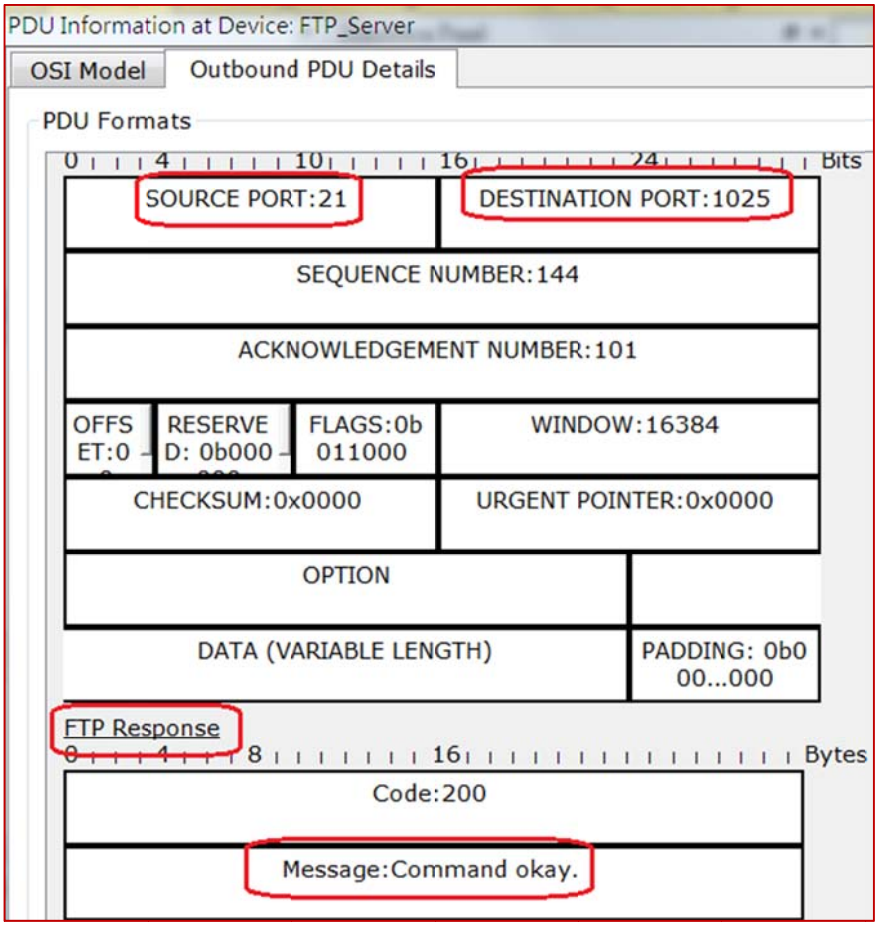

得到下列結果：

- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.1、DES IP = 192.168.0.251。
- TCP 標頭：Source Port = 1025、DES Port = **21**。

- FTP 封包： FTP Command：TYPE

## (B) FTP Command：okay 封包

此封包是 FTP Sever 同意 Client 制定 Data Channel 的型態。

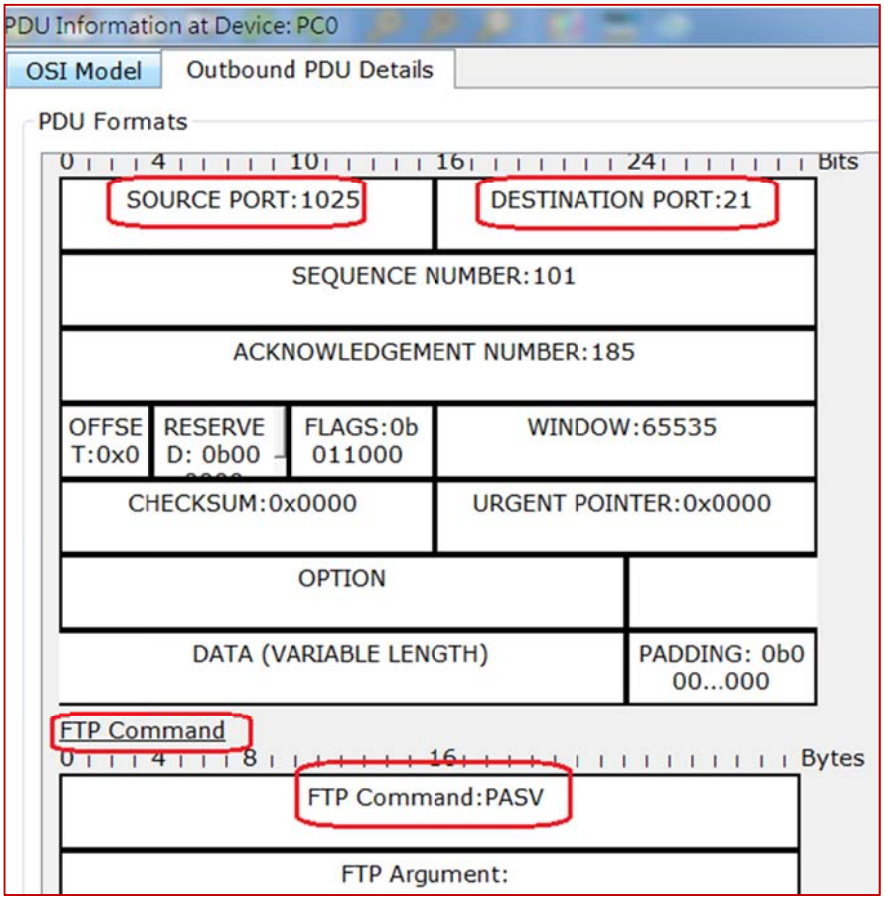



得到下列結果：

- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.251、DES IP = 192.168.0.1。
- TCP 標頭：Source Port = 21、DES Port = **1025**。
- FTP 封包： FTP Command：okay

## (C) FTP Command：PASV 封包

此封包是 FTP Client 制定 Data Channel 的型態為 PASV。

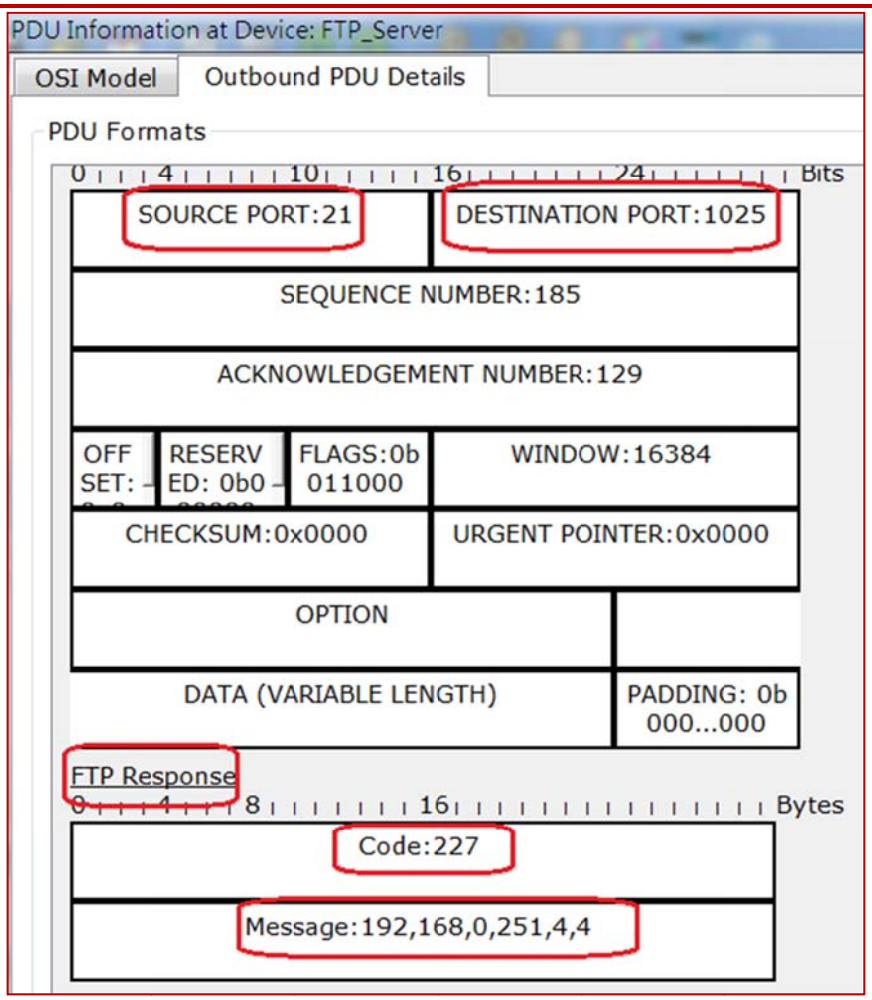



得到下列結果：

- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.1、DES IP = 192.168.0.251。
- TCP 標頭：Source Port = 1025、DES Port = **21**。
- FTP 封包： FTP Command：PASV

## (D) FTP Response：Message：192,168,0,251,4,4

此封包是 FTP Server 同意使用 PASV Mode 傳輸，並告知 Data Channel 埠口是 1028。

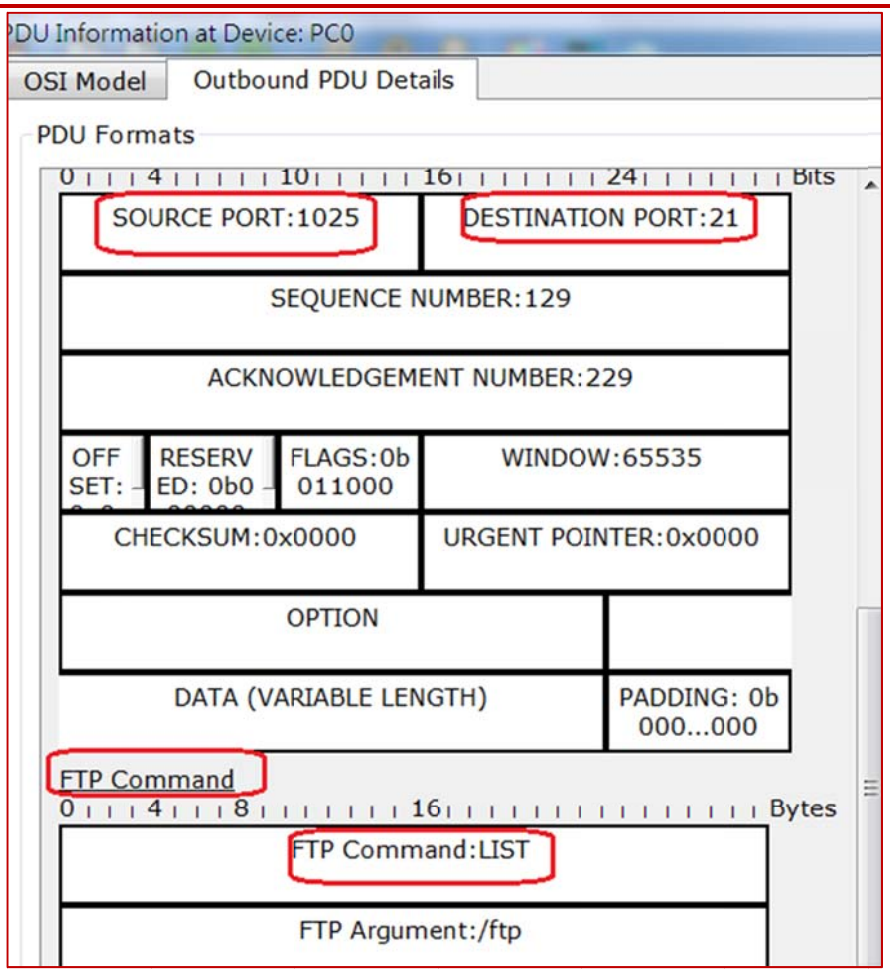



得到下列結果：

- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.251、DES IP = 192.168.0.1。
- TCP 標頭：Source Port = 21、DES Port = **1025**。
- FTP 封包： FTP Response：Message：192,168,0,251,4,4。**(192.168.0.251:1028)**

## (E) FTP Command：LIST 封包

此封包是 FTP Client 向 Sever 端下 dir 命令，要求顯示目錄內容。

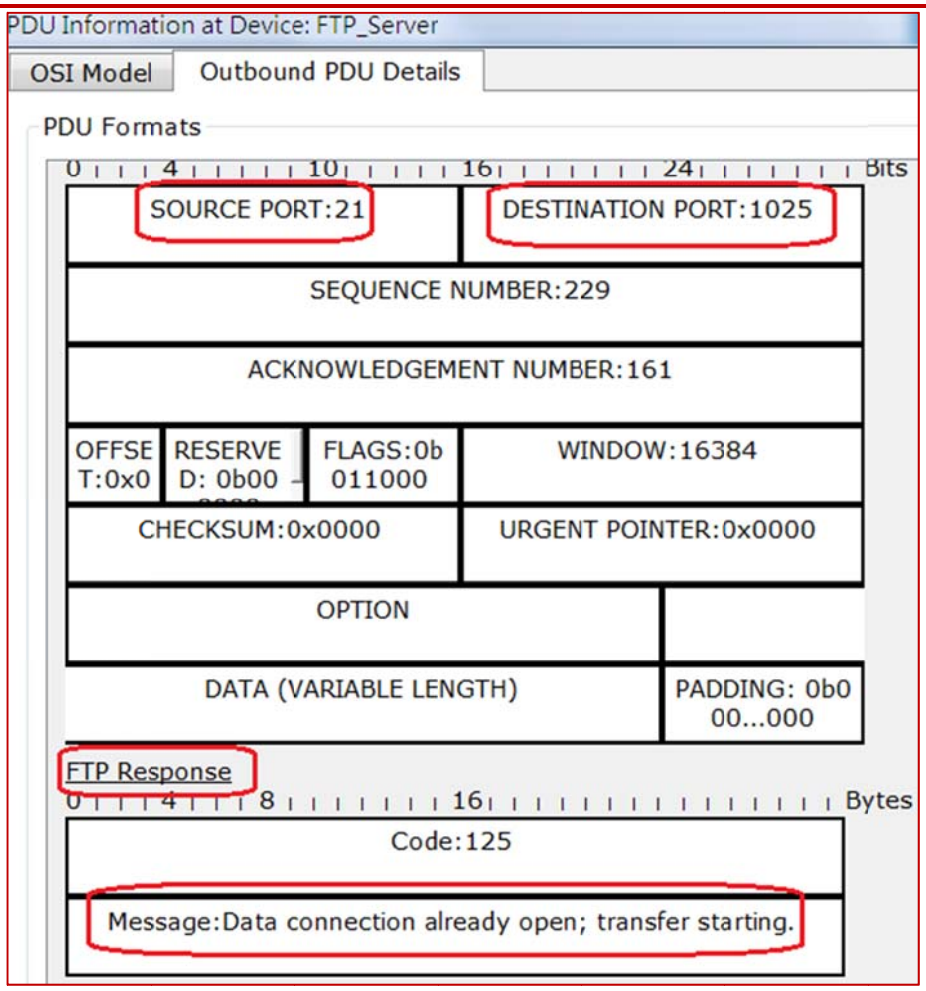



得到下列結果：

- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.1、DES IP = 192.168.0.251。
- TCP 標頭：Source Port = 1025、DES Port = **21**。
- FTP 封包： FTP Command：LIST

## (F) FTP Response：transfer starting

此封包是 FTP Sever 端同意並開始傳送資料。

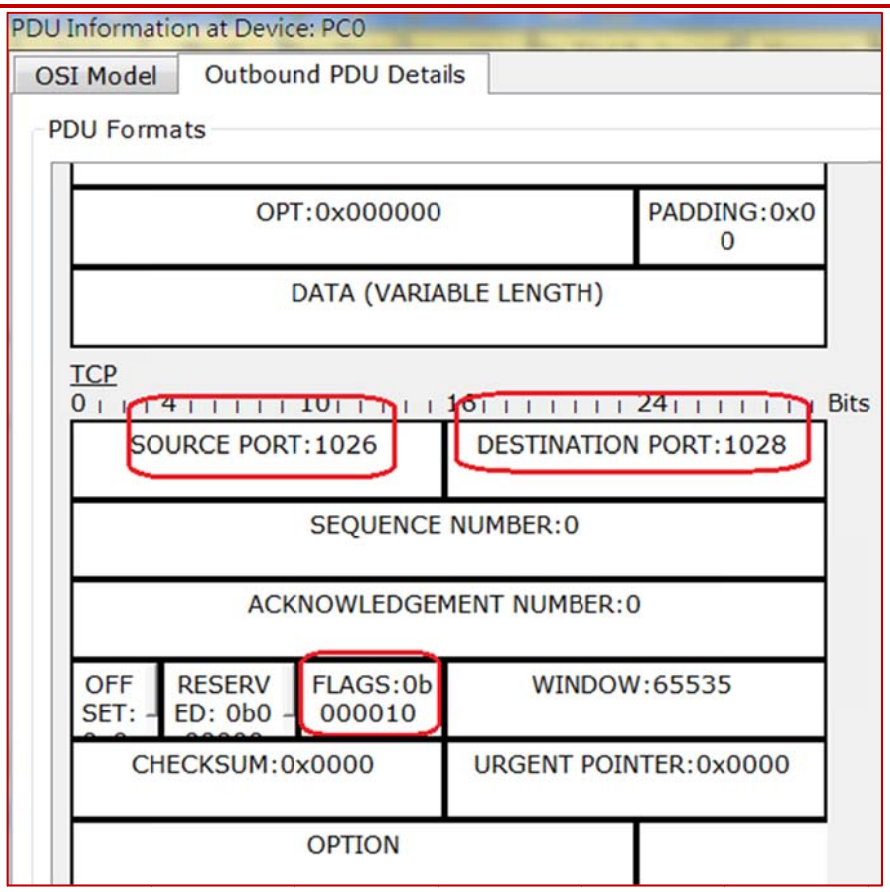



得到下列結果：

- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.251、DES IP = 192.168.0.1。
- TCP 標頭：Source Port = 21、DES Port = **1025**。
- FTP 封包： FTP Command：transfer starting

## (G) TCP Connect Request

此封包是 FTP Client 端要求建立資料傳輸的 TCP 連線。

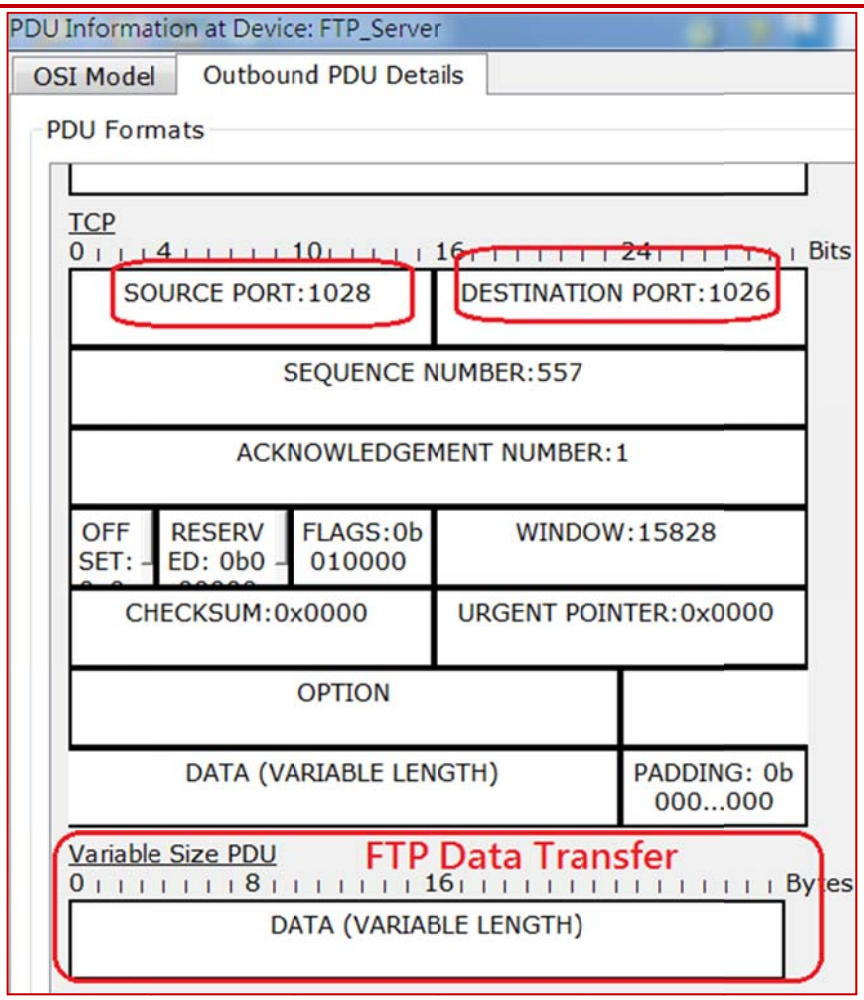



得到下列結果：

- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.1、DES IP = 192.168.0.251。
- TCP 標頭：Source Port = 1026、DES Port = **1028**。**(FTP Server 告知的埠口)**

## (H) TCP Data Transfer

上述要求連線後，會有一連串的三向式聯絡法封包，就不再敘述。建立連線後，即開始 FTP Dtat 傳輸，但它還是採用 TCP Data Transfer 封包傳送，如下：




得到下列結果：

- IP 標頭：PRO = 0x06、SRC IP = 192.168.0.151、DES IP = 192.168.0.1。
- TCP 標頭：Source Port = 1028、DES Port = **1026**。
- TCP Data。

## 5-2-6 分析 FTP 終止連線封包

請自行擷取下列封包練習：

- TCP Data Channel 終止連線封包。
- 當 Client 端輸入 > quit 命令後，擷取 FTP 終止連線封包。

# 5-3 網域名稱系統

## 5-3-1 DNS 系統功能

**『網域名稱系統』( Domain Name System, DNS )** 是目前網路上最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。目前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，也無法連結到網路上

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。

DNS 系統最基本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 5-10 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。

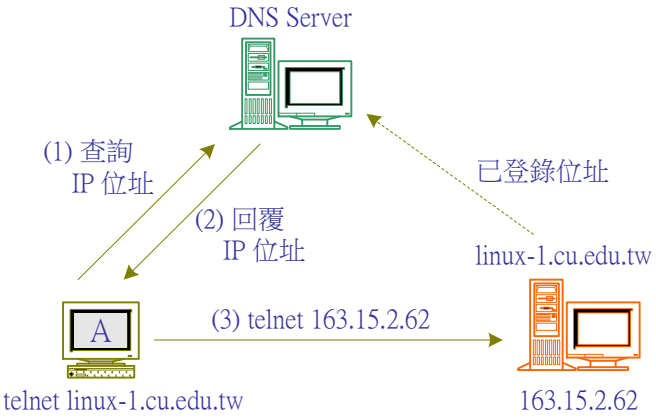



圖 5-10 DNS 正向解譯功能

## 5-3-2 DNS 命名方式

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。

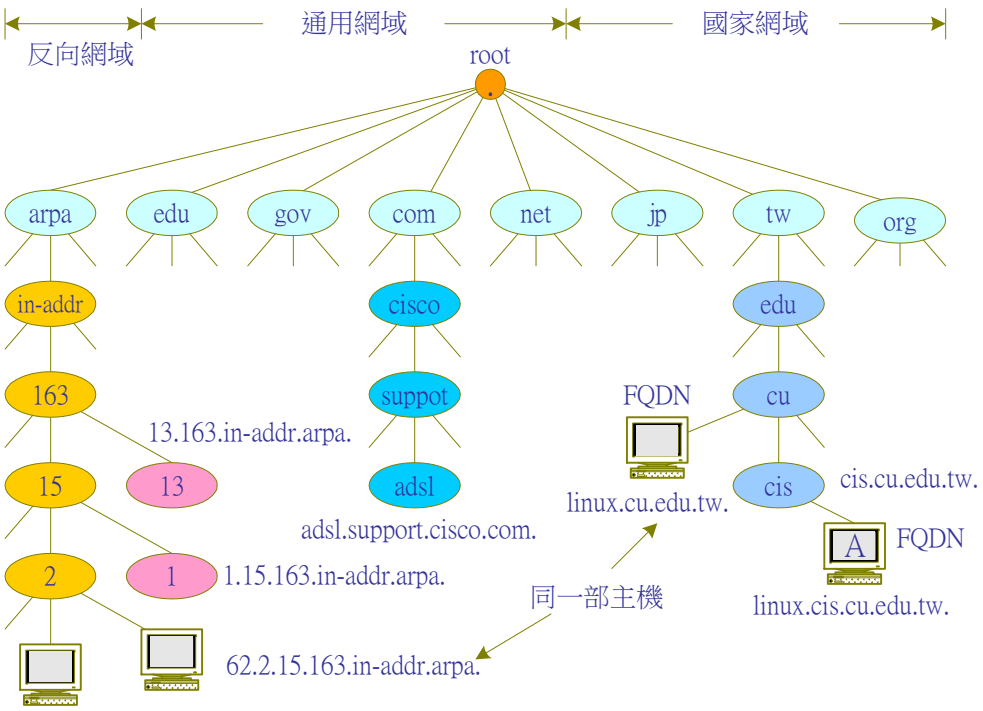



圖 5-11 DNS 網域名稱階層

### (A) 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 5-4 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。

### (B) 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 5-4 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。

## 5-3-3 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。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。

## (A) 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。

## (B) 搜尋順序

瞭解遞迴查詢和反覆查詢動作之後，我們用圖 5-12 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。

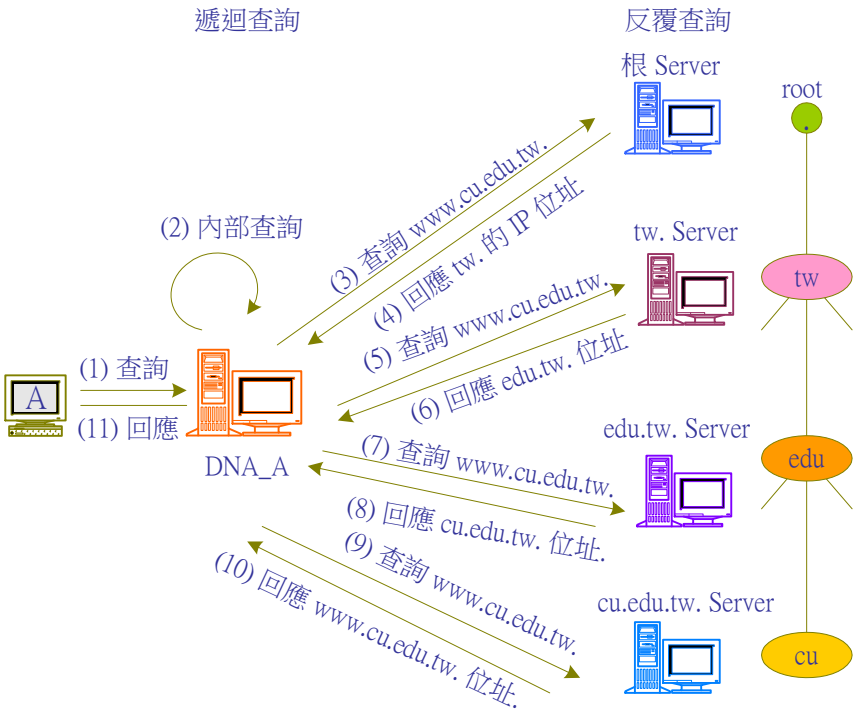



**圖 5-12 查詢順序**

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。

## 5-3-4 DNS 伺服器種類

當 DNS Server 收到一筆並非自己管轄的網域名稱時，如果都要透過由根網域開始，經過遞迴查詢與反覆查詢，才能查出其 IP 位址的話，那麼 DNS 服務的效率實在太低了。其實，我們透過許多措施來提升查詢效率，簡單的原理是：**『查詢過的資料就將它保存下來，如果有重複查詢的話，就直接回覆就好，不用再重新查詢』**。儲存查詢過的資料就是**『快取』**(Cache)，任何一部主機或 DNS 伺服器都具有快取的功能。另外，DNS 伺服器也有許多種類，說明如下：

### (A) 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。**(可利用 ipconfig /flushdns 命令清除)**

### (B) 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。

### (C) 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 )**。

### (D) 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。

### (E) 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如圖 5-13 所示。

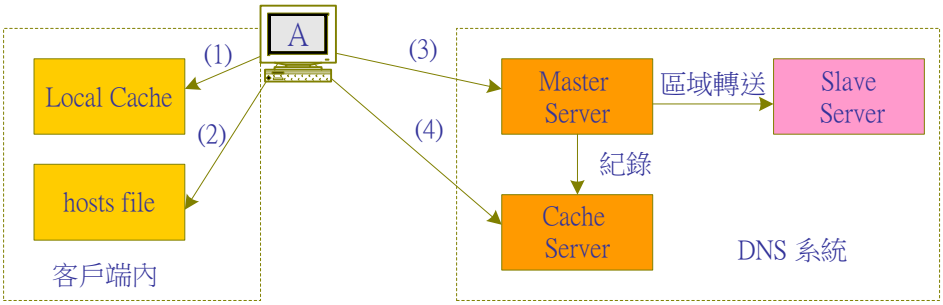



**圖 5-13 DNS 伺服器種類與查詢順序**

## 5-3-5 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，它不僅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）。

- **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。
- **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。

- **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。
- **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。
- **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。

## 5-3-6 DNS 封包格式

圖 5-13-1 (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。

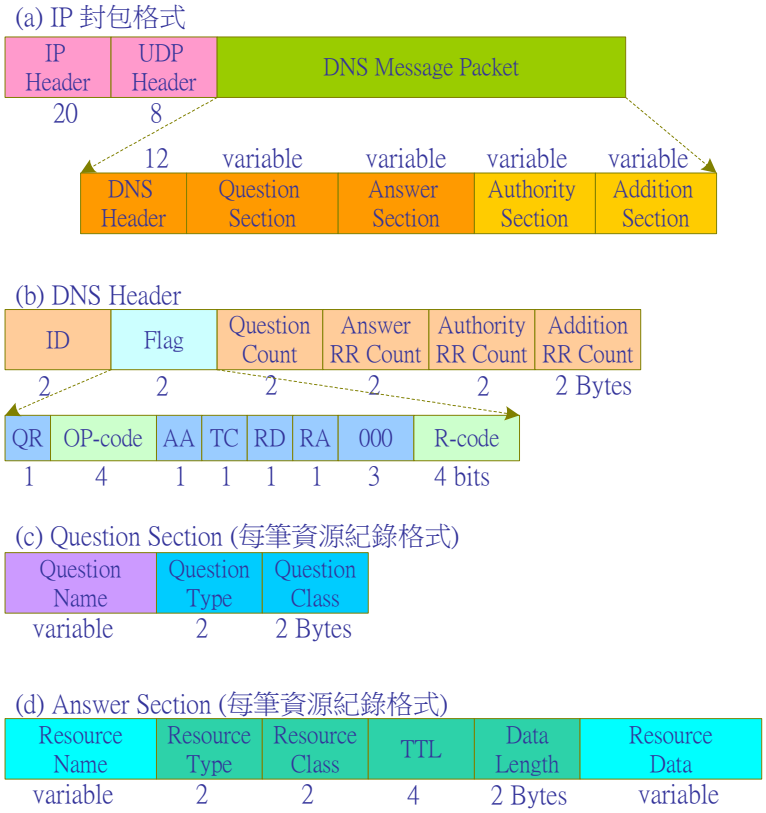



**圖 5-13-1 DNS 訊息封包格式**

## (A) DNS Header

圖 5-13-1 (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）、OP-code（Operating Code）、AA（Authoritative Answer）、TC( Truncated )、RD( Recursive Desired )、RA( Recursive Available )、R-code( Response Code )。

- **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。

## (B) Question Section

**『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 5-13-1 (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。各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。

- **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：

| 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 )。

## (C) Answer Section

『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 5-13-1 (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 )**

▲ **資源型態 ( Resource Type )**

▲ **資源類別 ( Resource Class )**。

▲ **存活時間 ( Time-To-Live, TTL )**

▲ **資源資料長度 ( Resource Data Length )**。

▲ **資源資料 ( Resource Data )**。

## 5-3-7 DNS 系統規劃與建置

### (A) 網路規劃與建置

我們利用 Cisco Packet Tracer 規劃與建置 DNS 系統，來觀察它的運作模式。雖然如此建立的系統是模擬真實情況，但幾乎能與真實網路完全相符。吾人需選擇下列元件來建置：

(1) Server-PT：模擬伺服器主機。於該主機上可選擇開啟多種服務，譬如： HTTP、DHCP、DNS、FTP 等伺服器功能，本範例選擇開啟 DNS 服務。

(2) PC-PT：模擬客戶端主機。該主機上提供多種客戶端套件，譬如：Terminal、Command Prompt、Web Browser、Email 等等。本範例選擇使用 Command Prompt 介面。

(3) 2960-24TT。模擬 24 埠口 Layer 2 交換器。作為連結 Server-PT 與 PC-PT 的設備。

另外，吾人選擇 192.168.0.0/24 私有網路區段，並指定 192.168.0.254 為 Default Gateway 與 DNS = 168.95.1.1，雖然本範例沒有用到此功能，但還是依照標準作業程序完成它。主機的 IP 位址設定與連接埠口位置，如下表所示：(請自行輸入主機的網路參數)

| 裝置 | URL 名稱 | IP 位址 | 連接埠口 |
|---|---|---|---|

| | | | |
|---|---|---|---|
| HTTP_Server | www.tsnin.idv.tw | 192.168.0.250 | SW1(fa0/24) |
| FTP_Server | ftp.tsnien.idv.tw | 192.168.0.251 | SW1(fa0/23) |
| DNS_Server | dns.tsnien.idv.tw | 192.168.0.252 | SW1(fa0/22) |
| PC0 | pc0.tsnien.idv.tw | 192.168.0.1 | SW1(fa0/1) |
| Default gateway = 192.168.0.254、DNS = 192.168.0.252 | | | |

依照上述參數建構網路型態如下：**[請下載：DNS Server 系統.pkt]**

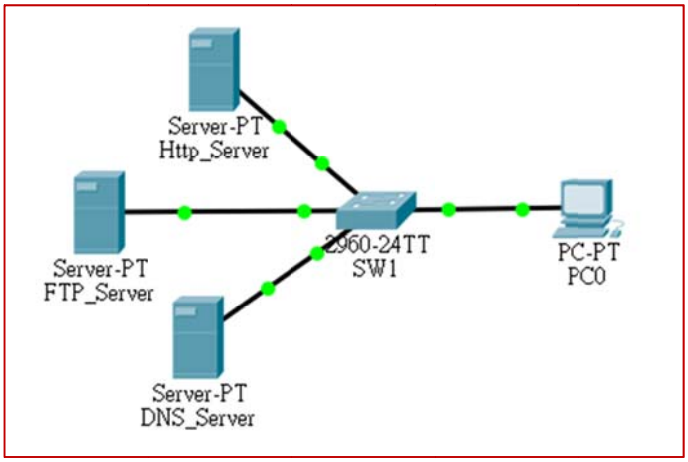
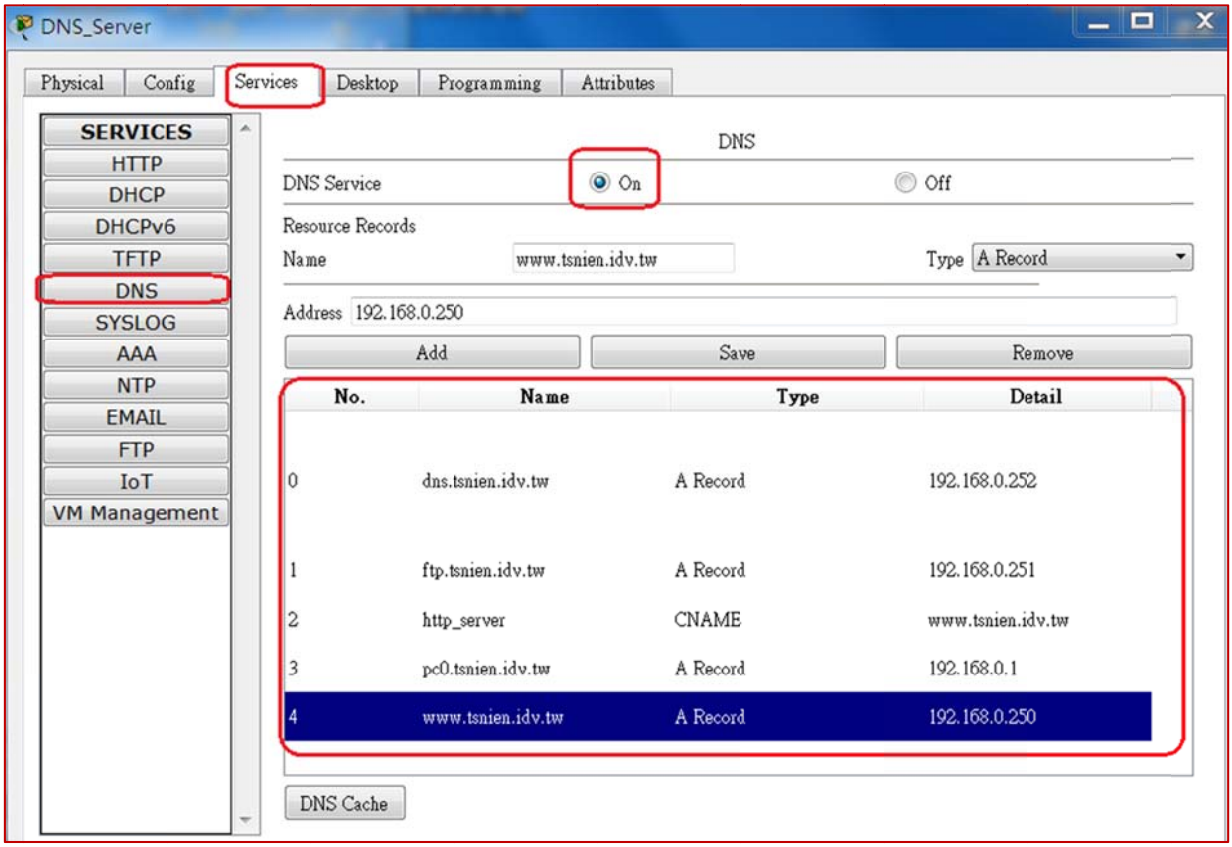



**圖 5-14 DNS 網路系統**

## (B) 伺服器設定與連線

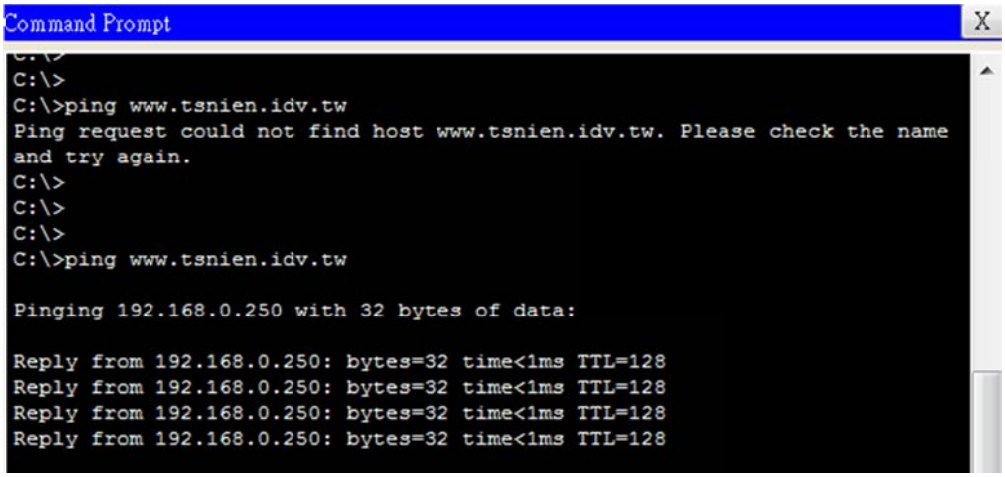
**(1) 步驟 1：**由 DNS_Server 上開啟 DNS 服務，並輸入下列資源紀錄。說明如下：



- Name = dns.tsnien.idv.tw、Type = A Record、Address = 192.168.0.252
- Name = ftp.tsnien.idv.tw、Type = A Record、Address = 192.168.0.251
- Name = www.tsnien.idv.tw、Type = A Record、Address = 192.168.0.250
- Name = pc0.tsnien.idv.tw、Type = A Record、Address = 192.168.0.1
- Name = http_server、Type = CNAME、Host Name = www.tsnien.idv.tw

**(2) 步驟 2：**於 PC0 上開啟 Desktop => Command Prompt，並輸入：

- > ping www.tsnien.idv.tw => OK
- > ping dns.tsnien.idv.tw => OK
- > ping ftp.tsnien.idv.tw => OK




**(3) 步驟 3：**於 Http_Server 上開啟 Desktop => Command Prompt，並輸入：

- > ping pc0.tsnien.idv.tw => OK

## 5-3-8 DNS 協定分析

一般主機透過 DNS 伺服器詢問網域名稱的相對應 IP 位址之後，會將結果儲存 DNS Cache 內，下次遇到相同的網域名稱，就不需要發動 DNS 詢問程序，直接取用即可。在 Windows 系統下可執行 ipconfig 命令將 DNS Cache 清除，如此才可以強迫主機發動詢問程序，如下：

```
> ipconfig    /fushdns
```

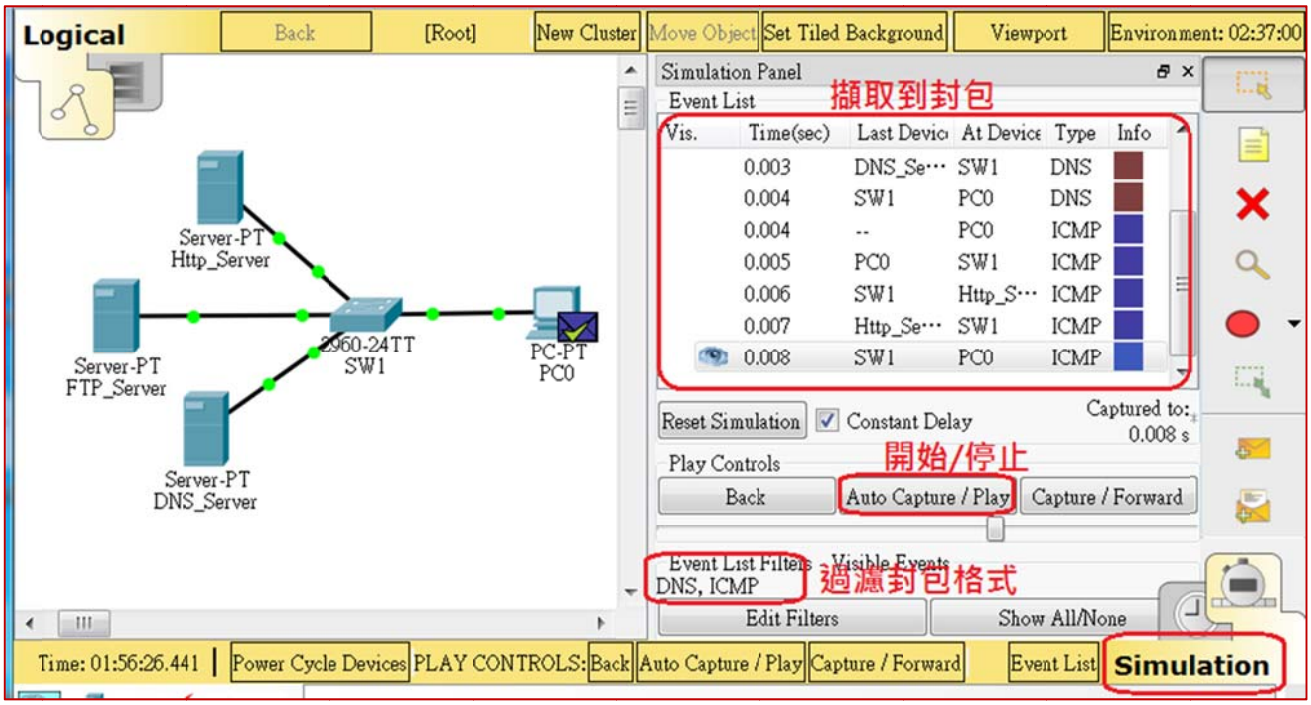
但 Packet Tracer 模擬系統並沒有 DNS Cache 功能，因此，擷取 DNS 封包之前，不需要清除它。

## (A) Packet Tracer 擷取封包

(1) 設定 Packet Tracer 為 Simulation Mode，並擷取 DNS 與 ICMP 封包。

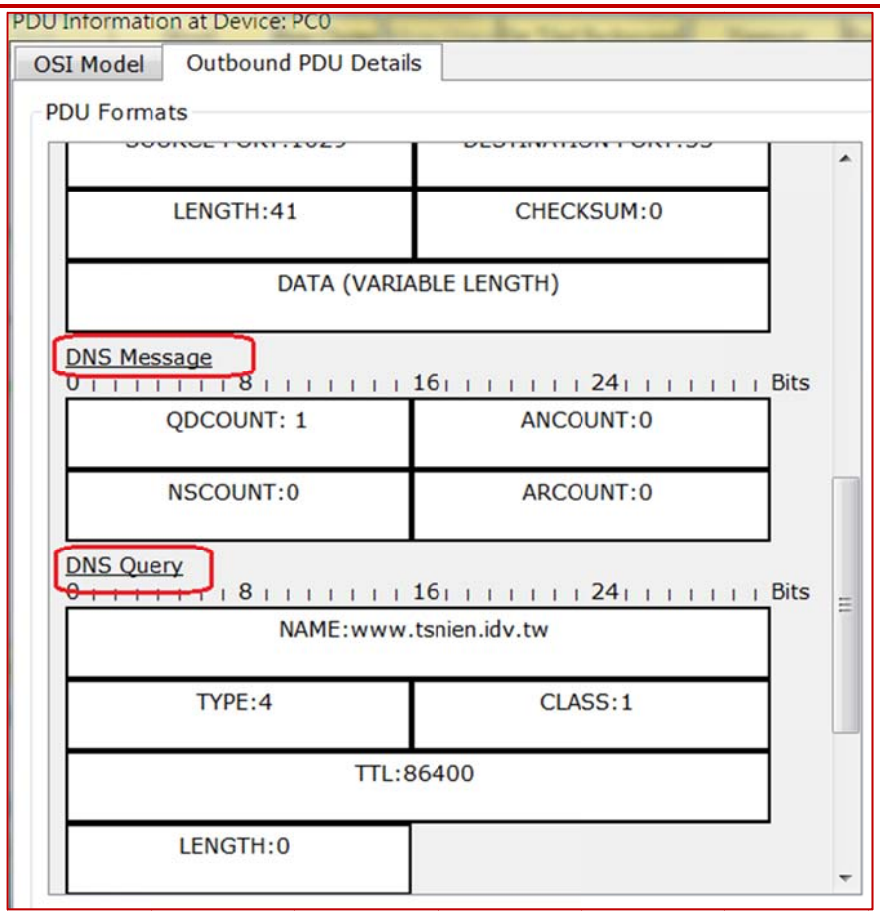
(2) 由 PC0 上開啟 Desktop => Command Prompt，並輸入：> ping www.tsnien.idv.tw

擷取到封包如下圖：




## (B) DNS Query 封包

此封包是 PC0 向 DNS Server (192.168.0.252) 詢問 URL = www.tsnien.idv.tw 的 IP 位址如何？

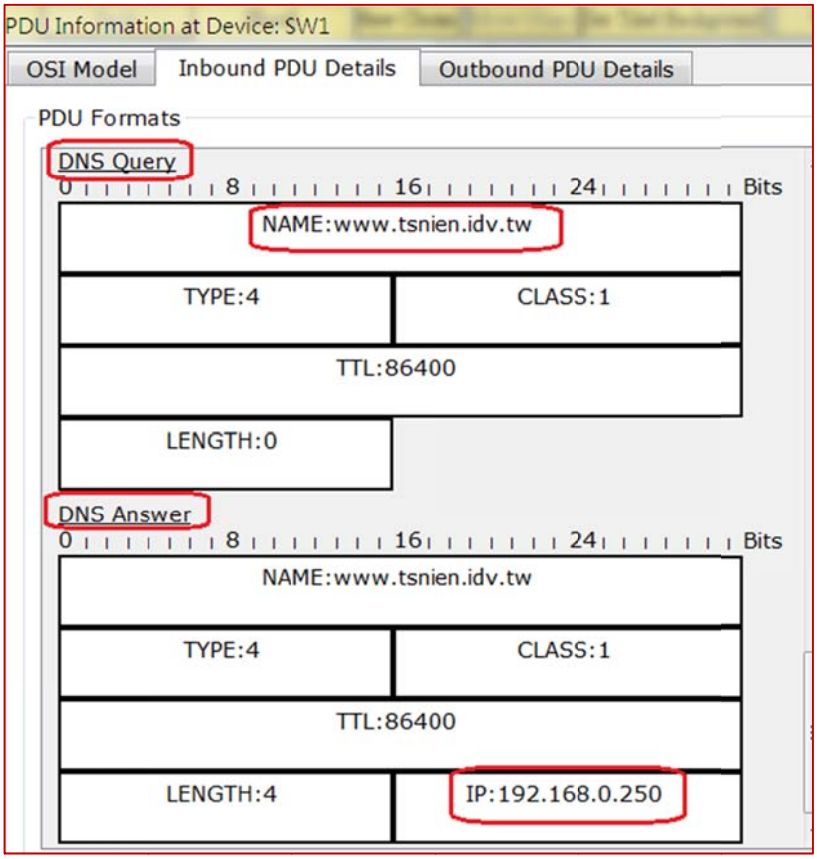



得到下列結果：

- IP 標頭：PRO = 0x11(UDP)、SRC IP = 192.168.0.1、DES IP = 192.168.0.252。
- UDP 標頭：Source Port = 1029、DES Port = **53**。
- DNS Message 標頭
- DNS Query：NAME：www.tsnien.idv.tw、Type = 4、Class=1。

## (C) DNS Answer 封包

此封包是 DNS Server 回應 PC0 詢問的封包。

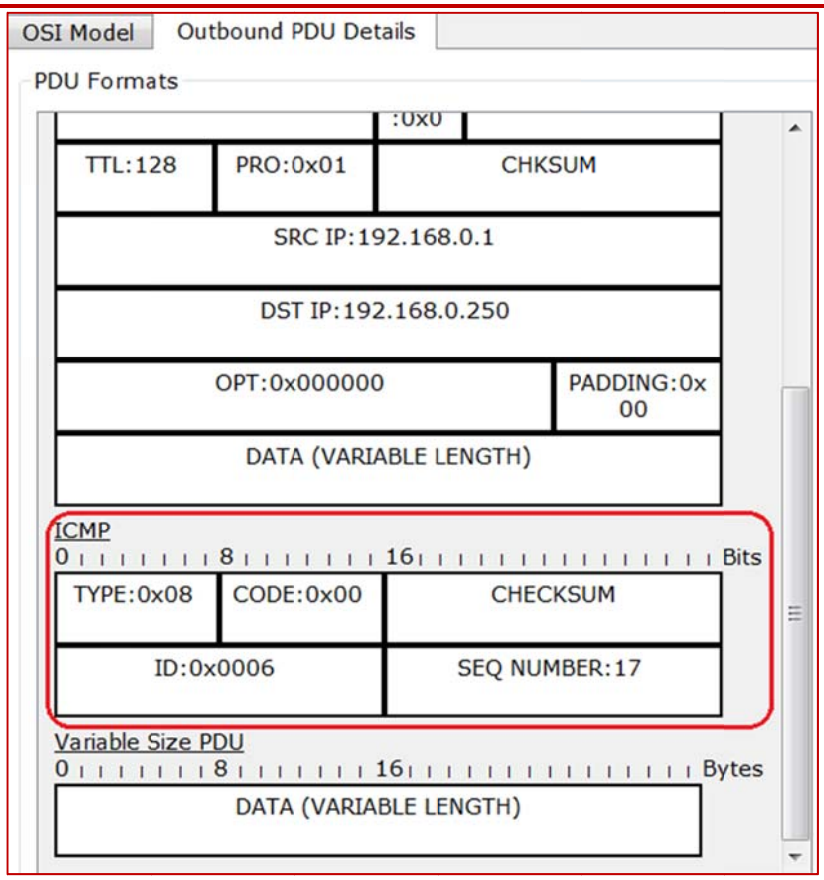



得到下列結果：

- IP 標頭：PRO = 0x11(UDP)、SRC IP = 192.168.0.252、DES IP = 192.168.0.1。
- UDP 標頭：Source Port = 53、DES Port = **1029**。
- DNS Message 標頭
- DNS Query：NAME：www.tsnien.idv.tw、Type = 4、Class=1。
- DNS Answer： NAME = www.tsnien.idv.tw、IP = 192.168.0.250

## (D) ICMP/ping 封包

當 PC0 得到 www.tsnien.idv.tw 網址相對應的 IP 位址後，則利用此 IP 位址發送 ICMP，擷取封包內容如下：




得到下列結果：

- IP 標頭：PRO = 0x01(ICMP)、SRC IP = 192.168.0.1、DES IP = 192.168.0.250。
- ICMP 標頭：TYPE=0x08。( Echo Request)

# 5-4 動態主機組態系統

## 5-4-1 DHCP 系統簡介

### (A) 分配 IP 位址與提供網路參數

『動態主機組態協定』(Dynamic Host Configuration Protocol, HDCP) 系統是伺服端提供客戶端相關網路參數，如『**IP address、Netmask、DNS address、Default Gateway、、、**』等相關網路位址。一般主機網路參數有：靜態設定(Static) 與動態設定(Dynamic) 兩種模式，如選用 Static mode，則必須直接輸入上述相關參數；如設定 Dynamic Mode (或 DHCP mode)，則主機開機時，會自動到網路上尋找 DHCP 伺服器，並要求給予相關參數，取得之後再自動設定。然而，主機啟動之後，如何與 DHCP 伺服器溝通取得網路參數的運作，則須仰賴 HDCP 協定的運作。

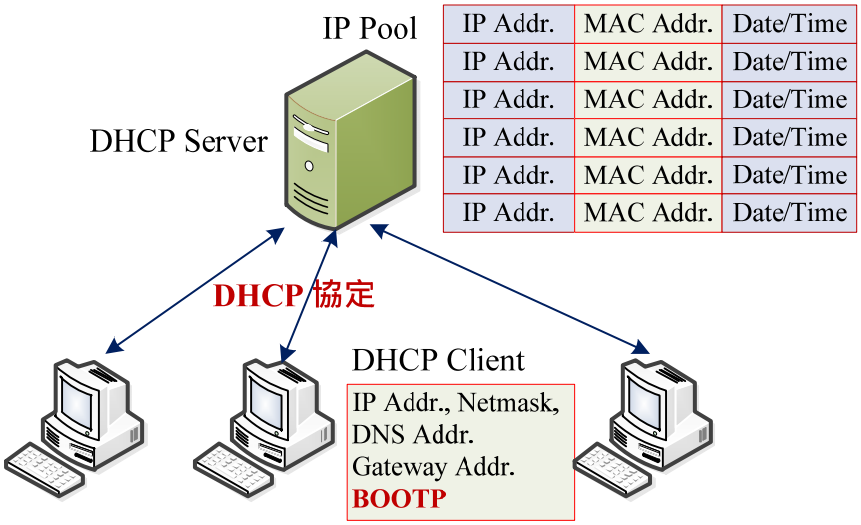



圖 5-15-1 DHCP 系統功能

### (B) 提供網路啟動

DHCP 伺服器除了分配 IP 位址與網路參數外，也提供網路啟動的功能，即是『Bootstrap Protocol (BOOTP)』。有些主機為了安全起見，並沒有安裝啟動硬碟，或甚至沒有硬碟，則它網路卡上安裝有 BOOT ROM，起動時會向 DHCP 伺服器要求開機程式位址，DHCP 伺服器會給予一個 Boot file，並讓它取得開機程式。但此類型 DHCP 伺服器大多不支援 IP 分配，因它分配 IP 位址之後，租約期限將無上限。

## 5-4-2 DHCP 協定運作

DHCP 協定是提供伺服端與客戶端之間，協議動態 IP 位址的分配，並幫客戶端指定 default gateway、DNS Server 位址、WINS Server 等參數。當主機啟動後，**第一次登錄運作程序**如圖 5-15 所示，說明如下：

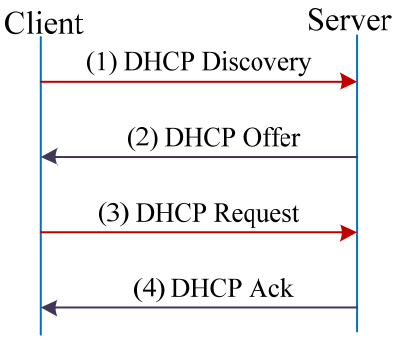



圖 5-15 DHCP 運作程序

### (A) 尋找 DHCP 伺服器：DHCP Discovery

當主機啟動時，發現本機並沒有指定靜態 IP，以及相關參數，而是動態分配網路參數時，它便發出 DHCP Discovery 封包廣播到網路上，詢問 DHCP 伺服器在哪裡。此時客戶端還不知道是屬於哪一個網路區段，因此來源位址設定為 0.0.0.0，目的位址設定為 255.255.255.255。然而，伺服端埠口位於 67/udp，客戶端是 68/udp。

### (B) 提供 IP 組用位址：DHCP Offer

當 DHCP Server 監聽到 DHCP Discovery 時，便會回應一個 DHCP Offer 訊息給客戶端，也許網路上有多個 DHCP Server，客戶端同時收到多個 Offer 訊息，大多以最早收到的訊息為主。當 DHCP Server 發出訊息之前，它會在 IP Pool 內尋找一個空閒的 IP 位址，**再利用 ARP 封包廣播到網路上**，探測是否此 IP 是否已被使用中。如果沒有主機回應此 ARP 封包，則表示未被使用，則連同其他相關參數，包裝成 DHCP Offer 廣播到網路上，並指定客戶端的 HW 位址(Ethernet 位址)為目的位址。

### (C) 接受 IP 租約：DHCP Request

客戶端收到 DHCP Offer 封包後，由封包內取出被分配的 IP 位址，並利用 ARP 封包探測此 IP 位址是否被使用，如果沒有則發出 DHCP Request 封包給 Server 端，要求使用此 IP 位址；如果發現此 IP 位址已被使用，則回應 DHCP Decline 訊息給 Server 端，並拒絕使用。

### (D) 租約確認：DHCP Ack

當 DHCP Server 收到客戶端的 DHCP Request 後，會對客戶端發出 DHCP Ack 訊息，表示租約 IP 正式有效，並開始使用。

客戶端收到 DHCP Ack 之後，表示確定可以使用該 IP 位址，但它也**再利用 ARP 封包廣播到網路上**，探測是否此 IP 是否已被使用中。真的沒有其他主機使用，才繼續使用該 IP 位址。

### (D) 租約有效期限：DHCP Request/DHCP Ack

當客戶端取得 IP 位址之後，除非租約失效而且 IP 位址也重新設定為 0.0.0.0，否則無須再發送 DHCP Discovery 尋找 DHCP 伺服器。當取得 IP 位址主機重新啟動時，它直接發送 DHCP Request 並之前取得的 IP 位址，發送給之前的 DHCP Server，收到 DHCP Server 回應 DHCP Ack 訊息表示可以繼續使用，如收到 DHCP Nack，則表示需重新發送 DHCP Discovery 尋找 DHCP Server 要求給予服務。

## 5-4-3 DHCP 封包格式

在 DHCP 協定運作當中各種封包 (DHCP Discovery/Offer/Request/Ack 等等)封裝格式大致相同，僅內部參數欄位識別而已。另外 DHCP 封包係利用 IP + UDP 封包包裝，客戶端埠口位於 68/udp，伺服端在 67/udp 埠口。因客戶端未取得 IP 位址以前，都是用 0.0.0.0 表示，又不知道伺服端 IP 位址，皆採用廣播位址 255.255.255.255。圖 5-15-1 為 UDP 包裝 DHCP 封包格式，說明如下

| Ethernet Header | IP Header | UDP Header | HDCP Header/Body |
|---|---|---|---|
| Des.MAC<br>Source MAC<br>Type = 0x0800 | Protocol = 17<br>Source IP<br>Dest. IP<br>... | Source Port<br>Dest. Port<br>Port =67/68 | |

圖 5-15-2 DHCP Over UDP 封包包裝

- **IP Header：**
  - **Protocol ID = 17**
  - **Source IP：**DHCP Client 還未有 IP 之前設定為 0.0.0.0。
  - **Destination IP：**DHCP Client 還不知道 DHCP Server 之前設定為 255.255.255.255(廣播位址)。
- **UDP Header：**
  - **Source Port：**DHCP Client = 68，DHCP Server = 67。
  - **Destination：**DHCP Client = 68，DHCP Server = 67
- **DHCP Message Payload：**

如圖 5-15-2 所示。

圖 5-15-2 是 DHCP 封包包裝，各欄位說明如下：

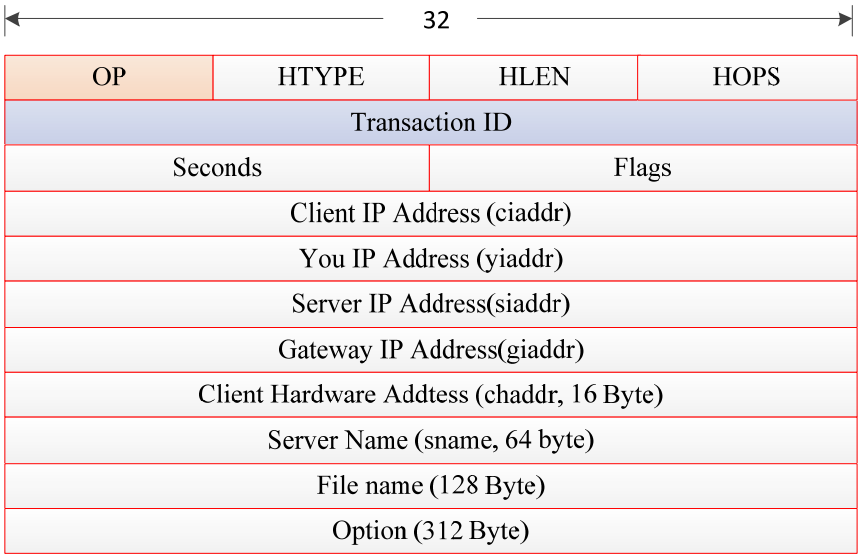



**圖 5-15-3 DHCP 封包格式**

各欄位說明如下：

- **OP**：辨識 DHCP Request (OP = 1)或 DHCP Response (OP = 0)。
- **HTYPE**：硬體類別。Ethernet HW 為 1。
- **HLEN**：硬體位址長度。Ethernet HW 為 6。
- **HOPS**：累計封包經過路由器轉送次數，網內為 0。
- **Transaction ID**：DHCP Request 封包序號，DHCP Response 依此序號回應。
- **Seconds**：DHCP Client 啟動時間。
- **Flage**：16 bits。最左邊為 1 表示 Server 廣撥給 Client，其他未用。
- **ciaddr**：Client 想使用之前向 Server 取用的位址。
- **yiaddr**：Server 分配給 Client 的 IP 位址 (DHCP Offer 與 DHCP ACK)。
- **siaddr**：若 Client 需要網路開機 (BOOTP)，則儲存開機程式儲存的 IP 位址 (於 DHCP Offer 或 DHCP Ack 封包內)。

- **giaddr**：若需跨網域進行 DHCP 請求時，此欄位為 Relay Agent 位址。
- **chaddr**：Client 的硬體位址(Ethernet 位址)。
- **sname**：Server 的名稱字串，以 0x00 結尾。
- **file**：若 Client 需要網路開機，則儲存開機程式的檔案名稱。
- **Option**：提供更多設定資訊，如 NetMask、Gateway、DNS 、、等等。每一筆資料以 Code、LEN、Value 等三個欄位填寫，如圖 5-15-3 所示。


圖 5-15-4 DHCP Option 欄位格式

更重要的，DHCP 封包還利用此欄位來辨識封包格式，如表所示。(節錄)

| CODE | Value | DHCP 封包類別 |
|---|---|---|
| 53 | 1 | DHCP Discovery |
| 53 | 2 | DHCP Offer |
| 53 | 3 | DHCP Request |
| 53 | 4 | DHCP Decline |
| 53 | 5 | DHCP Ack |
| 53 | 6 | DHCP Nack |
| 53 | 7 | DHCP Release |

另外，DHCP Option 也可當 DHCP Offer 封包存放存放網路參數的位置，客戶端發送 DHCP Request 攜帶網路參數尋求伺服端同意否。網路訊息編號如下：

| CODE | Value | DHCP 封包類別 |
|---|---|---|
| 01 | 255.255.255.0 | Sub-net mask = 255.255.255.0 |
| 03 | … | Router Address |
| 06 | 168.95.1.1 | DNS Address = 168.95.1.1 |
| 0F | tsnien.idv.tw | Domain name = tsnien.idv.tw |
| 2C | … | WINS Server Address |

## 5-4-4 DHCP 系統規劃與建置

## (A) 系統分析

吾人利用 Packet Tracer 建置一套 DHCP 模擬系統，需要下列兩個主要設備，如下：

(1) DHCP 伺服器：提供動態 IP 分配的功能。

(2) PC-PT 主機：網路參數選擇動態分配。

## (B) 規劃網路架構

我們利用 Cisco Packet Tracer 規劃與建置 DHCP 伺服系統，來觀察它的運作模式吾人需選擇下列元件來建置：

(1) Server-PT：模擬伺服器主機。選用 4 只，包含：HTTP_Server 、FTP_Server、DNS_Server 與 DHCP_Server，其中包含靜態位址分配。

(2) PC-PT：模擬客戶端主機。選用 PC0 與 PC1 客戶端兩只。

(3) 2960-24TT。選用 1 只，為各主機之間連線使用。

主機的 IP 位址設定與埠口位置，如下所示：

| 裝置 | URL 名稱 | IP 位址 | 連接埠口 |
|---|---|---|---|
| DHCP Server | | 192.168.0.253 | SW1(fa0/21) |
| PC0 | | DHCP 動態分配 | SW1(fa0/1) |
| PC1 | | DHCP 動態分配 | SW1(fa0/2) |
| 整體環境 | Gateway = 192.168.0.254、DNS = 192.168.0.252 | | |

依照上述參數建置網路如下：**[請下載：DHCP Server 系統.pkt]**

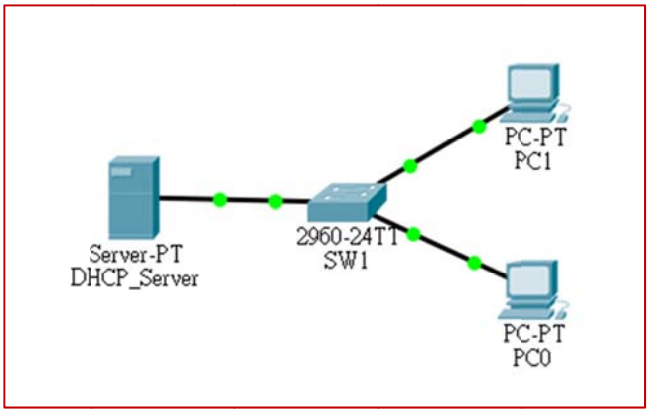
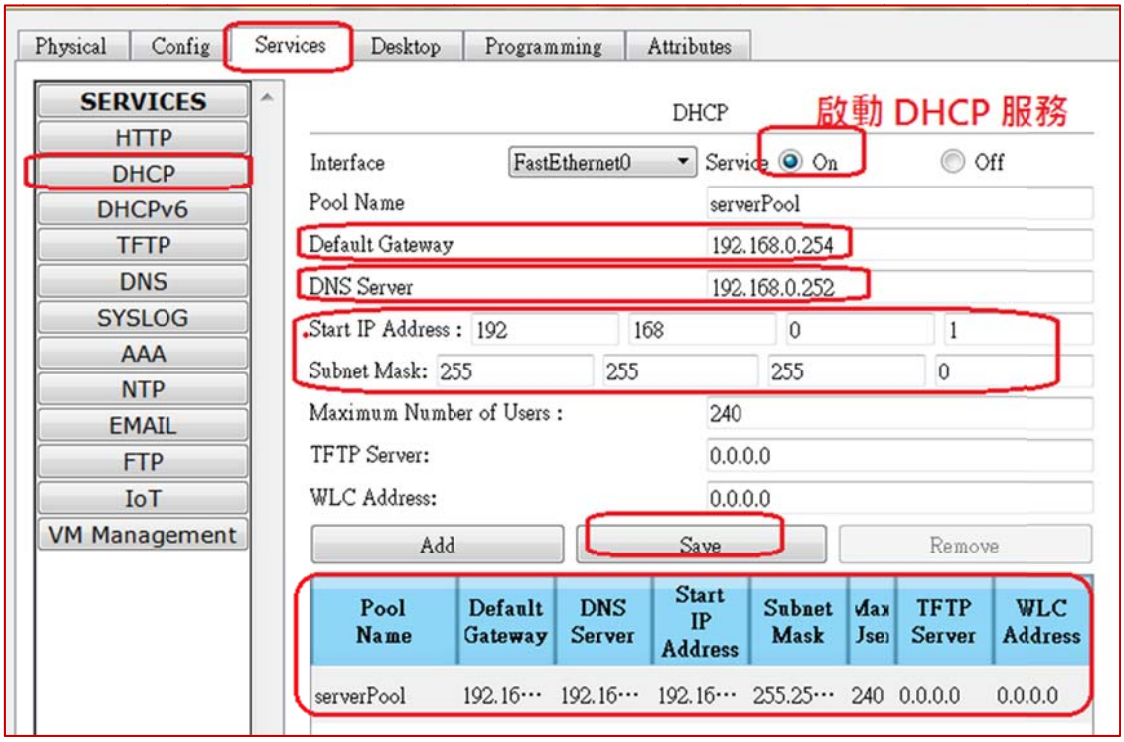


圖 5-16 DHCP 網路系統

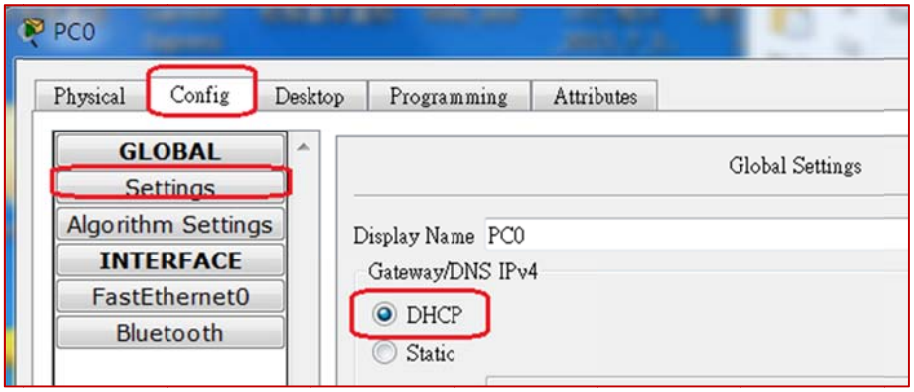
## (C) DHCP 伺服器設定

**(1) 步驟 1：**由 DHCP_Server 上開啟 DHCP 服務，並輸入 IP 指定範圍，以及 Default Gateway 與 DNS 位址。如下：

- Default Gateway = 192.168.0.254
- DNS = 192.168.0.252
- IP 範圍：192.168.0.1 ~ 192.168.0.240 (其餘保留靜態設定)
- Subnet Mask = 255.255.255.0




**(2) 步驟 2：**於 PC0 與 PC1 設定成 DHCP 取得網路參數，如下： 上開啟 Desktop => Command Prompt，並輸入：



**(3) 步驟 3：**於 PC0 上開啟 Desktop => Command Prompt，並輸入 **c:\> ipconfig**，如下：

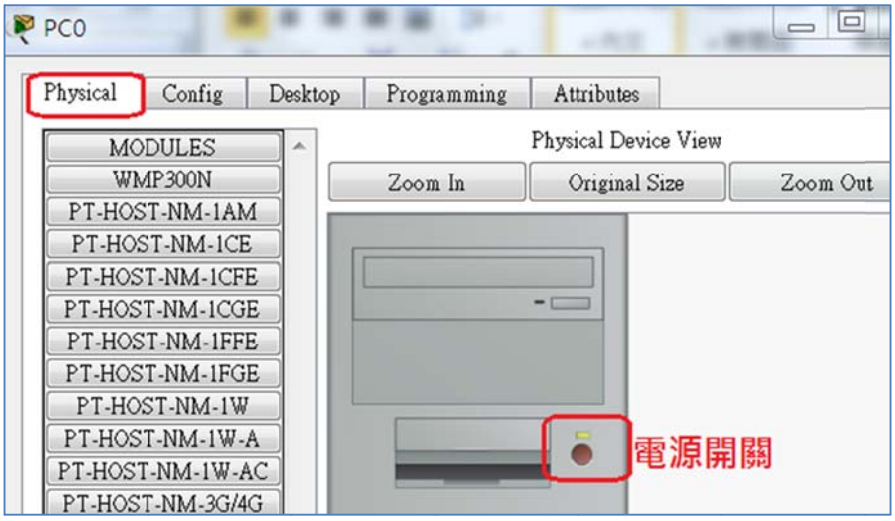
```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::2E0:A3FF:FEDD:30D9
   IP Address.....: 192.168.0.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.0.254

C:\>
```

- 查詢得知，PC0 被分配的 IP 位址為 192.168.0.1，以及相關參數，並測試與 DHCP Sever 之間連線，如下
  - > ping 192.168.0.253　　=> **OK**

## 5-4-5 DHCP 協定分析

### (A) PC0 主機關機/開機

當主機啟動時，會立即發出 DHCP Discovery 訊息尋找 DHCP Server。因此，吾人必須將主機關機，在它開機時擷取 DHCP 相關封包。譬如選擇 PC0 關機，則點選 PC0 -> Physical，將開關關閉，如下：



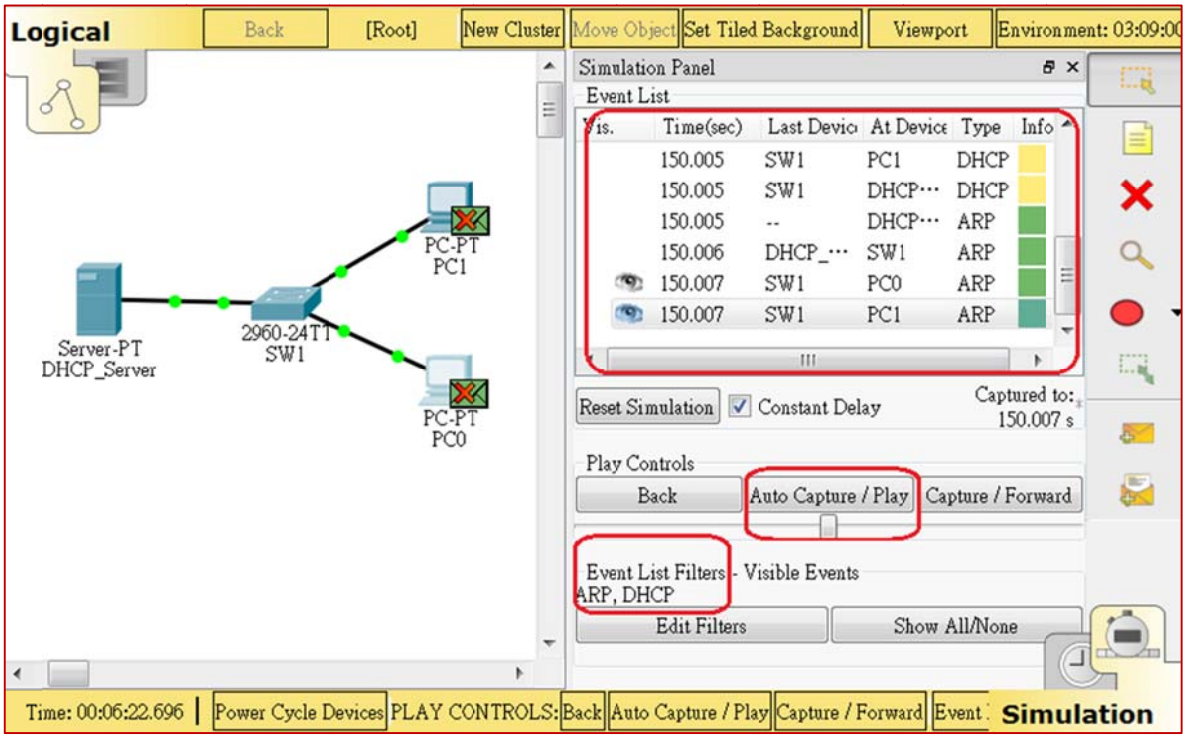

也可執行 ipconfig /release 釋放網路參數，再執行 ipconfig /renew 重新要求分配 IP 位址，如下：

```
C:\>ipconfig /release

   IP Address.....................: 0.0.0.0
   Subnet Mask....................: 0.0.0.0
   Default Gateway................: 0.0.0.0
   DNS Server.....................: 0.0.0.0

C:\>ipconfig /renew

   IP Address.....................: 192.168.0.1
   Subnet Mask....................: 255.255.255.0
   Default Gateway................: 192.168.0.254
   DNS Server.....................: 192.168.0.252
```

## (B) Packet Tracer 擷取封包

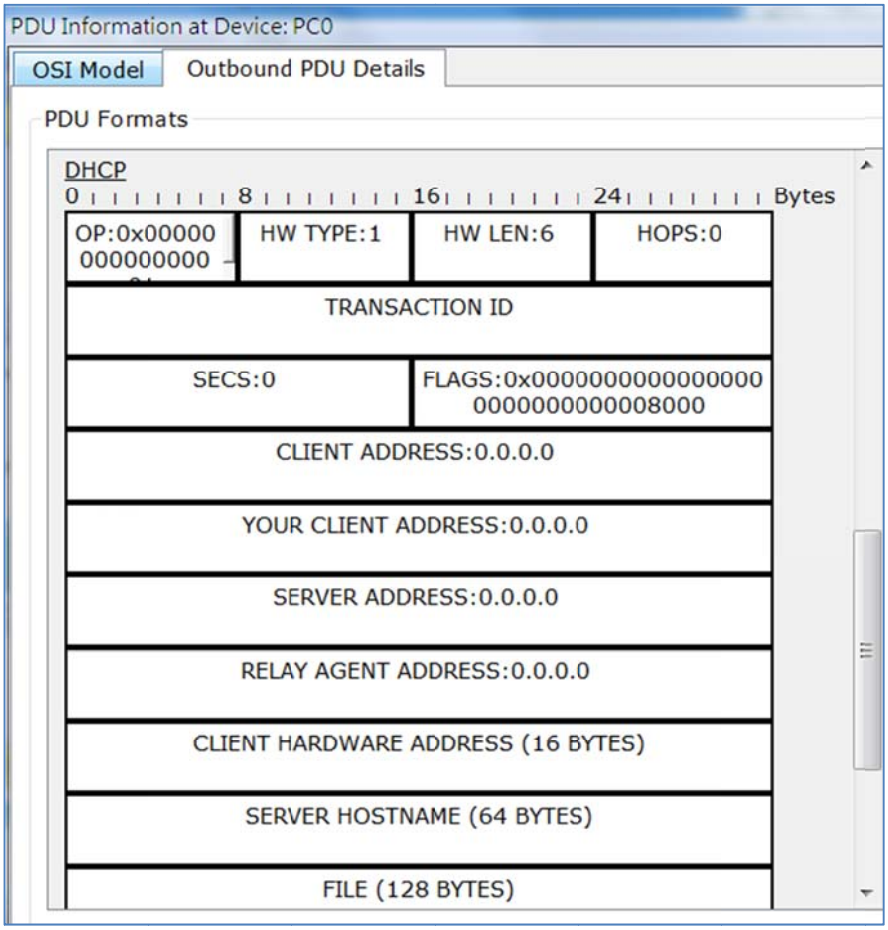
(1) 設定 Packet Tracer 為 Simulation Mode，並擷取 ARP 與 DHCP 封包。

(2) 再開啟 PC0 主機電源，於 Packet Tracer 上按下 Auto Capture/Play，擷取到封包如下圖：




## (C) DHCP Discovery 封包

此封包是 PC0 開機後，發出尋找 DHCP Server 之封包。

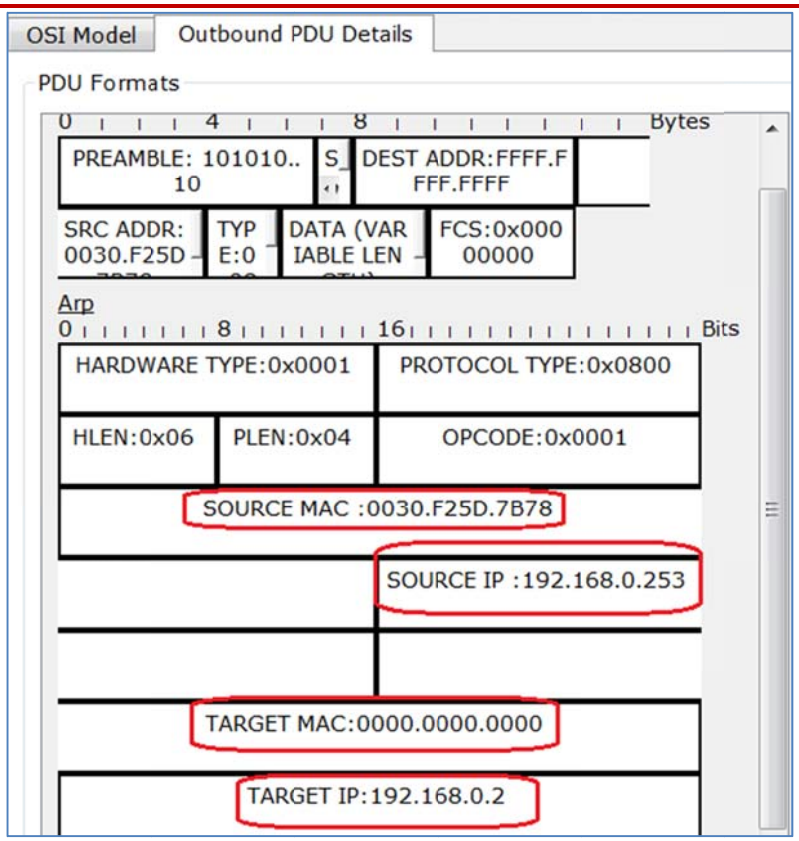



得到下列結果：

- IP 標頭：PRO = 0x11(UDP)、SRC IP = 0.0.0.0、DES IP = 255.255.255.255。(廣播封包)
- UDP 標頭：Source Port = 68、DES Port = **67**。
- DHCP 標頭：空白未填入。
- DHCP Client Identifier Option：Client 端(PC0)的 Ethernet Address。

## (D) ARP query 封包

DHCP Server 尋找一個 IP 位址(192.168.0.2)後，發出 ARP 封包詢問是否有其他主機使用此 IP 位址。




得到下列結果：

- ARP 標頭：SRC IP = 192.168.0.253、Target IP = 192.168.0.2。)

### (E) DHCP Offer/Request/Ack 封包

請自行擷取分析。

# 5-5 電子郵件系統

## 5-5-1 E-mail 系統簡介

圖 5-17-1 為 E-mail 系統的架構圖，包含下列元件所構成：

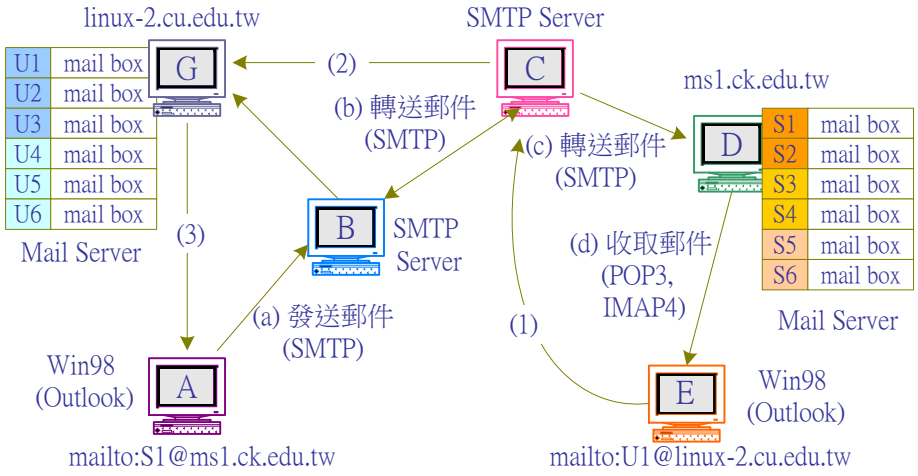



圖 5-17-1 E-mail 系統架構圖

## （A）郵件伺服器 - POP3 Server

『郵件伺服器』( Mail Server ) 的功能如同一般郵局的郵政信箱一樣，將遠端所傳送過來的信件存入信箱內，受信者再到信箱內索取信件。收信端電腦和郵件伺服器間必須透過標準協議來通訊，目前使用最普遍的是 POP 和 IMAP 協定，因此，一般郵件伺服器也稱之為『POP Sever』或『IMAP Server』。

『郵局協定』( Post Office Protocol, POP ) 的功能和一般郵政系統的郵政信箱非常類似，目前大多使用第三版本 ( Version 3 )，一般以『POP3』稱呼之。POP3 協定用於客戶端電腦和郵件伺服器之間的通訊，讓使用者可以從郵件伺服器上下載信件，它的功能就如同使用者到郵局的信箱索取信件一樣。

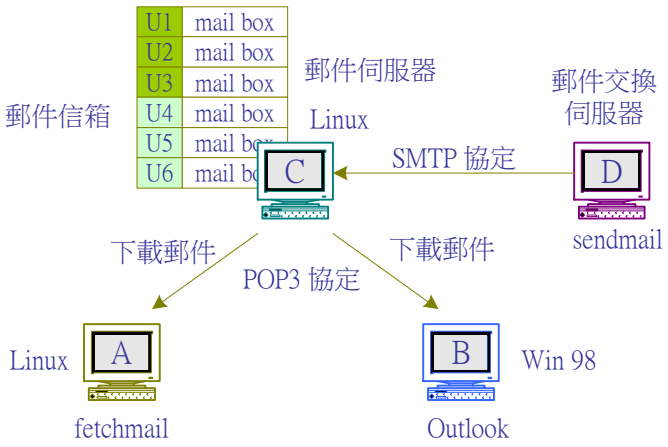



圖 5-17 POP3 協定

## （B）郵件伺服器 - IMAP Server

『交談式郵件存取協定』( Interactive Mail Access Protocol, IMAP ) 是提供客戶端電腦和郵件伺服器之間通訊使用，讓使用者直接登入郵件伺服器，從事郵件存取的工作 ( 閱讀或刪除 )。IMAP 和 POP3 有很大的不同點，前者是直接在郵件伺服器上處理信件；而後者是直接將信件下載到客戶端電腦，使用者再由客戶端電腦處理信件。

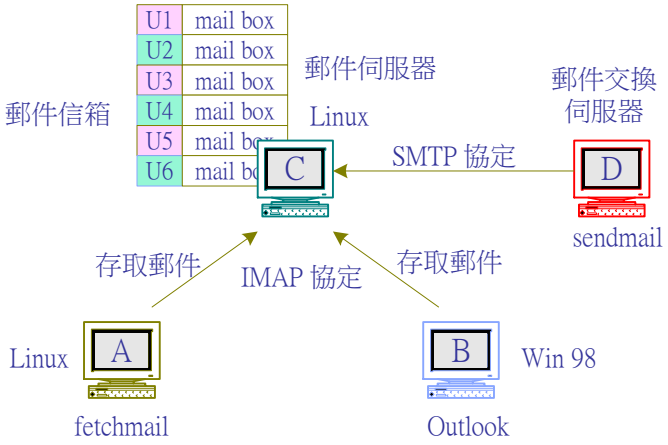



圖 5-18 IMAP Server 服務

## ( C ) 郵件交換伺服器 – SMTP 協定

郵件在網路上也許會經由若干個『郵件交換伺服器』( Mail Exchange Server ) 的轉送，才會到達目的端的郵件伺服器 ( 如 POP Server )。另一方面，傳送端也需要一部郵件交換伺服器來負責傳送信件。因此，在客戶端和郵件交換伺服器之間、或是信件轉送中的郵件交換伺服器之間，需要一個共通協定來通訊，目前最廣泛使用的是『簡易郵件傳輸協定』( Simple Mail Transfer Protocol, SMTP )，也因此，一般郵件交換伺服器稱之為『SMTP Server』。SMTP Server 的功能如同郵局收發信件一樣。如圖 14-1 所示，客戶端 ( Outlook ) 將信件發送到 SMTP 伺服器，再由此 SMTP 伺服器轉送到其它 SMTP 伺服器或郵件伺服器。目前 SMTP 伺服器大多以 Sendmail 郵件軟體安裝而成。

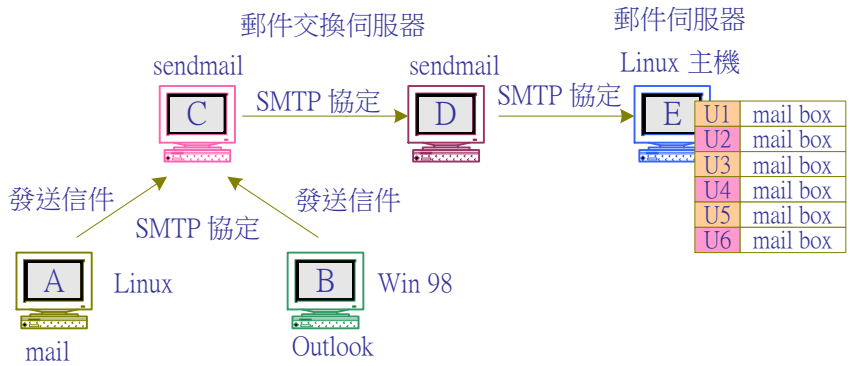


圖 5-19 SMTP Server 服務

### （C）郵件地址

郵件伺服器上都會依照使用者名稱，將每一使用者建立一個獨立信箱，以接收該使用者的信件，稱之為『**郵件信箱**』(**Mail Box**)。一般 Unix/Linux 系統建立使用者後，大多會針對每一個使用者安裝信箱，並以使用者名稱命名。郵件信箱的命名方式是『**使用者名稱**』『**@**』『**主機名稱**』，譬如在某一郵件伺服器（linux-2.cu.edu.tw）上的使用者（U1），而它的郵件信箱為：

**U1@linux-2.cu.edu.tw**

其中，『**@**』表示『**at**』(**在**)的意思，這就是一般所稱的『**E-mail 位址**』。如果郵件伺服器是一個合法的網域名稱位址，則該伺服器下的 E-mail 位址，便可以通行世界各地了。

### （E）DNS 網址解譯

另外，所有郵件地址都是用網域名稱(Domain Name)，不允許直接使用 IP 位址來表示，也就是不允許『user01@192.168.0.220』方式。因此，E-mail 系統一定需要 DNS 來解譯網域名稱，運作方式如下所示。

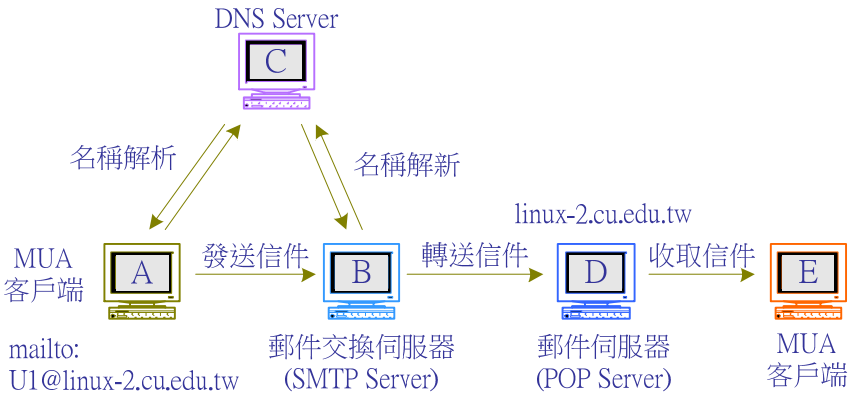



圖 5-20 E-mail 系統元件

## 5-5-2 E-mail 系統規劃與建置

### (A) 系統分析

吾人利用 Packet Tracer 建置一套 E-mail 模擬系統，需要下列三個主要設備，如下：

(1) DNS 伺服器：電子郵件的網址並無法直接使用 IP 位址，而必須使用網域名稱，因此需要一只 DNS Server 將網址解譯成 IP 位址。

(2) SMTP 伺服器：此伺服器具有轉送郵件的功能，即是使用者將郵件傳送到 SMTP Server，它再將郵件上的目地地址，傳送到適當郵件伺服器上。使用者主機與伺服器之間，就是透過 SMTP 協議，來協商傳送郵件相關程序。

(3) POP3 伺服器：此為郵件儲存的伺服器。在此伺服器上建立若干個帳戶名稱，每一個帳戶皆有一個專屬信箱，當郵件轉送過來時，則存放於信箱內。使用者電腦再以 POP3 協定到此信箱上下載信件。

基本上 SMTP Server 具有轉送信件的功能，但 Packet Tracer 模擬 SMTP 伺服器並不具有此功能，因此，只能當作傳送與接收信件。

## (B) 網路規劃與建置

我們利用 Cisco Packet Tracer 規劃與建置網頁系統，來觀察它的運作模式吾人需選擇下列元件來建置：

(1) Server-PT：模擬伺服器主機。選用 2 只，一只開啟 SMTP 與 POP3 服務，另一只開啟 DNS 服務。

(2) PC-PT：模擬客戶端主機。選用 user01 與 User02n 客戶端兩只。

(3) 2960-24TT。選用 2 只，一只為伺服端，另一只為客戶端連線。。作為連結 Server-PT 與 PC-PT 的設備。

主機的 IP 位址設定與連接埠口位置，如下表所示：

| 裝置 | URL 名稱 | IP 位址 | 連接埠口 |
|---|---|---|---|
| SMTP_Server | smtp.tsnin.idv.tw | 192.168.0.251 | SW1(fa0/23) |
| POP3_Server | pop3.tsnien.idv.tw | 192.168.0.251 | SW1(fa0/23) |
| DNS_Server | dns.tsnien.idv.tw | 192.168.0.250 | SW1(fa0/24) |
| User01 | | 192.168.0.1 | SW2(fa0/1) |
| User02 | | 192.168.0.2 | SW2(fa0/2) |
| 整體環境 | Gateway = 192.168.0.254、DNS = 192.168.0.250 | | |

依照上述參數，建置網路如下：**[請下載：E-mail 系統.pkt]**

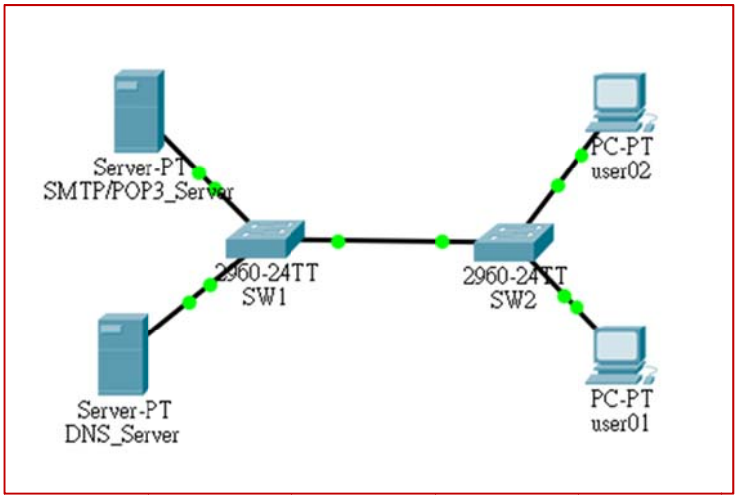
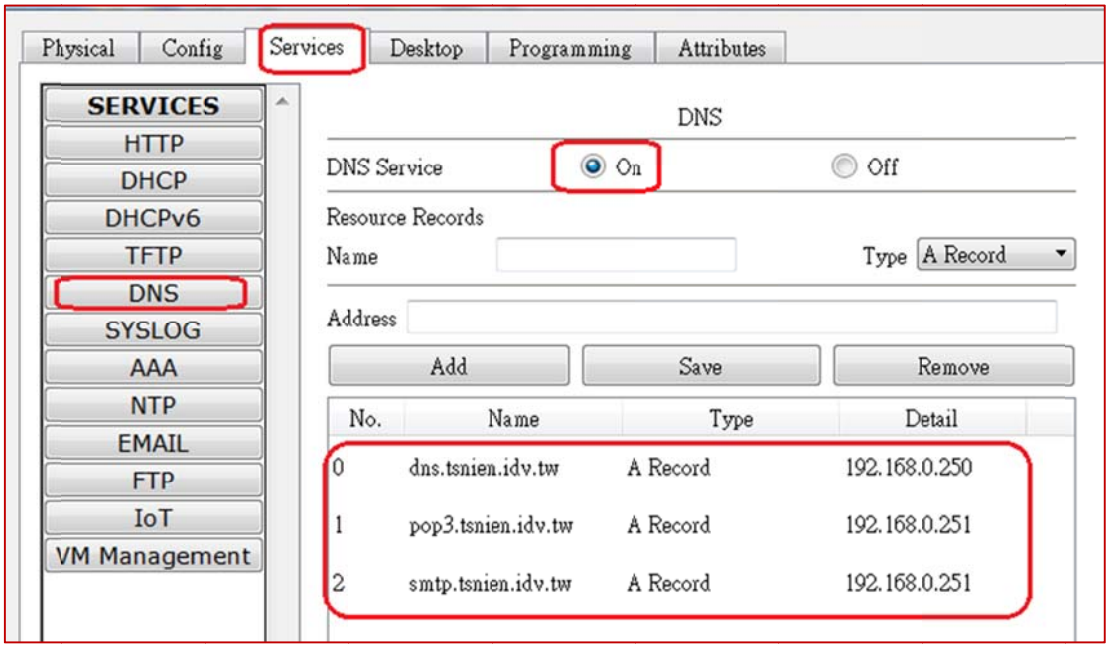



**圖 5-21 E-mail 系統架構**

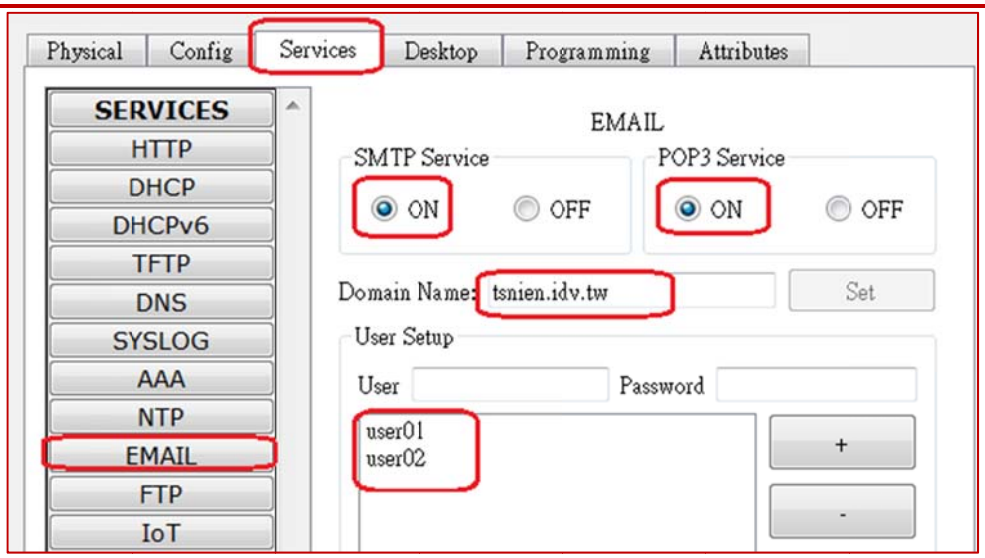
## (C) DNS 伺服器設定

在 DNS_Server 主機上開啟 DNS Service，建立資源紀錄如下：




## (D) SMTP/POP3 伺服器設定

由 SMTP/POP3_Server 上開啟 E-Mail 服務(包含 SMTP 與 POP3 Service)，建立 Domain Name = tsnien.idv.tw，並增加 user01 與 usaer02 等個帳戶(密碼：123456)，則兩帳戶的 E-mail 名稱為 user01@tsnien.idv.tw 與 user02@tsnien.idv.tw。如下：




## 5-5-3 收發信件測試

### (A) user01 發送信件

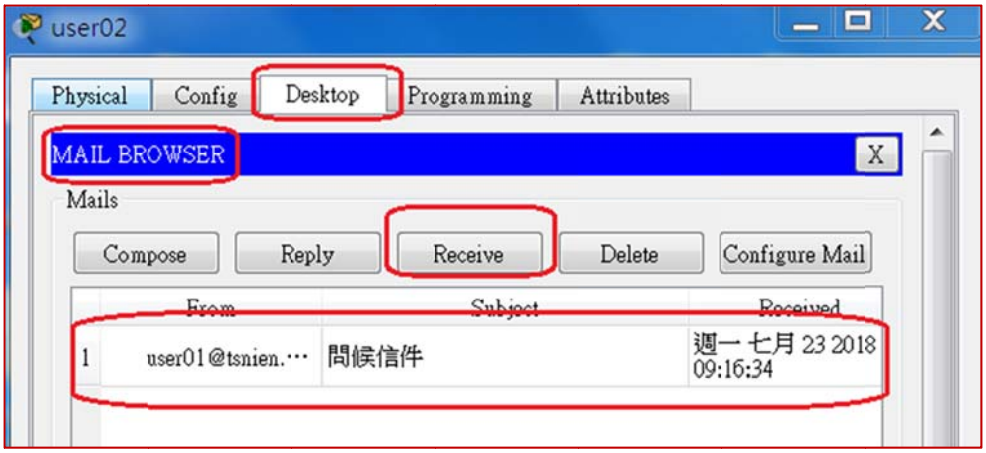
**(1) 步驟 1：**於 user01 主機上設定 E-mail 帳戶為 user01@tsnien.idv.tw，操作方法由 Desktop => Email => Configure Mail，如下：


**(2) 步驟 2：**儲存後，由 user01 發送一封信件給 user02，由 Mail Browser => Compose，如下：


### (B) user02 收取信件

**(1) 步驟 2：**於 user02 主機上設定 E-mail 帳戶為 user02@tsnien.idv.tw，操作方法由 Desktop => Email => Configure Mail (如同 user01 主機設定)。

**(2) 步驟 2：**儲存後於 user02 主機上收取信件，由 Mail Browser => Receive，如下：




## 5-5-4 擷取/分析 SMTP 封包

請自行演練

## 5-5-5 擷取/分析 POP3 協定

請自行演練