

3C-15

# 2015 智慧電子創新應用與設計競賽 智慧電子創新產品說明書

3C 電子創意組

## DHCP snooping on Raspberry Pi

蔡龍佑

黃鴻碩

許嘉修

2015/05/13

## 章 節 目 錄

|                    |    |
|--------------------|----|
| 1. 前言.....         | 6  |
| 2. 創作背景.....       | 6  |
| 3. 系統功能與規格.....    | 8  |
| 3.1. 系統功能.....     | 8  |
| 3.2. 系統硬體建置圖.....  | 8  |
| 3.3. 系統軟體架構圖.....  | 9  |
| 3.4. 系統流程.....     | 9  |
| 3.5. 系統規格.....     | 10 |
| 3.6. 系統軟體關鍵技術..... | 12 |
| 4. 標準的使用.....      | 13 |
| 5. 實現與量產的考量.....   | 14 |
| 6. 結論.....         | 14 |
| 7. 參考資料.....       | 14 |

## 圖 目 錄

|  |    |
|--|----|
| 圖 1 DHCP spoofing 情境 .....                 | 6  |
| 圖 2 DHCP spoofing 封包 .....                 | 7  |
| 圖 3 DHCP snooping 機制 .....                 | 7  |
| 圖 4 具有 Layer2 功能之設備價格 .....                | 7  |
| 圖 5 以 Layer2 網路設備建置 DHCP snooping 環境 ..... | 7  |
| 圖 6 系統硬體建置圖 .....                          | 8  |
| 圖 7 軟體架構圖 .....                            | 9  |
| 圖 8 系統流程 .....                             | 9  |
| 圖 9 Raspberry Pi .....                     | 10 |
| 圖 10 I Watchman 建置情境 .....                 | 11 |
| 圖 11 Raspberry Pi 結合 16 x 2 LCD .....      | 11 |
| 圖 12 Ethernet Type Frame .....             | 12 |
| 圖 13 消耗惡意 DHCP servic 示意圖 .....            | 12 |
| 圖 14 I Watchman 建置 .....                   | 13 |
| 圖 15 I Watchman LCD 獲取 IP .....            | 14 |
| 圖 16 取得正常 DHCP Server IP .....             | 14 |
| 圖 17 I Watchman 設定 .....                   | 15 |
| 圖 18 I Watchman 開始偵測網路 .....               | 15 |

|                                      |    |
|--------------------------------------|----|
| 圖 19 I Watchman 偵測模式 .....           | 16 |
| 圖 20 I Watchman 啟動網路防禦機制.....        | 16 |
| 圖 21 I Watchman 寄送 Email 通知使用者 ..... | 17 |
| 圖 22 I Watchman 居家區域網路防護.....        | 19 |

## 表格 目 錄

|                                     |    |
|-------------------------------------|----|
| 表 1 Raspberry 規格 .....              | 10 |
| 表 2 DHCP Snooping Switch 建置成本 ..... | 19 |
| 表 3 I Watchman 建置成本.....            | 19 |

## 1. 前言

在這個房價高漲人們買不起房屋的世代租屋變的相當普遍，而科技進步網路發達導致網路對於一般人而言已是不可或缺的資源了，但是網路相關的路由器、Switch、Wi Fi 分享器…等，相關設定並不是如此簡易上手，在租屋的區域網路配置下若有人設定錯誤恐導致整個網絡癱瘓無法使用，屋主為避免此問題需加裝具有 DHCP snooping Switch 功能的路由器來解決問題，卻因成本相當高昂，房東或網管業者不願花費高成本購買硬體設備，更趨向於購買成本低廉的 Hub。本文以 DHCP snooping on Raspberry Pi 為主題提出新產品 I Watchman 用較低成本解決此問題。

## 2. 創作背景

身為大學生到外地求學並在外租屋已是常態，在外租屋確實常遇到網路突然無法使用的狀況是非常令人困擾的，然而造成網路終止服務的原因卻是其他租屋的學生，因分不清楚 WLAN 與 LAN 隨意插入網路孔造成網路異常發生 DHCP spoofing(如圖 1)，房東雖可從中架設具有 DHCP snooping 的 Layer 2 Switch 即可解決此問題，但是因本考量而無法付諸行動，因此有了創作 I Watchman 的想法，用更低廉的價格解決此問題。

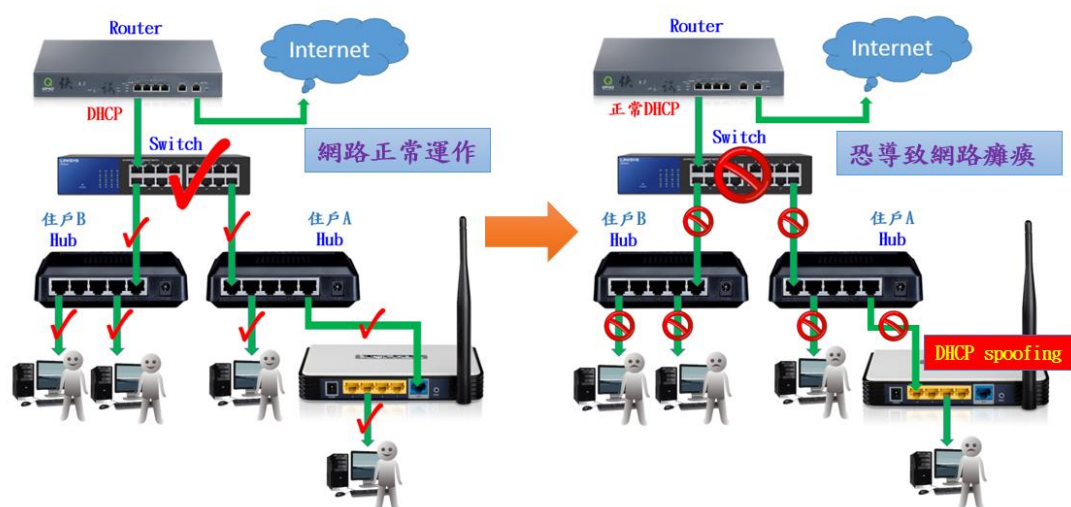
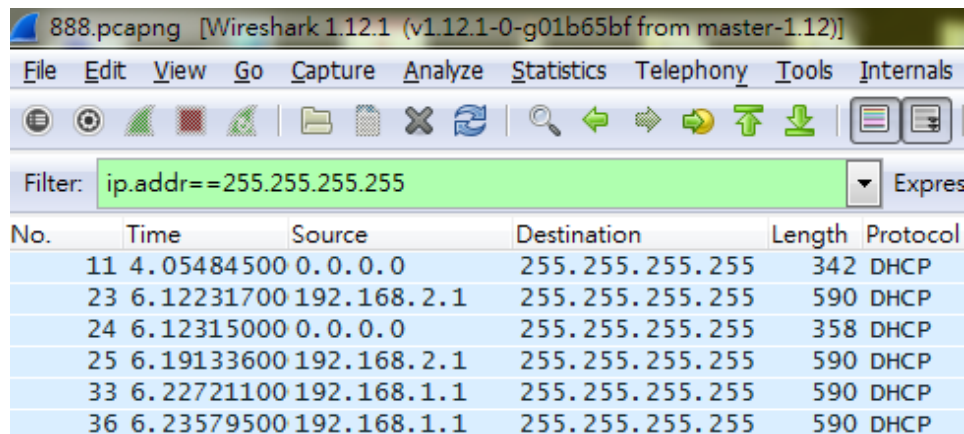


圖 1 DHCP spoofing 情境

DHCP spoofing 所偵測之封包，區域網路正常 DHCP Server 為 192.168.1.1，而在區域網路內卻出現惡意 DHCP Server 為 192.168.2.1，（如圖 2）。



| No. | Time       | Source      | Destination     | Length | Protocol |
|-----|------------|-------------|-----------------|--------|----------|
| 11  | 4.05484500 | 0.0.0.0     | 255.255.255.255 | 342    | DHCP     |
| 23  | 6.12231700 | 192.168.2.1 | 255.255.255.255 | 590    | DHCP     |
| 24  | 6.12315000 | 0.0.0.0     | 255.255.255.255 | 358    | DHCP     |
| 25  | 6.19133600 | 192.168.2.1 | 255.255.255.255 | 590    | DHCP     |
| 33  | 6.22721100 | 192.168.1.1 | 255.255.255.255 | 590    | DHCP     |
| 36  | 6.23579500 | 192.168.1.1 | 255.255.255.255 | 590    | DHCP     |

圖 2 DHCP spoofing 封包

在使用 DHCP 的環境中，終端使用者不循正常方式使用 DHCP，例如：私自架設的 DHCP 伺服器在網路上配發 IP，這種狀況一旦出現，將會造成正常 DHCP 使用者無法連線，然而 DHCP snooping 的功能主要是防止因 DHCP spoofing 而造成的不當 DHCP 租用行為。

DHCP Snooping 原理是 Switch 會監看 DHCP 的活動，只允許指定的 Switch Port 放行 DHCP Server 回應封包，其他的 DHCP Server 一律不准。為解決此惡意 DHCP Server 問題，網路設備廠商在 Layer2 實現 DHCP Snooping 機制（如圖 3）解決此問題。

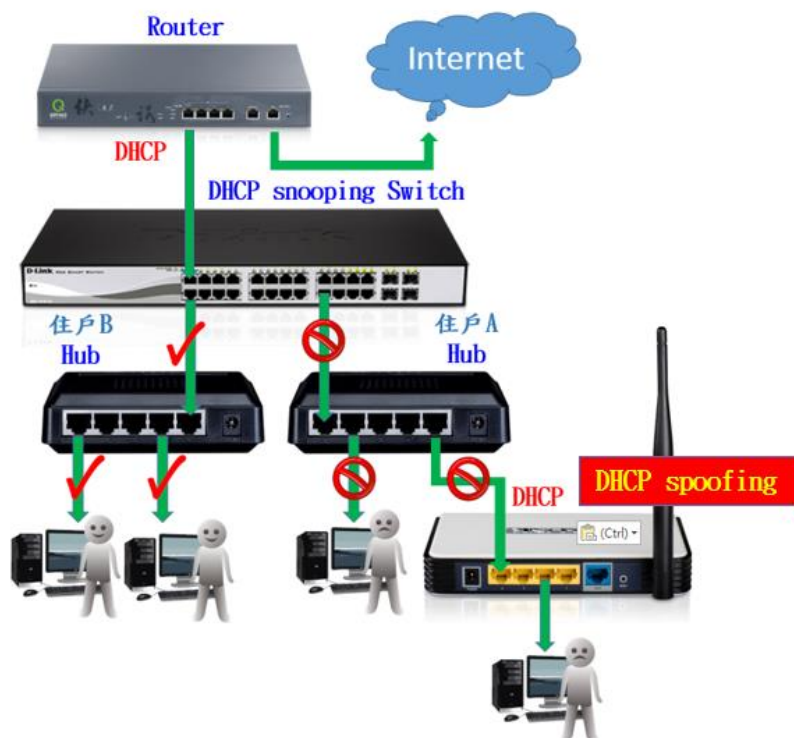


圖 3 DHCP snooping 機制

由於 Layer2 的網路設備(如圖 4)價格相當昂貴，房東或網管業者不願花費高成本購買硬體設備，更趨向於購買成本低廉的 Hub。



**俠諾 DOWNLOOP G24V 24埠GIGA 超高速乙太網路VLAN Switch**

起標價格 **\$7,500** / 0 次出價

出價增額 \$ 100

最高出價者 無

數 量 1 件

立即結標價 \$ 7,500

自動出價 直接出價

**我要出價**

**D-LINK 24埠智慧型Gigabit交換器DGS-1210-24**

建議售價 \$40,290

**\$7,990**

12 期 0 利率 每期 665 元起 分期表>

- DGS-1210-24支援節能功能
- 提供Green Ethernet技術
- 獨特線路偵測技術
- 直覺化ACL設定方式，更易佈建ACL規則

圖 4 具有 Layer2 功能之設備價格

如要讓整個網路結構都具有 DHCP snooping 機制，則(如圖 5)住戶 A、住戶 B 的路由器也需連結 Layer2 網路設備，需耗費相當大的成本。

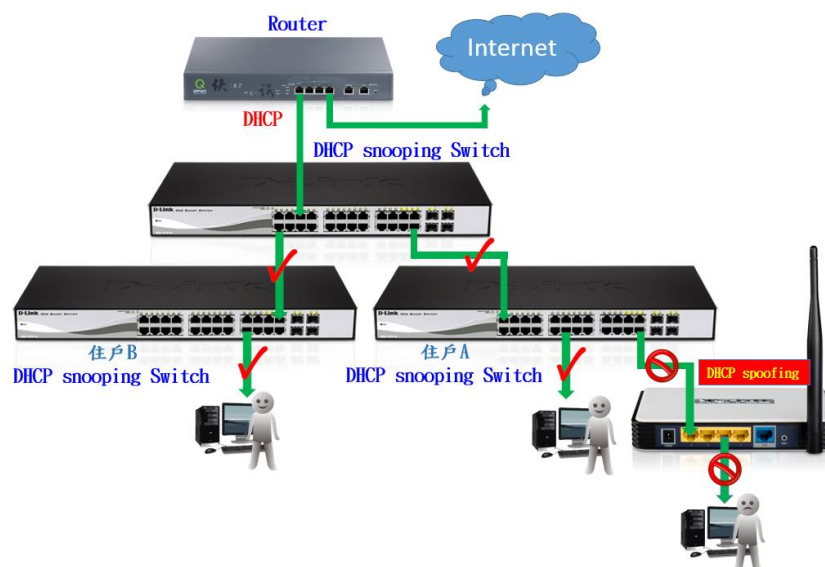


圖 5 以 Layer2 網路設備建置 DHCP snooping 環境



### 3. 系統功能與規格

#### 3.1. 系統功能

本系統功能如下列表：

- 建置 DHCP snooping 環境
- 寄發 Email 通知管理者網路異常狀況
- 阻止惡意 DHCP Service

#### 3.2. 系統硬體建置圖

本系統只需建置在 Router 下層路由器，其系統建置(如圖 6)。

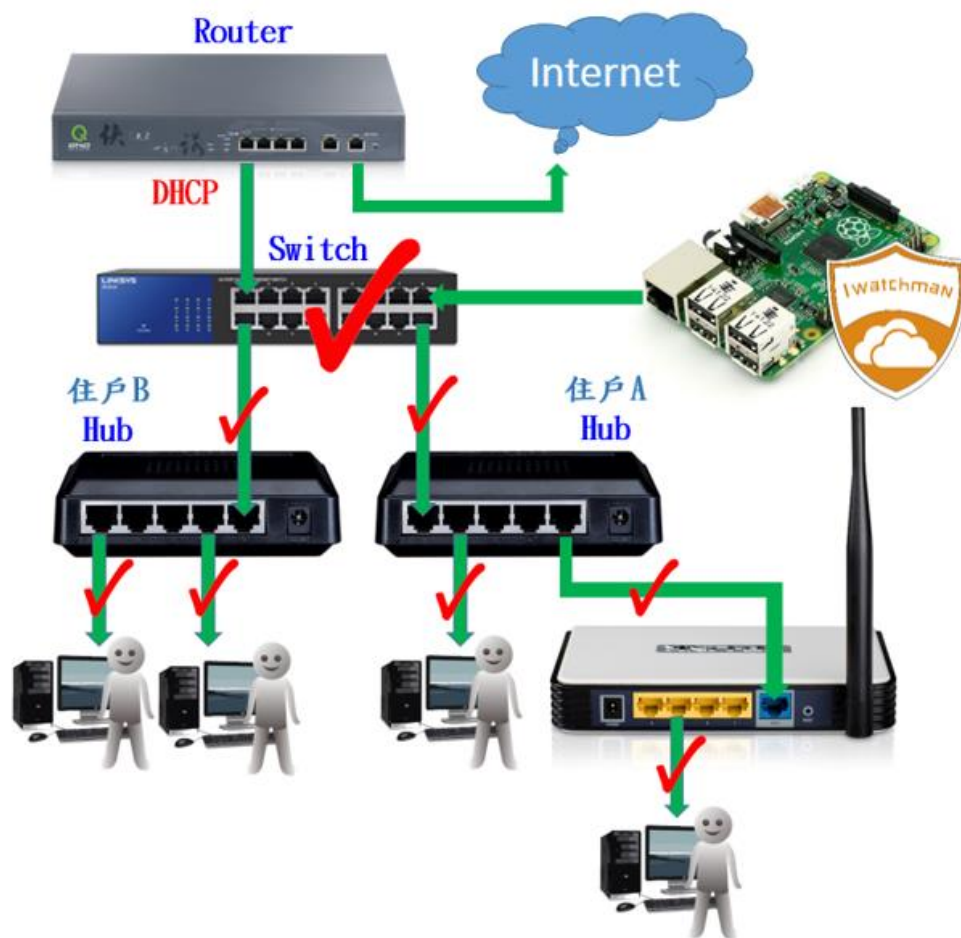


圖 6 系統硬體建置圖

### 3.3. 系統軟體架構圖

於 Raspberry Pi 安裝 Linux OS 後架設 Web Server 讓使用者透過 Web 介面進行相關設定，由偵測模組偵測是否有惡意 DHCP Server，若偵測到惡意 DHCP service 則寄發 Email 通知網路管理者並啟動排除模組，終止惡意 DHCP service，其軟體架構圖(如圖 7)。



圖 7 軟體架構圖

### 3.4. 系統流程

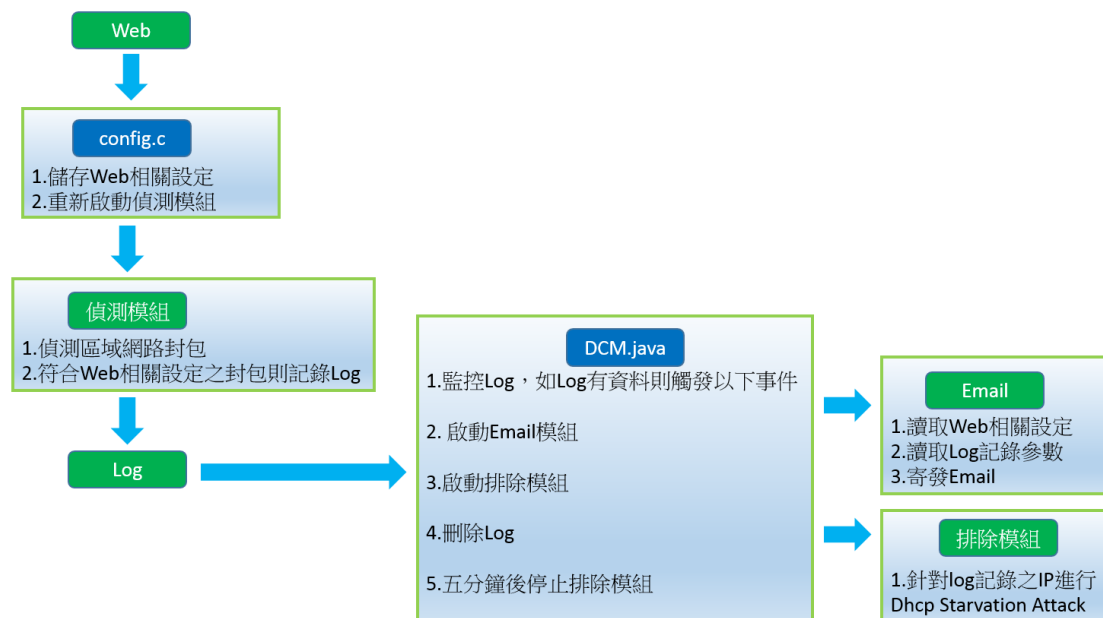


圖 8 系統流程

### 3.5. 系統規格

本系統使用之 Raspberry Pi(如圖 9)，其規格如表 1。

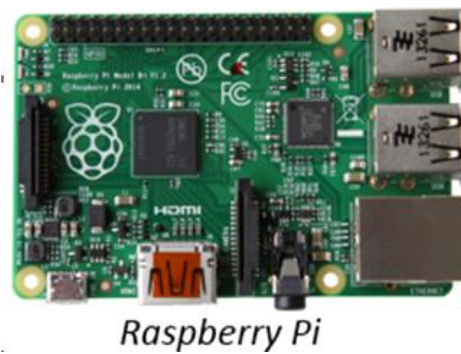


圖 9

表 1 Raspberry Pi 規格

|         |   |
|---------|---|
| 名稱      | Raspberry Pi B+   |
| SoC     | BroadcomBCM2835 (CPU, GPU DSP 和 SDRAM, USB)   |
| CPU     | ARM1176JZF-S 核心 (ARM11 系列) 700MHz   |
| GPU     | Broadcom VideoCore IV[41], OpenGL ES 2.0, 1080p 30 h.264/MPEG-4 AVC 高畫質解碼器  |
| 記憶體     | 512 MByte   |
| USB 2.0 | 4 個   |
| 影像輸出    | Composite RCA (PAL & NTSC), HDMI (rev 1.3 & 1.4) [44], raw LCD Panels via DSI[45][46]<br>14 HDMI resolutions from 640 x 350 to 1920x1200 plus various PAL and NTSC standards. |
| 音源輸出    | 3.5mm 插孔, HDMI  |
| 板載儲存    | SD / MMC / SDIO 卡插槽   |
| 網路介面    | 10/100 乙太網介面 (RJ45 介面)  |
| 外設      | 8 x GPIO、UART、I <sup>2</sup> C、帶兩個選擇的 SPI 匯流排, +3.3 V, +5 V, ground (負極)  |
| 電源輸入    | 5V / 透過 MicroUSB 或 GPIO 頭   |
| 總體尺寸    | 85.60 x 53.98 mm (3.370 x 2.125 in)   |
| 重量      | 45 g (1.6 oz)   |
| 操作系統    | GNU/Linux(Debian, Fedora, Arch Linux ARM) [49], RISC OS, FreeBSD, Plan 9  |

I Watchman 建置在 DHCP 環境下(如圖 10)，需透過 Web 設定相關參數，可從 LCD 獲取 I Watchman IP，(如圖 11)。

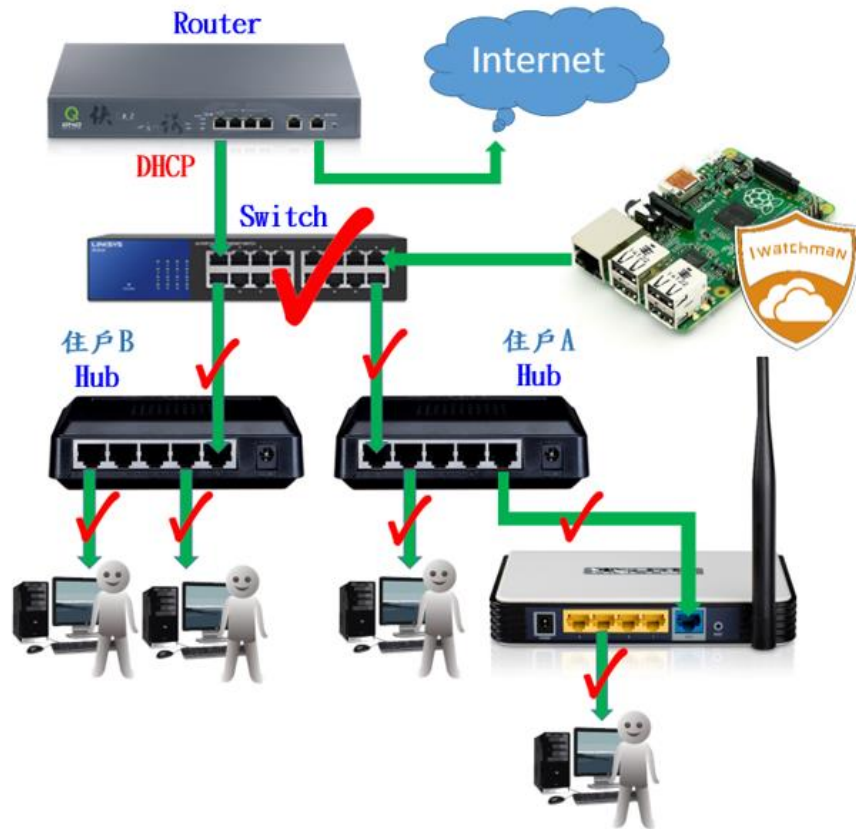


圖 10 I Watchman 建置情境



圖 11 Raspberry Pi 結合 16 x 2 LCD

### 3.6. 系統軟體關鍵技術

I Watchman OS 裝載 Kali Linux，如偵測網路異常先由 I Watchman 發送 Email 通知網路管理者，再針對惡意 DHCP Server 進行 DHCP Starvation Attack，偽造大量 Mac address 針對惡意 DHCP Server 租用 DHCP，使惡意 DHCP Server 癱瘓而不再配發 IP 給正常使用者。偵測封包工具可使用 tshark 或 snort，DHCP Starvation Attack 可使用 dhcpstarv 或 Yersinia。

DHCP Starvation Attack 能篡改封包標頭中的 Source MAC 位址（綠色段）以欺騙網路上的電腦及裝置（如圖 12）。

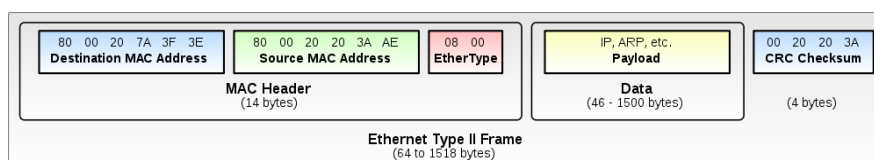


圖 12 Ethernet Type Frame

DHCP Starvation Attack 針對惡意 DHCP Server 消耗 DHCP 示範（如圖 13）。

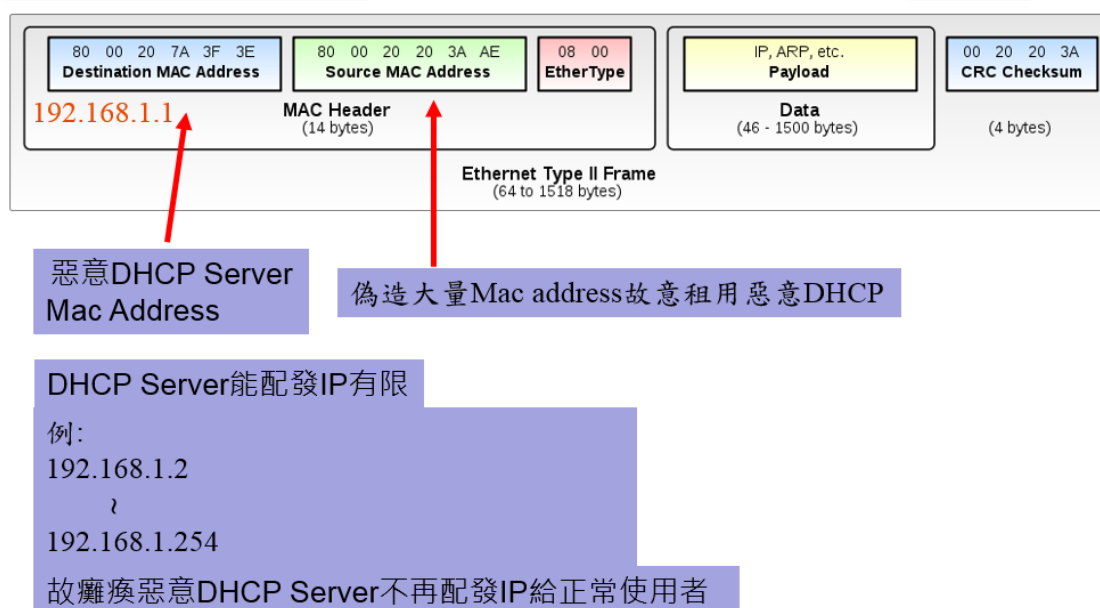


圖 13 消耗惡意 DHCP servc 示意圖

## 4. 標準的使用

使用者於區域網路 Router 下層路由器建置 I Watchman 並設定完成後，即可啟動網路偵測模組，當終端使用者在區域網路內架設分享器設定錯誤出現 DHCP spoofing 將導致網路癱瘓時，I Watchman 將會寄送 Email 通知使用者，並終止該終端使用者架設分享器配發 IP。

Step.1 使用者於區域網路 Router 下層路由器建置 I Watchman (如圖 14)。

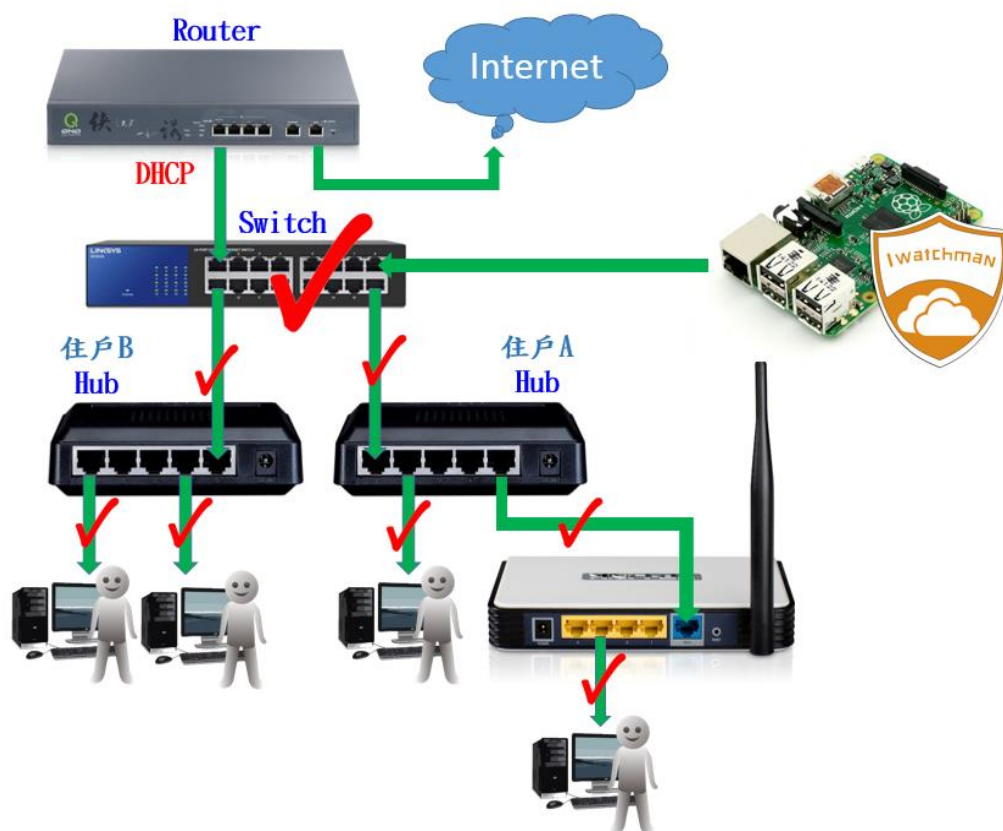


圖 14 I Watchman 建置

Step2. 透過 I Watchman LCD 顯示獲取 I Watchman IP，並開啟 Web 輸入 I Watchman IP，預設帳號 admin、預設密碼 admin，（如圖 15）。



圖 15 I Watchman LCD 獲取 IP

Step3. 取得正常 DHCP Server IP，（如圖 16）。



圖 16 取得正常 DHCP Server IP



Step4. 於 I Watchman Web 輸入正常 DHCP Server IP，並輸入區域網路發生 DHCP spoofing 時將寄送之 Email，(如圖 17)。

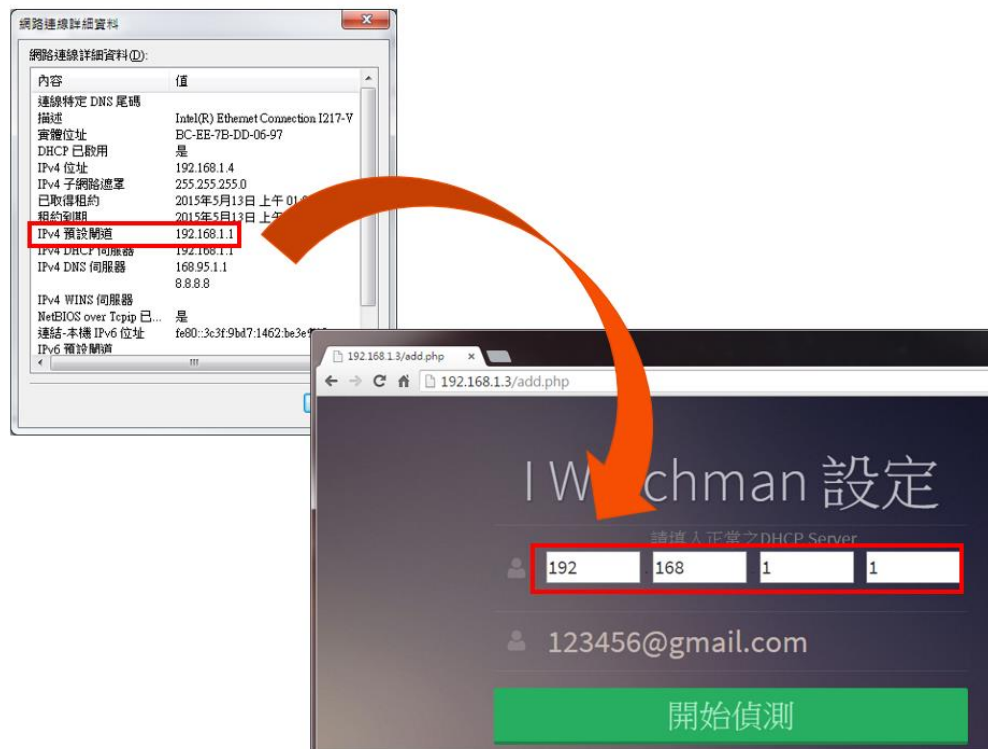


圖 17 I Watchman 設定

Step5. 開始網路偵測後即完成 I Watchman 設定，(如圖 18)。



圖 18 I Watchman 開始偵測網路



Step6. 如網路狀態正常，I Watchman 為偵測模式，(如圖 19)。

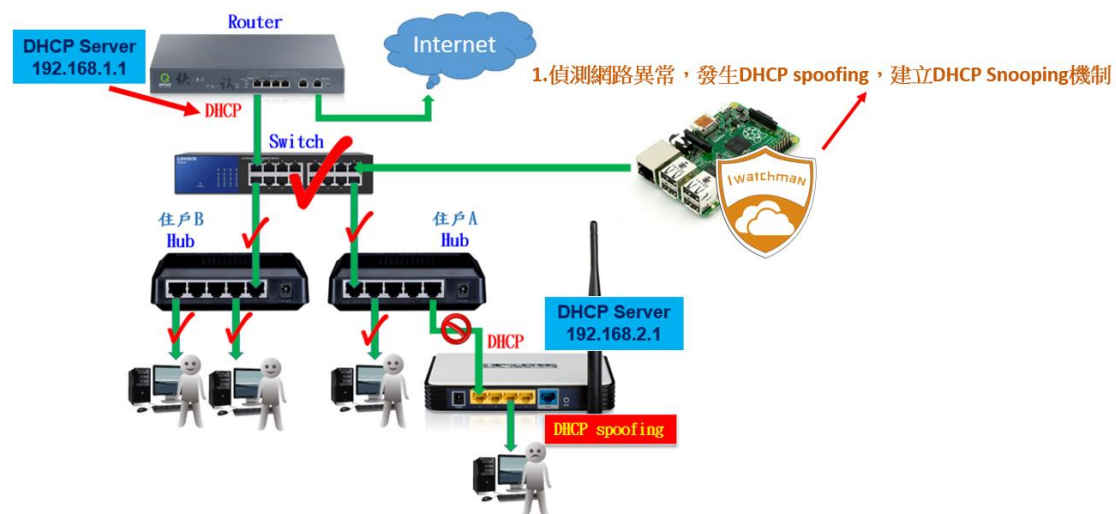


圖 19 I Watchman 偵測模式

Step7. 如網路狀態異常，I Watchman 啟動區域網路防禦機制，(如圖 20)。

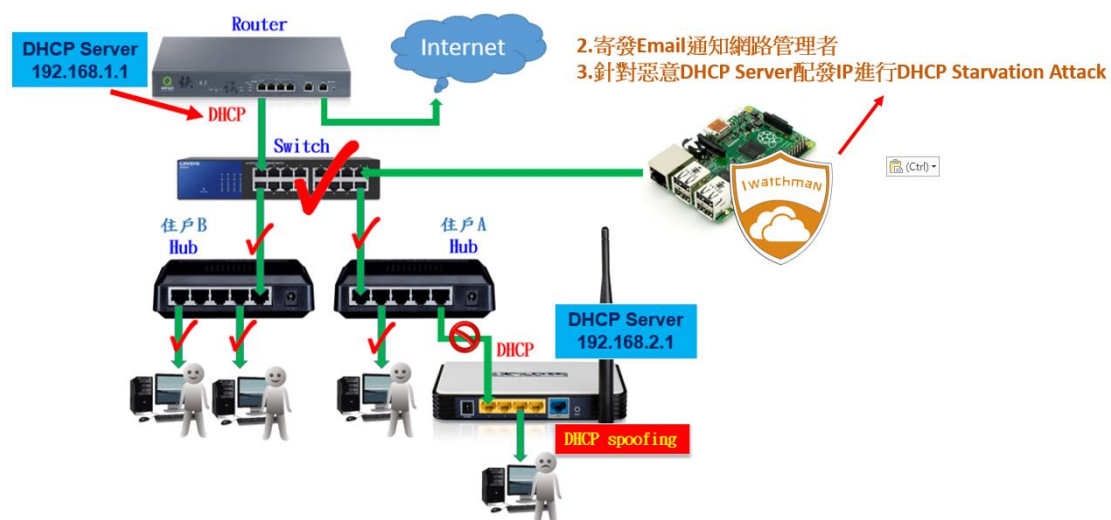


圖 20 I Watchman 啟動網路防禦機制

Step8. 當終端使用者在區域網路內架設分享器設定錯誤出現 DHCP spoofing 時，I Watchman 將會寄送 Email 通知使用者，(如圖 21)。

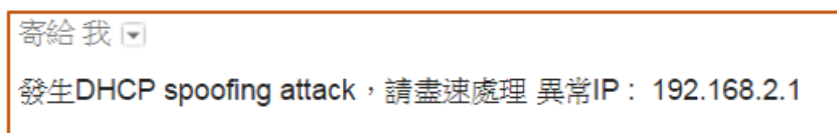


圖 21 I Watchman 寄送 Email 通知使用者

## 5. 實現與量產的考量

如以 Layer2 網路設備建置 DHCP snooping 環境，並讓每個網路使用者享有 DHCP snooping 機制則需要在每個資訊設備的終端接上 Layer2 網路設備，需耗費相當的成本，其估算成本(如表 2)。

表 2 DHCP Snooping Switch 建置成本(以五層樓為例)

| 型號          | 品名     | 台數 | 價格   | 總價    |
|-------------|--------|----|------|-------|
| Vigor 2920  | Router | 1  | 6000 | 6000  |
| DGS-1210-24 | Switch | 5  | 8000 | 40000 |
| 合計          |        |    |      | 46000 |

I Watchman 以宿舍網路建置成本為考量，只須把 I Watchman 建置在 Router 下層路由器(一般 Switch 或 Hub)，即可讓每個網路使用者享有 DHCP snooping 機制，其估算成本(如表 3)。

表 3 I Watchman 建置成本(以五層樓為例)

| 型號         | 品名         | 台數 | 價格   | 總價    |
|------------|------------|----|------|-------|
| Vigor 2920 | Router     | 1  | 6000 | 6000  |
| ES1100-24E | Switch     | 5  | 8000 | 8500  |
| I Watchman | I Watchman | 1  | 3000 | 3000  |
| 合計         |            |    |      | 17500 |

I Watchman 不僅可以佈建在學生宿舍及社區網路也可使用在居家區域網路防護，(如圖 22)。

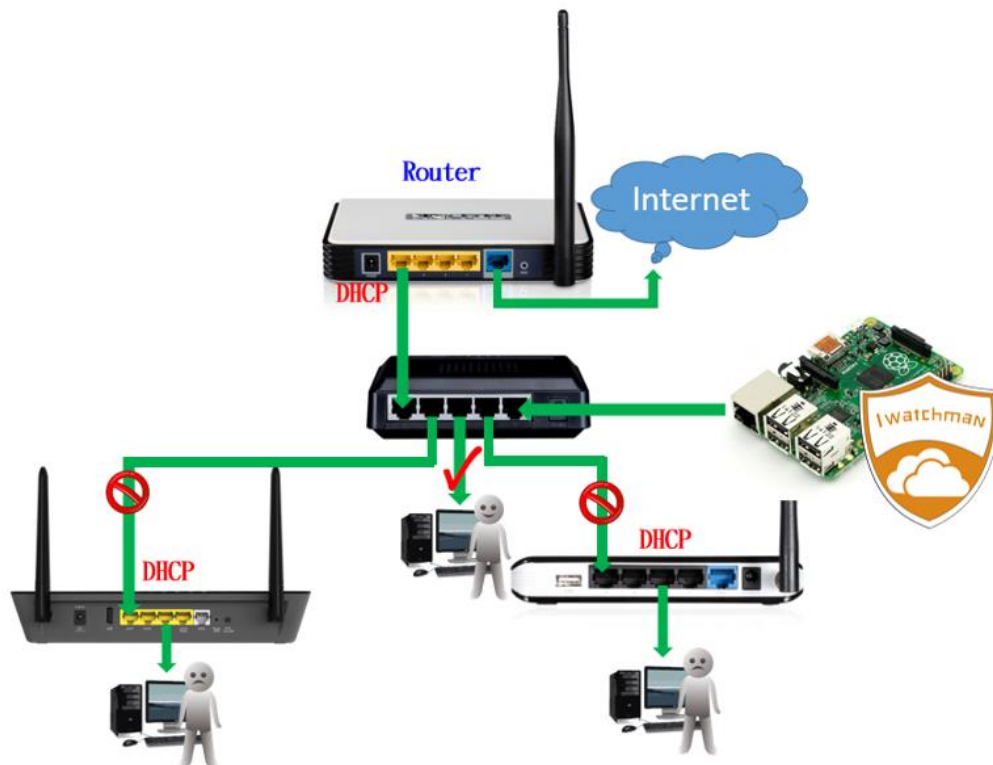


圖 22 I Watchman 居家區域網路防護

## 6. 結論

採用本系統即可以低成本建置出 DHCP snooping 環境，並有效防止 DHCP spoofing，針對學生宿舍及社區網路有極大的幫助。

若偵測封包工具使用 Snort，也可加以利用自建入侵偵測系統，達到 Raspberry Pi 小型電腦多工處理成效。

智慧三創

創新：Snort 本為入侵偵測系統，I Watchman 改為區域網路防護使用。

創意：Dhcpstarv 本具攻擊性工具，I Watchman 改為阻止惡意 DHCP Server 配發 IP。

創造：以 Raspberry Pi 建置開發，打造區域網路低成本 DHCP Snooping 環境。

## 7. 參考資料

永磐科技:

[http://www.mikotek.com.tw/suppor/suppor\\_s4.htm](http://www.mikotek.com.tw/suppor/suppor_s4.htm)

麟瑞科技:

<http://www.ringline.com.tw/epaper/forum961101.htm>

恆逸教育訓練中心:

<http://www.uuu.com.tw/public/content/article/110912tips.htm>

圖片引用:

<http://resdoss.blogspot.tw/2013/03/raspberry-pi-usb.html>

[http://www.xhome.com.tw/product\\_info.php?info=XHome-DownLoop-E16V.html](http://www.xhome.com.tw/product_info.php?info=XHome-DownLoop-E16V.html)

<http://zh.wikipedia.org/wiki/ARP%E6%AC%BA%E9%A8%99>