# MSI RG54G3
# 802. 11g 無線寬頻分享器

使用手冊

# 目錄

# 第 1 章　簡介

恭喜您購買此款優秀的無線寬頻分享器。本產品是特別針對小型企業和家庭企業而設計，提供完整的 SOHO 網路漫遊解決方案，設定簡單、操作容易，甚至連非專業的使用者都可以迅速上手。本產品的安裝和設定操作說明都可在此手冊中找到。安裝本產品之前，請先詳閱此手冊，以充分利用本產品功能。

## 功能與特性

### 分享器基本功能

- **具自動偵測功能的乙太網路交換器**
  配備具自動偵測功能的 4 埠乙太網路交換器。
- **WAN 類型**
  分享器支援 WAN 類型包括：Static、Dynamic、PPPoE、PPTP、L2TP、Dynamic IP with Road Runner。
- **內建防火牆**
  外來侵入者傳送的不受歡迎封包都會被阻擋在外，以保護您的內部網路。
- **DHCP 伺服器**
  所有聯網電腦都可以從本產品自動取得 TCP/IP 設定。
- **以網頁為基礎的設定方式**
  可使用 Netscape 或 Internet Explorer 透過任何聯網電腦的網頁瀏覽器進行設定。
- **伺服器**
  可讓您開放區域網路上的 WWW、FTP 和其他服務，供網際網路使用者存取。
- **使用者自訂特定軟體通道**
  使用者可以定義屬性以支援需要多方連線的特殊應用程式，如線上遊戲、視訊會議和網際網路電話等，本產品可以感測應用程式類型，並為其開啟多埠通道。
- **支援 DMZ 主機**
  允許聯網電腦完全開放於網際網路上；當特定軟體通道不敷使用時，便可使用此功能使應用程式正常運作。
- **WAN 統計**
  可讓您監控輸入和輸出封包。

## 無線網路功能

- **高速無線區域網路連結**
  整合正交分頻多工（OFDM）技術，資料傳輸速度最高可達 54 Mbps。
- **漫遊**
  可在 IEEE 802.11b（11M）及 802.11g（54M）無線網路架構間無縫漫遊。
- **支援 IEEE 802.11b 標準（11M）**
  允許不同廠牌產品間的交互操作。
- **支援 IEEE 802.11g 標準（54M）**
  允許不同廠牌間的交互操作。
- **自動偵測**
  自動偵測資料傳輸速率，在 802.11g 模式下資料傳輸速率為 54M、48M、36M、24M、18M、12M、6M；
- 在 802.11b 模式下資料傳輸速率為 11M、5.5M、2M、1M。

## 安全功能

- **支援封包過濾**
  **封包過濾功能**可分析內送和外送封包，依據來源和目的地的 IP 位址決定讓封包通過或停止傳輸，藉此協助控制網路的存取。
- **支援網域過濾**
  可防止本裝置下的使用者存取特定 URL。
- **支援 URL 封鎖**
  URL 封鎖功能只要利用一個**關鍵字**就可以封鎖數百個網站連結。
- **VPN Pass-through**
  分享器也支援 VPN 透通連接功能。
- **支援 802.1X**
  啟用 802.1X 功能時，無線網路使用者必須先通過本分享器的身分驗證才能使用網路服務。
- **支援 WPA-PSK 和 WPA**
  啟用 WPA 功能時，無線網路先通過本分享器的驗證才能使用網路服務。
- **支援 SPI 模式**
  啟用 SPI 模式時，分享器會檢查每個內送的封包以偵測封包是否有效。
- **支援 DoS 攻擊偵測功能**
  啟用此功能時，分享器會偵測並記錄來自網際網路的 DoS 攻擊。

## 進階功能

- **支援系統時間**
  可讓您使系統時間與網路時間伺服器同步。
- **支援電子郵件警示**
  分享器能透過電子郵件發送通知。
- **支援動態 DNS**
  目前分享器內建 3 組 DDN：DynDNS、TZO.com 和 dhs.org。
- **支援 SNMP**
  分享器支援基本 SNMP 功能。

- **支援路由表**
  目前，分享器支援靜態路由。
- **支援時程規則**
  用戶可以控制何時要存取或封鎖某些功能，如虛擬伺服器和封包過濾。

### 其他功能

- **支援 UPNP（通用隨插即用）**
  分享器亦支援此功能。應用程式：X-box、Msn Messenger。

## 產品包裝清單

- 無線寬頻分享器
- 安裝光碟
- 電源轉換器
- CAT-5 UTP 高速乙太網路線

# 第 2 章　硬體安裝

## 2.1 面板

### 2.1.1.前端面板


圖 2-1　前端面板

| 1. LED 指示燈 | 2. 功能 | 3. 顏色 | 4. 狀態 | 5. 說明 |
|---|---|---|---|---|
| **POWER** | 電源指示燈 | 綠色 | 亮 | 本產品已接通電源。 |
| **6. 狀態** | 7. 系統狀態 | 8. 綠色 | 9. 閃爍 | 10. M1 每秒閃爍一次表示系統運作中。 |
| **11. USB** | 12. USB 埠活動 | 13. 綠色 | 14. 亮 | 15. 已連結 USB 埠。 |
| **16. WAN** | 17. WAN 埠活動 | 18. 綠色 | 19. 亮 | 20. 已連結 WAN 埠。 |
| | | | 21. 閃爍 | 22. WAN 埠正在傳送或接收資料。 |
| **23. WLAN** | 24. 無線網路活動 | 25. 綠色 | 26. 閃爍 | 27. 正透過無線網路傳送或接收資料。 |
| **28. Link/Act. 1~4** | 29. 連結狀態 | 30. 綠色 | 31. 亮 | 32. 某個使用中的工作站連接到對應的 LAN 埠。 |
| | | | 33. 閃爍 | 34. 對應 LAN 埠正在傳送或接收資料。 |
| **35. RESET** | 36. 重設設定 | 37. | 38. | 39. 將系統設定重設為出廠預設值。 |

### 2.1.2.後端面板

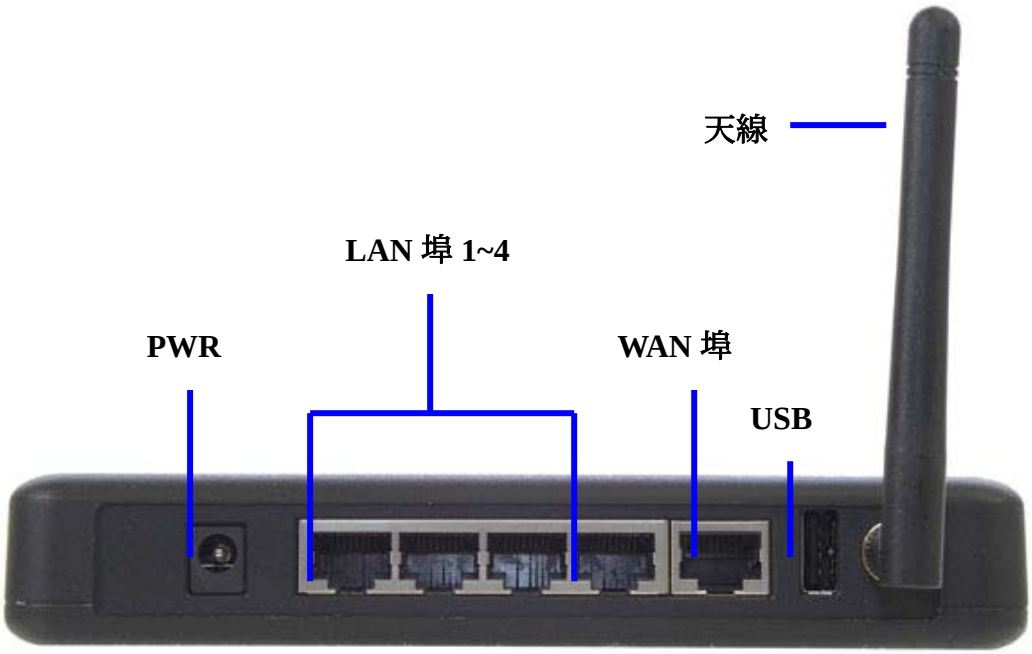



圖 2-2　後端面板

| | |
|---|---|
| **40. 連接埠** | **41. 說明** |
| **42. PWR** | 43. 電源輸入口 |
| **44. WAN** | 45. 連接 Cable（或 DSL）數據機或乙太網路路由器的埠。 |
| **46. Port 1-4** | 連接聯網電腦和其他裝置的埠。 |
| **47. USB** | 連接 USB 印表機 |

## 2.2 硬體安裝程序

**2. 決定無線寬頻分享器的放置地點**

48. 可以將無線寬頻分享器放置在桌面或其他平坦的表面上，也可以掛在牆上。若想得到最佳效能，請將無線寬頻分享器置於辦公室（或居家）的中心點，並且遠離金屬牆或微波爐等潛在干擾源。此地點必須靠近電源和網路連線。

**2. 建立區域網路（LAN）連線**

a. 有線區域網路連線：將乙太網路線從電腦的乙太網路埠連接到本產品任一個 LAN 埠。

b. 無線區域網路連線：將本產品放置在適當位置以獲得最佳傳輸效能。


圖 2-3　建立本產品的區域網路和廣域網路連線。

**3. 建立廣域網路（WAN）連線**

準備一條乙太網路線，將本產品連接到 Cable / xDSL 數據機或乙太網路骨幹。圖 2-3 說明此廣域網路連線。

**4. 開啟電源**

將電源線連接到電源輸入口再開啟電源開關，本產品便會自動進入自我測試階段。處於自我測試階段時，指示燈 M1 會亮起約 10 秒，然後再閃爍 3 次指示自我測試作業已經完成。最後，M1 將持續每秒閃爍一次，指示本產品正常運作中。

# 第 3 章　網路設定和軟體安裝

49. 若要正確使用本產品，您必須正確設定電腦的網路組態並將隨附的安裝程式安裝至 MS Windows 平台（Windows 95/98/NT/2000）。

## 3.1 設定正確的電腦網路組態

本產品的預設 IP 位址是 192.168.1.254，預設子網路遮罩是 255.255.255.0。這些位址可隨您的需要變更，但必須使用本手冊所提供的預設值。如果尚未設定電腦的 TCP/IP 環境，可參閱**附錄 A** 進行設定。例如，

1. 將 IP 設為 192.168.1.1，子網路遮罩設為 255.255.255.0，閘道設為 192.168.1.254，或用更簡單的方式，設定電腦自動載入 TCP/IP 設定，亦即，透過本產品的 DHCP 伺服器取得設定值。
2. 安裝 TCP/IP 通訊協定之後，就可以使用 **ping** 指令檢查電腦是否成功連接到本產品。下列範例說明在 Windows 95 平台上進行的 Ping 程序。首先，執行 **ping** 指令

**ping 192.168.1.254**

如果出現下列訊息：

**Pinging 192.168.1.254 with 32 bytes of data:**

**Reply from 192.168.1.254: bytes=32 time=2ms TTL=64**

代表電腦與本產品之間已成功建立通訊連結。但如果得到下列訊息：

**Pinging 192.168.1.254 with 32 bytes of data:**

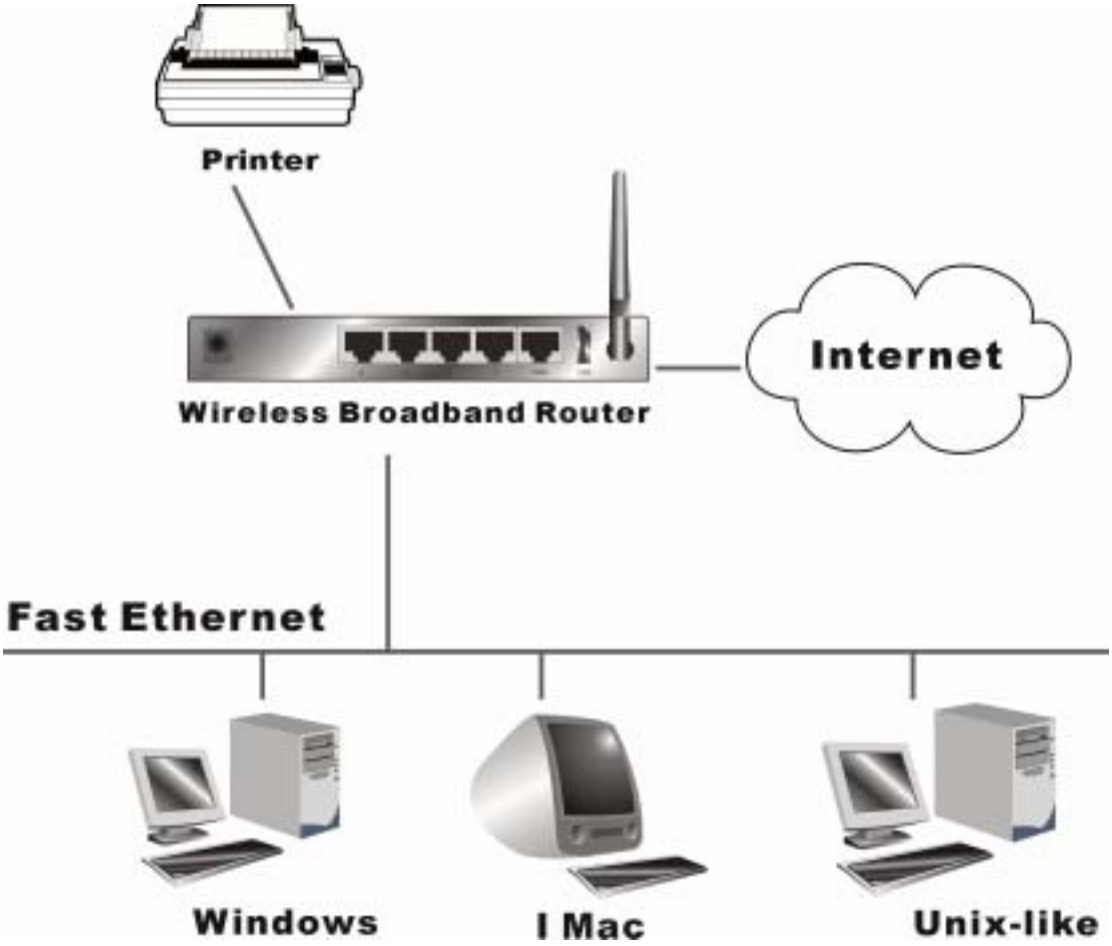
**Request timed out.**

則代表安裝過程中必定出現錯誤。您必須循序檢查下列項目：

1. 本產品和電腦之間的乙太網路線是否連接正確？
   **提示**：本產品的 LAN LED 指示燈和電腦網路卡的連結 LED 指示燈都必須是亮著的。
2. 電腦的 TCP/IP 環境是否設定正確？
   **提示**：如果本產品的 IP 位址是 192.168.1.254，則電腦的 IP 位址必須是 192.168.1.X，預設閘道必須是 192.168.1.254。

# 第 4 章　設定無線寬頻分享器

50. 本產品提供網頁式的組態設定方案，亦即，透過 Netscape Communicator 或 Internet Explorer 等網頁瀏覽器進行設定。MS Windows、Macintosh 或 UNIX 平台都適用此設定方式。



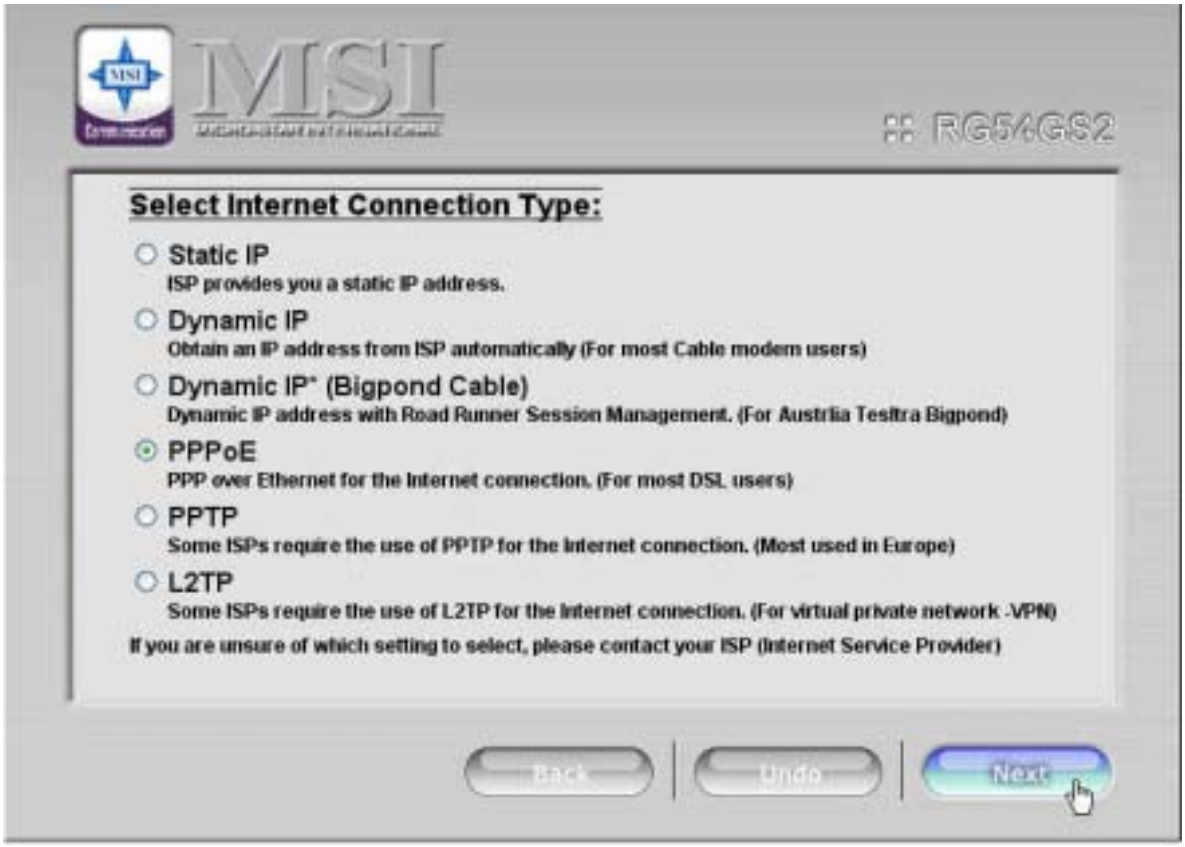
## 4.1 啟動和登入


啟動瀏覽器，並**停用 Proxy** 或**將本產品的 IP 位址新增至例外狀況**。接著，在網址欄（Netscape 是 Location，IE 是 Address）輸入本產品的 IP 位址，再按 ENTER。例如 **http://192.168.1.254**。

連線建立之後，將可以看到本產品的網頁使用介面。若要登入為管理員，請在**密碼**欄位輸入系統密碼（出廠預設設定是「**admin**」）再按一下**確定按鈕**。如果密碼正確，網頁外觀就會變更為管理員設定模式。如主功能表所列，有數個選項可供系統管理員選用。

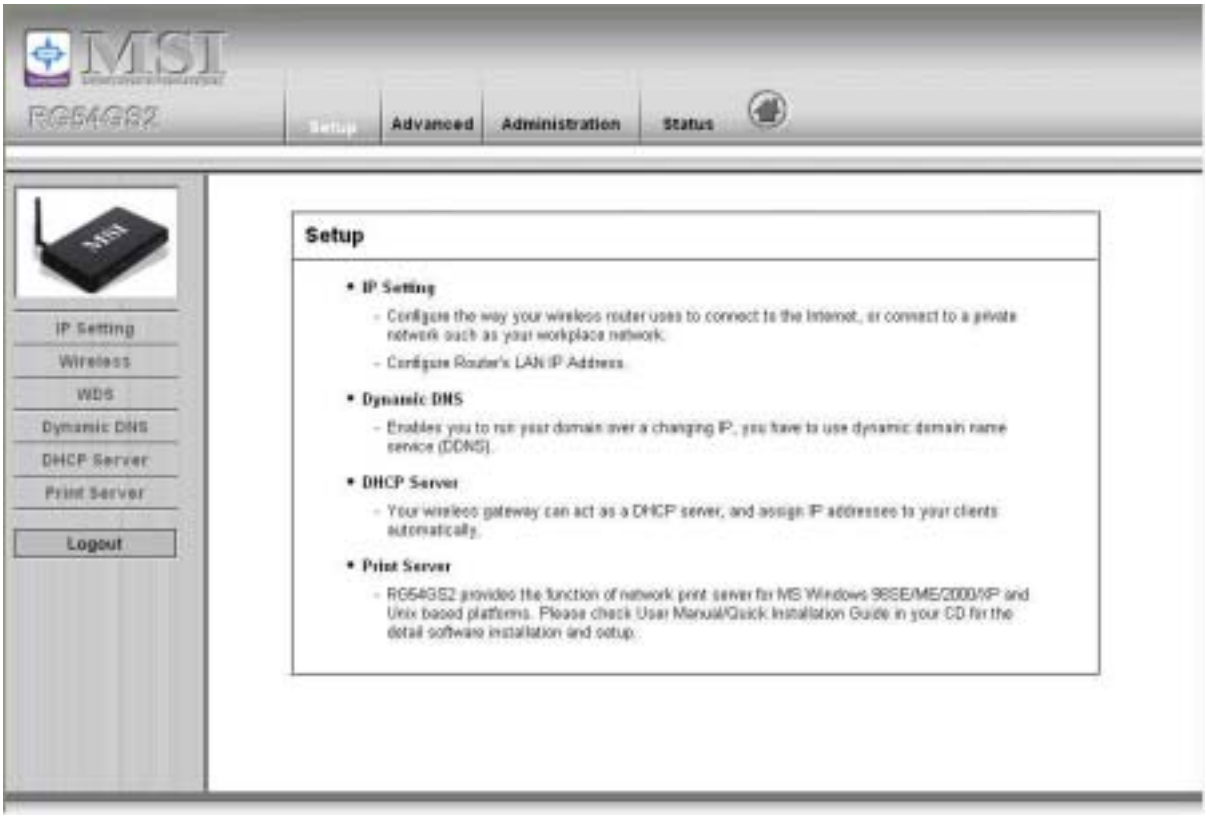
## 4.2 精靈


按「**Next >**」（**下一步**），Setup Wizard（安裝精靈）就會逐步引導您完成基本組態設定程序。



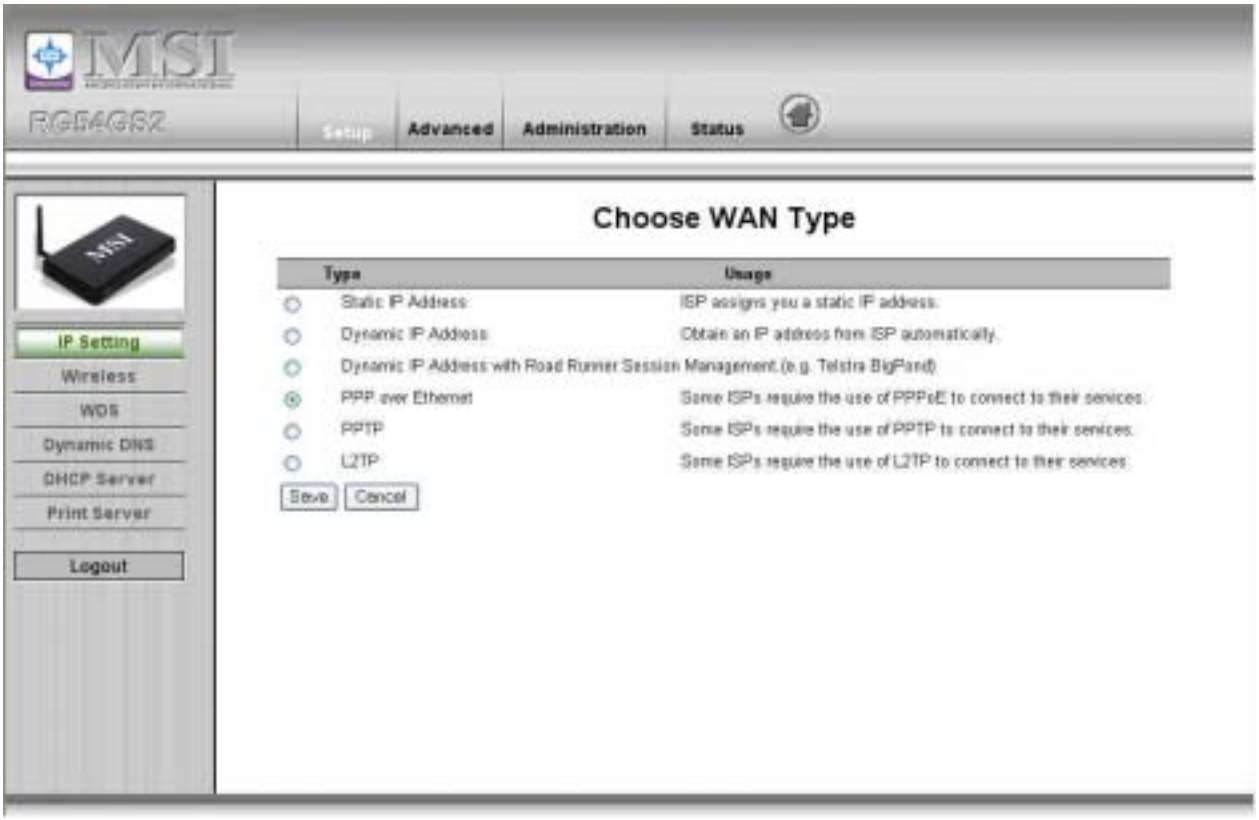

**安裝精靈－選取 WAN Type**：如需詳細設定值，請參閱 **4.3.1 IP Setting**。

## 4.3 Setup（設定）



**51. 4.3.1 IP Setting – WAN Type, IP Mode（IP設定－WAN類型、IP模式）**


按「**Change**」（**變更**）




此選項主要目的是讓本產品正常運作。設定項目和網頁外觀須視廣域網路類型而定。啟動之前請選擇正確的廣域網路類型。

1. **LAN IP Address（區域網路 IP 位址）**：本裝置的本機 IP 位址。網路上的電腦必須使用分享器的 LAN IP 位址作為預設閘道。如有需要可以變更。
2. **WAN Type（廣域網路類型）**：ISP 的 WAN 連線類型。您可以按一下 **Change** 按鈕，從下列四個選項選擇正確的類型：
   A. Static IP Address：ISP 指派一個靜態 IP 位址給您。
   B. Dynamic IP Address：自動從 ISP 取得 IP 位址。
   C. Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)
   D. PPP over Ethernet：有些 ISP 要求用戶使用 PPPoE 協定連線至他們的服務。
   D. PPTP：有些 ISP 要求用戶使用 PPTP 協定連線至他們的服務。
   F. L2TP：有些 ISP 要求用戶使用 L2TP 協定連線至他們的服務。

#### 4.3.1.1 Static IP Address（靜態IP位址）

WAN IP Address、Subnet Mask、Gateway、Primary and Secondary DNS（WAN IP 位址、子網路遮罩、閘道、主要和次要 DNS）：輸入 ISP 所提供的正確設定。

#### 4.3.1.2 Dynamic IP Address（動態IP位址）

1. Host Name（主機名稱）：選擇性，例如，某些 ISP 要求填入@Home。
2. Renew IP Forever（永遠更新 IP）：此功能可使本產品在租用時間屆滿時自動更新您的 IP 位址，即使系統閒置亦不例外。

#### 4.3.1.3 Dynamic IP Address with Road Runner Session Management. (e.g. Telstra BigPond)（與Road Runner Session Management共存的動態IP位址（如Telstra BigPond）

1. LAN IP Address 是本裝置的本機 IP 位址，這必須是您電腦的預設閘道。
2. WAN Type 是 Dynamic IP Address。如果 WAN 類型不正確，請進行變更！
3. Host Name（主機名稱）：選擇性，例如，某些 ISP 要求填入@Home。
4. Renew IP Forever（永遠更新 IP）：此功能可使本產品在租用時間屆滿時自動更新您的 IP 位址，即使系統閒置亦不例外。

#### 4.3.1.4 PPP over Ethernet

PPPoE Account and Password（PPPoE 帳號和密碼）：ISP 指派給您的帳號和密碼。為安全起見，此欄位顯示為空白。如果不想變更密碼，請保留空白。

PPPoE Service Name（PPPoE 服務名稱）：選擇性。如果 ISP 要求提供服務名稱，則請輸入，否則，請保留空白。

Maximum Idle Time（最長閒置時間）：沒有出現任何動作的時間若達此數，則中斷 PPPoE 工作連線。

將此項目設為零或啟用自動重新連接可停用此功能。

**Maximum Transmission Unit (MTU)**（最大傳輸單位）：大部分 ISP 都會提供 MTU 值給使用者。最常見的 MTU 值是 1492。

Connection Control（連線控制）：有 3 種模式可供選取：

Connect-on-demand（視需要連線）：裝置會在用戶端傳送外送封包時向 ISP 取得連結。

Auto-Reconnect (Always-on)（自動重新連線（永遠開啟））：裝置會一直向 ISP 取得連結，直到連線建立為止。

Manually（手動）：裝置不會進行連結，除非有人按了 Staus 頁面中的連接按鈕。

**4.3.1.5 PPTP**

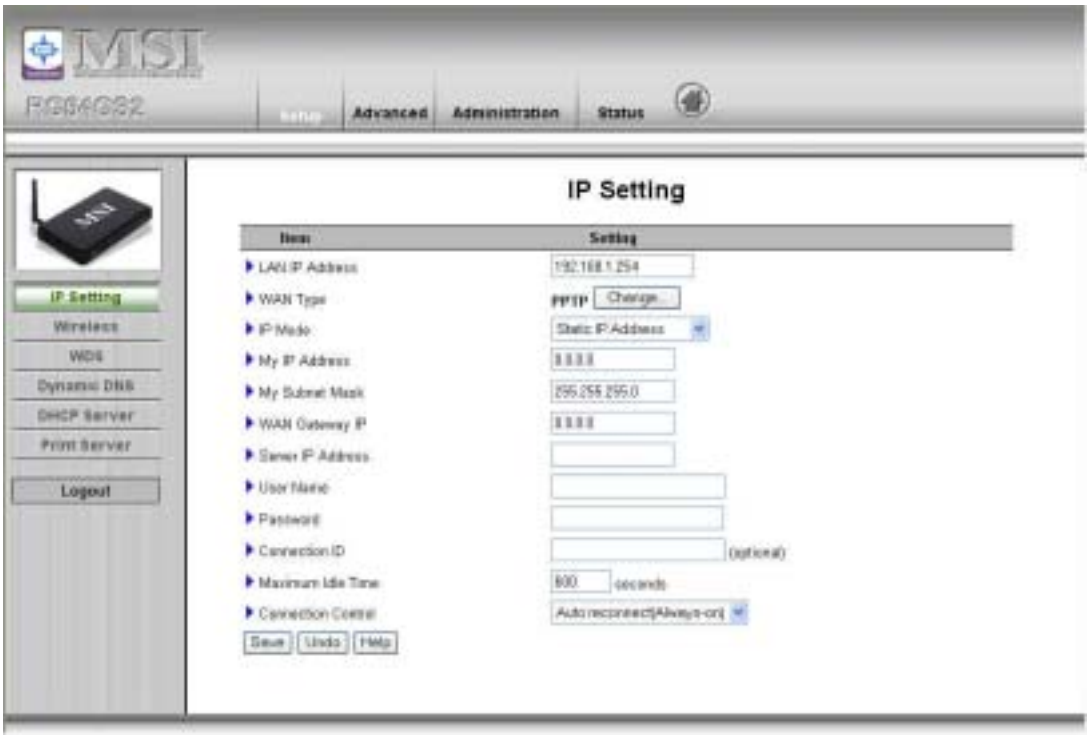
1. My IP Address and My Subnet Mask（我的 IP 位址和子網路遮罩）：ISP 指派給您的私人 IP 位址和子網路遮罩。
2. Server IP Address（伺服器 IP 位址）：PPTP 伺服器的 IP 位址。
3. PPTP Account and Password（PPTP 帳號和密碼）：ISP 指派給您的帳號和密碼。如果不想變更密碼，請保留空白。
4. Connection ID（連線 ID）：選擇性。如果 ISP 要求提供連線 ID，則請輸入。
5. Maximum Idle Time（最長閒置時間）：沒有出現任何動作的時間若達此數，則中斷 PPTP 工作連線。將此項目設為零或啟用自動重新連接可停用此功能。如果啟用自動重新連接，本產品將在系統重新啟動或連線中斷時自動連線到 ISP。

Connection Control（連線控制）：有 3 種模式可供選取：

Connect-on-demand（視需要連線）：裝置會在用戶端傳送外送封包時向 ISP 取得連結。

Auto-Reconnect (Always-on)（自動重新連線（永遠開啟））：裝置會一直向 ISP 取得連結，直到連線建立為止。

Manually（手動）：裝置不會進行連結，除非有人按了 Staus 頁面中的連接按鈕。




**4.3.1.6 L2TP**

首先，請檢查 ISP 是否已有指派，再選取 Static IP Address 或 Dynamic IP Address。

例如：使用靜態 IP 位址

1. My IP Address and My Subnet Mask（我的 IP 位址和子網路遮罩）：ISP 指派給您的私人 IP 位址和子網路遮罩。
2. Server IP Address（伺服器 IP 位址）：PPTP 伺服器的 IP 位址。
3. PPTP Account and Password（PPTP 帳號和密碼）：ISP 指派給您的帳號和密碼。如果不想變更密碼，請保留空白。
4. Connection ID（連線 ID）：選擇性。如果 ISP 要求提供連線 ID，則請輸入。
5. Maximum Idle Time（最長閒置時間）：沒有出現任何動作的時間若達此數，則中斷 PPTP 工作連線。將此項目設為零或啟用自動重新連接可停用此功能。如果啟用自動重新連接，本產品將在系統重新啟動或連線中斷時自動連線到 ISP。

Connection Control（連線控制）：有 3 種模式可供選取：

Connect-on-demand（視需要連線）：裝置會在用戶端傳送外送封包時向 ISP 取得連結。

Auto-Reconnect (Always-on)（自動重新連線（永遠開啟））：裝置會一直向 ISP 取得連結，直到連線建立為止。

Manually（手動）：裝置不會進行連結，除非有人按了狀態頁中的連接按鈕。


**4.3.2 Wireless Setting, and 802.1X setting（無線網路設定和802.1X設定）**

Wireless Setting 可讓您設定無線網路的組態項目。

1. **Network ID (SSID)（網路 ID）**：網路 ID 用以辨識無線區域網路（WLAN）。透過本產品和其他網路 ID 相同的無線基地台，用戶端工作站可以自由漫遊。（出廠設定為「**default**」）
2. **Channel（頻道）**：無線電頻道編號。允許使用的頻道須視「管制網域」而定。
   出廠設定如下：**北美是頻道 6**；**歐洲是**頻道 7（ETSI）；**日本是**頻道 7。
3. **WEP Security（WEP 安全機制）**：選取所要的資料隱私演算法。啟用安全機制可保護工作站之間傳輸的資料。此處所使用的是標準的 IEEE 802.11 WEP（128 或 64 位元）規格。
4. **WEP Key 1, 2, 3 & 4（WEP 金鑰 1、2、3 和 4）**：當啟用 128 或 64 位元 WEP 金鑰安全機制時，請選取要使用的 WEP 金鑰並輸入 26 或 10 個十六進位（0、1、2…8、9、A、B…F）字元。
5. Pass-phrase Generator（通關密語產生器）：由於十六進位字元不易記住，所以本裝置提供轉換工具，將簡單的字或詞轉換成十六進位。
6. **802.1X Setting（802.1X 設定）**

**52. 802.1X**

核取方塊用以切換 802.1X 功能。啟用 802.1X 功能時，無線網路使用者必須先通過本分享器的**身分驗證**才能使用網路服務。
RADIUS Server（RADIUS 伺服器）
IP 位址或 802.1X 伺服器的網域名稱。
RADIUS Shared Key（RADIUS 共用金鑰）

53. 金鑰值為 RADIUS 伺服器和本分享器所共用。此金鑰值與 RADIUS 伺服器的金鑰值相同。

54.


**55. WPA-PSK**

56. 1. 選取 Preshare Key Mode（預先共用金鑰模式）

57. 如果選取 HEX，必須填入 64 個十六進位（0、1、2…8、9、A、B…F）字元。

58. 如果選取 ASCII，預先共用金鑰的長度則為 8 至 63。

59. 2. 填入金鑰，Ex 145678。

60.


**61. WPA**

核取方塊用以切換 WPA 功能。啟用 WPA 功能時，無線網路使用者必須先通過本分享器的**驗證**才能使用網路服務。RADIUS Server（RADIUS 伺服器）
IP 位址或 802.1X 伺服器的網域名稱。
RADIUS Shared Key（RADIUS 共用金鑰）

62. 金鑰值為 RADIUS 伺服器和本分享器所共用。此金鑰值與 RADIUS 伺服器的金鑰值相同。

**63.**

### 4.3.3 WDS

64. 無線網路分配架構（WDS）支援點對點 AP 通訊。選取 **Enable（啟用）**允許分享器間的 Bridge（WDS）模式或選取 **Disable（停用）**封鎖分享器間的通訊。

65. 若要啟用 **WDS**，請將 **Wireless Bridging (WDS)** 功能設定為 **Enable**。以冒號分開兩字元的方式輸入分享器的 Wireless MAC 位址再按一下 **Save（儲存）**。


### 4.3.4 Dynamic DNS（動態DNS）

若要將主機裝載於變動的 IP 位址上，您必須使用動態網域名稱服務（DDNS）。

如此一來，任何想到達您主機的人只需知道主機名稱即可，雖然每次連線到網際網路服務供應商的 IP 位址都不一樣，但動態 DNS 會將主機名稱對應到您目前的 IP 位址。

啟用 **Dynamic DNS** 之前，必須先在 **provider（提供者）**欄位所列的其中一個動態 DNS 伺服器上註冊帳號。

若要啟用 **Dynamic DNS**，請按一下 **DDNS 欄位中 Enable** 旁的核取方塊。

接著可以輸入有關所用動態 DNS 伺服器的正確資訊。

您必須定義下列項目：

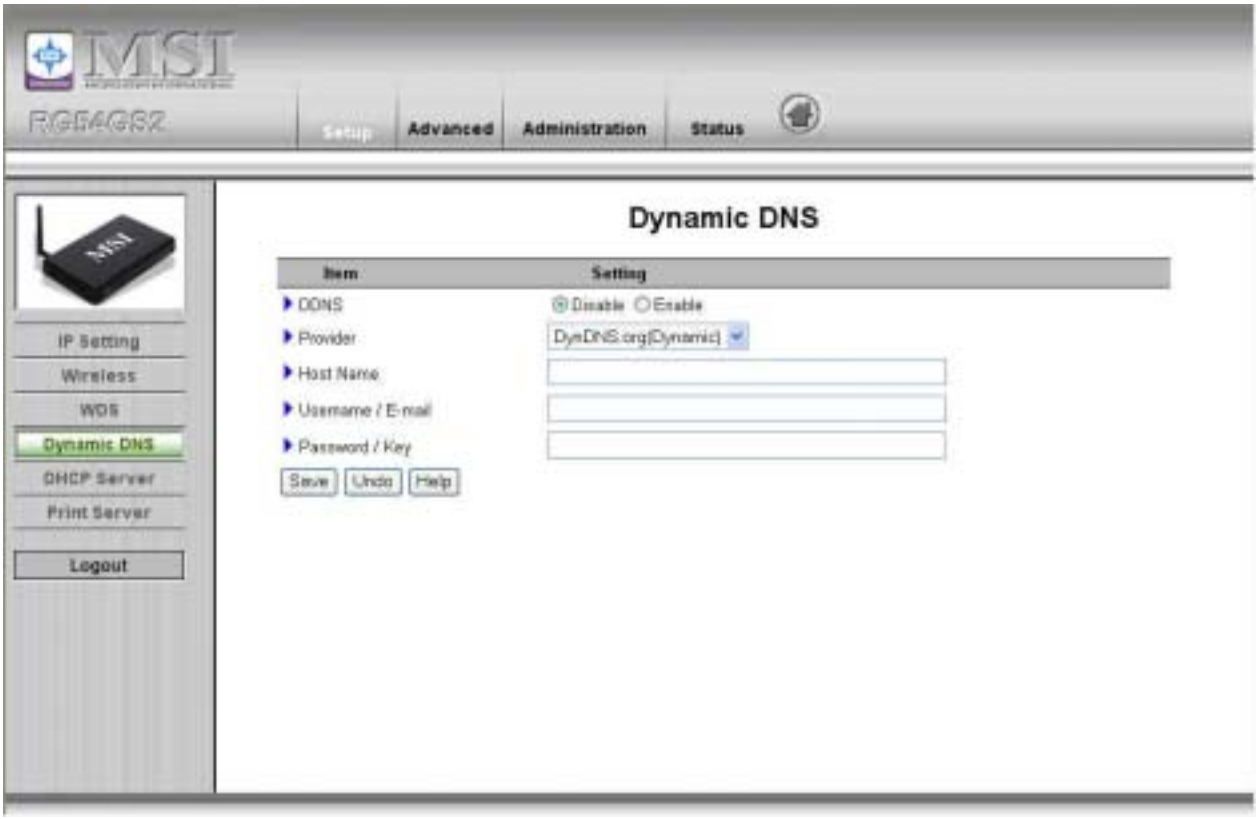
Provider（提供者）

Provider（主機名稱）

Provider（使用者名稱/電子郵件信箱）

Password/Key（密碼/金鑰）

在動態 DNS 伺服器上完成帳號註冊後就可以取得這些資訊。




### 4.3.5 DHCP Server（DHCP伺服器）

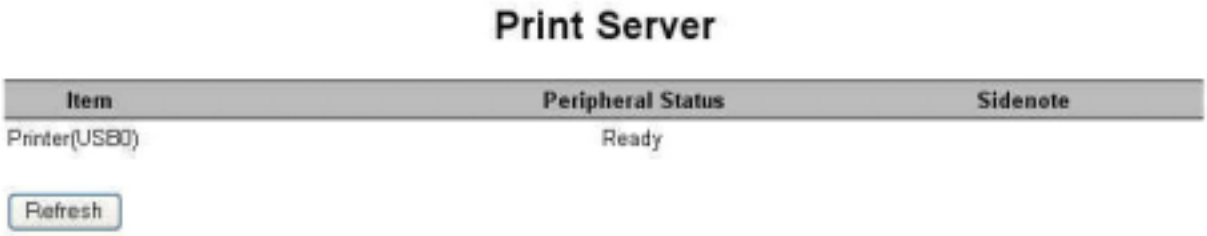
按「**More>>**」（**更多設定**）

TCP/IP 環境中的設定包含主機 IP、子網路遮罩、閘道和 DNS 組態。手動設定網路上的所有電腦和裝置，不是輕鬆的工作，所幸，DHCP Server 項目提供了比較簡單的方法處理設定這些設定。本產品支援 DHCP 伺服器的功能。如果啟用本產品的 DHCP 伺服器且將電腦設定為「IP 自動分配」模式，則當電腦開啟時，系統將會自動從本產品載入合適的 TCP/IP 設定。DHCP 伺服器的設定包含下列項目：

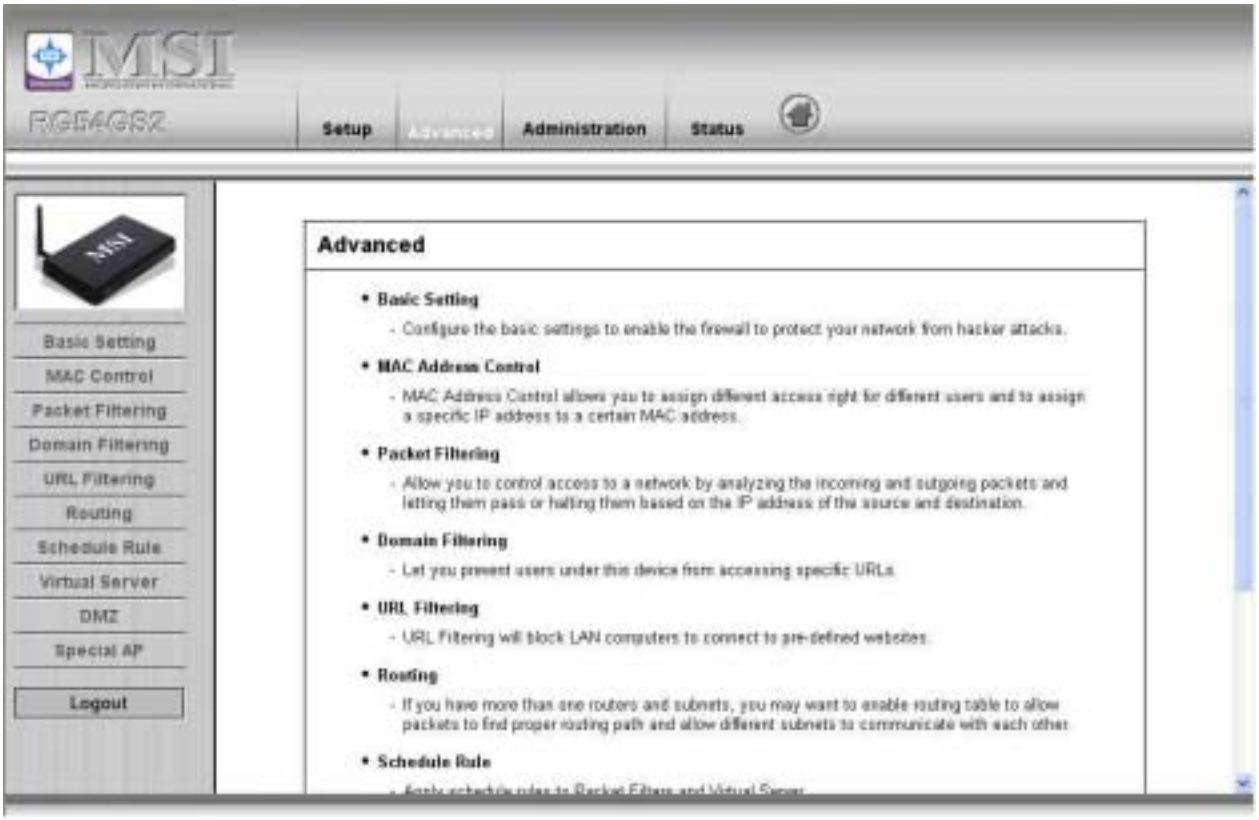
1. **DHCP Server**：選擇停用「Disable」或啟用「Enable」。
2. **Lease Time（租用時間）：**定義租用 IP 位址的時段。
3. **IP starting Address/ IP pool ending Address（IP 集區起始位址/IP 集區結束位址）**：不論何時出現要求，DHCP 伺服器都會自動從 IP 位址集區選取一個未使用的 IP 位址分配給提出要求的電腦。您必須指定 IP 位址集區的起始和結束位址。
4. **Domain Name（網域名稱）**：選擇性，此資訊將會傳送給用戶端。
5. **Primary DNS/Secondary DNS（主要 DNS/次要 DNS）**：此功能可讓您指派 DNS 伺服器。
6. **Primary WINS/Secondary WINS（主要 WINS/次要 WINS）**：此功能可讓您指派 WINS 伺服器。
7. **Gateway（閘道）**：此閘道位址是替代閘道的 IP 位址。
   如果個人電腦的 IP 是 DHCP 伺服器所提供，此功能可讓您指派其他閘道給您的電腦。

#### 4.3.6 Print Server（列印伺服器）

此項目顯示列印是否就緒。




## 4.4 Advanced（進階設定）



### 4.4.1 Basic Setting（基本設定）


**Discard PING from WAN side（封鎖廣域網路的PING）**
此功能啟用時，廣域網路上的任何主機都無法偵測到此產品。

**SPI Mode（SPI模式）**
此功能啟用時，分享器會記錄通過的封包資訊，例如 IP 位址、連接埠位址、ACK、SEQ 編號等。此外，分享器還會檢查每個內送的封包以偵測封包是否有效。

**DoS Attack Detection（DoS攻擊偵測）**
啟用此功能時，分享器會偵測並記錄來自網際網路的 DoS 攻擊。目前，分享器可以偵測下列 DoS 攻擊：SYN Attack、WinNuke、Port Scan、Ping of Death、Land Attack 等。

### 4.4.2 MAC Address Control（MAC位址控制）


MAC Address Control 功能可讓您指派不同的存取權給不同的使用者，亦可指派特定 IP 位址給特定 MAC 位址。

**MAC Address Control**

勾選「Enable」可啟用「MAC Address Control」。只要勾選「Enable」，此頁面中的所有設定都會生效。

**Connection control（連線控制）**

勾選「Connection control」可控制哪些有線和無線網路用戶端能夠連線到本裝置。如果用戶端連線本裝置遭拒，則代表它也無法存取網際網路。選擇「allow」或「deny」可允許或拒絕 MAC 位址不在「控制表」（請見下表）中的用戶端連線到本裝置。

**Association control（關聯控制）**

勾選「Association control」可控制哪些無線網路用戶端可以

連線到無線區域網路。如果用戶端連線無線區域網路遭拒，則代表它無法透過本裝置傳送或接收任何資料。選擇「allow」或「deny」可允許或拒絕 MAC 位址不在「控制表」中的用戶端連線到無線區域網路。

**控制表**


「控制表」是位於「MAC Address Control」頁面底部的表格。此表各列指示用戶端的 MAC 位址及其預期 IP 位址對應。此表有四個欄位：

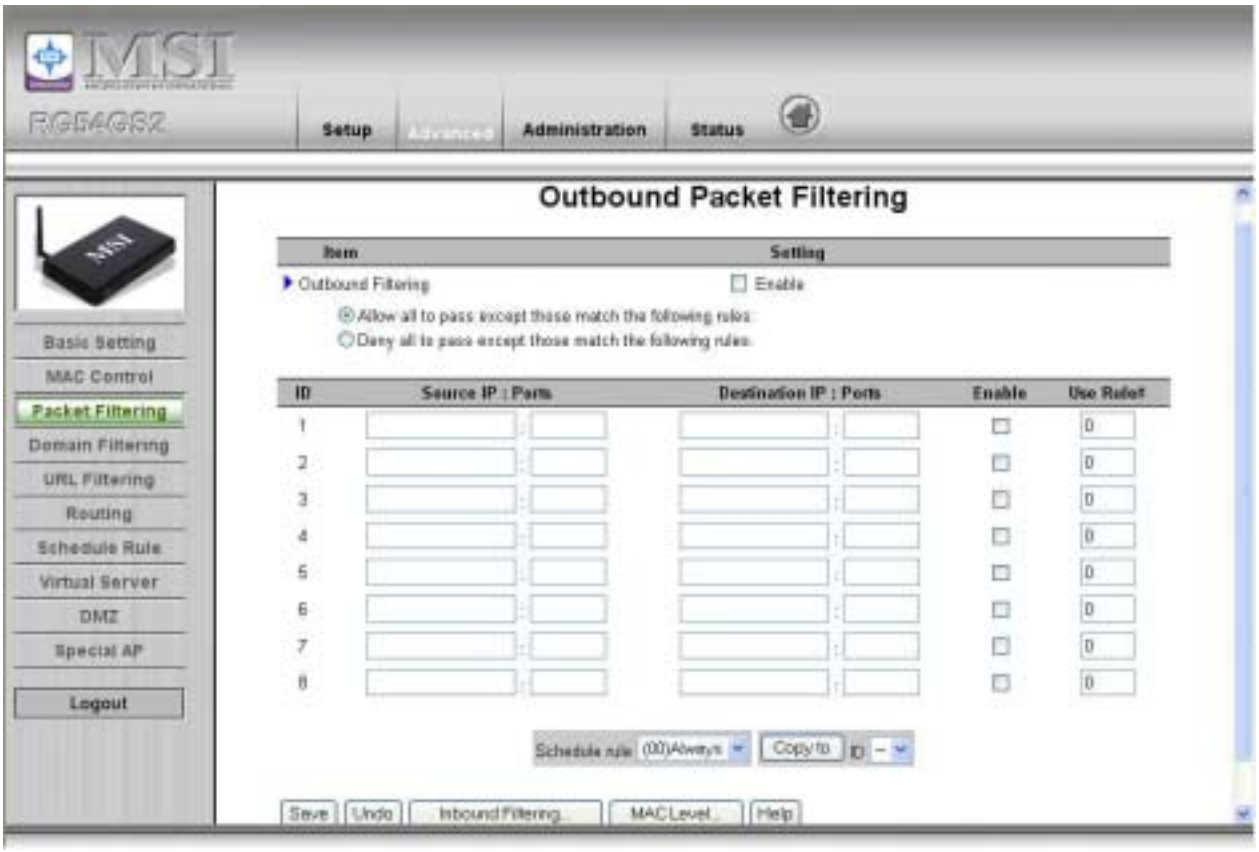
| | |
|---|---|
| **MAC Address** | MAC 位址代表某個特定用戶端。 |
| **IP Address** | 對應用戶端的預期 IP 位址。如果您不在意該用戶端的 IP 位址，請將此欄位保留空白。 |
| **C** | 如果勾選了「Connection control」，按一下「C」將可允許對應用戶端連線到此裝置。 |
| **A** | 如果勾選了「Association control」，按一下「A」將可允許對應用戶端連線到無線區域網路。 |

在此頁面中，我們提供下列下拉式方塊和按鈕以協助您輸入 MAC 位址。


您可以在「DHCP clients」下拉式方塊中選與特定用戶端，再按一下「Copy to」按鈕，將所選用戶端的 MAC 位址複製到「ID」下拉式方塊中的選取 ID。

**Previous page and Next Page（上一頁和下一頁）** 為了使此設定頁面簡單明瞭，我們將「控制表」分成數頁，您可以使用這些按鈕瀏覽不同頁面。

### 4.4.3 Packet Filtering（封包過濾）




Packet Filter 可讓您控制何種封包可通過分享器。輸出過濾適用於所有輸出封包，但輸入過濾只適用於送往虛擬伺服器或 DMZ 主機的封包。您可以選擇下列其中一種過濾原則：

1. Allow all to pass except those match the specified rules（除符合指定規則的封包外，允許所有封包通過）
2. Deny all to pass except those match the specified rules（除符合指定規則的封包外，拒絕所有封包通過）

輸入或輸出方向都可以指定 8 個規則。在每個規則中，您可以定義下列項目：

- 來源 IP 位址
- 來源埠位址
- 目的 IP 位址
- 目的埠位址
- 通訊協定：TCP 或 UDP 或兩者兼用
- 使用規則#

就來源或目的 IP 位址而言，您可以定義單一 IP 位址（4.3.2.1）或某一範圍的 IP 位址（4.3.2.1-4.3.2.254），空白則代表所有 IP 位址。
就來源或目的埠而言，您可以定義單一埠（80）或某一範圍的埠（1000-1999）。加入首碼「T」或「U」可指定 TCP 或 UDP 通訊協定，例如 T80、U53、U2000-2999。沒有首碼代表同時定義 TCP 和 UDP。空白則代表所有埠位址。**Packet Filter** 可與 **Scheduling Rules（時程規則）**一起使用，讓使用者具有更靈活的存取控制。如需詳細資訊，請參閱 **Scheduling Rules**。

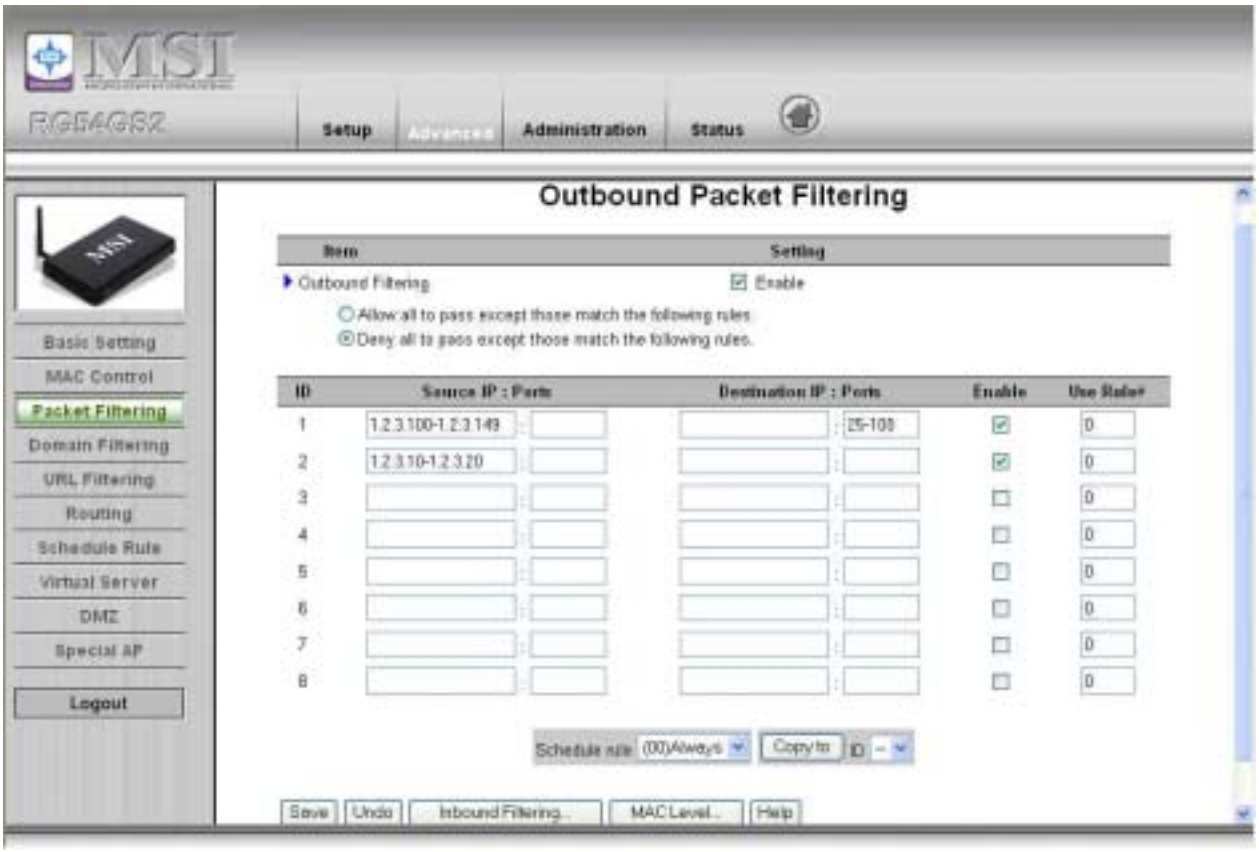
每個規則都可以單獨啟用或停用。

Inbound Filter（輸入過濾）：

若要啟用**輸入封包過濾**，請按一下 **Inbound Packet Filter** 欄位中 **Enable** 旁的核取方塊。

假設您在虛擬伺服器或 DMZ 主機中定義了 SMTP 伺服器（25）、POP 伺服器（110）、Web 伺服器（80）、FTP 伺服器（21）和 News 伺服器（119）。

**範例1：**




（1.2.3.100-1.2.3.149）它們可以傳送郵件（埠 25）、接收郵件（埠 25）以及瀏覽網際網路（埠 80）。

（1.2.3.10-1.2.3.20）它們可以進行所有作業（沒有任何封鎖）。

其它全部封鎖。

**範例2：**


（1.2.3.100-1.2.3.119）它們可以進行讀取新聞（埠 119）和透過 FTP 傳送檔案（埠 21）以外的任何作業。其它全部允許。

設定 **Inbound Packet Filter** 組態之後，請按一下 **save（儲存）**按鈕。

Outbound Filter（輸出過濾）：

若要啟用**輸出封包過濾**，請按一下 **Outbound Packet Filter** 欄位中 **Enable** 旁的核取方塊。

**範例1：**


(192.168.1.100-192.168.1.149) 它們可以傳送郵件（埠 25）、接收郵件（埠 25）以及瀏覽網際網路（埠 80）；需有埠 53（DNS）才能解析網域名稱。

（192.168.1.10-192.168.1.20）它們可以進行所有作業（沒有任何封鎖）。

其它全部封鎖。

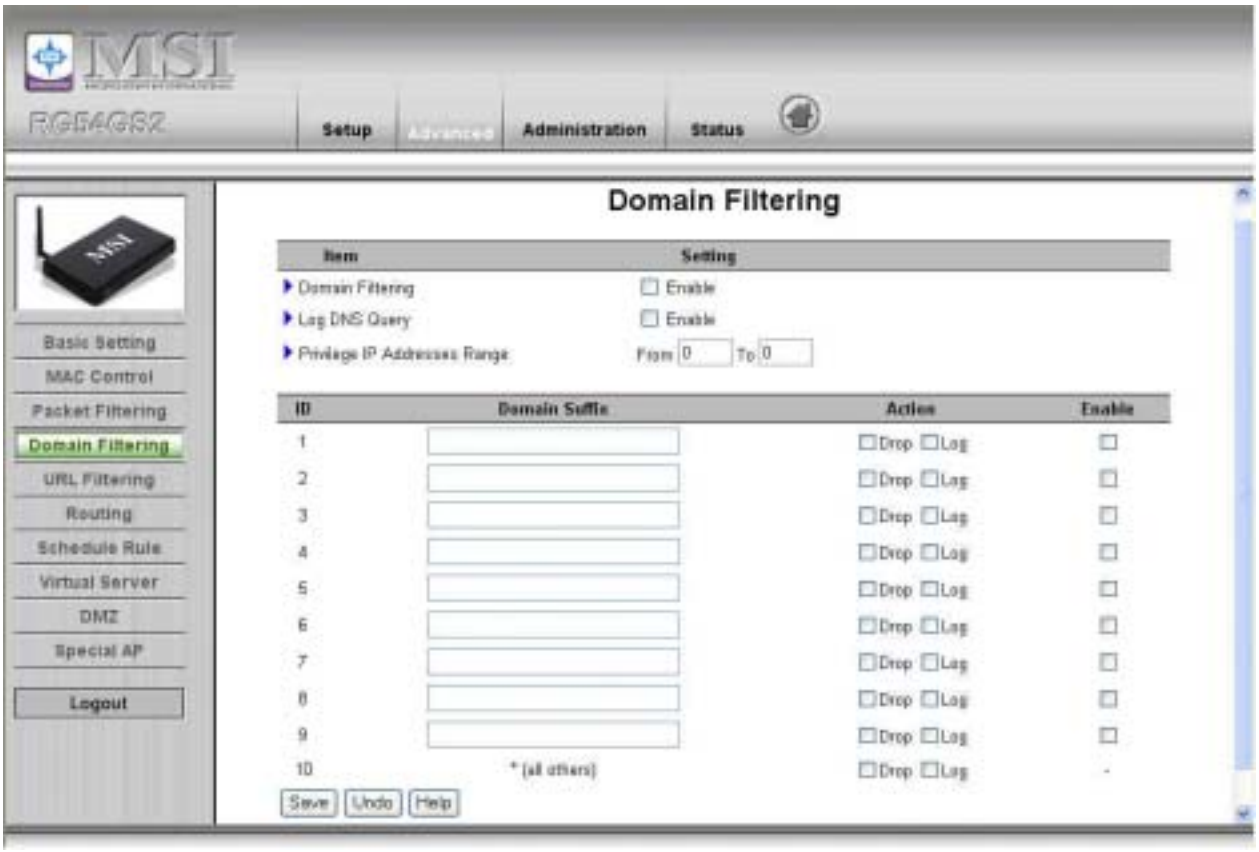
**範例2：**


（192.168.1.100-192.168.1.119）它們可以進行讀取新聞（埠 119）和透過 FTP 傳送檔案（埠 21）以外的任何作業。

其它則都允許。

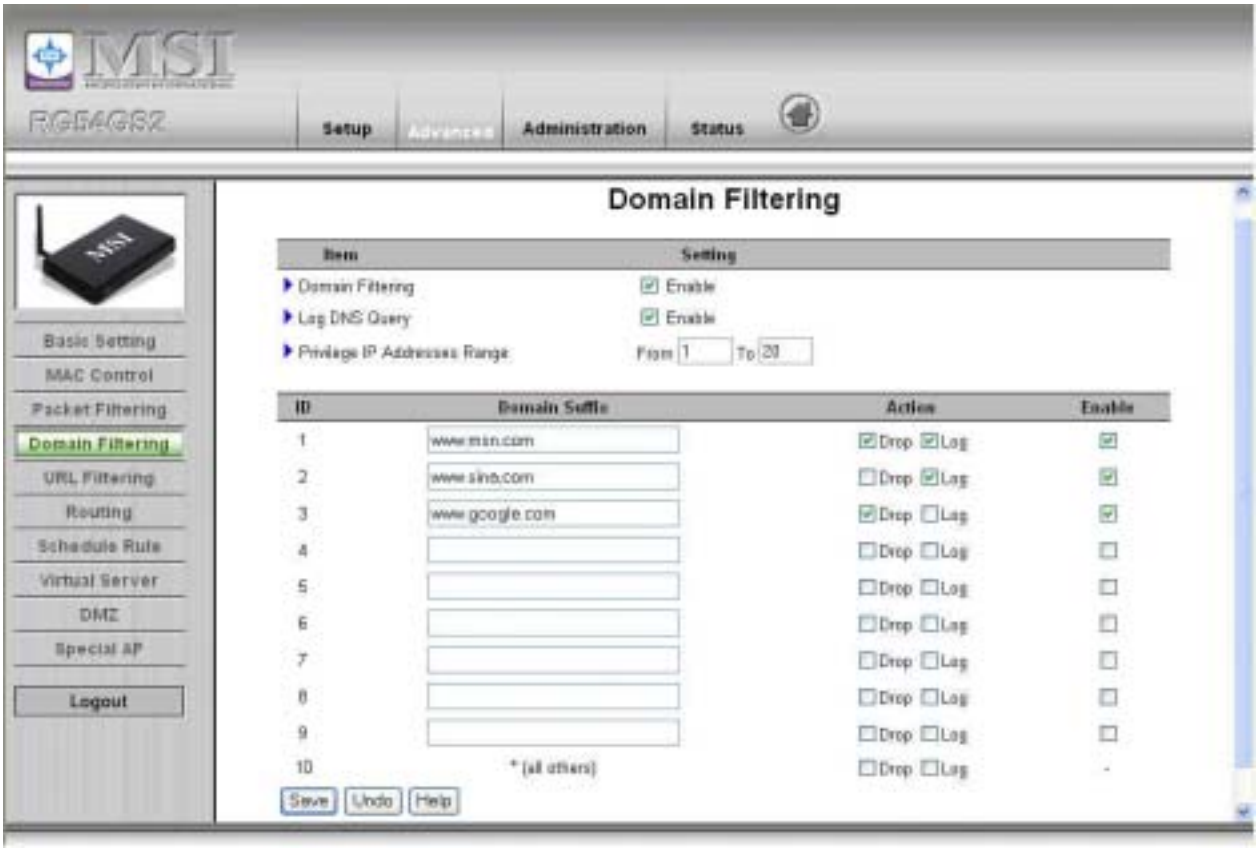
設定 **Outbound Packet Filter** 組態之後，請按一下 **save（儲存）**按鈕。

## 66. 4.4.4 Domain Filtering（網域過濾）




**Domain Filter（網域過濾）**
可防止本裝置下的使用者存取特定 URL。
**Domain Filter Enable（網域過濾啟用）**
如果要啟用網域過濾請勾選此項。
**Log DNS Query（記錄 DNS 查詢）**
如果要記錄某人存取特定 URL 的行動請勾選此項。
**Privilege IP Addresses Range（優先 IP 位址範圍）**
設定主機群組，並賦予權限使其可以自由存取網路。
**Domain Suffix（網域尾碼）**
要限制存取的 URL 尾碼。例如「com」和「xxx.com」。
**Action（動作）**
若有人正在存取符合網址尾碼的 URL，您所要採取的動作。
勾選 Drop 可封鎖存取。勾選 Log 則記錄這些存取。
**Enable（啟用）**
勾選可啟用各規則。

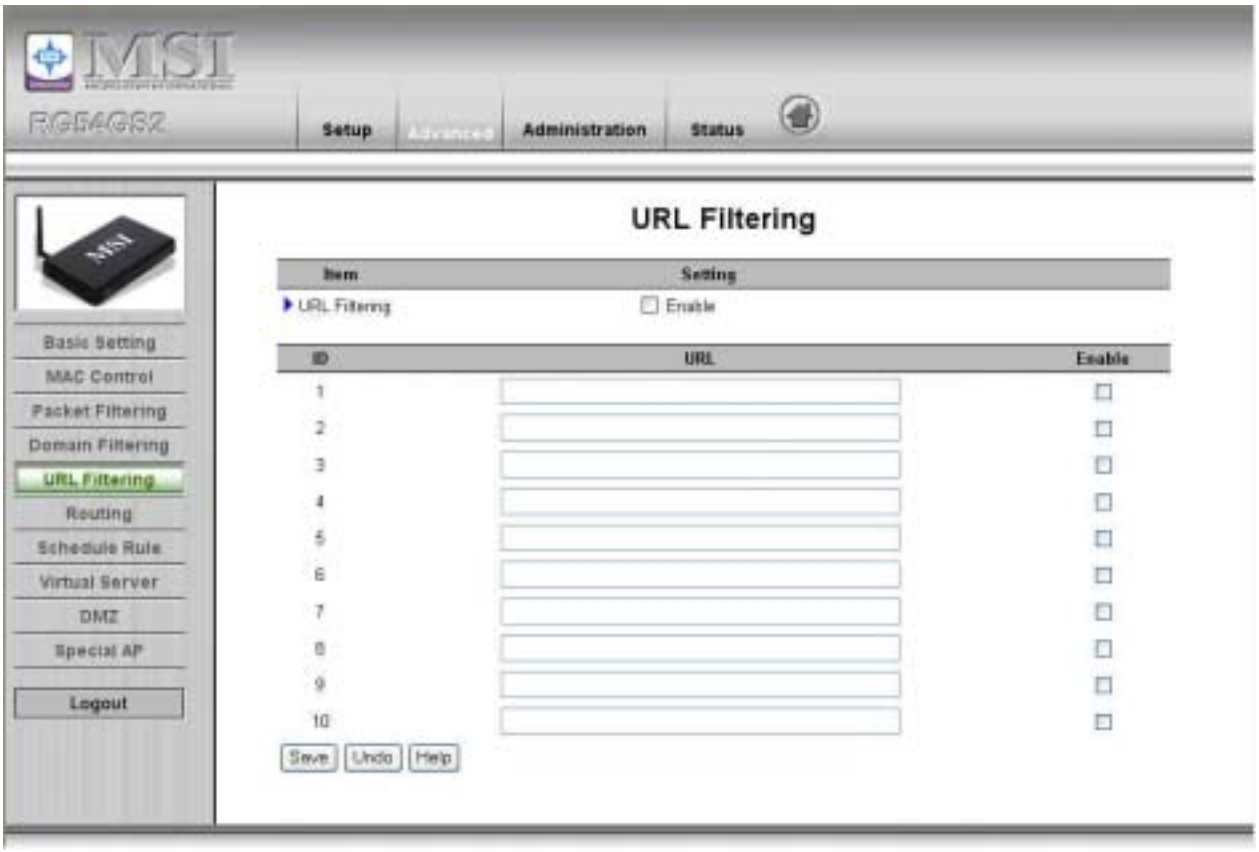
**範例：**




在此範例中：

1. 網址中包含「www.msn.com」的網站都會遭封鎖，動作也會記錄到日誌檔中。
2. 網址中包含「www.sina.com」的網站不會遭封鎖，但動作會記錄到日誌檔中。
3. 網址中包含「www.google.com」的網站都會遭封鎖，但動作不會記錄到日誌檔中。
4. IP 位址 X.X.X.1~X.X.X.20 可以自由存取網路。

## 67. 4.4.5 URL Filtering（URL過濾）




**URL Blocking** 可封鎖區域網路電腦連線到預先定義的網站。
「Domain filter」和「URL Blocking」的不同之處在於，Domain filter 會要求使用者輸入尾碼（如 com 或.org 等），而 URL Blocking 則只會要求使用者輸入一個關鍵字。換句話說，Domain filter 可以封鎖特定網站，而 URL Blocking 則透過一個**關鍵字**就可以封鎖數百個網站。

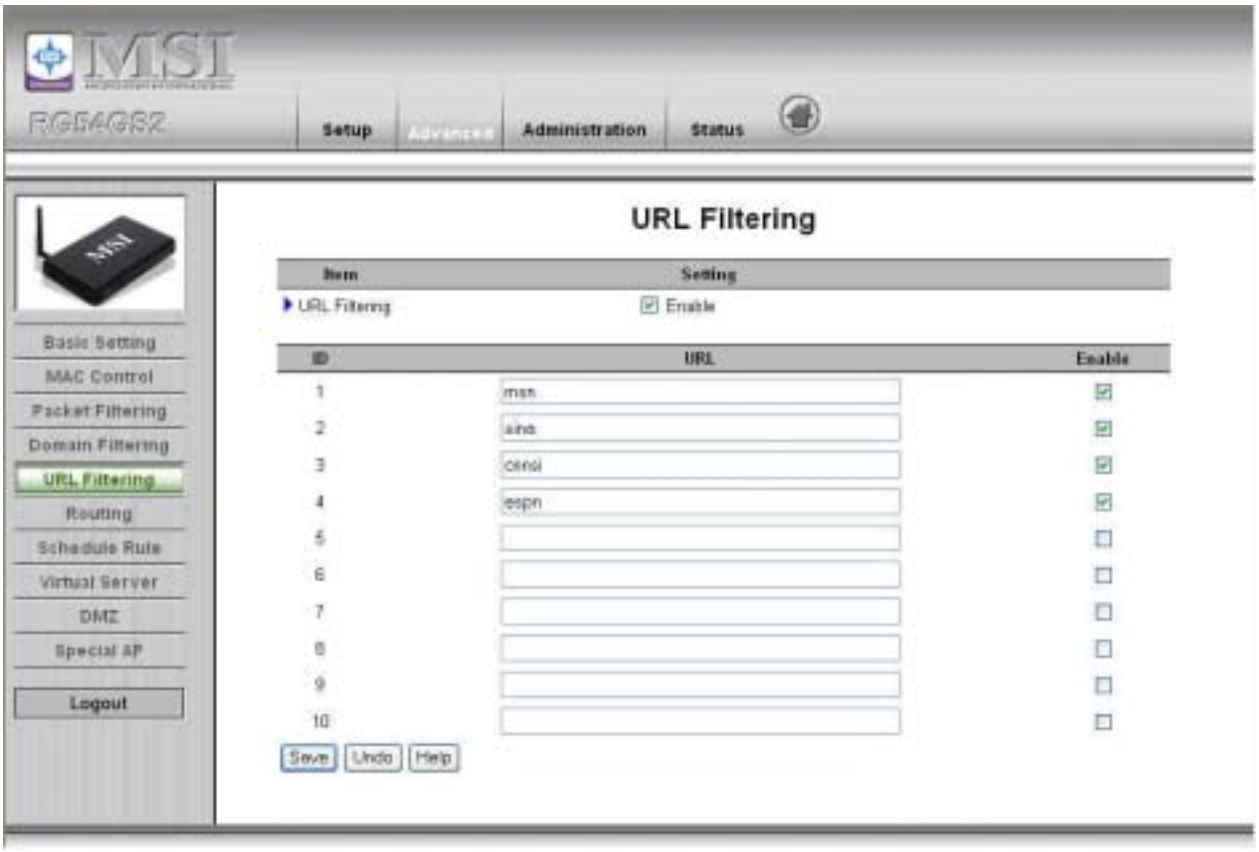
**URL Blocking Enable（啟用 URL 封鎖）**
如果要啟用 URL 封鎖請勾選此項。

**URL**

如果網站 URL 的任何部分符合預先定義的字，連線就會遭封鎖。
例如，可使用預先定義字「sex」來封鎖 URL 中包含預先定義字「sex」的所有網站。

**Enable（啟用）**

勾選可啟用各規則。




在此範例中：

1. URL 中包含「msn」的網站都會遭封鎖，動作會記錄到日誌檔中。
2. URL 中包含「sina」的網站都會遭封鎖，但動作會記錄到日誌檔中。
3. URL 中包含「cnnsi」的網站不會遭封鎖，但動作會記錄到日誌檔中。
4. URL 中包含「espn」的網站都會遭封鎖，但動作會記錄到日誌檔中。

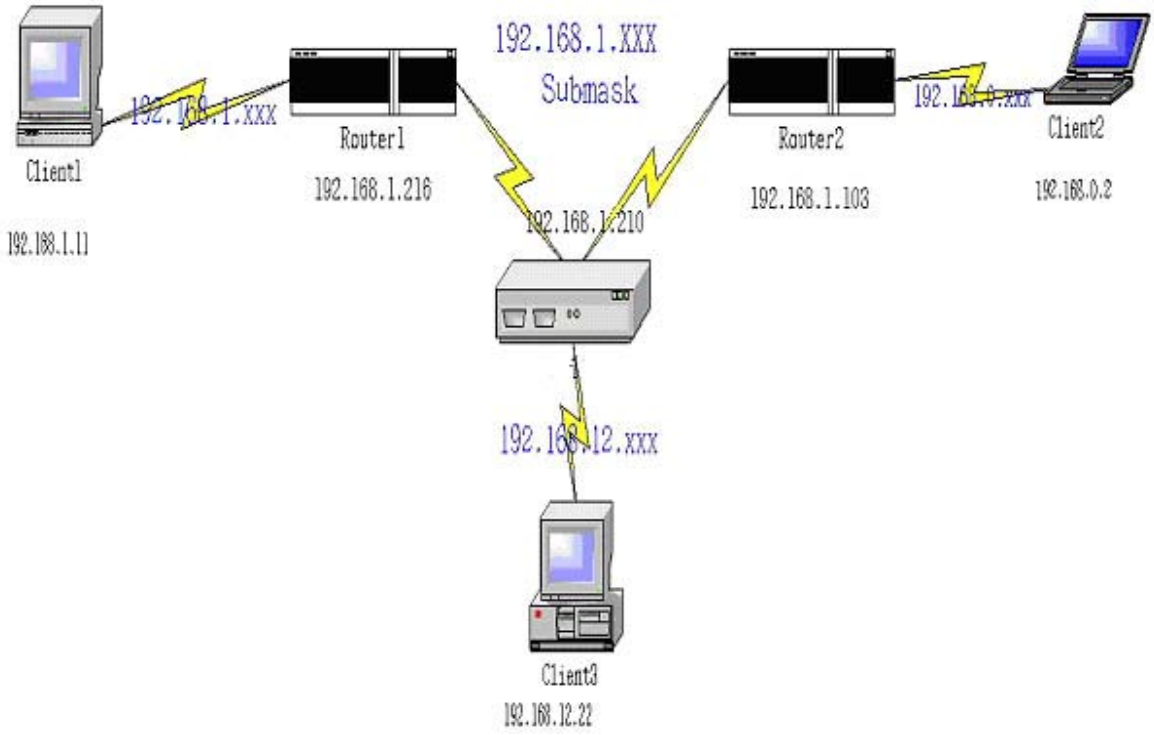
**68. 4.4.6 Routing Table（路由表）**


**Routing Table** 可讓您決定哪些實體介面位址要用於輸出 IP 資料包。如果您的分享器和子網路不只一個，則需要啟用路由表以允許封包尋找適當的路由路徑以及讓不同的子網路可以相互通訊。

Routing Table 設定是用於設定靜態功能的組態。

**Static Routing（靜態路由）**：就靜態路由而言，最多可以指定 8 個路由規則。您可以為每個路由規則輸入目的 IP 位址、子網路遮罩、閘道和躍點，再勾選或取消勾選 Enable 核取方塊以啟用或停用規則。

**範例：**

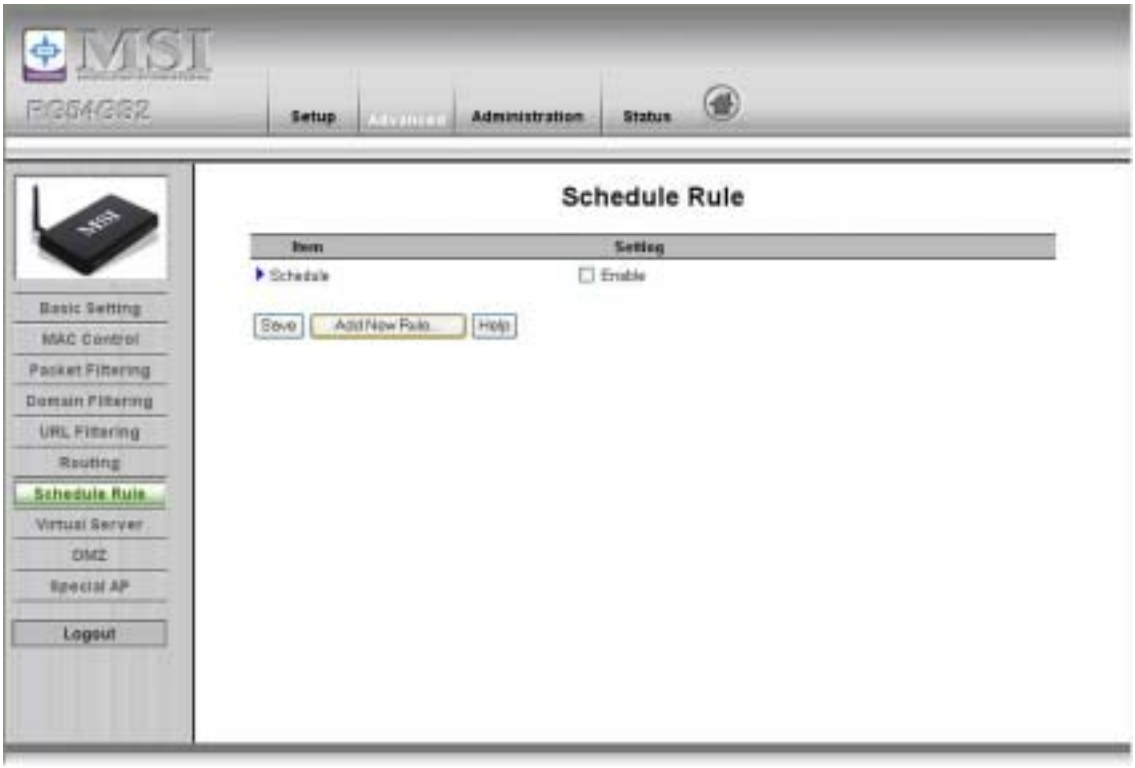



NAT 分享器的組態

| 目的 | 子網路遮罩 | 閘道 | 躍點 | 啟用 |
|---|---|---|---|---|
| 192.168.1.0 | 255.255.255.0 | 192.168.1.216 | 1 | ˇ |
| 192.168.0.0 | 255.255.255.0 | 192.168.1.103 | 1 | ˇ |

例如，client3 要傳送 IP 資料包到 192.168.0.2，它使用上表判斷必須經由 192.168.1.103（閘道器）進行。
如果傳送封包到 192.168.1.11 則必須經由 192.168.1.216 進行。
每個規則都可以單獨啟用或停用。
設定**路由表**組態之後，請按一下 **save（儲存）**按鈕。

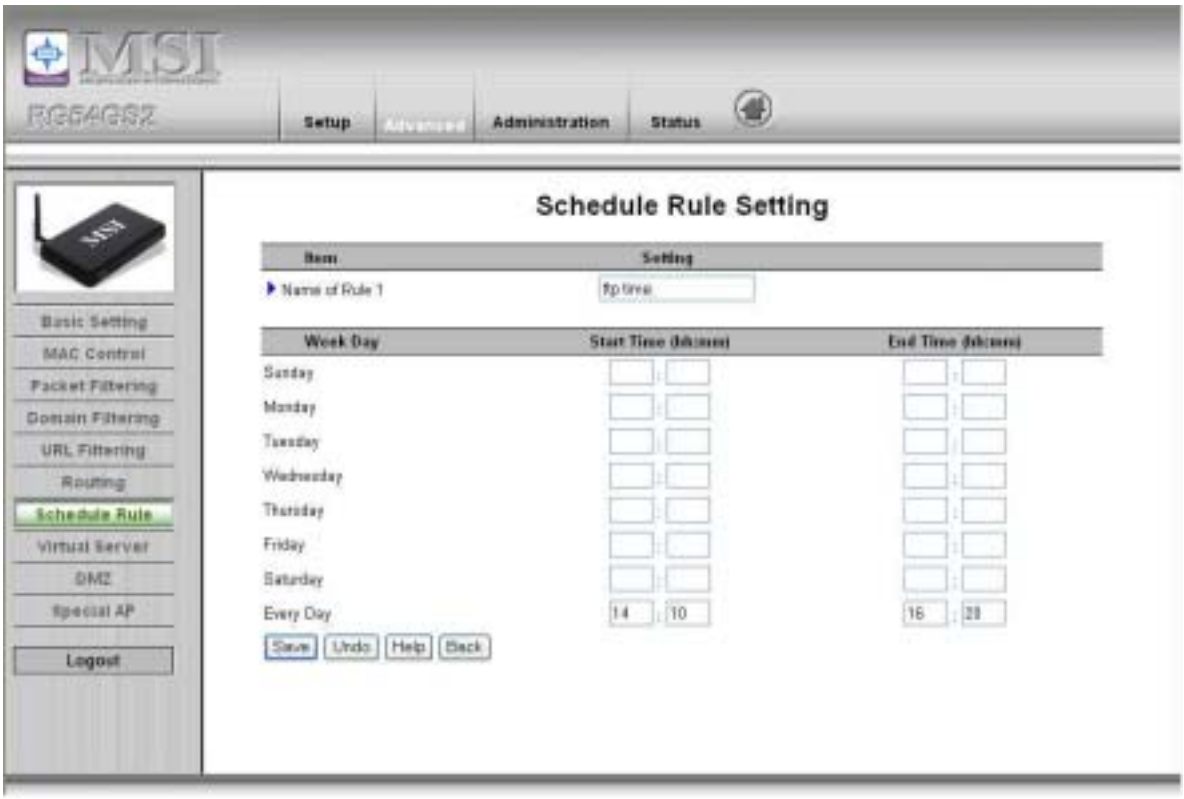
**69. 4.4.7 Schedule Rule（時程規則）**



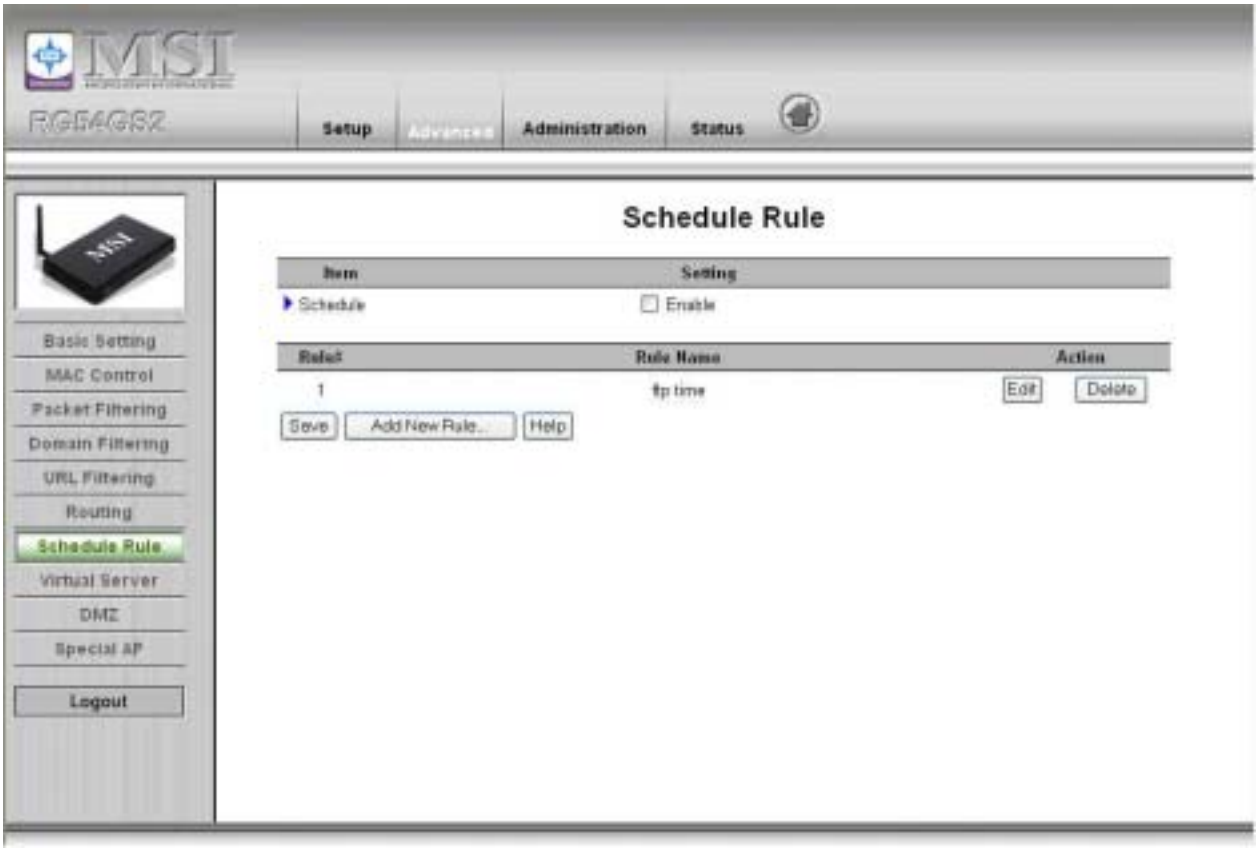

您可以設定時程決定服務何時開放或關閉。選取「enable」（啟用）項目

按**「Add New Rule」（新增新規則）**

可以寫入規則名稱並設定時程「Start Time」（起始時間）和「End Time」（結束時間）的日期和時間。下列範例設定每天 14：10 至 16：20 為「FTP 時間」

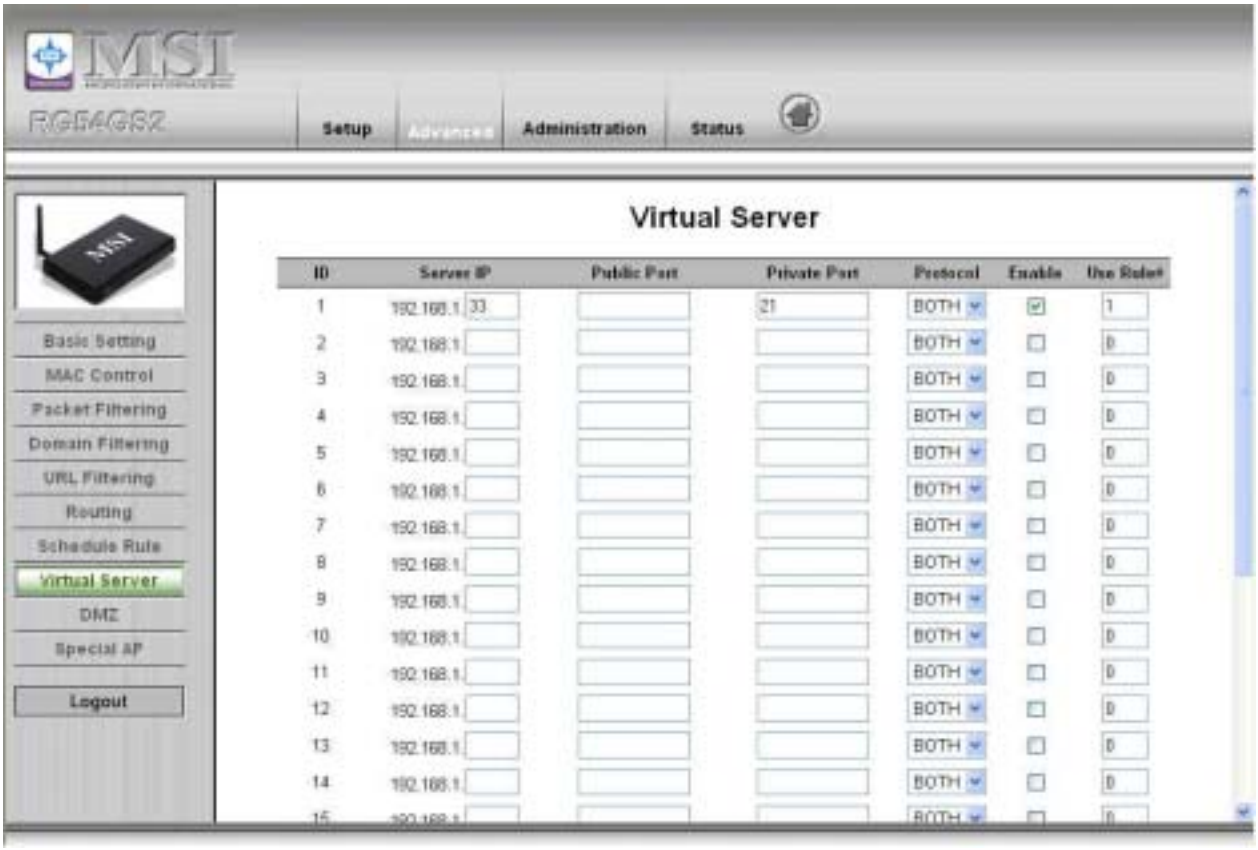


**設定 Rule 1 之後→**

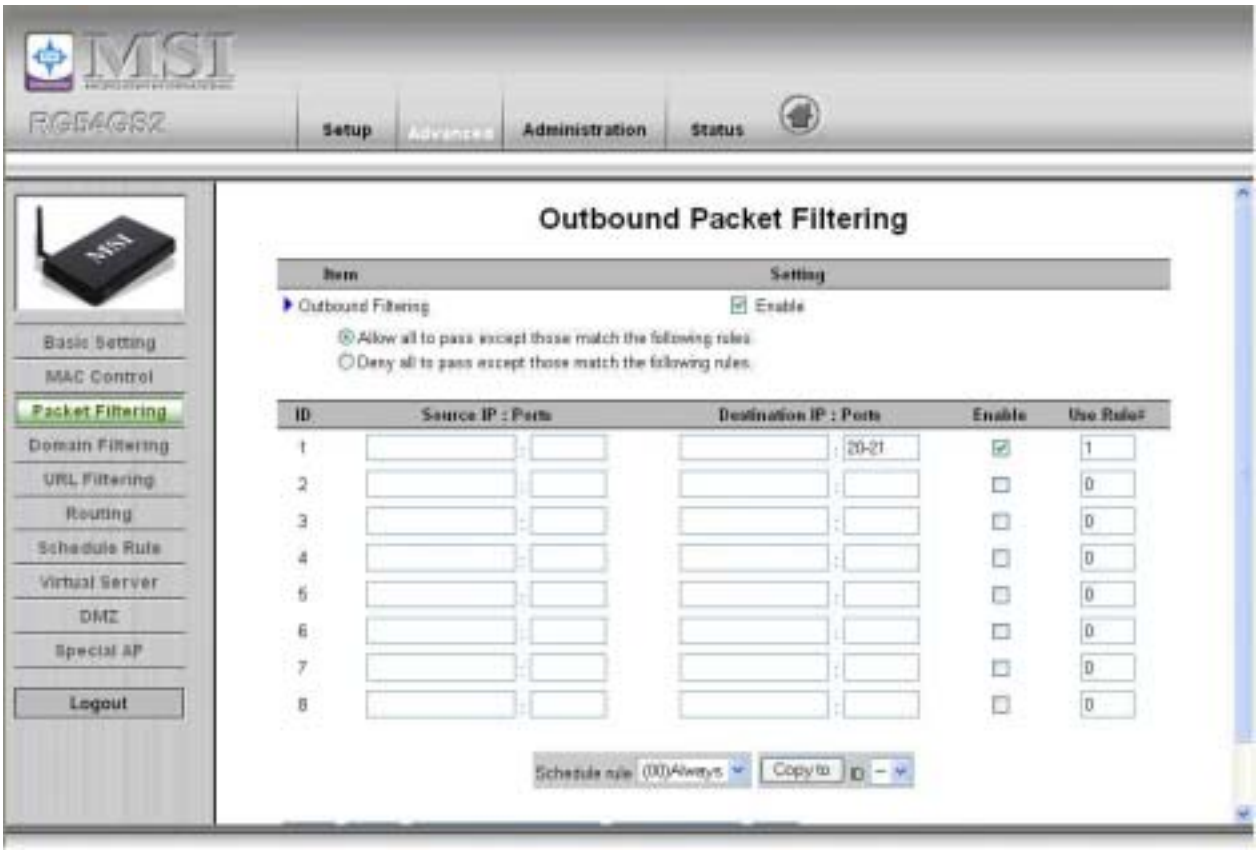



**Schedule Enable（啟用時程）**
如果要啟用時程計算器請選取此項。
**Edit（編輯）**
可編輯時程規則。
**Delete（刪除）**
可刪除時程規則，已刪除規則之後的規則編號（rule#）會自動減號。
Schedule Rule 適用於虛擬伺服器和封包過濾功能，例如：

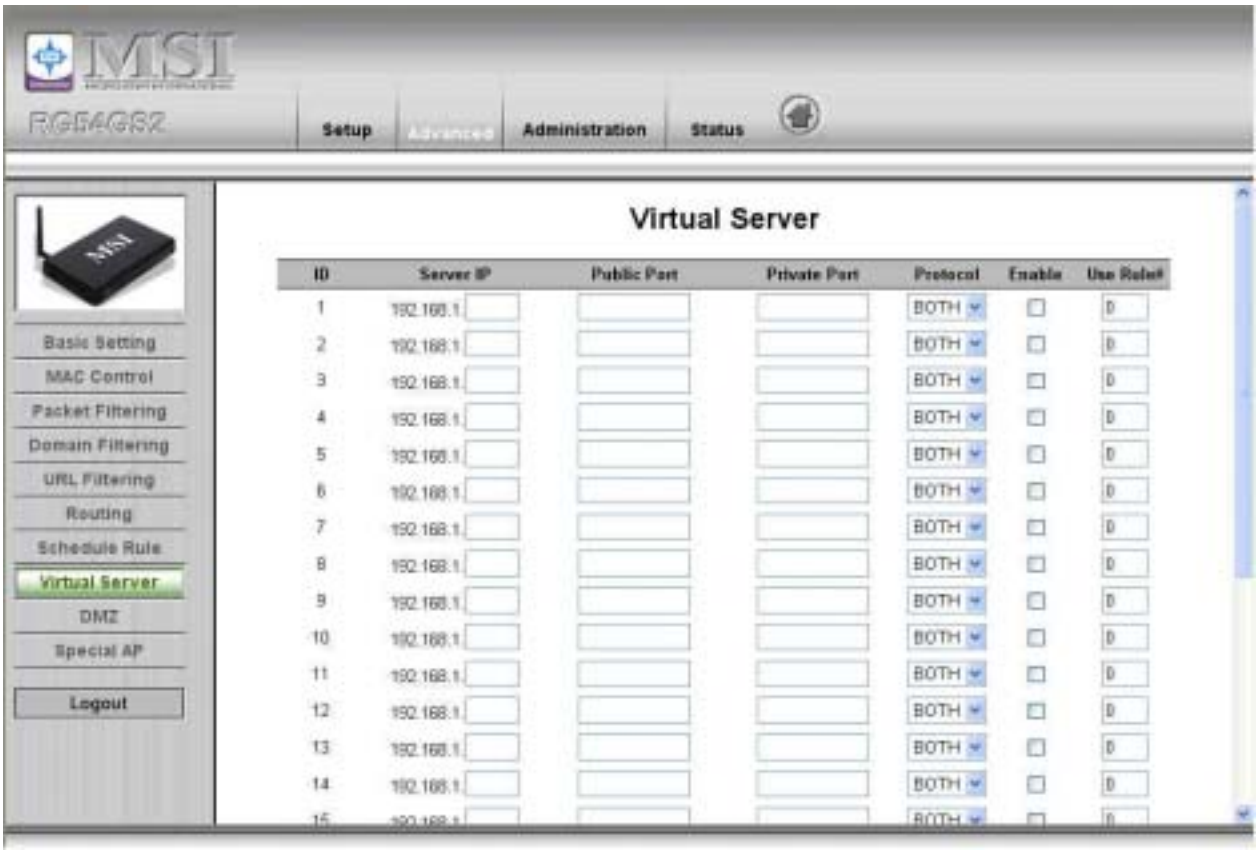
範例：**Virtual Server**－套用 Rule#1（FTP 時間：每天 14：10 至 16：20）




範例：**Packet Filter**－套用 Rule#1（FTP 時間：每天 14：10 至 16：20）



### 70. 4.4.8 Virtual Server（虛擬伺服器）



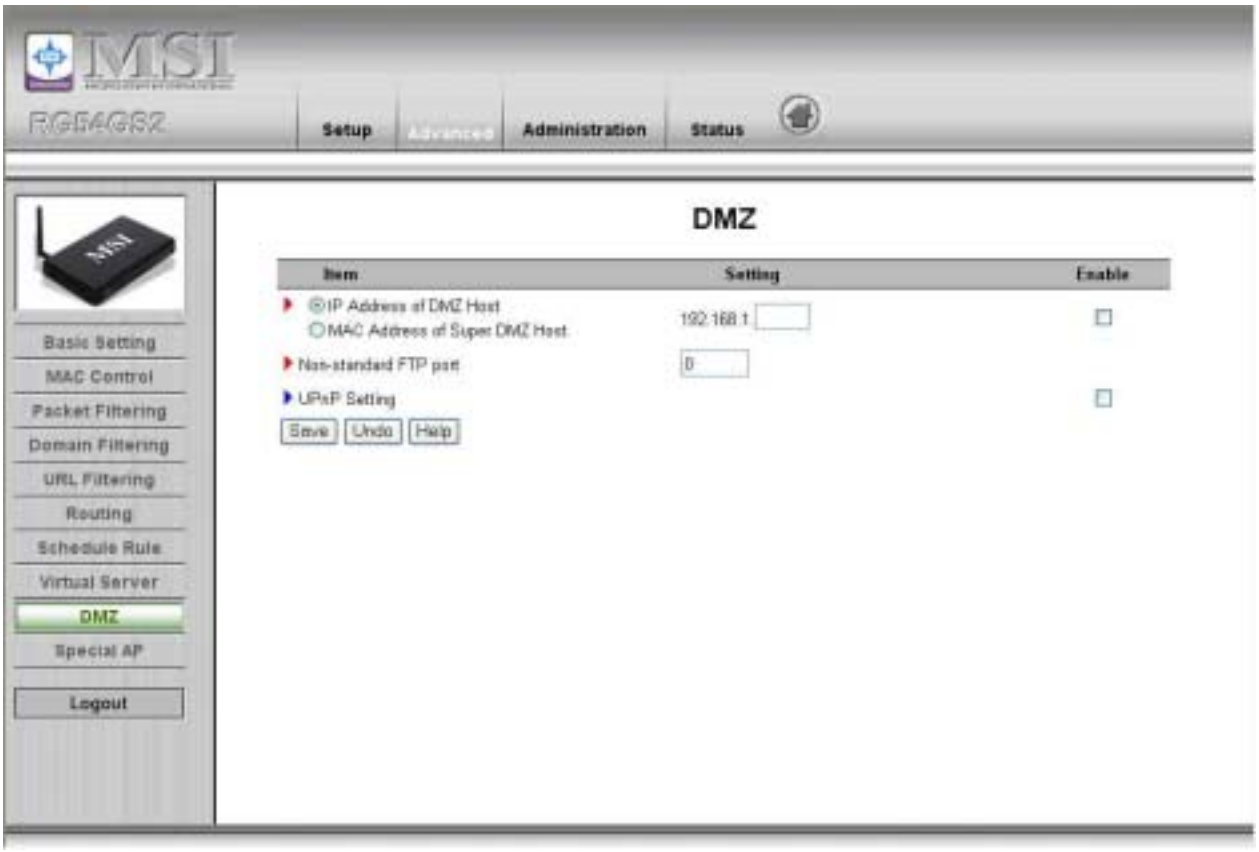

本產品的 NAT 防火牆會過濾掉未經認可的封包以保護您的內部網路；本產品保護下的主機外界皆無從看見。如果要開放讓某些人存取，啟用 Virtual Server Mapping（虛擬伺服器對應）即可。

將虛擬伺服器定義為**服務埠**，所有傳送到此埠的的要求都會重新導向至 **Server IP（伺服器 IP）**所指定的電腦。**Virtual Server** 可與 **Scheduling Rules** 一起使用，讓使用者具有更靈活的存取控制。如需詳細資訊，請參閱 **Scheduling Rule**。

例如，您有 FTP 伺服器（埠 21）位於 192.168.1.1，Web 伺服器（埠 80）位於 192.168.1.2 以及 VPN 伺服器位於 192.168.1.6，接著您需要設定下列虛擬伺服器對應表：

| 服務埠 | 伺服器 IP | 啟用 |
|---|---|---|
| 21 | 192.168.1.1 | V |
| 80 | 192.168.1.2 | V |
| 1723 | 192.168.1.6 | V |

**71. 4.4.9 DMZ**

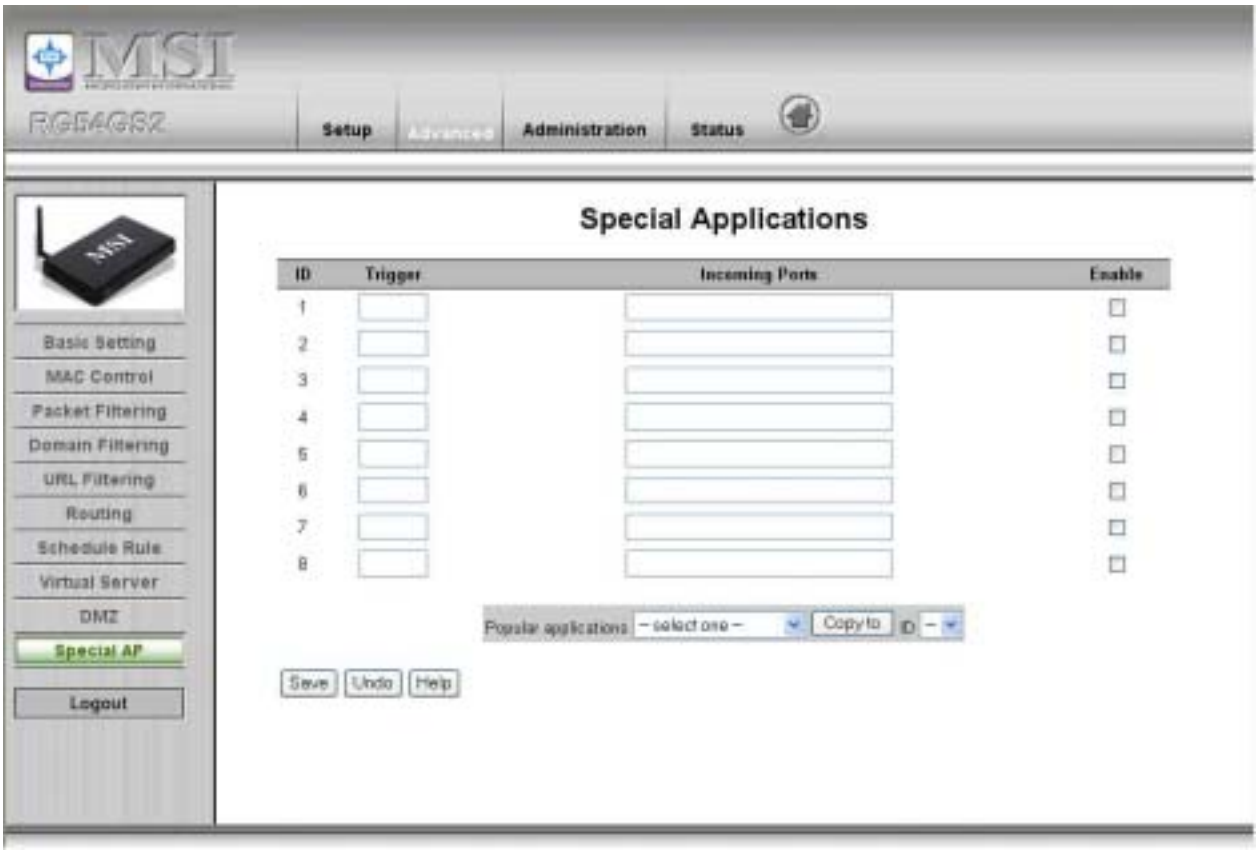



**IP Address of DMZ Host（DMZ 主機的 IP 位址）**
DMZ（非軍事區）主機是沒有防火牆保護的主機。它允許電腦開放在沒有限制的雙向通訊中，以便網路遊戲、視訊會議、網路電話和其他特殊應用程式自由存取網路。

注意：此功能只有在需要時才能使用。

**Non-standard FTP port（非標準 FTP 埠）**
如果要存取埠號非 21 的 FTP 伺服器，必須設定此項目。此設定在重新開機之後會取消。

## 72. 4.4.10 Special AP（特殊AP）



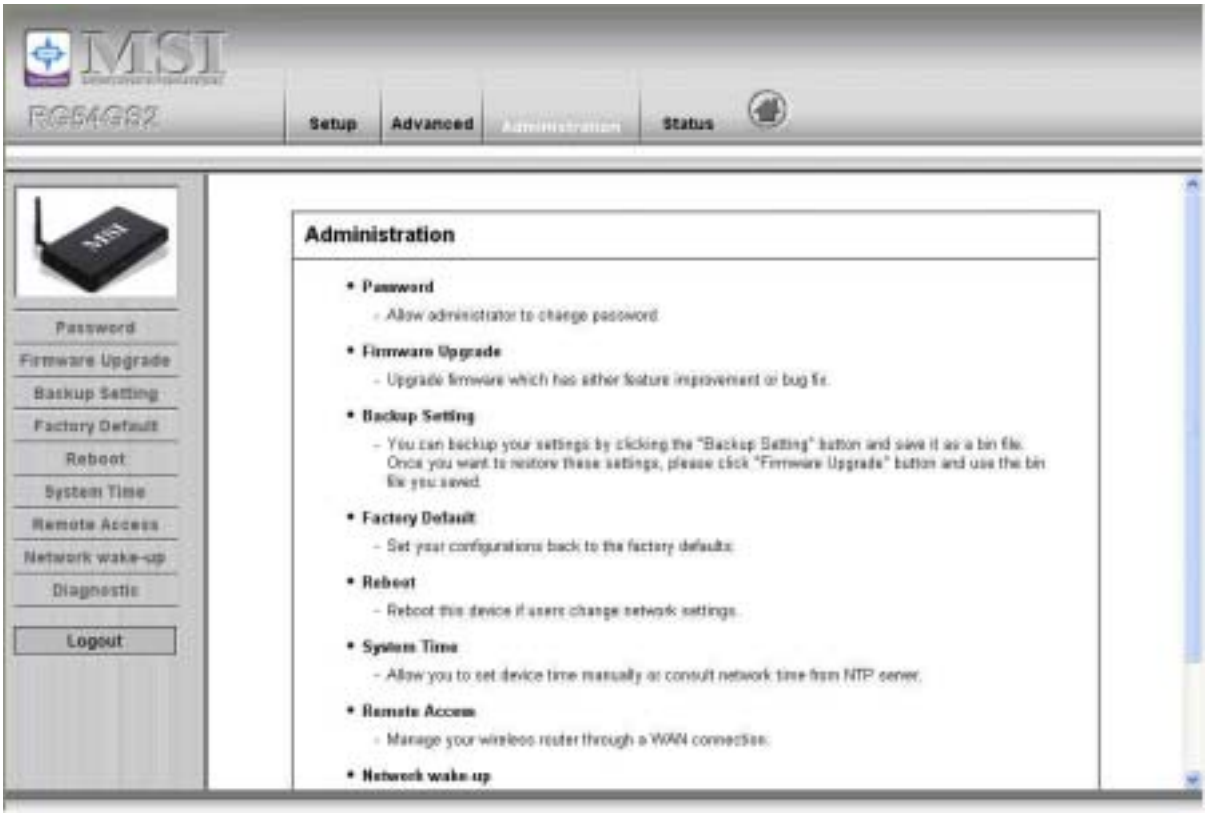

線上遊戲、視訊會議和網路電話等應用程式需要多方連線，但因為防火牆功能，這些應用程式無法與純 NAT 分享器一起使用。**Special Applications（特殊應用程式）**功能可讓上述部分應用程式與本產品一起使用。如果特殊應用程式的機制無法使應用程式正常運作，請嘗試將電腦設定為 **DMZ** 主機。

1. **Trigger（觸發器）**：應用程式所發的輸出埠號。
2. **Incoming Ports（內送埠）**：偵測到觸發器封包時，輸入封包會傳送到可通過防火牆的指定埠號。

本產品提供若干預先定義的設定。請選取應用程式再按一下 **Copy to（複製到）**將預先定義的設定新增到您的清單中。

注意！無論何時，每個特殊應用程式通道都只容許一台個人電腦使用。

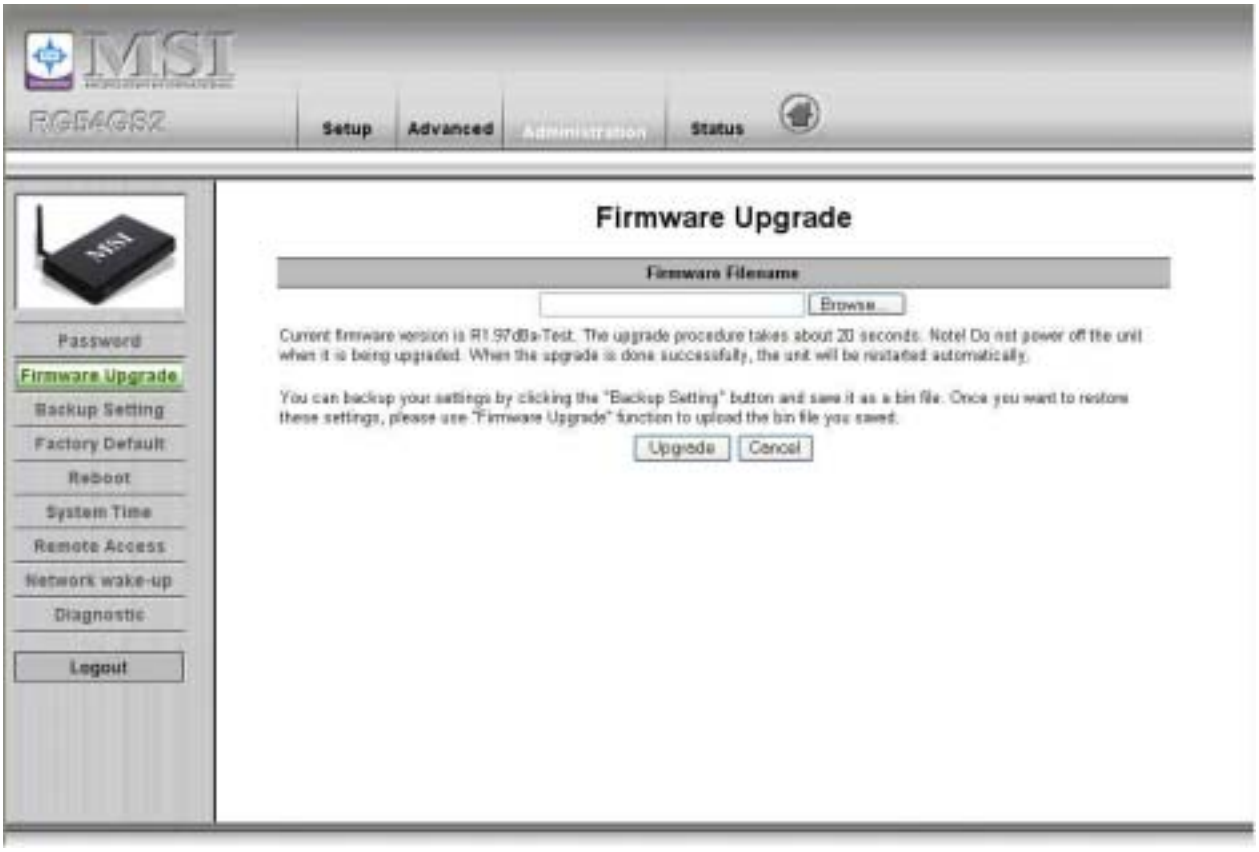
## 4.5 Administration（管理）




### 4.5.1 Change Password（變更密碼）

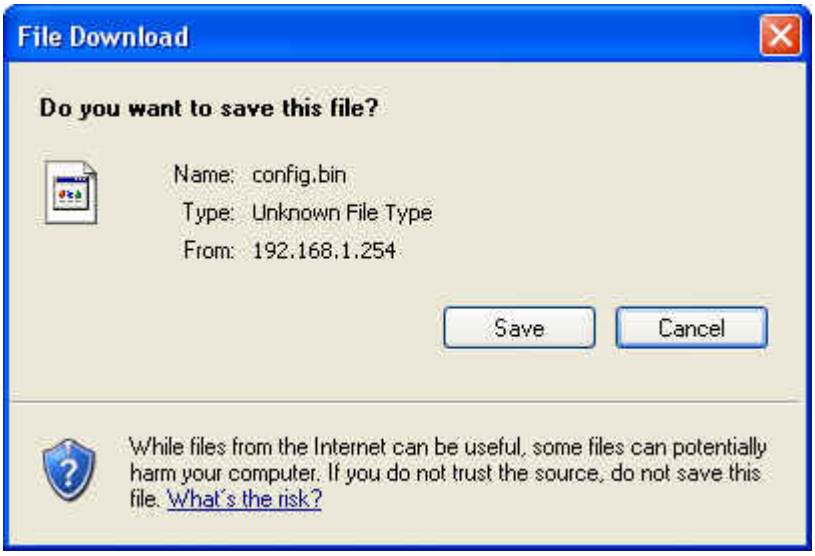

您可以在此頁面變更密碼。為安全起見，**強烈**建議您變更系統密碼。

### 4.5.2 Firmware Upgrade（韌體更新）




按一下 Firmware Upgrade 按鈕就可以更新韌體。

### 4.5.3 Backup Setting（備份設定）




按一下 **Backup Setting** 按鈕就可以備份您的設定將其儲存為 bin 檔, 如果要還原這些設定, 請按一下 **Firmware Upgrade** 按鈕並使用先前所儲存的 bin 檔。

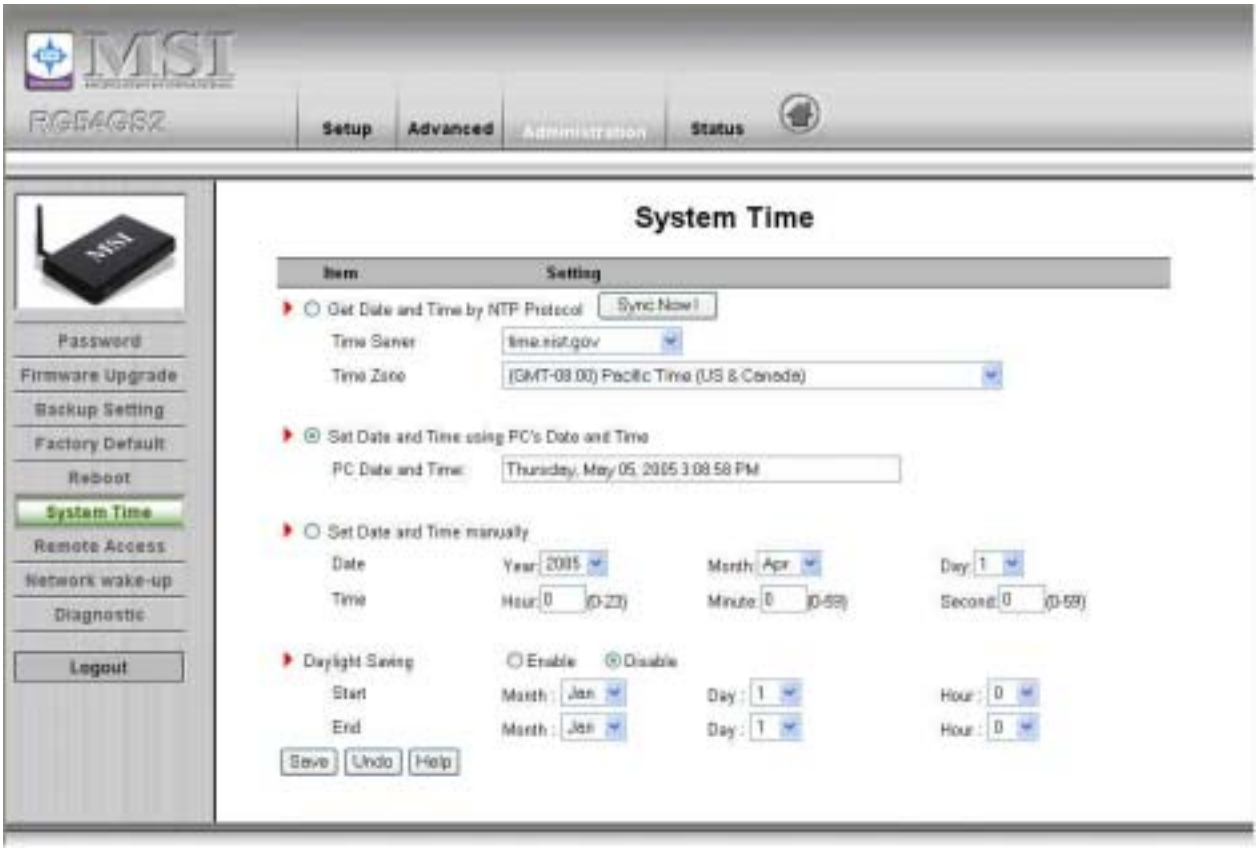
### 4.5.4 重設為出廠預設值


您也可以將本產品重設為出廠預設值，按一下 **Reset to default（重設成預設值）**按鈕即可。

### 4.5.5 Reboot（重新開機）


您也可以將本產品重新開機，按一下 **Reboot（重新開機）**按鈕即可。

### 73. 4.5.6 System Time（系統時間）




**Get Date and Time by NTP Protocol（透過 NTP 協定取得日期和時間）**
如果要透過 NTP 協定取得日期和時間請選取此項。

**Time Server（時間伺服器）**
選取一個 NTP 時間伺服器查閱 UTC 時間。

**Time Zone（時區）**
選取本裝置所在的時區。

**Set Date and Time manually（手動設定時間和日期）**
如果要手動設定時間和日期請選取此項。

**Set Date and Time manually（手動設定時間和日期）**
如果要手動設定時間和日期請選取此項。

**功能按鈕**

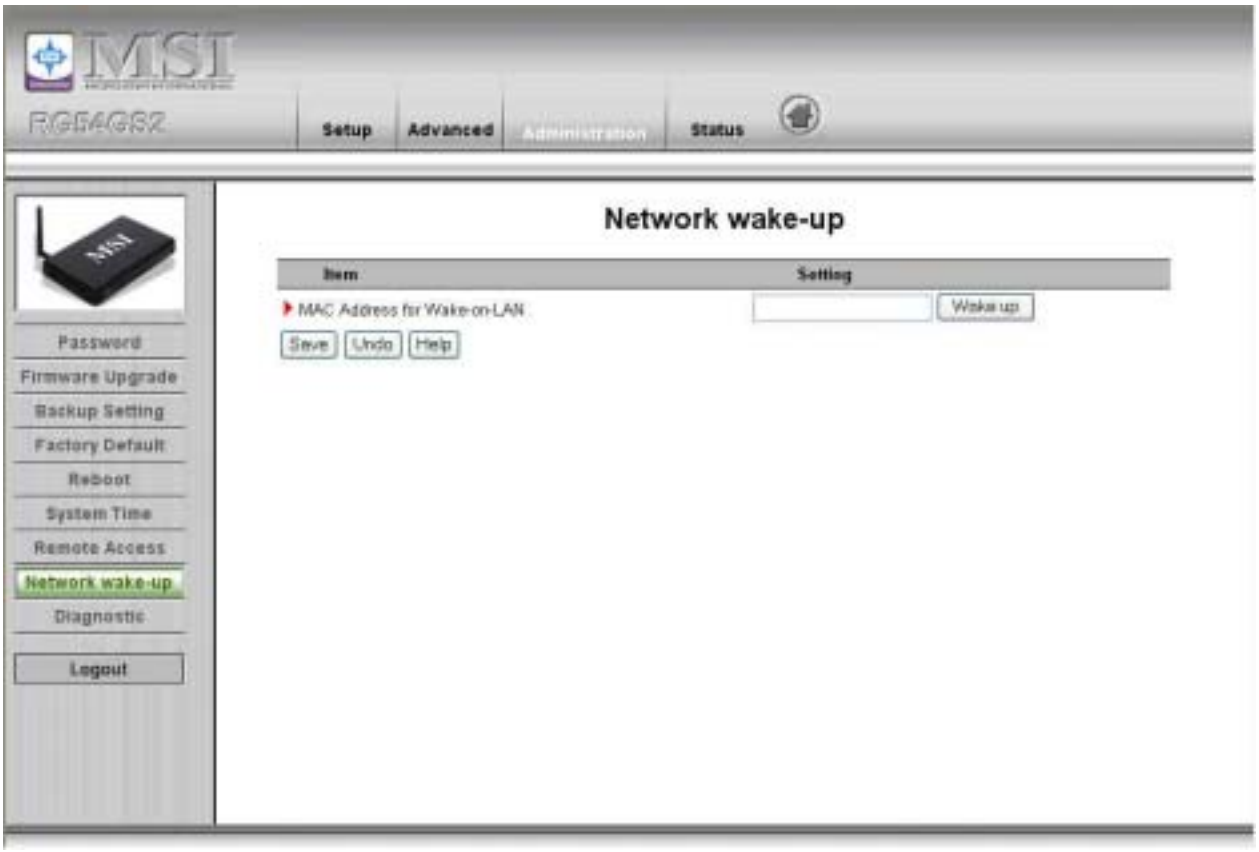
**Sync Now（即時同步）：**使系統時間與網路時間伺服器同步。

**Daylight Saving（日光節約）：**設定位置所在。

### 4.5.7 Remote Access（遠端存取）


**Remote Administrator Host/Port（遠端管理員主機/埠）**
一般而言，只有內部網路的使用者可以瀏覽內建網頁，執行管理工作，但此功能可讓您從遠端主機執行管理工作。如果啟用此功能，只有指定的 IP 位址可以執行遠端管理。如果指定的 IP 位址是 0.0.0.0，則所有主機都可以連線到本產品執行管理工作。您可以使用子網路遮罩位元「/nn」標記，指定受信任的 IP 位址群組；例如「10.1.2.0/24」。
注意：啟用遠端管理功能時，Web 伺服器埠會偏移到 88。也可以自行將 Web 伺服器埠變更至其他埠。
**Administrator Time-out（管理員等候時間）**
閒置到自動登出的時間。將此項目設為零可停用此功能。

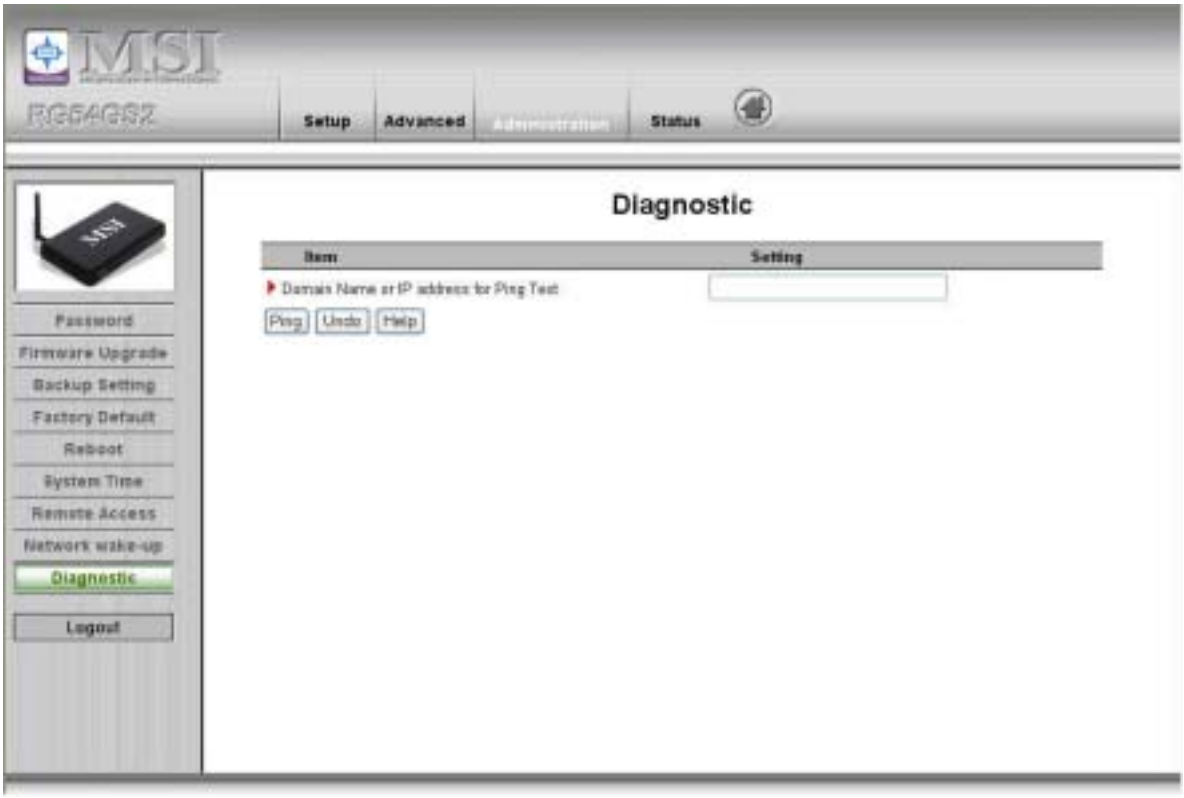
### 4.5.8 Network wake-up（網路喚醒）




**MAC Address for Wake-on-LAN（網路喚醒用的MAC位址）**

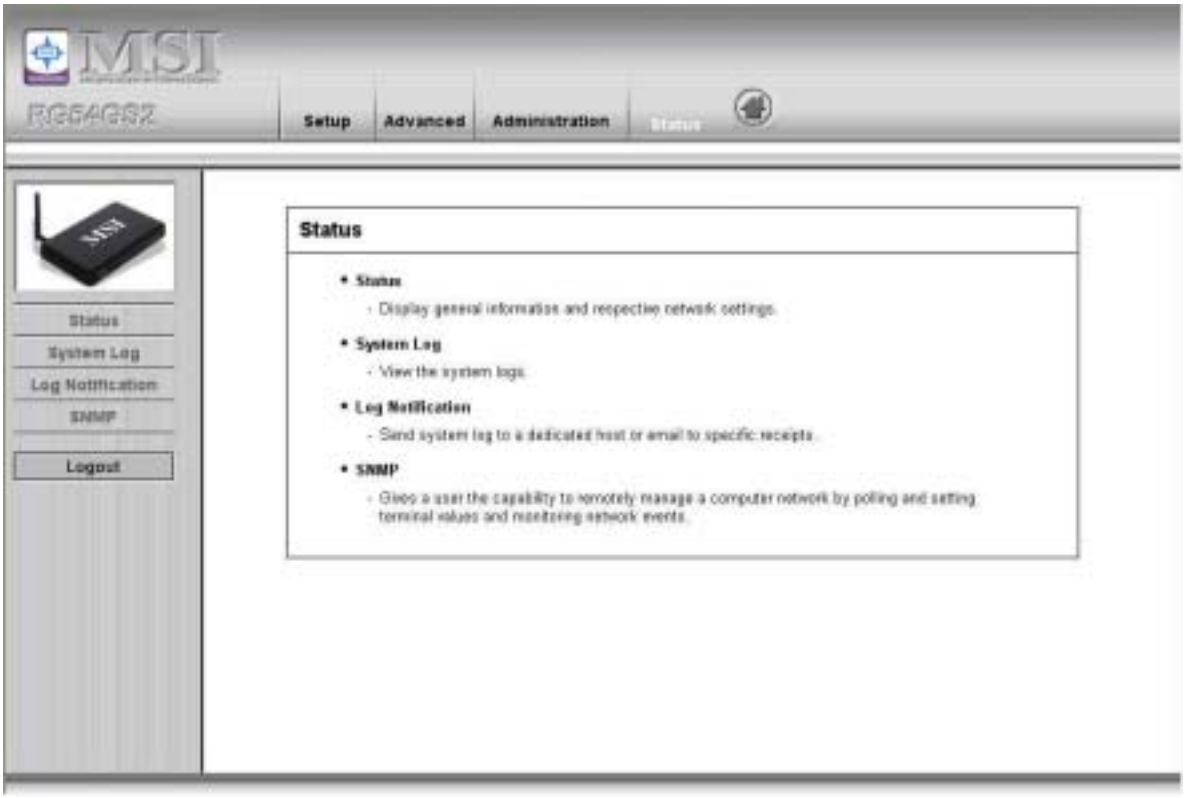
Wake-on-LAN 是一項可從遠端開啟聯網裝置的技術。為了使用此功能，目標裝置必須支援網路喚醒功能，您也必須知道本裝置的 MAC 位置（即 00-11-22-33-44-55）。按一下「Wake up」按鈕可使分享器立即傳送喚醒訊框到目標裝置。

### 4.5.9 網路診斷

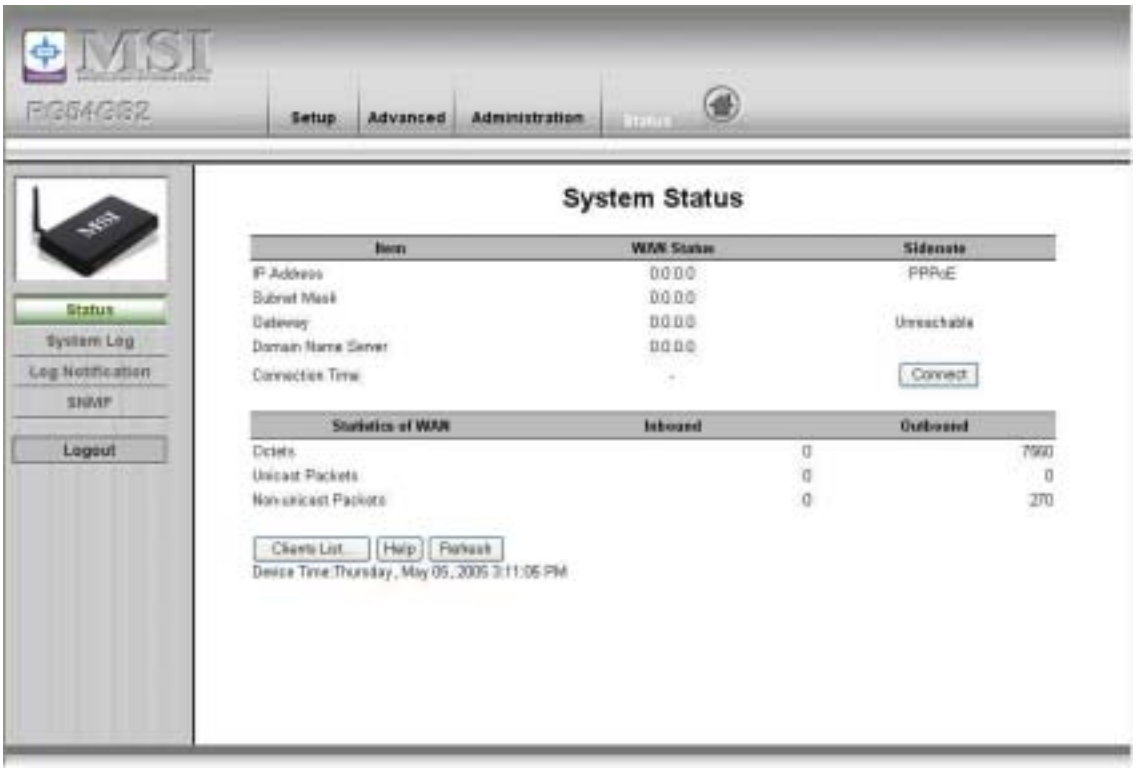



這是「**Ping**」指令的圖形介面，您可以輸入網域名稱或 IP 位置以偵測其是否正常運作。

## 4.6 Status（狀態）

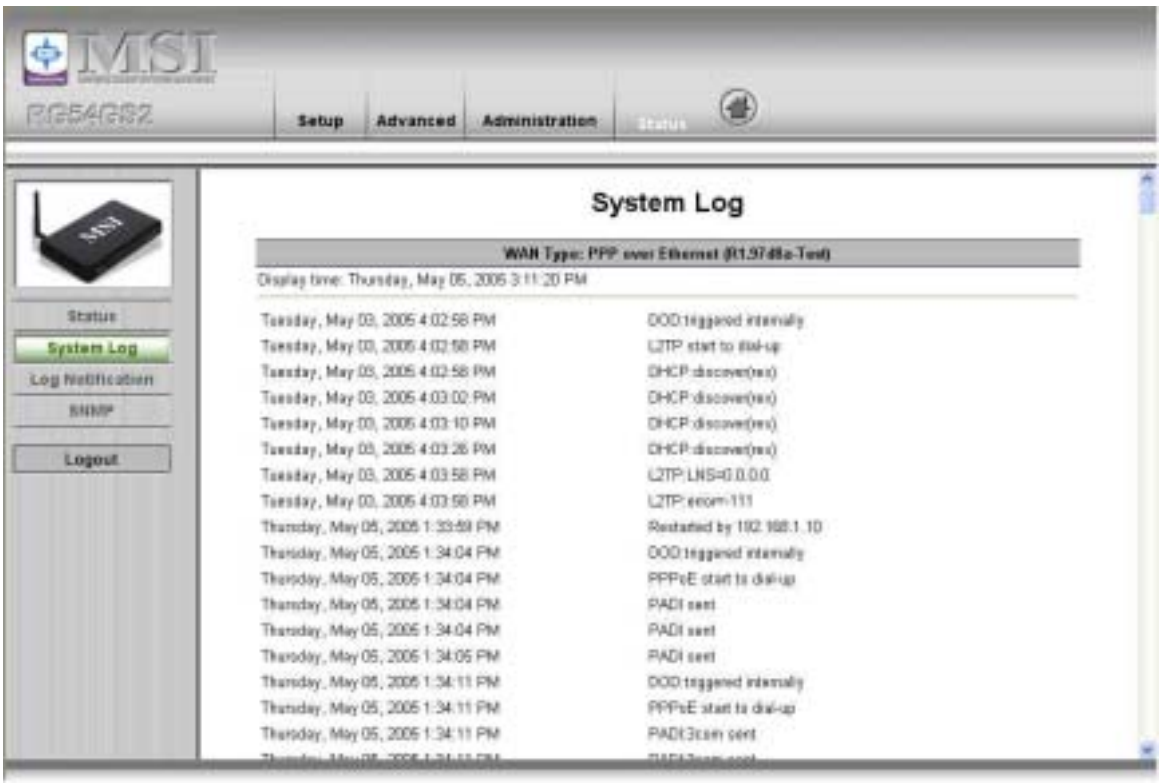


### 4.6.1 System Status（系統狀態）



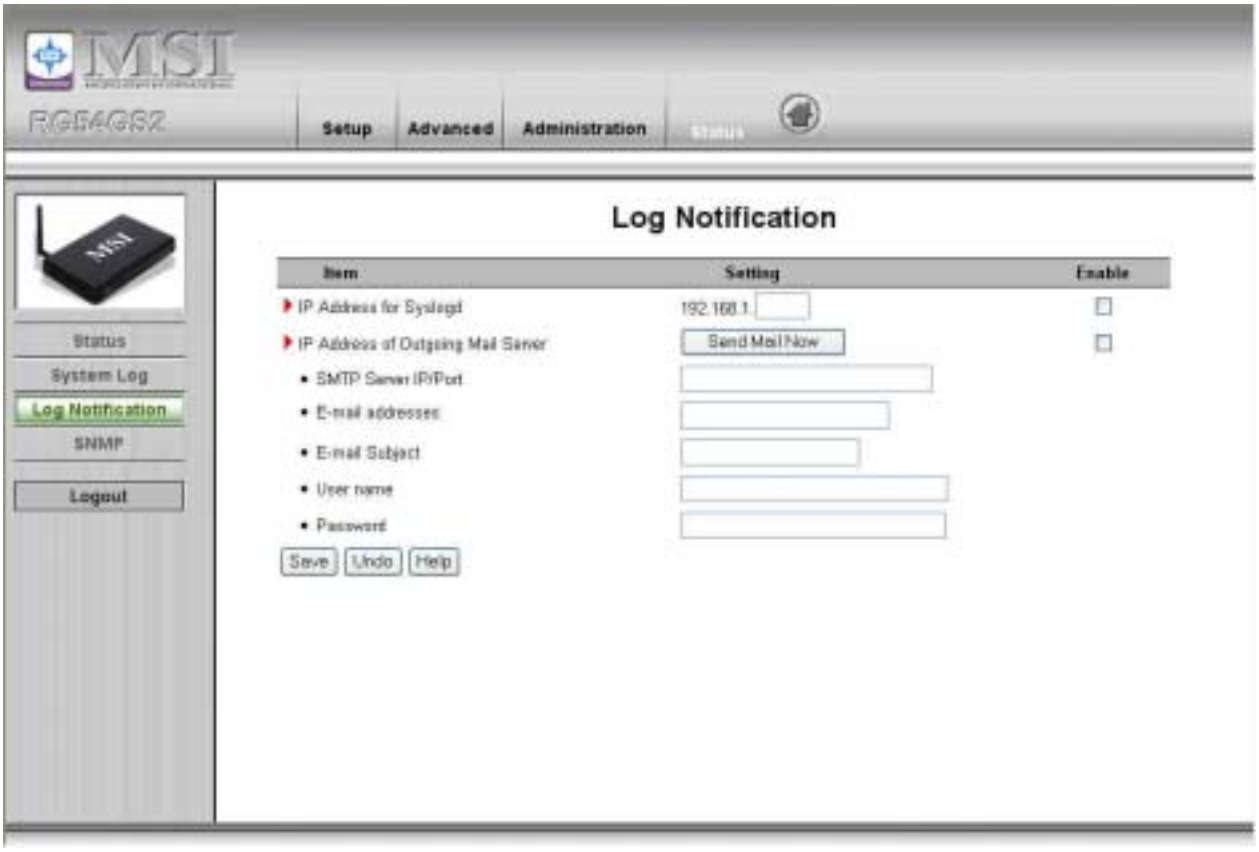

此項目顯示分享器的靜態資料。

### 4.6.2 System Log（系統日誌）




**74.　按一下** View Log（檢視日誌）**按鈕即可檢視系統日誌。**

### 4.6.3 Log Notification（日誌通知）




此頁面利用 syslog (UDP) 和 SMTP (TCP)，支援兩種可將系統日誌匯出到指定目的地的方式。必須設定的項目包括：

**IP Address for Syslog（Syslog 的 IP 位址）**

Syslog 傳送目的地的主機 IP。
勾選 **Enable** 可啟用此功能。

**E-mail Alert Enable（啟用電子郵件警示）**

如果要啟用電子郵件警示（經由電子郵件傳送）請勾選此項。

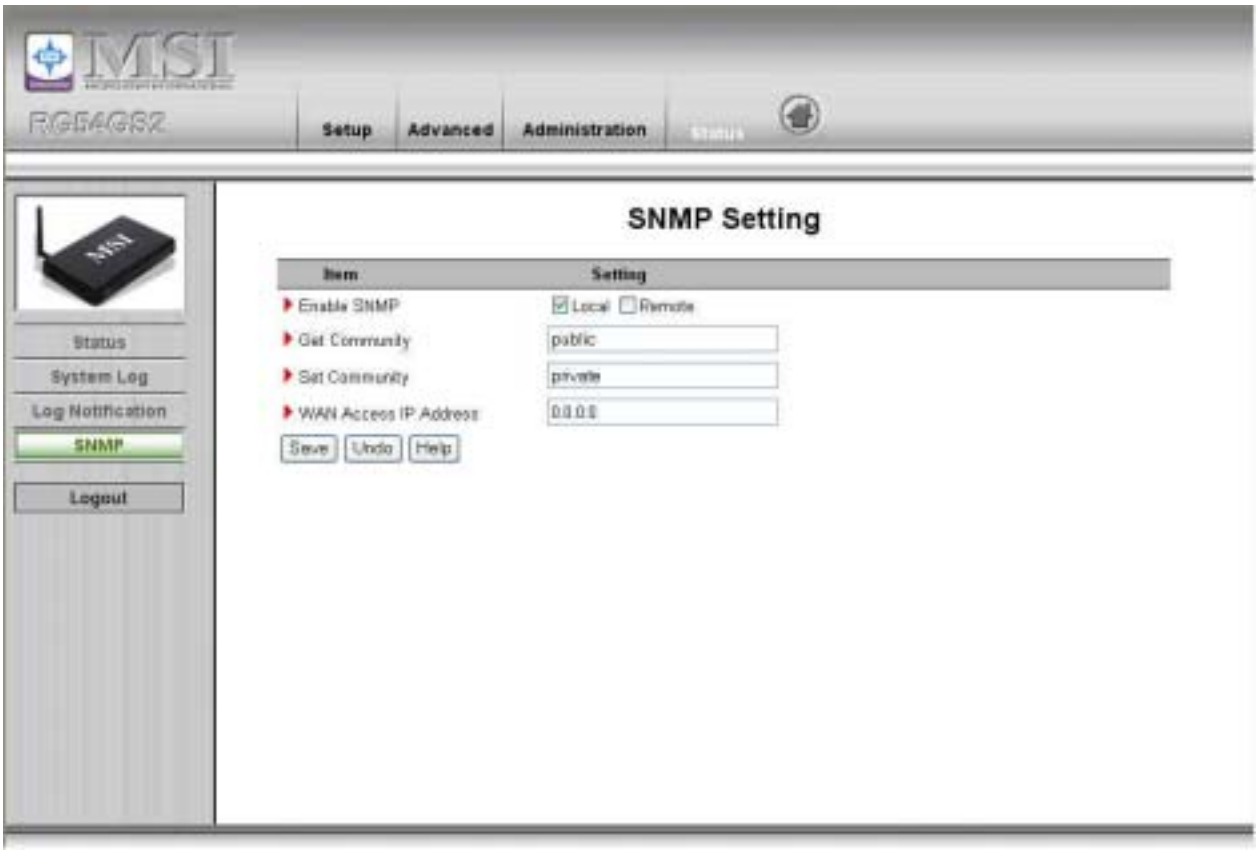
**SMTP Server IP and Port（SMTP 伺服器 IP 和連接埠）**

輸入 SMTP 伺服器和 IP 連接埠，兩者以「：」串接，如果不指定埠號，預設值是 25；例如「mail.your_url.com」或「192.168.1.100：26」。

**Send E-mail alert to（傳送電子郵件警示到）**

收件人會收到系統日誌。可以指派 1 位以上的收件人，只要使用「;」或「,」分隔電子郵件位址即可。

### 75. 4.6.4 SNMP Setting（SNMP設定）




簡單地說，SNMP（簡易網路管理通訊協定）是專為進行遠端管理而設計的通訊協定，它透過輪詢、設定終端值以及監控網路事件，讓使用者可以從管端管理電腦網路。

**Enable SNMP（啟用 SNMP）**

您必須勾選 Local（本機）、Remote（遠端）或兩者一起勾選才能啟用 NMP 功能。如果勾選 Local，本裝置將回應來自區域網路的要求；如果勾選 Remote，本裝置則回應來自廣域網路的要求；

**Get Community（取得社群）**

設定裝置會回應的 GetRequest 社群。

**Set Community（設定社群）**

設定裝置會接受的 SetRequest 社群。

# 附錄 A　Windows 95/98 的 TCP/IP 組態

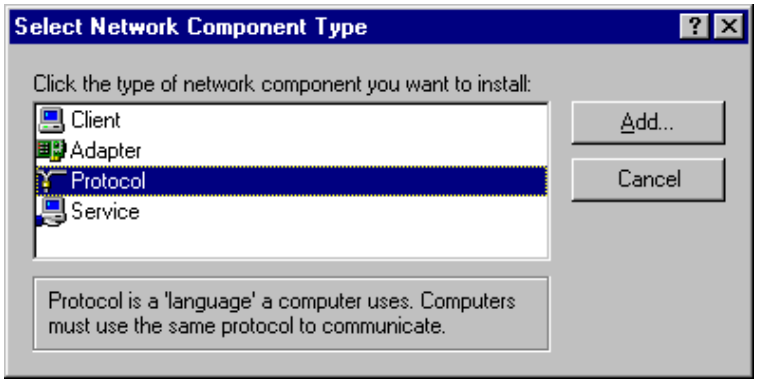
本節介紹如何將 TCP/IP 通訊協定安裝至個人電腦中。假設您已經在個人電腦中成功安裝了網路卡。如果尚未安裝，請參閱網路卡的使用手冊。此外，B.2 一項說明如何設定 TCP/IP 值才能與此 NAT 分享器一起正常運作。

**A.1 TCP/IP通訊協定安裝至PC**

1. 按一下**開始按鈕再**選擇**設定**，然後按一下**控制台**。
2. 按兩下**網路**圖示再選取網路視窗中的**組態**標籤。
3. 按一下**新增**按鈕，將網路元件新增到 PC 中。
4. 按兩下**通訊協定**，新增 TCP/IP 通訊協定。

78.

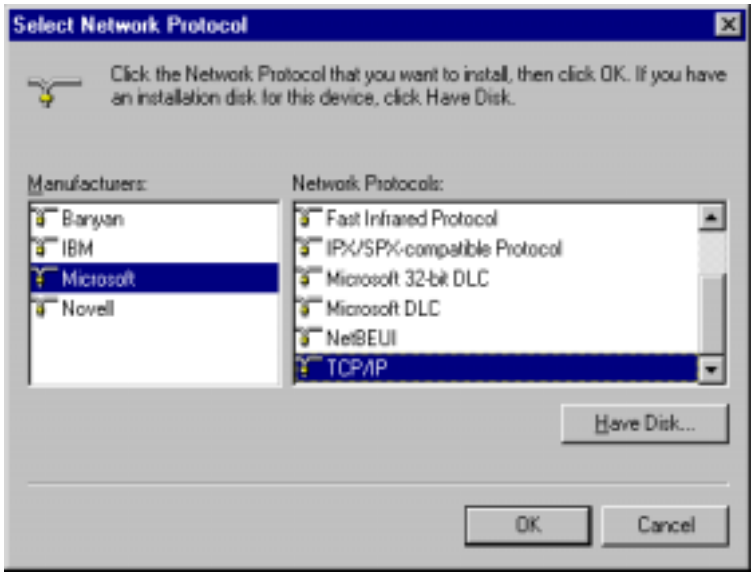
79.




80.

5. 在製造商清單中選取 **Microsoft** 項目，再選擇網路通訊協定中的 **TCP/IP**。按一下**確定**按鈕，回到網路視窗。

81.

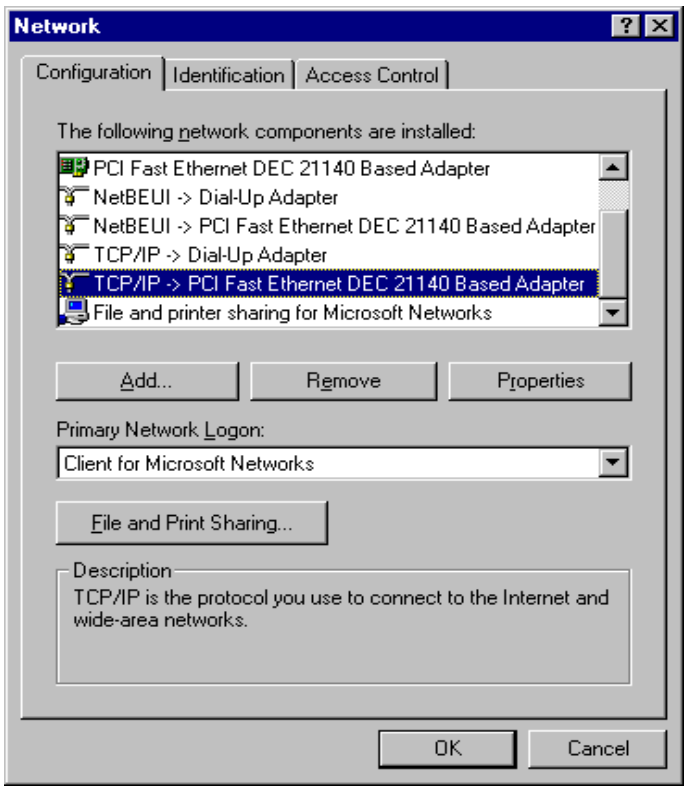


6. TCP/IP 通訊協定應該已列在網路視窗中。按一下**確定**，完成安裝程序再重新啟動 PC 以啟用 TCP/IP 通訊協定。

82.

### A.2 設定TCP/IP通訊協定與NAT分享器一起使用

1. 按一下**開始按鈕再**選擇**設定**，然後按一下**控制台**。
2. 按兩下**網路**圖示。選取 TCP/IP 行，此選項在網路視窗的**組態**標籤中已與您的網路卡建立連結。

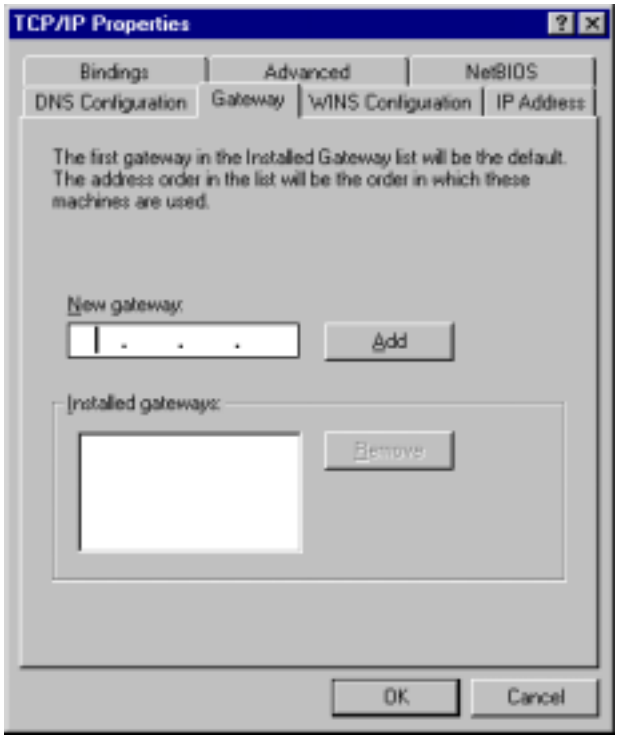



3. 按一下**內容**按鈕，設定本 NAT 分享器的 TCP/IP 通訊協定。
4. 接下來有兩種設定方式：

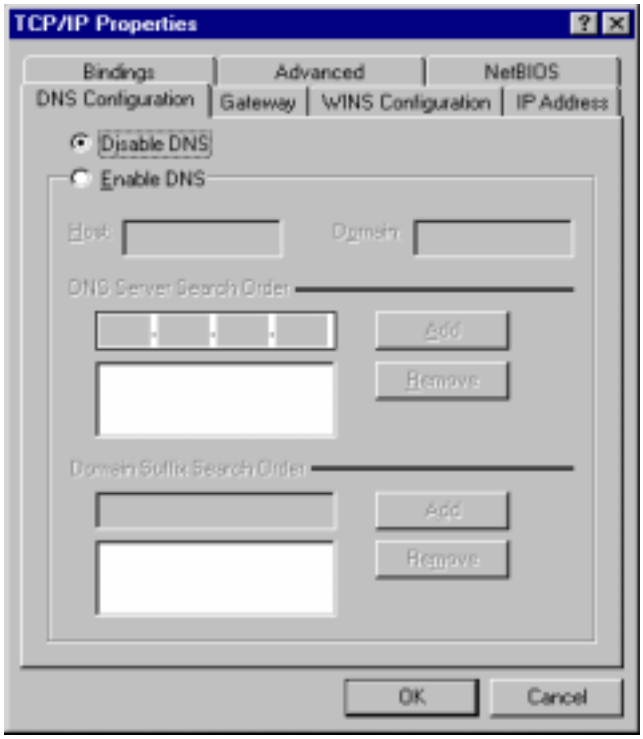
83.

a. 在 IP 位址標籤中選取**自動獲得 IP 位址**。


b. 不要在閘道標籤輸入任何數值。

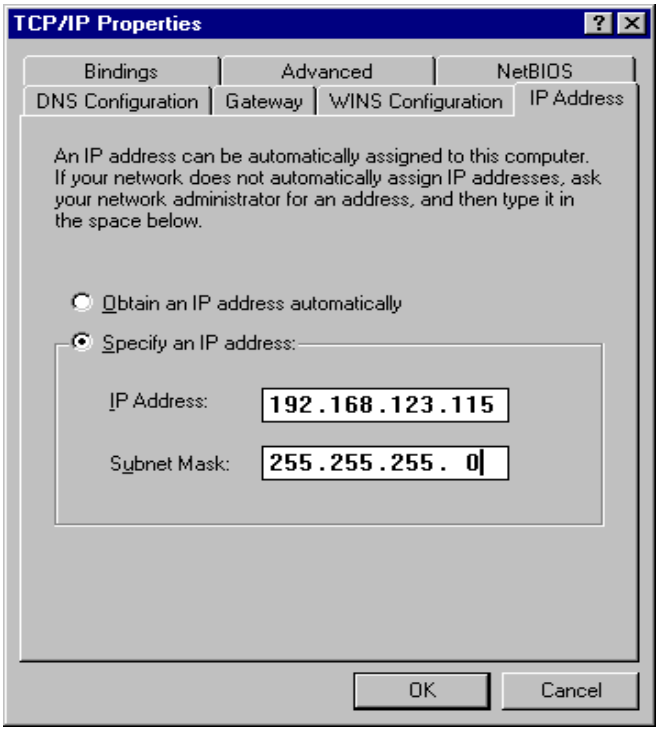


c. 在 DNS 組態標籤中選擇**停用 DNS**。

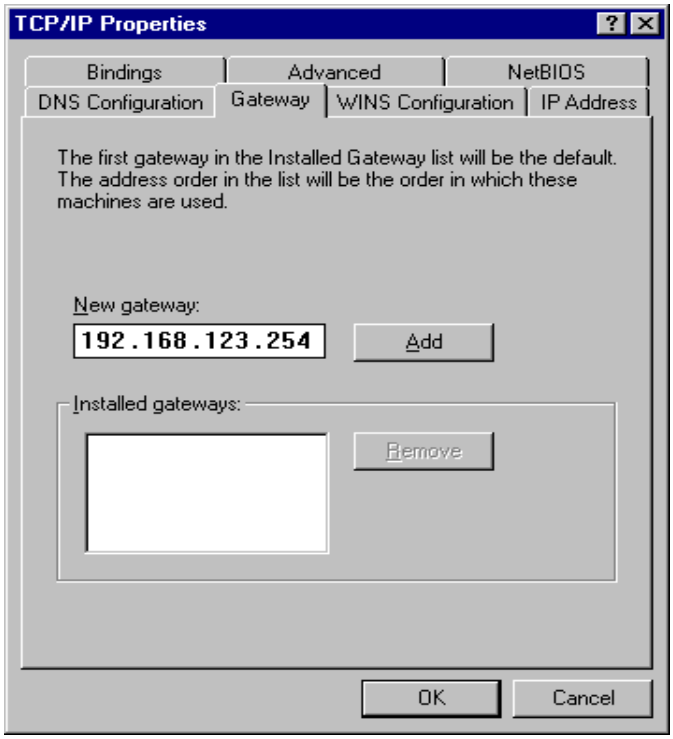



B. 手動設定 IP

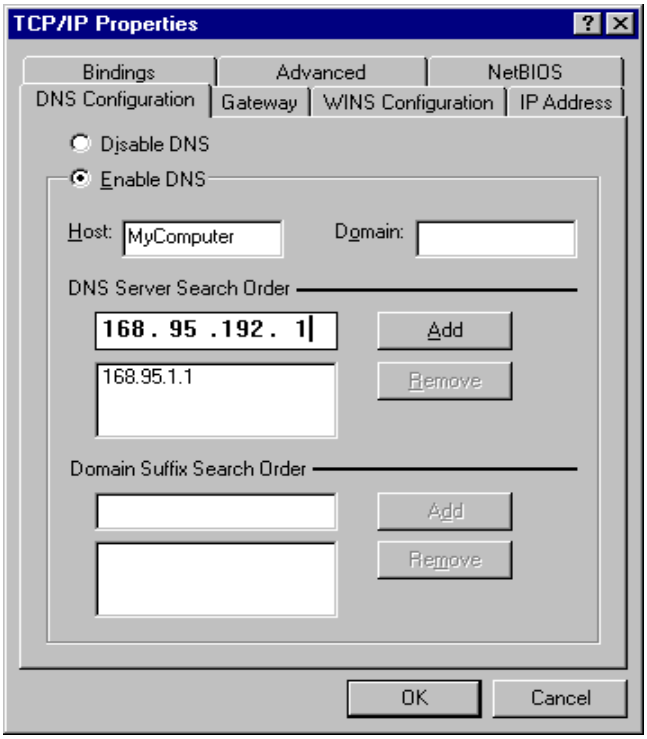
a. 在 IP 位址標籤中選取**指定 IP 位址**。本產品的預設 IP 位址是 192.168.1.254, 因此在 IP 位址欄位中請使用 192.168.1.xxx（xxx 介於 1 至 253 之間），子網路遮罩欄位中則使用 255.255.255.0。



b. 在閘道標籤的新增閘道欄位中，新增本產品的 IP 位址（預設 IP 是 192.168.1.254）再按一下**新增**按鈕。




c. 在 DNS 組態標籤中，將 ISP 提供的 DNS 值新增到 DNS 伺服器搜尋順序欄位中，再按一下**新增**按鈕。



# 附錄 B　802.1x 設定

84.

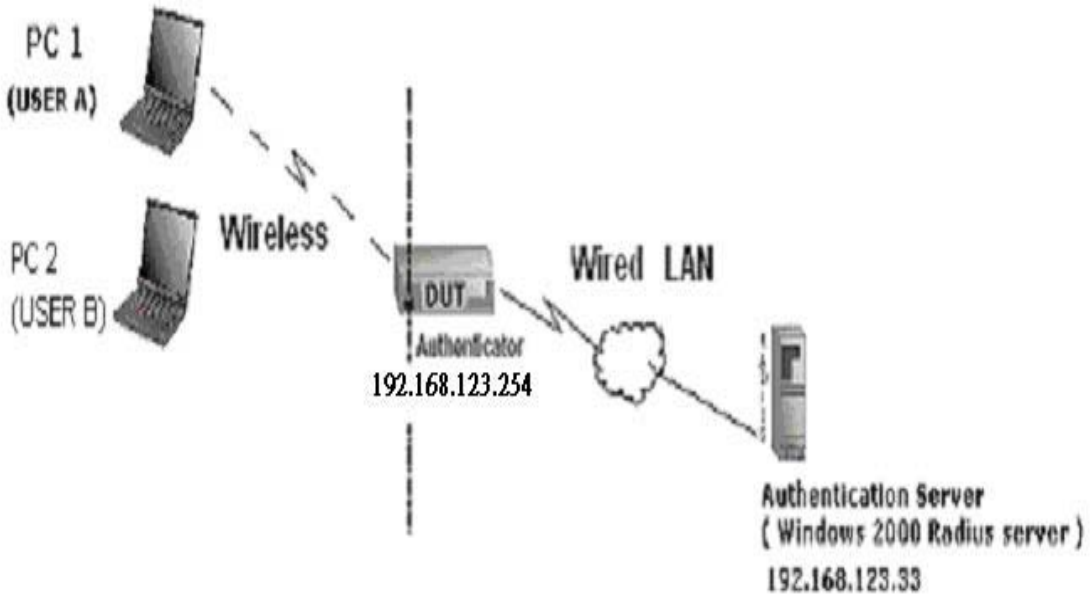



圖 1：測試環境（使用 Windows 2000 Radius 伺服器）

**1 設備詳細資訊**

PC1：

Microsoft Windows XP Professional 未安裝 Service Pack 1。

D-Link DWL-650+無線網路卡

驅動程式版本：3.0.5.0（驅動程式日期：03.05.2003）

PC2：

Microsoft Windows XP Professional 安裝了 Service Pack 1。

Z-Com XI-725 USB 無線網路卡

驅動程式版本：1.7.29.0（驅動程式日期：10.20.2001）

驗證伺服器：Windows 2000 RADIUS 伺服器，安裝了 Service Pack 3 和 HotFix Q313664。

註.升級到 Service Pack 3 和 HotFix Q313664 之後，Windows 2000 RADIUS 伺服器僅支援 PEAP
*（可至下列網址取得詳細資訊 http ：//support.microsoft.com/default.aspx?scid=kb; en-us;313664）*

**2 DUT**

**組態：**

1.啟用 DHCP 伺服器。

2.WAN 設定：靜態 IP 位址。

3.LAN IP 位址：192.168.1.254/24。

4.設定 RADIUS 伺服器 IP。

5.設定 RADIUS 伺服器共用金鑰。

6.設定 WEP 金鑰和 802.1X 設定。

以下測試將利用智慧卡或 Windows XP Professional 其他的憑證使用內建的 802.1X 驗證方式，例如 EAP_TLS、PEAP_CHAPv2（僅限 Windows XP with SP1）和 PEAP_TLS（僅限 Windows XP with SP1）。

**3. DUT 和 Windows 2000 Radius 伺服器設定**

3-1-1. 設定 Windows 2000 RADIUS 伺服器

我們必須將驗證方式變更為 MD5_Challenge 或是依據測試條件使用智慧卡或 RADIUS 伺服器的其它憑證。

3-1-2. 設定 DUT

1.啟用 802.1X（勾選「啟用」核取方塊）。

2.輸入 RADIUS 伺服器 IP。

3.輸入共用金鑰。（此金鑰為 RADIUS 伺服器和 DUT 所共用）。

4.我們會變更 802.1X 加密金鑰的長度以符合不同的測試條件。

3-1-3. 設定 PC 的網路介面卡

1.選擇 IEEE802.1X 作為驗證方式。（圖 2）

註.

圖 2 是 Windows XP 在未安裝 Service Pack 1 情況下的設定畫面。如果使用者升級到 Service Pack 1，在 EAP 類型清單中便無法看到 MD5-Challenge，不過會有新選項「受保護的 EAP (PEAP)」。

2.選擇「MD5-Challenge」或「智慧卡或其他憑證」作為 EAP 類型。

3.如果選擇使用智慧卡或憑證作為 EAP 類型，則選取使用本電腦的憑證。（圖 3）

4.我們會變更 EAP 類型以符合不同的測試條件。

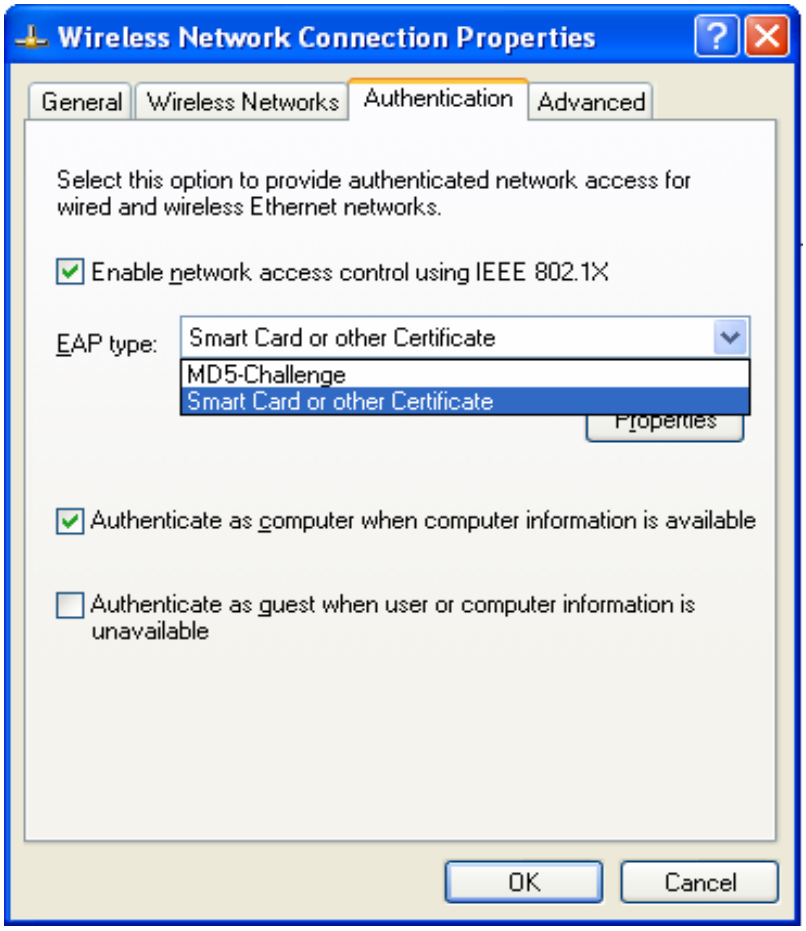



圖 2：啟用 IEEE 802.1X 存取控制

圖 3：智慧卡或憑證內容

**4. Windows 2000 RADIUS伺服器驗證測試：**

4.1 DUT 使用憑證驗證 PC1。（PC2 依循相同的測試程序。）

1. 下載憑證並將其安裝於 PC1。（圖 4）
2. PC1 選擇 DUT 的 SSID 作為存取點。
3. 將無線網路用戶端和 RADIUS 伺服器的驗證類型都設定為 EAP_TLS。
4. 停用無線連線，然後再次啟用。
5. DUT 會將使用者的憑證傳送到 RADIUS 伺服器，然後再將驗證訊息傳送到 PC1。（圖 5）
6. Windows XP 會提示驗證過程成功或失敗再結束驗證程序。（圖 6）
7. 當 PC1 成功取得動態 IP 和 PING 到遠端主機時，中止測試步驟。

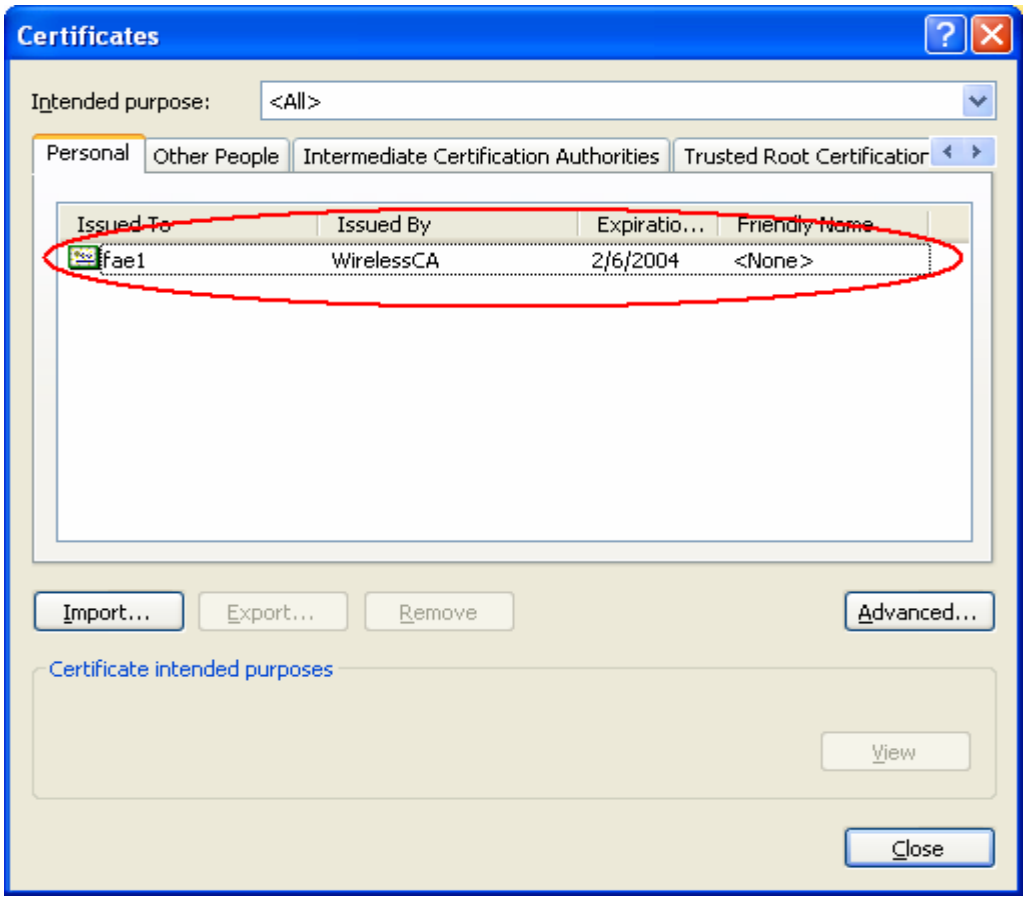



圖 4：PC1 的憑證資訊

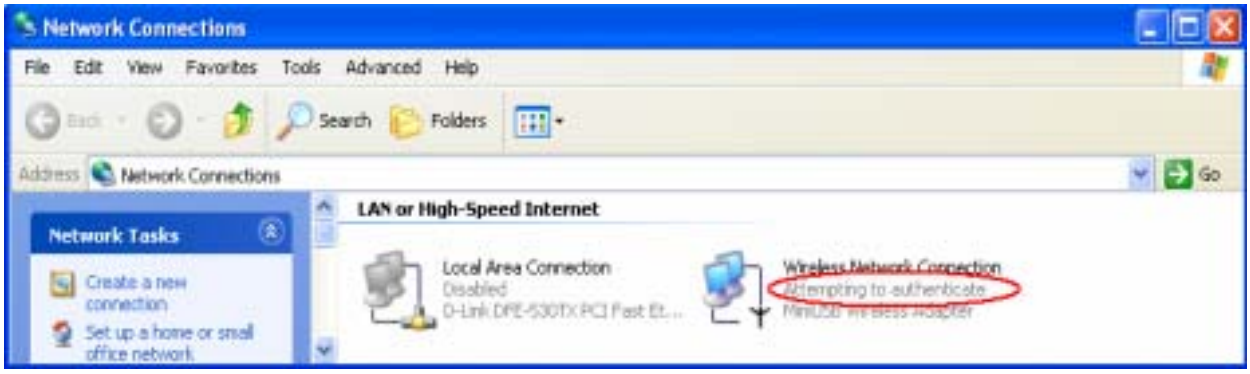



圖 5：驗證中


圖 6：驗證成功

**4.2** DUT 使用 PEAP-TLS 驗證 PC2。

1. PC2 選擇 DUT 的 SSID 作為存取點。
2. 將無線網路用戶端和 RADIUS 伺服器的驗證類型都設定為 PEAP_TLS.
3. 停用無線連線，然後再次啟用。
4. DUT 會將使用者的憑證傳送到 RADIUS 伺服器，然後再將驗證訊息傳送到 PC2。
5. Windows XP 會提示驗證過程成功或失敗再結束驗證程序。
6. 當 PC2 成功取得動態 IP 和 PING 到遠端主機時，則中止測試步驟。

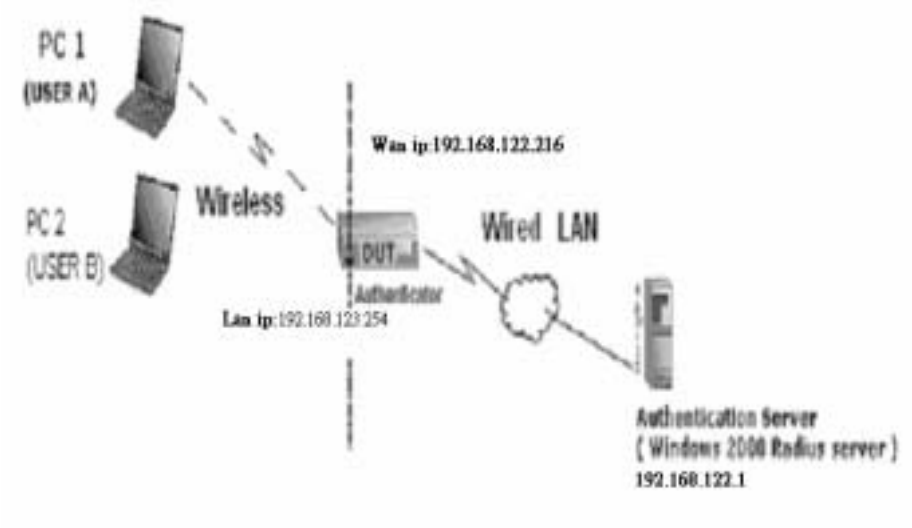
**支援類型：分享器支援的802.1x驗證類型：**
**PEAP-CHAPv2和PEAP-TLS。**

註.

1. PC1 位在沒有安裝 Service Pack 1 的 Windows XP 平台上。
2. PC2 位在安裝 Service Pack 1 的 Windows XP 平台上。
3. 只有安裝 Service Pack 1 的 Windows XP 才會支援 PEAP。
4. 必須啟用資料加密功能，安裝 Service Pack 1 的 Windows XP 才會能進行 802.1x 驗證。

85.

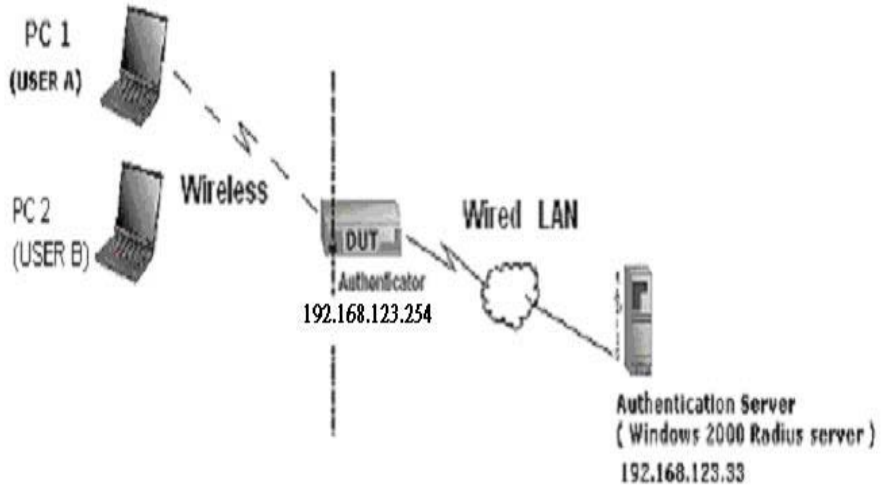
# 附錄 C　WPA-PSK 和 WPA




86.

無線分享器：LAN IP：192.168.123.254
　　WAN IP：192.168.122.216
Radius 伺服器：192.168.122.1
UserA：XP 無線網路卡：Ti-11g
工具：Odyssey Client Manager
請參考：www.funk.com
下載位址：http：//www.funk.com/News&Events/ody_c_wpa_preview_pn.asp

其他組態：

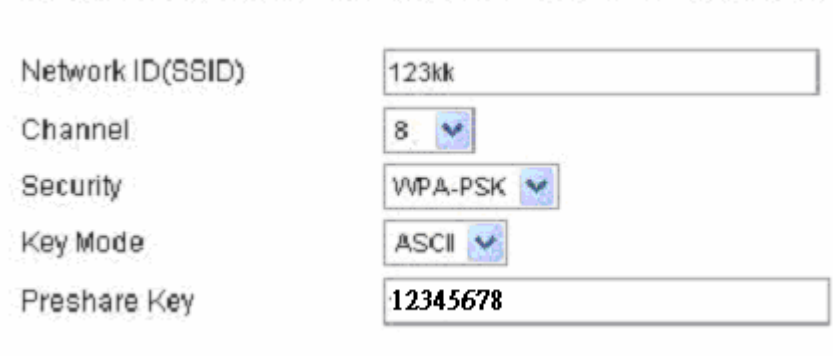



WPA-PSK

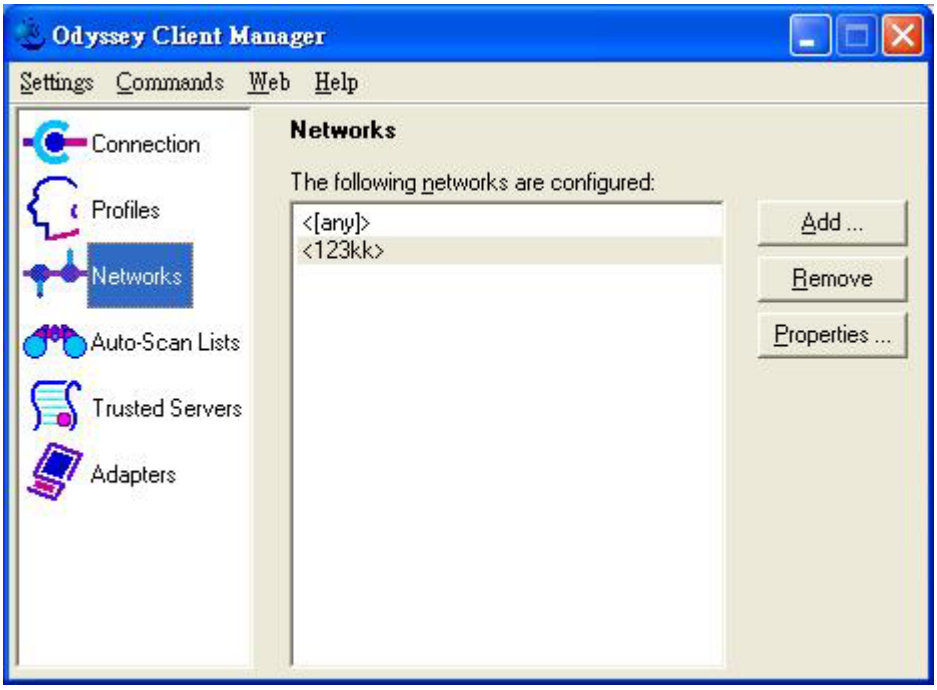
事實上，此功能並不需要 Radius 伺服器驗證，用戶端和無線分享器會自行驗證。

方式 1：

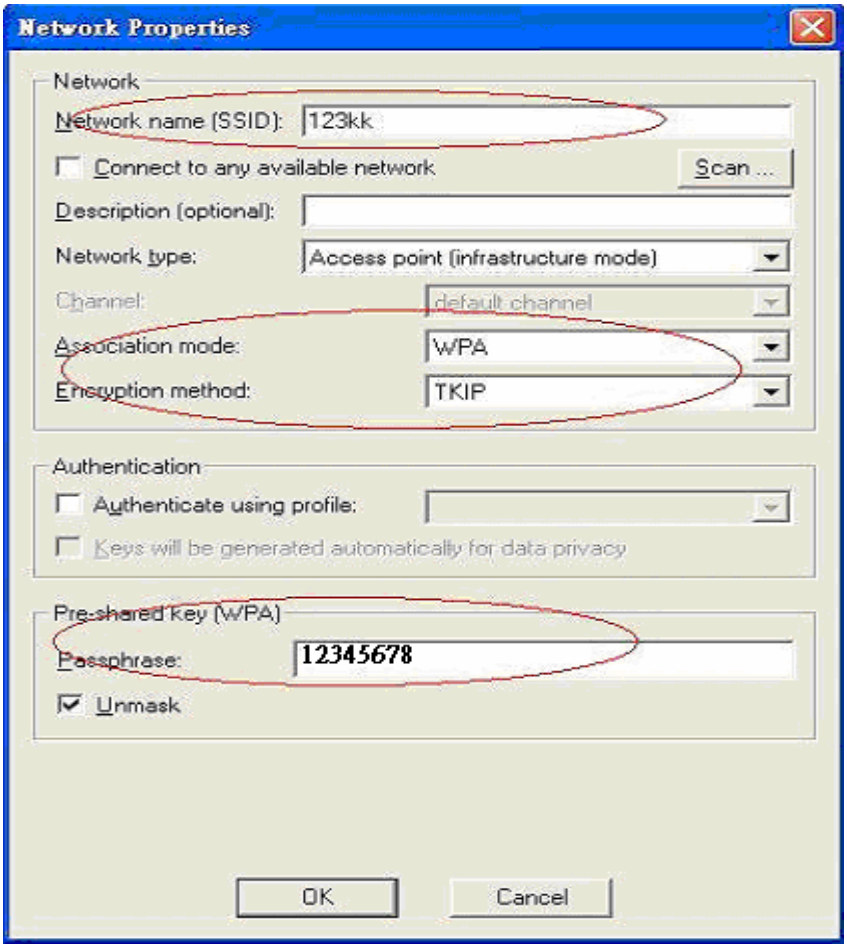
1. 前往無線分享器的 Web 管理員進行設定，如下所示：



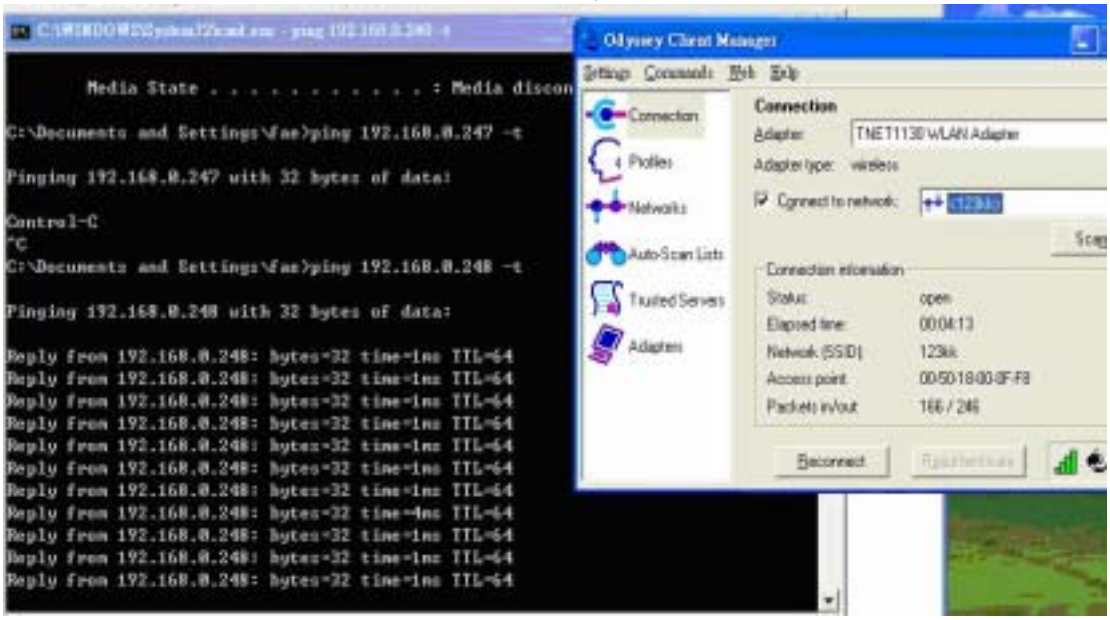

2. 前往 Odyssey Client Manager，首先選擇「Network」（網路）
執行此動作之前，應先確認軟體是否可顯示無線網路卡。
開啟「Adapters」（介面卡）


Odyssey Client Manager
Settings Commands Web Help
Connection
Profiles
Networks
Auto-Scan Lists
Trusted Servers
Adapters
Networks
The following networks are configured:
<[any]>
<123kk>
Add ...
Remove
Properties ...

3. 新增和編輯設定：


Network Properties
Network
Network name (SSID): 123kk
Connect to any available network
Scan ...
Description (optional):
Network type: Access point (infrastructure mode)
Channel: default channel
Association mode: WPA
Encryption method: TKIP
Authentication
Authenticate using profile:
Keys will be generated automatically for data privacy
Pre-shared key (WPA)
Passphrase: 12345678
Unmask
OK
Cancel

4. 返回連線：
   然後選取「Connect to network」（連線到網路），您將會看到：

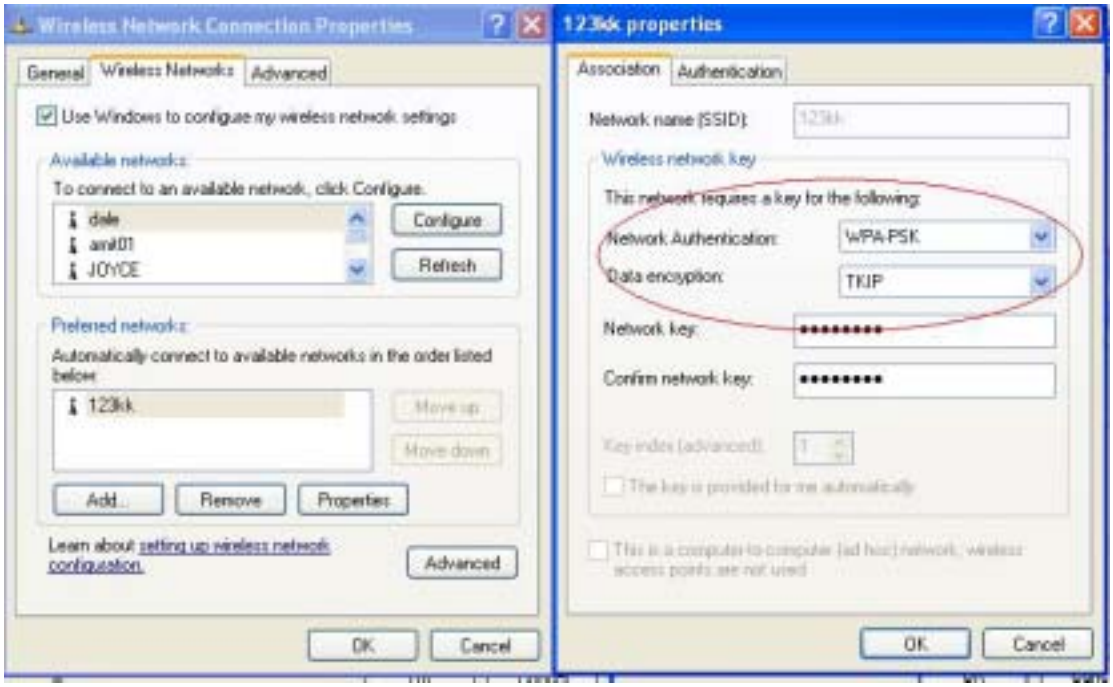



方式 2：

1. 首先，修補 Windows XP 並安裝「Service package 1」。
   下載更新程式：
   http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=5039ef4a-61e0-4c44-94f0-c25c9de0ace9
2. 然後重新開機。
3. 分享器和用戶端的設定：

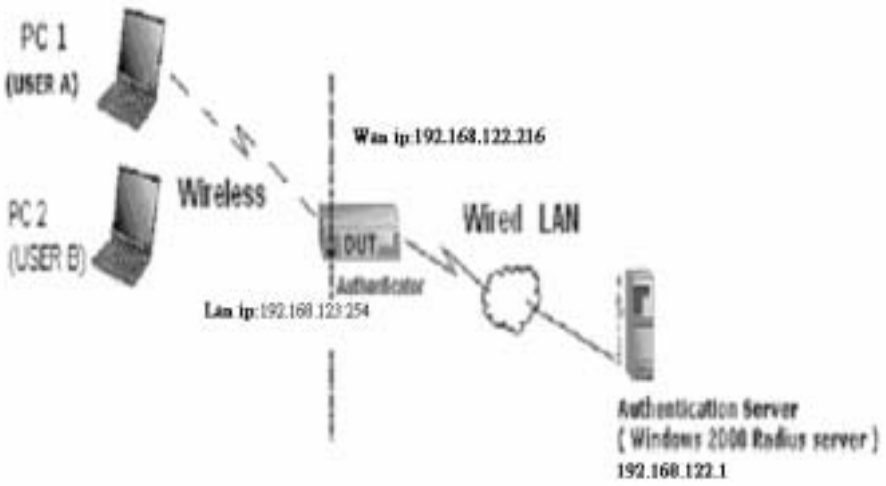
分享器：


用戶端：
前往「網路連線」，選取無線網路卡。
選擇「檢視可用的無線網路」，如下所示：
進階→選擇「1kk」


Wireless Network Connection Properties
General
Wireless Networks
Advanced
Use Windows to configure my wireless network settings
Available networks:
To connect to an available network, click Configure.
dale
anil01
JOYCE
Configure
Refresh
Preferred networks:
Automatically connect to available networks in the order listed below:
123kk
Move up
Move down
Add...
Remove
Properties
Learn about setting up wireless network configuration.
Advanced
OK
Cancel
123kk properties
Association
Authentication
Network name (SSID):
Wireless network key
This network requires a key for the following:
Network Authentication:
WPA-PSK
Data encryption:
TKIP
Network key:
Confirm network key:
Key index (advanced):
The key is provided for me automatically
This is a computer-to-computer (ad hoc) network; wireless access points are not used
OK
Cancel

WPA：

就此功能而言，我們需要伺服器才能進行驗證。此功能類似 802.1x。



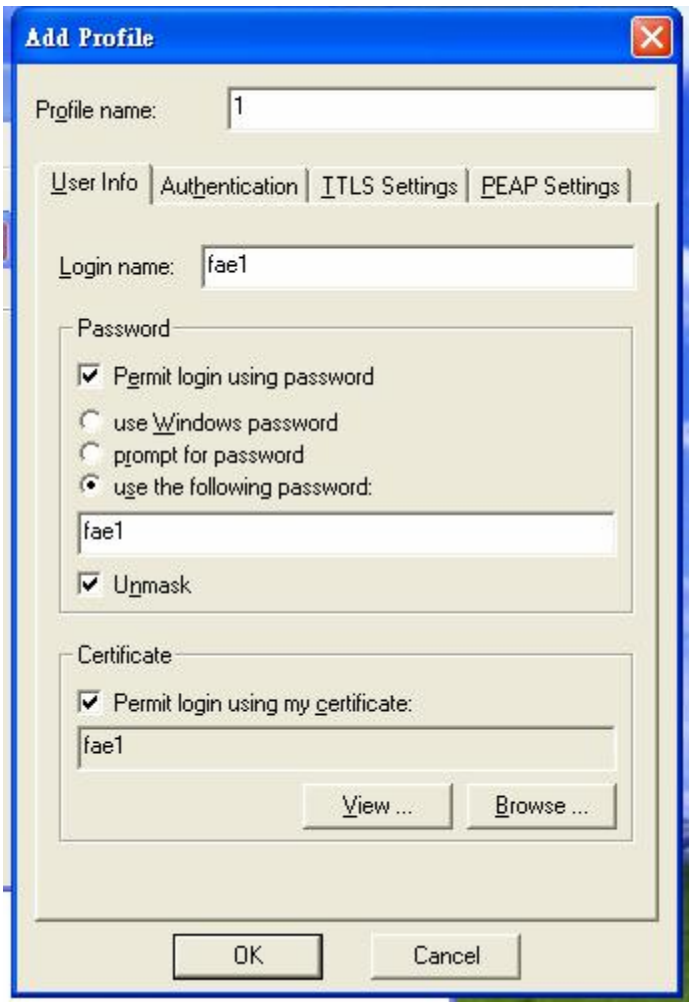

以上是我們的環境：

方式 1：

1. UserA 或 UserB 必須先從 Radius 取得憑證，網址是
http：//192.168.122.1/certsrv
帳號：fae1
密碼：fae1

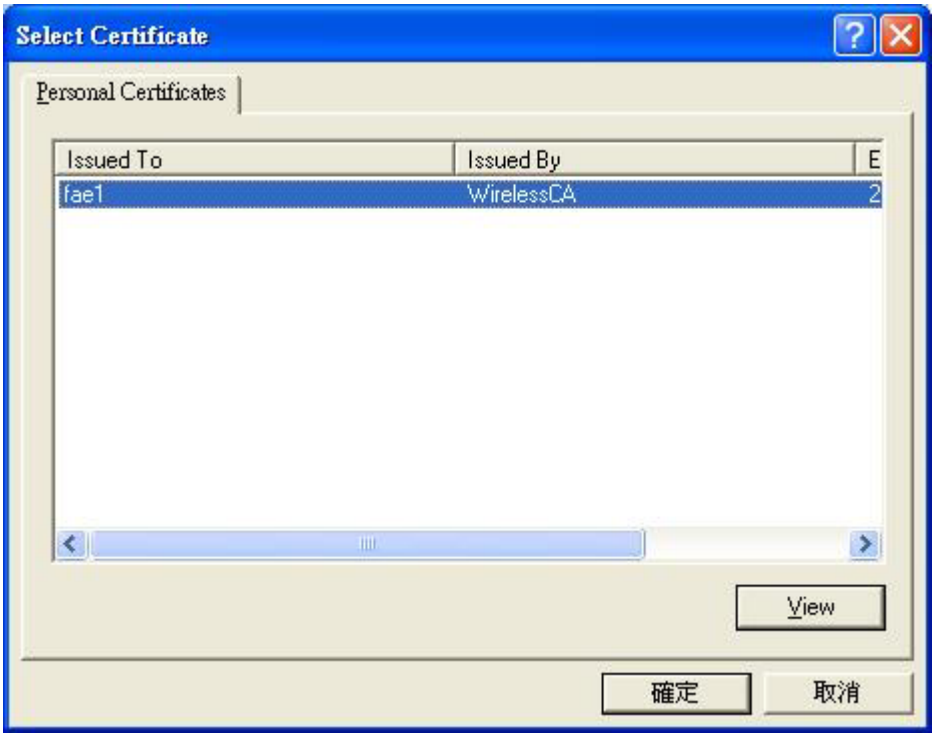

2. 然後，安裝此憑證並完成程序。
3. 前往無線分享器的 Web 管理員進行設定，如下所示：


4. 前往 Odyssey Client Manager，選擇「Profiles」（指令集）並設定指令集名稱為「1」。



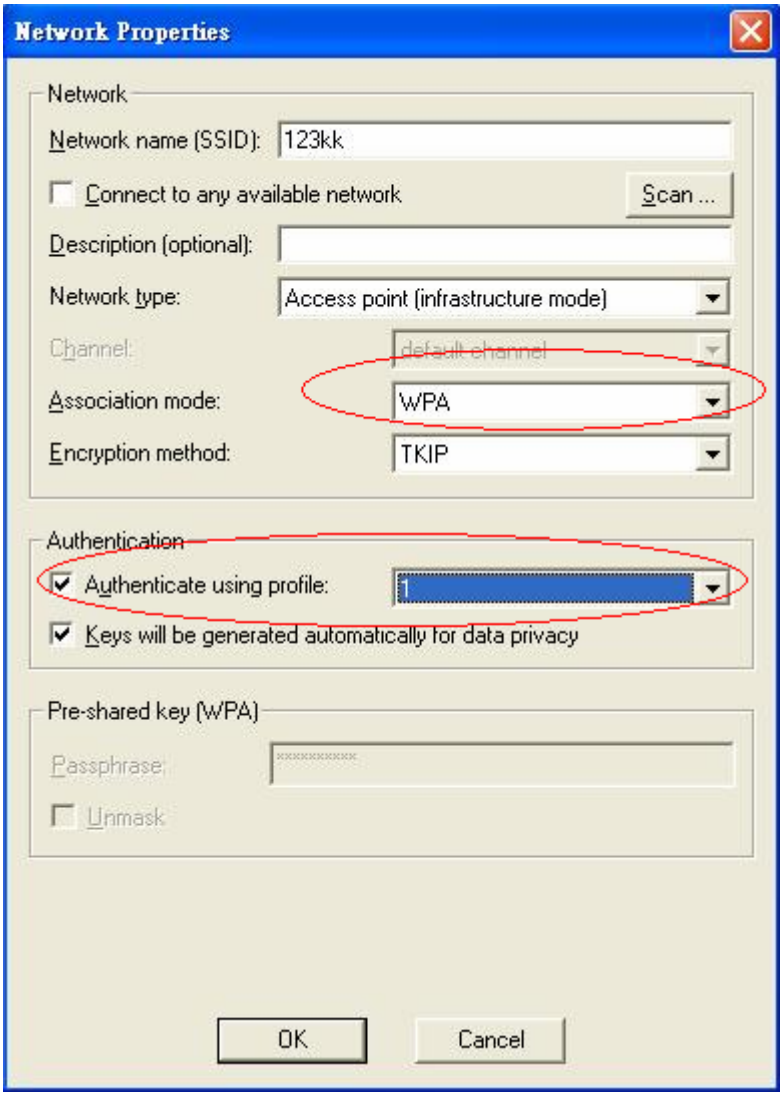

登入名稱和密碼皆為 fae1。
記住您在步驟 1 從 Radius 取得的憑證。

5. 再選擇「certificate」（憑證），如上所示。

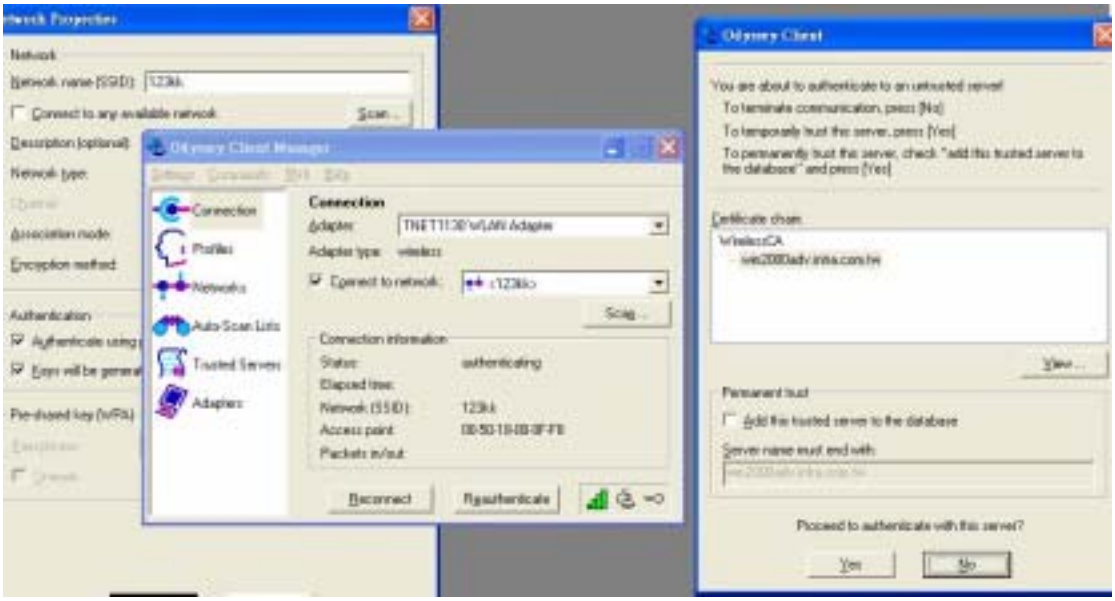



6. 然後前往驗證，先移除 EAP/TLS 然後再新增一次 EAP/TLS。

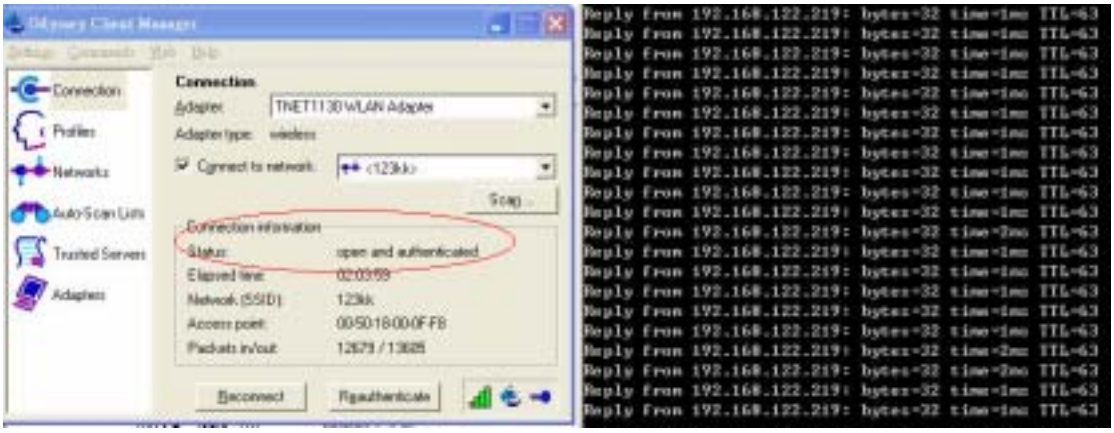
7. 前往「Network」，選取「1」，然後按確定



8. 返回連線，選取「1kk」。
如果**成功**，無線網路用戶端必須使用 Radius 伺服器驗證，如下所示：



9. 結果：



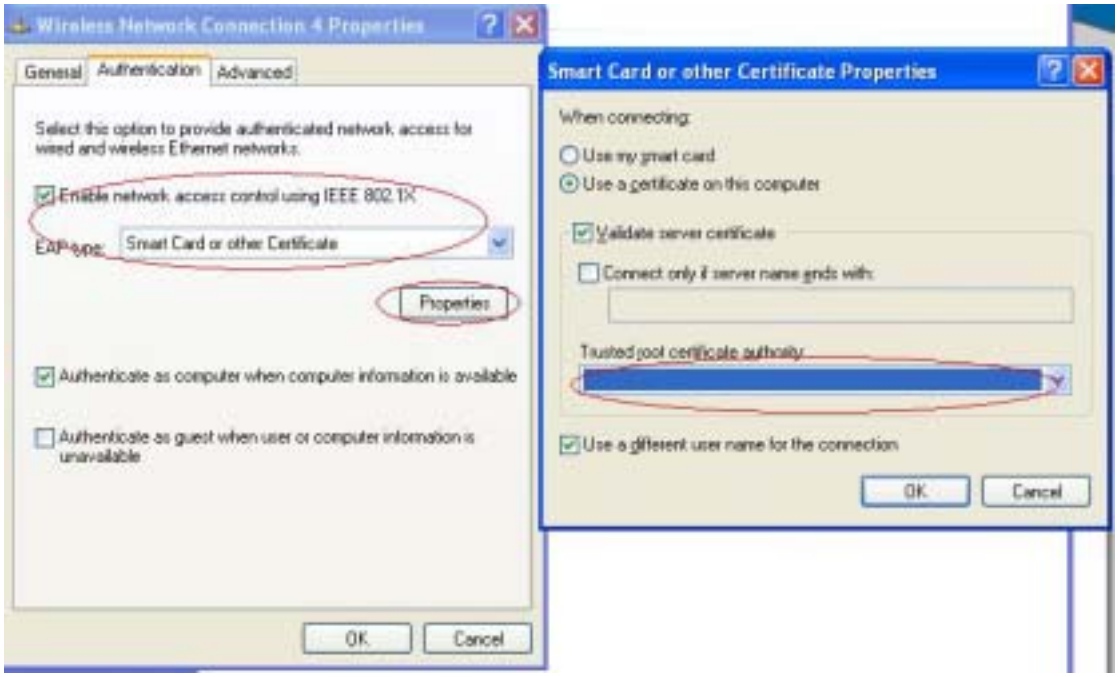
方式 2：

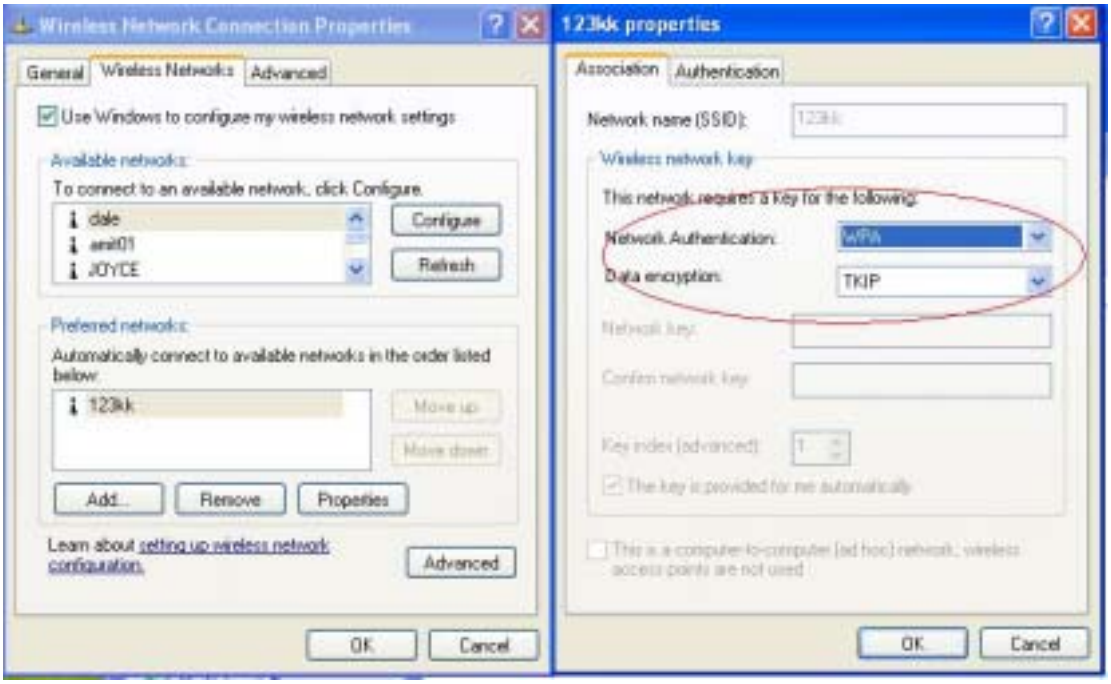
1. UserA 或 UserB 必須先從 Radius 取得憑證，網址是
http：//192.168.122.1/certsrv
帳號：fae1
密碼：fae1


2. 然後，安裝此憑證並完成程序。
3. 分享器和用戶端的設定：

分享器：

用戶端：
前往「網路連線」，選取無線網路卡。
選擇「檢視可用的無線網路」，如下所示：
進階→選擇「1kk」
在受信任的根憑證授權單位中選取「WirelessCA 和啟用」：




如果無線網路用戶端想要連線，它必須要求驗證。

# 附錄 D　常見問答集和疑難排解

87.

## 重設為出廠預設值

重設為預設值的方式有兩種。

**1. 使用 RESET（重設）按鈕還原**

首先，關閉分享器再按下 RESET 按鈕。接著，打開分享器電源，按住 RESET 按鈕直到 M1 及/或 M2 LED 指示燈（LED 狀態指示燈）開始閃爍才放開手指。LED 指示燈閃爍約 8 次，則代表還原程序已經完成。但如果 LED 指示燈閃爍兩次，則請重複上述步驟。

2. **開啟分享器時直接還原**

首先，按住 RESET 按鈕約 5 秒（M1 會開始閃爍，約 5 秒），再放開手指。還原程序即完成。