RX3041H

高速路由器

使用手冊

1.0 版
2004 年 11 月

版權資訊

本產品所有部分，包括配件與軟體等，其所有權都歸華碩電腦公司（以下簡稱華碩）所有，未經華碩公司許可，不得任意地仿製、拷貝、摘抄或轉譯。

本用戶手冊沒有任何形式的擔保、立場表達或其他暗示。若有任何因本用戶手冊或其所提到產品的所有資訊，所引起直接或間接的資料流程失、利益損失或事業終止，華碩及其所屬員工恕不爲其承擔任何責任。除此之外，本用戶手冊所提到的產品規格及資訊只能參考，內容亦會隨時升級，恕不另行通知。本用戶手冊的所有部分，包括硬體及軟體，若有任何錯誤，華碩沒有義務爲其承擔任何責任。

當下列兩種情況發生時，本產品將不再受到華碩公司之擔保及服務：（1）該產品曾經非華碩授權之維修、規格更改、零件替換。（2）產品序號模糊不清或喪失。

用戶手冊中所談論到的產品名稱僅做識別之用，而這些名稱可能是屬於其他公司的注冊商標或是版權。

產品規格或驅動程式改變，用戶手冊都會隨之更新。更新的詳細說明請您到華碩的網際網路主頁 tw.asus.com 瀏覽，或是直接與華碩公司聯絡。

華碩的聯絡資訊

華碩電腦公司 ASUSTeK COMPUTER INC.（亞太地區）

市場訊息

地址　：臺灣臺北市北投區立德路 15 號
電話　：886-2-2894-3447

技術支援

電話　：886-2-2890-7902

免費服務電話　：0800-093-456（臺灣區）

傳真　：886-2-2890-7698
全球資訊網　：tw.asus.com

ASUS COMPUTER INTERNATIONAL（美國）

市場訊息

地址　：44370 Nobel Drive, Fremont ,CA 94538, USA
傳真　：+1-510-608-4555
電子郵件　：tmdl@asus.com

技術支援

傳真　：+1-502-933-8713
電話　：+1-502-995-0883
電子郵件　：tsd@asus.com
全球資訊網　：www.asus.com

ASUS COMPUTER GmbH（德國 / 奧地利）

市場訊息

地址　：Harkort Str. 25, D-40880 Ratingen, Germany
電話　：49-2102-95990
傳真　：49-2102-959911
全球資訊網　：www.asuscom.de
線上聯絡　：www.asuscom.de/sales

技術支援

電話　：49-2102-95990 ... 主機板/其他產品
：49-2102-959910 ... 筆記型電腦
傳真　：49-2102-959911
線上支援　：www.asuscom.de/support

目 錄

手冊中圖的索引

手冊中表格的索引

1 產品介紹

首先，恭喜您成爲華碩 RX3041H 網際網路安全路由器的使用者！您區域網路（LAN）內的電腦現在將可如同那些使用 ADSL 或 cable modem 的電腦一樣，擁有高速的寬頻聯線來接入網際網路。

此外，本用戶手冊也將指導您如何安裝這台高性能的網際網路安全路由器，並針對您自己的需要設定各項功能，讓本產品可以發揮最大的效能。

1.1 產品功能

- 10/100Base-T 乙太網路由器爲您區域網路（LAN）內的所有電腦提供網際網路連線。
- 防火牆、NAT（網路位址轉換）及 IP 安全 VPN 功能爲您的區域網路（LAN）提供安全的網路連線。
- 透過 DHCP 伺服器提供自動的網路位址分配。
- 服務包括 IP 路由、DNS 和 DDNS 設定、 RIP 及 IP 性能監控。
- 本產品的設定全部透過瀏覽器完成，您必須具備網頁瀏覽器 Internet Explorer 軟體，版本在 5.5 以上，或者 Netscape 瀏覽器，版本在 7.0.2 以上。

1.2 系統需求

您在使用本網際網路安全路由器接入網際網路時，請注意以下事項：

- 具備可使用的 ADSL 或是 cable modem 寬頻服務，並具備至少一個公共的網際網路位址指定給您的廣域網（WAN）使用。
- 一台以上具備 10Base-T/100Base-T 乙太網路介面卡（NIC）的電腦。
- 如果您需要將本產品連接在超過四台電腦的乙太網路上，您必須另外選購一台乙太網路集線器/交換器。
- 本產品的設定全部透過瀏覽器完成，您必須具備網頁瀏覽器 Internet Explorer 軟體，版本在 5.5 以上，或者 Netscape 瀏覽器，版本在 7.0.2 以上。

1.3 關於這本用戶手冊

1.3.1 提示符號的說明

- 本手冊將在縮寫詞第一次出現時解釋其意義，並將其意義解釋收入術語表中。
- 爲簡潔起見，“網際網路安全路由器”有時簡稱爲“路由器”。
- 在提到某個地方的一組乙太網連線的電腦時，術語***區域網路（LAN）***和***網路（network）***將交替使用。

1.3.2 印刷樣式的說明

- *斜體* 用來標出術語表解釋的術語。
- **黑體字** 表示在功能表或其他電腦顯示頁面中選中的選項。

1.3.3 特別資訊

這本手冊使用下列圖示來提醒您注意特殊的說明和解釋。

注意

向您提供有助於完成某項工作的訣竅或其它額外的資訊。

名詞解釋

向您闡釋多數用戶不太熟悉的術語或縮寫詞，這些術語解釋也將在術語表中集中出現。

小心

提醒您在進行某項工作時要注意的重要資訊，包括要請您注意個人安全和勿傷害系統完整的資訊。

2 認識 RX3041H 高速路由器

2.1 零件目錄表

除本手冊之外，您的包裝盒內還應包含以下配件：

- RX3041H 高速路由器
- 電源供應器
- 乙太網路線（straight-through）
- （可選）主控台（console）埠線纜（RJ-45）

2.2 前面板

請參考下圖。前面板包括數個 LED 指示燈，顯示各項操作狀態。

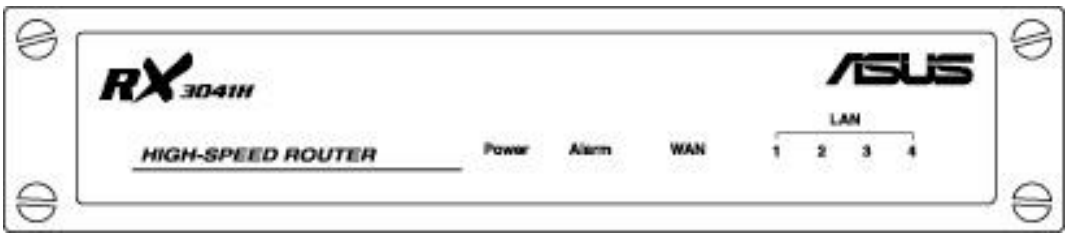


圖 2.1. 前面板 LED 指示燈

表 2.1. 前面板標簽和 LED 指示燈

指示燈	顏 色	功 能
POWER	綠 燈	燈亮：電源開啓 燈滅：電源關閉
ALARM	綠 燈	（僅在工廠測試使用）
WAN	綠 燈	燈亮：WAN 有連線 閃爍：資料正透過 WAN 傳輸 燈滅：WAN 無連線
LAN1 – LAN4	綠 燈	燈亮：LAN 有連線 閃爍：資料正透過 LAN 傳輸 燈滅：LAN 無連線

2.3 後面板

請參考下圖。後面板包括各種連接埠。

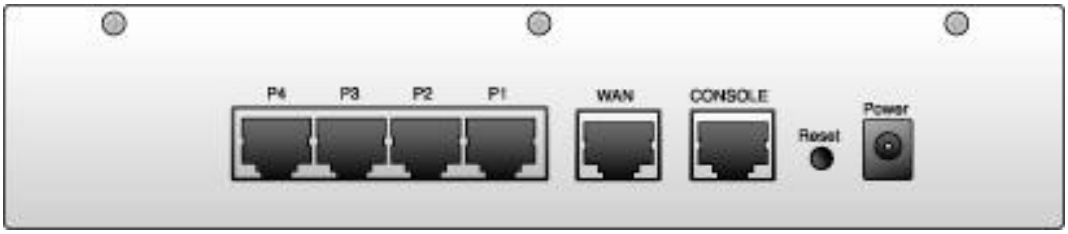


圖 2.2. 後面板連接埠

表 2.2. 後面板標簽和 LED 指示燈

標 簽	功 能
⏻	電源開關
POWER	電源插座，連接電源供應器
Reset	重置鍵
CONSOLE	RJ-45 埠連線主控台
WAN	RJ-45 埠連接您的 WAN 裝置，譬如 ADSL 或 cable modem
P1 – P4	RJ-45 埠連接您 PC 的乙太網介面，或是連接至區域網路（LAN）集線器/交換器等介面，請使用本產品所附的網路線。

2.4 主要規格

2.4.1 防火牆規格

應用於路由器的防火牆提供下列規格來保護網路不受攻擊，以及確保您的網路不被用作攻擊的跳板。

- 位址分享及管理（Address Sharing and Management）
- 封包過濾（Packet Filtering）
- 狀態封包檢測（SPI）
- 防止拒絕服務攻擊（Defense against Denial of Service Attacks）
- 應用程式內容過濾（Application Content Filtering）
- 記錄與警報（Log and Alert）
- 遠程訪問（Remote Access）
- URL 過濾關鍵字（Keyword based URL Filtering）

2.4.1.1 位址分享及管理（Address Sharing and Management）

網際網路安全路由器防火牆提供 NAT（網路位址轉換）來分享單一的高速網際網路連線，以及爲您節省區域網路（LAN）部分連線至網際網路安全路由器時的多重連線增加的額外成本。此特性隱藏了網路位址，並阻止它們公開。它爲主機連線到 LAN 的未註冊的 IP 位址對應有效位址以接入網際網路。網際網路安全路由器防火牆更提供反向 NAT 能力，讓 SOHO 用戶也能享有多種服務，如 e-mail、網頁瀏覽等。NAT 規則決定著 NAT 路由器的轉換機制。網際網路安全路由器支援下列 NAT 形式：

- 靜態 NAT – 對應從內部主機位址到全球有效網際網路位址圖（一對一）。所有的封包用映射中包含的資訊直接轉換。
- 動態 NAT – 動態對應從內部主機位址到全球有效網際網路位址圖。映射中一般包含多個內部 IP 位址池和全球有效網際網路 IP 位址池，數量上內部 IP 位址往往多於全球有效網際網路 IP 位址。在先到先服務的基礎上，每個內部 IP 位址與一個外部 IP 位址相連。
- 網路位址與埠轉換（NAPT ，Network Address and Port Translation）– 對應從多個內部主機位址到一個全球有效網際網路位址圖。映射中一般包含多個用來轉換的網路埠。每個封包用全球有效網際網路位址進行轉換。
- 反向靜態 NAT – 本形式爲入站位址映射，它對應了從全球有效網際網路位址到內部主機位址圖（一對一）。到達外部位址的所有封包均傳遞至內部位址。本形式將在主機由內部機器提供服務時發揮作用。
- 反向 NAPT – 亦被稱爲入站位址映射、埠位址映射及虛擬伺服器。任何抵達路由器的封包均能傳遞至基於協定、埠號或規則中指定的 IP 位址的內部主機。本形式將在主機由不同的內部機器提供多重服務時發揮作用。


注意

欲知所有支援的NAT ALG 服務的詳盡列表，請參考附錄 A "ALG 設定"。

2.4.1.2 訪問控制表（ACL，Access Control List）

ACL 規則是網路安全的一個基本組成部分。防火牆監控著 ACL 規則允許範圍內的單個封包，解釋著入站和出站通信的重要資訊，以及或是防止封包傳遞，或是允許封包傳遞某些基於來源位址、目標位址、來源埠、目標埠、協定和其他規範等基礎之上的內容，例如過濾申請、時間變更等。

ACL 是保持子網之間獨立性的合適的措施。它可以被用作阻止某些類型的入站封包抵達受保護網路的的第一道防線。

網際網路安全路由器防火牆的 ACL 方法支援：

- 基於目標和來源 IP 位址、埠號及協定的過濾
- 使用百搭牌來組成過濾規則
- 過濾規則優先次序
- 基於時間的篩檢程式
- 應用特殊的篩檢程式
- 遠端存取用戶群組篩檢程式

2.4.1.2 封包狀態檢查（Stateful Packet Inspection）

網際網路安全路由器防火牆利用"封包狀態檢查"工具來提取封包安全判斷需要的與狀態有關的資訊和維持評估後續連線嘗試所需要的資訊。它允許動態連線，這樣除了需要的埠之外，其餘埠就無須打開。這提供高度安全的解決方式和可量測性及可擴展性。

2.4.1.3 防止 DoS 攻擊（Defense against DoS Attacks）

網際網路安全路由器防火牆具有防止攻擊的引擎，可保護內部網路免于網際網路可知類型的攻擊。它提動了防止"拒絕服務"（Denial of Service，DoS）攻擊的保護，例如 SYN flooding、IP smurfing、LAND、Ping of Death 以及所有合成型的攻擊。它能夠讓 ICMP 停止改變方向，以及停止 IP 來源路由封包。例如，網際網路安全路由器防火牆提供防止 WinNuke——網際網路中一個廣泛應用的遠端攻擊未受保護的 Windows 的程式——的保護。網際網路安全路由器防火牆還能夠提供防止多種多樣的普通網際網路攻擊的保護，例如 IP Spoofing、 Ping of Death、Land Attack、Reassembly 以及 SYN flooding。

網際網路安全路由器防火牆提供的攻擊保護詳見下面的表 2.3.

表 2.3. DoS 攻擊

攻擊類型	攻擊名稱
Re-assembly攻擊	Bonk, Boink, Teardrop (New Tear), Overdrop, Opentear, Syndrop, Jolt
ICMP 攻擊	Ping of Death, Smurf, Twinge
Flooders	ICMP Flooder, UDP Flooder, SYN Flooder
Port Scans	TCP XMAS Scan, TCP Null Scan TCP SYN Scan, TCP Stealth Scan
TCP 攻擊	TCP sequence number prediction, TCP out-of sequence attacks
PF規則提供的保護	Echo-Chargen, Ascend Kill
其他種類的攻擊	IP Spoofing, LAND, Targa, Tentacle MIME Flood, Winnuke, FTP Bounce, IP unaligned time stamp attack

2.4.1.4 應用程式命令過濾（Application Command Filtering）

網際網路安全路由器防火牆允許網路管理員阻止、監控和報告網路用戶訪問非商業和被禁止的網頁的內容。這種高性能訪問內容管理導致了激增的生產力、低帶寬使用和漸少的法律責任。

網際網路安全路由器防火牆有能力處理在某些應用協定下的現行內容過濾，例如 HTTP、FTP、SMTP 和 RPC。

- HTTP – 您能定義 HTTP 副檔名基礎上的模組化過濾進度表
  - ActiveX
  - Java Archive
  - Java Applets
  - Microsoft Archives
  - 檔案副檔名基礎上的 URLs
- FTP – 允許您詳細說明和加強站點或用戶群組的檔案傳輸協定
- SMTP – 允許您過濾某些洩露了接收者過多資訊的操作，例如 VRFY、EXPN 等
- RPC – 允許您過濾基於 RPC 程式序號的程式

2.4.1.5 應用程式標準閘道（ALG，Application Level Gateway）

應用程式例如 FTP 、遊戲等，打開了基於各自應用參數的動態連線。爲透過網際網路安全路由器防火牆，封包屬於應用程式，因而就要求一個相應的允許規則。當缺少這個規則時，封包將被網際網路安全路由器防火牆阻止。因爲爲多種應用程式建立新的動態協定並不可行（在缺乏折衷安全性的同時），應用程式標準閘道（ALG，Application Level Gateway）形式的智慧地用來爲應用程式解析封包和打開動態聯繫。網際網路安全路由器防火牆爲流行的應用程式如 FTP、H.323、RTSP、Microsoft Games、SIP 等，提供 ALG 的一個序號 。

2.4.1.6 URL 過濾

我們可以定義不該在 URL（Uniform Resource Locator，例如 www.yahoo.com）中出現的關鍵字。任何包含一個或多個此類關鍵字的 URL 都將被阻止。這是一個規則獨立的特性，例如，它並未與 ACL 規則想關聯。這個特性能被獨立地開啓或關閉，但是只能在防火牆開啓的情況下工作。

2.4.1.7 記錄與警報（Log and Alert）

可能影響安全性的網路事件將被記錄在網際網路安全路由器的日誌檔案裏。事件細節以（WELF WebTrends Enhanced Log Format）格式記錄下來以便統計工具能被用來製作例行報告。網際網路安全路由器防火牆還能促使私人網路內的 Syslog 伺服器產生 Syslog 資訊。

網際網路安全路由器防火牆支援：

- 用 e-mail 向管理員發送警報
- 維持最小數量的日誌細節，例如封包抵達時間、防火牆運作描述及運作原因
- 支援 UNIX Syslog 格式
- 按網路管理員的日程安排發送日誌報告 e-mail，或者在日誌檔案已滿時按預設值設定發送
- 所有的資訊都按照 WELF 格式發送
- ICMP 日誌記錄展示代碼和類型

2.4.1.8 遠端存取（Remote Access）

網際網路安全路由器防火牆允許網路管理員將用戶社區按訪問規則分割爲一個個訪問群組。用戶可以連線上主機使用登入介面。當用戶成功透過識別之後，網際網路安全路由器防火牆動態地啓動用戶群訪問規則設定。

接下來，這些規則將得到加強，直到用戶離開，或是直到非活動性的休息過程已經停止。

3 快速安裝指南

本安裝指南將告訴您如何連接本產品至您的電腦及區域網路（LAN），並連線至網際網路。

- 第一部分提供您設定硬體的說明。
- 第二部分告訴您如何在您的個人電腦上設定網際網路參數。
- 第三部分引導您正確設定網際網路安全路由器的基本設定，將區域網路接入網際網路。

在您設定好各項設備之後，您就可以參照第 20 頁的說明來檢查本產品是否正常運作。

本快速安裝指南假定您已經透過您的網路服務供應商（ISP）安裝了 ADSL 或是 cable modem。這些說明提供的基本設定方法都必須與您家裏或小型辦公室的網路設定一致。請參閱後面的章節來獲得更多的設定指導。

3.1 第一部分 — 連接硬體

在第一部分，請您先將本產品連接至 ADSL 或是 cable modem（也就是連接到電話線或是線纜接頭上）、連接電源線以及個人電腦，或是其他網路裝置。

小心

連接各項設備之前，請將所有設備電源開關關閉，包括您的電腦、區域網路（LAN）集線器/交換器，以及網際網路安全路由器。

圖 3.1 圖解了硬體之間的連接。請參考並按照下列步驟操作。

3.1.1 Step 1. 連接 ADSL 或 cable modem

將乙太網路線的一端連接到本產品後面板的 WAN 的連接埠，另一端連接到 ADSL 或是 cable modem 的乙太網路埠。

3.1.2 Step 2. 連接個人電腦或區域網路（LAN）

如果您的區域網路連接的電腦不超過四台，請直接將每台電腦乙太網路線連接到本產品後面板的 LAN 連接埠（P1—P4）即可。每一台電腦用一條乙太網路線連接到本產品後面板標示爲 P1—P4 的任意一個 LAN 連接埠。

如果您的區域網路連線的電腦超過四台，您必須用乙太網路線一端連接一台選購的集線器/交換器（可能是上行線連接埠，請參考該集線器/交換器用戶手冊），另一端連接至本產品後面板的 LAN 連接埠（標示爲 P1—P4）。

注意：本產品可以使用交叉的或是直的乙太網路線。

3.1.3 Step 3. 連接電源供應器

請將電源線的一端連接到本產品後面板標示爲 POWER 的電源插座，另一端請連接到牆壁上的電源插座。

3.1.4 Step 4. 開啓網際網路安全路由器、ADSL 或是 cable modem 的電源，並打開您的個人電腦

請按下本產品後面板的電源開關至 ON 位置，開啓 ADSL 或是 cable modem 的電源，並打開每一台連接到路由器上的個人電腦，打開任何 LAN 設備（如集線器/交換器）的電源。

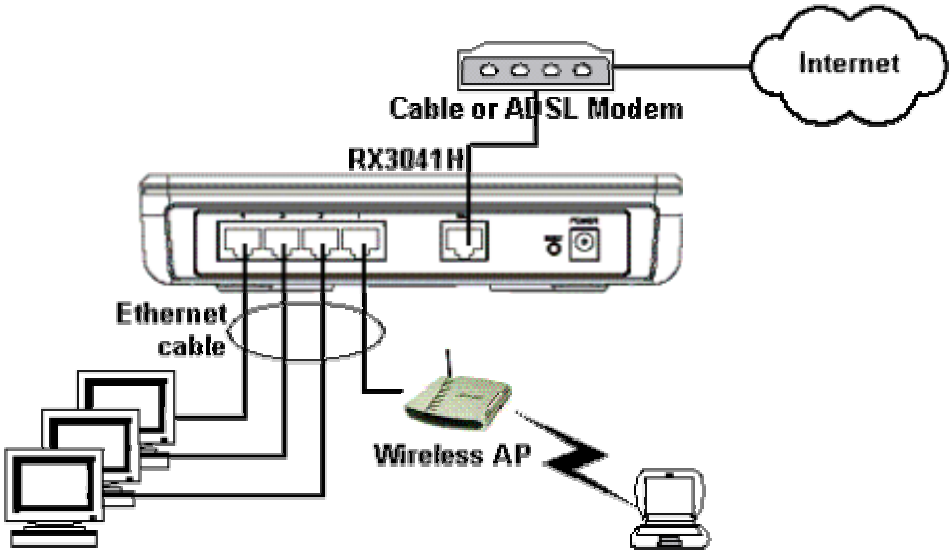


圖 3.1. 硬體連接概況

您必須確認 LED 指示燈是否如表 3.1 所示運作正常。

表 3.1. LED 指示燈

指示燈	狀 態
POWER	亮綠燈顯示電源連接正常；倘若燈不亮，請檢查電源線是否有連接到牆壁上的電源插座，連接至本產品後面板電源插座的電源線是否連接妥當。
LAN1—LAN4	亮綠燈顯示本產品可以正常地與您的區域網路設備聯線；閃爍代表本產品正在與您的區域網路設備傳送或接受資訊。
WAN	亮綠燈顯示本產品已與您的網際網路服務供應商聯線；閃爍代表本產品正在從網際網路傳送或接收資訊。

若指示燈如上表預期一樣運作正常，則代表本產品已妥當連接且運作正常。

3.2 第二部分 — 設定網際網路參數

第二部分告訴您如何在您的個人電腦上設定網際網路參數以與網際網路安全路由器協調工作。

3.2.1 在您開始之前

本產品預設值將會自動設定您的電腦所有必需的網路設定，您只需要讓您的電腦接受這些設定即可。


注意

在某些狀況下，您可能希望手動設定某幾台或是所有電腦的相關網路設定參數，而不接受網際網路安全路由器的自動設定值，請參考第 13 頁"手動靜態 IP 位址設定"的說明。

- 如果您已經透過乙太網路將您的個人電腦與網際網路安全路由器相連，請參考以下不同作業系統的操作步驟來設定您的參數。

3.2.2 Windows® XP：

1. 在 Windows 桌面任務列中點選 **<開始>** ，然後點選 **<控制台>**。
2. 雙擊 **<網路連線>** 圖示。
3. 在 **<LAN> 或<高速 Internet>** 視窗，在您的個人電腦相關的網路介面卡（NIC）圖示（通常顯示爲 **<區域連線>**）按下右鍵，點選 **<內容>**。

   <區域連線 內容> 對話窗將列出一串目前已經安裝的網路選項。
4. 請確認 **<Internet 協定（TCP/IP）>** 左邊的選取方塊爲打勾，點選該選項，然後點選 **<內容>** 。
5. 在 **<Internet 協定（TCP/IP）>** 對話窗，點選 **<自動取得 IP 位址>**，再點選 **<自動取得 DNS 伺服器位址>**。
6. 點選 **<確定>** 兩次，以保存您的設定，並關閉 **<控制台>**。

3.2.3 Windows® 2000：

首先請確定系統是否安裝了 **Internet 協定（TCP/IP）**，若無則必須安裝：

1. 在 Windows 桌面任務列中點選 **<開始>** ，再點選 **<設定>**，然後點選 **<控制台>**。
2. 雙擊 **<網路和撥號連線>** 圖示。
3. 在 **<網路和撥號連線>** 視窗，在 **<區域連線>** 圖示按下右鍵，點選 **<內容>**。

   <區域連線 內容> 對話窗將列出一串目前已經安裝的網路選項，若 **Internet 協定（TCP/IP）**在已安裝的列表中，請跳至步驟 10。
4. 若 **Internet 協定（TCP/IP）**不在已安裝的列表中，請點選 **<安裝>** 。
5. 在 **<選擇網路元件類型>** 對話窗，請點選 **<通訊協定>** ，然後點選 **<新增>** 。
6. 在**通訊協定**列表中，點選 **<Internet 協定（TCP/IP）>**，然後點選 **<確定>** 。

   安裝程式可能需要您將 Windows 2000 安裝光碟放入光碟機中，請依照螢幕指示操作。
7. 在接下來的對話窗，點選 **<確定>**，用新的設定重新啓動電腦。

   接下來，設定您的電腦以接受網際網路安全路由器的自動設定：
8. 在控制台視窗，雙擊 **<網路和撥號連線>** 圖示
9. 在 **<網路和撥號連線>** 視窗，在 **<區域連線>** 圖示按下右鍵，點選 **<內容>**。
10. 在 **<區域連線 內容>** 對話窗，點選 **Internet 協定（TCP/IP）**，然後點選 **<內容>**。

11. 在 **<Internet 協定（TCP/IP）>** 對話窗，點選 **<自動取得 IP 位址>**，再點選 **<自動取得 DNS 伺服器位址>**。
12. 點選 **<確定>** 兩次，以保存您的設定，並關閉 **<控制台>**。

3.2.4 Windows® 95/ 98/ Me：

1. 在 Windows 桌面任務列中點選 **<開始>** ，再點選 **<設定>**，然後點選 **<控制台>** 。
2. 雙擊 **<網路>** 圖示。

   <網路 內容> 對話窗將列出一串目前已經安裝的網路選項，請尋找 **<TCP/IP>** 開頭，且字串中顯示您的網路配置卡的選項。若 **<TCP/IP>** 在已安裝的列表中，請跳至步驟 9。
3. 若 **<TCP/IP>** 不在已安裝的列表中，請點選 **<確定>**。
4. 在 **<選擇網路元件類型>** 對話窗，請點選 **<通訊協定>** ，然後點選 **<新增>**。
5. 在**製造廠商**部分點選 **Microsoft**，在**網路通訊協定**中，點選 **< TCP/IP>**，然後點選 **<確定>**。

   安裝程式可能需要您將 Windows 95、98 或 ME 安裝光碟放入光碟機中，請依照螢幕指示操作。
6. 在接下來的對話窗，點選 **<確定>**，用新的設定重新啓動電腦。

   接下來，設定您的電腦以接受網際網路安全路由器的自動設定：
7. 在控制台視窗，雙擊 **<網路>** 圖示。
8. 在 **<網路 內容>**視窗，點選 **<TCP/IP>** 開頭，且字串中顯示您的網路配置卡的選項，然後點選 **<內容>**。

   倘若您有不只一個 **<TCP/IP>** 網路元件，請選擇屬於您的網路配置卡相關的元件。
9. 在 **<TCP/IP 內容>** 視窗，點選 **<TCP/IP>** 索引卷標，點選 **<自動取得 IP 位址>**。
10. 在 **<TCP/IP 內容>** 視窗，點選 **<預設閘道>** 索引卷標，在 **<新的閘道>** 欄位輸入 **192.168.1.1**，然後點選 **<新增>**。
11. 點選 **<確定>** 兩次，以儲存您的設定，並關閉 **<控制台>**。
12. 如果系統要您重新開機，請點選 **<是>** ，重新啓動電腦。

3.2.5 Windows® NT 4.0 工作站：

首先請確定系統是否安裝了 **Internet 協定（TCP/IP）**，若無則必須安裝：

1. 在 Windows 桌面任務列中點選 **<開始>** ，再點選 **<設定>**，然後點選 **<控制台>**。
2. 在控制台視窗，雙擊 **<網路>** 圖示。
3. 在 **<網路>** 視窗，點選 **<協定>** 圖示。

   <協定> 對話窗將列出一串目前已經安裝的網路選項，若 **Internet 協定（TCP/IP）**在已安裝的列表中，請跳至步驟 9。

4. 若 **Internet 協定（TCP/IP）**不在已安裝的列表中，請點選 **<新增>**。
5. 在**通訊協定**列表中，點選 **<Internet 協定（TCP/IP）>**，然後點選 **<確定>**。

   安裝程式可能需要您將 Windows NT 安裝光碟放入光碟機中，請依照螢幕指示操作。

   當所有的檔案都安裝好後，螢幕上會跳出視窗提醒您，被稱爲 DHCP 的 TCP/IP 服務已建立來動態分配 IP 資訊。
6. 點選 **<是 >** 繼續，再點選 **<確定>**，用新的設定重新啓動電腦。

   接下來，設定您的電腦以接受網際網路安全路由器的自動設定：
7. 打開**控制台**視窗，雙擊 **<網路>** 圖示。
8. 在 **<網路>** 視窗，點選 **<協定>** 圖示。
9. 在 **<協定>** 對話窗，點選 **Internet 協定（TCP/IP）**，然後點選 **<內容>**。
10. 在 **<TCP/IP 內容>** 視窗，點選 **<TCP/IP>** 索引卷標，點選 **<從 DHCP 伺服器自動取得 IP 位址>** 。
11. 點選 **<確定>** 兩次，以保存您的設定，並關閉 **<控制台>**。

3.2.6 手動固定 IP 位址設定

在某些狀況下，您可能希望手動設定某幾台或是所有電腦的相關網路設定，而不接受網際網路安全路由器的自動設定值。在下列情況中，這種狀況是有需求的，但並非必需：

- 您已經獲得了一個或多個公共 IP 位址，而且您希望經常性地與某些特定的電腦聯繫（例如，您將電腦用作公共網路服務器）。
- 您在區域網路（LAN）內設有子網路。

本產品預設的區域網路位址是 192.168.1.1，無論如何，第一次設定本產品時，您必須將您的電腦的 IP 位址指定在 192.168.1.0 子網路下（譬如 192.168.1.2）以建立本產品與您電腦的聯線。子網路遮罩必須輸入 255.255.255.0，預設閘道設定爲 192.168.1.1 ，這些設定可以稍後再修改以符合真實的網路環境。

對那些欲設定靜態 IP 位址的電腦，請參考第 11 到 14 頁的方法，將原本**自動設定 IP 位址**的部分，改成**指定 IP 位址**，並輸入子網路遮罩 255.255.255.0，預設閘道 192.168.1.1 。


注意

每一台電腦都必須設定不同的 IP 位址，但都必須在 192.168.1.0 子網路下（譬如192.168.1.2…）。如果您要爲所有的區域網路電腦設定 IP 資訊，您可以按照第五章的說明來相應地更改區域網路介面 IP 位址。

3.3 第三部分 — 快速設定網際網路安全路由器

第三部分將帶您登入網際網路安全路由器設定管理程式，進行相關的基本設定。您的網路服務供應商已經提供了一些相關資訊可以完成本基本設定。本快速安裝僅提供基本設定指南，詳細的設定及高級功能請參考相應章節。

3.3.1 設定按鈕說明

本產品提供一個預先安裝的設定管理程式（Configuration Manager），可以讓您透過瀏覽器設定您的網際網路安全路由器。設定精靈將帶領您一步一步的完成設定，以下是您在設定過程中將會遇到的按鈕說明。

按鈕	*功 能*
Next	點選此按鈕跳到下一個設定步驟，倘若該頁設定不需任何修改，可以直接按下此按鈕，跳到下一個步驟。
Back	點選此按紐跳回上一個設定步驟。

3.3.2 設定網際網路安全路由器

請參考下列步驟：

1. 在登入本產品設定頁面之前，請您務必關閉 HTTP 代理伺服器。點選 IE 瀏覽器的**工具 ➔ 網路選項 ➔ 連線 ➔ 區域網路設定**，將**爲 LAN 使用代理伺服器**核取方塊取消。

2. 在任何一台連接本產品的網路電腦上，請打開網路瀏覽器輸入以下網址，然後按下 **<Enter>**：

   http://192.168.1.1

   這是預先定義好設在互聯網安全路由器 LAN 埠的 IP 位址 。

   將會出現如圖 3.2 登入頁面：

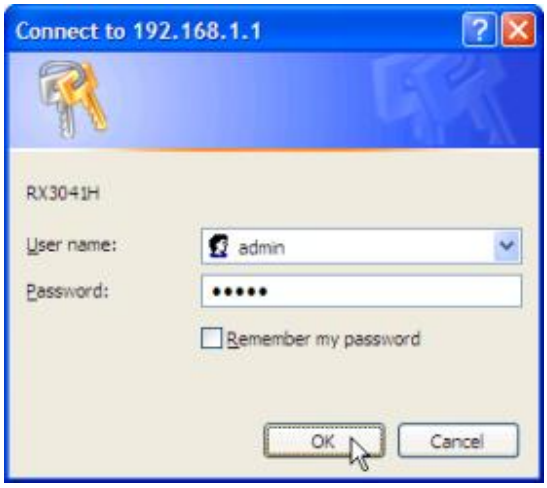


圖 3.2. 登入頁面

   倘若您無法連線到網際網路安全路由器，未出現登入頁面，您必須確認該電腦是否已接受網際網路安全路由器自動設定的 IP 位址，另一個方法是手動設定該電腦的 IP 位址在 192.168.1.0 的子網路下，譬如將 IP 位址設定爲 192.168.1.2。

3. 第一次登入時，請在上圖登入頁面輸入以下預設的姓名及密碼，然後點選 OK。登入之後您可以自行修改密碼。

   User Name 預設值： admin

   Password 預設值： admin

注意

您可以隨時更改密碼（請參考第 124 頁 11.1.1 更改登入密碼）

登入之後將出現以下設定主頁面（請參看第 15 頁圖 3.3）。

圖 3.3. 設定主頁面

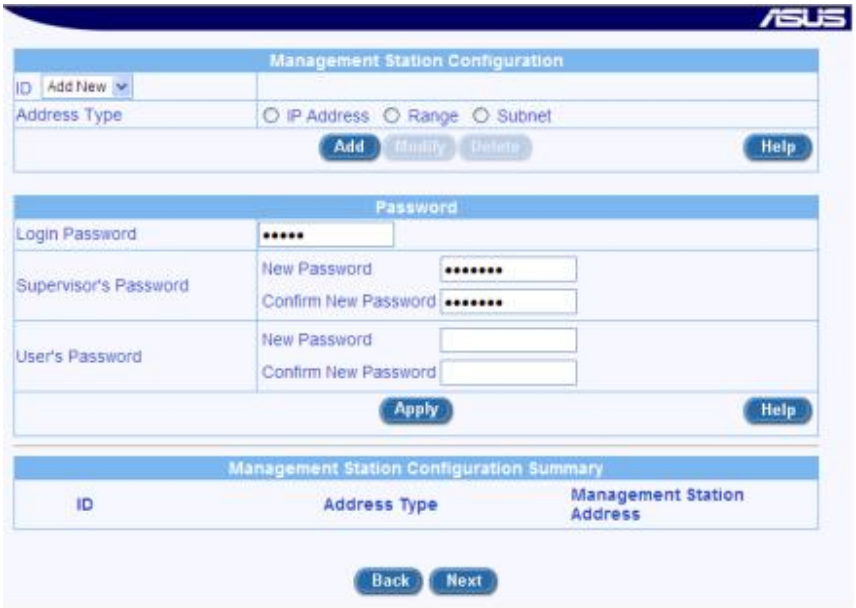


圖 3.4. 密碼設定頁面

4. 點選 Next 按鈕進入圖 3.4 密碼設定頁面，若不想修改密碼，請按下 Next 按鈕。
改變密碼前，首先要在 **login password** 欄位輸入目前的密碼，在 **New Password** 及 **Confirm New Password** 欄位輸入新的密碼，然後點選 Apply 按鈕以保存設定。

5. 出現圖 3.5 所示頁面，請在各欄位輸入相關資訊，然後點選 Apply 按鈕以保存設定。否則，按下 Next 按鈕，直接跳到下一個設定頁面。

圖 3.5. 系統資訊設定頁面

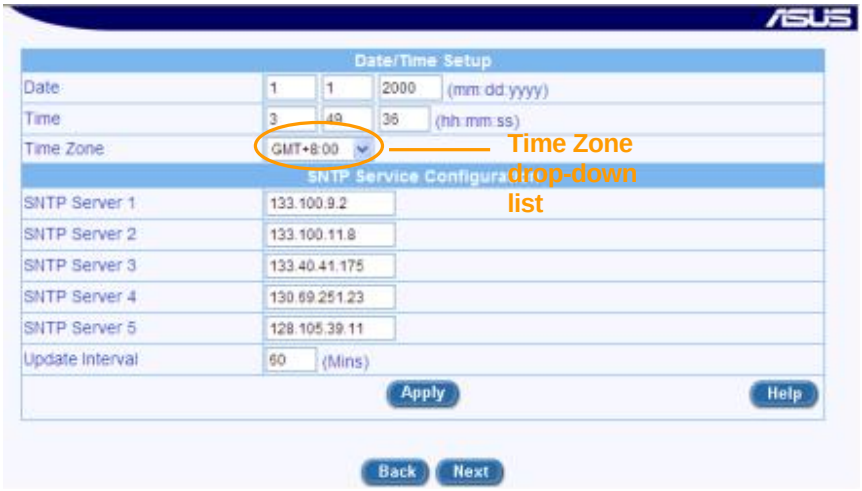


圖 3.6. 日期 / 時間設定頁面

6. 在圖 3.6 頁面，請在 Time Zone 欄位右邊按下拉式選單選取本產品所在時區，然後點選 Apply 按鈕以保存設定。點選 Next 按鈕跳到下一個設定頁面。

   本產品內部並無時鐘，系統的日期 / 時間是透過外部的網路服務器管理，因此不需要在此處設定日期 / 時間，除非您無法進入外部的網路服務器，或是您想透過網際網路安全路由器來管理日期 / 時間。

7. 出現圖 3.7 區域網路 IP 設定頁面，請勿現在更改預設的區域網路 IP 位址，直到您完成以下設定，並確認您的網際網路操作正常。點選 Next 按鈕跳到下一個設定頁面。

圖 3.7. 區域網路 IP 設定頁面

圖 3.8. DHCP 伺服器設定頁面

8. 在圖 3.6 DHCP 伺服器設定頁面，請勿修改 DHCP 伺服器預設值，直到您完成以下設定，並確認您的網際網路操作正常。點選 Next 按鈕跳到下一個設定頁面。

9. 圖 3.7. 是網際網路安全路由器的廣域網 WAN 設定，本項目視您的網路服務供應商 ISP 提供的連線模式而定，您可以從圖 3.9 connection mode 下拉式功能表的三個選項中選擇一設定 ：PPPoE、Dynamic 和 Static。

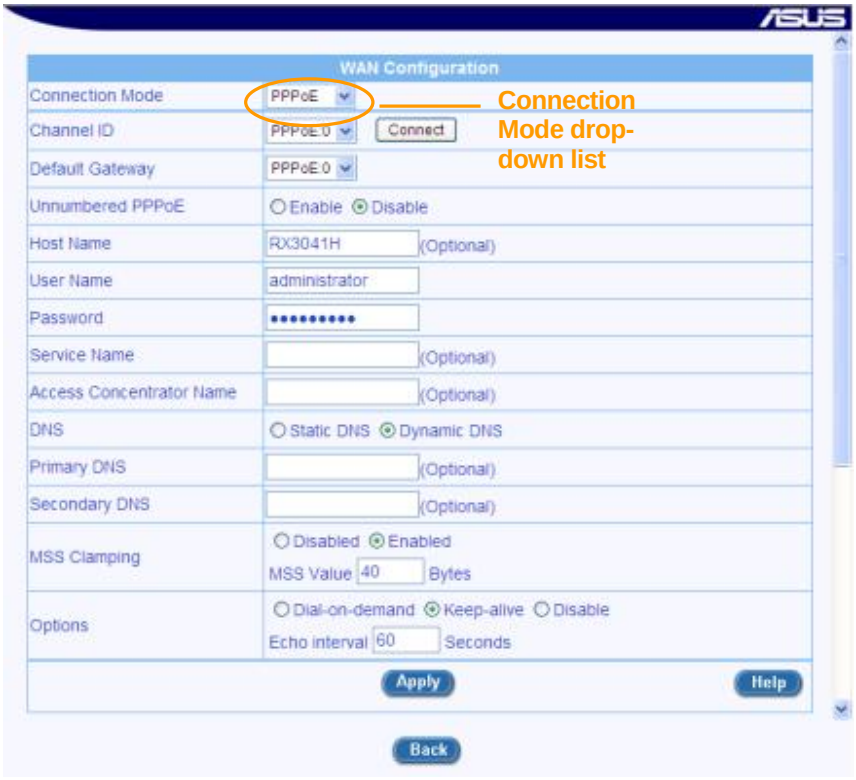


圖 3.9. WAN PPPoE 設定頁面

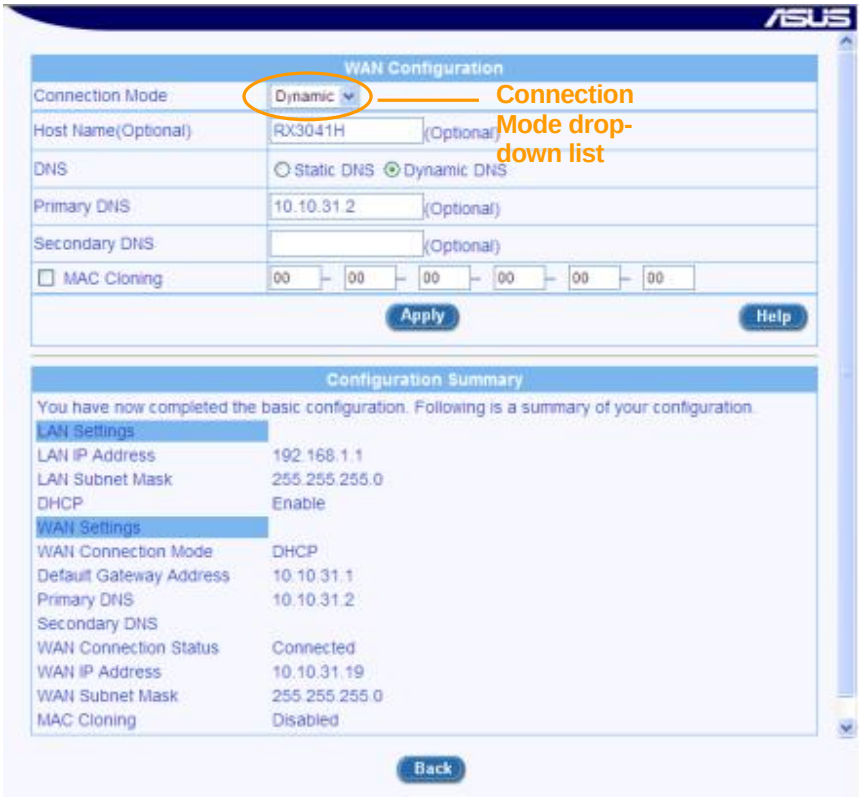


圖 3.8. WAN 動態 IP 設定頁面

a) PPPoE 連線模式（參看圖 39）

- 您不需輸入 primary/secondary DNS IP 位址，PPPoE 連線模式可自動從您的 ISP 獲得相關資訊，若您想用您慣用的 DNS 伺服器，您可以在此輸入位址。
- Host name 非必要，若您的 ISP 並未提供 host name，該處可以留下空白。
- 在 user name 及 password 欄位輸入您的 ISP 提供的 user name 及 password。
- 點選 Apply 按鈕以保存 PPPoE 設定。

b) 動態 IP 連線模式（參看 圖 3.8）

- 您不需輸入 primary/secondary DNS IP 位址，DHCP 用戶端可自動從您的 ISP 獲得相關資訊，若您想用您慣用的 DNS 伺服器，您可以在此自行輸入位址。
- Host name 非必要，若您的 ISP 並未提供 host name，該處可以留下空白。
- 倘若您事先已在 ISP 設定了 MAC 位址以連上網際網路，請在 MAC cloning 欄位輸入該 MAC 位址，並記得點選左邊的選取方塊。
- 點選 Apply 按鈕以保存動態 IP 設定。

圖 3.9. WAN 靜態 IP 設定頁面

c) 靜態 IP 連線模式

- 在 IP Address 欄位裏輸入 WAN IP 位址，本資訊由您的 ISP 提供。

- 在 Subnet Mask 欄位輸入子網路遮罩，本資訊由您的 ISP 提供，通常是 255.255.255.0。
- 在 gateway address 欄位輸入閘道位址，本資訊由您的 ISP 提供。
- 在 primary DNS IP 欄位輸入您的 ISP 提供的 IP 位址，Secondary DNS IP 非必要，若您的 ISP 有提供再填。
- 點選 

按鈕以保存固定的 IP 設定。

您已經完成本產品的基本設定。請參考以下部分確定您是否已經連入網際網路。

3.3.3 測試您的設定

您已經完成本產品的基本設定，連接在本產品的區域網路上的電腦可以透過網際網路安全路由器所連接的 ADSL 或是 cable modem 連線到網際網路。

打開您區域網路上電腦的網路瀏覽器，輸入任何一個外部網站（譬如 *http://www.asus.com*），標示爲 WAN 的指示燈將會快速閃爍，等到連上之後就會保持亮燈狀態，您將可以看到網頁頁面。

倘若指示燈並未閃爍或亮燈網頁也未出現，請參考附錄 15 “解決問題” 章節內容中更爲詳盡的說明。

3.3.4 路由器預設設定

除了控制 DSL 連線到 ISP 上之外，網際網路安全路由器還能爲您提供多種多樣的網路服務。您的路由器已經預設好了適合典型家庭和小型辦公室網路應用的預設設定。

表 3.2 列出了一些最重要的預設設定。這些設定和其他一些規格將在下面的章節中詳盡介紹。如果您熟悉您的網路預設設定，請查看表 3.2 中的設定來確定它們是否符合您網路的要求。如需要，請根據說明來更改設定。如果您對設定不太熟悉，那麼請勿更改設定，或者請聯絡您的網路供應商 ISP 尋求幫助。

在您更改任何設定之前，請參考第 4 章獲取連線和使用 Configuration Manager program（設定管理器程式）的綜合資訊。我們強烈推薦您在更改預設設定之前聯絡您的網路供應商！

表 3.2. 預設設定摘要

選 項	預設設定	解釋 / 說明
DHCP（主機動態設定協定）	DHCP 伺服器在以下位址起作用： 192.168.1.10 透過 192.168.1.108	網際網路安全路由器爲您的區域網路（LAN）中的電腦提供一些私人 IP 位址的動態分配。要享受此項功能帶來的好處，您必須按照“快速安裝指南” 第二部分中描述的那樣設定您的電腦，以便能夠動態地接收 IP 資訊。請參看第 5.2 節中關於 DHCP 伺服器的說明。
LAN 埠 IP 位址	靜態 IP 位址：192.168.1. 1 子網路遮罩：255.255.255.0	這是 LAN 埠在網際網路安全路由器上的 IP 位址。LAN 埠將您的電腦接入乙太網路。一般來說，您並不需要改變這個位址。請參考第 5.1 節中區域網路（LAN）位址的說明。

4 從設定管理器程式安裝

網際網路安全路由器已經預先安裝了一個名爲 *設定管理器* 的程式，這個程式提供本產品已安裝好的軟體介面。它能讓您設定本產品來符合您網路的要求。您可以從任何以 LAN 或 WAN 接入網際網路安全路由器的 PC 上的網頁瀏覽器接入。

本章將幫助您使用設定管理器來安裝。

4.1 登入設定管理器

設定管理器程式已經預先安裝在網際網路安全路由器上。要進入該程式，您需要：

- 接入網際網路安全路由器 LAN 或 WAN 埠的電腦設定請參考第 3 章"快速安裝指南"。
- 在電腦上安裝網頁瀏覽器。您必須具備網頁瀏覽器 Internet Explorer 軟體，版本在 5.5 以上，或者 Netscape 瀏覽器，版本在 7.0.2 以上。

您可以從任何透過 LAN 或 WAN 埠連接網際網路安全路由器的電腦進入該程式。但是，我們在這裏提供的說明僅針對透過 LAN 埠連接網際網路的電腦。

1. 將電腦接入 LAN，打開網頁瀏覽器，輸入下面的網址，按 **<Enter>**鍵：

   http://192.168.1.1

   這是預先定義好的網際網路安全路由器 LAN 埠的 IP 位址。登入頁面將如圖 4.1 所示：

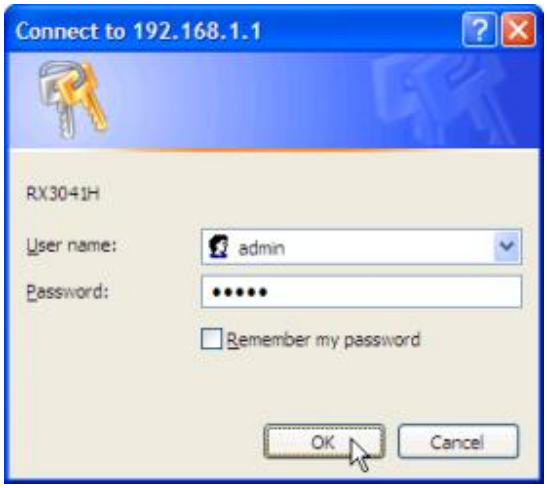


圖 4.1. 設定管理器登入頁面

2. 輸入您的 user name 和 password，然後點選 OK。

   在您第一次進入程式時，請選擇下列預設值：

   Default User Name: admin

Default Password: admin

4.1.1 您可以在任何時候更改 password（請參看第 124 頁 11.1.1 節 變更登入密碼

當您第一次登入設定管理員，您可以使用預設的使用者名稱與密碼:admin 與 admin 。系統會允許兩種使用者登入，分別爲系統管理員（administrator: username:admin）與訪客（guest:username:guest）。其中系統管理員具有權力去修改設定，而訪客則只能檢視系統設定。至於這兩組使用者的密碼則爲 admin 與 guest，系統管理員可針對密碼進行變更。

Note

此處的使用者名稱與密碼只用來登入設定管理員之用，此一帳號密碼與您用來與 ISP 連線的帳號密碼不同。

請依照下列步驟來變更密碼:

1. 藉由點選 System **Management ➔ Password** 選單來開啓密碼設定頁面。
2. 輸入既有的密碼在 **Login Password** 欄位。
3. 在 New **Password** 欄位輸入新的密碼，並在 Confirm **New Password** 欄位重新輸入一次密碼。

注意

密碼可以是十六位數字，當您登入時，您必需在上方與下方的欄位輸入新的密碼。

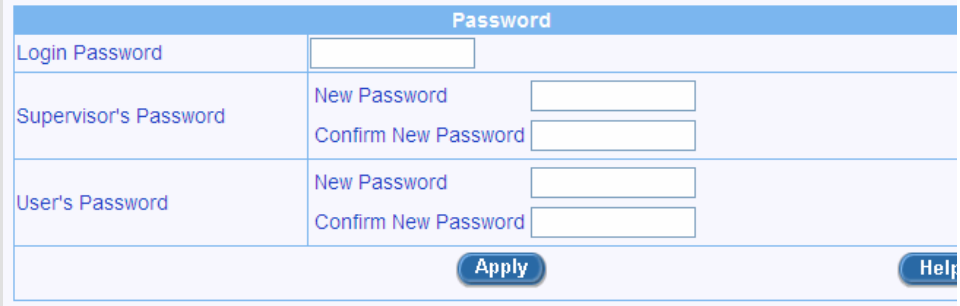


圖 11.2. 密碼設定

4. 點選 Apply 按鍵來儲存新的密碼。請注意只有在密碼輸入正確並在正確的欄位才會生效。

4.1.2 設定管理站

有時候，您可能想要限制主機對路由器進行設定。在預設值中，只要輸入的帳號與密碼正確，則可讓系統管理員從任何電腦登入。這樣的作法可讓未經認證者在知道設定管理員介面的帳號與密碼的情況下進行登入。在此設定頁面中您可利用輸入單一 IP 位址、IP 位址範圍或網路位址與子網路遮罩，最多設定八組的管理站。

WARNING

若管理站群組未經設定，則管理員可從任何地方登入路由器。然而，若有一組一組或更多的管理站群組被設定，則只有經過設定之特定管理站群組可以設定路由器。若您忘記管理群組的設定，您將無法存取路由器的設定管理員介面，除非按下路由器的重置鍵進行重置。F

管理站參數設定

表 11.1 敘述管理站設定頁面中可進行設定的參數。

表 11.1. 管理站參數設定

欄位	敘述
ID	
Add New	點選此選項來新增一組新的管理群組。
Number	從下拉式選單中選擇管理群組以變更設定。
Address Type 本選項可讓您選擇您要如何指定工管理站群組使用的IP位址。在此共有三種選項可供設定，分別是: IP 位址、範圍與子網路。	
IP Address	本選項可讓您指定管理站的IP位址。
Address	指定一組適當的IP位址。
Range	本選項可讓您從管理站群組指定IP位址範圍。當本選項被選擇，則以下的欄位便可以進行設定:
Begin	輸入起始的IP位址範圍。
End	輸入中止的IP位址範圍。
Subnet	本選項可讓您指定所有連接到相同IP子網路的電腦作爲一管理站群組。當本選項被選擇，則以下的項目便可以加以輸入:
Network Address	輸入適當的IP位址。
Subnet Mask	輸入對應的子網路遮罩。

新增一組管理站群組

請依照以下介紹來新增一組管理站群組:

5. 藉由點選 System **Management ➔ Password** 選單來開啓密碼設定頁面。
6. 從“ID”下拉式選單中選取 “Add **New”** 。
7. 在以下三選項選擇 “Address Type”（位址類型） **– IP Address, Range** 與 **Subnet** ，接著請輸入您想要輸入的 IP 位址資訊。

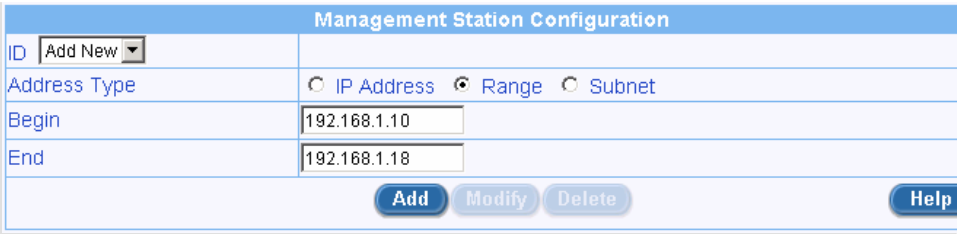


圖 11.3. 管理站設定

8. 點選 Add 按鍵來新增一組新的管理站群組。您將可看到新增的管理站群組摘要顯示在同一設定頁面。

圖 11.4. 管理站摘要

變更管理站群組

請依照以下介紹來變更管理站群組:

9. 藉由點選 System **Management ➔ Password** 選單來開啓密碼設定頁面。
10. 從 ID 下拉式選單中選擇一管理群組。
11. 請在“Address **Type”項目中設定想要進行的變更並輸入對應的** IP 位址資訊。
12. 點選 Modify 按鍵來變更設定。

刪除管理站群組

如欲刪除管理站群組，您只要點選點選選項前的 圖示 (在管理站摘要列表中)即可加以刪除，或是依照以下介紹進行刪除:

13. 藉由點選 System **Management ➔ Password** 選單開啓密碼設定頁面。
14. 從“ID”下拉式選單中選擇一組管理群組的號碼。
15. 點選 Delete 按鍵來刪除管理站群組。

）

當您每次登入程式時，設定頁都會出現。（請參看第 23 頁）

4.2 功能性設定

一般來說，設定管理器頁面包括兩個獨立的頁面，如圖 4.2 所示，左邊的頁面包括所有的設備設定。功能表將會用圖示 提示您，相關的功能表將分類標出，例如 LAN、WAN 等等。基於功能表中是否有子資料夾，分別以不同的資料夾圖示 或 標出。您可以點選任意的功能表來進入特定的設定頁。

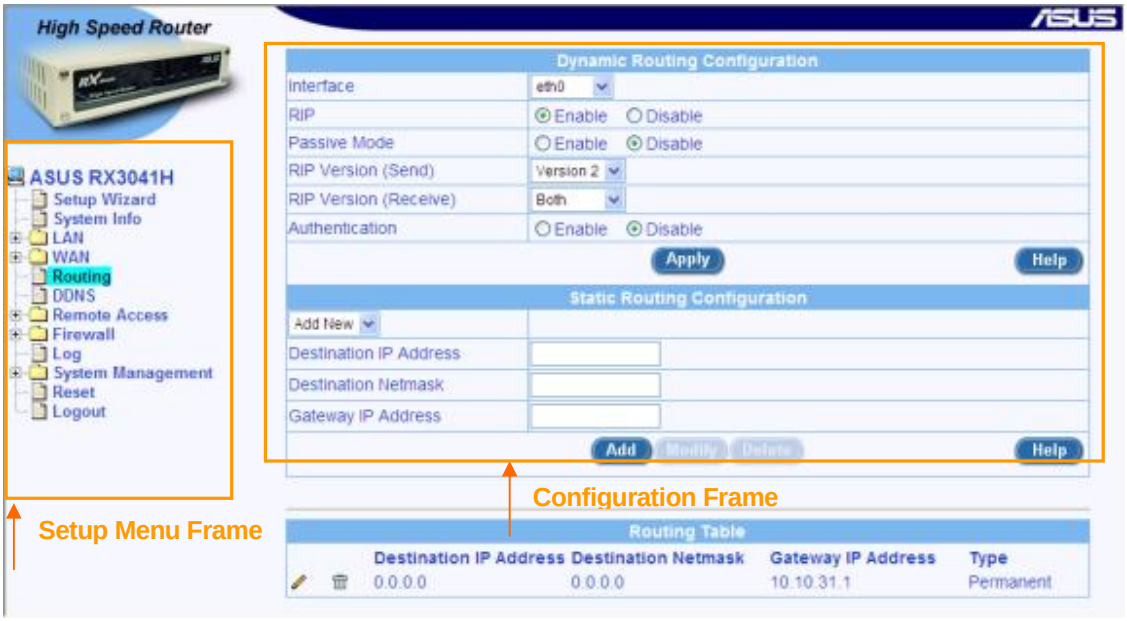


圖 4.2. 一般設定管理器頁面

每個功能表都會顯示右邊頁面中的獨立頁面。例如，圖 4.2 中的設定頁面表示 DHCP 設定。

4.2.1 建立功能表導航提示

- 要擴展到一系列相關的功能表：點選 **+** ，然後點選相應資料夾的圖示。
- 要縮短顯示的相關功能表：點選 **–** ，然後點選打開的資料夾圖示。
- 要打開特定的設定頁，點選資料圖示，然後進入您的目標選項。

4.2.2 經常用到的按鈕和圖示

下面的按鈕和圖示將在很多地方用到。下表列出了每個按鈕和圖示的功能。

表 4.1. 經常用到的按鈕和圖示

按鈕/圖示	*功 能*
Apply	隨時保存您在當前頁面上所做的任何更改。
Add	將現有的設定保存至系統，例如，靜態路由線路或防火牆 ACL 規則等等。
Modify	更改系統現有的設定，例如，靜態路由線路或防火牆 ACL 規則等等。

按鈕圖示	功 能
Delete	刪除已選的選項，例如靜態路由線路或防火牆 ACL 規則等等。
Help	在獨立的瀏覽器視窗中開啓爲現有主題設定的在線幫助。任何主要主題的幫助頁面均可用。
Refresh	重新顯示現有頁面更新後的統計表或設定。
	選擇要編輯的選項。
	刪除已選的選項。

4.3 系統設定概述

要概覽整個系統設定，請以管理員身份登入設定管理器，然後點選**系統資訊**功能表。 圖 4. 顯示了系統資訊頁面的一些資訊。

圖 4.3. 系統資訊頁

5 設定區域網路 LAN

本章將向您說明如何設定連接您的 LAN 電腦的網際網路安全路由器 LAN 介面的 LAN 屬性。在本章，您將學會如何爲您的區域網路設定 IP 位址、DHCP 和 DNS 伺服器。

5.1 區域網路（LAN） IP 位址

如果您將多台 PC 連入網際網路安全路由器，您必須透過內建的乙太網交換器上的乙太網區域網路（LAN）埠連接。您必須指派一個唯一的 IP 位址給每個連接到區域網路（LAN）的設備。區域網路（LAN）的 IP 位址把網際網路安全路由器認作您網路的一個節點。那就是說，它的 IP 位址必須與您的 PC 處於相同的區域網路（LAN）的子網路中。網際網路安全路由器預設的區域網路（LAN）IP 位址爲 192.168.1.1。


名詞解釋

*當某一設備連線進入網路，它就可以被認爲是**網路節點**，例如網際網路安全路由器的 LAN 埠，PC 的網路介面卡等，請參考附錄 A 對子網路的解釋。*

您可以將預設值按照您想要使用的網路 IP 位址改變。


注意

網際網路安全路由器自身能夠爲您接入區域網路的電腦起到 DHCP 伺服器的作用，正如第 5.2.2 節 設定，但是不能作爲它自身的 LAN 埠。

5.1.1 區域網路（LAN） IP 設定參數

表 5.1說明了區域網路（LAN） IP 設定的現有參數。

表 5.1. 區域網路（LAN） IP 設定參數

設定	說明
IP 位址	網際網路安全路由器的區域網路（LAN）IP 位址。此 IP 被您的電腦用來識別網際網路安全路由器的 LAN 埠。請注意，您的網路供應商指派給您的公共 IP 位址**並非**您的區域網路（LAN）的 IP 位址。公共 IP 位址確認進入網際網路的安全路由器上的 WAN 埠。
子網路遮罩	區域網路（LAN）的子網路遮罩確認區域網路（LAN）的 IP 位址的哪個部分整體提及您的網路，以及哪個部分特別提及網路的節點。您的設備已經預先設定好了預設的子網路遮罩 255.255.255.0。

5.1.2 設定區域網路（LAN）的 IP 位址

請參照以下步驟來更改預設的區域網路（LAN）IP 位址：

1. 以管理員身份登入設定管理員程式，然後點選 LAN 功能表。

   當 LAN 設定的子功能表出現時，點選 IP 子功能表以顯示如圖 5.1 所示的設定頁面。

圖 5.1. LAN IP 位址設定頁面

2. 進入 LAN 的 IP 位址和網際網路安全路由器提供的子網路遮罩。
3. 點選 Apply 以保存區域網路（LAN）IP 位址。

   倘若您正在使用過去的乙太連線，並已經改變了 IP 位址，那麼連線將被中斷。
4. 如需要，請預先設定您的 PC，使他們的 IP 位址將他們置於與 LAN 埠的新 IP 位址相同的子網路下。 請參看“快速安裝指南”一章的第二部分 。
5. 在您的網頁瀏覽器/位址中輸入新的 IP 位址，登入設定管理器。

5.2 DHCP（動態主機控制協定）

5.2.1 簡介

5.2.1.1 什麼是 DHCP?

DHCP 是一種網路協定，它能使網路管理員集中管理網路中電腦 IP 資訊的指派和分配。

當您在網路上啓動 DHCP 時，您的設備 — 例如網際網路安全路由器 — 就可以給您的電腦分配臨時的 IP 位址，無論它們是否接入了網路。分配的設備稱爲 *DHCP 伺服器*， 接收設備稱爲 *DHCP 用戶端*。

注意

倘若您遵照“快速安裝指南”的說明行事，您要麼已經爲區域網路中的每台 PC 都設定了 IP 位址，要麼您已經認定 PC 將動態（自動）接收 IP 資訊。倘若您選擇動態接收資訊，那麼，您就已經將您的電腦設定爲 DHCP 用戶端，它將接受 DHCP 伺服器（例如網際網路安全路由器）指派的 IP 位址。

DHCP 伺服器掌握了一系列特定的 IP 位址，然後，當您需要接入網際網路時，再在特定的時間把它們“釋放”給您的電腦。

在啓動了 DHCP 的網路上，IP 資訊是 *動態* 而不是 *靜態* 地分配的。每次連入網路時，DHCP 用戶端分配到的位址都不同。

5.2.1.2 爲什麼使用 DHCP?

DHCP 允許您透過網際網路安全路由器管理和分配 IP 位址。如果沒有 DHCP，您就得逐一爲每台電腦設定 IP 位址和相關的資訊了。DHCP 常被用於大型網路和頻繁擴張或更新的網路。

5.2.2 設定 DHCP 伺服器

注意

網際網路安全路由器已經被預設定義爲 LAN 領域的 DHCP 伺服器，其預先定義的 IP 位址爲透過 192.168.1.42（子網路遮罩 255.255.255.0）的 192.168.1.10。要改變位址域，請按照本節中說明的程式進行。

5.2.2.1 DHCP 參數設定

表 5.2 敘述在 DHCP 服務中可進行設定的相關參數

表 5.2. DHCP 設定參數

選項	說明
IP 開始/結束的位址池	指定了 DHCP 位址池中開始和結束的位址 。
子網路遮罩	輸入 DHCP 位址池使用的子網路遮罩。
租用的時間	指派位址租用的時間將被連接到 LAN 的設備使用。
預設的閘道 IP 位址	接收 IP 位址的電腦閘道的預設位址在本領域。預設的閘道是 DHCP 用戶端最先連線到網際網路的設備。一般來說，將會是網際網路安全路由器的區域網路（LAN）埠的 IP 位址。
Primary/Secondary DNS 服務器 IP 位址	*網域名稱系統* 伺服器的 IP 位址將被從本領域接收 IP 位址的電腦使用。DNS 伺服器會把您輸入網頁瀏覽器的普通網際網路名稱轉換爲相同意義的 IP 位址。一般來說，伺服器由您的網路供應商設定，然而，您可以輸入網際網路安全路由器區域網路（LAN）的 IP 位址，因爲它是 LAN 電腦的 DNS 代理，並且促使 DNS 指令從 LAN 傳遞至 DNS 伺服器，以及把結果傳回 LAN 電腦。請注意，Primary 和 secondary DNS 伺服器均爲可選選項。
Primary/Secondary WINS 伺服器 IP 位址 (可選)	從 DHCP 伺服器的 IP 位址域接收 IP 位址的電腦將使用 IP WINS 伺服器的位址。直到您的網路擁有 WINS 伺服器後，您才需要輸入此資訊。

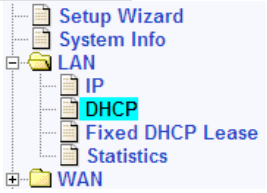
6. 點選 Apply 以保存 DHCP 伺服器設定。

5.2.2.2 設定 DHCP 伺服器

注意

網際網路安全路由器已經被預設定義爲 LAN 領域的 DHCP 伺服器，其預先定義的 IP 位址爲透過 192.168.1.42（子網路遮罩 255.255.255.0）的 192.168.1.10。要改變位址域，請按照本節中說明的程式進行。

首先，您必需設定讓您的 PC 可以接受由 DHCP 伺服器所指派的 DHCP 資訊:



7. 藉由點選 **LAN ➔ DHCP** 選單來開啓 DHCP 伺服器設定頁面。在此您將可看到既有的 DHCP 伺服器設定資訊，與當您開啓本頁面時的 IP 借出列表。
8. 輸入供 **IP 位址池 (Begin/End Address)**, **Subnet Mask**, **Lease Time** and **Default Gateway IP Address** 的相關資訊於對應的欄位; 至於其他像是 **Primary/Secondary**

DNS 伺服器的 IP 位址 與 **Primary/Secondary WINS 伺服器的 IP 位置** 則非必需輸入的. 然而，我們仍建議在 primary DNS 伺服器的欄位輸入對應的 IP 位址。此外，您可能需要輸入 LAN IP 位址或是您 ISP 的 DNS IP 位址在 primary DNS 伺服器的 IP 位址欄位中。如欲取得更多關於設定此參數的相關資訊，請參閱表 5.2 的介紹。

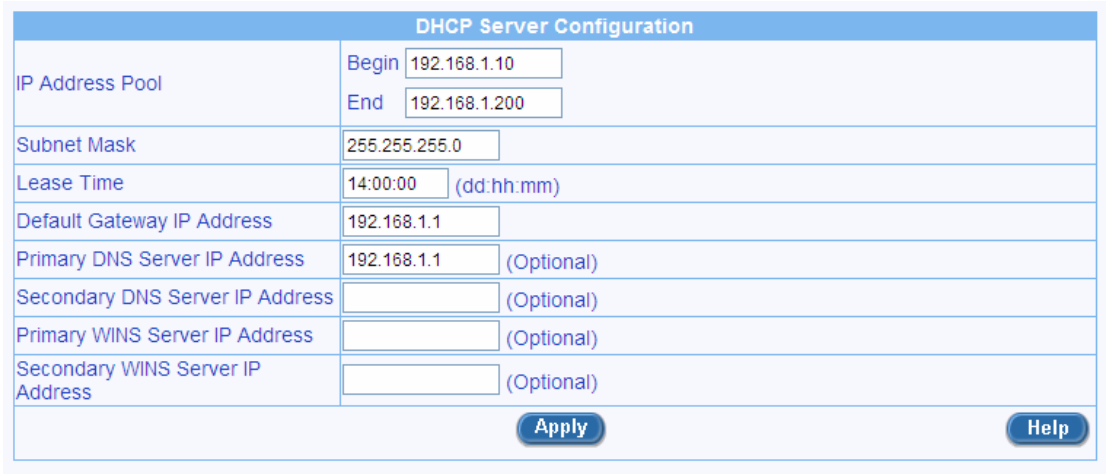


圖 5.2. DHCP 設定

9. 點選 Apply 以儲存 DHCP 伺服器的設定值。

5.2.2.3 查看目前已借出的 IP 位址

當在您的區域網路中 RX3041H 的功能是作爲 DHCP 伺服器的功能使用，則其將會借出 IP 位址給予您的電腦。如欲查看目前以借出的借出列表，只要藉由點選 **LAN ➔ DHCP** 選單以開啓 DHCP 伺服器設定頁面。接下來，如圖圖 5.3 I 所示的列表將會顯示在 DHCP 設定頁面的下半部。

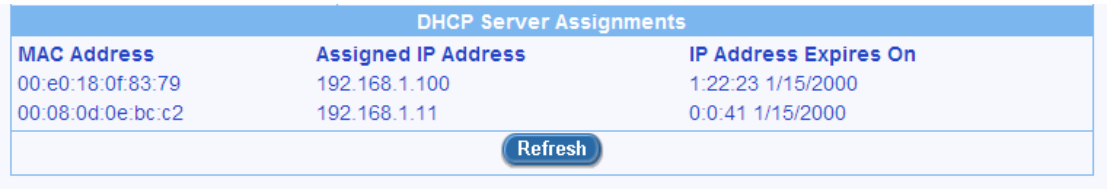


圖 5.3. DHCP 借出範例列表

在 DHCP 伺服器借出列表中將會顯示目前所有提供給區域網路裝置的 IP 位址。 表 5.3 敘述每一個 DHCP 借出列表中的參數資訊。

表 5.3. 指定 DHCP 位址參數

Field	Description
MAC Address	DHCP 伺服器中每一個裝置的硬體 ID。
Assigned IP Address	從位址池中所借出的位址。
IP Address Expired on	借出位址的中止時間。

5.2.3 固定 DHCP 借出

固定 DHCP 借出功能是當主機需要自 DHCP 伺服器中取得一組固定的 IP 位址時使用。要使用本功能，首先您需要設定您的 PC，使其可以接受 DHCP 伺服器所指派的 DHCP 資訊。

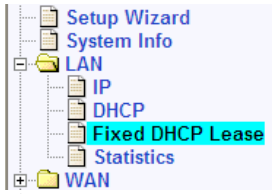
5.2.3.1 固定 DHCP 借出參數設定

表 5.4 敘述在 DHCP 借出功能中可以進行設定的參數。

表 5.4. 固定 DHCP 借出功能參數設定 s

欄位	敘述
Fixed DHCP Lease MAC	需要自 DHCP 伺服器中取得一組固定 IP 位址的硬體裝置 ID。
Fixed DHCP Lease IP	自 DHCP 伺服器中所借出的 IP 位址。本欄位建議設定 DHCP IP 位址池以外的 IP 位址。

5.2.3.2 新增一組固定 DHCP 借出



請依照下列的介紹來新增一組新的 DHCP 借出:

10. 藉由點選 **LAN ➔ Fixed DHCP Lease** 選單來開啓固定的 DHCPO 借出設定頁面。
11. 輸入主機要求之固定 IP 位址與 MAC 位址。關於每一項參數設定的細節，請參閱表表 5.4.。

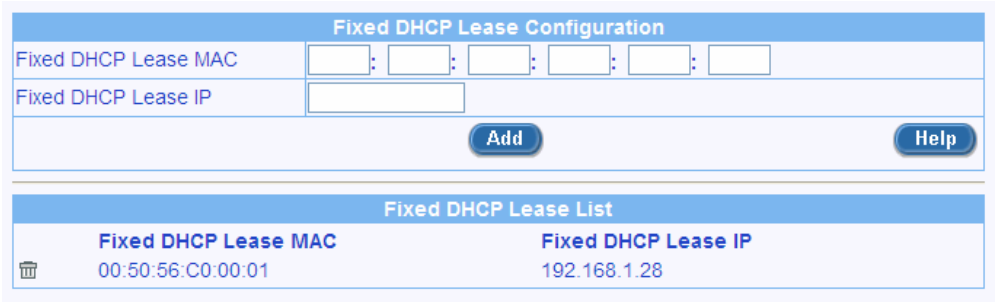


圖 5.4. 固定 DHCP 借出設定頁面

12. 點選 Add 按鍵以新增一組固定的 DHCP 借出登錄。

5.2.3.3 刪除一組固定的 DHCP 借出設定

如欲刪除一組固定的 DHCP 借出設定，您只需點選 DHCP 借出列表中的 圖示即可。

5.2.3.4 檢視固定的 DHCP 借出列表

如欲檢視既有的固定 DHCP 借出列表，您只要藉由點選 **LAN ➔ Fixed DHCP Leas** 選單來開啓固定 DHCP 借出設定頁面。

5.3 DNS

5.3.1 關於 DNS

網域名稱系統（DNS，Domain Name System）用來將用戶輸入到網頁瀏覽器的（例如，yahoo.com）網域名稱轉換爲可用來網際網路路由的相同意義的 IP 位址。

當 PC 用戶把網域名稱輸入瀏覽器時，PC 必須首先輸送要求至 DNS 伺服器以獲得相同意義的 IP 位址。DNS 伺服器將在自己的資料庫中檢查網域名稱，當它無法在本地找到這個名稱時，將會去與更高級的 DNS 伺服器溝通。當找到位址時，它會把資訊反饋給 PC，然後與餘下的 IP 封包參考溝通。

5.3.2 指派 DNS 位址

當任何一台伺服器死機或遇到阻止時，多個 DNS 位址提供的選擇將十分有用。一般來說，網路供應商提供 Primary 和 Secondary DNS 位址，還可能提供附加的位址。您的區域網路 PC 將會用下列方式中的一種獲得 DNS 位址：

- **靜態:** 倘若您的網路供應商提供給了您 DNS 伺服器的位址，您就可以透過修改 PC 的 IP 屬性而將它們指派給每台 PC。
- **動態（從 DHCP 位址池開始）:** 您可以設定 DHCP 伺服器和建立將 DNS 位址分配至 PC 的位址池。如何建立 DHCP 位址池，請參考第 27 頁設定 DHCP 伺服器的部分。

您可以指定真實的網路供應商 DNS 伺服器位址（在 PC 上或在 DHCP 域內），或指定網際網路 LAN 埠的位址（例如，192.168.1.1）。當您指定了 LAN 埠的 IP 位址，路由器就會進行 *DNS 傳遞* 了，具體請參考接下來的部分。


注意

如果您在 PC 上或在 DHCP 位址池指定了真實的 DNS 位址，DNS 傳遞不可用。

5.3.3 設定 DNS 傳遞

當您指定設備的 LAN 埠 IP 位址爲 DNS 位址時，網際網路安全路由器將會自動進行“DNS 傳遞”。因爲設備自身並非 DNS 伺服器，它會轉發由 LAN 端 PC 來的網域名稱查詢至 ISP 端的 DNS 伺服器。然後，它把 DNS 伺服器的回應傳遞給 PC。

當進行 DNS 傳遞時，網際網路安全路由器必須保持它所連線的 DNS 伺服器的 IP 位址。它能用下列兩種方式獲得這些位址：

- **從 PPPoE 或 動態 IP 連線獲得:** 如果網際網路安全路由器使用 PPPoE （請參考第 6.3.1 節 爲廣域網（WAN）設定）或動態 IP （參考第 6.4.2 節 爲廣域網（WAN）設定動態 IP ）連線到網路供應商 ISP，Primary 和 Secondary DNS 位址能夠透過 PPPoE 協定獲得。如果 ISP 改變他們的 DNS 位址，那麼本選項可讓您無須再次設定 PC 或網際網路安全路由器
- **設定網際網路安全路由器:** 您可以在 WAN 設定頁面指定 ISP 的 DNS 位址，如圖 6.1. ，圖 6.2. WAN 動態 IP (DHCP 用戶端，或 圖 6.3. WAN 靜態。

請按照下列步驟設定您的 DNS 傳遞：

1. 在 DHCP 設定頁面的 DNS 伺服器 IP 位址中輸入 LAN IP ，如**錯誤! 找不到參照來源。**所示。

2. 爲區域網路 PC 設定使用網際網路安全路由器的 DHCP 伺服器指派的 IP 位址，或將網際網路安全路由器的區域網路 IP 位址作爲 DNS 伺服器位址，然後爲區域網路內的所有 PC 手動輸入。

注意

指派給優先進行 DNS 傳遞的區域網路 PC 的 DNS 位址將持續作用直至 PC 重啓。DNS 傳遞只在 PC 的 DNS 位址爲區域網路的 IP 位址時啓動。

類似的，在開始 DNS 傳遞之後，如果您在 DHCP 域或 PC 上動態地指定 DNS 位址 (而不是區域網路 IP 位址)，那麼這個位址將取代 DNS 傳遞位址而被使用。

5.4 查看 LAN 統計表

您可以在您的網際網路安全路由器上查看 LAN 通信量的統計表。您並非需要經常查看此資料，但是當您協助網路供應商查找網路和網際網路資料傳輸問題時，會發現統計表十分有用。

想要查看 LAN IP 統計表，請點選 LAN 子功能表的統計表，圖 5.5 是 LAN 統計表頁面：

圖 5.5. LAN 統計表頁面

想要顯示更新後的統計表，點選 Refresh 。

6 設定廣域網 WAN

本章將向您說明如何爲與網路供應商連線的網際網路安全路由器 WAN 介面設定 WAN。您可以從中學會爲您的 WAN 設定 IP 位址、DHCP 和 DNS 伺服器。

6.1 廣域網（WAN）連線模式

網際網路安全路由器支援 WAN 的三種模式 – PPPoE、 動態 IP 和靜態 IP。您可從連線模式表中選擇一種您的網路供應商支援的模式，參考圖 6.1。

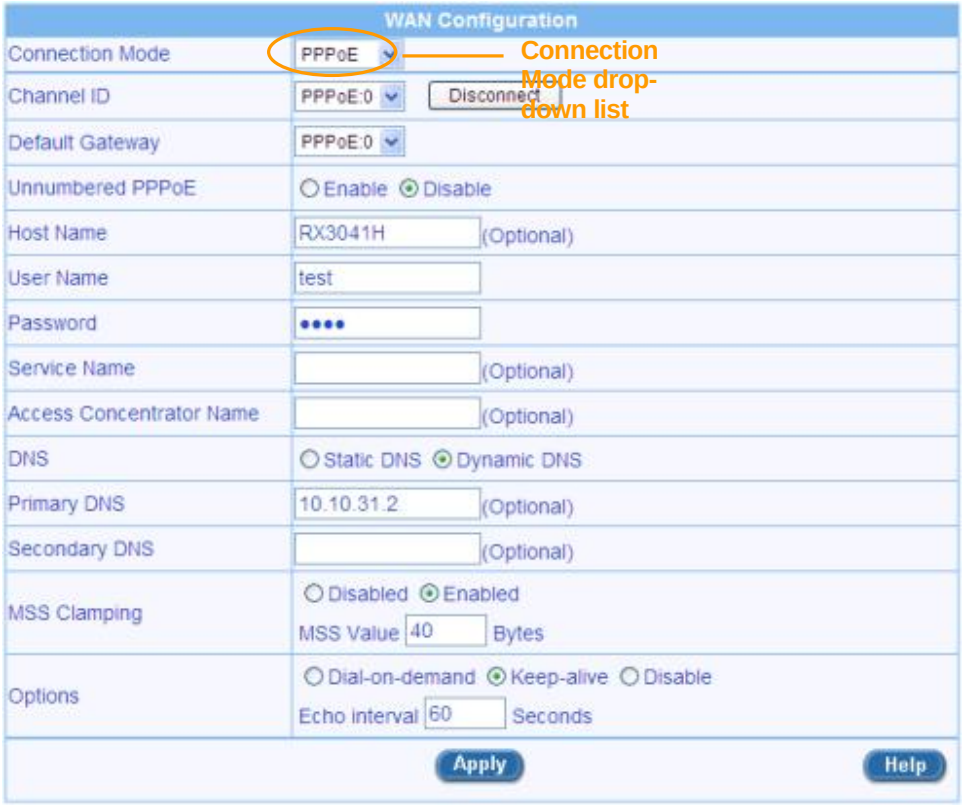


圖 6.1. WAN PPPoE 設定頁面

6.2 PPPoE

6.2.1 廣域網（WAN）PPPoE 設定參數

表 6.1說明了PPPoE 連線模式需要的設定參數。

表 6.1. WAN PPPoE 設定參數

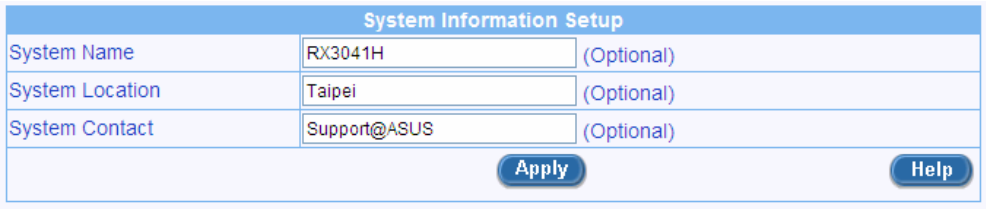
設定	說明
主機名稱	主機名稱可選，但某些 ISP 可能有特定要求。

設定	說明
User Name 和 Password	輸入您登入 ISP 的 Username 和 Password 。（注意：這和您登入設定管理器的資訊不相同。）
Primary/ Secondary DNS	Primary 和/或 Secondary DNS 的 IP 位址可選，並且 PPPoE 將自動偵測您的 ISP 設定的 DNS IP 位址。然而，如果您使用了其他的 DNS 服務器，請輸入空間提供的 IP 位址。
連線選項	本選項的預設值爲“Disable”。若需要，您亦能選擇 Dial-On-Demand 或 Keep-Alive 。
Dial-On-Demand	6.3 輸入當無通信量時您想要的斷開路由器的非活動時間點。非活動時間點的最小值爲 30 秒。如果啓動 RIP 和 SNTP 服務的話，可能會干擾此項功能。請確保系統日期與時間的內部設定（在系統管理 / 日期 / 時間設定的頁面 – 請參考第 11.3 節 設定系統辨識
Keep Alive	如果您想保持您網際網路連線的活動狀態，即便在無通信量時，也請啓動本選項。輸入您想要路由器階段性地輸出某些資料給 ISP 的“回應間隔”值。預設的“回應間隔”值爲 60 秒。

一些特定的系統資訊，像是系統名稱（本裝置的特定名稱）、系統位置（本裝置的所在位置），與在裝置中的個人聯絡資訊都可以在系統辨識設定頁面中進行設定。

請依照以下介紹來變更特定的系統資訊:

3. 藉由點選 System **Management ➔ System Identity** 選單來開啓系統辨識設定頁面。
4. 變更系統名稱、系統位置與聯絡資訊等想要進行的設定。請注意！在此欄位中，您可輸入任何數字字母。
5. 點選 Apply 按鍵來儲存設定值。



）大於非活動時間點。

6.3.1 爲廣域網（WAN）設定 PPPoE

請按照下列步驟來設定 PPPoE：

1. 從如圖 6.1 所示的連線模式列表中選擇 PPPoE。
2. （可選）若 ISP 要求，請輸入空間提供的主機名稱。
3. 如果您使用 PPPoE 連線網際網路，除非您想使用喜愛的 DNS 伺服器，可能您必須在 PPPoE 設定頁面中輸入 User Name 和 Password，如圖 6.1 所示。

4. （可選）如果您希望使用您喜愛的 DNS 伺服器，請輸入 Primary 和 Secondary DNS 伺服器 IP 位址；否則，跳過此步驟。
5. 選擇連線選項，如需要，輸入合適的設定。預設值爲“Disable”。
6. 當您完成設定後，點選 Apply 以保存 PPPoE 設定。您將在設定頁面的下半頁看到 WAN 設定的摘要。注意：若預設閘道位址沒有立即顯示，請點選 WAN 功能表再次打開 WAN 設定頁面。

6.4 動態 IP

6.4.1 廣域網（WAN）動態 IP 設定參數

表 6.2 說明了動態IP連線模式的可選設定參數。

表 6.2. WAN 動態 IP 設定參數

選項	說明
主機名稱	主機名稱可選，但某些 ISP 可能有特定要求。
Primary/ Secondary DNS	Primary 和/或 Secondary DNS 的 IP 位址可選，並且 DHCP 將自動偵測您的 ISP 設定的 DNS IP 位址。然而，如果您使用了其他的 DNS 伺服器，請輸入空間提供的 IP 位址。
MAC Cloning	預設的使用 WAN 介面的 MAC 位址。然而，如果您事先已經在 ISP 註冊了 MAC 位址，您需要在這裏輸入這個 MAC 位址。

6.4.2 爲廣域網（WAN）設定動態 IP

請按照下列步驟來設定動態 IP：

1. 從圖 6.2 所示的連線模式列表中選擇動態。
2. （可選）若 ISP 要求，請輸入空間提供的主機名稱。
3. （可選）如果您希望使用您喜愛的 DNS 伺服器，請輸入 Primary 和 Secondary DNS 伺服器 IP 位址；否則，跳過此步驟。
4. 如果您已經事先在 ISP 註冊了特別的 MAC 位址來接入網際網路，，請確認您已經把 MAC cloning 打勾。
5. 當您完成設定後，點選 Apply 以保存動態 IP 設定。您將在設定頁面的下半頁看到 WAN 設定的摘要。注意：若預設閘道位址沒有立即顯示，請點選 WAN 功能表再次打開 WAN 設定頁面。

圖 6.2. WAN 動態 IP (DHCP 用戶端) 設定頁面

6.5 靜態 IP

6.5.1 廣域網（WAN）靜態 IP 設定參數

表 6.3說明了靜態IP連線模式的可選設定參數。

表 6.3. WAN 靜態 IP 設定參數

設定	說明
IP 位址	WAN 的 IP 位址由您的 ISP 提供。
子網路遮罩	WAN 的子網路遮罩由您的 ISP 提供。一般來說，設定爲 255.255.255.0。
閘道位址	閘道 IP 位址由您的 ISP 提供。它必須與路由器處於相同的子網路中。
Primary/ Secondary DNS	您必須至少要輸入 Primary DNS 伺服器的 IP 位址。Secondary DNS 可選。

6.5.2 爲廣域網（WAN）設定靜態 IP

圖 6.3. WAN 靜態 IP 設定頁面

請按照下列步驟來設定靜態 IP：

1. 從圖 6.3 所示的連線模式列表中選擇靜態。
2. 在 IP 位址欄中輸入 WAN IP 位址。位址資訊應由您的 ISP 提供。
3. 輸入 WAN 的子網路遮罩。遮罩由您的 ISP 提供。一般來說，設定爲 255.255.255.0。
4. 輸入您的 ISP 提供的閘道位址。
5. 輸入 Primary DNS 伺服器的 IP 位址。位址資訊應由您的 ISP 提供。Secondary DNS 伺服器可選。
6. 當您完成設定後，點選 Apply 以保存動態 IP 設定。您將在設定頁面的下半頁看到 WAN 設定的摘要。

6.6 查看 WAN 統計表

您可以在您的網際網路安全路由器上查看 WAN 通信量的統計表。您並非需要經常查看此資料，但是當您協助網路供應商查找網路和網際網路資料傳輸問題時，會發現統計表十分有用。

想要查看 WAN IP 統計表，請點選 WAN 子功能表的統計表，圖 6.4 是 WAN 統計表頁面：

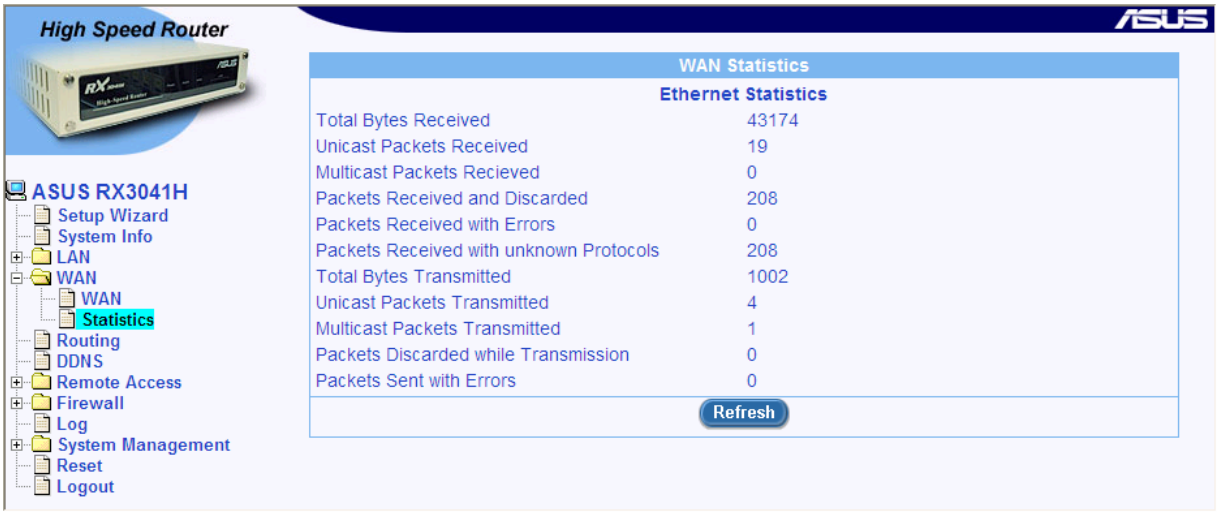


圖 6.4. WAN 統計表頁面

想要顯示更新後的統計表，點選 Refresh 。

7 設定路徑

您可利用設定管理器來爲您的網際網路和網路資料通訊定義特別的路徑。本章將向您說明基礎的路由概念以及指導您建立路由路徑。

注意：大多數的用戶並不需要定義路徑。

7.1 IP 路徑總覽

路由器遇到的核心挑戰是：當它接收到有特定傳輸目標的資料時，何者爲它應該把資料傳遞過去的下一個設備呢？當您定義了 IP 路徑，您就提供了網際網路安全路由器做出決定的規則。

7.1.1 我需要定義 IP 路徑嗎?

大多數用戶並不需要定義 IP 路徑。在典型的小型家庭或辦公室局域網內，現有的路徑爲您區域網路和網際網路安全路由器的電腦設立了預設的閘道，也將爲您所有的網際網路通信量提供最合適的路徑。

- 在區域網路電腦內，預設的閘道指導著所有的網際網路通信量流向路由器的區域網路埠。如果當您修改區域網路電腦的 TCP/IP 屬性時您已經給它們指派了閘道，或者如果無論它們何時接入網際網路，您都已經設定它們動態地從伺服器接收資訊，那麼區域網路電腦就知道它們的預設閘道了。（每個過程都已在“快速安裝指南”的第二部分中說明，請參考。）
- 對於網際網路安全路由器自身，預設的閘道已被定義來指導所有要出去的網際網路通信量流向網路供應商的路由器。無論設備何時協商與網際網路連線，預設的閘道由網路供應商自動指派。（增加預設路徑的過程在第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**中詳細說明。）

如果您的家裏需要兩個或更多的網路或子網路，如果您與兩個或更多的供應商連線，或者如果您與遠端企業區域網路相連線，那麼您可能需要定義路徑。

7.2 使用 RIP（Routing Information Protocol）的動態路由

RIP（路由資訊協定）讓路由器之間產生路由資訊交換。因此，路徑會在不需要人類干預的情況下自動更新。我們推薦您在系統服務設定頁面啓動 RIP，如圖 11.1 所示。

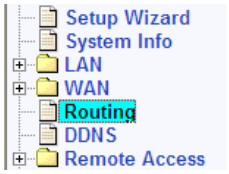
7.2.1 開啓/關閉 RIP

請按照下列步驟來開啓或關閉 RIP：

1. 在系統服務頁面（如圖 11.1 所示），根據您想開啓或關閉 RIP，點選“Enable” 或 “Disable” 按鈕。
2. 點選 Apply 來開啓或關閉 RIP。

7.2.2 設定 RIP

請依照以下介紹來設定 RIP:



3. 請藉由點選 **Routing** 選單來開啓路由設定頁面。
4. 在系統服務設定頁面中 (如圖 11.1 所示)，依照您要開啓或關閉 RIP 服務點選 “Enable” 或 “Disable” 按鍵。若您已進行設定，請略過此一步驟。

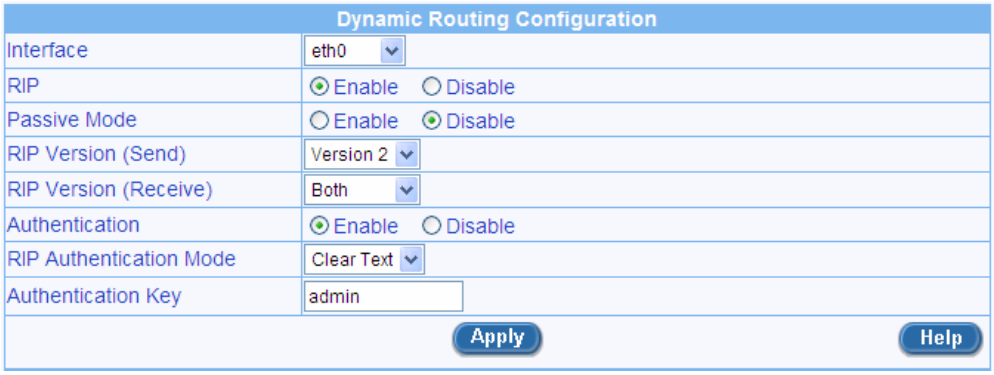


圖 7.1. IP 路由列表頁面 RIP 設定

5. 從下拉選單選擇介面，透過這項設定路由資料便會被變更。
6. 藉由點選 “Enable” 或 “Disable” 按鍵來開啓或關閉關於 RIP 設定的特定選項。
7. 藉由點選“Enable” or “Disable”按鍵來開啓或關閉 RIP passive 模式。
8. 選擇 RIP 版本來自下拉式列表中選擇傳送與接收資訊。
9. 藉由點選“Enable” or “Disable” 按鍵來開啓或關閉認證。若認證功能設定爲開啓，則您必需開啓認證模式並輸入認證金鑰。
10. 若您想設定其他項目以支援路由資訊變更，請重複步驟 5 至 9 。
11. 點選 

鍵來儲存 RIP 設定。

7.3 靜態路由

7.3.1 靜態路徑設定參數

下表定義了靜態路徑設定可供選擇的參數。

表 7.1. 靜態路由設定參數

選項	說明
目的地 IP 位址	指派目的地電腦或者整個目標網路的 IP 位址。它亦能全被指派爲零以顯示此路徑應被用來達到其他路徑無定義的目的地（這就是建立預設閘道的路徑）。請注意，IP 目的地必須是網路 ID。預設路徑使用的目的地 IP 爲 0.0.0.0。請參考附錄 A 關於網路 ID 的解釋。
目的地網路遮罩	指出哪部分目的地位址涉及網路，哪部分涉及網路中的電腦。請參考附錄 A 關於網路遮罩的解釋。網路遮罩預設的路徑爲 0.0.0.0.

選項	說明
閘道 IP 位址	閘道 IP 位址

7.3.2 增加靜態路徑

請按照下列步驟來增加靜態路徑至路徑表：

1. 在靜態路徑設定頁面內（如**錯誤! 找不到參照來源。**所示），輸入相應選項的靜態路由資訊，例如目的地 IP 位址、目的地網路遮罩以及閘道 IP 位址。

   請參考表 7.1. 的詳細說明。

   想爲您的區域網路建立定義預設閘道的路徑，在目的地 IP 位址和目的地網路遮罩選項中均輸入 0.0.0.0 。

2. 點選 Add 增加新的路徑。

7.3.3 刪除靜態路徑

請按照下列步驟來刪除路徑表中的靜態路徑：

1. 在靜態路徑設定頁面（如**錯誤! 找不到參照來源。**所示）的服務下拉表中選擇路徑，或者點選 靜態路徑表中要刪除的路徑圖示。

2. 點選 Delete 以刪除選擇的路徑。

小心

除非您明確了動作的目的，否則不要移除預設閘道的路徑。移除預設的路徑將導致斷開互聯網。

7.3.4 查看靜態路由表

所有開啓 IP 功能的電腦和路由器都保存了用戶通常接入的 IP 位址表。對於每個*目的地 IP 位址*，表中列出了資料採取的第一次跳躍的 IP 位址。此表又被稱爲設備的*路徑表*。

想要查看路由器路徑表，請點選路徑功能表。靜態路徑表在靜態路徑頁面的下半頁，如**錯誤! 找不到參照來源。**所示：

靜態路徑表中的一行顯示了每個現有的路徑，路徑中包含了目的地網路的 IP 位址、目的地網路的子網路遮罩以及閘道 IP 位址。此表只顯示用戶增加的路徑。

8 設定 DDNS

動態 DNS 是一種允許電腦使用相同網域名稱的服務。此項服務甚至在 IP 位址時刻改變時也能提供。（在重啓或當 ISP 的 DHCP 伺服器重啓 IP 租用）。無論 WAN 的 IP 位址是否改變，路由器都連線至動態 DNS 伺服器。它支援建立網頁服務，例如使用網域名稱替代 IP 位址的網頁伺服器、FTP 伺服器。動態 DNS 支援 DDNS 用戶端的下列規格：

- 當外部介面出現時，刷新 DNS 記錄（增加的）
- 促使 DNS 刷新

動態 DNS 支援兩種模式，即 RFC-2136 DDNS 用戶端 和 HTTP DDNS 用戶端。

RFC-2136 DDNS 用戶端

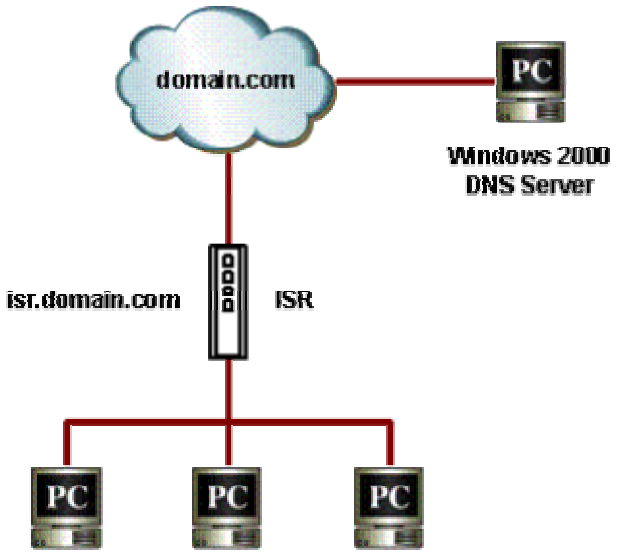


圖 8.1. RFC-2136 DDNS 網路撥號

任何外部介面狀況的改變都會給 DNS 伺服器送出 DDNS 的更新資訊。當連線 Primary DNS 伺服器的舉動失敗時，路由器會更新 Secondary DNS 伺服器。當管理員迫使 DNS 更新時，更新資訊被傳送到所有活動的外部伺服器。

HTTP 動態 DNS 用戶端

HTTP DDNS 用戶端利用流行的 DDNS 服務提供商提供的機制來動態地更新 DNS 記錄。既然這樣，那麼服務提供商就可以更新 DNS 中的 DNS 記錄了。路由器運用 HTTP 來促進此種更新。

路由器支援下列服務供應商的 HTTP DDNS 更新：

- www.dyndns.org
- www.zoneedit.com
- www.dns-tokyo.jp

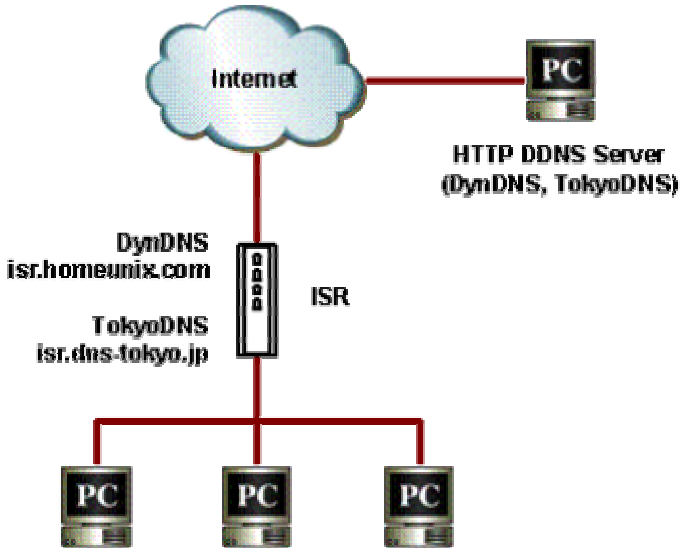


圖 8.2. HTTP DDNS 網路撥號

無論已設定的 DDNS 介面的 IP 位址何時更改，DDNS 更新都被送到指派的 DDNS 服務提供商。網際網路安全路由器應該設定好從 DDNS 服務提供商那裏獲得的 DDNS Username 和 Password。

8.1 DDNS 設定參數

表 8.1 說明了 DDNS 服務的設定參數：

表 8.1. DDNS 設定參數

選項	說明
DDNS 狀態	
Enable	點選此按鈕來開啓DDNS服務
Disable	點選此按鈕來關閉DDNS服務
DDNS 類型 – 選擇DDNS 服務類型: HTTP 或 RFC-2136 DDNS	
HTTP DDNS	如需要HTTP DDNS，點選此按鈕。
RFC-2136 DDNS	如需要RFC-2136 DDNS ，點選此按鈕。
DNS Zone Name 在本選項中輸入網路服務供應商提供的已註冊的網域名稱。（注意：路由器的主機名稱必須在系統資訊設立頁面正確地設定好。）例如，如果路由器主機名稱爲“host1”，DNS Zone 名稱爲“yourdomain.com”，網域名稱的全稱（FQDN）爲 “host1.yourdomain.com”。	
RFC-2136 DDNS 特殊設定	
Primary/Secondary DNS 伺服器 [僅在RFC-2136 DDNS] 在本選項中輸入Primary 和 Secondary DNS 伺服器的IP位址。這個位址從WAN設定頁面得到。除非您想改變WAN的設定，否則請保持不變。	

選項	說明
HTTP DDNS 特殊設定	
DDNS 服務 [僅對 HTTP DDNS]	
dyndns	請訪問 http://www.dyndns.org 以獲得更多資訊。
zoneedit	請訪問 http://www.zoneedit.com 以獲得更多資訊。
dyn-tokyo	請訪問 http://www.dns-tokyo.jp 以獲得更多資訊。
DDNS Username [僅對HTTP DDNS] 在本選項中輸入DDNS服務提供商提供的Username。	
DDNS Password [僅對HTTP DDNS] 在本選項中輸入DDNS服務提供商提供的Password。	

8.2 設定 RFC-2136 DDNS 用戶端

圖 8.3. RFC-2136 DDNS 設定頁面

請按照下列步驟來設定 RFC-2136 DDNS：

1. 首先您需要要求系統管理員在 DNS 伺服器上開啓 DNS 動態更新功能。如果您正在運行 Windows 2000/XP/2003 DNS 伺服器，請參考 Microsoft 基礎知識文章 "*Q317590: Configure DNS Dynamic Update in Windows 2000*"。
2. 請確認您擁有爲路由器設定的主機名稱；若沒有，請至**系統資訊設定**頁面（系統管理➔系統認證）進行設定。
3. 打開 DDNS 設定頁面（參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**）。
4. 在 DDNS 設定頁面，選擇"Enable" 的 DDNS 狀態和 "RFC-2136 DDNS" 的 DDNS 類型。RFC-2136 DDNS 設定頁面如圖 8.3 所示。
5. 在 DNS Zone Name 選項欄輸入網域名稱。
6. 無須改變 Primary 和 Secondary DNS 伺服器的 IP 位址。因爲這個位址從 WAN 設定頁面得到。除非您想改變 WAN 的設定，否則請保留不變。
7. 點選 Apply 按鈕向 Primary DNS 和 Secondary DNS 選項指派的 DNS 伺服器發送更新 DNS 的要求。注意，無論 WAN 埠狀況是否改變，更新 DNS 的要求同樣也會自動送給 DNS 伺服器 。

8.3 設定 HTTP DDNS 用戶端

圖 8.4. HTTP DDNS 設定頁面

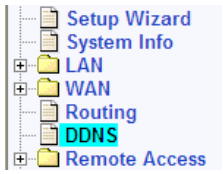
請按照下列步驟來設定 HTTP DDNS：

1. 首先，您應該已經向 DDNS 服務供應商註冊了網域名稱。如果您還沒有註冊，請訪問 www.dns-tokyo.jp 或 www.dyndns.org 以獲得更多資訊。
2. 請確認您擁有爲路由器設定的主機名稱；若沒有，請至**系統資訊設定**頁面（系統管理➔系統認證）進行設定。
3. 打開 DDNS 設定頁面（參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**）。
4. 在 DDNS 設定頁面，選擇“Enable” 的 DDNS 狀態和 “HTTP DDNS” 的 DDNS 類型。HTTP DDNS 設定頁面如圖 8.4 所示。
5. 在 DNS Zone Name 選項欄輸入網域名稱。
6. 從 DDNS 服務下拉表中選擇 DDNS 服務。
7. 輸入 DDNS 服務供應商提供的 Username 和 Password。
8. 點選 Apply 按鈕向 DDNS 服務供應商發送更新 DNS 的要求。注意，無論 WAN 埠狀況是否改變，更新 DNS 的要求同樣也會自動送給 DDNS 服務供應商。

8.4 設定近端主機列表

此爲供路由器標示主機名稱與其 IP 位址的近端主機列表。本列表可作爲您區域網路中的伺服器部署之用。舉例來說，您可以爲您的伺服器在這組列表中建立一組主機登錄，讓區域網路中的主機可以藉由使用主機名稱，像是 telnet myServer.myCompany.com.來存取伺服器的資料。

8.4.1.1 新增一組主機登錄



請依照以下介紹來新增一組主機登錄:

9. 藉由點選 **DDNS** 選單來開啓 DDNS 設定頁面。
10. 自下拉列表中選擇 “**Add New**” 。
11. 在對應的欄位輸入主機名稱與對應的 IP 位址。圖 8.5 顯示使用登錄來在主機列表中新增一組新主機來標示主機名稱，myServer.myCompany.com 與一組 IP 位址 192.168.1.20 。

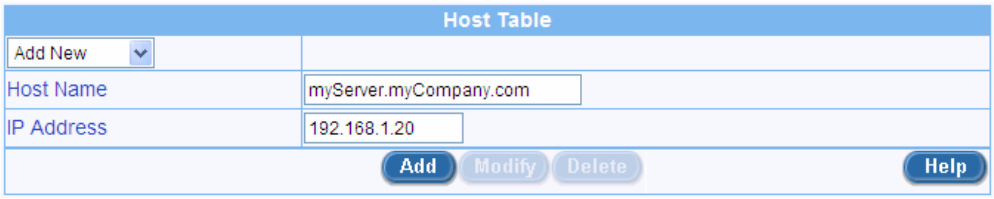


圖 8.5. 主機列表設定

12. 點選 Add 鍵來建立一組新的主機登錄。新的主機登錄其後會顯示在 DDNS 設定頁面下方的主機列表中。

圖 8.6. 主機列表

8.4.1.2 更改主機列表中的登錄

請依照下列介紹來更正主機列表中的登錄:

13. 藉由點選 **DDNS** 選單來開啓 DDNS 設定頁面。
14. 點選主機列表登錄中的 圖示來從下拉式主機列表中更正主機列表或選擇主機列表登錄。
15. 接下來您可以在主機名稱與 IP 位址進行所想要加以變更的設定。
16. 點選 Modify 鍵以儲存變更。主機列表中新的設定值會顯示於 DDNS 設定頁面下方的主機列表中。

8.4.1.3 刪除主機列表登錄

如欲刪除主機列表登錄，請依照下列介紹的指示點選 圖示來進行刪除:

17. 藉由點選 **DDNS** 選單來開啓 DDNS 設定頁面。
18. C 在主機列表中點選 圖示以便從下拉式主機列表中選擇要加以刪除的主機登錄。
19. 點選 Delete 鍵來刪除登錄。請注意！被刪除的主機登錄將會自 DDNS 設定頁面下方的主機列表中移除。

8.4.1.4 檢視主機列表

如欲檢視既有的主機列表，您只要藉由點選 **DDNS** 選單來開啓 DDNS 設定頁面即可。

9 設定防火牆/NAT

網際網路安全路由器提供內建的防火牆/NAT 功能，在提供網際網路訪問共用的同時，保護您的系統免受拒絕服務（DoS）的攻擊，以及免於對區域網路的其他類型的惡意訪問。您亦能指定如何監視攻擊企圖，以及誰應該被自動通報。

本章說明了如何建立/修改/刪除訪問控制列表 ACL（Access Control List）規則以控制流經網路的資料。R 您將使用防火牆設定頁面來：

- 建立、修改、刪除以及檢查入站/出站的 ACL 規則。
- 建立、修改及刪除預先定義的服務、IP 域、NAT 域、應用程式過濾以及入站/出站 ACL 設定的時間範圍。
- 檢查防火牆統計表。

注意: 當您定義 ACL 規則時，您指導路由器來檢查封包接收到的每個資料，判斷它是否符合規則規定標準的要求。*標準包括它所支援的網路或網際網路協定、它傳遞的方向（例如，從區域網路到網際網路，反之亦然）、來源電腦的 IP 位址、目的地 IP 位址，以及封包資料的其他特性。*

如果封包符合規則標準的要求，那麼根據規則中規定的的動作，封包會被接收（促使它流向目的地），或拒絕（摒棄）。

9.1 防火牆概述

9.1.1 靜態封包檢查

靜態封包檢查網際網路安全路由器中的引擎保存的一個狀態工作臺，這個工作臺被用來記錄所有流經防火牆的封包的連線狀態。如果屬於已建立的連線的封包的狀態與靜態封包檢查引擎維護的狀態相吻合，防火牆將開"口"允許封包透過。否則，封包會被拒絕透過。這個"口"在連線過程終止時將被關閉。靜態封包檢查不需要任何設定；當防火牆啓動時它自動開啓。請參看第**錯誤! 找不到參照來源。**節**錯誤! 找不到參照來源。**以開啓或關閉路由器防火牆服務。

9.1.2 拒絕服務（DoS，Denial of Service）保護

拒絕服務的保護和狀態封包檢查共同承擔您網路的第一道防線。兩者都不需要進行任何設定，當路由器防火牆啓動時它自動開啓。防火牆預設值在出廠時就已設置好。請參看第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**以開啓或關閉路由器防火牆服務。

9.1.3 防火牆及訪問控制列表 （ACL，Access Control List）

9.1.3.1 ACL 優先順序規則

所有的 ACL 規則都有指派的規則 ID – 規則 ID 越小，優先權越大。防火牆從封包中抽取重要資訊，然後透過檢視重要資訊與 ACL 規則表是否吻合，再摒棄或傳送封包，防火牆透過此舉監視著流通的資訊。請注意，ACL 規則檢查從最小的規則 ID 開始，直到出現了兩者匹配的資訊或所有的 ACL 規則都已檢查完畢。如果二者之間並無匹配，那麼封包被摒棄；另外，基於匹配的 ACL 規則定義的舉動，封包會被摒棄，或被傳送。

9.1.3.2 追蹤連線狀態

防火牆的靜態檢查引擎持續追蹤網路連線的狀態進展。透過在狀態表中存儲所有的連線資訊，網際網路安全路由器能快速判斷流經防火牆的封包是否屬於已建立的連線形式。若是，封包就直接流經防火牆而無須透過 ACL 規則評判。

例如，ACL 規則允許出站的從 192.168.1.1 到 192.168.2.1 的 ICMP 封包。當 192.168.1.1 送出 ICMP 請求至 192.168.2.1 時，192.168.2.1 將送出 ICMP 回應給 192.168.1.1。在網際網路安全路由器中，您無須建立另外的 ACL 規則，因爲靜態封包檢查引擎將記住連線狀況，並允許 ICMP 回應透過防火牆。

9.1.4 預設的 ACL 規則

網際網路安全路由器支援三種預設的訪問規則：

- 入站訪問規則：目的爲控制入站局域網電腦的訪問。
- 出站訪問規則：目的爲控制出站區域網路主機至外部網路的訪問。
- 自身訪問規則：目的爲控制對路由器自身的訪問。

預設的入站訪問規則

無已設定的預設入站訪問規則。也就是說，所有從外部主機到內部主機的流通均被拒絕。

預設的出站訪問規則

預設的出站訪問規則允許所有來自區域網路的資訊流通到外部使用 NAT 的網路。

WARNING

您無需把預設的 ACL 規則從 ACL 規則表中移除！建立優先權高於預設 ACL 規則的更佳。

9.2 NAT 總覽

網路位址轉換允許使用單一設備，例如網際網路安全路由器，扮演網際網路（公共網路）與本地網路之間的代理人。這意味著 NAT 的 IP 位址對外能代表整個電腦群體。NAT 是一種在大型網路中保存已註冊的 IP 位址和使 IP 位址管理簡單化的機制。因爲 IP 位址的轉換，NAT 還把您真正的 IP 位址從別人眼前隱藏起來，並提供某種程度的本地網路保護。

NAT 模式支援靜態 NAT、動態 NAT、NAPT、反向靜態 NAT 以及反向 NAPT。

9.2.1 靜態（一對一）NAT

靜態 NAT 對應了從內部主機位址到有效全球網際網路位址（一對一）。而每個封包的 IP 位址都會被直接轉換成爲一個有效的全球網際網路位址。圖 9.1 闡明了四個私人 IP 位址與四個有效全球 IP 位址之間的映射關係。請注意，這種映射是靜態的，例如除非管理員手動更改，映射並不隨著時間而改變。這意味著主機將對其所有的出站資訊一直使用相同的有效全球 IP 位址。

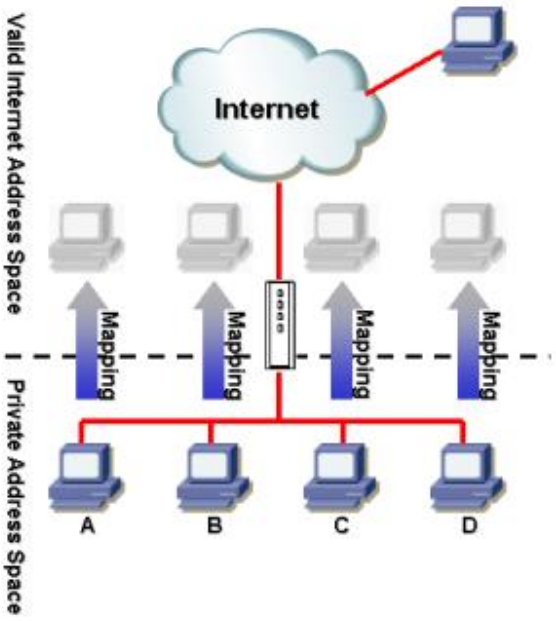


圖 9.1 靜態 NAT – 對應從四個私人 IP 位址到四個有效全球 IP 位址

9.2.2 動態 NAT

動態 NAT 動態地對應從內部主機到有效全球網際網路位址（m 到 n）。映射常常包含一些內部 IP 位址池（m）和有效全球網際網路 IP 位址（n），且 m 常常大於 n。每個內部 IP 位址都在"先來先服務"的基礎上與一個外部 IP 位址相連。圖 9.2 顯示，PC B、C 和 D 都分別與一個有效全球 IP 位址連線，而 PC A 並不與任何有效全球 IP 位址連線。如果 PC A 想要接入網際網路，它必須等到一個有效全球 IP 位址可用時才行。例如，在圖 9.3 中，PC B 必須先從網際網路斷開，然後 PC A 才能接入網際網路。

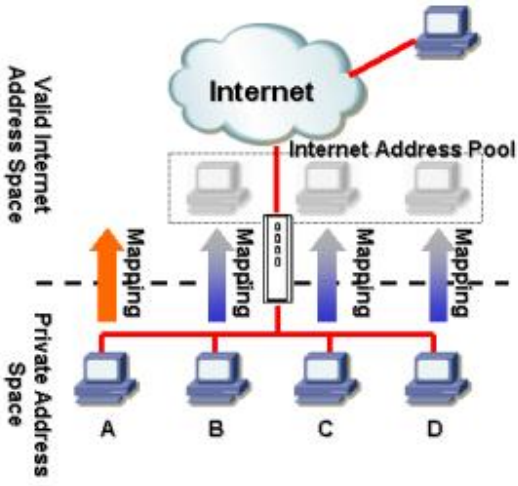


圖 9.2 動態 NAT – 從四個私人 IP 位址到三個有效 IP 位址

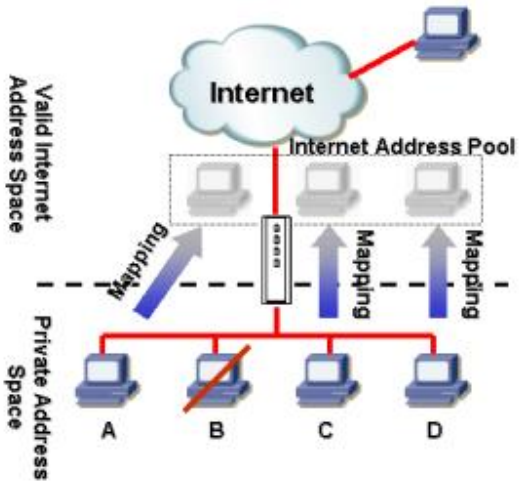


圖 9.3 動態 NAT – PC-A 能在 PC-B 斷開後得到 NAT 連線

9.2.3 NAPT（Network Address and Port Translation，網路位址和埠轉換）或 PAT（Port Address Translation，埠位址轉換）

這個特性對應了許多從內部主機到一個有效全球 IP 位址。映射包含被用來轉換的一些埠。每個封包都隨著有效全球網際網路位址轉換，而埠數目則隨著一個未用的網路埠轉換。圖 9.4 顯示，所有的本地網路主機都透過網路埠位址池對應外部有效的 IP 位址和不同的埠號來達到連接網際網路的目的。

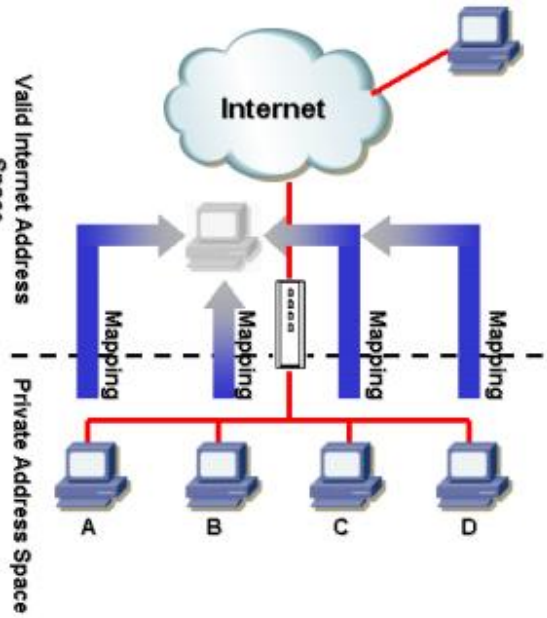


圖 9.4 NAPT – 對應從任何內部電腦到單一全球 IP 位址

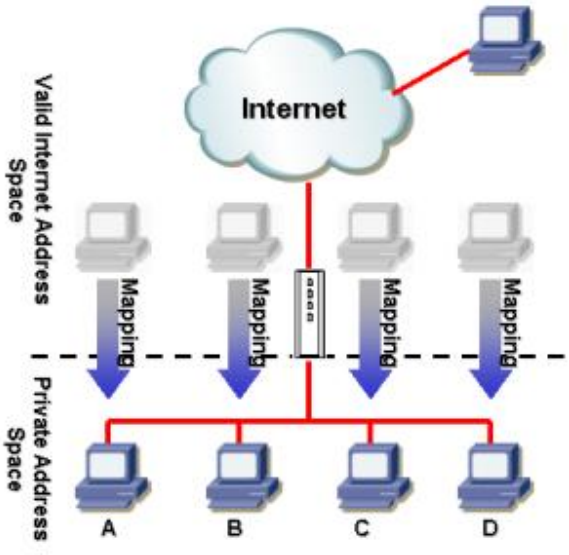


圖 9.5 反向 NAT – 對應一個全球 IP 位址到一台內部電腦

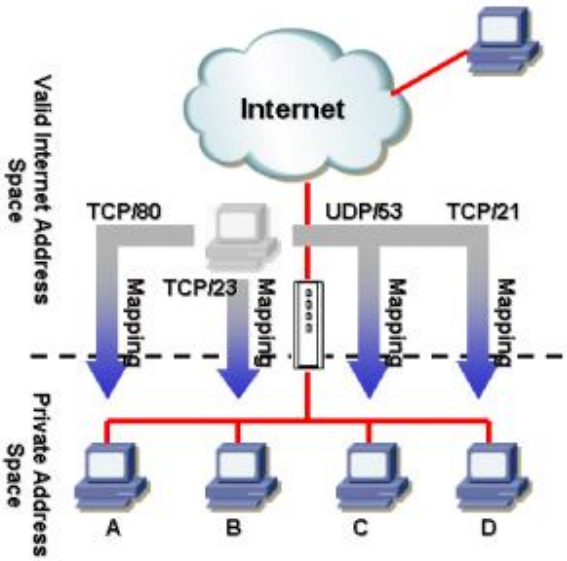


圖 9.6 反向 NAPT – 以協定、埠號或 IP 位址爲基礎轉送封包到內部主機

9.2.4 反向靜態 NAT

反向靜態 NAT 爲入站資訊對應了從有效全球 IP 位址到內部主機位址映射。所有流向有效全球 IP 位址的封包都傳遞到網際網路位址上。這在當內部主機提供應用服務時十分有用。圖 9.5 顯示了從四個有效全球 IP 位址到四個內部網路主機的映射，而且每個都可用作爲入站資訊的主機服務，例如 FTP 伺服器。

9.2.5 反向 NAPT / 虛擬伺服器

反向 NAPT 又被稱爲入站映射、埠對應或虛擬伺服器。任何傳送到路由器的封包都能被傳遞到基於協定、埠號和/或在 ACL 規則內指派 IP 位址的內部主機上。這在當不同的內部主機提供多種服務時十分有用。圖 9.6 顯示了網頁伺服器（TCP/80）連在 PC A 上，遠端網路服務器（TCP/23）在 PC B 上，DNS 伺服器（UDP/53）在 PC C 上，FTP 伺服器（TCP/21）在 PC D 上。這意味著這四台伺服器入站的資訊將被直接傳導至各自的服務主機。

9.3 ACL 規則參數設定

表 9.2 敘述ACL規則中可以進行的參數設定項。

表 9.1. ACL 規則參數設定

欄位	敘述
ID	
Add New	點選此項目以新增一組 ACL 規則
Rule Number	從下拉式列表中選擇一項規則，並修改其屬性
Action	
Allow	選擇此按鍵以設定像是 **allow** 規則的設定 當符合上述設定之規則的封包將被允許通過
Deny	選擇此按鍵以設定像是 **deny** 規則的設定 當符合上述設定之規則的封包將被阻擋無法通過
Mave to 本選項可讓您設定本規則的優先權。RX3041H 防火牆是以此一規則的優先權來決定是否讓封包通過。您可藉由在規則列表中指定一特定數字來決定規則的優先權。	
1 (First)	本數字代表最高的優先權
Other numbers	選擇要指定給其他規則的優先順序號碼
Source IP 本選項可以讓您設定套用該規則的 **來源網路** 。使用下拉式選單來選擇下列選項：	
Any	本選項可以讓您套用本規則在來源網路中的所有電腦，像是那些網際網路上符合入埠ACL規則者或是區域網路中符合出埠ACL規則者。
IP Address	本選項可讓您爲套用本規則者指定一組 IP 位址
IP Address	指定適當的網路位址
Subnet	本項目可讓您涵蓋所有在同一IP子網路內的電腦。當本項目被選定，則以下欄位便可以加以輸入:

欄位	敘述
Address	輸入適當的 IP 位址
Mask	輸入對應的子網路遮罩
Range	本項目可讓您涵蓋所有套用此規則的 IP 位址。當本項目被選定，則以下欄位便可以加以輸入:
Begin	輸入起始的 IP 位址範圍
End	輸入中止的 IP 位址範圍
IP Pool	本項目可以讓您以此一規則與預設的 IP 位址池產生關連。您可從 IP位址池下拉式選單列表中選取 IP 位址池。
Destination IP 本項目可讓您選擇套用此規則的 **目的地網路**。 請使用下拉式選單來選擇以下的選項:	
Any	本項目可讓您將此規則套用到處在目的地網路下的所有電腦，像是那些區域網路中符合 入埠 ACL 規則的電腦，與網際網路中符合出埠 ACL 規則的電腦。
IP Address, Subnet, Range and IP Pool	請選擇這些選項中的任一選項並輸入如前述 **Source IP** 一節中所提到的相關細節敘述。
Source Port 本項目可讓您設定欲套用此一規則的來源連接埠。請使用下拉式選單來選擇以下的選項:	
Any	若您想以任一來源埠號來將此規則套用到應用程式上，則請選擇此項目
Single	本項目可讓您用特定的來源埠號來套用此規則
Port Number	輸入來源埠埠號
Range	若您要將本規則用此連接埠範圍套用到應用程式中，請選擇本項目。當本項目被選擇，則以下的欄位將會變成可以進行輸入的。
Begin	輸入起始連接埠號的範圍
End	輸入中止連接埠號的範圍
目的地連接埠 本選項可讓您設定欲套用本規則的目的地連接埠。請使用下拉式來選擇以下任一選項：	
Any	若您想要將此一規則利用任一目的地連接埠埠號來套用到所有的應用程式，則請選擇本項。
Single, Range	選擇任一項並在 **Source Port** 欄位輸入細節敘述
Service	請在本項目中選擇任何的預設服務(自下拉選單中選取)而非自目的地連接埠選取。以下則爲服務之範例: BATTLE-NET, PC-ANYWHERE, FINGER, DIABLO-II, L2TP, H323GK, CUSEEME, MSN-ZONE, ILS, ICQ_2002, ICQ_2000, MSN, AOL, RPC, RTSP7070, RTSP554, QUAKE, N2P, PPTP, MSG2, MSG1, IRC, IKE, H323, IMAP4, HTTPS, DNS, SNMP, NNTP, POP3, SMTP, HTTP, FTP, TELNET.

欄位	敘述
	Note: 本服務是通訊協定與連接埠號的結合。這些項目只有當您在 “Firewall Service” 設定頁面加以新增後才會出現。
Protocol 本項目可讓您從下拉式選單中選擇通訊協定類型。這邊可供選擇的設定有 All, TCP, UDP, ICMP, AH 與 ESP。請注意！若您選擇 “service” 作爲目的連接埠，則本選項將無法進行設定。	
NAT 本項目可以讓您選擇 NAT 傳輸的類型。	
None	若您不想要在此 ACL 規則中使用 NAT，則請選擇本項目。
IP Address	**作爲入埠 ACL 規則:** 若您想要外來傳輸可被偵測，請選擇本項以指定電腦的 IP 位址 (通常是您區域網路中的伺服器) 。請注意！本項目又被稱作反向 NAPT 或是虛擬伺服器。 **作爲出埠 ACL 規則:** 若您想使用出埠傳輸，則請選擇本項目。請注意！本項目又被稱作 NAPT 或是 Overload。
NAT Pool	選擇本項目來與預設的 NAT 位址池建立關連。**作爲入埠 ACL 規則，** 只有反向靜態 NAT 與反向 NAPT 位址池可被使用。**作爲出埠 ACL 規則，** 只有靜態、動態與 Overload的 NAT 位址池可被使用。
Interface (Outbound ACL only)	**本項目僅可用於出埠 ACL 規則。** 選擇本選項以使用廣域網路WAN外部IP位址做爲出埠傳輸之用。請注意！廣域網路IP必需被設定爲優先方可設定本選項。本項目共有三個選項可供選擇：eth0, pppoe0 and pppoe1。 若您的廣域網路WAN使用固定或動態IP 則請選擇 eth0 ;若您使用PPPoE方式連線，則請選擇pppoe0，而若是使用 PPPoE1介面，則請選擇 pppoe1。
Time Ranges 選擇預設的時間範圍，在此一範圍中規則是生效的。選擇 “Always” 可讓規則一直生效無時間限制	
Application Filtering 本項目可讓您從下拉選單中選擇預設的 FTP, HTTP, RPC 與/或 SMTP 應用程式過濾功能	
Log 點選 “Enable” 或 “Disable” 按鍵以開啓或關閉登入此一 ACL 規則者	

9.4 設定入站 ACL 規則

在入站ACL設定頁面建立ACL規則，如圖 9.7所示，您可控制對您區域網路電腦的訪問（允許或拒絕）。

本設定頁面的選項有：

- 增加規則，並設定參數
- 修改現有的規則
- 刪除現有的規則
- 檢查設定的 ACL 規則

圖 9.7. 入站 ACL 設定頁面

9.4.1 入站 ACL 規則設定參數

表 9.2 說明了防火牆入站ACL規則可供選擇的設定參數。

表 9.2. 入站 ACL 規則設定參數

選項	說明
ID	
Add New	點選本選項以增加新的"基本"防火牆規則。
Rule Number	從列表中選擇規則，修改屬性。
Action	
Allow	按此按鈕以設定**允許**的規則。 當限制爲防火牆時，此規則將允許匹配的封包透過。
Deny	按此按鈕以設定**拒絕**的規則。 當限制爲防火牆時，此規則將**不**允許匹配的封包透過。
Move to 本專案允許您設立規則的優先順序。路由器防火牆在優先順序規則基礎上作用于封包。請以它在規則表的位置的指定序號爲基礎設立優先順序：	
1 (First)	此序號表示最高優先權：
Other numbers	選擇其他的數位以說明您想要指定的優先順序。
Source IP 本選項允許您設定規則必須應用的**來源網路**。請從下表中選擇選項：	
Any	本選項允許您將本規則應用到所有來源網路的電腦上，例如那些接入網際網路的電腦。

選項	說明
IP Address	本選項允許您指定規則應用的IP位址。
IP Address	指定合適的網路位址。
Subnet	本選項允許將所有連線到同一IP子網路遮罩的電腦都包括進來。當選擇了本選項時，下列欄目可選：
Address	輸入合適的IP位址。
Mask	輸入相應的子網路遮罩。
Range	本選項允許將範圍內的IP位址都包括進應用規則。當選擇了本選項時，下列欄目可選：
Begin	輸入範圍起始的IP位址。
End	輸入範圍結束的IP位址。
IP 位址池	本選項允許您將預先設定好的IP域與規則挂鈎。您可在下表中選擇IP域。
Destination IP 本選項允許您設定能應用本規則的**目標網路**。請在下表的選項中選擇：	
Any	本選項允許您將規則應用到本地網路所有的電腦上。
IP Address, Subnet, Range and IP 位址池	請按照上文**Source IP**部分的說明選擇任一選項，並輸入詳細資訊。
Source Port 本選項允許您設定本規則得以應用的來源埠。請在下表的選項中選擇：	
Any	如果您希望將本規則應用到所有任意來源埠號的應用程式上，請選擇本選項。
Single	本選項允許您將本規則應用到某一指定來源埠號的應用程式上。
Port Number	輸入來源埠號
Range	如果您希望將本規則應用到本埠範圍的應用程式上，請選擇本選項。當選擇了本選項時，下列欄目可選：
Begin	輸入範圍的起始埠號
End	輸入範圍的結束埠號
Destination Port 本選項允許您設定能應用本規則的**目標埠**。請在下表的選項中選擇：	
Any	本選項允許您將規則應用到所有任意來源埠號的應用程式上。
Single, Range	請按照上文**Source Port**部分的說明選擇任一選項，並輸入詳細資訊。
Service	本選項允許您選擇任何預先設定好的服務（請從下表中選擇），而不是目

選項	說明
	標埠。下面列出了一些服務選項： BATTLE-NET, PC-ANYWHERE, FINGER, DIABLO-II, L2TP, H323GK, CUSEEME, MSN-ZONE, ILS, ICQ_2002, ICQ_2000, MSN, AOL, RPC, RTSP7070, RTSP554, QUAKE, N2P, PPTP, MSG2, MSG1, IRC, IKE, H323, IMAP4, HTTPS, DNS, SNMP, NNTP, POP3, SMTP, HTTP, FTP, TELNET. **注意:** 服務是協定與埠號的結合。它們將在您把它們增加進設定頁面的 “Firewall Service” 後出現。
Protocol 本選項允許您從下表中選擇協定的類型。可供選擇的設定爲All, TCP, UDP, ICMP, AH 和 ESP。注意，如果您爲目標埠選擇 “service” ，本選項將不可用。	
NAT 本選項允許您選擇入站資訊NAT的類型。	
None	如果您不想在入站ACL規則裏啓用NAT，請選擇此選項。
IP Address	選擇本選項以指定您期望入站資訊流向的電腦（通常是區域網路中的伺服器）的IP位址。注意，此選項被稱爲反向NAPT 或虛擬伺服器。
NAT 位址池	選擇本選項來將預先設定好的NAT域接入規則。注意，只有反向靜態NAT和反向NAPT域才能用來連線入站ACL的規則 。
Time Ranges 選擇預先設定好的規則起作用的時間範圍。選擇“Always”來使規則一直起作用。	
Application Filtering 本選項允許您選擇下拉表中預先設定好的FTP, HTTP, RPC 和/或 SMTP 應用程式篩檢程式。	
Log 點選 “Enable” 或 “Disable” 按鈕以開啓或關閉ACL規則logging功能。	
VPN 若您想要資訊流經VPN，請點選 “Enable” 按鈕；否則，點選 “Disable” 按鈕。	

圖 9.8. 入站 ACL 設定實例

9.4.2 增加入站 ACL 規則

想要增加入站 ACL 規則，請參考下列步驟：

1. 打開入站 ACL 規則設定頁面（請參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**）。
2. 在“**ID**”表中選擇 “**Add New**” 。
3. 從“**Action**”表中設定期望的動作（允許或拒絕）。
4. 改動任一或所有下列欄目：source/destination IP, source/destination port, protocol, port mapping, time ranges, application filtering, log, 和 VPN。請參考表 9.2 中對這些欄目的解釋。

5. 透過選擇 “**Move to**” 表中的序號來爲規則指定優先順序。注意，序號 1 表示優先勸最高。防火牆將按照優先勸的高低進行檢查。

6. 點選 Add 按鈕以建立新的 ACL 規則。新的 ACL 規則同時在入站 ACL 設定頁面下半頁的“入站訪問控制表”中出現。

圖 9.8 說明了如何建立接受入站 HTTP （例如，網頁伺服器） 服務的規則。 此規則允許入站 HTTP 資訊流向 IP 位址 192.168.1.28 的主機。

9.4.3 修改入站 ACL 規則

想要修改入站 ACL 規則，請參考下列步驟：

1. 打開入站 ACL 規則設定頁面（請參考第 **錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**）。
2. 點選 圖示，修改入站 ACL 表的規則或從“**ID**”表中選擇規則序號。
3. 改動任一或所有下列欄目：action, source/destination IP, source/destination port, protocol, port mapping, time ranges, application filtering, log, 和 VPN。請參看表 9.2 中對這些欄目的解釋。
4. 點選 Add 按鈕以修改 ACL 規則。新的 ACL 規則設定同時在入站 ACL 設定頁面下半頁的“入站訪問控制表”中出現。

9.4.4 刪除入站 ACL 規則

想要刪除入站 ACL 規則，請點選待刪規則前面的圖示，並參考下列步驟：

1. 打開入站 ACL 規則設定頁面（請參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**）。
2. 點選 圖示，刪除待刪的入站 ACL 表的規則或從“**ID**”表中選擇規則序號。
3. 點選 Delete 按鈕以刪除 ACL 規則。新的 ACL 規則設定同時在入站 ACL 設定頁面下半頁的“入站訪問控制表”中出現。

9.4.5 入站 ACL 規則展示

想要參看現有的入站 ACL 規則，您只需打開入站 ACL 規則設定頁面，如第***錯誤! 找不到參照來源。***節 ***錯誤! 找不到參照來源。*** 所示。

9.5 設定出站 ACL 規則

在出站ACL設定頁面建立ACL規則，如圖 9.9所示，您可控制對您區域網路電腦對網際網路或外部網路的訪問（允許或拒絕）。

本設定頁面的選項有：

- 增加規則，並設定參數
- 修改現有的規則
- 刪除現有的規則
- 檢查設定的 ACL 規則

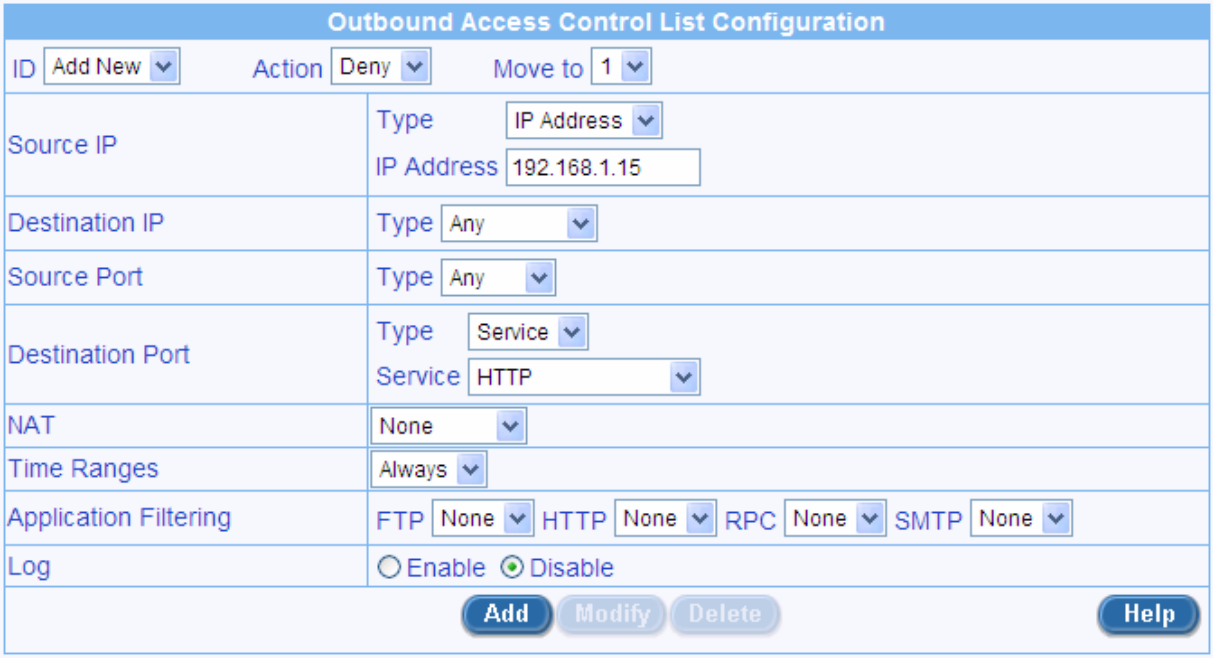


圖 9.9. 出站 ACL 設定頁面

9.5.1 出站 ACL 規則設定參數

表 9.3 說明了防火牆出站ACL規則可供選擇的設定參數。

表 9.3. 出站 ACL 規則設定參數

選項	說明
ID	
Add New	點選本選項以增加新的"基本"防火牆規則。
Rule Number	從列表中選擇規則，修改屬性。
Action	
Allow	按此按鈕以設定**允許**的規則。 當限制爲防火牆時，此規則將允許匹配的封包透過。
Deny	按此按鈕以設定**拒絕**的規則。 當限制爲防火牆時，此規則將**不**允許匹配的封包透過。
Move to 本選項允許您設立規則的優先順序。路由器防火牆在優先順序規則基礎上作用于封包。請以它在規則表的位置的指定序號爲基礎設立優先順序：	
1 (First)	此序號表示最高優先權：
Other numbers	選擇其他的數位以說明您想要指定的優先順序。

選項	說明
Source IP 本選項允許您設定規則必須應用的**來源網路**。請從下表中選擇選項：	
Any	本選項允許您將本規則應用到所有來源網路的電腦上，例如那些接入網際網路的電腦。
IP Address	本選項允許您指定規則應用的IP位址。
IP Address	指定合適的網路位址。
Subnet	本專案允許將所有連線到同一IP子網路遮罩的電腦都包括進來。當選擇了本選項時，下列欄目可選：
Address	輸入合適的IP位址。
Mask	輸入相應的子網路遮罩。
Range	本選項允許將範圍內的IP位址都包括進應用規則。當選擇了本選項時，下列欄目可選：
Begin	輸入範圍起始的IP位址。
End	輸入範圍起始的IP位址。
IP 位址池	本選項允許您將預先設定好的IP域與規則挂鈎。您可在下表中選擇IP域。
Destination IP 本選項允許您設定能應用本規則的**目標網路**。請在下表的選項中選擇：	
Any	本選項允許您將規則應用到本地網路所有的計算機上。
IP Address, Subnet, Range and IP 位址池	請按照上文**Source IP**部分的說明選擇任一選項，並輸入詳細資訊。
Source Port 本選項允許您設定本規則得以應用的來源埠。請在下表的選項中選擇：	
Any	如果您希望將本規則應用到所有任意來源埠號的應用程式上，請選擇本選項。
Single	本選項允許您將本規則應用到某一指定來源埠號的應用程式上。
Port Number	輸入來源埠號。
Range	如果您希望將本規則應用到本埠範圍的應用程式上，請選擇本選項。當選擇了本選項時，下列欄目可選：
Begin	輸入範圍的起始埠號。
End	輸入範圍的結束埠號。

選項	說明
Destination Port 本選項允許您設定能應用本規則的**目標埠**。請在下表的選項中選擇：	
Any	本選項允許您將規則應用到所有任意來源埠號的應用程式上。
Single, Range	請按照上文**Source Port**部分的說明選擇任一選項，並輸入詳細資訊。
Service	本選項允許您選擇任何預先設定好的服務（請從下表中選擇），而不是目標埠。下面列出了一些服務選項： BATTLE-NET, PC-ANYWHERE, FINGER, DIABLO-II, L2TP, H323GK, CUSEEME, MSN-ZONE, ILS, ICQ_2002, ICQ_2000, MSN, AOL, RPC, RTSP7070, RTSP554, QUAKE, N2P, PPTP, MSG2, MSG1, IRC, IKE, H323, IMAP4, HTTPS, DNS, SNMP, NNTP, POP3, SMTP, HTTP, FTP, TELNET. **注意:** 服務是協定與埠號的結合。它們將在您把它們增加進設定頁面的 “Firewall Service” 後出現。
Protocol 本選項允許您從下表中選擇協定的類型。可供選擇的設定爲All, TCP, UDP, ICMP, AH 和 ESP。注意，如果您爲目標埠選擇 “service” ，本選項將不可用。	
NAT 本選項允許您選擇出站資訊NAT的類型。	
None	如果您不想在出站ACL規則裏啓用NAT，請選擇此選項。
IP Address	選擇本選項以指定您期望出站資訊流向的電腦（通常是區域網路中的伺服器）的IP位址。注意，此選項被稱爲反向NAPT 或虛擬伺服器。
NAT 位址池	選擇本選項來將預先設定好的NAT域接入規則。注意，只有反向靜態NAT和反向NAPT域才能用來連線出站ACL的規則。
Interface	選擇本選項爲出站資訊選擇WAN介面IP位址。注意，WAN IP必須事先設定再選擇此項。
Time Ranges 選擇預先設定好的規則起作用的時間範圍。選擇“Always”來使規則一直起作用。	
Application Filtering 本選項允許您選擇下表中預先設定好的FTP, HTTP, RPC 和/或 SMTP 應用程式篩檢程式。	
Log 點選 “Enable” 或 “Disable” 按鈕來開啓或關閉ACL規則logging功能。	
VPN 若您想要資訊流經VPN，請點選 “Enable” 按鈕；否則，點選 “Disable” 按鈕。	

9.5.2 增加出站 ACL 規則

想要增加出站 ACL 規則，請參考下列步驟：

1. 打開出站 ACL 規則設定頁面（請參考第 9.4.2 節**錯誤! 找不到參照來源。** ）。
2. 在“**ID**”表中選擇 “**Add New**” 。
3. 從“**Action**”表中設定期望的動作（允許或拒絕）。
4. 改動任一或所有下列欄目：source/destination IP, source/destination port, protocol, port mapping, time ranges, application filtering, log, 和 VPN。請參考表 9.2 中對這些欄目的解釋。
5. 透過選擇 “**Move to**” 表中的序號來爲規則指定優先順序。注意，序號 1 表示優先勸最高。防火牆將按照優先勸的高低進行檢查。
6. 點選 Add 按鈕以建立新的 ACL 規則。新的 ACL 規則同時在出站 ACL 設定頁面下半頁的“出站訪問控制表”中出現。

圖 9.10 說明了如何建立接受出站 HTTP （例如，網頁伺服器） 服務的規則。 此規則允許出站 HTTP 資訊流向主機 WAN/ IP 位址 192.168.1.15。

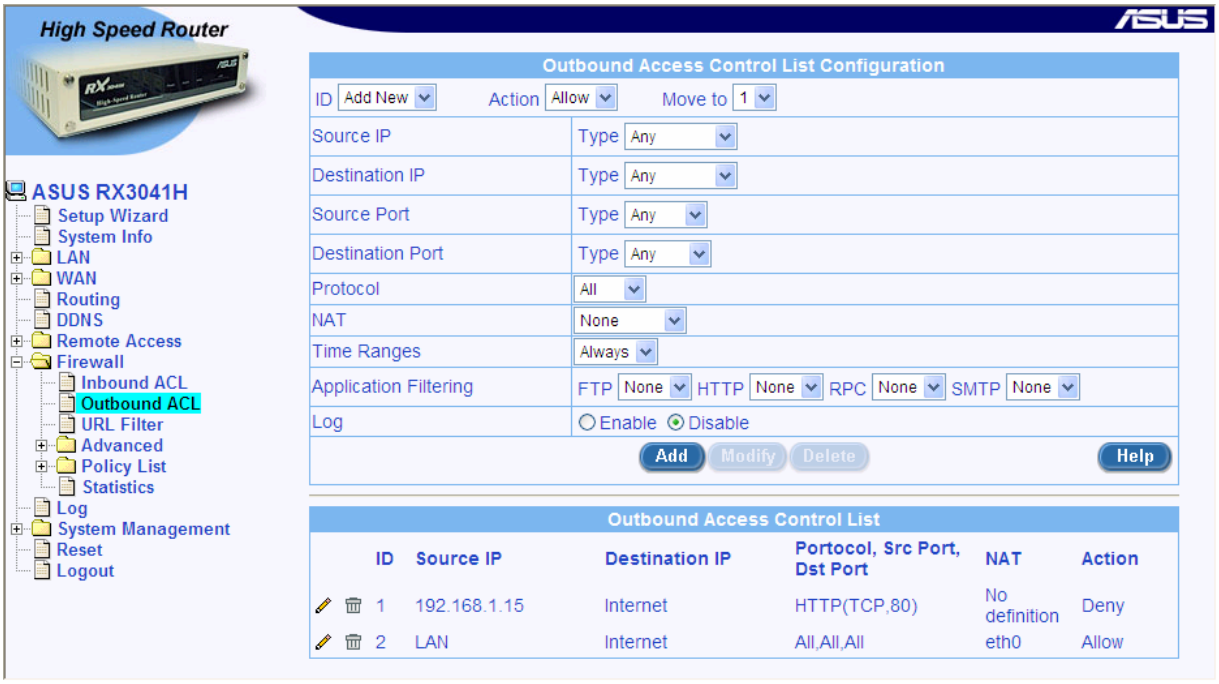


圖 9.10. 出站 ACL 設定頁面

9.5.3 修改出站 ACL 規則

想要修改出站 ACL 規則，請參考下列步驟：

1. 打開出站 ACL 規則設定頁面（請參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。** ）。
2. 點選 圖示，修改出站 ACL 表的規則或從“**ID**”表中選擇規則序號。

3. 改動任一或所有下列欄目：action, source/destination IP, source/destination port, protocol, port mapping, time ranges, application filtering, log, 和 VPN。請參看表 9.2 中對這些欄目的解釋。

4. 點選 Modify 按鈕以修改 ACL 規則。新的 ACL 規則設定同時在出站 ACL 設定頁面下半頁的“出站訪問控制表”中出現。

9.5.4 刪除出站 ACL 規則

想要刪除出站 ACL 規則，請點選待刪規則前面的圖示，並參考下列步驟：

1. 打開出站 ACL 規則設定頁面（請參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**）。

2. 點選 圖示，刪除待刪的出站 ACL 表的規則或從“**ID**”表中選擇規則序號。

3. 點選 Delete 按鈕以刪除 ACL 規則。新的 ACL 規則設定同時在出站 ACL 設定頁面下半頁的“出站訪問控制表”中出現。

9.5.5 出站 ACL 規則展示

想要參看現有的出站 ACL 規則。您只需打開出站 ACL 規則設定頁面，如第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。** 所示。

9.6 設定 URL 篩檢程式

以 URL（Uniform Resource Locator，例如 www.yahoo.com）爲基礎的關鍵字過濾允許您定義一個或多個不應在 URL 出現的關鍵字。任何 URL 都包含一個或多個將被鎖定的關鍵字。這是一個獨立的特性，例如它與 ACL 規則沒有關聯。此特性能被獨立地開啓/關閉，但是只在開啓防火牆的狀態下工作。

9.6.1 URL 篩檢程式設定參數

表 9.4 說明 了URL過濾規則可供選擇的設定參數。

表 9.4. URL 篩檢程式設定參數

選項	**說明**
URL篩檢程式狀態	點選“Enable” 或 “Disable” 按鈕開啓或 關閉URL過濾功能。
代理伺服器埠	輸入爲您網頁瀏覽器設定的代理伺服器（網頁伺服器）埠號。注意，代理伺服器埠的改變需要您關閉再開啓防火牆來使其生效。
ID	
Add New	點選本選項以增加新的URL篩檢程式規則。
Rule Number	從下表中選擇規則修改屬性。
Keyword	定義一個不會在URL中出現的關鍵字。

9.6.2 增加 URL 篩檢程式規則

想要增加 URL 篩檢程式，請參考下列步驟：

1. 打開 URL 設定頁面（請參考第 9.5.2 節**錯誤! 找不到參照來源。** ）。

2. 在“**ID**”表中選擇 “**Add New**” 。
3. 在關鍵字欄目中輸入關鍵字。
4. 點選 Add 按鈕以建立 URL 篩檢程式規則。新的規則同時在 URL 篩檢程式設定摘要表中出現。

9.6.3 修改 URL 篩檢程式規則

想要修改 URL 篩檢程式規則，您必須首先刪除現有的 URL 篩檢程式規則（參看第 9.6.4 節），然後增加新的（參看第 9.6.2 節 增加 URL）。

9.6.4 刪除 URL 篩檢程式規則

想要刪除 URL 篩檢程式規則，請點選待刪規則前面的圖示，並參考下列步驟：

1. 打開 URL 設定頁面（請參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**）。
2. 點選 圖示，刪除待刪的 URL 篩檢程式設定摘要表的規則或從“**ID**”表中選擇規則序號。
3. 點選 Delete 按鈕以刪除 URL 規則。

9.6.5 檢查設定的 URL 篩檢程式規則

想要檢查現有的 URL 篩檢程式規則，您只需打開 URL 篩檢程式設定頁面，如第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**所示。

9.6.6 URL 篩檢程式規則實例

圖 9.11 顯示了 URL 篩檢程式規則實例，它示範了：

- 如何增加關鍵字“abcnews”，任何 URL 包含的關鍵字都會被鎖定。
- 設定代理網頁伺服器序號到 80（您可以爲您的代理伺服器使用不同的埠號）。這意味著 URL 篩檢程式規則應用的範圍將超過代理伺服器埠 80，以防萬一代理網頁伺服器已被使用。如果您沒有爲您的瀏覽器使用代理伺服器，此設定將被忽略。注意，在做此改變之前您必須先關閉然後再打開防火牆。請參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**中對開啓和關閉防火牆服務的詳細說明。

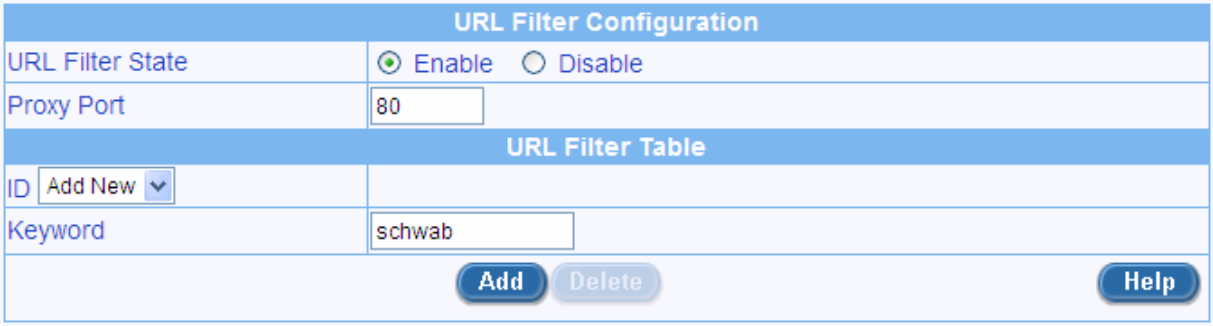


圖 9.11. URL 篩檢程式規則實例

9.7 設定高級防火牆規格 – （防火牆 ➔ 高級）

本選項將在螢幕上顯示下列子欄目供您設定高級防火牆規則：

- 自主訪問（self Access）– 本選項允許您針對目標爲路由器本身的封包去設定規則。

- 服務（Services） – 選擇本選項來設定服務（應用程式使用指定的埠號）。每個服務記錄都包含了服務名稱、IP 協定值以及相應的埠號。
- DoS – 選擇本選項來設定 DoS – 拒絕服務 – 參數。此選項列出了反抗路由器防火牆保護的 DoS 攻擊的預設設定。

下列章節說明了這些選項的用法

9.7.1 設定自主訪問（Self Access）規則

自主訪問（Self Access）規則控制對互聯網安全路由器自身的訪問。您可以使用自主訪問規則設定頁面，如圖 9.12 所示，進行下列步驟：

- 增加自主訪問規則，並設定參數
- 修改現有的自主訪問規則
- 刪除現有的自主訪問規則
- 檢查現有的自主訪問規則

圖 9.12. 自主訪問規則設定頁面

9.7.1.1 自主訪問設定參數

表 9.5 說明了自主訪問設定頁面可供選擇的設定參數。

表 9.5. 自主訪問設定參數

選項	說明
Protocol	從下表中選擇協定- TCP/ UDP/ICMP
Port	輸入埠號。
Direction 選擇資訊被允許流通的方向。	

選項	說明
From LAN	選擇Enable 或 Disable來允許或拒絕從區域網路（內部網路）到路由器的通信方向。
From WAN	選擇Enable 或 Disable來允許或拒絕從WAN（外部網路）到路由器的通信方向。

9.7.1.2 增加自主訪問規則

想要增加自主訪問規則，請參考下列步驟：

1. 打開自主訪問規則設定頁面（請參考第 9.6.1.2 節**錯誤! 找不到參照來源。** ）。
2. 從自主訪問規則下拉表中選擇 “**Add New**” 。
3. 從協定的下拉表中選擇一項，如果您選擇了 TCP 或 UDP 協定，您將需要輸入埠號。
4. 點選 Add 按鈕以建立新的自主訪問規則。新的規則同時在自主訪問列表下半頁的“自主訪問規則設定頁面”中出現。

實例

圖 9.12 顯示了螢幕上的條目用來：

- 增加新的自主訪問規則到：
  - 允許 TCP 埠 80 從 LAN 流過來的通信量（例如 HTTP 通信量），以及拒絕從 WAN 埠（例如外部網路）流向網際網路安全路由器的 HTTP 通信量。

9.7.1.3 修改自主訪問規則

想要修改自主訪問規則，請參考下列步驟：

1. 打開自主訪問規則設定頁面（請參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。** ）。
2. 點選 圖示，修改自主訪問規則表或從自主訪問下拉表中選擇自主訪問規則。
3. 您可以從 LAN 或 WAN 或二者同時來開啓或關閉通信。注意，如果 TCP 或 UCP 協定已選的話，埠號不能再更改。想要修改埠號，您必須首先刪除現有的自主訪問規則以及增加新的自主訪問規則代替。
4. 點選 Modify 按鈕以保存更改。新的自主訪問規則設定同時在自主訪問規則設定頁面下半頁的自主訪問規則表中出現。

9.7.1.4 刪除自主訪問規則

想要刪除自主訪問規則，請點選待刪規則前面的圖示，並參考下列步驟：

1. 打開自主訪問規則設定頁面（請參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**）。
2. 點選 圖示，刪除待刪的自主訪問規則表或從自主訪問規則下拉表中選擇自主訪問規則。
3. 點選 Delete 按鈕以刪除規則。注意，已刪除的規則將從設定頁面下半頁的自主訪問規則表中移除。

9.7.1.5 檢查設定的自主訪問規則

想要檢查現有的自主訪問規則，您只需打開自主訪問規則設定頁面，如第**錯誤! 找不到參照來源。**節 ***錯誤! 找不到參照來源。***所示。

9.7.2 設定服務列表

服務是協定和埠號的聯合，被用在入站和出站ACL規則設定中。您可以使用服務設定頁面來：

- 增加自主訪問規則，並設定參數
- 修改現有的自主訪問規則
- 刪除現有的自主訪問規則
- 檢查現有的自主訪問規則

圖 9.13 顯示了防火牆列表的設定頁面。已設定的服務在頁面的下半頁顯示：

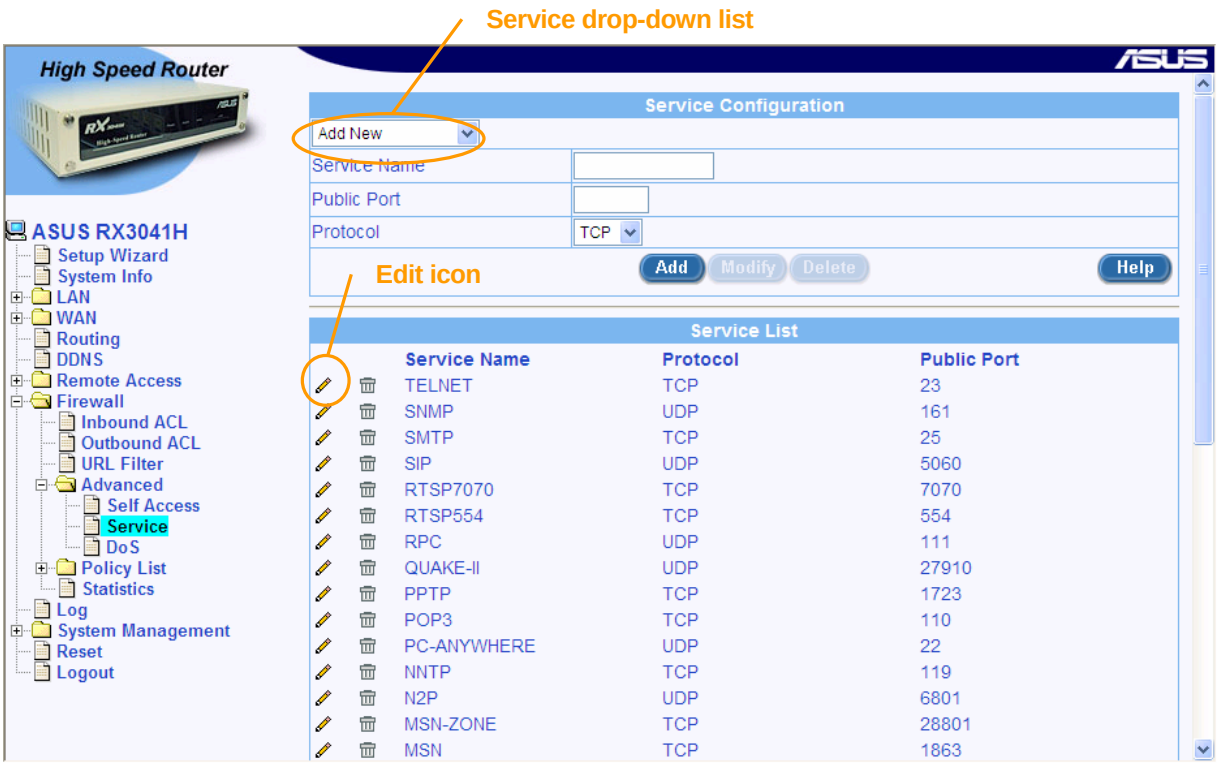


圖 9.13. 服務列表設定頁面

9.7.2.1 服務列表參數設定

表 9.6 說明了防火牆服務列表可供選擇的設定參數。

表 9.6. 服務列表參數設定

選項	說明
Service Name	輸入待增加的服務名稱，注意，名稱只由文字與數位組成。
Protocol	輸入服務使用的協定的類型。
Port	輸入爲服務設立的埠號。

9.7.2.2 增加服務選項

想要增加服務選項，請參考下列步驟：

1. 打開服務列表設定頁面（請參考第 9.6.2.2 節**錯誤! 找不到參照來源。** ）。
2. 從服務下拉表中選擇 “**Add New**” 。
3. 在 “**Service Name**” 欄目輸入您想要的名稱，最好是能表現出服務特性的有意義的名稱。注意，名稱只由文字與數位組成。
4. 更改下列任一或所有欄目：public port 和 protocol。請參看表 9.6 中對本欄目的解釋。
5. 點選 Add 按鈕以建立新的服務選項。新的服務選項同時在服務設定頁面下半頁的服務列表中出現。

9.7.2.3 修改服務選項

想要修改服務選項，請參考下列步驟：

1. 打開服務列表設定頁面（請參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。** ）。
2. 從服務下拉表中選擇服務選項，或者點選服務列表中需要修改的 圖示。
3. 更改下列任一或所有欄目：service name, public port 和 protocol。請參看表 9.6 中對本欄目的解釋。
4. 點選 Modify 按鈕以保存更改。新的服務設定同時在服務設定頁面下半頁的服務列表中出現。

9.7.2.4 刪除服務選項

想要刪除自主訪問規則，請參考下列步驟：

1. 打開服務列表設定頁面（請參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**）。
2. 從服務下拉表中選擇服務選項，或者點選服務列表中需要刪除的 圖示。
3. 點選 Delete 按鈕以刪除規則。注意，已刪除的規則將從設定頁面下半頁的服務列表中移除。

9.7.2.5 檢查設定的服務選項

想要檢查現有的服務列表，請參考下列步驟：

1. 打開服務列表設定頁面（如第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**所示）。
2. 服務列表在服務設定頁面下半頁出現，顯示了所有已設定好的服務選項。

9.7.3 設定 DoS

網際網路安全路由器擁有一個專用的抵禦攻擊的引擎，能保護內部網路免受 DoS（拒絕服務）攻擊，例如 SYN flooding, IP smurfing, LAND, Ping of Death 以及所有封包重組的攻擊。這個引擎還能丟棄 ICMP 的重寄及拒絕 IP loose/strict 來源路由封包。例如，路由器防火牆提供防止“WinNuke”的保護的安全設備，網際網路中遠端攻擊未受保護的 Windows 系統的一個廣泛應用的程式。網際網路安全路由器還提供對多種普通網際網路攻擊的保護，例如 IP Spoofing, Ping of Death, Land Attack, Reassembly 以及 SYN flooding。要參考路由器提供的 DoS 保護完全列表，請看表 2.3。

9.7.3.1 DoS 保護設定參數

表 9.7 說明了DoS保護可供使用的設定參數。

表 9.7. DoS 保護設定參數

選項	說明
SYN Flooding	打勾或不打勾本選項以開啓或關閉防止SYN Flood攻擊的保護功能。此攻擊包括向伺服器發出連線要求，但是不全部完成連線。當不能從有效的用戶那裏接收連線時，這將導致一些電腦陷入"當機狀態"（SYN是SYNchronize的簡寫；是打開網際網路連線的第一步）。如您期望保護網路免受TCP SYN flooding攻擊，您可選擇此項。SYN Flood保護預設爲開啓狀態。
Winnuke	打勾或不打勾本選項以開啓或關閉防止Winnuke攻擊的保護功能。一些Microsoft Windows作業系統的較老版本易遭受此項攻擊。如果區域網路電腦的作業系統沒有及時下載最新的版本/補丁來更新，那麼我們建議您開啓此項保護功能。
MIME Flood	打勾或不打勾本選項以開啓或關閉防止MIME攻擊的保護功能。您可選擇本選項以保護您網路內的郵件伺服器免受MIME flooding的攻擊。
FTP Bounce	打勾或不打勾本選項以開啓或關閉防止FTP Bounce攻擊的保護功能。簡言之，攻擊在誤用FTP協定中的PORT命令時才發生。攻擊者能建立FTP伺服器與另一系統中任意埠的連線。此連線可被用來繞開訪問控制。
IP Unaligned Time Stamp	打勾或不打勾本選項以開啓或關閉防止unaligned IP time stamp攻擊的保護功能。 某些作業系統在接收到未在32位邊界內的IP timestamp選項時會崩潰。
Sequence Number Prediction Check	打勾或不打勾本選項以開啓或關閉防止TCP Sequence Number Prediction攻擊的保護功能。對於TCP封包而言，Sequence Number 是被用來阻止對任意資料的接收或當Initial Sequence Number（ISN）隨意產生時被攻擊者惡意使用。因爲擁有有效的Sequence Number的僞造封包可騙取接收主機的信任。如此一來，攻擊者就能夠進入系統。請注意！此種攻擊只影響開始或終止於網際網路安全路由器的TCP封包。
Sequence Number Out of Range Check	打勾或不打勾本選項以開啓或關閉防止TCP out of range sequence number攻擊的保護功能。攻擊者可送出一個TCP封包，導致入侵偵測系統（IDS）在連線中變得與資料不同步。後來在此連線中發出的信框就可能被IDS忽略。這可能暗示著一次不成功的對TCP對話的搶奪企圖。
ICMP Verbose	打勾或不打勾本選項以開啓或關閉防止ICMP錯誤消息攻擊的保護功能。ICMP訊息可使用非期望的通信量來泛流您的網路。本選項預設值爲開啓狀態。
Maximum IP Fragment Count	輸入防火牆允許每個IP封包的片段的最大數目。當您與ISP的連線透過PPPoE進行時，本選項十分需要。此資料在傳輸或接收IP片段時使用。當大尺寸的封包透過路由器送出時，封包被分解爲最大傳輸單元（MTU，Maximum Transmission Unit）大小的片段。分解的數目預設爲45。如果介

選項	說明
	面的MTU爲1500（乙太網預設），那麼每個IP封包的最大片段數爲45。如果MTU越小，那麼片段的數目會越大。
Minimum IP Fragment Size	輸入防火牆允許每個IP封包的片段的最小數目。此限制不會在封包最後的片段上強制執行。如果網際網路通信量在產生了很多小的片段時，此數值將變小。此種情況在有多個封包遺失、速度變慢和日誌（log）經常產生的情況下（片段的大小比設定好的最小片段的大小還要小）常常出現。

9.7.3.2 設定 DoS

大多數支援的攻擊類型 DoS 保護都預設開啓。圖 9.14 顯示了 DoS 的預設設定。您可打勾或不打勾個別的攻擊保護類別以開啓或關閉針對特殊攻擊類型的保護。

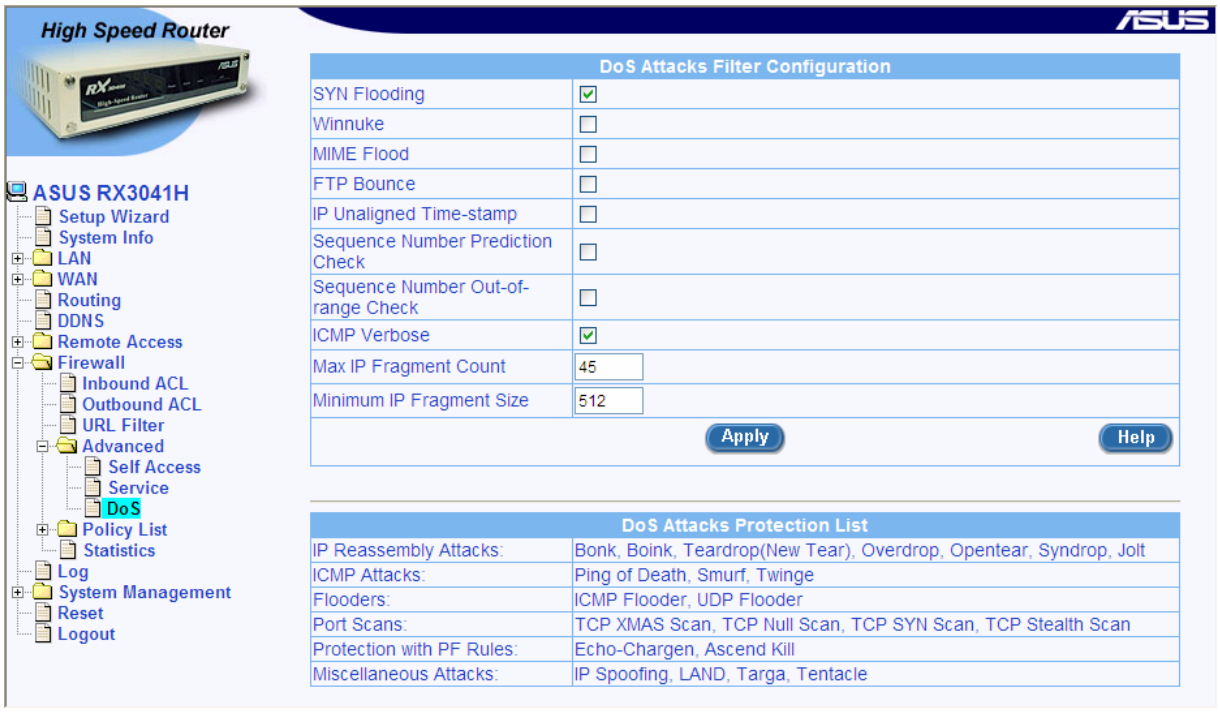


圖 9.14. DoS 設定頁面

9.8 防火牆規則列表 – （防火牆 ➔ 規則列表）

防火牆規則列表提供了管理防火牆 ACL 規則（入站/出站 ACL 規則和群組 ACL 規則）的方便之路。

- 應用程式篩檢程式 – 本選項允許您爲 FTP, HTTP, RPC 和 SMTP 應用程式設定命令篩檢程式。在這裏，在它們隸屬於規則之前設定篩檢程式。
- IP 位址池 – 本選項允許您爲 IP 位址池設置邏輯名稱，以及設定合適的 IP 位址。每個記錄都包含了 IP 記錄的名稱和 IP 位址的類型（單個的 IP 位址或 IP 位址域或子網路位址）。

- NAT 位址池 – 本選項允許您設定確保對應從內部 IP 位址到公共 IP 位址映射的 NAT 位址池 。在這裏，在它們隸屬於規則之前設定 NAT 位址池。
- 時間範圍 – 本選項允許您爲用戶透過路由器訪問網路設定時間視窗。

9.8.1 設定應用程式篩檢程式

應用程式篩檢程式允許網路管理員阻止、監視，以及報告網路用戶訪問非商業和不良內容。此高性能內容訪問管理將有助於生產力的提高、佔用更低的頻寬使用以及減少法律責任。

網際網路安全路由器具備控制積極和過濾某些應用程式協定內容的能力，例如 HTTP, FTP, SMTP 和 RPC。

- HTTP – 您能定義以阻止過濾 HTTP 副檔名

  ActiveX – *.ocx

  Java Archive – *.jar

  Java Applets – *.class

  Microsoft Archives – *.msar

  其他的以檔案副檔名爲基礎的 URL。
- FTP – 允許您爲站點和用戶群定義和強制執行檔案傳送規則
- SMTP – 允許您過濾揭示關於接收者超量資訊的操作，例如 VRFY, EXPN 等。
- RPC – 允許您過濾以指定的 RPC 程式號碼爲基礎的程式。

9.8.1.1 應用程式篩檢程式設定參數

表 9.8 說明了應用程式篩檢程式可供選擇的設定參數。

表 9.8. 應用程式篩檢程式設定參數

選項	說明
Filter Type	選擇篩檢程式的類型： FTP, HTTP, RPC 和 SMTP。
Filter Name	爲篩檢程式輸入名字。
Protocol	選擇應用程式篩檢程式使用的協定（TCP/UDP）。
Port	輸入應用程式篩檢程式使用的埠號。
Log 本選項包括開啓和關閉登入應用程式篩檢程式的按鈕。	
Enable	選擇本選項以開啓登入應用程式篩檢程式。
Disable	選擇本選項以關閉登入應用程式篩檢程式。
Action	
Allow	按此按鈕以設定**允許**的規則。 當限制爲防火牆時，此規則將允許匹配的封包透過。
Deny	按此按鈕以設定**拒絕**的規則。 當限制爲防火牆時，此規則將**不**允許匹配的封包透過。
Filter Commands	

選項	說明
本選項允許您輸入各自應用程式的命令。所支援的每個應用程式的命令列表如下所示：	
FTP Commands	增加下列命令至FTP篩檢程式到：
CWD	允許或拒絕改變目錄。
LIST	允許或拒絕檔案/目錄列表。
MKD	允許或拒絕建立目錄。
NLST	允許簡要的目錄內容列表。
PASV	允許被動資料內容的開始。
PORT	允許或拒絕參與主動的資料連線的埠號。
RETR	允許或拒絕從FTP伺服器獲得檔案。
RMD	允許移除目錄。
RNFR	允許重新命名自。
RNTO	允許重新命名到。
DELE	允許刪除檔案。
SITE	允許設定站點參數（FTP伺服器提供的特殊服務）。
STOR	允許或拒絕把檔案傳送至FTP伺服器。
SMTP Commands	增加下列命令至SMTP過濾器到：
MAIL	允許或拒絕開始郵件處理。
RCPT	允許或拒絕識別郵件資料的個別接收。
DATA	允許或拒絕郵件資料。
VRFY	允許或拒絕核實用戶的存在。
EXPN	允許或拒絕郵寄表的鑒別。
TURN	允許或拒絕用戶端與伺服器交換角色而寄送反向郵件。
SEND	允許或拒絕開始郵件處理。
HTTP (Deny Following Files)	增加下列命令至HTTP篩檢程式到：
Java Applet	拒絕所有 *.class 檔案。
Java-archive	拒絕所有*.jar檔案。
MS Archive	拒絕所有*.msar檔案。
ActiveX	拒絕所有*.ocx檔案。
RPC Numbers	
RPC numbers	增加此命令至RPC篩檢程式以允許或拒絕RPC程式數目。

9.8.1.2 訪問應用程式篩檢程式設定頁面 –（防火牆 ➔ 規則列表 ➔ 應用程式篩檢程式）

以管理員身份登入設定管理器，點選 **Firewall** 功能表，點選 **Policy List** 子功能表，然後點選 **Application Filter** 子功能表。應用程式篩檢程式設定頁面將如圖 9.9 所示。

注意，當您打開應用程式篩檢程式設定頁面時，現有的應用程式篩檢程式規則同時在設定頁面的下半頁出現，如圖 9.9 所示。

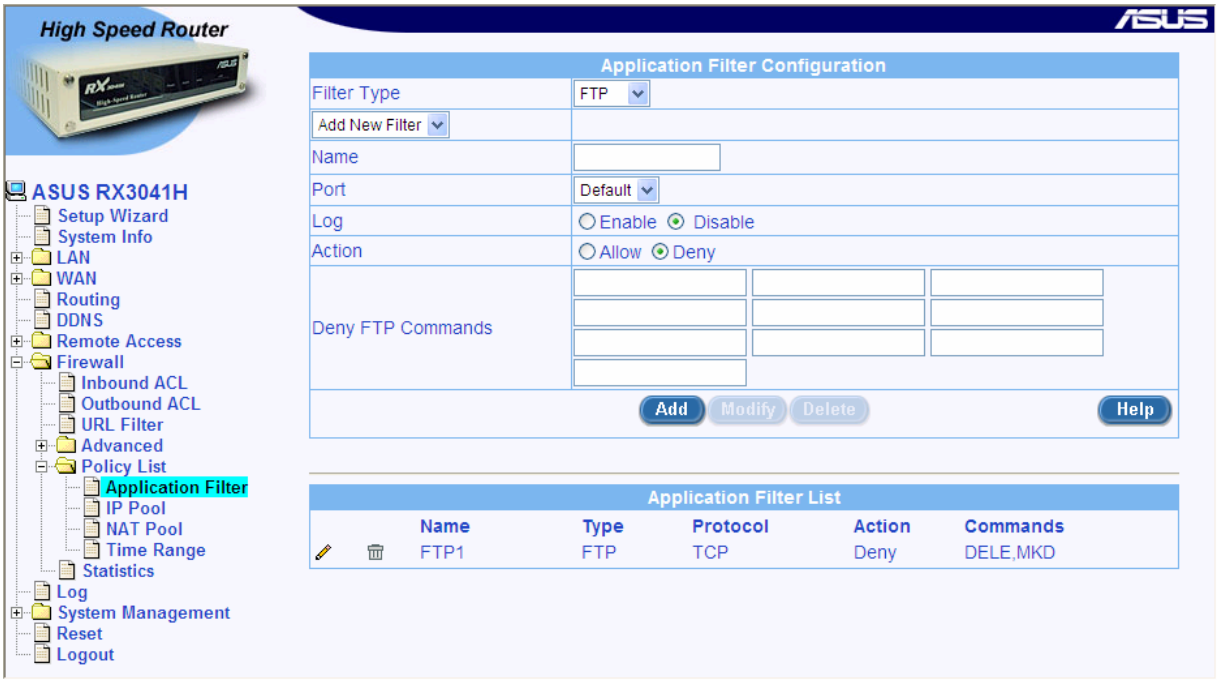


圖 9.15. 應用程式篩檢程式設定頁面

9.8.1.3 增加應用程式篩檢程式

應用程式篩檢程式設定最好用一些實例來闡釋。注意，爲 RPC 和 SMTP 進行的設定 FTP 相類似，這裏將不 提及。

FTP 實例：增加 FTP 篩檢程式規則以阻止 FTP 刪除命令

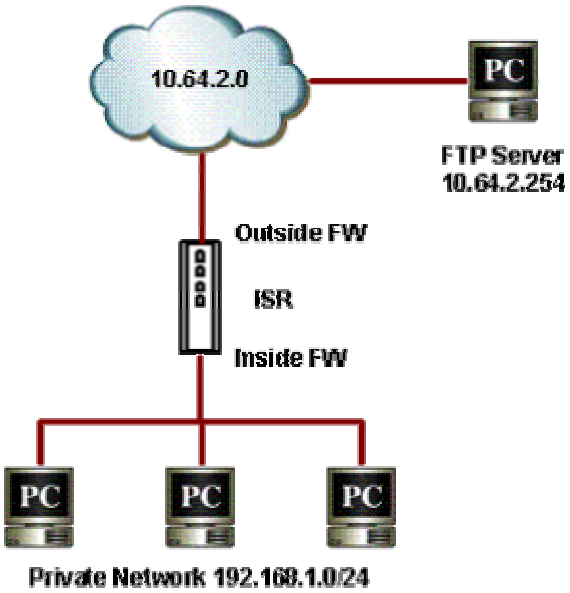


圖 9.16 對 FTP 篩檢程式實例進行的網路診斷 – 阻止 FTP 刪除命令

1. 打開應用程式篩檢程式規則設定頁面（防火牆 ➔ 規則列表 ➔ 應用程式篩檢程式）

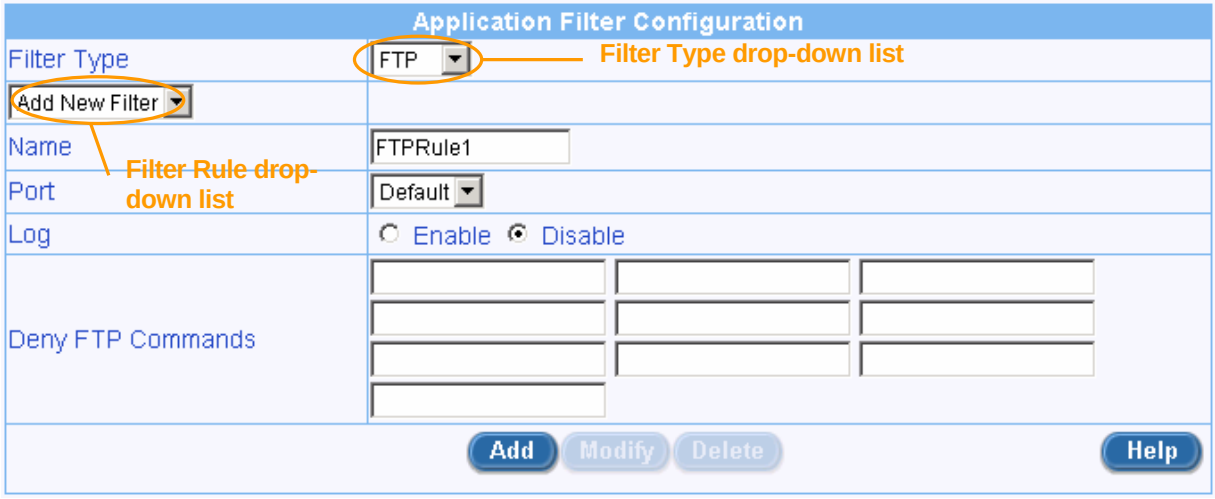


圖 9.17. FTP 篩檢程式實例 – 設定 FTP 篩檢程式規則

2. 從篩檢程式程式下拉表中選擇 FTP。
3. 從篩檢程式規則下拉表中選擇 “Add New Filter” 。
4. 爲規則輸入名稱 – 在此實例中，爲 FTPRule1。
5. 如需要，改變埠號。然而，我們推薦您保持預設的設定值不變。
6. 選擇開啓或關閉登入選項，預設的設定是關閉。
7. 點選第一個 FTP 命令欄目，防火牆設定助手頁面將出現。

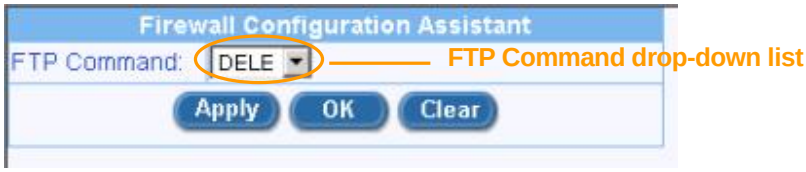


圖 9.18 FTP 篩檢程式實例 – 防火牆設定助手

8. 從 FTP 命令下拉表中選擇您需要的 FTP 命令，然後點選 OK 按鈕。選中的 FTP 命令將被添加到已選的拒絕 FTP 命令欄目中。

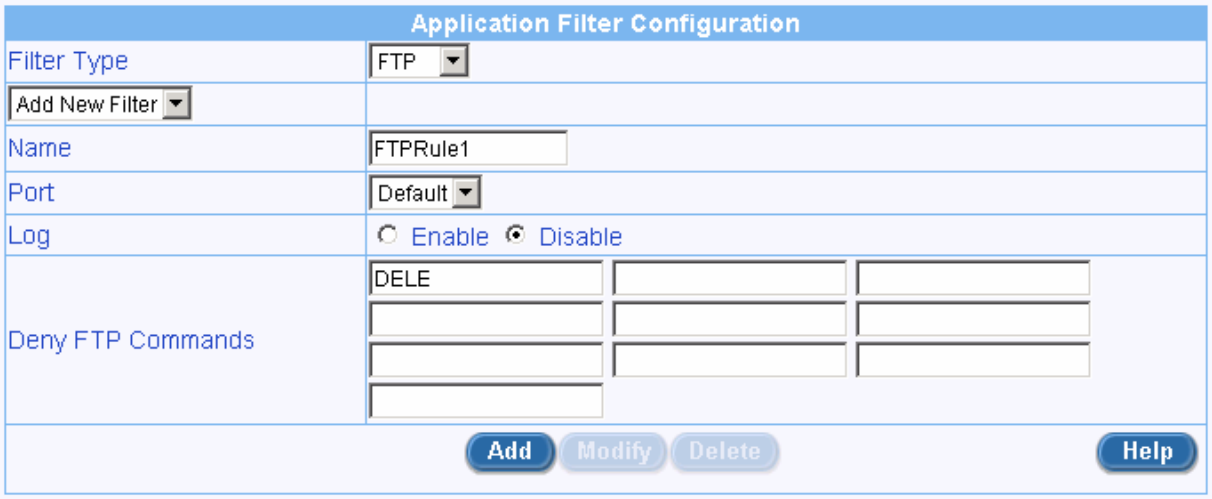


圖 9.19 FTP 篩檢程式實例 – 增加 FTP 篩檢程式以拒絕 FTP 刪除命令

9. 如果需要添加更多的命令，請重復步驟；否則，請繼續下一步。

10. 點選 Add 按鈕以建立 FTP 應用程式篩檢程式規則。

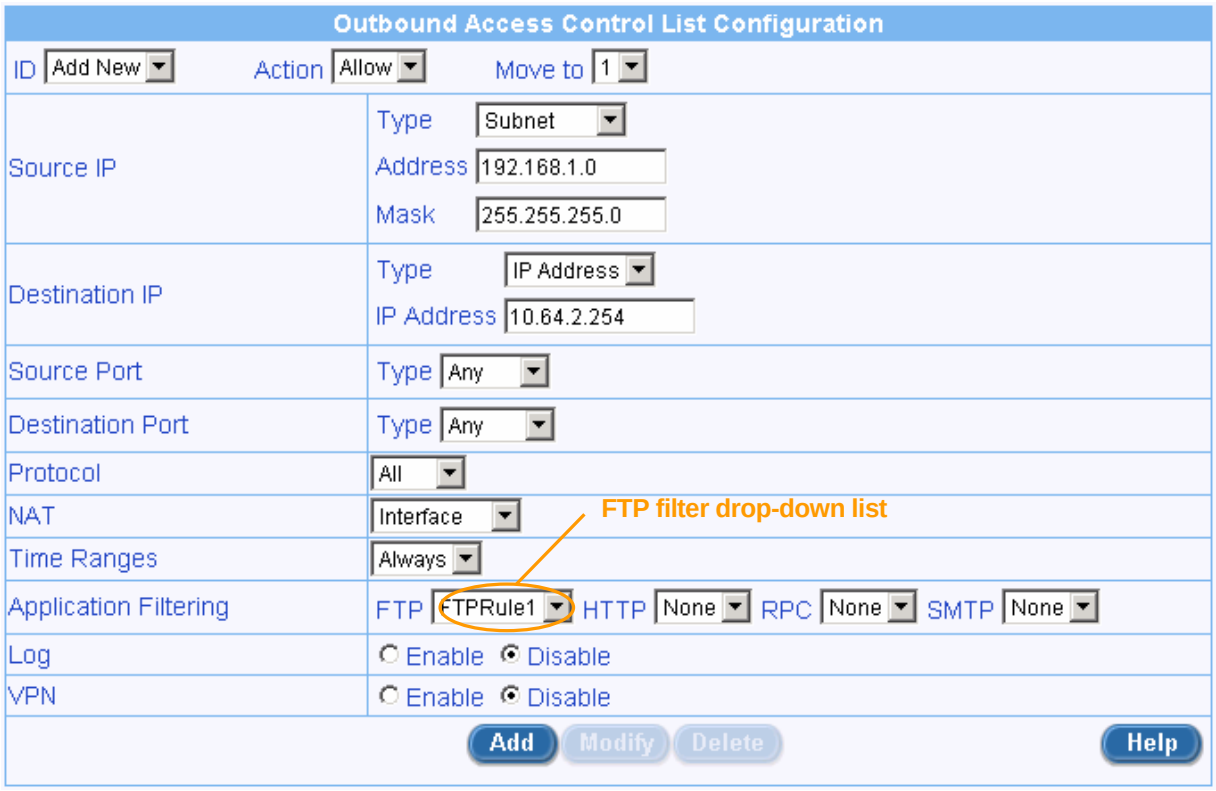


圖 9.20. FTP 篩檢程式實例 – 聯合 FTP 篩檢程式至 ACL 規則

11. 透過從 FTP 篩檢程式下拉表（參考圖 9.20）中選擇 FTP 篩檢程式，聯合新近增加的 FTP 應用程式篩檢程式至防火牆 ACL 規則（入站、出站或群組 ACL）上，然後點選 Add 或 Modify 按鈕以保存設定。

HTTP 實例：增加 HTTP 篩檢程式規則以 阻止 JAVA Applet 以及 Java archive 程式

1. 打開應用程式篩檢程式規則設定頁面（防火牆 ➔ 規則列表 ➔ 應用程式過濾器）

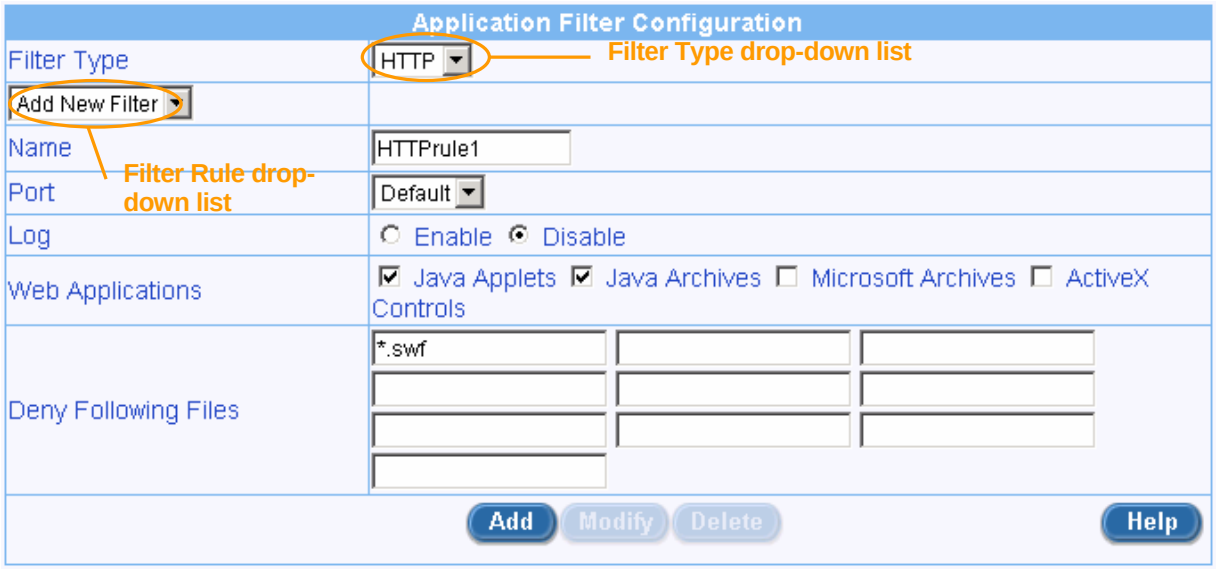


圖 9.21. HTTP 篩檢程式實例– 設定 HTTP 篩檢程式規則

2. 從篩檢程式程式下拉表中選擇 HTTP。
3. 從篩檢程式規則下拉表中選擇 “Add New Filter” 。
4. 爲規則輸入名稱 – 在此實例中，爲 HTTPrule1。
5. 如需要，改變埠號。然而，我們推薦您保持預設的設定值不變。
6. 選擇開啓或關閉登入選項，預設的設定是關閉。
7. 檢查網頁應用程式檔案以阻止 – 在本例中，爲 JAVA Applet 程式以及 Java archive 檔案。
8. 輸入附加的網頁應用程式檔案以阻止。如需要，在“Deny Following Files”欄目輸入檔案副檔名。圖 9.21 顯示了除了 JAVA Applet 及 Java archive 檔案之外，被阻止的 flash 檔案（檔案的副檔名爲 *.swf）。
9. 點選 Add 按鈕以建立 HTTP 應用程式篩檢程式規則。
10. 透過從 HTTP 篩檢程式下拉表（參考圖 9.20）中選擇 HTTP 篩檢程式，聯合新近增加的 HTTP 應用程式篩檢程式至防火牆 ACL 規則（入站、出站或群組 ACL）上，然後點選 Add 或 Modify 按鈕以保存設定。

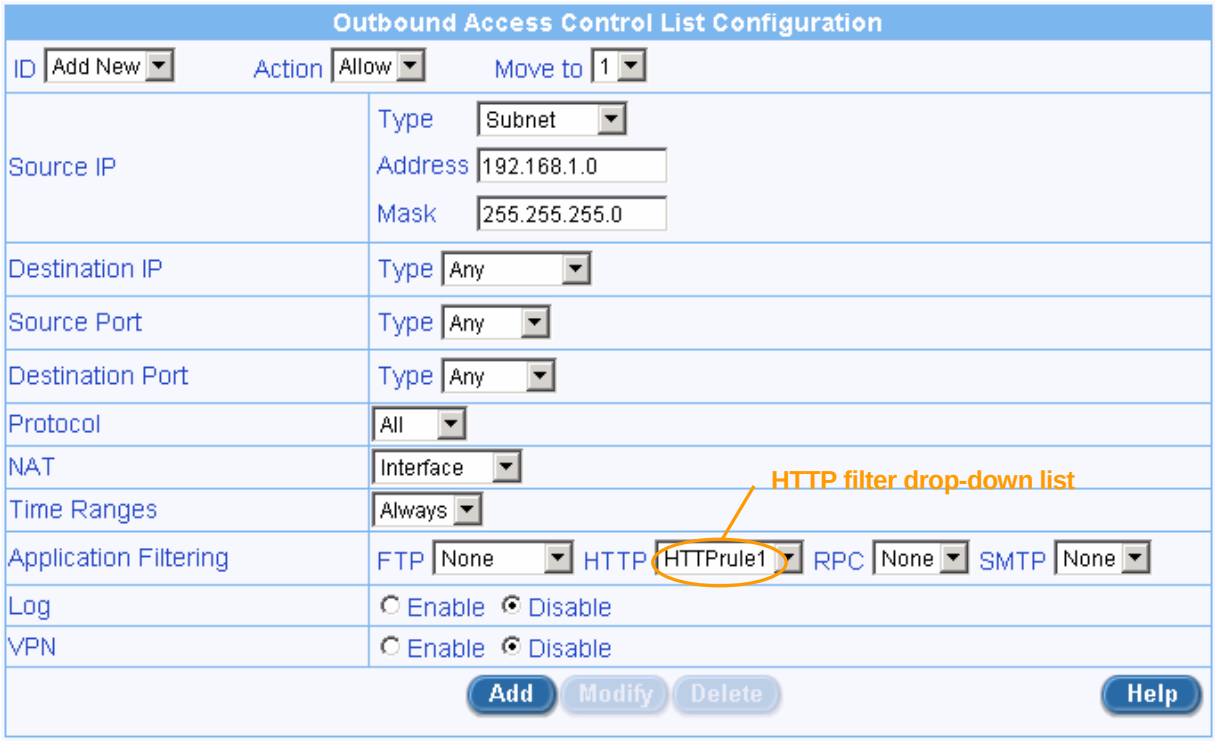


圖 9.22. HTTP 篩檢程式實例– 聯合 HTTP 篩檢程式規則至 ACL 規則

9.8.1.4 修改應用程式篩檢程式

想要修改 IP 域，請參考下列步驟：

1. 打開應用程式篩檢程式設定頁面（請參考第**錯誤! 找不到參照來源。**節 訪問應用程式篩檢程式設定頁面 –（防火牆 ➔ 規則列表 ➔）。

2. 選擇要修改的應用程式篩檢程式，點選應用程式篩檢程式列表中將要修改的應用程式過濾器的 圖示，或者從篩檢程式類型下拉表中選擇篩檢程式類型，然後從篩檢程式規則下拉表中選擇篩檢程式規則。
3. 對下列欄目做您想要的修改：Port number, logging option 等。
4. 點選 Modify 按鈕以保存新的設定。應用程式篩檢程式的新的設定將顯示在應用程式篩檢程式列表中。

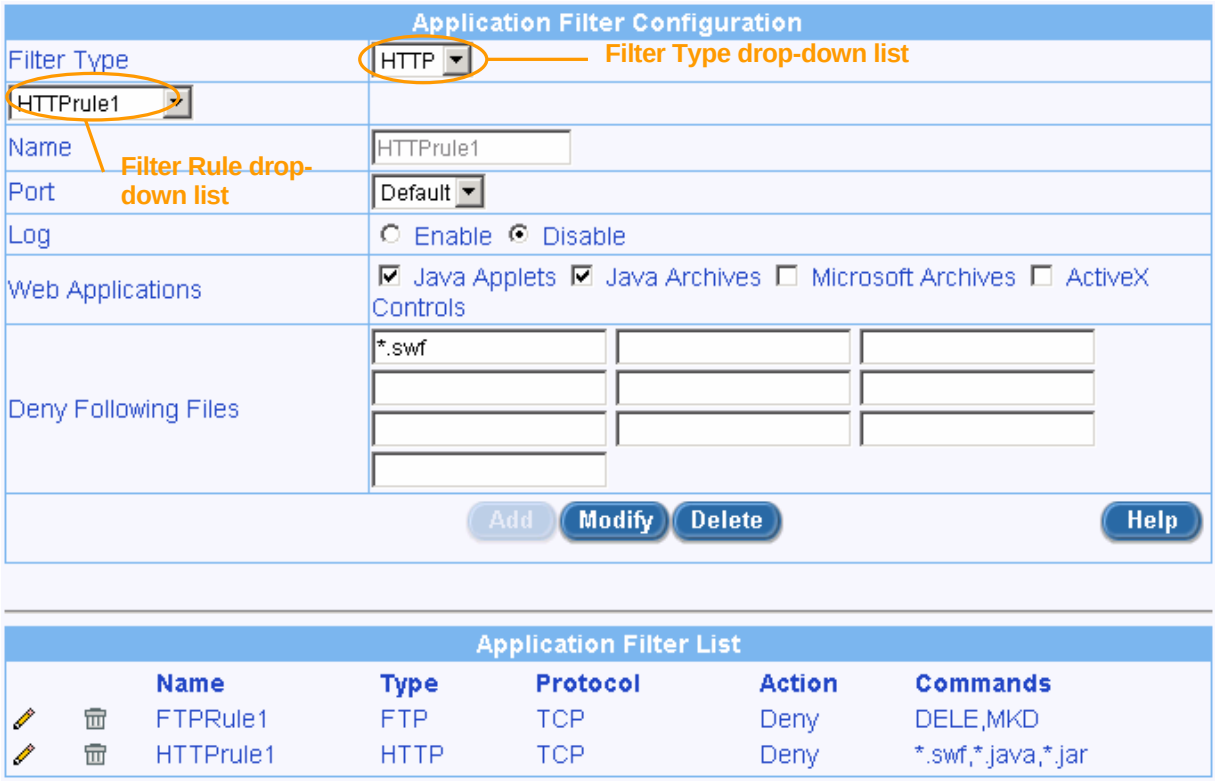


圖 9.23. 修改應用程式篩檢程式

9.8.1.5 刪除應用程式篩檢程式

想要刪除應用程式篩檢程式，請點選待刪篩檢程式前面的 圖示，並參考下列步驟：

1. 打開應用程式篩檢程式設定頁面（請參考第**錯誤! 找不到參照來源。**節 訪問應用程式篩檢程式設定頁面 – （防火牆 ➔ 規則列表 ➔））。
2. 選擇要刪除的應用程式篩檢程式，點選應用程式篩檢程式列表中將要刪除的應用程式篩檢程式的 圖示，或者從篩檢程式類型下拉表中選擇篩檢程式類型，然後從篩檢程式規則下拉表中選擇篩檢程式規則。
3. 點選 Delete 按鈕以刪除篩檢程式。

9.8.2 設定 IP 位址池

9.8.2.1 IP 位址池設定參數

表 9.9 說明了IP位址池可供使用的設定參數。

表 9.9. IP 位址池設定參數

選項	說明
IP Pool Name	輸入本地 IP 名字。
IP Pool Type	選擇 IP 位址池的類型。
IP Range	本選項允許您設定 IP 位址的範圍。
Start IP	輸入 IP 範圍的起始位址。
End IP	輸入 IP 範圍的終止位址。
Subnet	本選項允許您把所有連線到 IP 子網的電腦都包括進來。
Subnet Address	輸入合適的 IP 位址。
Subnet Mask	輸入相應的遮罩。
IP Address	本選項允許您設定單一的 IP 位址。
IP Address	輸入 IP 位址。

9.8.2.2 修改 IP 位址池

想要修改 IP 位址池，請參考下列步驟：

1. 打開 IP 位址池設定頁面（請參考第**錯誤! 找不到參照來源。** 節**錯誤! 找不到參照來源。**）。
2. 從 IP 位址池下拉表中選擇 IP 位址池，或者點選 IP 位址池列表中需要修改的 IP 位址池 圖示。
3. 更改下列任一或所有欄目： 位址池 name、位址池 type 和 IP address。
4. 點選 Modify 按鈕以保存更改。新的設定同時在 IP 位址池列表中出現。

9.8.2.3 刪除 IP 位址池

想要刪除 IP 位址池，請點選待刪 IP 位址池前面的 圖示，或者參考下列步驟：

1. 打開 IP 位址池設定頁面（請參考第**錯誤! 找不到參照來源。** 節**錯誤! 找不到參照來源。**）。
2. 點選待刪 IP 位址池列表前面的 圖示，或者從 IP 位址池下拉表中選擇 IP 位址池。
3. 點選 Delete 按鈕以刪除 IP 位址池。

9.8.2.4 IP 位址池實例

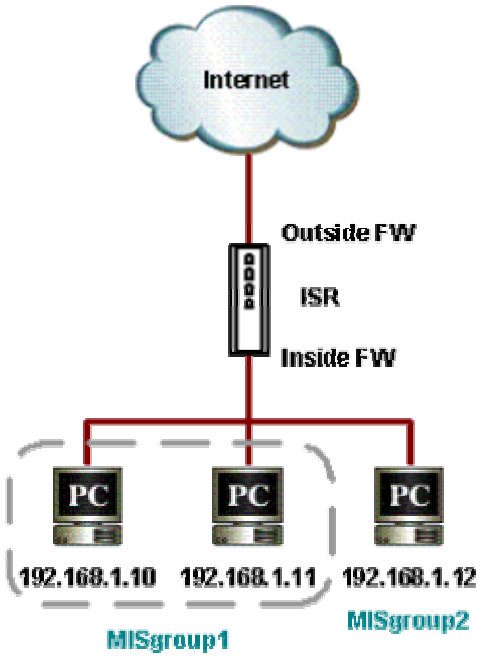


圖 9.24.網路診斷對 IP 位址池的設定

1. 打開 IP 位址池設定頁面以建立兩個 IP 位址池 – 請參看圖 9.25。

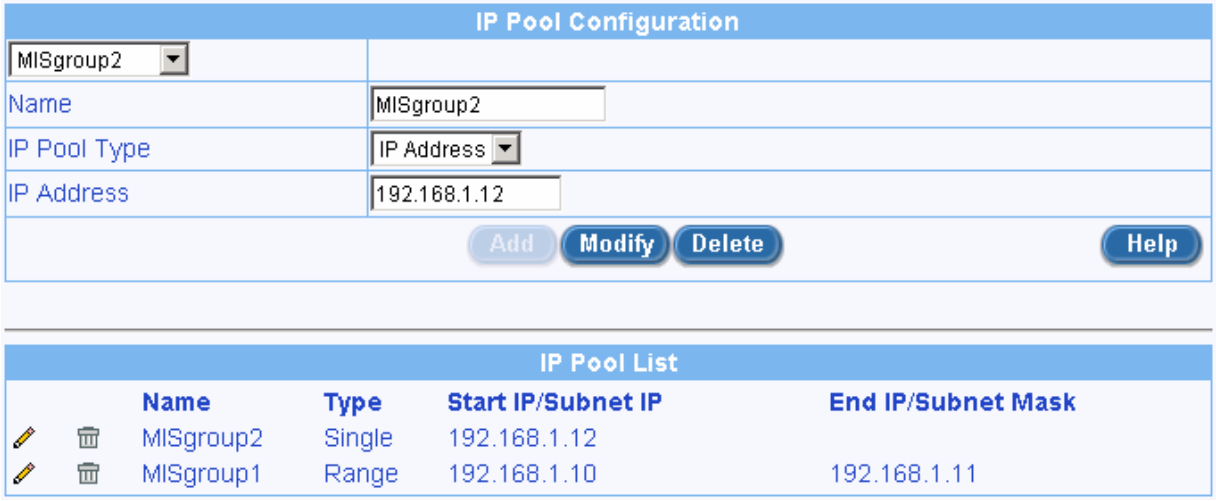


圖 9.25. IP 位址池實例 – 增加兩個 IP 位址池 – MISgroup1 和 MISgroup2

2. 透過從來源 IP 類型下拉表中選擇"IP 位址池"，把 IP 位址池聯合到防火牆 ACL 規則 – 入站、出站或者群組 ACL，然後從 IP 位址池下拉表中選擇 IP 位址池。在這個實例，IP 位址池被用來與來源 IP 相聯合；另外，它還可被用來與目的地 IP 聯合。正如圖 9.26，MISgroup1 不允許玩網路遊戲，Quake-II 何時都行。

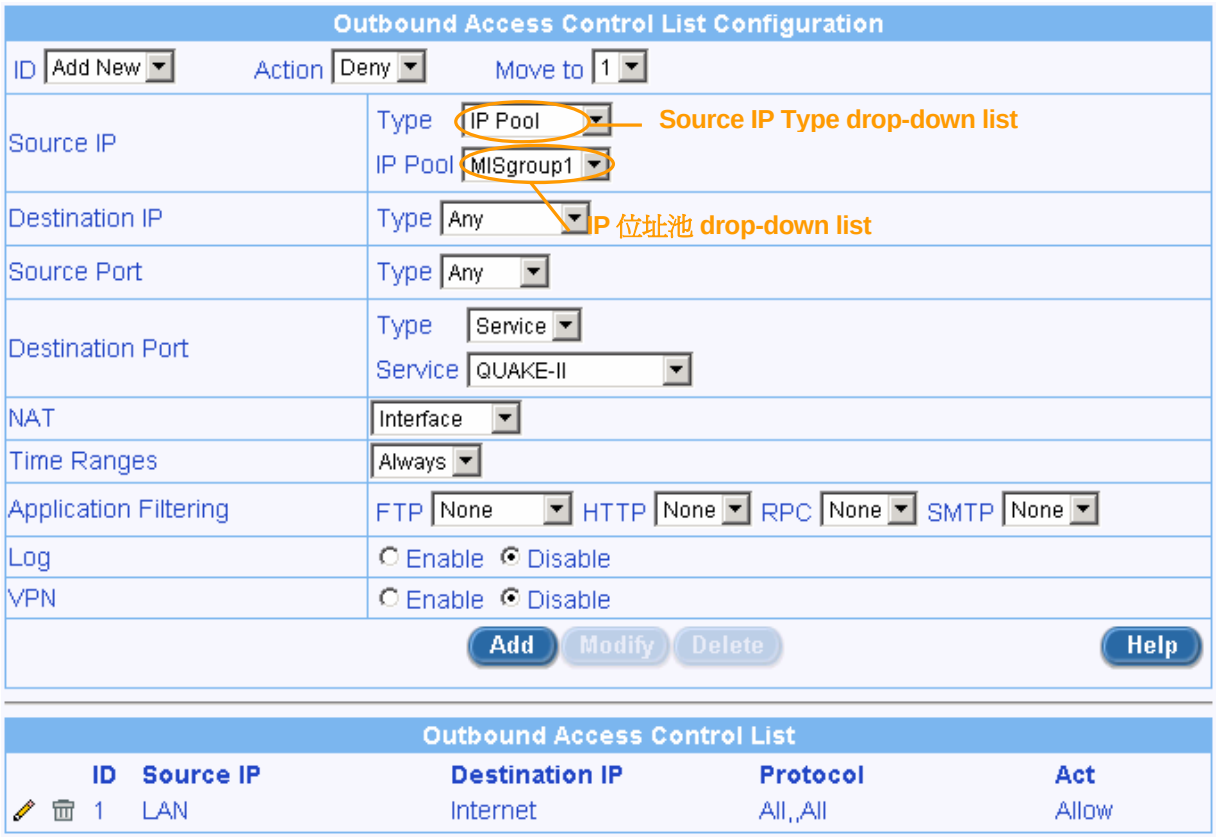


圖 9.26. IP 位址池實例 – 拒絕 QUAKE-II 與 MISgroup1 的連線

9.8.3 設定 NAT 位址池

9.8.3.1 NAT 位址池設定參數

表 9.10 說明了NAT位址池可供使用的設定參數。

表 9.10. NAT 位址池設定參數

選項	說明
NAT Pool Name	輸入NAT位址池的名字。
NAT Pool Type	選擇NAT位址池的類型並建立合適的IP位址的條目。
Static 選擇 NAT 類型以設定網際網路位址與外部位址之間一對一的映射。	
LAN IP range	爲網際網路位址而設
Start IP	輸入起始的IP位址。
End IP	輸入終止的IP位址。
Internet IP Range	爲外部位址而設
Start IP	輸入起始的IP位址。
End IP	輸入終止的IP位址。

選項	說明
Dynamic 選擇本 NAT 類型以對應一套從內部（企業）電腦到公共IP位址的映射。請確保LAN IP範圍與網際網路IP範圍如上所述。	
Overload 選擇本 NAT 類型以使用單一的公共IP位址來連接多個內部（LAN）電腦到外部（網際網路）網路。	
NAT IP Address	對於overload，輸入NAT IP位址。

9.8.3.2 增加 NAT 位址池

想要增加 NAT 位址池，請參考下列步驟：

1. 打開 NAT 位址池設定頁面（請參考第 9.7.3.2 節**錯誤! 找不到參照來源。**）。
2. 在 NAT 位址池下拉表中選擇"**Add New Pool**"。
3. 在名稱欄目中輸入一個位址池名。
4. 從類型下拉表中選擇一個位址池類型。
5. 如果選擇的是 "Static" 或者 "Dynamic" 位址池類型，輸入起始的 IP 位址和終止的 IP 位址，並對應起始的 IP 位址和終止的 IP 位址映射。如果選擇的是 "Overload" 位址池類型，輸入 NAT IP 位址。如果您想使用與 NAT IP 位址一樣爲 WAN 埠指定的 IP 位址，選擇 Interface 位址池類型。
6. 點選 Add 按鈕以建立新的 NAT 位址池。新的 NAT 位址池同時在 NAT 位址池列表中出現。

9.8.3.3 修改 NAT 位址池

想要修改 NAT 位址池，請參考下列步驟：

1. 打開 NAT 位址池設定頁面（請參考**錯誤! 找不到參照來源。 錯誤! 找不到參照來源。**）。
2. 從 NAT 位址池下拉表中選擇 NAT 位址池，或者點選 NAT 位址池列表中需要修改的 NAT 位址池 圖示。
3. 更改下列任一或所有欄目： 位址池 name, 位址池 type 和 IP address。
4. 點選 Modify 按鈕以保存更改。新的設定同時在 NAT 位址池列表中出現。

9.8.3.4 刪除 NAT 位址池

想要刪除 NAT 位址池，請點選待刪 NAT 位址池前面的 圖示，或者參考下列步驟：

1. 打開 NAT 位址池設定頁面（請參考第 9.7.3.2 節**錯誤! 找不到參照來源。**）。
2. 點選待刪 NAT 位址池列表前面的 圖示，或者從 NAT 位址池下拉表中選擇 NAT 位址池。
3. 點選 Delete 按鈕以刪除 NAT 位址池。

9.8.3.5 NAT 位址池實例

圖 9.27 顯示了網路診斷的 NAT 位址池實例。

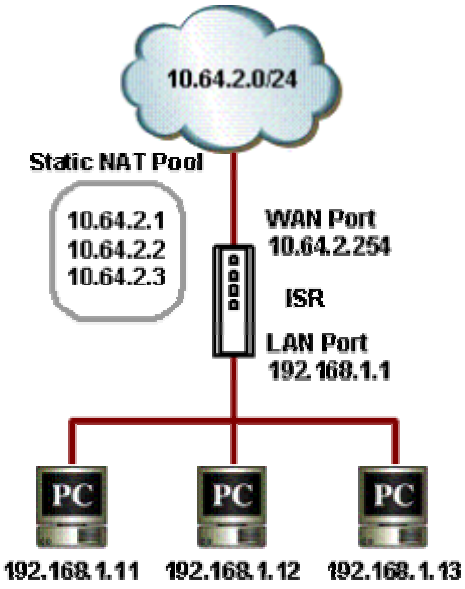


圖 9.27. 網路診斷 NAT 位址池實例

1. 爲靜態 NAT 建立 NAT 位址池 – 參看圖 9.28。

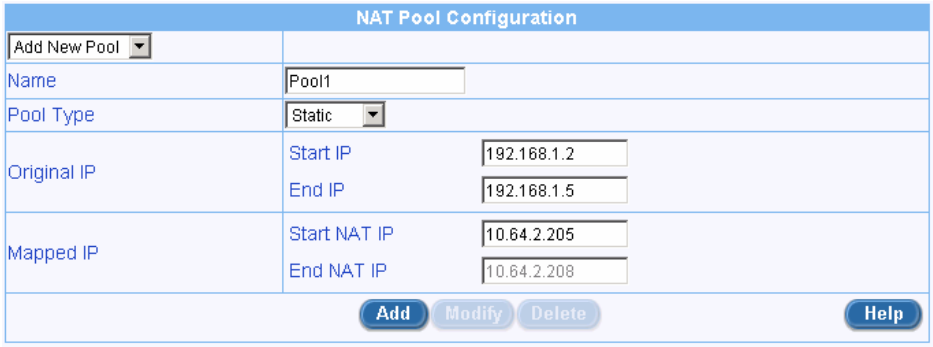


圖 9.28. NAT 位址池實例 – 建立靜態 NAT 位址池

2. 透過從 NAT 類型下拉表中選擇“NAT 位址池”，把 NAT 位址池聯合到出站 ACL 規則，然後從 NAT 位址池下拉表中選擇現有的 NAT 位址池。

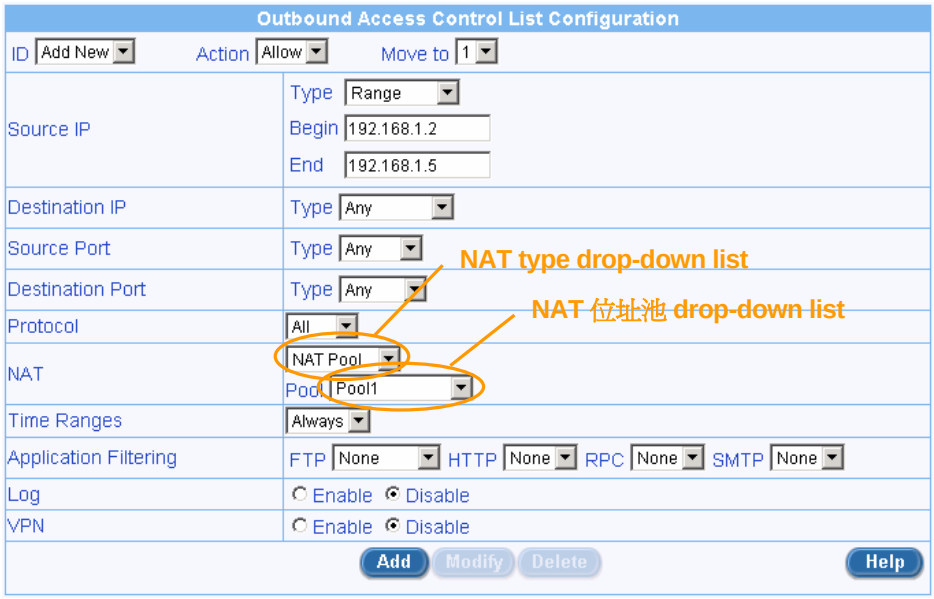


圖 9.29. NAT 位址池實例–聯合 NAT 位址池 ACL 規則

9.8.4 設定時間範圍

爲與 ACL 規則建立永久性的聯繫，您可利用本項目來設定訪問時間範圍。與時間範圍相聯合的 ACL 規則將只在預定的時段內有效。如果 ACL 規則在從 10:00hrs 到 18:00hrs 之間拒絕了 HTTP 訪問，那麼，在 10:00hrs 之前和 18:00hrs 之後，HTTP 流量將允許透過。一個時間範圍能包含三個時間段。例如：

工作日的辦公時間可能包含下列時間段：

- 9:00 到 13:00 Hrs 之間的午餐前時間段
- 14:00 到 18:30 Hrs 之間的午餐後時間段

周末的辦公時間可能包含下列時間段：

- 從 9:00 到 12:00 Hrs

這個變動的時間段能設定成單一的時間範圍。訪問規則可在時間段的基礎上啓動。

9.8.4.1 時間範圍設定參數

表 9.11 說明了可供時間範圍使用的設定參數。

表 9.11. 時間範圍設定參數

選項	說明
Time Range drop-down list	選擇 "Add New Time Range" 以增加新的時間範圍或從下拉表中選擇現有的時間範圍。
Time Range Name	爲時間範圍輸入名字。
Schedule drop-down list	選擇 "Add New Schedule" 以增加新的日程表或從下拉表中選擇日程表。
Days of Week	爲日程表設定天數。
Time (hh:mm)	爲日程表以hh:mm格式設定時間窗口。

9.8.4.2 增加時間範圍

想要增加時間範圍，請參考下列步驟：

1. 打開時間範圍設定頁面（請參考第 9.7.4.2 節**錯誤! 找不到參照來源。**））。
2. 在時間範圍下拉表中選擇"**Add New Time Range**"。
3. 在時間範圍名稱欄目中輸入一個網域名稱。
4. 在日程表下拉表中選擇 "**Add New Schedule**"。
5. 選擇一周內的某天。例如，從周日到周六。
6. 輸入一天中的時間段。例如，從 08:00 到 18:00。
7. 點選 Add 按鈕以建立新的日程表。

9.8.4.3 修改時間範圍

想要修改時間範圍，請參考下列步驟：

1. 打開時間範圍設定頁面（請參考**錯誤! 找不到參照來源。 錯誤! 找不到參照來源。**））。
2. 從時間範圍下拉表中選擇時間範圍，或者點選時間範圍列表中需要修改的時間範圍的 圖示。
3. 從時間範圍下拉表中選擇日程表。
4. 更改下列任一或所有欄目： Days of week and hours。
5. 點選 Modify 按鈕以保存新的設定。

9.8.4.4 刪除時間範圍

想要刪除時間範圍，請點選待刪時間範圍前面的 圖示。

9.8.4.5 在時間範圍內刪除日程表

想要在時間範圍內刪除日程表，請參考下列步驟：

1. 打開時間範圍設定頁面（請參考第 9.7.4.2 節**錯誤! 找不到參照來源。**））。
2. 點選待刪時間範圍列表前面的 圖示，或者從時間範圍下拉表中選擇時間範圍。
3. 從下拉表中選擇日程表。
4. 點選 Delete 按鈕以刪除日程表。

9.8.4.6 時間範圍實例

1. 建立時間範圍 – 請參看圖 9.28。

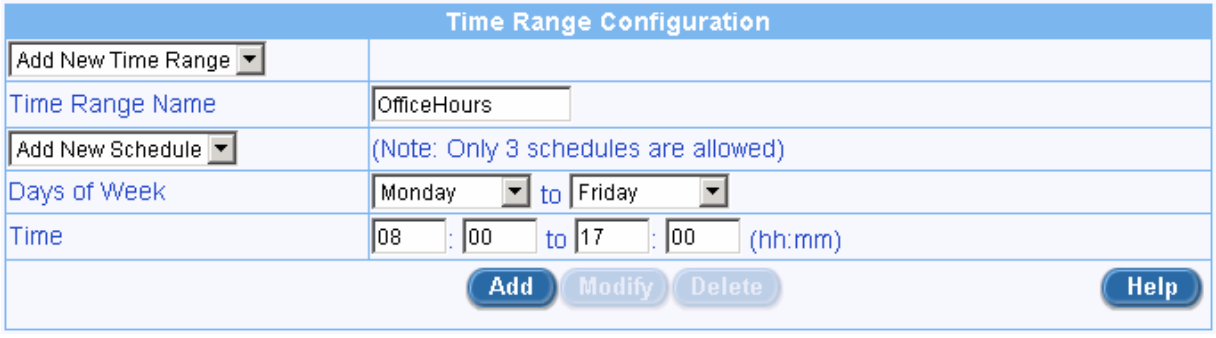


圖 9.30. 時間範圍實例 – 建立時間範圍

2. 透過從時間範圍下拉表中選擇現有的時間範圍，將時間範圍聯合到出站 ACL 規則。圖 9.31 顯示了 MISgroup1 在辦公時間內拒絕了 FTP 訪問。

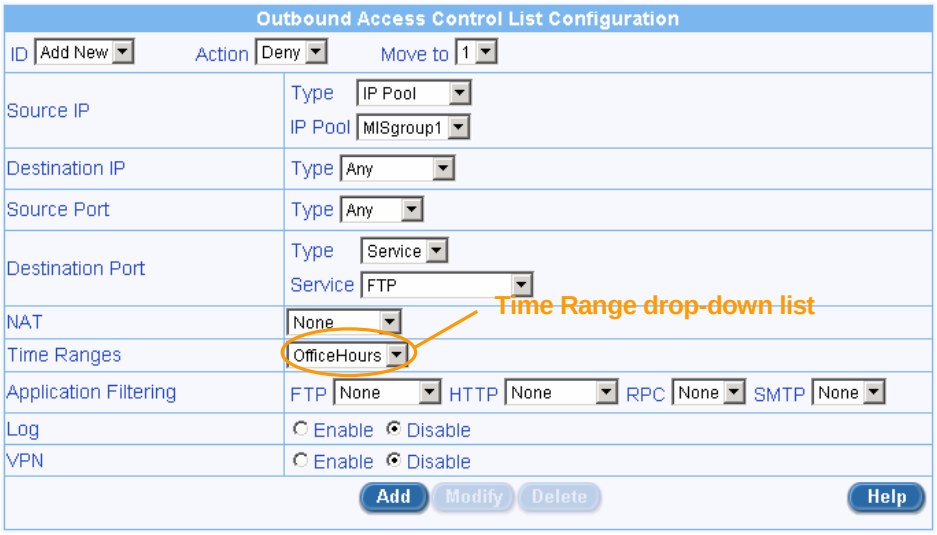


圖 9.31. 時間範圍實例 – 爲 MISgroup1 在辦公時間內拒絕 FTP 訪問

9.9 防火牆統計表 – 防火牆 ➔ 統計表

防火牆統計表頁面說明了關於活動連線的細節內容。圖 9.32 顯示了一個典型的防火牆對活動連線的統計表。要想參看已更新的統計表，點選 Refresh 按鈕。

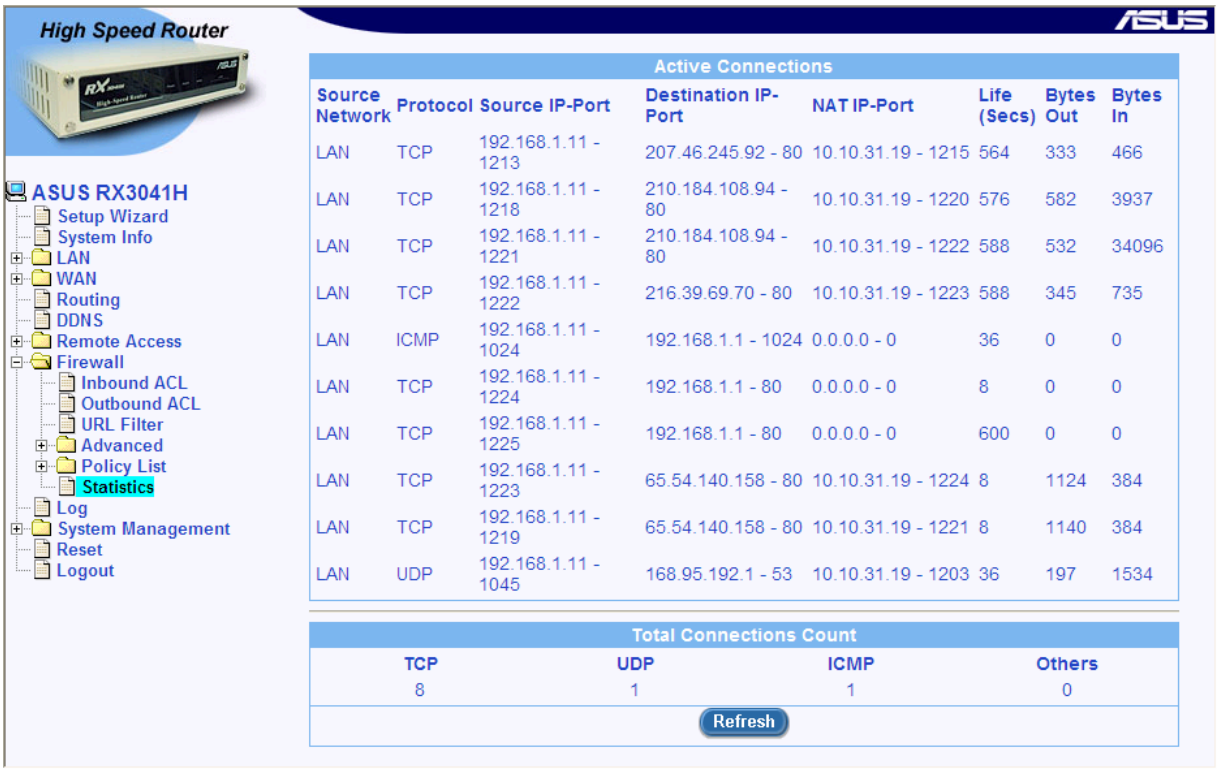


圖 9.32. 防火牆活動連線統計表

10 設定遠端存取

10.1 遠端存取

網際網路安全路由器防火牆允許遠距離工作者們利用以群組、用戶與訪問規則爲基礎的遠端存取機制安全地訪問企業內部網路。每個群組都與屬於群組的用戶登入之後啓動的一套訪問原則相關聯。網際網路安全路由器保留了爲遠端存取群組定義的訪問規則細節。這些訪問列表定義了遠端用戶被允許訪問的資源和應用到所有群組用戶的休止時間。

當屬於某群組的用戶透過網際網路或本地網路登入，網際網路安全路由器防火牆啓動了與群組想關聯的訪問規則，並建立了與用戶相關聯的動態規則。這些動態規則可資每個與用戶的連線參考。一旦用戶脫離了網際網路安全路由器或以防休止時間的來臨，它們將被刪除。

一個典型的爲遠端存取進行的設定包括下列舉措：

- 增加/修改/刪除新用戶群組和群組用戶的資訊（包括用戶名、密碼等）。
- 對於 VPN 遠端存取，每個遠端存取用戶都需要指派虛擬 IP 位址。
- 增加/修改/刪除群組訪問規則。

10.2 管理用戶群組以及用戶

遠端存取選項允許您設定用戶和群組。

10.2.1 用戶群組設定參數

表 100.1說明了可供遠端存取用戶群組以及用戶使用的設定參數。

表 100.1. 用戶群組設定參數

選項	說明
User Group	
User Group Drop-down list	選擇 “Add New User Group” 以增加新的群組或從下拉表中選擇一個現有的群組。
User Group Name	爲您將要增加的群組輸入一個獨有的用戶群組名。
Group State	點選Enable 或 Disable 按鈕以開啓或關閉群組。關閉群組將迫使所有的用戶從已登入的用戶群組中斷開。所有用戶的進一步註冊將被關閉。開啓群組將允許所有的群組用戶登入。
Inactivity Timeout	輸入終止的時間段長度，當無資訊流經連線時，此長度將被用來刪除與用戶相關的會議。
User	
User Drop-down list	選擇 “Add New User” 以增加新的用戶或從下拉表中選擇一個現有的用戶。

選項	說明
User Name	爲您將要增加的群組輸入一個獨有的用戶名。
User State	點選Enable 或 Disable 按鈕以開啓或關閉用戶。關閉用戶將迫使用戶斷開。那個特定用戶的進一步註冊將被關閉。開啓用戶將允許那個特定用戶登入。
Password	輸入用戶密碼。

10.2.2 增加用戶群組與/或用戶

想要增加用戶群組與新用戶，請參考下列步驟：

1. 打開用戶群組設定頁面（請參考第 10.2.2 節**錯誤! 找不到參照來源。**）。
2. 從用戶群組下拉表中選擇 “**Add New User Group**” 。
3. 在用戶群組名稱欄目中輸入一個名字。請確認此名字在現有的群組中無重名。注意，群組名字 is case sensitive。例如， Group1 與 group1 被視作獨立的群組。
4. 在群組狀態欄目中點選 “Enable” 或 “Disable” 按鈕以開啓或關閉本群組。
5. 輸入休止時間段長度。預設的長度爲 300 秒。
6. 如果您想要增加用戶到新建立的群組，請繼續下列步驟；否則，請跳至第 12 步來完成設定。
7. 從用戶下拉表中選擇 “**Add New User**”。
8. 在用戶名稱欄目中輸入一個獨有的名字。
9. 在用戶狀態欄目中點選 “Enable” 或 “Disable” 按鈕以開啓或關閉此用戶。
10. 在密碼欄目中輸入此用戶的密碼。
11. 再次確認用戶密碼。請確認您與上步輸入的是相同的密碼。
12. 點選 Add 按鈕以建立新的群組與新用戶。

想要增加新用戶，請參考下列步驟：

1. 打開用戶群組設定頁面（請參考第 11.2.2 節**錯誤! 找不到參照來源。**））。
2. 從用戶群組下拉表中選擇一個現有的群組。
3. 在用戶下拉表中選擇 “**Add New User**”。
4. 在用戶名稱欄目中輸入一個獨有的名字。
5. 在用戶狀態欄目中點選 “Enable” 或 “Disable” 按鈕以開啓或關閉此用戶。
6. 在密碼欄目中輸入此用戶的密碼。
7. 再次確認用戶密碼。請確認您與上步輸入的是相同的密碼。
8. 點選 Add 按鈕以增加新用戶。

10.2.3 修改用戶群組或用戶

想要修改用戶群組與/或用戶，請參考下列步驟：

1. 打開用戶群組設定頁面（請參考第 11.2.2 節**錯誤! 找不到參照來源。**））。

2. 從用戶群組下拉表中選擇一個現有的群組。如果您只是想修改現有用戶的屬性，請跳至第 4 步。
3. 在群組狀態與/或休止時間欄目中進行您想要的更改。如果您並不想修改現有群組中用戶的屬性請跳至第 6 步。注意，群組名不能作任何更改。要想改變群組名字，您必須首先刪除現有的群組，並用您想要的名字建立一個新的群組。
4. 從用戶下拉表中選擇一個現有的用戶。
5. 在用戶狀態、密碼和密碼確認欄目中進行您想要的更改。注意，用戶名不能作任何更改。要想改變用戶名字，您必須首先刪除現有的用戶，並用您想要的名字建立一個新的用戶。
6. 點選 Modify 按鈕以保存新的設定。

10.2.4 刪除用戶群組或用戶

想要刪除用戶群組，請參考下列步驟：

1. 打開用戶群組設定頁面（請參考第 11.2.2 節**錯誤! 找不到參照來源。**））。
2. 從用戶群組下拉表中選擇一個現有的用戶群組。
3. 點選 Delete 按鈕以刪除此用戶群組。注意，用戶群組只有在所有屬於群組的用戶都被刪除後才能刪除。

想要刪除用戶，您只需點選用戶群組設定頁面遠端用戶表中待刪用戶的 圖示，或參考下列步驟：

1. 打開用戶群組設定頁面（請參考第 11.2.2 節**錯誤! 找不到參照來源。**））。
2. 點選遠端用戶表中待刪用戶的 圖示，或從用戶下拉表中選擇一個用戶。
3. 點選 Delete 按鈕以刪除此用戶。

10.2.5 用戶群組和用戶設定實例

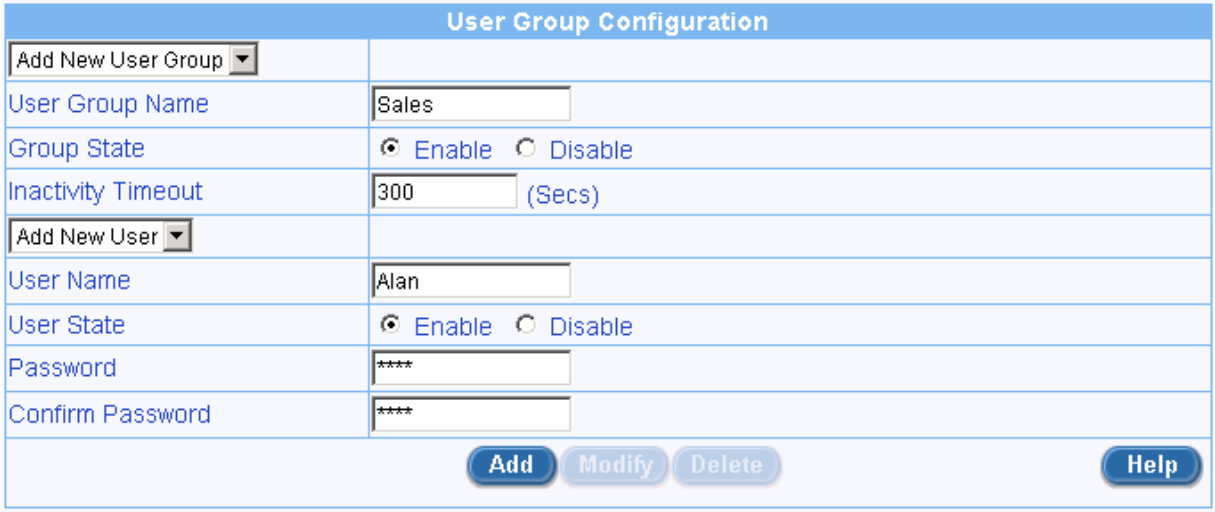


圖 10.1. 用戶群組和用戶設定實例

實例

圖 10.1 顯示了螢幕上的條目：

- 增加新的用戶群組和新用戶

- 群組 “Sales”
- 用戶 “Alan”

10.3 設定群組 ACL 規則

群組 ACL 用來控制本地或遠端群組訪問的特權。除了兩個附加選項（規則類型和群組名字，請參看**錯誤! 找不到參照來源。**）之外，它的設定與防火牆入站/出站 ACL 規則十分類似。關於設定群組 ACL 規則的詳細步驟，請參考第 9.4 或 9.5 節。

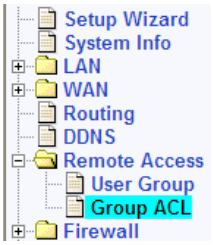
10.3.1 群組 ACL 特殊設定參數

表 10.2 說明了群組 ACL 規則的特殊設定參數。剩下的設定參數與防火牆入站/出站ACL 規則相同。請參考表 9.2 和 表 9.3 以獲得普通設定參數的詳細資訊。

表 10.2. 群組 ACL 特殊設定參數

選項	說明
Type 選擇本規則所應用的流量的類型。	
Inbound	若規則爲入站資訊設定時請選擇此項。
Outbound	若規則爲出站資訊設定時請選擇此項。
Group 從群組下拉表中選擇本規則應用的物件。注意，想要設定群組ACL規則，必須先設定好用戶群組。請參考第 **錯誤! 找不到參照來源。** 節來進行用戶群組設定。	

10.3.2 新增群組的 ACL 規則 Add a Group ACL



請依照下列介紹來新增一組群組 ACL 規則:

4. 藉由點選 **Firewall ➔ Remote Access ➔ Group ACL** 選單的方式來開啓時間範圍設定頁面。
5. 自下拉式選單中選擇 “**Add New**” 。
6. 從“**Action**”下拉式選單中設定您所要進行設定的動作 (Allow 或 Deny)。
7. 從規則類型的下拉式選單中選擇 Outbound 或 Inbound 規則。
8. 從群組下拉式選單中選擇一個群組。
9. 從以下欄位中進行變更設定: 來源/目的地 IP, 來源/目的地連接埠, 通訊協定, NAT, 時間範圍, 應用程式過濾, 與 登錄。 請參閱 表 9.2 中關於這些欄位的解釋。圖 9.10 是表示如何建立一規則來自 IP 位址 192.168.1.15 的主機拒絕一出埠 HTTP 傳輸。

圖 10.2. 群組 ACL 設定範例

10. 藉由從下拉式選單中的"**Move to**"選項來指定一組規則的優先順序。請注意！選單中的數字代表優先順位的高低，其中數字 1 代表優先順序最高者。優先順序越高者將比優先順序越低者較先受到防火牆的檢查。

11. 點選 Add 按鍵以建立一組新的 ACL 規則。新的 ACL 規則將會被顯示在 ACL 設定頁面下方的 ACL 群組列表中。

圖 10.3. ACL 群組列表

10.3.3 修改 ACL 群組規則

請依照下列介紹來修改 ACL 群組規則:

12. 藉由點選手動 **Firewall ➔ Remote Access ➔ Group ACL** 選單來開啓時間範圍設定頁面。

13. 請點選 圖示來修改 ACL 列表中的規則，或是從下拉式選單中的"**ID**"項目來選擇規則所代表的號碼。

14. 在以下各欄位中進行您所要進行的設定: 動作, 群組規則類型, 群組, 來源/目的地 IP 位址, 來源/目的地連接埠, 通訊協定, NAT, 時間範圍, 應用程式過濾, 與登錄。請參考表 9.2 與表 10.2 中針對這些欄位的解釋。

15. 點選 Modify 按鍵來變更此一 ACL 規則。針對此一 ACL 規則的新設定將會顯示在 ACL 群組設定頁面下半部的 ACL 群組列表中。

10.3.4 刪除 ACL 群組規則

如欲刪除 ACL 群組規則，您只要依照下列指示點選規則前方的 圖示即可進行刪除。:

16. 藉由點選 **Firewall ➔ Remote Access ➔ Group ACL** 選單來開啓時間範圍設定頁面。

17. 點選規則中的 圖示來刪除 ACL 群組列表中的規則，或是從下拉式選單中的"**ID**" 項目選擇代表規則的號碼。

18. 點選 Delete 按鍵來刪除此一 ACL 規則。請注意！被刪除的 ACL 規則將會自設定頁面下半部的 ACL 群組列表中刪除。

10.3.5 顯示既有的 ACL 規則

如欲查看既有的 ACL 規則，您只要藉由點選開啓 **Firewall ➔ Remote Access ➔ Group ACL** 選單來開啓 ACL 群組設定頁面。

10.4 遠端用戶登入步驟

對於屬於某個用戶群組連線到路由器上的用戶而言，他/她必須首先進行特別的登入以啓動用戶群組規則；否則，路由器將拒絕所有用戶的連線請求。爲登入路由器和啓動有關的訪問原則，某個用戶群組的用戶可在瀏覽器內輸入下列 URL。

http://<IP Address>/login

登入控制臺將出現，如圖 10.4 所示

圖 10.4. 登陸控制臺

在成功登入之後，螢幕將如圖 10.5 所示。

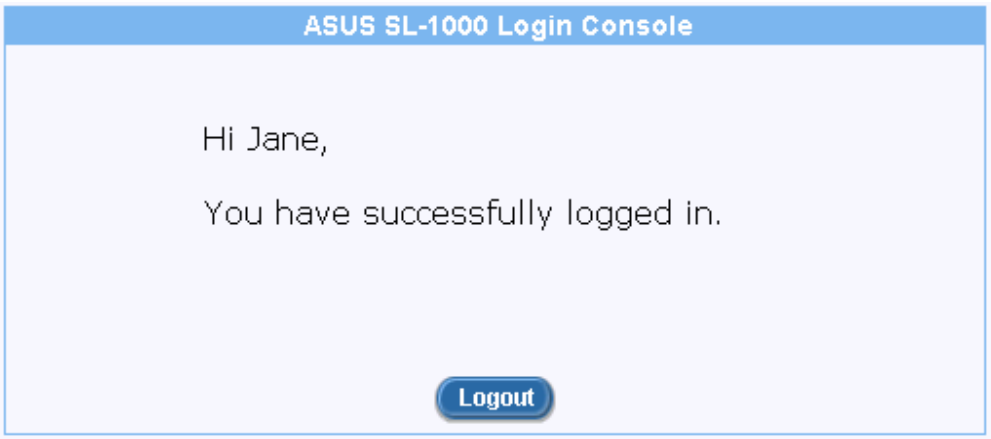


圖 10.5. 登入狀況螢幕

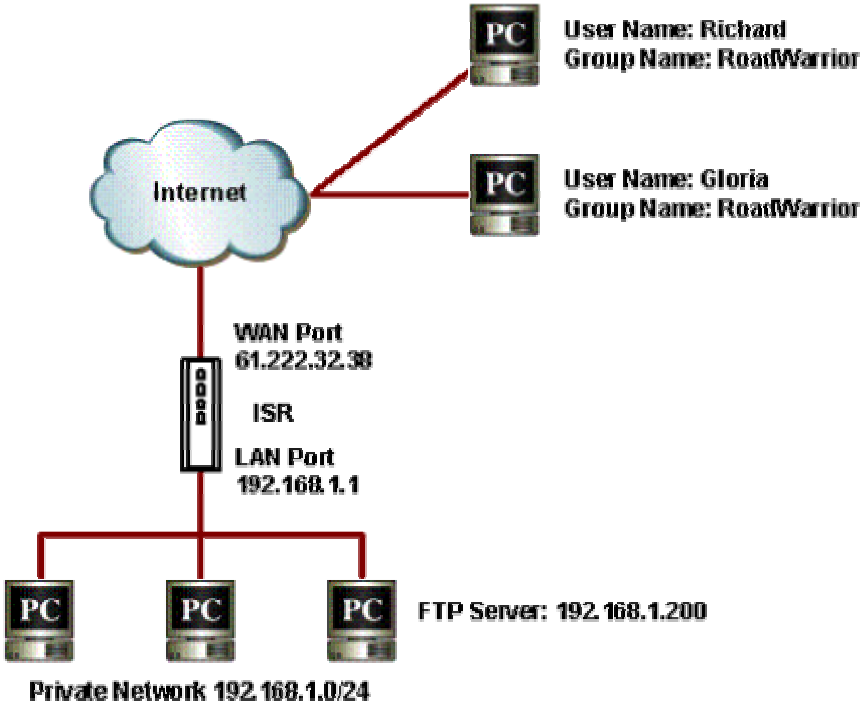


圖 10.6. 對入站遠端存取進行的網路診斷

10.5 爲遠端存取設定防火牆

遠端存取常被用來支援企業的移動用戶訪問公司的網路而不犧牲掉安全性。遠端存取所需要的設定路由器的步驟最好由一個實例來解釋。下文說明了遠端用戶 Richard 和 Gloria 訪問處於被保護的網路（例如公司區域網路）之內的 FTP 伺服器時對路由器進行設定所需要的步驟。圖 10.6 顯示了對此實例進行的網路診斷。

1. 如需要建立遠端存取用戶和群組。圖 10.7 說明了建立一個新用戶 Gloria 的過程。想要知曉關於如何爲遠端存取增加新用戶與/或新用戶群組更多細節，請參考第**錯誤! 找不到參照來源。**節 **錯誤! 找不到參照來源。**。

User Group Configuration

RoadWarrior	
User Group Name	RoadWarrior
Group State	Enable / Disable
Inactivity Timeout	300 (Secs)
Add New User	
User Name	Gloria
User State	Enable / Disable
Password	****
Confirm Password	****

Add | Modify | Delete | Help

Remote User List

	User Name	Group Name	Logged in from	State
	Jane	Group1	None	Enabled
	Jim	Group1	None	Enabled
	John	Group2	None	Enabled
	Richard	RoadWarrior	None	Enabled

圖 10.7. 用戶與用戶群組設定實例

Group Access Control Configuration

ID: Add New | Action: Allow | Type: Inbound | Group: Group1 | Move to: 1

Source IP	Type: WAN
Destination IP	Type: IP Address IP Address: 61.222.32.38
Source Port	Type: Any
Destination Port	Type: Service Service: FTP
NAT Type	Type: IP Address IP Address: 192.168.1.200
Time Range	Always
Application Filters	FTP: None HTTP: None RPC: None SMTP: None
Log	Enable / Disable
VPN	Enable / Disable

Add | Modify | Delete | Help

圖 10.8. 群組 ACL 設定實例

2. 建立入站群組 ACL 規則（請參看圖 10.8）以允許遠端存取用戶 Richard 和 Gloria 訪問企業網路內的 FTP 伺服器。
3. 遠端用戶 Richard 和 Gloria 可在瀏覽器內輸入下列 URL，以登入到路由器上訪問 FTP 伺服器：

http://61.222.32.38/login

11 系統管理

本章說明了您可利用設定管理器完成的管理任務：

- 設定系統服務
- 修改密碼
- 修改系統資訊
- 修改系統日期和時間
- 重新設定、備份和保存系統設定
- 升級韌體
- 退出設定管理器

您可從系統管理功能表訪問這些任務。

11.1 設定系統服務

如圖 11.1 所示，您可使用系統服務設定頁面來開啓或關閉網際網路安全路由器支援的服務功能。所有的服務, 防火牆, VPN, DNS, DHCP 和 RIP 都在這裏被開啓。想要關閉或開啓個人服務，請參考下列步驟：

1. 以管理員身份登入設定管理器，點選 **System Management** 功能表，然後點選 **System Services** 子功能表。系統服務設定頁面將如圖 9.9 所示。
2. 點選相應的“Enable” 或 “Disable” 按鈕以開啓或關閉您想要的服務。
3. 點選 Apply 按鈕以保存修改。

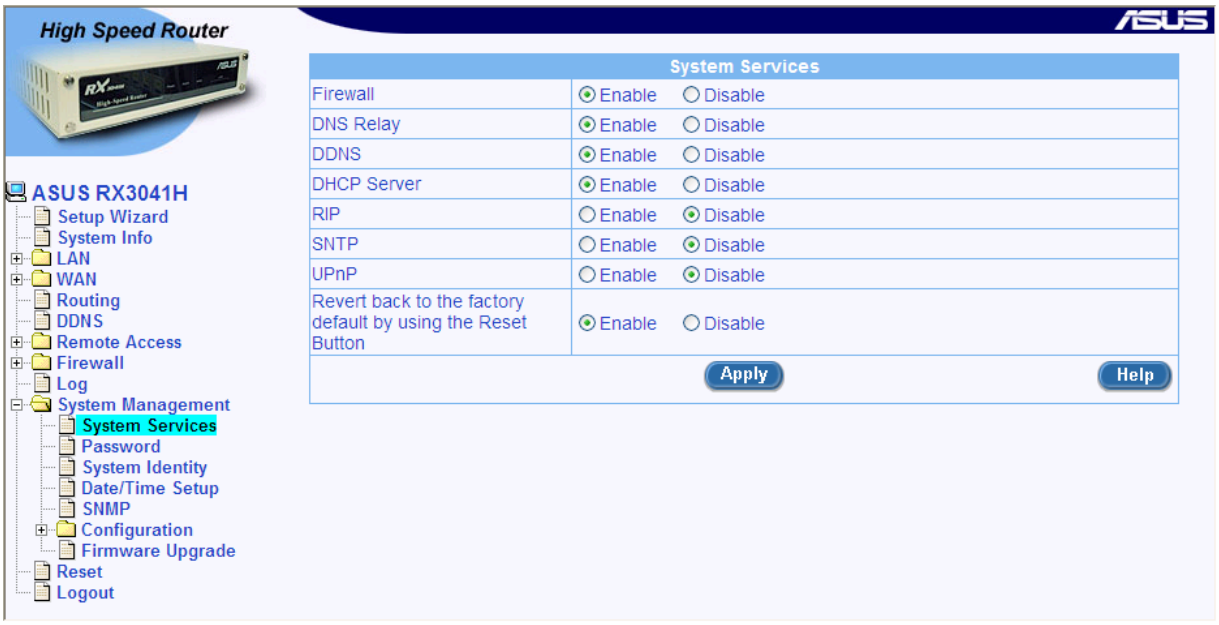


圖 11.1. 系統服務設定頁面

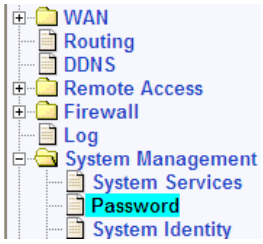
11.1.1 變更登入密碼

當您第一次登入設定管理員，您可以使用預設的使用者名稱與密碼:admin 與 admin 。系統會允許兩種使用者登入，分別爲系統管理員（administrator: username:admin）與訪客（guest:username:guest）。其中系統管理員具有權力去修改設定，而訪客則只能檢視系統設定。至於這兩組使用者的密碼則爲 admin 與 guest，系統管理員可針對密碼進行變更。


Note

此處的使用者名稱與密碼只用來登入設定管理員之用，此一帳號密碼與您用來與 ISP 連線的帳號密碼不同。

請依照下列步驟來變更密碼:



4. 藉由點選 **System Management ➔ Password** 選單來開啓密碼設定頁面。
5. 輸入既有的密碼在 **Login Password** 欄位。
6. 在 **New Password** 欄位輸入新的密碼，並在 **Confirm New Password** 欄位重新輸入一次密碼。

   密碼可以是十六位數字，當您登入時，您必需在上方與下方的欄位輸入新的密碼。

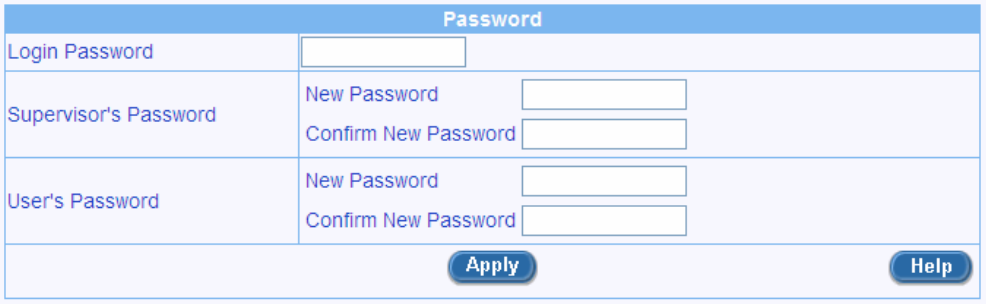


圖 11.2. 密碼設定

7. 點選 Apply 按鍵來儲存新的密碼。請注意只有在密碼輸入正確並在正確的欄位才會生效。

11.1.2 設定管理站

有時候，您可能想要限制主機對路由器進行設定。在預設值中，只要輸入的帳號與密碼正確，則可讓系統管理員從任何電腦登入。這樣的作法可讓未經認證者在知道設定管理員介面的帳號與密碼的情況下進行登入。在此設定頁面中您可利用輸入單一 IP 位址、IP 位址範圍或網路位址與子網路遮罩，最多設定八組的管理站。


WARNING

若管理站群組未經設定，則管理員可從任何地方登入路由器。然而，若有一組一組或更多的管理站群組被設定，則只有經過設定之特定管理站群組可以設定路由器。若您忘記管理群組的設定，您將無法存取路由器的設定管理員介面，除非按下路由器的重置鍵進行重置。F

管理站參數設定

表 11.1 敘述管理站設定頁面中可進行設定的參數。

表 11.1. 管理站參數設定

欄位	敘述
ID	
Add New	點選此選項來新增一組新的管理群組。
Number	從下拉式選單中選擇管理群組以變更設定。
Address Type 本選項可讓您選擇您要如何指定工管理站群組使用的IP位址。在此共有三種選項可供設定，分別是: IP 位址、範圍與子網路。	
IP Address	本選項可讓您指定管理站的IP位址。
Address	指定一組適當的IP位址。
Range	本選項可讓您從管理站群組指定IP位址範圍。當本選項被選擇，則以下的欄位便可以進行設定:
Begin	輸入起始的IP位址範圍。
End	輸入中止的IP位址範圍。
Subnet	本選項可讓您指定所有連接到相同IP子網路的電腦作爲一管理站群組。當本選項被選擇，則以下的項目便可以加以輸入:
Network Address	輸入適當的IP位址。
Subnet Mask	輸入對應的子網路遮罩。

新增一組管理站群組

請依照以下介紹來新增一組管理站群組:

8. 藉由點選 **System Management ➔ Password** 選單來開啓密碼設定頁面。
9. 從“**ID**”下拉式選單中選取 “**Add New**” 。
10. 在以下三選項選擇 “Address Type”（位址類型） – **IP Address**, **Range** 與 **Subnet** ，接著請輸入您想要輸入的 IP 位址資訊。

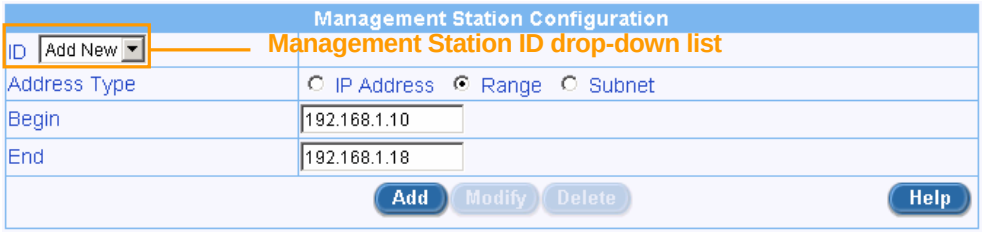


圖 11.3. 管理站設定

11. 點選 Add 按鍵來新增一組新的管理站群組。您將可看到新增的管理站群組摘要顯示在同一設定頁面。

圖 11.4. 管理站摘要

變更管理站群組

請依照以下介紹來變更管理站群組:

12. 藉由點選 **System Management ➔ Password** 選單來開啓密碼設定頁面。
13. 從 **ID** 下拉式選單中選擇一管理群組。
14. 請在"**Address Type**"項目中設定想要進行的變更並輸入對應的 IP 位址資訊。
15. 點選 Modify 按鍵來變更設定。

刪除管理站群組

如欲刪除管理站群組，您只要點選點選選項前的 圖示 (在管理站摘要列表中)即可加以刪除，或是依照以下介紹進行刪除:

16. 藉由點選 **System Management ➔ Password** 選單開啓密碼設定頁面。
17. 從"**ID**"下拉式選單中選擇一組管理群組的號碼。
18. 點選 Delete 按鍵來刪除管理站群組。

11.2 修改系統資訊

如圖 11.5 所示，您可利用系統資訊設定頁面來輸入系統的特定資訊，如系統名稱（對於設備來說的唯一的名稱）、系統位置（設備擺放的位置）以及設備聯繫人的資訊。注意，所有的欄目都只允許字元名稱。當您完成了系統特定資訊的輸入之後，請點選 Apply 按鈕以保存修改。

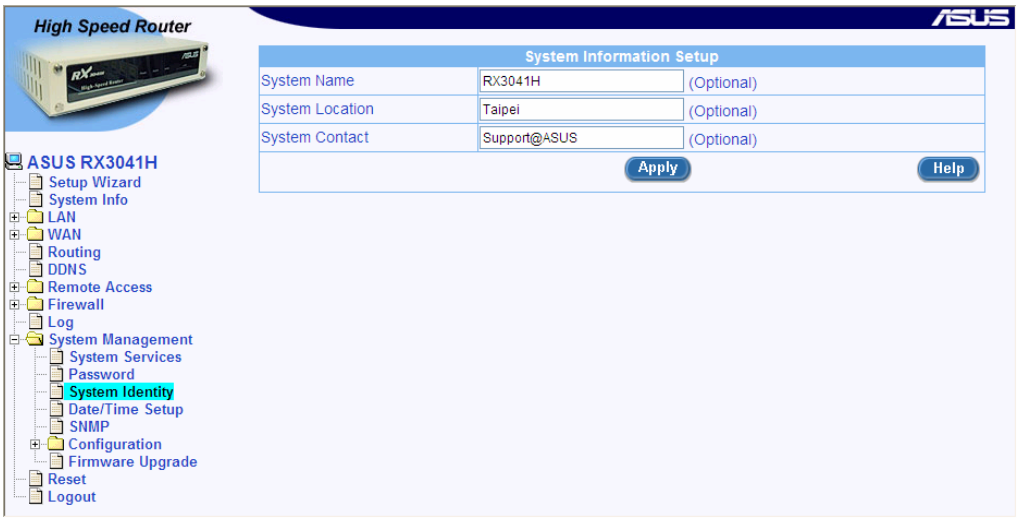
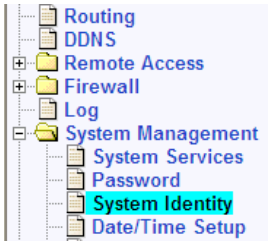


圖 11.5. 系統資訊設定頁面

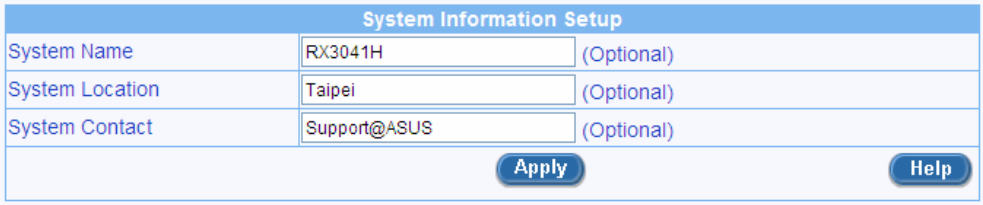
11.3 設定系統辨識

一些特定的系統資訊，像是系統名稱（本裝置的特定名稱）、系統位置（本裝置的所在位置），與在裝置中的個人聯絡資訊都可以在系統辨識設定頁面中進行設定。

請依照以下介紹來變更特定的系統資訊:



19. 藉由點選 **System Management ➔ System Identity** 選單來開啓系統辨識設定頁面。
20. 變更系統名稱、系統位置與聯絡資訊等想要進行的設定。請注意！在此欄位中，您可輸入任何數字字母。
21. 點選 Apply 按鍵來儲存設定值。



11.4 設定時間與日期

在路由器中會儲存目前日期與時間的紀錄，而這份資料是用來計算與回報關於系統運作的資料之用。

Note

變更路由器上的日期與時間並不會同時變更您 PC 上的日期與時間。

在路由器中，便沒有即時時鐘，然而，路由器可由外部時間伺服器取得正確的日期與時間資訊。您可以設定最多五組時間伺服器。請注意！在 **System Services** 設定頁面中的 SNTP 服務必需開啓，如此路由器才能存取外部時間伺服器的資料。

11.4.1 日期/時間 參數設定

以下列表敘述參數設定中可供設定的日期與時間設定。

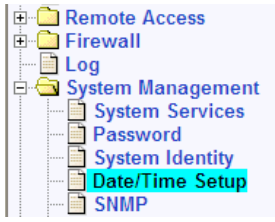
表 11.2. 日期時間 參數設定

欄位	敘述
Date	本日期當路由器重置並且無 SNTP 服務時，可以重置到 1/1/2000。若 SNTP 服務欄位設定爲開啓且可存取則正確的時間將會顯示在此欄位。
Time	當路由器重置或無 SNTP 服務時，可以重置到 00:00:00。若 SNTP 服務欄位設定爲開啓且可存取則正確的時間將會顯示在此欄位。
Time Zone	輸入您所在地的時區。
SNTP Server 1 – 5	輸入 SNTP 伺服器的 IP 位址。您可以設定最多五組的 SNTP 伺服器以取得正確的日期與時間。
Update Interval	以分鐘爲單位輸入路由器從時間伺服器中更新日期與時間的間隔。此欄位的預設值爲 60 分鐘。

11.4.2 維護日期與時間

日期與時間可藉由在 **Date** 與 **Time** 欄位輸入正確的日期與時間設定值來讓路由器自身進行維護。請注意！當 RX3041H 路由器每次進行重置動作後，您必需以手動方式再次進行日期與時間的設定。

建議您使用外部時間伺服器來協助維護您路由器中正確的日期與時間設定。請依照以下設定來 SNTP 伺服器以維護您路由器中的日期與時間設定:



22. 藉由點選 **System Management ➔ Date/Time** 選單來開啓日期/時間設定頁面。
23. 從"**Time Zone**"下拉式選單中選擇您所在地的時區。
24. 輸入最多 5 組 SNTP 伺服器的 IP 位址來存取您所在地的日期與時間資料。
25. 在"**Update Interval**" 欄位輸入時間更新的間隔時差。本項目的預設值爲 60 分鐘。

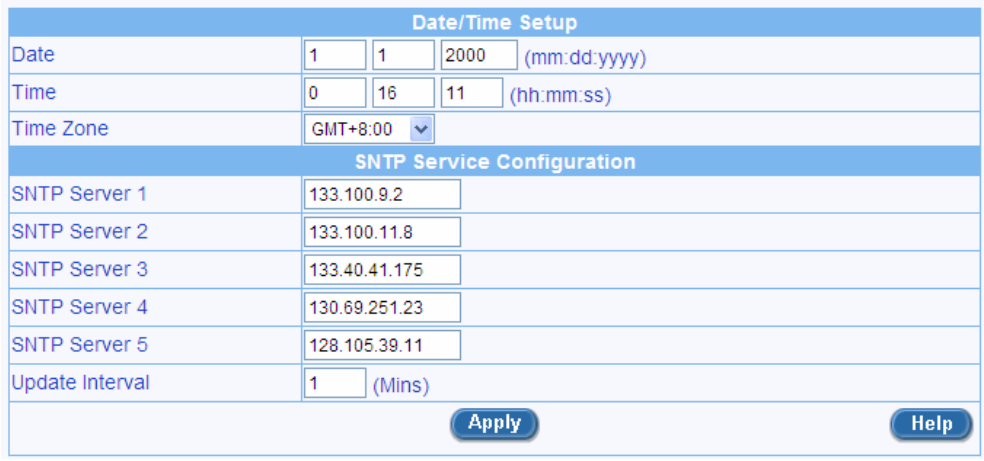


圖 11.6. 日期與時間設定頁面

26. 點選 Apply 按鍵以儲存設定值。

11.4.3 檢視系統的日期與時間

藉由點選 **System Management ➔ Date/Time** 選單來開啓日期/時間設定頁面，以檢視系統的日期與時間。

11.5 SNMP 設定

SNMP (簡易網路管理協定) 如同其名稱一般主要是用來作爲網路管理的用途。您可以利用 SNMP 設定頁面來開啓或關閉 SNMP 支援功能。

11.5.1 SNMP 參數設定

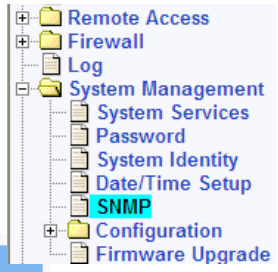
表 11.3 敘述在 SNMP 設定中可以進行設定的參數項目。

表 11.3. 固定 DHCP Lease 參數設定

欄位	敘述
SNMP	點選 “Enable” 或 “Disable” 鍵來開啓或關閉 SNMP 的支援。
RO Community Name	連線串爲一清楚的文字串，這些文字串是被用來作爲 SNMP 管理站 RX3041H 間的密碼。此一 “唯讀” 連線名稱是被用來作爲 SNMP 管理站在 RX3041H 中讀取設定之用。
RW Community Name	連線串爲一清楚的文字串，而這些文字串是作爲 SNMP 管理站與 RX3041H 間的密碼。此一 “讀與寫” 連線名稱是由 SNMP 管理戰使用，用來在 RX3041H 中讀取設定之用。
Trap Address	由 RX3041H 所傳送的 Trap 訊息，是用來告知 SNMP 管理站 RX3041H 正有某些事件發生。此一欄位可用來輸入負責接收來自 RX3141H 中 trap 訊息之 SNMP 管理站的 IP 位址。

11.5.2 設定 SNMP

27. 請藉由點選 **System Management ➔ SNMP** 選單來開啓 SNMP 設定頁面。
28. 點選 “Enable” 或 “Disable” 按鍵來開啓或關閉 SNMP 功能支援。
29. 請輸入 RO (唯讀) 與 R/W (讀與寫) 的通訊名稱。
30. 輸入可從 RX3041H 中接收 trap 訊息的 SNMP 管理站 IP 位址。



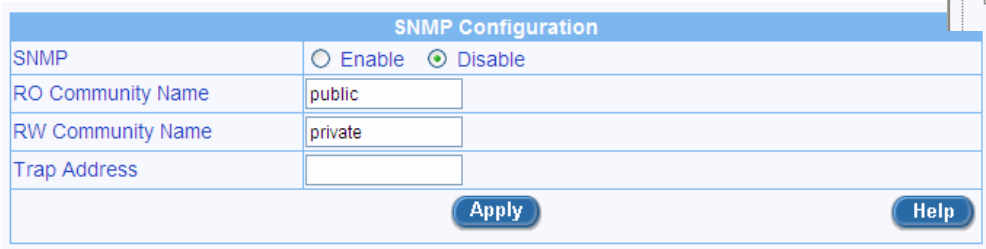


圖 11.7. SNMP 設定

31. 請點選 Apply 鍵來儲存設定值。在設定頁面下幫的設定列表中，您可從既有的 SNMP 設定列表中確認您的設定。

SNMP Configuration	
SNMP	Disable
RO Community Name	public
RW Community Name	private
Trap Address	

圖 11.8. 既有的 SNMP 設定

11.6 系統設定管理

11.6.1 重新進行系統設定

有時，您可能會想要回復設定至出廠預設值的設定來消除由於不正確的系統設定導致的問題。請參考下列步驟來重新啓動系統設定：

1. 以管理員身份登入設定管理器，點選 **System Management** 功能表，點選 **Configuration** 子功能表,然後點選 **Default Settings** 子功能表。預設設定的設定頁面將如圖 9.9 所示。

2. 點選 Apply 按鈕來回復系統設定至出廠預設值。注意，網際網路安全路由器將重新啓動以使出廠預設值生效。

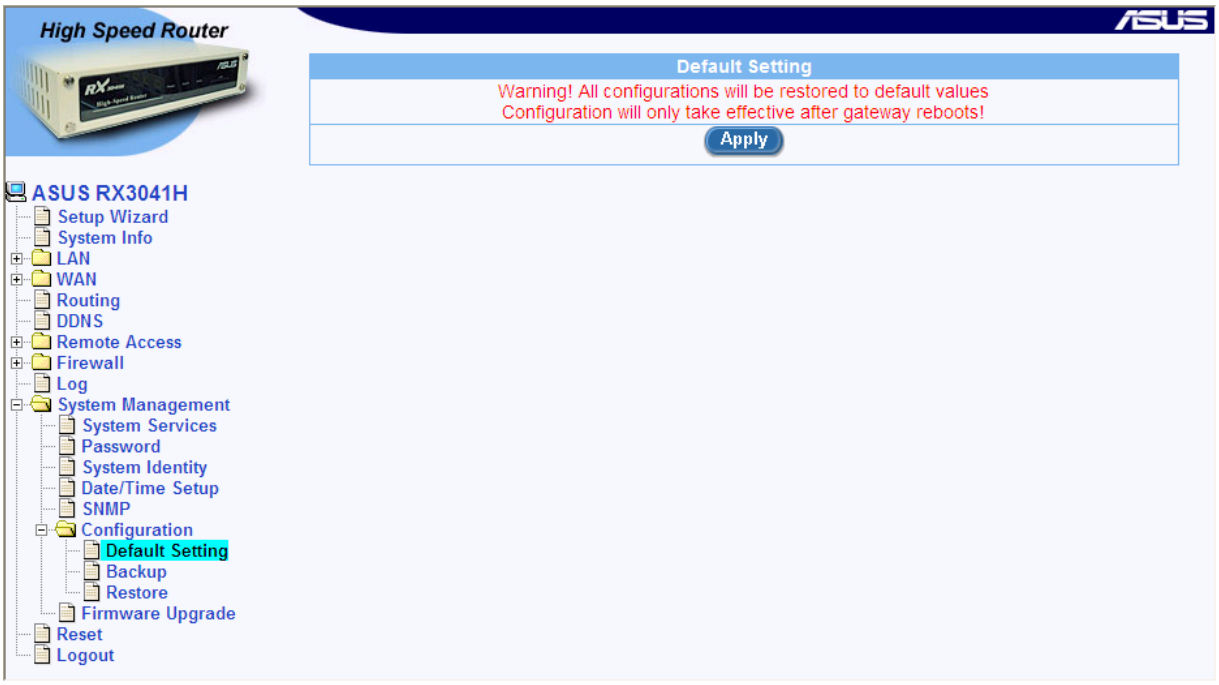


圖 11.9. 預設設定的設定頁面

有時，您可能會發現您無法訪問網際網路安全路由器，例如，您忘記了密碼。唯一辦法就是重新將系統設定回復至出廠預設值，請參考下列如何使用 Reset 鍵的步驟：

1. 斷開路由器的電源。
2. 重新接上路由器的電源，等待約 5~6 秒後按下 Reset 鍵.
3. 等待約 5~6 秒後, 再次按下 Reset 鍵。此時網際網路安全路由器將回復至出廠預設值。如果您這時改變了主意，您可再次按下 Reset 鍵，或關閉電源以取消這次的動作。

11.6.2 備份系統設定

請按照下列步驟來備份系統設定：

1. 以管理員身份登入設定管理器，點選 **System Management** 功能表，點選 **Configuration** 子功能表，然後點選 **Backup** 子功能表。備份系統設定頁面將如圖 9.9 所示。

2. 點選 Apply 按鈕以備份系統設定。

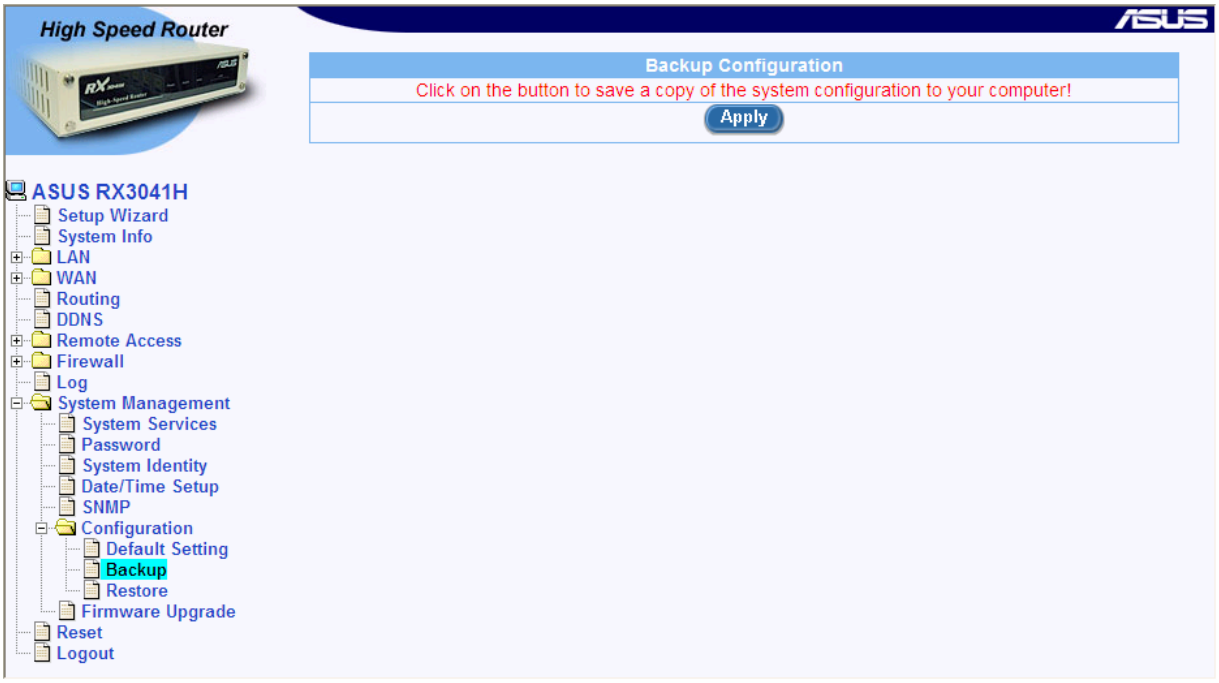


圖 11.10. 備份系統設定頁面

11.6.3 保存系統設定

請按照下列步驟來保存系統設定：

1. 以管理員身份登入設定管理器，點選 **System Management** 功能表，點選 **Configuration** 子功能表，然後點選 **Restore** 子功能表。保存系統設定頁面將如圖 9.9 所示。

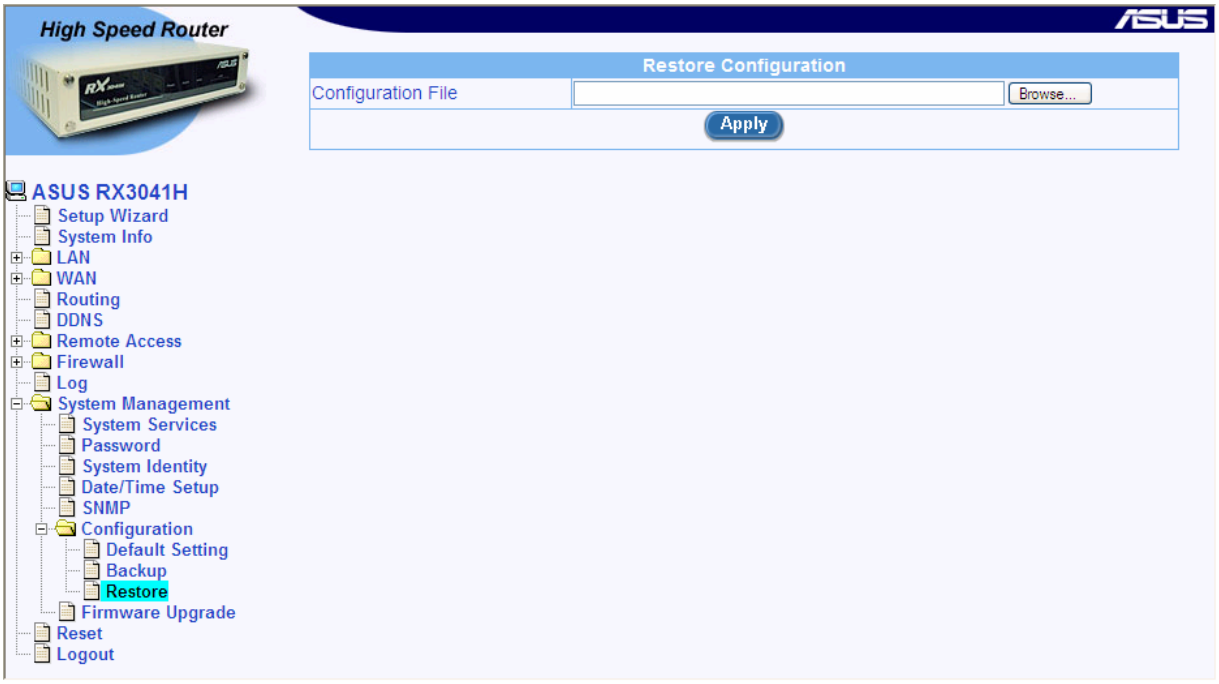


圖 11.11. 保存系統設定頁面

2. 輸入您想保存在 “Configuration File” 中的系統設定檔案的路徑與名稱。 除此之外，您也可以點選 Browse... 按鈕以搜尋您硬碟上的系統設定檔案。一個類似於圖 11.16 的窗口將突然出現，提示您選擇要保存的設定檔案。

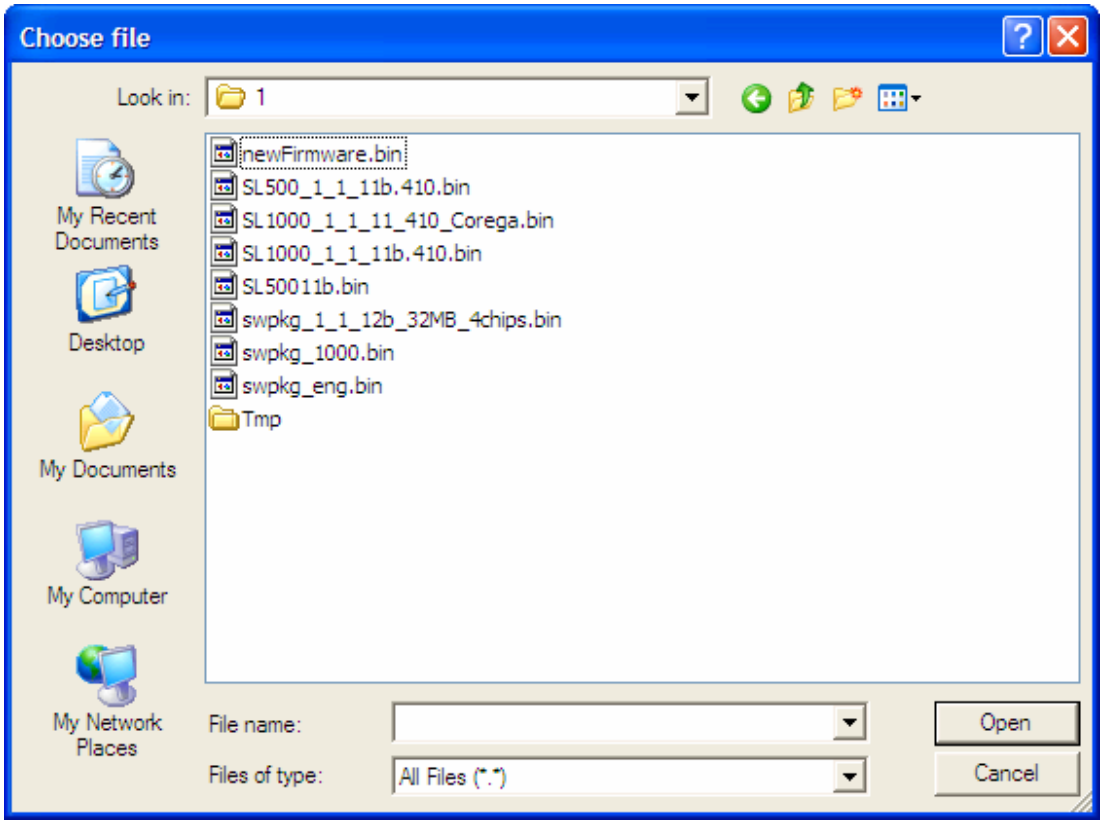


圖 11.12. Windows 檔案瀏覽器

3. 點選 Apply 按鈕以保存系統設定。注意，網際網路安全路由器將重新啓動以使新的系統設定有效。

11.7 升級韌體

華碩有可能不時地提供您升級路由器所運行的韌體的機會。所有的系統軟體都被包含在一個單獨的檔案內，名爲 *image*。 設定管理器提供了上傳新 image 的簡易方法。想要升級 image，請參考下列步驟：

1. 以管理員身份登入設定管理器，點選 **System Management** 功能表，然後點選 **Firmware Upgrade** 子功能表。韌體升級頁面將如圖 9.9 所示。

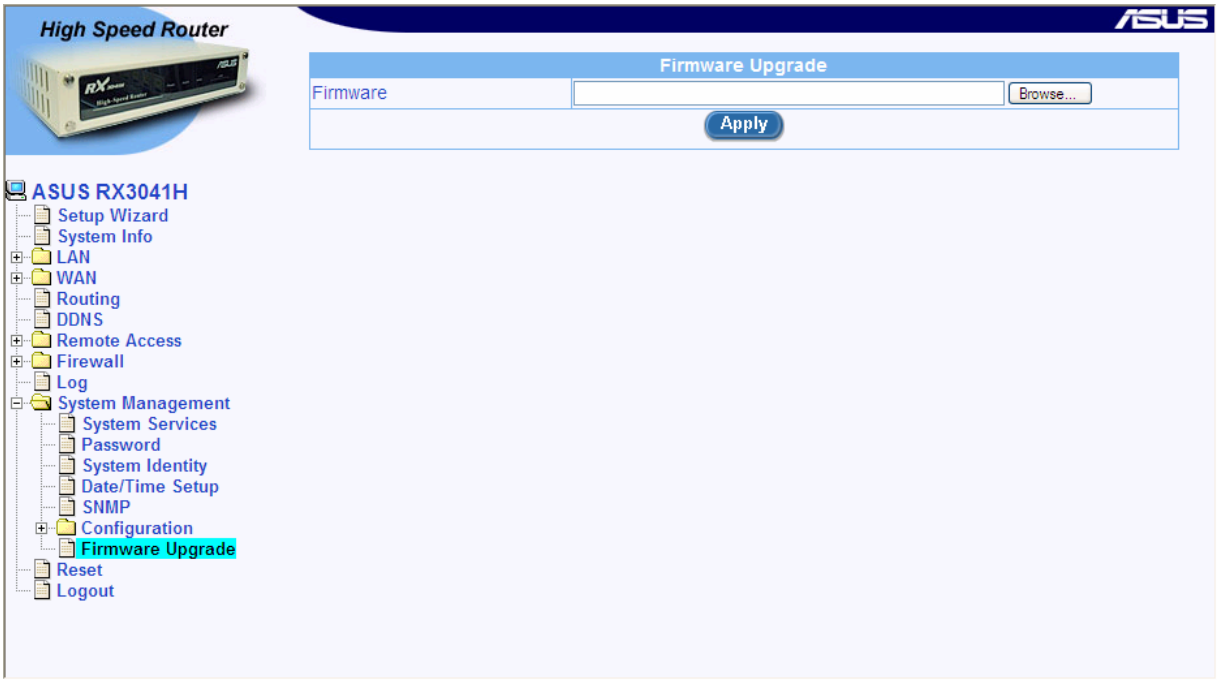


圖 11.13. 韌體升級頁面

2. 在韌體文字框輸入韌體 image 檔案的路徑與名稱。除此之外，您還可以點選 Browse... 按鈕以從硬碟內尋找。

3. 點選 Apply 按鈕以升級韌體。注意，可能要花費至少 5 分鐘的時間來進行韌體升級。在韌體升級過程結束之後，網際網路安全路由器將重啓系統以使新韌體生效。

11.8 重新設定 RX3041H 高速路由器

想要重新設定 RX3041H 高速路由器，在設定管理器 Reset 頁面點選 Apply 按鈕。

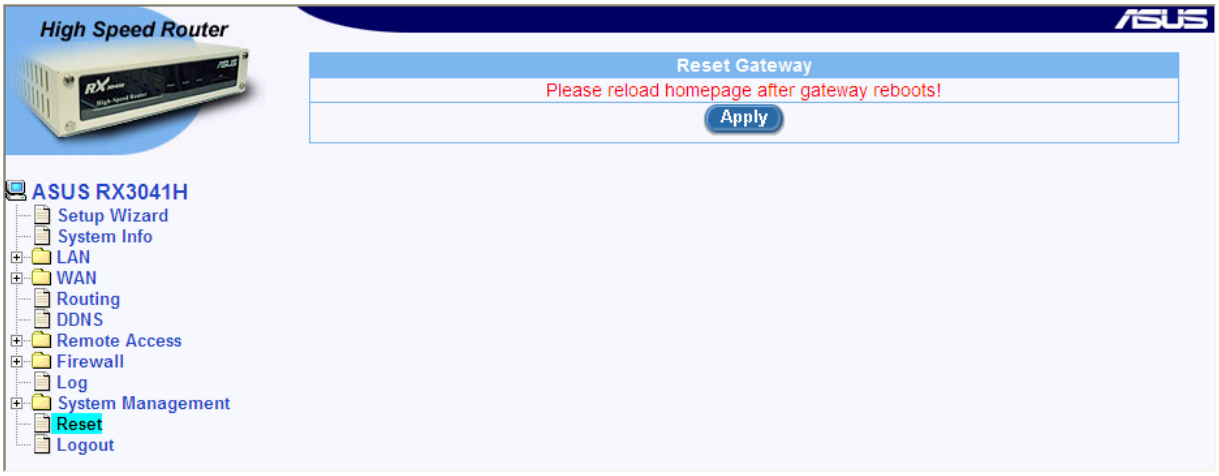


圖 11.14. 設定管理器 Reset 頁面

11.9 退出設定管理器

想要退出設定管理器，點選設定管理器退出頁面的 Apply 按鈕。如果您使用 IE 作爲您的瀏覽器，一個類似於圖 11.16 的窗口將提示您在關閉瀏覽器之前確認退出。

圖 11.15. 設定管理器退出頁面

圖 11.16. 確認退出瀏覽器（IE）

.

A. ALG 設定

表 A.1 列出了支援的所有 ALG（Application Layer Gateway）。

表 A.1. 支援的 ALG

ALG/應用程式名稱	**協定與埠**	**預先設定的服務名稱**	**測試軟體版本**
PCAnywhere	UDP/22	PC-ANYWHERE	pcAnywhere 9.0.0
RTSP-554	TCP/554	RTSP554	RealPlayer 8 Plus QuickTime Version 6
	UDP/53	DNS	
	TCP/80	HTTP	
RTSP-7070	TCP/7070	RTSP7070	RealPlayer 8 Plus
	UDP/53	DNS	QuickTime Version 6
	TCP/80	HTTP	
Net2Phone	UDP/6801	N2P	Net2Phone CommCenter Release 1.5.0
	TCP/80	HTTP	
	TCP/443	HTTPS	
	UDP/53	DNS	
CUSeeMe	TCP/7648	CUSEEME	CUSeeMe Version 5.0.0.043
	TCP/80	HTTP	
	UDP/53	DNS	
Netmeeting	TCP/1720	H323	
	UDP/53	DNS	
Netmeeting with ILS	TCP/1720	H323	Windows Netmeeting Version 3.01 Opengk Version 1.2.0
	TCP/389	ILS	
	UDP/53	DNS	
Netmeeting with GK	TCP/1720	H323	
	UDP/1719	H323GK	
	UDP/53	DNS	
SIP	UDP/5060	SIP	SIP User Agent 2.0
Intel Video Phone	TCP/1720	H323	Intel Video Phone Version 5.0
	UDP/53	DNS	
FTP	TCP/21	FTP	WFTPD version 2.03 Redhat Linux 7.3
	UDP/53	DNS	
安全 ALG			

ALG/應用程式名稱	協定與埠	預先設定的服務名稱	測試軟體版本
L2TP	UDP/1701	L2TP	Windows 2000 Server built-in
	UDP/53	DNS	
PPTP	TCP/1723	PPTP	Windows 2000 Server built-in
	UDP/53	DNS	
IPSec (Only Tunnel Mode with ESP)	UDP/500	IKE	Windows 2000 Server built-in
	ESP		
	UDP/53	DNS	
聊天			
AOL Chat	TCP/ 5190	AOL	AOL Instant Messenger Version 5.0.2938
	TCP/80	HTTP	
	UDP/53	DNS	
ICQ Chat NB: Application should be configured to use TCP/5191	TCP /5191	ICQ_2000	ICQ 2000b
	TCP/80	HTTP	
	UDP/53	DNS	
IRC	TCP/ 6667	IRC	MIRC v6.02
	TCP/80	HTTP	
	UDP/53	DNS	
MSIM	TCP/1863	MSN	MSN Messenger Service Version 3.6.0039
	TCP/80	HTTP	
	UDP/53	DNS	
遊戲			
Flight Simulator 2002 (Gaming Zone)	TCP/47624	MSG1	Flight Simulator 2002, Professional Edition
	TCP/28801	MSN-ZONE	
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Quake II (Gaming Zone)	UDP/ 27910	QUAKE	Quake II
	TCP/28801	MSN-ZONE	
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Age Of Empires	TCP/47624	MSG1	Age of Empires, Gold

ALG/應用程式名稱	協定與埠	預先設定的服務名稱	測試軟體版本
(Gaming Zone)	TCP/28801	MSN-ZONE	Edition
	TCP/443	HTTPS	
	TCP/80	HTTP	
	UDP/53	DNS	
Diablo II (BATTLE-NET-TCP, BATTLE-NET-UDP)	TCP/4000	DIABLO-II	Diablo II
	TCP/ 6112	BATTLE-NET-TCP, BATTLE-NET-UDP	
	UDP/53	DNS	
	UDP/6112	Diablo II	
其他的應用程式			
POP3	TCP/110	POP3	Outlook Express 5
	UDP/53	DNS	
IMAP	TCP/143	IMAP4	Outlook Express 5
	UDP/53	DNS	
SMTP	TCP/25	SMTP	Outlook Express 5
	UDP/53	DNS	
HTTPS / TLS / SSL	TCP/443	HTTPS	Internet Explorer 5
	TCP/80	HTTP	
	UDP/53	DNS	
LDAP	TCP/389	ILS	Openldap 2.0.25
	UDP/53	DNS	
NNTP	TCP/119	NNTP	Outlook Express 5
	UDP/53	DNS	
Finger	TCP/79	FINGER	Redhat Linux 7.3
	UDP/53	DNS	

B. 系統規格

甲、 硬體規格

表 B.1. 硬體規格

電源供應器	輸入	Varied w/ regions. Note your AC adapter only works w/ your region.
	輸出	15VAC, 700mA
記憶體	Flash	4MB
	SDRM	16MB
連接埠	WAN	1 – 10/100Mbps, auto speed negotiation
	LAN	4 – 10/100Mbps, auto MDI/MDIX, auto speed negotiation
	Reset button	For use on system reboot and reset to factory settings
	Console port	For use by ASUS only
環境需求	操作	Temperature: 0°C ~ 40°C (32°F ~ 105°F)
		Humidity: 10% ~ 90%, non-condensing
	放置	Temperature: -20°C ~ 65°C (-4°F ~ 149°F)
		Humidity: 10% ~ 90%, non-condensing

乙、 系統預設值

表 B.2 l 是關於本路由器的預設值。在此表格中並不列出預設值的相關參數。

表 B.2. 系統預設值

區域網路 LAN		
IP	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
DHCP Server	IP Address Pool	192.168.1.10 ~ 192.168.1.200
	Subnet Mask	255.255.255.0
	Lease Time	14 days
	Default Gateway	192.168.1.1
	Primary DNS	192.168.1.1
廣域網路 WAN		
Default Connection Mode		PPPoE
PPPoE (PPPoE:0,	Unnumbered PPPoE	Disable
	Host Name	RX3041H

PPPoE:1)	Obtain DNS	Automatically
	MSS Clamping	Enabled, MSS Value – 40 bytes
	Options	Keep Alive, Echo Interval – 60 seconds
Dynamic (DHCP Client)	Host Name	RX3041H
	Obtain DNS	Automatically
	MAC Cloning	Disable
路由設定		
動態路由	RIP	Enable
	Passive Mode	Disable
	RIP Version (Send)	Version 2
	RIP Version (Receive)	Both
	Authentication	Disable
	RIP Authentication Mode	Clear Text
	Authentication Key	admin
遠端存取		
使用者群組	Inactivity Timeout	300 seconds
防火牆		
入埠 ACL		Deny all inbound traffic
出埠 ACL		Allow all outbound traffic, NAT – WAN interface, Time Ranges – always, Application Filtering – none, Log - disable
URL 過濾		Enable
	Proxy Port	80
Advanced ➔ Self Access		From LAN: ICMP; TCP 23, 80, 10081; UDP 161, 162, 53
Advanced ➔ DoS	Enable	SYN Flooding, ICMP Verbose, Max IP Fragment Count – 45, Min IP Fragment Size – 512 bytes
	Disable	Winnuke, MIME Flood, FTP Bounce, IP Unaligned Time-stamp, Sequence Number Prediction Check, Sequence Number Out-of-range Check, ICMP Verbose
Log		
	File	Enable for Access, System and Firewall
	Log File Backup via Email	Disable
	Email	Disable
	Syslog Server	Disable

系統管理		
System Services	Enable	Firewall, DNS Relay, DHCP Server, Revert back to the factory default by using the Reset button
	Disable	DDNS, RIP, SNTP, UPnP
Password	Administrator	Username: admin (cannot be changed)
		Password: admin
	Guest	Username: guest (cannot be changed)
		Password: guest
System Identity	System Name	RX3041H
Date/Time	Date	1/1/2000 (moth/day/year)
	Time	00:00:00 (hour:min:sec)
	Time Zone	GMT+8:00
	SNTP Update Interval	60 minutes
SNMP		Disable
	RO (Read-Only) Community Name	public
	RW (Read-and-Write) Community Name	private

C. IP 位址，網路遮罩及子網

甲、 IP 位址


注意

本章節只適合 IPv4 IP 位址（網際網路協定第 4 版）。IPv6 位址並不適用。

本章節假定您已經掌握了一些基本知識，如二進位數字、位元組（byte）、位（bit）。欲知更多細節請參考附錄 A。

IP 位址，類似於網際網路的電話號碼，被用來確定網際網路上的個人節點（電腦或其他設備）。每個 IP 位址都包括四個數位，每個都是從 0 到 255，由點（句點）分開，例如 20.56.0.211。這些數位按照從左到右的順序被稱爲 field1, field2, field3, and field4。

這種用點分開十進位的數位的書寫 IP 位址的風格被稱爲*帶點的十進位符號*。IP 位址 20.56.0.211 讀作"二十點五十六點零點二一一"。

i. IP 位址結構

IP 位址與電話號碼相類似，是一種分等級的設計。例如，一個 7 位數的電話號碼，它的前三位確定了成千上萬條電話線的一個群組，而後四位元數位則確定了群組中的一條特定的電話線。

類似的，IP 位址也包含兩類資訊。

- *Network ID*
  確定了網際網路或內部網路中的一片特定的網路
- *Host ID*
  確定了網路中一台特定的電腦或其他設備

每個 IP 位址的第一部分都包括了 network ID，其餘的部分就包括了 host ID。網路 ID 的長度取決於網路等級 network *class*（請參看下面的部分）。表 C.1 說明了 IP 的結構。

表 C.1. IP 位址結構

	Field1	Field2	Field3	Field4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

這裏有一些有效 IP 位址的實例：

Class A: 10.30.6.125 (network = 10, host = 30.6.125)
Class B: 129.88.16.49 (network = 129.88, host = 16.49)
Class C: 192.60.201.11 (network = 192.60.201, host = 11)

乙、 網路等級

三個常用的網路等級爲 A、B 和 C。（還有一個等級 D，但是它有特殊用途，已經超過了本次討論的範圍。）這些等級分別有不同的用途和特性。

等級 A 網路是網際網路最大的網路，每個都擁有超過 1 千 6 百萬主機的空間。對於總數超過 20 億的主機而言，最多可存在 126 個如此巨大的網路。因爲它們的超大尺寸，這些網路被用作 WAN 以及被網際網路基礎結構水平的組織使用，如您的網路供應商 ISP。

等級 B 網路比 A 稍小一些，但仍舊很大，每個都能容納 6 萬 5 千主機。最多可存在 16,384 個等級 B 的網路。一個等級 B 的網路可適用於大型組織，如商業或政府代理處。

等級 C 網路是最小的一個，最多只能容納 254 主機，但是等級 C 網路可能的總數可超過 20 億（確切地說，是 2,097,152）。連線到網際網路上的區域網路 LAN 通常是等級 C 網路。

下面是關於 IP 位址的一些重要的注意事項：

- 透過 field1 我們很容易就可以判斷網路的等級：
  field1 = 1-126: Class A
  field1 = 128-191: Class B
  field1 = 192-223: Class C
  （若 field1 的值沒有顯示出來，則表明被保留以作特定用途 uses）
- host ID 能夠擁有任意值，除了所有 field 的值均設爲 0 或所有的 field 均設爲 255 之外，因爲這些值被保留以作特定用途。

丙、 子網路遮罩

名詞解釋
遮罩（mask）

遮罩看起來很像一個規則的 IP 位址，但是卻包含了位（bit）的形態，能夠告訴您 IP 位址的哪個部分是 network ID 以及哪個部分是 host ID：bit 設定成 1 表明"此 bit 是 network ID 的一部分"，bit 設定成 0 表明"此 bit 是 host ID 的一部分"。

子網路遮罩 被用來定義 *子網路*（您在將網路分割成一小片一小片之後所得到的）。子網的網路 ID 是透過從位址的 host ID 部分"借用"一個或多個 bit 而建立的。子網路遮罩識別這些 host ID 的 bit。

例如，等級 C 網路 192.168.1。想要將它分成兩個子網路，您得使用子網路遮罩：

255.255.255.128

如果我們用二進位來書寫，將更容易看到發生了什麼：

11111111. 11111111. 11111111.10000000

而對於任意等級 C 位址，從 field1 到 field 3 的所有 bit 都是 network ID 的一部分，但是請注意，遮罩是如何指定 field 4 的第一個 bit 也包含在內。由於這個額外的 bit 只有兩個值（0 和 1），這意味著有兩個子網。每個子網爲 host ID 使用了 field 4 保留的 7 個 bit，它的範圍從 0 到 127（而不是等級 C 通常的 0 到 255）。

類似的，將等級 C 的網路分成四個子網，遮罩爲：

255.255.255.192 或 11111111. 11111111. 11111111.11000000

這兩個 field 4 內額外的 bit 有四個值（00, 01, 10, 11），因此有四個子網。每個子網爲 host ID 使用了 field 4 保留的 6 個 bit，範圍從 0 到 63。


注意

*有時，子網路遮罩並不特別指定任何額外的 network ID bit，因此就沒有子網路。這樣的遮罩被成爲*預設的子網路遮罩。*這些遮罩爲：*

Class A: 255.0.0.0
Class B: 255.255.0.0
Class C: 255.255.255.0

*這些被稱爲*預設值*是因爲它們在當網路預先設定好時被使用，此時它沒有子網路。*

D. 解決問題

本附錄爲您在安裝或使用網際網路安全路由器的過程中可能遇到的問題提出了供參考的解決方法，並爲如何使用 IP 工具來診斷問題提供了參考說明。

如果下列建議不能爲您解決問題，請聯繫華碩客戶服務部門。

問題	解決方法
LED 燈	
Power LED 燈在產品開關打開後不亮。	請檢查您是否使用由設備所提供的電源供應器，且安全地連線到網際網路安全器和電源插座上。
LINK WAN LED 燈在乙太網線纜連線好後不亮。	請檢查設備提供的乙太網線纜已經安全地連接到了您 ADSL 或 cable modem 的乙太網埠和路由器的廣域網埠上面。請確認您的 ADSL 或 cable modem 的電源是開啓的。等待 30 秒的時間以允許路由器與您的寬頻 modem 有協商時間。
LINK LAN LED 燈在乙太網線纜連接好後不亮。	請檢查設備提供的乙太網線纜已經安全地連接到了您的區域網路集線器或 PC 以及網際網路安全路由器上。請確認 PC 和/或集線器已經開啓。 請檢查您的纜線足夠應付您的網路需求。100 Mbit/秒的網路（100BaseTx）應該使用 Cat 5 的纜線。10Mbit/秒的網路可以接受品質稍低的纜線。
訪問 Internet	
PC 無法訪問 Internet	使用下面即將討論到的 ping 工具，以檢查您的 PC 是否能夠與網際網路安全路由器的區域網路 IP 位址（預設值爲 192.168.1.1）通訊。如不能，請檢查乙太網的纜線。 如果您靜態地爲電腦指定了一個私人 IP 位址，（並非已註冊的公共位址），請檢查下列事項： • 檢查電腦閘道 IP 位址是您的公共 IP 位址，（參看"快速安裝指南"一章，第二部分對於檢查 IP 資訊的說明）。如果不是，那麼改正此位址或將 PC 設定成自動接收 IP 資訊。 • 與您的網路供應商確認指定給 PC 的 DNS 伺服器 是有效的。請改正此位址或將 PC 設定成自動接收 I 資訊。 • 請檢查網路位址轉換(NAT)規則已經在您的網際網路安全路由器上設定好以將私人位址轉換成公共 IP 位址。指定的 IP 位址必須包含在指定的 NAT 規則中。或者，設定 PC 接收另一設備指定的位址（參看第 3.2 節 第二部分 設定網際網路參數）。預設的設定包括一個在預先定義好的位址池 內的所有動態指定位址而設定的 NAT 規則。

問題	解決方法
PC 無法顯示網際網路的網頁。	請檢查 PC 指定的 DNS 伺服器對您的網路供應商來說是正確的，如上文選項所述。您可使用下面即將討論到的 ping 工具測試與您網路供應商的 DNS 伺服器的連通性。
設定管理員程式	
您忘記/遺失了您的設定管理員用戶 ID 或密碼。	如果您還未更改預設的密碼，請嘗試使用"admin"作爲您的 用戶 ID 以及密碼。另外，您可將設備重新設定成預設值（請參考第 **錯誤! 找不到參照來源。**節"**錯誤! 找不到參照來源。**"提供的說明）。 **小心:** 重新設定本設備將導致原有設定被刪除，且所有的設定均回復至預設值。
從您的瀏覽器無法訪問設定管理員。	使用下面即將討論到的 ping 工具，以檢查您的 PC 是否能夠與網際網路安全路由器的區域網 IP 位址（預設值爲 192.168.1.1）通訊。如不能，請檢查乙太網的纜線。 請檢查您使用的瀏覽器爲 Internet Explorer v5.5、Netscape 7.0.2 或以上版本。想要使用 Javascript® 必須得到瀏覽器的支援；想要使用 Java® 同樣也需要支援。 請檢查 PC 的 IP 位址與指定給路由器區域網路埠的 IP 位址位於相同的子網下。
對設定管理員的更改沒有保留下來。	請確認點選了 Apply 按鈕以保存更改。

甲、 使用 IP 工具診斷問題

i. ping

Ping 是用來檢查您的 PC 是否能夠辨認出您網路或網際網路內其他電腦的命令。Ping 命令送出一個訊息到您指定的電腦上。如果電腦接收了訊息，它將送出訊息回覆。使用這個工具，您必須知道您與之通訊的電腦的 IP 位址。

對 Windows 系統的電腦，您可從**開始**功能表執行 Ping 命令。點選**開始**按鈕，然後點選**執行**。在文字框輸入下列內容：

ping 192.168.1.1

點選 OK。您可用網際網路站點名稱取代任何區域網路內的私人 IP 位址或公共 IP 位址。

如果目標電腦收到了此資訊，命令提示視窗將出現，如圖 D.1 所示。

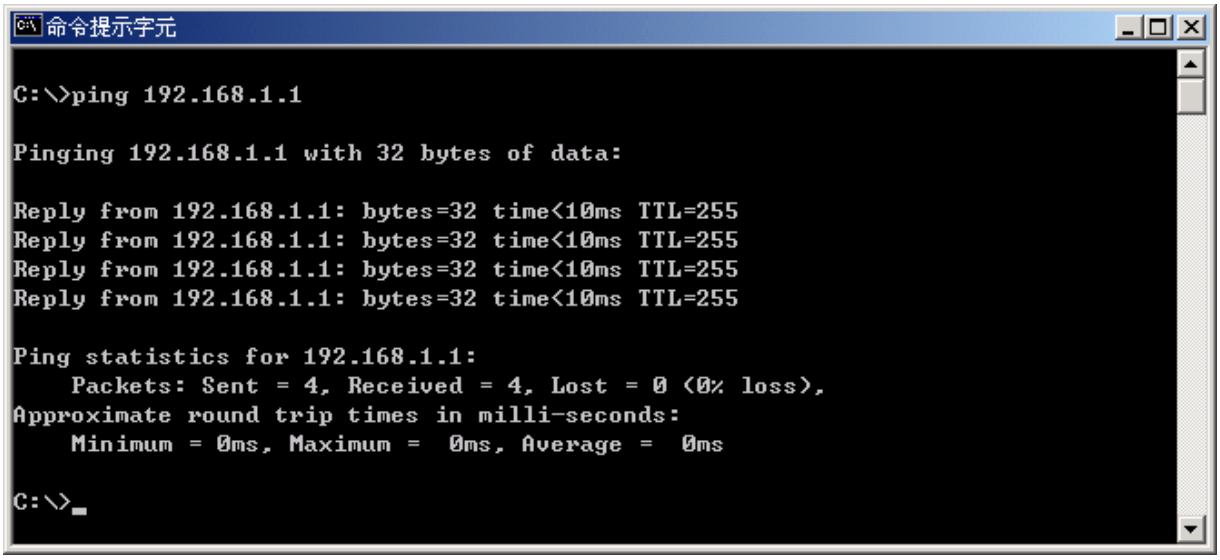


圖 D.1. 使用 ping 工具

如果目標電腦不存在，那麼您將接收此消息 “Request timed out”。

使用 ping 命令，您可以測試到達路由器的路徑是否起作用（使用預先設定好的區域網路 IP 位址 192.168.1.1），或者另外一個您指定的位址。

您還可以透過輸入外部位址，例如 www.yahoo.com （216.115.108.243）測試網際網路連線是否來起作用。如果您不知道特定網際網路位置的 IP 位址，您可使用 nslookup 命令，如下面章節的說明。

對於大多數 IP-enabled 的作業系統，您可在命令提示時或透過系統管理工具執行相同的命令。

ii. nslookup

您可使用 nslookup 命令來決定與網際網路站點名稱相對應的 IP 位址。您指定了一般的名稱，然後使用 nslookup 命令在您的 DNS 伺服器（通常放置在您的網路服務供應商）上查詢此名稱。如果那個名稱並不存在您網路服務供應商的 DNS 表格中，那麼此請求將涉及另一個更高等級伺服器，直到該項目被找到。最後，伺服器會回應與該名稱相對應的 IP 位址。

對 Windows 系統的電腦，您可從**開始**功能表找到 nslookup 命令並執行之。點選**開始**按鈕，然後點選**執行**。在文字框輸入下列內容：

nslookup

點選 OK 。一個命令提示窗口將與括弧同時出現（>）。根據提示，輸入您感興趣的網際網路位址名稱，例如 www.absnews.com。

此視窗將顯示相關聯的 IP 位址，如圖 D.2 所示。

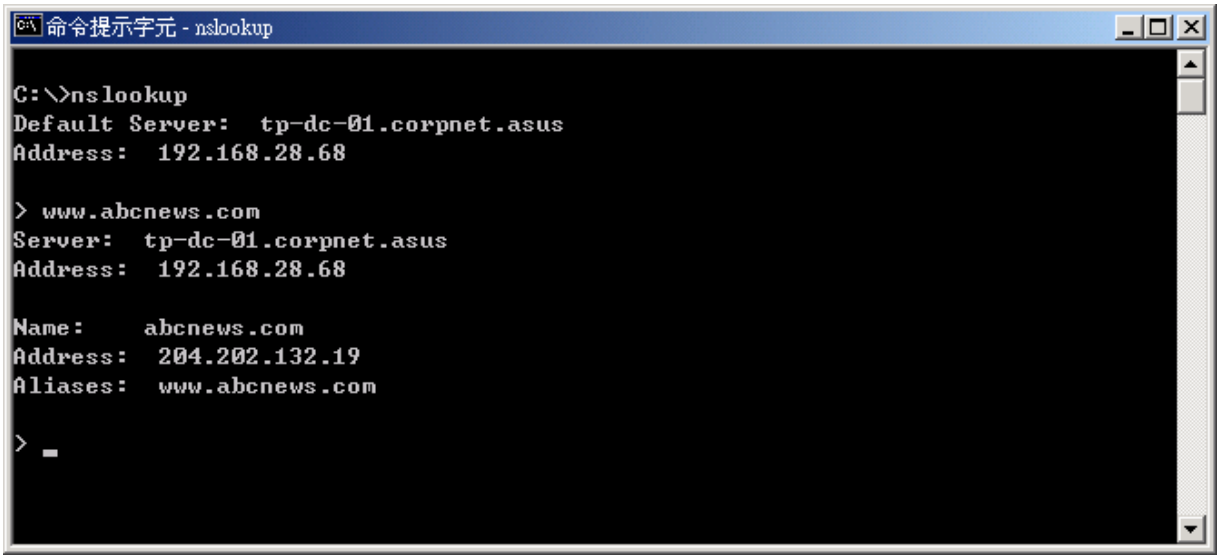


圖 D.2. 使用 nslookup 工具

可能會出現很多的 IP 位址名稱對應到同一名稱。這對經常接收到巨大流量的網頁站點來說很平常；他們使用多台的伺服器來傳遞相同的資訊。

想要離開 nslookup 模式，請在命令提示頁面中輸入 **exit**，然後按下 **<Enter>** 鍵。

E. 術語表

10BASE-T 乙太網路使用的配線的名稱，資料傳輸率爲 10 Mbps。又被稱爲 Category 3（CAT 3）配線。*又見資料傳輸率，Ethernet*。

100BASE-T 乙太網路使用的配線的名稱，資料傳輸率爲 100 Mbps。又被稱爲 Category 5（CAT 5）配線。*又見資料傳輸率， Ethernet*。

ADSL Asymmetric Digital Subscriber Line，非對稱式數位用戶迴路
對於家庭用戶來說最常用的 DSL。Asymmetrical 非對稱性指的是它不平衡的下載與上載資料傳輸率（下載速率要比上載速率快）。非對稱性有益於家庭用戶，因爲他們通常下載的資料量要比上載的多得多。

authenticate 用來檢驗用戶的身份，例如提示輸入密碼。

binary 二進位，兩個最基礎的數位系統之一，僅使用兩個數位（0 和 1）來代表所有的數位。在二進位裏，數位 1 寫成 1，2 寫成 10， 3 寫成 11，4 寫成 100，如此類推。儘管爲方便起見，IP 位址常常用十進位的數位來表達，但實際上，IP 位址是二進位數字字；例如，209.191.4.240 在二進位內是 11010001.10111111.00000100.11110000。*又見 bit, IP address, network mask*。

bit 比特，"binary digit，二進位數字字" 的簡寫，一個 bit 其實是有 0 或 1 兩個值的數位。*又見 binary*。

bps 每秒比特數

broadband 寬頻，一種通訊技術，能夠透過相同的媒介傳送不同類型的資料。DSL 就是寬頻技術的一種。

broadcast 廣播，把資料傳送到網路中所有的電腦上。

DHCP Dynamic Host Configuration Protocol，動態主機配置協定
DHCP 自動進行位址分配與管理。當電腦連線上區域網路（LAN），DHCP 從共用的 IP 位址位址池中指派 IP 位址；在指定的時間界限結束之後，DHCP 又將位址歸還給了位址池。

DHCP relay Dynamic Host Configuration Protocol relay，動態主機配址協定中繼
DHCP relay 是指在要求 IP 位址的電腦與指派位址的 DHCP 伺服器之間傳遞 DHCP 資訊的電腦。路由器的每個介面都能設定成 DHCP relay。*詳見 DHCP 章節*。

DHCP server Dynamic Host Configuration Protocol server，動態主機配址協定伺服器
DHCP 伺服器是指負責爲 LAN 中的電腦指派 IP 位址的電腦。*詳見 DHCP 章節*。

DNS Domain Name System，領域名稱系統
DNS 將網域名稱對應到 IP 位址上去。DNS 資訊按等級穿過網際網路分配給稱作 DNS 伺服器的電腦。當您開始訪問網頁站點時，DNS 伺服器會檢查被要求的網域名稱，以找到相應的 IP 位址。如果 DNS 伺服器不能找到 IP 位址，那麼它將與更高一級的 DNS 伺服器聯絡，以確定 IP 位址。*又見 domain name*。

domain name 網域名稱，是代替與之相對應的用戶容易掌握使用的 IP 地址名稱。例如，www.hinet.net 與 IP 位址 168.95.1.88 相關聯的網域名稱。網域名稱必須是獨一無二的；它們被國際指派名稱與序號的網際網路公司（ICANN）進行分配 。網域名稱並非 URL 的要素，URL 在網頁站點確認特定的檔案，例如， http://www.asus.com。*詳見 DNS 章節*。

download 下載，從網際網路傳遞資料給用戶。

DSL Digital Subscriber Line，數位用戶迴路
一種同時允許數位資料與類比聲音信號透過現有銅製電話線的技術。

Ethernet 乙太網，最普遍應用的電腦網路技術，常使用雙絞線電纜。乙太網資料傳輸率爲 10 Mbps 與 100 Mbps。又見 *10BASE-T, 100BASE-T, twisted pair*。

filtering 過濾，以過濾規則爲基礎篩選出資料的類型。過濾可被應用在一個方向（上載或下載），或雙向。

filtering rule 過濾規則，一個指定路由設備將接收和/或拒絕何種類型的資料的規則。過濾規則被定義爲在某一介面（或多個介面）操作且朝著特定的方向（下載、上載，或雙向）。

firewall 防火牆，指保護接入網際網路的電腦或區域網路不受外界的侵擾或攻擊的任意方法。一些防火牆保護可由封包過濾和網路位址轉換服務提供。

FTP File Transfer Protocol，檔案傳輸協定
一個被用來在接入網際網路的電腦之間傳遞檔案的程式。通常的應用包括向網路服務器上載新的或更新後的檔案，以及從網路服務器下載檔案。

hop 跳躍，當您透過網際網路傳送資料時，資料首先從您的電腦傳送至路由器，然後從一台路由器傳送到另一台，直到最後達到直接連線到接收者的路由器爲止。資料的傳遞旅程中每個單個的"leg" 都被稱爲一次跳躍。

hop count 跳躍次數，指數據在到達目的地的路徑中所經歷的跳躍的次數。另外，亦可指一個封包在被丟棄之前被允許經歷的最大跳躍次數（*又見 TTL*）。

host 主機，連接到網路的設備（通常是指電腦）。

HTTP Hyper-Text Transfer Protocol，超文字傳輸協定
HTTP 是用在 Web 瀏覽器與 Web 伺服器之間傳輸檔案（如文字或圖片檔案）的協定 。*又見 web browser, web site*。

ICMP Internet Control Message Protocol，網際網路控制訊息協定
網路層面的網際網路協定，負責錯誤報告及提供 IP 封包處理相關的資訊。Ping 命令就使用了 ICMP。

IGMP Internet Group Management Protocol，網際網路群組管理協定
一個使電腦能在多點廣播內與相鄰路由器與分享成員資訊的網際網路協定。多點廣播群組是指成員已經被認定爲願意從其他電腦那裏接收特定內容的資訊感興趣的群組。對 IGMP 群組的多點廣播可同時被用來更新移動用戶群組位址薄，或將公司的時事通訊傳送到名單上的用戶。

Internet 網際網路，最大的全球性網路，連接全世界上萬個網路，爲私人和商業用戶使用。

intranet 內部網路，一個私人的，或企業內部的網路，看起來像網際網路的一部分（用戶使用網頁瀏覽器訪問資訊），但是僅爲內部成員使用。

IP *見 TCP/IP*。

IP address Internet Protocol address，網際網路協定位址
網際網路上主機（電腦）的位址，由四個數位組成，每個都是從 0 到 255，以點號隔開，例如，209.191.4.240。IP 位址由確認主機所屬的特殊網路的 *network ID* 與確認主機自身處於網路的獨一無二的 *host ID* 構成。網路遮罩被用來定義 network ID 與 host ID。因爲每個成員的 IP 位址均不相同，所以他們常常擁有相關聯可被指定的的網域名稱。又見 *domain name, network mask*。

ISP Internet Service Provider，網路服務供應商
提供顧客訪問網際網路收費服務的公司。

LAN Local Area Network，區域網路
局限於一個小的地理區域的網路，例如，家庭、辦公室，或小型建築。

LED Light Emitting Diode，發光二極體
透過轉換電子能量的方式來發射光線的半導體設備。一般硬體設備上的狀態燈都是典型的 LED。

MAC address Media Access Control address，媒體存取控制位址
由製造商指定的設備的永久硬體位址。MAC 位址用六組字元(byte)來表示。

mask *見 network mask*。

Mbps 每秒百萬比特，Megabits per second 的簡寫。網路資料傳輸率通常用 Mbps 來表示。

NAT Network Address Translation，網路位址轉換
用以減低對 IP 位址必須全球唯一的需求的機制。NAT 透過將位址轉換成可在全球傳遞的位址，使得某一組織連線到互聯網的 IP 位址可以不是全球唯一的。

NAT rule NAT 規則，已定義的在您區域網路的公共與私人 IP 位址之間傳輸資訊的方法。

network 網路，一群可透過傳輸媒體互相通信的電腦、印表機、交換器及其它的設備。網路可以很小，如區域網路 *LAN*，也可以非常大，如網際網路 *Internet*。

network mask 網路遮罩，指一系列當忽略掉 host ID 時被應用於 IP 位址選擇的一系列 bit。Bit 設定爲 1 意味著"選擇此位"，而當 bit 設定爲 0 則意味著"忽略此位"。例如，如果網路遮罩 255.255.255.0 應用到 IP 位址 100.10.50.1，那麼 network ID 爲 100.10.50，host ID 爲 1。*又見 binary, IP address, subnet*。

NIC Network Interface Card，網路介面卡
插入您的電腦，並能爲網路線纜提供實體介面的介面卡，典型的乙太網 NIC 是 RJ-45 連接器。*見 Ethernet, RJ-45*。

packet 封包，在網路上傳輸資料的單位。每個封包都包含資料、添加的資訊例如它從那裏來（來源位址）以及將到哪里去（目標位址）。

ping Packet Internet (or Inter-Network) Groper，訊息及其回覆
用來檢驗與 IP 位址相關聯的主機是否已連線的程式。它亦能被用來顯示給定網域名稱的 IP 位址。

port 埠，電腦、路由器等設備的物理接入點，資料透過連接埠來傳入和傳出此設備。

PPP Point-to-Point Protocol，點對點協定
提供透過同步或非同步傳輸電路路由器對路由器和對主機的連線。廣域網（WAN）的路由器介面使用兩種形式的 PPP ，稱爲 PPPoA 與 PPPoE。*又見 PPPoA, PPPoE*。

PPPoE Point-to-Point Protocol over Ethernet，乙太網的點對點協定
您能定義虛擬電路（VC）的兩種 PPP 介面之一，另一種爲 PPPoA。您能爲每個 VC 定義一個或多個 PPPoE 介面。

protocol 協定，管理設備如何在網路上交換資訊的一套規則和規範的正式稱呼。

remote 遠端，物理上分離的位置。例如，員工在出差的途中登入公司內部網路，爲遠端用戶。

RIP Routing Information Protocol，路由資訊協定
最初的 TCP/IP 路由協定。有兩個 RIP 版本：版本 I 與版本 II。

RJ-45 8-pin 的插頭用來代替電話線傳輸資料。乙太網線纜通常使用此種類型的連接器。

routing 路由，找到一條到達目的地主機路徑的程式。在大型網路裏，路由是非常複雜的，因爲封包在抵達目的地之前，可經過的中間節點非常多。履行路由職責的設備被稱爲路由器。

rule *見 filtering rule, NAT rule*。

SDNS Secondary Domain Name System （server），二級網域名稱系統（伺服器）
指在 primary DSN 伺服器不可用時，能被使用的 DNS 伺服器。*見 DNS*。

SNMP Simple Network Management Protocol，簡單網路管理協定
用於網路管理的指 TCP/IP 協定。

subnet 子網，在 IP 網路裏，分享某一特別子網位址的網路。子網是由網路管理者爲了提供多級、階層式路由結構，而同時能夠避免所附著網路的子網的指定地址的複雜度。*又見 network mask*。

subnet mask 子網路遮罩，定義子網的遮罩。*又見 network mask*。

TCP *見 TCP/IP*。

TCP/IP Transmission Control Protocol/Internet Protocol，傳輸控制協定/網際網路協定
網際網路所使用的基本協定。TCP 負責分割需傳遞資料至封包並在目的地將它們重新組裝起來，而 IP 負責將封包從來源地傳輸至目的地。當 TCP 和 IP 與高級應用程式如 HTTP, FTP, Telnet 等捆綁在一起時，TCP/IP 指的是整套協定。

Telnet 互動式的、通常用在使得用戶能登入遠端的系統就如同在本地般使用其資源的遠端終端機連線。HTTP（網路協定）與 FTP 僅允許您從遠端電腦下載檔案，而 Telnet 可允許您從遠端登入及使用電腦。

TFTP Trivial File Transfer Protocol，簡易檔案傳輸協定
FTP 的簡化版，允許在網路上傳送和接收檔案的協定，但是沒有 FTP 的功能強大，安全性也較差。

TTL Time To Live，存活時間
IP 表頭中的選項，用來指出一個封包被認爲有效的時間有多長。TTL 爲零時，封包將被丟棄。

twisted pair 雙絞線，包含兩條被絞成螺旋狀絕緣線的低速傳輸媒體。此絕緣線可以是遮蔽或無遮蔽。雙絞線是語音通訊應用中常見的媒體，且日漸在資料網路上逐漸普遍。對於乙太網 LAN，一個更高等級的 Category 3 (CAT 3) 正在爲 10BASE-T 網路所應用，一個更高等級的 Category 5 (CAT 5)正在爲 100BASE-T 網路所應用。又見 *10BASE-T, 100BASE-T, Ethernet*。

upstream 上行，資料傳輸的方向是從用戶到網際網路。

WAN Wide Area Network，廣域網
由電信公司所提供，服務于廣大區域使用者的資料通訊網路。對於網際網路安全路由器來說，WAN 指整個網際網路。

Web browser 使用檔案傳輸協定 HTTP 來從網路站點下載資訊，並爲用戶顯示由檔案、圖形、音頻或視頻組成的資訊的用戶端應用軟體。例如，Internet Explorer、Mosaic 和 Netscape Navigator。*又見 HTTP, web site, WWW*。

Web page 網頁，網站點檔案，一般包括文本、圖形以及鏈結到本站點及其它站點的網頁的超鏈結（前後對照）。當用戶訪問網路站點時，顯示的第一個頁面稱爲主頁 *home page*。*又見 hyperlink, web site*。

Web site 網路站點，指網際網路上透過網頁瀏覽器分配資訊給遠端用戶、以及從遠端用戶獲得資訊的電腦。網路站點一般由包含文本、圖形以及超鏈結的網頁組成。*又見 **hyperlink**, **web page***。

WWW World Wide Web，全球資訊網
又被成爲*環球網*。提供超鏈結及其它服務給執行像瀏覽器等用戶端軟體的網際網路伺服器的大型網路。

F. 索引