

# RX3141

## 使用手冊



T1742  
1.0 版  
2004 年 12 月

## RX 系列

---

本產品的所有部分，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、謄抄或轉譯。本產品使用手冊沒有任何型式的擔保、立場表達或其它暗示。若有任何因本使用手冊或其所提到之產品的所有資訊，所引起直接或間接的資料流失、利益損失或事業終止，華碩及其所屬員工恕不為其擔負任何責任。除此之外，本使用手冊所提到的產品規格及資訊僅供參考，內容亦會隨時更新，恕不另行通知。本使用手冊的所有部分，包括硬體及軟體，若有任何錯誤，華碩沒有義務為其擔負任何責任。

使用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註冊商標或是版權，在此聲明如下：

- Windows、MS-DOS 是 Microsoft 公司的註冊商標
- Adobe、Acrobat 是 Adobe System 公司的註冊商標

版權所有，不得翻印 ©2004華碩電腦

注意！倘若本產品上之產品序號有所破損或無法辨識者，則該項產品恕不保固！

產品名稱:	華碩 RX 3141 路由器
手冊版本:	T1742 V1.00
發表日期:	2004 年 12 月

## 華碩電腦公司ASUSTeK COMPUTER INC.(亞太地區)

### 市場訊息

地址 : 台灣臺北市北投區112立德路15號  
電話 : +886-2-2894-3447  
傳真 : +886-2-2890-7798  
電子郵件 : info@asus.com.tw

### 技術支援

免費服務電話 : 0800-093-456  
服務時間 : 週一至週五 AM 9:00 ~ PM 9:00  
週六、日 AM 9:00 ~ PM 6:00  
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 : +1-502-608-4555  
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  
電子郵件 : sales@asuscom.de  
線上連絡 : www.asuscom.de/sales

### 技術支援

電話 : 49-2102-9599-0 .....主機板/其他產品  
49-2102-9599-10 .. 筆記型電腦  
傳真 : 49-2102-9599-11  
線上支援 : www.asuscom.de/support

本使用手冊包含了所有當您在使用本產品時所需的相關資訊，各章節的內容安排如下：

## 章節說明

### 1. 介紹

您可以在本章節中發現諸多華碩所賦予 RX3141 的優異特色，利用簡潔易懂的說明及圖示，迅速掌握華碩 RX3141 的各項功能及特性。

### 2. 認識您的 RX3141

本章節中將介紹 RX3141 的產品包裝、硬體規格，與功能燈號配置，讓您可以在最短的時間內對 RX3141 路由器能初步的認識。

### 3. 快速安裝手冊

本章節介紹 RX3141 的基本安裝及相關週邊裝置的使用方法，讓您能夠迅速地掌握 RX3141 的各項操作技巧。

### 4. 使用設定管理員

本章節介紹 RX3141 所搭載之網路管理介面的各項功能設定。

### 5. 路由器設定

本章將指導您如何進行區域與廣域網路的連線設定。

### 6. 設定 DHCP 伺服器

本章提供您關於 DHCP 的知識與相關設定方式。

### 7. 設定靜態路由

本章提供您關於路由方面的知識與相關設定。

### 8. 設定 DDNS

本章提供您關於 DDNS 的相關設定方式。

### 9. 設定防火牆 / NAT 設置

本章提供您關於防火牆與 NAT 等相關設定方式。

### 10. 虛擬伺服器與特別應用程式

本章提供您關於虛擬伺服器的相關設定方式。

### 11. 系統管理

本章提供關於設定 RX3141 時，IP 位址、網路遮罩與子網路設定的相關資訊。

### 12. IP 位址、網路遮罩和子網路

本章提供您關於 DHCP 的知識與相關設定方式。

### 13. 疑難排解

本章中將指導您使用 IP 公用程式進行網路連線問題診斷，另外也將提供關於更換系統風扇與簡易維修技巧的資訊。

### 14. 索引

提供本使用手冊中的相關名詞介紹頁面。

---

章節說明 .....	4
使用手冊目錄 .....	5
1. 介紹 .....	9
1.1 產品特色 .....	9
1.2 系統需求 .....	9
1.3 關於這本使用手冊 .....	9
2. 認識您的 RX3141 .....	11
2.1 零件明細表 .....	11
2.2 硬體功能 .....	11
2.3 軟體功能 .....	11
2.4 產品概觀 .....	14
2.5 擺放選項 .....	16
3. 快速安裝手冊 .....	17
3.1 Part 1 — 連接硬體 .....	17
3.2 Part 2 — 設定您的電腦 .....	19
3.3 Part 3 — 快速設定 RX3141 .....	23
4. 使用設定管理員 .....	26
4.1 登入設定管理員 .....	26
4.2 設定頁結構 .....	27
4.3 系統設定概觀 .....	28
5. 路由器設定 .....	29
5.1 區域網路設定 (LAN Configuration) .....	29
5.2 廣域網路的設定 (WAN Configuration) .....	30
6. 設定DHCP伺服器 .....	39
6.1 DHCP (動態主機配置協定) .....	39
7. 設定靜態路由 .....	42
7.1 IP 路由概述 .....	42
7.2 靜態路由 .....	42
8. 設定 DDNS .....	45
8.1 DDNS 參數設定 .....	46
8.2 設定 HTTP DDNS 用戶端 .....	46
9. 設定防火牆/NAT 設置 .....	47
9.1 防火牆概述 .....	47
9.2 路由器安全設定 .....	49
9.3 ACL 規則參數設定 .....	51
9.4 設定入埠 ACL 規則 .....	54

# RX 系列

---

9.5 設定出埠 ACL 規則 .....	56
9.6 設定自我存取 ACL 規則 — (Firewall → Router Setup → Self-Access) .....	59
9.7 防火牆登錄 — (Router Setup) .....	61
10. 虛擬伺服器與特別應用程式 .....	62
10.1 NAT 概述 .....	62
10.2 設定虛擬伺服器 .....	63
10.3 設定特別應用程式 .....	66
11. 系統管理 .....	69
11.1 登入密碼與 System-Wide 設定 .....	69
11.2 檢視系統資訊 .....	71
11.3 設定日期與時間 .....	71
11.4 恢復至出廠預設值 .....	72
11.5 更新韌體 .....	73
11.6 重新啟動系統 .....	75
11.7 系統設定管理 .....	76
12. IP 位址、網路遮罩，與子網路 .....	79
12.1 IP 位址 .....	79
12.2 IP 位址架構 .....	79
12.3 網路等級 .....	80
12.4 子網路遮罩 .....	80
13. 移難排解 .....	82
13.1 使用IP 公用程式診斷問題 .....	83
14. 索引 .....	85

## 圖示目錄

圖 2.1. 前面板 LEDs .....	14
圖 2.2. 後背板 .....	15
圖 3.1. 硬體連接示意圖 .....	18
圖 3.2. 登入畫面 .....	23
圖 3.3. 系統資訊頁面 .....	24
圖 4.1. 設定管理員登入畫面 .....	26
圖 4.2. 典型的設定管理員畫面 .....	27
圖 4.3. 系統資訊頁面 .....	28
圖 5.1. 路由設定 - 區域網路設定 .....	30
圖 5.2. 當計時結束時，您將會被提醒重新登入設定管理員 .....	30
圖 5.3. 網路設定 - 廣域網路設定 .....	31
圖 5.4. WAN - PPPoE 設定 .....	31
圖 5.5. WAN - PPPoE01 設定 .....	33
圖 5.6. WAN - PPPoE02 設定 .....	33
圖 5.7. WAN - PPPoE 區段正面封包使用第一個 ACL 規則設定 .....	34
圖 5.8. WAN - PPPoE 區段正面封包使用第二個 ACL 規則設定 .....	34
圖 5.9. WAN - PPPoE 多重區段的出埠 ACL 規則設定 .....	34
圖 5.10. WAN - 預設的 PPPoE 多重區段的出埠 ACL 規則設定 .....	34
圖 5.11. WAN - PPPoE Unnumbered 設定 .....	35
圖 5.12. WAN - 動態 IP (DHCP 用戶端) 設定 .....	36
圖 5.13. WAN - 靜態 IP 設定 .....	37
圖 6.1. DHCP 伺服器設定頁面 .....	40
圖 6.2. DHCP 借出列表 .....	41
圖 7.1. 路由設定頁面 .....	42
圖 7.2. 靜態路由設定 .....	43
圖 7.3. 路由範例列表 .....	44
圖 8.1. HTTP ddns 主題的網路圖 .....	45
圖 8.2. HTTP DDNS 設定頁面 .....	46
圖 9.1. 路由安全一般設定頁面 .....	51
圖 9.2. 入埠 ACL 規則設定頁面 .....	54
圖 9.3. 入埠 ACL 設定範例 .....	55
圖 9.4. 入埠 ACL 列表範例 .....	55
圖 9.5. 出埠 ACL 設定頁面 .....	57
圖 9.6. 出埠 ACL 設定範例 .....	58
圖 9.7. 出埠 ACL 列表範例 .....	58
圖 9.8. 自我存取 ACL 設定頁面 .....	59
圖 9.9. 自我存取 ACL 設定範例 .....	60
圖 9.10. 防火牆登錄範例 .....	61
圖 10.1. NAT - 映射任何內部 PC 至單一通用 IP 位址 .....	62
圖 10.2. 反面 NAT - 由外部進入的封包依照通訊、連接埠號碼或 IP 位址，被分配到各內部主機 .....	63
圖 10.3. 虛擬伺服器範例 .....	65
圖 10.4. 虛擬伺服器案例 - 入埠的 ACL 規則 .....	66
圖 10.5. 特別應用程式設定頁面 .....	67
圖 10.6. 特別應用程式案例 .....	68
圖 10.7. 出埠的 ACL 規則欄 .....	68
圖 11.1. 系統管理設定頁面 .....	69
圖 11.2. 系統狀態頁面 .....	71
圖 11.3. 日期與時間設定頁面 .....	71
圖 11.4. 工廠預設值重置頁面 .....	72
圖 11.5. 工廠預設值重置確認視窗 .....	73
圖 11.6. 工廠預設值重置計時秒數 .....	73

圖 11.7. 更新韌體頁面	74
圖 11.8. 檔案總管選擇畫面	74
圖 11.9. 更新韌體確認視窗	74
圖 11.10. 韌體更新狀態視窗	75
圖 11.11. 韌體更新倒數計時視窗	75
圖 11.12. 重新啓動系統頁面	75
圖 11.13. 重新啓動系統設定	76
圖 11.14. 重新啓動系統更新倒數計時視窗	76
圖 11.15. 系統設定備份視窗	76
圖 11.16. 系統設定備份畫面 - 檔案下載對話視窗	77
圖 11.17. 系統設定備份畫面 - 儲存檔案所的交談框	77
圖 11.18. 系統備份設定狀態提示	77
圖 11.19. 回復備份系統設定視窗	78
圖 11.20. 回復系統備份設定視窗 - 選擇檔案交談視窗	78
圖 11.21. 回復系統備份狀態提示	78
圖 13.1. 使用封包探測公用程式	83
圖 13.2. 使用 nslookup 公用程式	84

## 列表目錄

表 2.1. RX3141 提供的 DoS 攻擊類型防護/偵查	13
表 2.2. 前面板 LEDs 狀態說明	14
表 2.3. 後背板插座與指示燈說明	15
表 3.1. 燈號指示列表	18
表 3.2. 預設值摘要	25
表 4.1. 常用按鍵與圖示的功能敘述	28
表 5.1. 區域網路參數設定	29
表 5.2. 廣域網路的 PPPoE 參數設定	32
表 5.3. 廣域網路 PPPoE Unnumbered 參數設定	35
表 5.4. 廣域網路靜態 IP 參數設定	37
表 6.1. DHCP 參數設定	40
表 7.1. 靜態路由參數設定	43
表 8.1. DDNS 參數設定	46
表 9.1. 路由器安全基本參數設定	49
表 9.2. DoS 攻擊定義	50
表 9.3. ACL 規則參數設定	51
表 10.1. 虛擬伺服器參數設定	64
表 10.2. 常見應用程式連接埠號列表	64
表 10.3. 特別應用參數設定	66
表 10.4. 常見應用程式連接埠號列表	67
表 12.1. IP 位址架構	79



---

## 1. 介紹

恭喜您成爲RX3141的使用者。您的區域網路（LAN）現在將能透過使用 ADSL 或 Cable modem來使用高速寬頻連接網際網路。

### 1.1 產品特色

- LAN：4埠 Gigabit 交換器
- WAN：10/100Base-T 乙太網路，提供您區域網路中所有電腦進行網際網路的存取。
- 防火牆與 NAT（Network Access Translation）功能確保您區域網路連接網際網路時的安全性。
- 透過DHCP伺服器自動分發網路位址。
- 包括IP路由、DNS和DDNS設定服務。
- 可透過如微軟 Internet Explorer 6.0 或更新版本的網路瀏覽器，進行程式設定。

### 1.2 系統需求

爲了使用 RX3141 進行網際網路的存取，你必須有以下相關配備：

- 具備 ADSL 或 Cable modem 與對應的連線服務，並具備至少一組網際網路位置以指定給 WAN 使用。
- 一台或更多裝設有支援 10Base-T、100Base-T、1000Base-T 乙太網路傳輸速率網路介面卡（NIC）的個人電腦。
- 若您想要將交換器連接至四部或更多的個人電腦，則您需要具備一台乙太網路集線器/交換器。
- 爲了提供 Web-based GUI 設定需要：您的個人電腦必需安裝有微軟 Internet Explorer 6.0 或更新版本的網頁瀏覽器。

### 1.3 關於這本使用手冊

#### 1.3.1 提示符號的說明

本手冊針對首字縮寫是當他們在本文裡出現第一次時加以定義。

爲了手冊章節的整體簡潔性，RX3141 有時會被稱爲路由器或閘道器。

## RX 系列

---

在提到某個地方的一組乙太網路連線的電腦時，區域網路（LAN）與網路（network）將會交替使用。

滑鼠的行動順序由“→”來表示。舉例來說，Router Setup → Connection，代表雙按點選 Router Setup 選單，接著並點選 Connection 子目錄。

### 1.3.2 印刷樣式的說明

黑體字是用來表示在功能表或其他電腦顯示頁面中選中項目。

### 1.3.3 特別資訊

這本使用手冊使用下列圖示來提醒您注意特殊的說明與解釋。



---

**說明:** 進一步的資訊說明。

---



Definition

---

**重要:** 重點提示說明。

---



WARNING

---

**警告:** 禁止不當行為及操作，提醒您在進行某一項操作時要注意安全。

---

---

## 2. 認識您的 RX3141

### 2.1 零件明細表

- 除這份資料之外，RX3141 應該帶著如下內容來：
- 路由器主機
- AC 電源供應器
- 乙太網路線

### 2.2 硬體功能

#### 區域網路 (LAN)

- 4 埠區域網路交換器
- 自動速度協調
- 支援9KB Junbo Frame
- 4 K MAC 位址列表和自動學習與更新

#### 廣域網路 (WAN)

- 10/100M 乙太網路
- 自動 MDI/MDIX

### 2.3 軟體功能

#### 2.3.1 NAT 功能

RX3141 提供 NAT 功能來分享高速網際網路連線並節省區域網路主機多重連線的連線成本。本項功能可以隱藏網路位址避免其公開。本功能會分配虛擬網路位址給連接到路由器的區域網路電腦，而對外則以同一公開的網路位址進行連線。而本項功能也提供有反向的 NAT 能力，它可讓使用者架設如 E-mail、Web 伺服器在內的多個主機。NAT 規則主導傳輸架構，而以下便是 RX3141 所支援的 NAT 類型。

- NAPT (網路位址與連接埠轉譯，Network Address and Port Translation) — 亦被稱做 IP 偽裝或 ENAT (增強 NAT，Enhanced NAT)。指定許多內部主機透過一組全球有效的 IP 位址來連線。而這項指定工作通常都是透過一個用來轉譯的網路連接埠位址池來進行。每一個封包都是透過此一全球有效的 IP 位址進行傳輸。

- 反向 NAT — 亦被稱做入埠指定，連接埠指定或虛擬伺服器。任何來到路由器的封包都可被重新放置到一內部主機中連接埠的埠號與/或 IP 位址也是基於此項規則加以指定。當多重服務是由不同的內部主機主導時，這項功能是非常有用的。

### 2.3.2 防火牆功能

整合於 RX3141 中的防火牆功能提供下列功能來保護您的網路環境免於遭受攻擊，並避免您的網路被利用作為發動攻擊的跳板。

- 封包檢查 (Stateful Packet Inspection)
- 封包過濾 (ACL)
- 防範 DoS 攻擊
- 登入記錄

#### 2.3.2.1 封包檢查 (Stateful Packet Inspection)

RX3141 防火牆利用「封包狀態檢查」功能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。

#### 2.3.2.1 封包過濾 (Packet Filtering - ACL)

ACL 規則是建立網路安全基本過濾作業之一。防火牆會監控每一個獨立的封包，並解讀其出埠與入埠的標頭資訊。這項功能是以 IP 位址為對象的網路存取控制法。防火牆常會和過濾器合併，以允許或否決使用者進入或離開區域網路的能力。封包過濾法也可用於根據封包的來源地來決定接受或拒絕封包（如 E-mail），以確保在私人網路上的安全性。

ACL 能提供一個子網與另一個子網的隔離保護。從而達到被保護的網路堵塞回傳的具體封包類型，能被用來作網路裡的第一個防守線。

RX3141 防火牆 ACL 規則支援：

- 基於目的地與來源 IP 位址、埠號與通訊協定的過濾方式。
- 使用萬用字元 Wild card 組成過濾規則。
- 過濾規則優先權。

### 2.3.2.3 防範 DoS 攻擊

RX3141 的防火牆具有一攻擊防範引擎，用以保護內部網路免於遭受來自網際網路已知類型的攻擊。本功能提供對於阻絕服務攻擊（DoS attack）的保護，像是 SYN Floodig、IP Smurfing、LAND、Ping of Death 與所有可能被假定的攻擊。舉例來說，RX3141 的防火牆功能提供對於“WinNuke”一種被廣泛用來自遠端網際網路癱瘓視窗作業系統的攻擊。此外，R X3141 的防火牆功能也提供多種來自網際網路的攻擊，像是 IP spoofing、Ping of Death、Land Attack 與 封包重組攻擊。

表2.1 下表中所列舉者為 RX3141 提供的攻擊類型防護/偵查

DoS 攻擊的類型	攻擊的名稱
封包重組式攻擊	Bonk , Boink , Teardrop(New Tear) , Overdrop , Opentear , Syndrop , Jolt , IP fragmentation
ICMP攻擊	Ping of Death , Smurf , Twinge
Flooders 攻擊	只紀錄 ICMP Flooder , UDP Flooder , SYN Flooder
連接埠掃描	只紀錄TCP SYN 掃描 丟棄攻擊封包： TCP XMAS掃描, TCP Null 掃描, TCP Stealth 掃描
PF規則的保護	Echo-Chargen , Ascend Kill
其他類的攻擊	IP spoofing , LAND , Targa , WinNuke

### 2.3.2.4 應用層閘道 (ALG)

應用程式如 FTP 需打開基於各自應用參數的動態連線。當封包通過建置在 RX3141 的防火牆時，依據所屬的應用程式，會需要一個相對應的入埠允許規則。當缺少此項規則時，封包會被 RX3141 的防火牆所阻擋。但為多種應用程式建立這些規則並不可行（亦在安全上缺乏折衷性）。應用層閘道可以智慧地解析應用程式的封包並打開動態的入埠規則連結。RX3141 裡的 NAT 功能針對常用的應用程式如 FTP 及 Netmeeting 等建立了相當數量的 ALG。

### 2.3.2.5 登入紀錄 (Log)

發生於網路環境中的事件，將有可能是企圖影響網路安全性的因素。而這些事件都會被紀錄在 RX3141 的系統登錄檔案中。這個登入記錄至少會維持包含有封包送達、防火牆動作記錄與原因在內最小的登入記錄。

## 2.4 產品概觀

### 2.4.1 前面板

在前面板上包含有用來表示路由器狀態的 LED 指示燈。

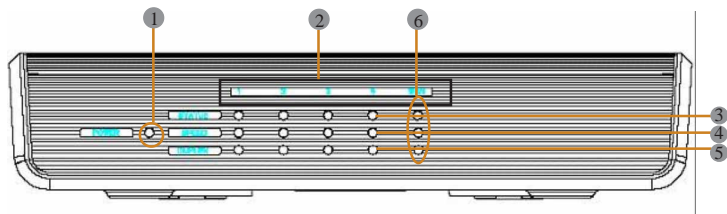


圖2.1 前面板 LEDs

表2.2 前面板 LEDs 狀態說明

LED 標籤	顏色	狀態	標示意義
① Power	綠色	在上 離開	RX3141被給通電 RX3141被切斷電源
② 1 - 4			識別區域網路LEDs 港口。3 LEDs 表明每個區域網路連接埠的狀態：狀態，速度和雙工。
③ STATUS	綠色	恆亮 閃爍 熄滅	乙太網路連線已建立且運作中 資料正被傳送或接收 沒有乙太網路連線
④ SPEED	綠色 橘色	恆亮 恆亮 熄滅	速度是1000Mbps 速度是100Mbps 速度是10Mbps或是沒有連線被建立。
⑤ DUPLEX	橘色	恆亮 閃爍 熄滅	區域網路正用全雙工模式操作。 區域網路正用半雙工模式操作，衝突（collision）正發生。 區域網路連接埠正用半雙工模式操作，沒有衝突被發現。
⑥ WAN			識別WAN 連接埠
③ STATUS	綠色	恆亮 熄滅	乙太網路連線已建立且運作中。 沒有乙太網路連接被建立。
④ SPEED	綠色	恆亮 閃爍	速度是100Mbps 綠色：資料正被傳送或接收
	橘色	恆亮 閃爍 熄滅	連線速度為10Mbps 資料正被傳送或者接收 沒有建立連線。
⑤ DUPLEX	橘色	恆亮 熄滅	區域網路連接埠正用全雙工模式。 區域網路連接埠正用半雙工模式運作，沒有衝突被發現。

## 2.4.2 後背板

後背板包含有區域網路（LAN）與廣域網路（WAN）連接埠、電源供應器插座與系統重置鍵。

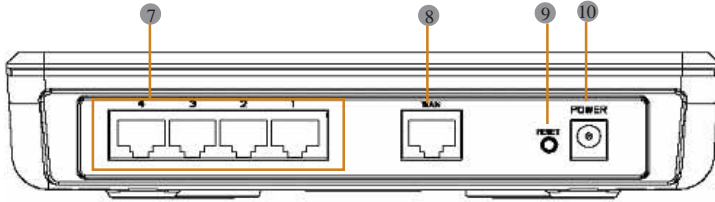
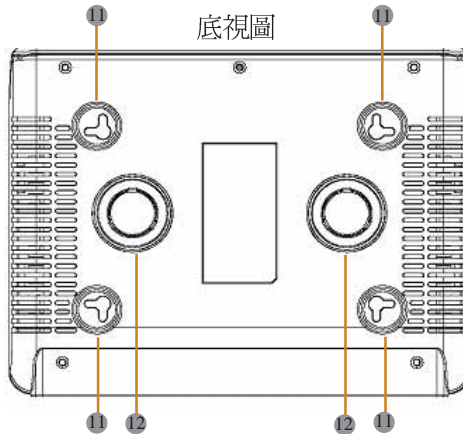


圖2.2 後背板插座

表2.3 後背板插座與指示燈號說明

標籤	標示意義
①	1 - 4 區域網路連接埠：請使用乙太網路纜線連接至您PC的乙太網路連接埠，或是連接到您集線器/交換器的 uplink 埠。
②	WAN WAN 連接埠：連接你的 WAN 端設備，例如ADSL 或Cable modem。
③	RESET 重置按鈕 重新啟動設備 如按住本按鍵超過5秒，則會將系統設定值重置回出廠預設值。
④	POWER 電源輸入插座：連接產品提供的AC電源供應器。



- ① 壁掛插孔：你可以使用這插孔來將 RX3141 掛在牆上放置以保留空間。您可以依照室內插座的位置、電源線的長度，與乙太網路纜線長度等需求來決定懸掛的位置。此外您也可以任意以本路由器的四個方位：前面板、後背板、左側與右側朝上的方式加以懸掛。
- ② 磁鐵：本路由器上的磁鐵可讓您將RX3141放置於任何金屬表面以節省擺放空間。

### 2.5 擺放選項

取決於您的環境，您可以為RX3141放置選擇3種支援的方法：平放、磁鐵吸附、壁掛安裝。

#### 2.5.1 桌面放置

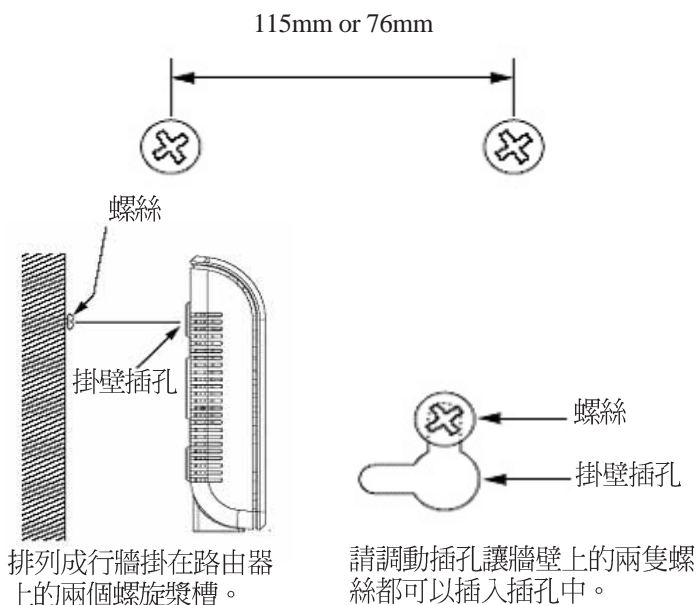
您可將RX3141放置於任何平面上。採用節省空間設計的RX3141只需佔用您桌面上的局部空間即可擺放。

#### 2.5.2 磁鐵吸附介紹

此外，也可以將RX3141 放置於任何磁鐵可吸附的金屬表面，如桌上型電腦機殼或機櫃等處。

#### 2.5.3 壁掛安裝介紹：

1. 先將兩隻螺絲固定於牆壁上，若您想以前面板或後背板朝上壁掛，則請讓兩隻螺絲相隔約 115 mm。此外，請確認兩隻螺絲是等高的，並請注意在 RX3141 機身底部是有四個壁掛插孔，您可任意選擇其中兩個相鄰插孔進行安裝。



2. 請將螺絲以上圖所標示的間距水平固定於牆上，接著將路由器底部的兩個螺絲插孔對準牆上的螺絲置入插孔中。接著請調整螺絲在插孔中的位置使交換器與牆上的螺絲穩固密合。



## 3. 快速安裝手冊

本快速安裝手冊可以提供將 RX3141 連接到電腦、網路與網際網路的基本介紹。

- Part 1 提供關於硬體安裝的相關介紹。
- Part 2 敘述如何在您的電腦端進行網際網路選項的設定。
- Part 3 引導您對 RX3141 進行基礎設定，讓您的區域網路可以連線到網際網路。

在安裝與設定本裝置後，請遵循 3.3 節的說明以確認交換器可以正常運作。

這迅速的入門指南假定你已經與你的互聯網服務供應商 (ISP) 建立 ADSL 或者電纜數據機服務。這些指令提供應該與你的家或者小的辦公室網路安裝相容的一個基本的構造。為附加構造指示參考隨後的章。

### 3.1 Part 1 — 連接硬體

在 Part 1 中，請您先將本裝置連接到 ADSL 或 Cable Modem（已連接電話線或是有線電視纜線），並接妥電源與您的個人電腦相連。



在你開始之前，為全部設備關掉動力。這些包括你電腦(s)，你的區域網路中心(如果適用)接通，以及 RX3141。

圖3.1 說明硬體連接。請依照以下步驟來進行正確的安裝。

#### 3.1.1 Step 1. 連接 ADSL 或 Cable Modem

對於 RX3141 來說：請將乙太網路纜線的一端連接到本裝置後背板標示有 WAN 的連接埠，並將網路纜線的另一端連接到 ADSL 或 Cable modem 的乙太網路連接埠。

#### 3.1.2 Step 2. 連接電腦或網路

如果您區域網路的電腦不超過4 部，則您可以使用乙太網路纜線直接連接 RX3141後背板上任一標示有 1-4 的區域網路連接埠。至於網路纜線的另一端則連接到個人電腦上的乙太網路連接埠。

而若是您的區域網路擁有超過 4 部以上的電腦，則您可以將乙太網路纜線的一端至集線器或交換器（一般來說是連接在集線器或交換器上的 Uplink 埠，請參閱集線器或交換器的相關安裝文件取得正確安裝訊息），至於另一端則連接到本裝置後背板上標示有 1-4 的區域網路連接埠。接下來在使用乙太網路纜線逐一連接集線器或交換器與您區域網路中電腦的乙太網路連接埠。

## RX 系列

請注意無論是雙絞或是直行的乙太網路線，只要交換器或集線器支援辨識這兩個種類的乙太網路線，便都可以用來連接內建交換器、個人電腦。

### 3.1.3 Step 3. 連接 AC 電源供應器

請將 AC 電源供應器的一端連接到本裝置後方的 POWER 電源插座，並將電源供應器另一端的插頭插到室內插座上。

### 3.1.4 Step 4. 開啓 RX3141、ADSL 或 Cable Modem 的電源並啓動您的電腦

請將 AC 電源供應器的一端連接至 RX3141 的電源插座。接著將 ADSL 或 Cable Modem 的電源開啓。最後請將您的電腦或像是無線網路基地台、交換器、集線器的電源開啓。

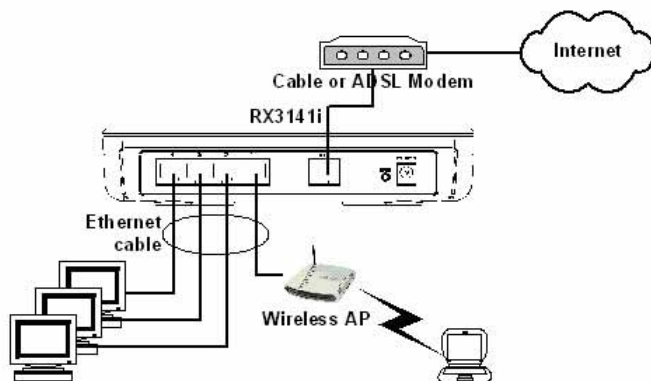


圖3.1 硬體連接示意圖

你應該確認本裝置上的 LEDs 燈號如同表格 3.1 所標示的一樣。

表 3.1 燈號指示列表

LED 標示	代表意思是：
POWER	綠色指示燈號所代表的是交換器的電源已開啓。若本燈號未亮起，請檢查連接於 RX3141 的電源供應器插頭是否妥善地連接在電源插座上。
1-4 STATUS LED	綠色指示燈號表示本裝置已與您的區域網路建立連線，而要是本燈號閃爍，代表本裝置正在傳送或接收來自於您區域網路個人電腦的資料。
WAN	綠色燈號代表本裝置已與您的 ISP 或是網際網路成功建立連線。而要是本燈號閃爍，代表本裝置正在網際網路傳送或接收資料。

如果 LEDs 燈號如同預期般地正確亮起，則代表本裝置正常運作中。

---

## 3.2 Part 2 — 設定您的電腦

本使用手冊的第 2 部分提供在您的電腦上針對 RX3141 進行相關網路設定的介紹。

### 3.2.1 在你開始之前

在預設值下，RX3141 會自動指定所有的您個人電腦端所需要的網路設定（如 IP 位址、DNS 伺服器 IP 位址、預設閘道器 IP 位址）。您只需設定讓您的個人電腦接受 RX3141 所提供的相關設定值。



有時候，如你想要針對網路進行手動設定，而非全部交由 RX3141 負責。此時請參閱「為您的個人電腦指定靜態 IP 位址」中的介紹。

---

如果你已經由乙太網路連接您的個人電腦與 RX3141，請依照您個人電腦中所安裝的作業系統對照下列說明進行設定。

### 3.2.2 安裝 Windows XP 作業系統之個人電腦：

1. 在 Windows 作業系統的工作列中，點選 <開始> 鍵接著點選控制台。
2. 點選網際網路連線圖示。
3. 在網際網路連線視窗中，點選符合您網路介面卡(NIC)的圖示並選擇 <內容>（通常此圖示會標示為區域連線）的正確點選和選擇特性。
4. 在區域連線的內容視窗中的對話欄位，會顯示目前已安裝的網路元件。
5. 請確認對話欄位中標示有網際網路協定 TCP/IP 的選項已勾選，並點選 <開始> 鍵。
6. 在網際網路協定內容的對話欄位中，請點選確定自動取得 IP 位址，並點選確定自動取得 DNS 伺服器位址，並且點選 <特性> 按鈕。
7. 連續點選兩次 <確定> 鍵來確認您的變更，接著請關閉控制台。

### 3.2.3 安裝 Windows 2000 作業系統之個人電腦：

首先，檢查 IP 協定和如有必要，請加以安裝：

1. 在 Windows 作業系統工作列中，點選 <開始> 鍵並指向設定，然後點選控制台。
2. 雙按網路和撥號連線圖示。

## RX 系列

---

3. 在網路和撥號連線視窗中，請以滑鼠右鍵點選區域連線圖示，並選擇內容。

區域網路連線內容選項會列出目前已安裝的網路元件。如果目錄包括網際網路協定 (TCP/IP)，則代表協定已開啓，請直接閱讀步驟 10。

4. 如果網際網路協定 (TCP/IP) 沒有顯示已安裝元件，則請點選<安裝>鍵。
5. 在選擇網路元件類型的選項中，選擇協定，然後點選<新增>按鈕。
6. 在通訊協定列表中選擇 Internet Protocol (TCP/IP) 接著點選<確定>鍵。
7. 若提示訊息出現，請點選<確定>鍵來套用新的設定值並重新啓動您的電腦。

接下來，請設定您的個人電腦來接受 RX3141 所指定的 IP 位址：

8. 在控制台中，點選網路和撥號連線圖示。
9. 在網路和撥號連線視窗中，請以滑鼠右鍵點選區域連線圖示並選擇內容。
10. 在區域連線內容選項中，請選擇 Internet Protocol (TCP/IP)，接著點選<確定>鍵。
11. 在網際網路協定 (TCP/IP) 的選項中，請點選確定自動取得 IP 位址，並點選確定自動取得 DNS 伺服器位址。
12. 連續點選兩次<確定>鍵來確認您的變更，接著請關閉控制台。

### 3.2.4 安裝 Windows 95、98 或 ME 作業系統的个人電腦

1. 在Windows作業系統工作列中，點選<開始>鍵並指向設定，然後點選控制台。
2. 點選網路圖示。

在網路選項中，請尋找起始為“<TCP/IP>”和包含有您網路配接卡名稱的登錄列，然後點選<內容>鍵。您可能需要捲動列表來尋找此登錄列。如果列表中包含有此一登錄列則表示 TCP/IP 協定已被啓用，請直接參閱步驟 8。

3. 如果通訊協定 (TCP/IP) 並未顯示已安裝此一元件，請點選<新增>鍵。
4. 在選擇網路元件類型的選項中，選擇協定並點選<新增>鍵。
5. 在製造商列表框裡選擇 Microsoft，並在網路協定列表中點選 TCP/

---

IP，接著並點選 <確定> 鍵。

6. 若提示訊息出現，請點選 <確定> 鍵來套用新的設定值並重新啓動您的電腦。

接下來，請設定您的個人電腦來接受 RX3141 所指定的 IP 資訊：

7. 在控制台視窗中，點選網路圖示。
8. 在網路選項中，請尋找起始為 “<TCP/IP>” 和包含有您網路配接卡名稱的登錄列，然後點選<內容>鍵。
9. 在網際網路協定 (TCP/IP) 的選項中，請點選確定自動取得 IP 位址。
10. 在 TCP/IP 內容選項中，點選“預設閘道器”標籤頁中的“新增閘道器”欄位輸入 192.168.1.1（此數值為 RX3141 預設的區域網路連接埠 IP 位址），並點選 <新增> 鍵來新增預設的網路閘道器登錄。
11. 點選 <確定> 鍵來確認並儲存您的變更，接著請關閉控制台。
12. 若提示訊息要您重新啓動電腦，則請點選 <確定> 鍵來套用新的設定值並重新啓動電腦。

### 3.2.5 安裝 Windows NT 4.0 Workstation 作業系統的個人電腦：

首先，檢查 IP 協定，如有必要，請進行安裝：

1. 在 Windows NT 工作列中，點選 <開始> 按鈕並指向設定，然後點選控制台。
2. 在控制台視窗中，請點選網路圖示。
3. 在網路選項中，點選協定標籤頁。

在協定標籤頁中，會列出目前已安裝的通訊協定。如果列表中包含 TCP/IP 通訊協定，則代表作業系統已安裝並啓動該通訊協定，如已安裝，則請直接參閱步驟 9。

4. 如果通訊協定 (TCP/IP) 並未顯示已安裝此一元件，請點選 <新增> 鍵。
5. 在通訊協定選項中，請點選 TCP/IP，接著請點選 <確定> 鍵。

您可能會看到需要從您的 Windows NT 安裝光碟或其他儲存媒體中安裝檔案的提示訊息，此時請依照螢幕指示來安裝檔案。

在所有檔案安裝完畢後，一個視窗會出現通知您有一 TCP/IP 服務 DHCP 能夠動態指定 IP 資訊。

## RX 系列

---

6. 點選 <是> 鍵進入下一步，接著若是訊息提示您重新啓動電腦，請點選 <確定> 鍵來重新啓動電腦。接下來請設定您的個人電腦使其可以接受 RX3141 此指定的 IP 位址。
7. 開啓控制台視窗，接著請點選網路圖示。
8. 在網路選項中，點選協定標籤頁。
9. 在協定標籤頁中，請選擇 TCP/IP 並點選 <內容> 鍵。
10. 在 Microsoft TCP/IP 內容選項中，請點選確定從 DHCP 伺服器取得 IP 位址。
11. 連續點選兩次 <確定> 鍵來確認您的變更，接著請關閉控制台。

### 3.2.6 指定靜態 IP 位址給您的個人電腦

有時候，您可能不想依照 RX3141 所指定的 IP 位址，而想要直接把 IP 位址分配給部分或是所有的個人電腦（通常稱做固定 IP）。在下列的狀況您可能需要進行這樣的設定（非必需）：

- 你已經取得一組或更多的對外 IP 位址，而您想要每次可以直接連線到這些特定的電腦（舉例來說，如果您的電腦是做為網路伺服器的用途）。
- 在您的區域網路中，您分別處於不同的子網路下。

不過，在您第一次設定 RX3141 時，在 192.168.1.0 的網路環境下，您可以指定 192.168.1.2 的 IP 位址給您的 PC，以便建立個人電腦與 RX3141 間的連線，在此一網路環境下，在預設的區域網路中，RX3141 的 IP 被預先設定為 192.168.1.1，並輸入 255.255.255.0 與 192.168.1.1 分別做為預設的子網路遮罩與預設閘道器。而上述這些設定值也將會反映到您的真實網路環境中。

在您想要指定靜態 IP 位址的每部個人電腦中，請依照 3.2 節中的介紹來檢查 IP 通訊協定是否已安裝，接下來請依照指示來顯示每個網際網路通訊協定 (TCP/IP) 的內容。接著請以點選本選項內容來開啓手動輸入 IP 位址、DNS 伺服器，與預設閘道器的設定值。



---

您的個人電腦 IP 位址必需與 RX3141 區域網路 (LAN) 連接埠處於相同的子網路中。若您想手動指定 IP 位址給予您區域網路中所有的個人電腦，則您可以依照第五章中的介紹來變更區域網路連接埠的 IP 位址。

---

### 3.3 Part 3 — 快速設定 RX3141

在第3部分，請您登入 RX3141 的設定管理員（Configuration Manager）並對您的路由器進行基礎設定。您的 ISP 必需提供給您設定所需的相關資訊以便完成這些步驟。請注意本節的用意在於讓您可以經由基本設定讓 RX3141 可以快速地啟動與運作，所以在敘述上採用較為簡潔精要的方式表達。若您想取得更多進一步資訊，請參考對應章節。

#### 3.3.1 設定 RX3141

請依照下列步驟來設定 RX3141：

1. 在您進入 RX3141 的設定管理員（Configuration Manager）之前，請先確定您網路瀏覽器的 HTTP proxy 設定已關閉。在微軟 Internet Explorer 中，請點選“工具”→“網際網路選項”→“連線”標籤頁→“區域網路設定”，接著請取消勾選“在您的區域網路使用 Proxy 伺服器”。
2. 在連接到 RX3141 上任一區域網路連接埠的個人電腦端，請開啓您的網路瀏覽器並在瀏覽器的位址欄輸入下列的 URL 並按下 <Enter> 鍵：

http://192.168.1.1

這是在 RX3141 上的區域網路連接埠所預先設定的 IP 位址。

接著如圖 3.2 所示一個登入視窗便會出現。



圖3.2 登入畫面

3. 如果你在連接 RX3141 時發生任何問題，則你可能要檢查您的個人電腦端是否設定為接受 RX3141 是所指派的 IP 位址，至於另一個方式便是將您個人電腦設定處於 192.168.1.0 的網路環境下，像是 192.168.1.2。

輸入您的使用者名稱與密碼，接著並點選  來進入設定管理員（Configuration Manager）。若您是第一次進入此一設定介面，請輸入下列預設的使用者名稱與密碼。

預設使用者名稱：	admin
預設密碼：	admin



你可以隨時變更密碼（在參閱第11.1 節登入密碼）。

每當您登入設定管理員時，系統資訊頁面頁式便會顯示出來（如圖 3.3所示）。



圖3.3 系統資訊頁面

4. 請遵照第 5 章 “Network Setup” 來為RX3141 進行LAN 與 WAN 的設定。

在為RX3141 完成基本設定之後，請閱讀以下內容來決定您是否可以連線至網際網路。

### 3.3.2 測試您的設定

在這個部分，您必需開啓任何連接至 RX3141 的區域網路電腦透過 ADSL 或 Cable Modem 來連線至網際網路。

若要測試連線到網際網路，請先打開你的網路瀏覽器，並且輸入任何外部網站的 URL（像是 <http://www.asus.com>）。接著標示 WAN 的燈號應該會快速閃爍並在連線到網站後，該燈號便維持恆亮狀態。然後，您便可以透過網路瀏覽器來瀏覽網站。

若 LEDs 燈號並未如預期般亮起或是無法連接至網站，則請參閱附錄 13 的相關疑難排解。



### 3.3.3 預設路由器設定

除了您 ISP 所提供的 DSL 連線服務外，RX3141 也可以提供多種的網路服務。本裝置乃是預先設定做為典型家庭或是小型辦公室用途。

表3.2 列舉一些最重要的預設值；這些與其他功能都將在其後的章節中詳細敘述。如果您對於網路環境設定較為熟悉，請再次檢查表 3.2 中所列舉出的項目，來確認這些項目皆可以符合您網路環境的需求。如有需要，則請依照本使用手冊中的敘述來變更這些設定。而若是您對網路設定不甚熟悉，則請先試著不要去變更設定值，或者請與您的 ISP 聯繫請求協助。

在您變更任何設定前，請再次參閱第 4 章來取得使用設定管理員的相關資訊。我們強烈建議您在進行任何預設設定的變更前，請先與您的 ISP 聯繫。

表3.2 預設值摘要

項目	預定設計	解釋/ 指示
DHCP (動態主機配置協定)	DHCP 伺服器開啓 下列的位址範圍： 192.168.1.100 至 192.168.1.149	RX3141 持有內部 IP 的位址池以作為動態指定給區域網路電腦之用。若要使用本項服務，您必需如同快速安裝指南第 2 部分一般先行設定電腦端讓電腦可以接受 RX3141 所配發的 IP 資訊。請見 6.1 節來取得更多關於 DHCP 服務的解釋。
區域網路連接埠 IP 位址	靜態的 IP 位址：192.168.1.1 子網路遮罩：255.255.255.0	這是在 RX3141 上的區域網路連接埠的 IP 位址。區域網路連接埠將本裝置連線到乙太網路。一般而言，您不需要變更此一地址。請參閱 5.1 節區域網路設定中的相關介紹  區域網路 IP 位址指示

# 4. 使用設定管理員

RX3141 包含有一預先安裝的設備管理員程式，此一程式提供安裝於本裝置中的一個軟體介面。這項功能可以讓您針對本裝置進行設定以符合您的網路環境需求。您可以透過與 RX3141 之區域網路或廣域網路連接埠連接的個人電腦中的網路瀏覽器進行設定。

在本章節中，將會針對使用設定管理員工能有一基本的描述與指導。

## 4.1 登入設定管理員

設定管理員為預先安裝於 RX3141 中的工具程式。如欲進入此程式，您需要具備以下條件：

- 如同快速安裝指南一章中之敘述，您需擁有一台連接至RX3141 上之區域網路或廣域網路連接埠的個人電腦。
- 電腦中安裝有網路瀏覽器。此一工具程式是專為在微軟 IE 6.0或更新版本的網路瀏覽器上獲得最佳執行效果所設計的。

你可以從任何連接於 RX3141 區域網路或廣域網路連接埠的電腦連線進入此程式。然而在本章節所提供的介紹是以連接於 RX3141 區域網路之個人電腦進行步驟式解說。

1. 從一部區域網路中的電腦，開啓網路瀏覽器並在瀏覽器的位址欄輸入下列網址（或位置），接著按下 <Enter> 鍵：

http://192.168.1.1

這是在RX3141上之區域網路連接埠所預先規定的IP 位址。接著如圖4.1所示，會顯示出登入視窗。



圖4.1 設定管理員登入畫面

輸入您的使用者名稱與密碼，接著點選 **Apply**。

當您第一次登入本程式，請輸入下列預設值：

預設使用者名稱：	admin
預設密碼：	admin



你可以隨時變更密碼（在參閱第 11.1 節登入密碼與全球系統設定）。

每當您登入設定管理員時，系統資訊頁面便會顯示出來（如圖 4.2 所示）。




## 4.2 設定頁結構

典型的設定頁由下列數種元素：選單邊框、選單、選單導覽要訣、設定，與線上說明所組成。您可以點選選單中的任何選項來延伸或縮小選單群組，或是開啓特定的設定頁面。內嵌設定是您要針對 RX3141 設定值進行設置而與設定管理員產生互動的區域。至於選單導覽要訣則會顯示如何透過選單來進行現階段頁面的設定。

The screenshot shows the 'Advanced / DHCP Server' configuration page for the ASUS RX3141 router. The page is annotated with labels: '選單邊框' (Menu Frame) at the top, '選單' (Menu) on the left sidebar, '設定' (Settings) in the main content area, and '線上說明' (Online Help) on the right. The DHCP Server Configuration section includes fields for IP Address Pool (Begin: 192.168.1.100, End: 192.168.1.149), Lease Time (86400), Default Gateway (192.168.1.1), and DNS/WINS server addresses.

圖4.2 典型的設定管理員頁面

### 4.2.1 選單導覽
















- 開啓相關選單的延伸群組：雙擊點選選單或是圖示，。
- 收回相關選單的延伸群組：雙擊點選選單或是圖示，。
- 開啓特定的設定頁面，點選選單或是圖示，。

## RX 系列

### 4.2.2 通用的按鍵與圖示

下列的按鍵與圖示通用於本工具程式中。至於下表中則是敘述每個按鍵與圖示的功能。

表 4.1 常用按鍵與圖示的功能敘述

按鍵/圖示	功能
	儲存任何您在本頁面所進行的設定。
	在系統中新增設定，如靜態路由或是防火牆 ACL 規則等。
	修改系統中一已存在的設定，如靜態路由或是防火牆的 ACL 規則等設定。
	重新顯示更新後的狀態或設定。
	對選擇頁進行編輯。
	刪除已被對擊的選擇項。
	瀏覽
	回復到上一動
	取消
	確定
	開啓
	儲存
	關閉目錄
	開啓目錄
	圖示

### 4.3 系統設定概觀

如要檢視系統整體的設定，請先登入設定管理員，接著請點選 System → Status 選單。圖 4.3 所展示的，便是在 System Information 頁中可取得的範例資訊。

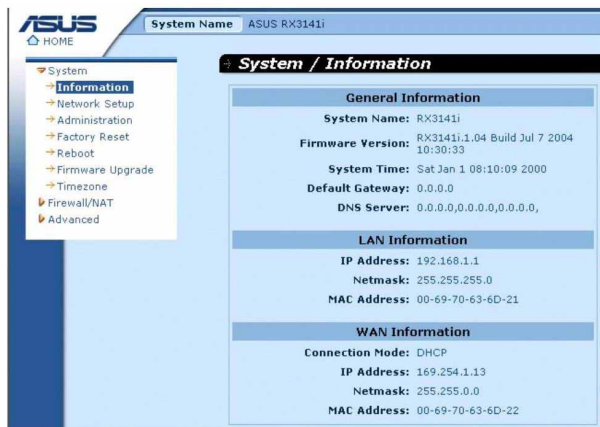


圖4.3。系統資訊頁面

## 5. 路由器設定

這章將描述怎樣為您的路由器進行基本的設定，以便讓您區域網路中的電腦可以相互連線並可以連接到網際網路。網路設定包含有區域網路（LAN）與廣域網路（WAN）兩方面的設定。

### 5.1 區域網路設定（LAN Configuration）

#### 5.1.1 區域網路的 IP 位址

如果您將 RX3141 用在多重 PC 的區域網路環境，則您必需使用內建乙太網路交換器來將您區域網路的電腦連接到乙太網路連接埠。您也必需指定為每個在您區域網路中的每台裝置指定一特定的 IP 位址。在您區域網路中的電腦必需與 RX3141 處在同一子網路下。RX3141 預設的區域網路 IP 位址是 192.168.1.1。



一個網路節點可以被認為是一個設備連接網路的任何界面，例如 RX3141 的區域網路連接埠與您個人電腦中的介面卡。請參閱附錄 12 中對於子網路的相關解釋。

你可以變更 IP 位址以反應在您的網路環境下所想使用的真實 IP 位址。

#### 5.1.2 區域網路參數設定

表 5.1 敘述區域網路 IP 設定中可以進行的參數設定。

表 5.1 區域網路參數設定

設定	描述
主機名	僅作為辨識之用。
IP 位址	RX3141 的區域網路 IP 位址。此一 IP 位址是您的電腦用來辨識區域網路連接埠。請注意！由您 ISP 所指派給您的 IP 位址不等於您區域網路的 IP 位址。對外的 IP 位址是用來辨識 RX3141 連接到網際網路的廣域網路（WAN）連接埠之用。
子網路遮罩	區域網路的子網路遮罩是區域網路 IP 位址的一部份，用遮罩可識別區域網路中的主機屬於哪部分的網路。而這些部分可視為網路環境中的節點。您的路由器裝置已經將子網路遮罩設定為預設值 255.255.255.0。

#### 5.1.3 設定區域網路的 IP 位址

請依照下列步驟來變更區域網路預設的 IP 位址。

1. 首先請先登入設定管理員，並雙按點選 Router Setup → Connection 選單。路由設定頁面接著會如圖 5.1 所示顯示出來。
2. （非必需步驟）輸入 RX3141 的主機名稱。請注意！主機名稱僅供辨識之用，並不能用於其他的用途。

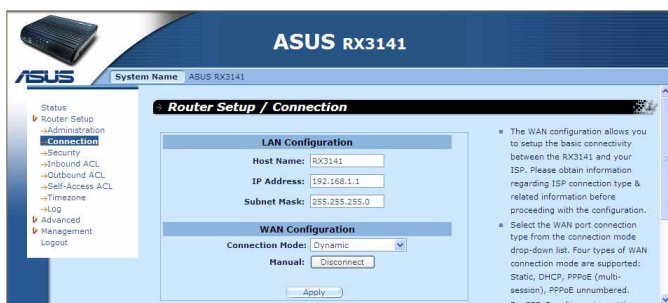


圖5.1 路由設定 - 區域網路設定

3. 輸入 RX3141 所提供的區域網路 IP 位址與子網路遮罩。
4. 若您還未設定廣域網路 (WAN) 連接埠，參考廣域網路 (WAN) 設定一節中的介紹，來進行廣域網路連接埠的設定。
5. 點選  來儲存設定。如果你正使用一個乙太網路連線，當變更 IP 位址時，連線狀態將會中斷。
6. 接著您將會看見如下圖所顯示的訊息。

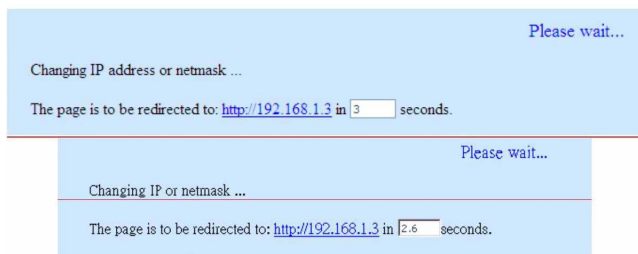


圖5.2 當計時結束，您將會被提醒重新登入設定管理員。

## 5.2 廣域網路的設定 (WAN Configuration)

本節中將會敘述如何對 RX3141 連線到您的 ISP 之廣域網路介面進行相關的設定。在本節中，您將可學習到如何為您的廣域網路環境設定 IP 位址、DHCP 伺服器，與 DNS 伺服器。

### 5.2.1 廣域網路的連接模式

RX3141 支援四種廣域網路的連線模式，分別是 PPPoE (multi-session)，PPPoE unnumbered，靜態 IP 與動態 IP 位址，可依照您 ISP 的連線方式，如圖 5.3 所示在網路設定頁面中的下拉式選單，選擇對應的連線模式。

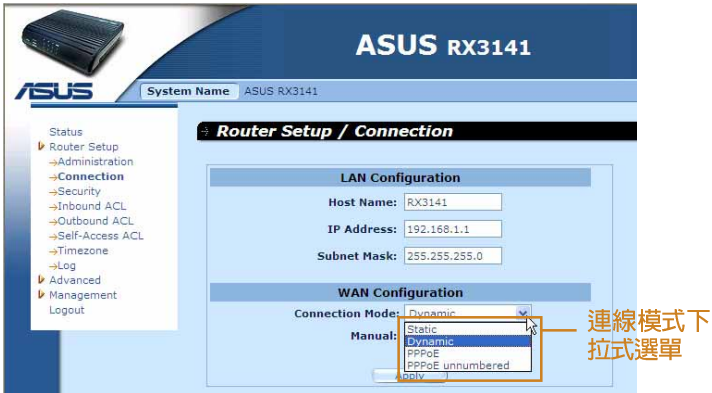


圖5.3 網路設定 - 廣域網路設定

## 5.2.2 PPPoE

PPPoE 連線模式是 ADSL 服務提供廠商最常採用的連線模式。



圖5.4 WAN — PPPoE 設定

### 5.2.2.1 廣域網路的PPPoE 參數設定

表 5.2 描述提供給PPPoE 連接模式的設定參數。


## RX 系列

表 5.2 廣域網路的 PPPoE 參數設定

設定	描述
連線模式 (Connection Mode)	從連線模式下拉式選單中選擇 PPPoE。
PPPoE 區段 (PPPoE Session)	請在本項目中選擇 PPPoE 區段 ID。請注意！本項目最多只支援兩組同時並行的 PPPoE 區段。
開啓(Enable)	勾選或取消勾選本選項來啓動此一 PPPoE 區段。
Connection on Demand	按下“Enabled”或“Disabled”圖示按鍵，就可以啓用或關閉這項功能。
Disconnect after Idle (min)	輸入當你的網路連線在多久時間內無任何傳輸流量時，即進行斷線動作。若您建立的數值為 0 時，則表示不進行斷線動作。請注意 SNTP 服務的動作，可能會干擾這個服務功能的進行。
使用者名稱與密碼 (User Name and Password)	請輸入您用來登入 ISP 連線的使用者名稱與密碼（請注意此一使用者名稱與密碼不同於您要登入設定管理員所需輸入的使用者名稱與密碼）。
服務名稱 (Service Name)	輸入您 ISP 所提供的服務名稱。此項目並非必需輸入的，但某些 ISP 要求輸入此項目。
AP Name	輸入您 ISP 的集中器位址名稱。此項目並非必需輸入的，但某些 ISP 要求輸入此項目。
IP Address	輸入一個靜態 IP 位址，當您的服務提供者要求您需要一個靜態 IP 給 PPPoE 來連結使用。這個 IP 位址必須是由您的服務提供者所提供。大部分的服務提供者不會要求使用者在 PPPoE 上輸入靜態 IP 位址。
Primary /Secondary DNS Server	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，請輸入提供的 IP 位址。
狀態 (Status)	On：在 PPPoE 的連線已建立。 Off：無 PPPoE 的連線建立。 Connecting：RX3141 正試圖使用 PPPoE 連線模式連線到您的 ISP。
手動斷線/連線(Manual Disconnect/Connect)	點選 Disconnect 或 Connect 按鍵來中斷或連接您的服務是提供者的 PPPoE 連線模式。

### 5.2.2.2 為廣域網路設定 PPPoE 連線

請依照下列步驟來進行 PPPoE 連線設定：

1. 開啓 Router Connection，藉由雙按點選 Router Setup → Connection 選單來開啓設定頁面。
2. 從 WAN 連線模式的下拉式選單中如圖 5.5 選擇 PPPoE。
3. 從 PPPoE 區段 ID 下拉式選單中選擇 PPPoE 區段 ID。以目前來說，最多支援兩個區段。
4. 輸入由您的 ISP 所提供的使用者名稱與密碼。
5. 若您的 ISP 需要，請輸入服務名稱（非必需）。
6. 輸入關於“Disconnect after idle (min)”與“Connect on Demand”的適當設定值。
7. 點選  來儲存設定值。



### 5.2.2.3 設定 WAN 的多重 PPPoE 區段

請依照下列步驟，如以下圖 5.4 的方式，來進行多重 PPPoE 區段設定：

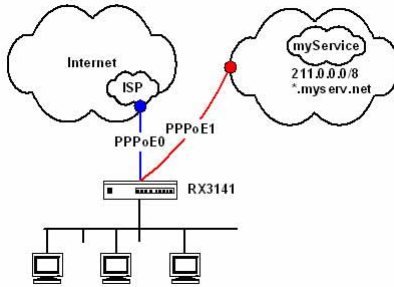


圖5.4 WAN — 多重 PPPoE 區段

1. 開啓 Router Connection畫面，雙按點選 Router Setup → Connection 選單來開啓設定頁面。
2. 參考 5.2.2.2 節的設定方式來進行設定 PPPoE。請注意最多支援兩組 PPPoE 區段。以下的圖片，則顯示如何設定兩組 PPPoE 區段。

WAN Configuration

Connection Mode: PPPoE

PPPoE Session: 0

Enable:

Connect on Demand:  Enable  Disable

Disconnect after Idle(min): 10

User Name: userName0

Password: \*\*\*\*\*

Service Name: (Optional)

AC Name: (Optional)

IP Address: 0.0.0.0 (Optional)

Primary DNS Server: 0.0.0.0 (Optional)

Secondary DNS Server: 0.0.0.0 (Optional)

Status: OFF

Manual: Disconnect

Apply

Thu, 2004/10/20 上午 12:37

圖5.5 WAN — PPPoE 01 設定

WAN Configuration

Connection Mode: PPPoE

PPPoE Session: 1

Enable:

Connect on Demand:  Enable  Disable

Disconnect after Idle(min): 10

User Name: myUsername1

Password: \*\*\*\*\*

Service Name: (Optional)

AC Name: (Optional)

IP Address: 0.0.0.0 (Optional)

Primary DNS Server: 0.0.0.0 (Optional)

Secondary DNS Server: 0.0.0.0 (Optional)

Status: OFF

Manual: Disconnect

Apply

圖5.6 WAN — PPPoE 02 設定

3. 設定防火牆出埠的 ACL 規則指定預定的 PPPoE 區段。請參考第9.5 節關於設定 ACL 規則的說明。圖5.7 和圖5.8 則是顯示設定的兩組 ACL 出埠規則，一個使用網路位址及子網路遮罩來指定目標網路，另一個則使用網域名稱。這兩個 ACL 規則只有其中一個需要建立。然而，如果您打算使用 IP 位址與網域名稱來存取“myService”網路，您就必須將兩者皆做規則設定。

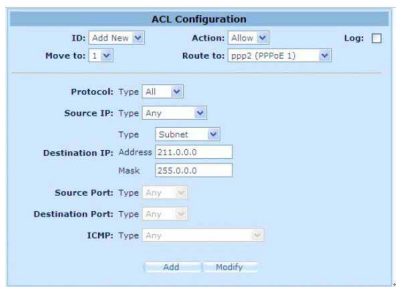


圖5.7 WAN - PPPoE 區段正向封包使用第一個 ACL 規則設定（使用網路位址/子網路遮罩）

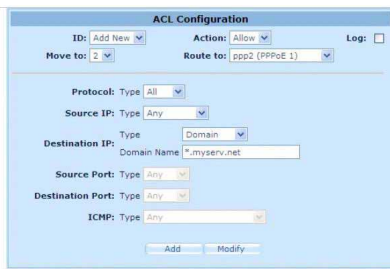


圖5.8 WAN - PPPoE 區段正向封包使用第二個 ACL 規則設定（使用網域名稱）

4. 參考下圖可以讓您於” Existing Outbound ACL” 欄中，來驗證所完成的 ACL 規則建立。注意圖中的第三項規則是預設的 ACL 規則，可以讓所有的送出的通訊通過防火牆做連線。若您已經刪除，您需設定這項規則（請參考預設的出埠 ACL 設定）。第三項的規則可讓所有出埠通訊經過 PPPoE0，要經過 PPPoE1 的除外。

**Existing Outbound ACL** ▼

	ID	Action	Protocol	Source	Destination	Service
	1	Allow	All	Any	211.0.0.0/255.0.0.0	Any
	2	Allow	All	Any	*.myserv.net	Any
	3	Allow	All	Any	Any	Any

圖5.9 WAN - PPPoE 多重區段的出埠 ACL 規則設定

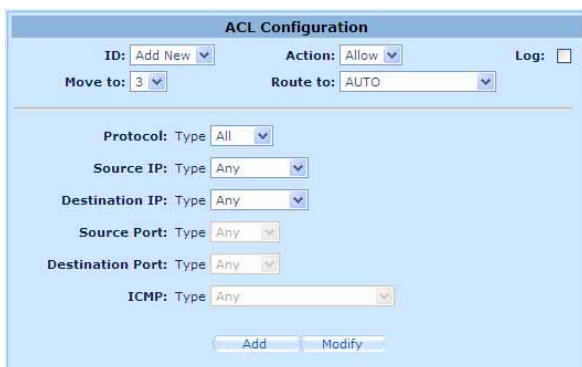


圖5.10 WAN - 預設的 PPPoE 多重區段的出埠 ACL 規則設定

### 5.2.3 PPPoE unnumbered

某些ADSL 服務提供商提供 PPPoE unnumbered 服務。若您的ISP提供這類連線服務，則請選擇此連線模式。



圖 5.11 WAN - PPPoE Unnumbered 設定

#### 5.2.3.1 廣域網路 PPPoE Unnumbered 參數設定

表5.3 描述在 PPPoE unnumbered 連接模式下的參數設定。

表5.3 廣域網路 PPPoE Unnumbered 參數設定


設定	描述
連線模式 (Connection Mode)	從連線模式下拉式選單中選擇 PPPoE Unnumbered。一般而言，每個網路介面都需有其特定的 IP 位址。然而，一組未編號的介面便沒有其特定的 IP 位址。這代表當本項目被選取時，則廣域網路與區域網路便使用相同的 IP 位址。也因為佔用較少的 IP 位址，網路資源可以獲得節省且路由列表也會變得較小。
Enabled NAT	按下這項可以開啓或關閉 NAT 的功能。
Connection on Demand	按下” Enabled” 或” Disabled” 圖示按鍵，就可以啓用或關閉這項功能。
Disconnect after Idle (min)	輸入當你的網路連線在多久時間內無任何傳輸流量時，即進行斷線動作。若您建立的數值為 0 時，則表示不進行斷線動作。請注意 SNTP 服務的動作，可能會干擾這個服務功能的進行。
IP Address	輸入一個靜態 IP 位址給 PPPoE 來連結使用，這個 IP 位址必須是由您的服務提供者所提供。
Unnumbered network address	透過您的 ISP 提供，來輸入一個網路位址。
Unnumbered netmask	透過您的 ISP 提供，來輸入一個子網路遮罩。
使用者名稱與密碼 (User Name and Password)	請輸入您用來登入 ISP 連線的使用者名稱與密碼（請注意此一使用者名稱與密碼不同於您要登入設定管理員所需輸入的使用者名稱與密碼）。
服務名稱 (Service Name)	輸入您 ISP 所提供的服務名稱。此項目並非必需輸入的，但某些 ISP 要求輸入此項目。

## RX 系列

設定	描述
AP Name	輸入您 ISP 的集中器位址名稱。此項目並非必需輸入的，但某些 ISP 要求輸入此項目。
Primary /Secondary DNS Server	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，請輸入提供的 IP 位址。
狀態 (Status)	On : PPPoE unnumbered 的連線已建立。 Off : 無 PPPoE unnumbered 的連線建立。 Connecting : RX3141 正試圖使用 PPPoE unnumbered 連線模式連線到您的 ISP。
手動斷線/連線(Manual Disconnect/Connect)	點選 Disconnect 或 Connect 按鍵來中斷或連接您的服務是供應者的 PPPoE unnumbered 連線模式。

### 5.2.3.2 設定供廣域網路使用的 PPPoE Unnumbered

請依照下列步驟來進行 PPPoE Unnumbered 設定：

1. 打開 Router Connection 設定頁面，並點選 Router Setup → Connection 選單。
2. 從廣域網路連線選單的下拉式選單中，如圖 5.11 所示選擇 PPPoE Unnumbered。
3. 輸入由您的ISP.提供的使用者名稱與密碼。
4. 如果您的ISP 需要，請輸入服務名稱（非必需）。
5. 輸入關於“Disconnect after idle (min)”與“Connect on Demand”的適當設定值。
6. 點選  來儲存設定值。

### 5.2.4 動態 IP (Dynamic IP)

動態 IP 最常為 cable modem 連線服務提供廠商所採用。

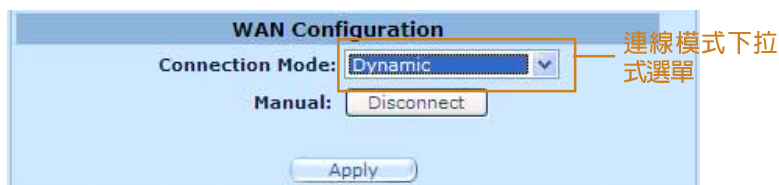



圖5.12 WAN - 動態 IP (DHCP用戶端) 設定

#### 5.2.4.1 設定供廣域網路使用的動態 IP

請依照下列介紹來進行動態 IP 設定：

1. 打開 Router Connection 安裝設定頁面，並雙按點選 Router Setup → Connection 選單。
2. 從廣域網路連線選單的下拉式選單中，如圖 5.12 所示選擇 Dynamic。請注意！主要與次要 DNS 伺服器的 IP 位址是由您的 ISP 之 DHCP 伺服器所指定。
3. 點選  來儲存設定值。

## 5.2.5 靜態 IP

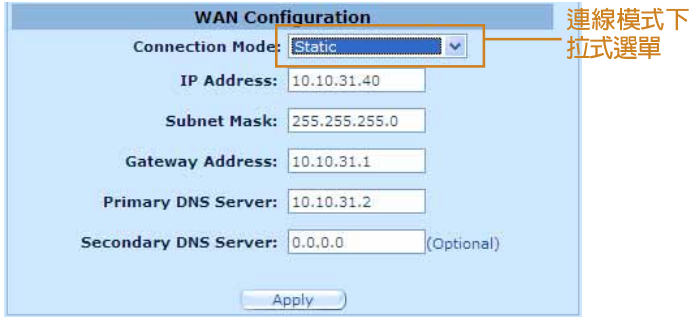


圖5.13 WAN - 靜態 IP 設定

廣域網路靜態 IP 參數設定

表5.4 是描述提供給靜態 IP 連線模式的參數設定。

表5.4 廣域網路靜態 IP 參數設定

設定	描述
連接模式 (Connection Mode)	從連線模式下拉式選單選擇 Static。
IP 位址 (IP Address)	由您的 ISP 提供的廣域網路 IP 位址。
子網路遮罩 (Subnet)	由您的ISP 提供的廣域網路子網路遮罩，一般而言，這項設定是被設定為255.255.255.0。
閘道器位址 (Gateway Address)	由您的ISP 所提供的閘道器IP 位址。該位址必需與 RX3141 的廣域網路處於相同的子網路下。
主要/次要 DNS (Primary/Secondary/DNS Server)	本項目中，您至少需要輸入主要的 DNS 伺服器位址。至於次要 DNS 伺服器 IP 位址則非必需輸入。


### 5.2.5.2 設定供廣域網路使用的靜態 IP

請依照下列介紹來設定靜態 IP 設定：

1. 打開 Router Connection 安裝設定頁面，並雙按點選 Router Setup → Connection 選單。
2. 從廣域網路連線選單的下拉式選單中，如圖 5.13 所示選擇 Static。
3. 在IP 位址輸入欄位輸入廣域網路的 IP 位址。本訊息是由您的 ISP 提供。
4. 輸入廣域網路的子網路遮罩，本訊息是由您的 ISP 提供。一般而言，本項設定值為：255.255.255.0。

## RX 系列

---

5. 輸入由您的 ISP 所提供的閘道器位址。
6. 輸入主要 DNS 伺服器的 IP 位址。本訊息是由您的 ISP 所提供，至於次要 DNS 伺服器 IP 位置則非必需輸入。
7. 點選  來儲存設定值。

---

## 6. 設定DHCP伺服器

### 6.1 DHCP（動態主機配置協定）

#### 6.1.1 何謂 DHCP 伺服器？

DHCP是讓網路管理員能夠統一管理網路環境中，把IP 資訊配發給電腦的一項通訊協定。

當你開啓 DHCP 伺服器後，您可讓像 RX3141 這類的裝置指定暫用的 IP 位址給連線至網路的電腦。這項指定的裝置便稱做 DHCP 伺服器，而接收裝置則稱做 DHCP 用戶端。



如果您依照快速安裝指南的介紹操作。您除了可以指定 IP 位址給予區域網路中的每一部電腦外，也可以指定其動態（自動）接受 IP 資訊。如果您選擇動態接收 IP 位址，則您可以設定您的電腦做為 DHCP 用戶端來接受像 RX3141 這類裝置所配發的 IP 位址。

DHCP伺服器會從一經過定義的IP 位址池中在特定的時間內借出這些IP 位址給提出上網需求的電腦。此外它也會監控、收集，並視需要配發這些 IP 位址。

在啓用 DHCP 的網路中，IP 訊息是經由動態配發而非靜態的。一個 DHCP 用戶端當每次進行網路連線時，便會從 DHCP 伺服器的 IP 位址池中被動態指定不同的 IP 資訊。

#### 6.1.2 為何要使用 DHCP 伺服器？

使用 DHCP 伺服器可以讓您透過使用 RX3141 管理與分配 IP位址。若是沒有 DHCP 伺服器，您便需要分別設定每部電腦的 IP位址與相關資訊。在較大的網路環境或是常擴充網路設備的環境中，DHCP 伺服器是較常被採用的 IP 配發方式。

#### 6.1.3 設定 DHCP 伺服器



預設值中，在區域網路中 RX3141 是被設定做為 DHCP 伺服器，使用預先設定從 192.168.1.100 至 192.168.1.149 的位址池（子網路遮罩則為 255.255.255.0）。若要變更位址範圍，請依照本節中接下來所敘述的步驟進行設定。。

首先，您必需設定您的個人電腦使其可以接收由 DHCP 伺服器所送出的資訊。

1. 請先開啓 DHCP 伺服器設定頁面，如圖 6.1 所示，並雙按點選 Advanced → DHCP Server 選單。

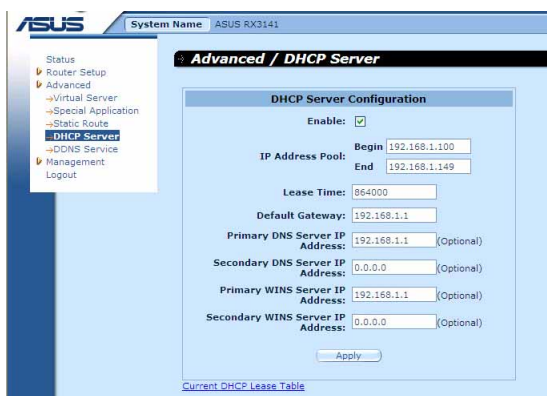


圖6.1 DHCP伺服器設定頁面

- 輸入IP位址時所需資訊（開始/結束位址），子網路遮罩，IP 借出時間與預設閘道器位址，其他像是 DNS 伺服器與主要/次要 WINS 伺服器 IP位址則是非必需輸入項目。然而，仍然建議您在對應空白欄位中輸入主要的DNS伺服器IP位址。在主要DNS伺服器IP位址欄位中，您可輸入區域網路的IP或您的ISP所提供的主要DNS伺服器IP位址。在表 6.1 中將詳細敘述 DHCP 參數設定。

表6.1DHCP 參數設定

欄位	描述
Enable	藉由勾選或取消勾選本選項來開啓或關閉供您在區域網路使用的 DHCP 伺服器。
IP Address Pool Begin / End	指定 DHCP 伺服器位址池中 IP 位址的最高與最低範圍。
Lease Time	以秒為計算單位，指定使用借出 IP 位址之個人電腦使用該 IP位址的時間。
Default Gateway IP Address	從 IP位址池中接收 IP 位址之電腦的預設閘道器位址。預設的閘道器位址是DHCP 用戶端電腦首先用來連接網際網路裝置的 IP 位址。一般而言，這便是指 RX3141 之區域網路連接埠的 IP位址。
Primary / Secondary DNS Server IP Address	網域名稱系統的 IP 位址是被由位址池中取得 IP 位址的電腦所使用。DNS 伺服器會自動轉譯您輸入在網址欄的名稱為數字化的 IP 位址。一般來說伺服器是位於您的 ISP。然而，您可以輸入 RX3141 區域網路 IP 位址把它當作是 區域網路電腦的 DNS proxy 或是轉發來自區域網路至 DNS 伺服器的 DNS 需求，並回復結果至區域網路的電腦。請注意！無論主要或次要的 DNS 伺服器都是非必需輸入的。
Primary / Secondary WINS Server IP Address(optional)	WINS 伺服器的 IP 位址是被由位址池中取得IP位址的點點所使用。您並不需要輸入此項訊息除非您的網路環境中有 WINS 伺服器。

- 點選  來儲存 DHCP 伺服器的設定。



### 6.1.4 檢視目前指定的 DHCP 位址

當RX3141 做為您區域網路中的 DHCP 伺服器使用時，它將會紀錄借出 IP 位址給予您電腦的時間。若要檢視所有 IP位址的配發列表，只要開啓 DHCP 伺服器設定頁面並點選位於頁面下方的“Current DHCP Lease Table”連結，如圖 6.2 所示的頁面便會出現。

DHCP 借出列表將會列出所有借出的 IP 位址與對應的 MAC 位址。



IP Address	MAC Address
192.168.1.100	00-07-40-1C-DC-0B

Reload

圖6.2 DHCP 借出列表

## 7. 設定靜態路由

您能使用設定管理員來為您的網際網路連線定義特定的路由。在本章節中，將會敘述基本路由觀念並提供關於建立靜態路由的相關介紹。請注意！大多數的使用者無需定義靜態路由。

### 7.1 IP 路由概述

對於路由器來說的一大挑戰是：當路由器接受到需送至一特定目的地的資料時，它需要將這份資料送至哪一個裝置？當您定義 IP 路由，您便需要提供這些相關規則來讓 RX3141 可以用來做出傳輸資料到何處的決定。

#### 7.1.1 我需要定義靜態路由嗎？

- 在您區域網路中的電腦，一組預設的閘道器會將所有網際網路傳輸的資料傳送到 RX3141 的區域網路連接埠。而由於您在 TCP/IP 內容所指定的位址，或是您設定區域網路的電腦使其連線到網際網路時動態地自一伺服器獲得，因此您區域網路中的電腦可以查知預設的閘道器位址。（上述內容的每一個步驟都在快速安裝指南的第二部分有相關說明。）
- 在 RX3141 本身，一組預設的閘道器被定義用來導引所有出埠的網際網路傳輸到您的 ISP 的路由器。當裝置開始與網際網路連線進行傳輸時，此一預設的閘道器會由您的 ISP 自動指定。（關於新增預設路由的步驟在 7.2.2 新增靜態路由一節中有進一步的介紹）

若您的家用設定包含有兩組或更多的網路或子網路、連線到兩個或以上的 ISP 服務，或是連線到一遠端辦公室的區域網路，則您需要定義靜態路由。

### 7.2 靜態路由

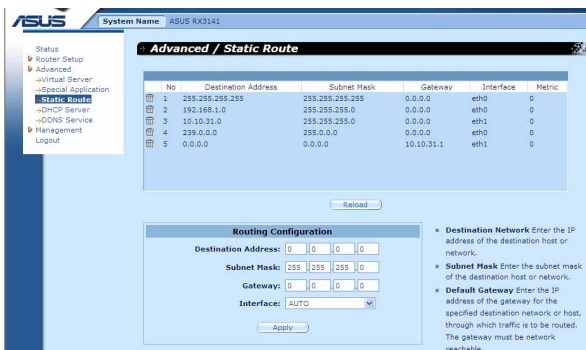


圖7.1 路由設定頁面

## 7.2.1 靜態路由的參數設定

下列表格為可供靜態路由設定的參數設定定義。

表 7.1 靜態路由參數設定

領域	描述
目的地位址	指定目的地電腦或整個目的地網路的 IP 位址。該設定可以都設定為 0 來代表此路由可用於所有未經定義的位址。（這便是建立為預設閘道器的路由）。請注意！目的地 IP 必需為一網路 ID。預設路由採用 0.0.0.0 的目的地 IP 位址，請參考附錄 12 關於網路 ID 的解釋。
子網路遮罩	指電腦位址與網路上其他電腦位址進行比對時所用的一種號碼，這種號碼可以找出屬於相同網域的電腦。請參閱附錄 12 中關於網路 ID 的解釋。預設路由使用 0.0.0.0 做為子網路遮罩。
閘道器	閘道器的 IP 位址。
介面	可供選擇的選項包括 AUTO, Eth0(LAN), Eth1(WAN), PPPoE:0 (unnumbered), PPPoE:1(1st PPPoE session), PPPoE:2(2nd PPPoE session)。這些選項可由下拉式選單中加以選擇。如果選擇 AUTO，路由器會根據閘道器 IP 位址自動指定一組介面。

## 7.2.2 新增靜態路由

The screenshot shows a 'Routing Configuration' window with the following fields and values:

- Destination Address: 0 | 0 | 0 | 0
- Subnet Mask: 255 | 255 | 255 | 0
- Gateway: 0 | 0 | 0 | 0
- Interface: AUTO (selected from a dropdown menu)
- An 'Apply' button is located at the bottom of the form.

圖7.2 靜態路由設定

請依照下列介紹來新增一組靜態路由到路由列表中。

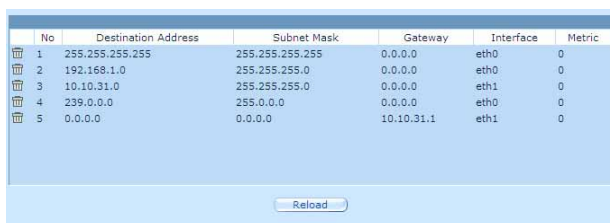
1. 請雙按點選 **Advanced** → **Static Route** 選單的順序來開啓靜態路由設定頁面。
2. 請輸入像是目的地 IP 位址、目的地子網路遮罩、閘道器 IP 位址與介面的靜態路由資訊在對應的欄位中。

如欲取得關於這些欄位的敘述，請參閱表 7.1 靜態路由參數設定。

如要為您的區域網路建立預設閘道器的路由，請在目的地 IP 位址與子網路遮罩欄位都輸入 0.0.0.0。

3. 點選  來新增一組路由設定。


## 7.2.3 刪除靜態路由



No	Destination Address	Subnet Mask	Gateway	Interface	Metric
1	255.255.255.255	255.255.255.255	0.0.0.0	eth0	0
2	192.168.1.0	255.255.255.0	0.0.0.0	eth0	0
3	10.10.31.0	255.255.255.0	0.0.0.0	eth1	0
4	239.0.0.0	255.0.0.0	0.0.0.0	eth0	0
5	0.0.0.0	0.0.0.0	10.10.31.1	eth1	0

圖7.3 路由範例列表

請依照下列介紹來刪除一組靜態路由到路由列表中。

1. 請依照 **Advanced** → **Sstatic Route** 選單的順序來開啓靜態路由設定頁面。
2. 點選  圖示來刪除路由列表中的路由設定。



不要除去預設閘道器的路由，除非你知道你正做什麼。除去預設路由將使得網際網路不能到達。

## 7.2.4 觀看靜態路由表

所有開啓 IP 功能的電腦與路由器都保存有一份被其使用者共同使用的 IP 位址表。對於每一個目的地 IP 位址，此表會列出傳輸資料要經過的第一個跳躍點（hop），此表便被稱作裝置的路由表。

爲了觀看 RX3141 的路由表，請雙按點選 **Advanced** → **Sstatic Route** 選單。接著路由表將會如圖 7.1 所示，被顯示在靜態路由設定頁面的上半部：

路由表會以列顯示的方式顯示每一個包含目的地網路 IP 位址、目的地網路子網路遮罩，與轉發傳輸資料的閘道器 IP 位址。

## 8. 設定 DDNS

動態 DNS 是一種可讓不同的電腦在 IP 位址不斷變動的狀況下（當重新啟動電腦或當 ISP 的 DHCP 伺服器重新配發 IP）使用相同網域名稱的服務。當 WAN IP 位址變更時，RX3141 變會連線到一動態 DNS 服務提供者。本功能可以設定使用網域名稱而非 IP 位址的 WEB、FTP 伺服器等網路服務。此外，動態 DNS 也支援 DDNS 用戶端以下功能：

- 更新 DNS 紀錄
- 強制 DNS 更新

● 本功能僅支援 HTTP DDNS 用戶端。

### HTTP 動態 DNS 用戶端

HTTP DDNS 客戶端使用 DNS 服務提供者所提供的架構來動態升級 DNS 紀錄。在此狀況下，服務提供者會更新 DNS 中的 DNS 紀錄。RX3141 使用 HTTP 來啟動更新作業。RX3141 支援以下列的服務提供者進行 HTTP DDNS 更新。

- [www.dyndns.org](http://www.dyndns.org)

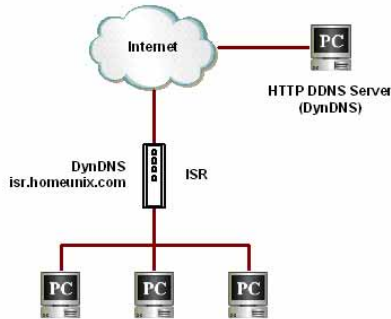


圖8.1 HTTP ddn主題的網路圖

每當 DDNS 介面的 IP 位址變更，則 DDNS 更新會傳送到指定的 DDNS 服務提供者。RX3141 應使用由您 DDNS 服務提供者處所取得的 DDNS 使用者名稱與密碼進行設定。

## 8.1 DDNS 參數設定

表8.1 描述 DDNS 服務中可進行的參數設定。

表8.1 DDNS 參數設定

欄位	描述
狀態	顯示 DDNS 的狀態。
動態 DNS	
Enable	點選此項來開啓 DDNS 服務
Disable	點選此項來關閉 DDNS 服務
網域名稱	請將由您的 ISP 所提供之已註冊的網域名稱填入此欄位。舉例來說，若您的 RX3141 的主機名稱是“host1”，網域名稱是“yourdomain.com”，則具備完整資格的網域名稱（FQDN）便是“host1.yourdomain.com”。
使用者名稱	請在此輸入由您 DDNS 服務提供者所提供的使用者名稱。
密碼	請在此輸入由您 DDNS 服務提供者所提供的密碼。

## 8.2 設定 HTTP DDNS 用戶端

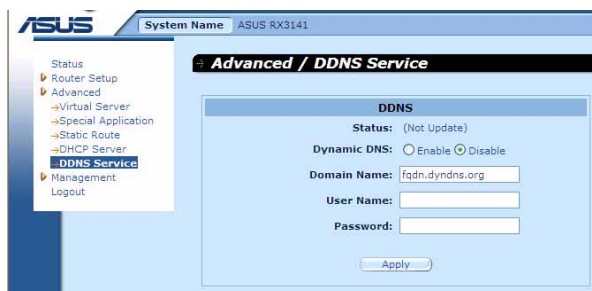


圖8.2 HTTP DDNS設定頁面

請依照以下介紹來設定 HTTP DDNS：

1. 首先，你應已至 DDNS 服務提供者處註冊網域名稱。若您還未進行註冊，請造訪 [www.dyndns.org](http://www.dyndns.org) 以取得更多相關資訊。
2. 登入設定管理員，接著請依照 Advanced → DDNS Service 選單的順序開啓 DDNS 設定頁面。
3. 在DDNS 設定頁面中，請選擇“Enable”動態 DNS。
4. 在網域名稱欄位輸入您所註冊的網域名稱。
5. 輸入由您的DDNS 服務提供者所提供的使用者名稱與密碼。
6. 點選 **Apply** 鍵來傳送 DNS 更新需求到您的DDNS 服務提供者。請注意！當 WAN 連接埠狀態變更時也會傳送DDNS 更新要求至您的 DDNS 服務提供者處。

## 9. 設定防火牆/NAT 設置

RX3141提供內建防火牆/NAT 的功能，這項功能可以讓您分享網際網路連線的同時，也保護您區域網路內的電腦免於遭受阻絕服務 (DoS) 攻擊與其他類型來自網際網路的惡意存取動作。此外，您也可以指定如何監控這些攻擊行為，並設定當這些攻擊發生時會報告網路位址。

本章節將敘述如何設定網路路由的安裝設定與建立/修改/刪除 ACL (Access Control List) 規則，來控制通過您網路環境的資料。您將會使用防火牆設定頁面進行：

- 設定路由安全與 DoS設置
- 建立，修改，刪除與檢視入埠/出埠/自我存取的 ACL 規則。
- 檢視防火牆登錄檔案。

**注意到：**當你定義一個 ACL 規則，便是指示RX3141 檢視每一個它所接收的資料封包並決定該封包是否符合繼續向前傳送的標準。這項標準可以包括網路或網際網路通訊協定，包括傳送封包的電腦 IP 位址、目的地的 IP位址，與其他封包資料的特性（舉例來說，由區域網路至網際網路，或反之亦然）。

若是該封包符合已建立規則的標準，則封包便可被接受（繼續向前傳送至目的地），或是遭到拒絕（放棄），而這些決定要視您所建立的規則而定。

### 9.1 防火牆概述

#### 9.1.1 Stateful 封包檢查

在RX3141中的stateful 封包檢查引擎存有一狀態列表，而這份列表是追蹤所有通過防火牆之封包的連線狀態。若封包屬於符合 stateful 封包檢查引擎中規則的類型，則防火牆會開啓一個“通道”來讓該封包通過；否則，該封包便會被丟棄。而當該通過封包的連線中止這個“通道”便會被關閉。您無需對 stateful 封包檢查進行任何設定，因為這項功能是當防火牆功能啟動時便預設為啟動的。請參閱 9.2.1 “防火牆基本參數設定 (Firewall Basic Configuration Parameters)” 一節中的介紹來開啓或關閉 RX3141 的防火牆服務。

#### 9.1.2 DoS (阻絕服務) 保護

DoS 保護與 stateful封包檢查皆提供您網路環境的第一線防護。當 RX3141 的防火牆功能被啟動後，您無需設定即可開啓上述兩項服務。而在預設值中，防火牆功能是被設定為開啓的。請參閱 9.2.1 “防火牆基本參數設定 (Firewall Basic Configuration Parameters)” 一節中的介紹來開啓或關閉 RX3141 的防火牆服務。

### 9.1.3 防火牆與存取控制列表 (ACL)

#### 9.1.3.1 ACL 規則的優先順序

所有的 ACL 規則都有被指定的規則 ID。較低的規則 ID，擁有較高優先順序。防火牆會以解讀封包標頭訊息的方式來監控網路傳輸，而接著這些標頭資訊會被檢查是否符合 ACL 規則列表中的規則來決定該封包是被放行繼續前往目的地或是被丟棄。

#### 9.1.3.2 ACL規則與連線狀態追蹤

在防火牆中的 stateful 封包檢查引擎會保持追蹤網路連線的狀態與進展。藉由在狀態列表中關於每一連線的儲存資訊，RX3141 可以很快地決定封包是否由一已建立的連線通過。若結果是肯定的，則封包便可以在無需經過 ACL 規則的狀態下通過防火牆。

舉例來說，一個 ACL 規則可以允許自 192.168.1.1 至 192.168.2.1 的 ICMP 封包通過。當 192.168.1.1 傳送一個 ICMP echo (如 ping 封包) 至 192.168.2.1，則 192.168.2.1 將回應一個 ICMP echo reply 至 192.168.1.1。在 RX3141 中，您無需另外建立另一個入埠規則，因為 stateful 封包檢查引擎追蹤記住連線狀態，並允許 ICMP echo 可以通過防火牆回覆。

### 9.1.4 預設的 ACL 規則

RX3141 支援 3 種類型的預設存取規則：

- 入埠存取規則：作為由外部存取您區域網路的管控用途。
- 出埠存取規則：作為控制由您區域網路內之主機向外存取外部網路的用途。
- 自我存取規則：作為控制 RX3141 自身存取動作的用途。

#### 預設入埠存取規則

在預設值中，沒有預設的入埠存取規則。也就是說，所有由外部主機連至內部主機的連線都是被拒絕的。

#### 預設出埠存取規則

在預設值中，預設的出埠存取設定是允許所有來自您區域網路的傳輸使用 NAT 傳至外部網路環境。

#### 預設自我存取規則

這個預設的自我存取規則可以讓 http、ping、DNS、DHCP 透過區域網路來連線 RX3141 路由器。



無需自 ACL 規則列表中移除預設的 ACL 規則！建議設定更高優先權的 ACL 規則來取代預設的規則。

---



## 9.2 路由器安全設定


### 9.2.1 路由器安全基本參數設定

表9.1 說明有關路由器安全的基本參數設定的相關描述。

表 9.1 路由器安全基本參數設定

欄位	描述
防火牆	勾選或取消勾選本選項來開啓或關閉防火牆。
NAT	勾選或取消勾選本選項來開啓或關閉 NAT。
偵測登錄Port Scan	當本項目設定為開啓，則嘗試連線到未開啓的埠會被紀錄。
Stealth 模式	若設定開啓，則 RX3141 將不會回應遠端嘗試對未開啓的 TCP/UDP 埠的連線。

如欲進行路由器安全基本設置，請依照下列介紹進行操作：

1. 開啓 Router Security（路由器安全）設定畫面，雙按點選如圖 9.1 所示 Router Setup → Security 選單，來開啓此設定頁面。
2. 勾選或取消勾選每一個安全選項的獨立選項。
3. 點選  來儲存設定值。

### 9.2.2 DoS 設定

RX3141 有一攻擊防禦引擎以保護內部網路免於遭受服務中止（DoS）攻擊，像是 IP spoofing、LAND、Ping of Death、smurf 與所有這類型的攻擊。此外，它也可以丟棄 ICMP 重新導向與 IP loose/strict 來源路由封包。舉例來說，RX3141 的防火牆可防範來自“WinNuke”用來癱瘓視窗作業系統的攻擊。下表 2.1 便是 RX3141 防火牆可提供保護的 DoS 攻擊類型列表。

## RX 系列

### 9.2.2.1 DoS 保護參數設定

表9.2 提供各種 DoS 攻擊類型的解釋。您可以藉由勾選或取消勾選本選項來開啓或關閉對於這種 DoS 攻擊或察覺的保護。

表 9.2 DoS攻擊定義

欄位	描述
IP Source	入侵者使用“Source routing”來闖入目標系統。
IP Spoofing	Spoofing 便是使用他人的 IP 位址來建立 TCP/IP 的封包。IP spoofing 是一種多重網路攻擊的結合。
Land	攻擊者把來源與目的 IP 位址相同的封包送至系統，並讓目標系統不停地連線到自身 IP 位址。而這種動作將可能導致目標系統的速度大幅下降。
Ping of Death	攻擊者發出容量大於 64KB 的封包，導致部分作業系統當機。
Smurf	攻擊者對一些廣播位址發出 ICMP 回應需求。這些封包帶有欺騙的 IP 來源位址。大多數被攻擊的主機會回應此 ICMP 回應請求，但卻不是回應給真實的來源主機。而被回應封包的主機則變成受害者，且其速度也將會大幅度地降低。
SYN/ ICMP / UDP Flooding	勾選或取消勾選這些本選項來開啓或關閉防止 SYN/ICMP/UDP flood 攻擊的保護功能。此攻擊包括在極短時間內向內部主機發出大量連線要求，但是不全部完成連線。這將導致一些電腦陷入“膠著狀態”（SYN 是 SYNchronize 的簡寫）。如果您想要網路免受此類型的攻擊，則您可以選擇此項。SYN/ICMP/UDP Flooding 保護預設為開啓狀態。
TCP XMAS/ NULL/FIN Scan	駭客可能利用這類特定格式的封包來掃描您的系統，並檢視系統中有何服務。有時候這麼做的目的是為了將來的攻擊預作準備，有時也可能是為了判斷您系統中何種服務較易受到攻擊。 XMAS Scan：是一種以0為序號且設定FIN、URG與 PUSH 位元的 TCP 封包。 NULL Scan：是一種以0為序號，且所有控制位元都設為0的 TCP 封包。 FIN Scan：駭客利用 Stealth 的潛行方式來掃描目標系統的連接埠。駭客這麼做的目的在於找出無需真的去使用 FIN Scan 便可以連線到目標系統。這種掃描方式會試圖關閉伺服器上一組並非真正存在的連線。或是系統也會依伺服器是否可連線而回應不同的錯誤報告。
Teardrop	當 teardrop 攻擊時，攻擊者的 IP 會放出一種混淆的偏移值（Offset Value）。若接收的作業系統未能因應這種狀況，便可能導致當機。
WinNUKE	勾選或取消勾選本選項以開啓或關閉防止WinNuke攻擊的保護功能。一些較舊版本的 Microsoft Windows 作業系統可能會遭受這類攻擊。如果區域網路電腦的作業系統沒有及時下載最新版本的修正程式更新，那麼建議您開啓此項功能。

### 9.2.2.2 進行 DoS 設定

1. 如圖 9.1 所示，開啓 Router Security（路由安全）設定畫面，藉由雙按點選 Router Setup → Security 選單開啓防火牆一般設定頁面。
2. 勾選或取消勾選每一項 DoS 攻擊的選項。
3. 點選  來儲存設定值。

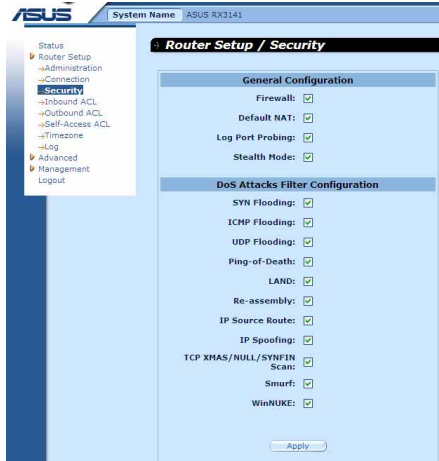


圖9.1 路由安全一般設定頁面

## 9.3 ACL 規則參數設定

### 9.3.1 ACL 規則參數設定

表9.3 敘述防火牆入埠、出埠與自我存取 ACL 規則的參數設定。

表9.3 ACL 規則參數設定

欄位	描述
ID	
Add New	點選本選項來新增 ACL 規則。
Rule Number	從下拉式選單中選擇一個規則，並修改它的設定。
Move	
	本選項可以讓您設定這項規則的優先權。RX3141 的防火牆基於規則的優先權進行運作。藉由在規則列表中指定號碼，便可以設定規則的優先順序：
1(First)	此號碼表示最高優先權。
Other numbers	選擇其他號碼來覺得您所希望設定的優先權順序。

## RX 系列

欄位	描述
Action	
Allow	點選本按鈕來設定 allow 的規則。 當本規則與防火牆結合可讓符合此規則的封包通過防火牆。
Deny	點選本按鈕來設定 deny 的規則。 當本規則與防火牆結合便不會讓符合此規則的封包通過防火牆。
Route to (適用出埠 ACL)	本欄位用來規劃 PPPoE unnumbered 或 PPPoE multi-session 所需的路由。可以選擇的選項有：AUTO、ppp0(unnumbered)、ppp1(1 <sup>st</sup> PPPoE session)、ppp2(2 <sup>nd</sup> PPPoE session)。這些選項可由下拉式選單中加以選擇。若是選擇 AUTO，路由器將基於路由表中的資訊來導引封包。
Log	勾選或不勾選本選項來開啓或關閉本 ACL 規則的登錄記錄。
Protocol	本項目可以讓您由下拉式選單中選擇協定類型。可以選擇的選項有 AII、TCP、UDP、ICMP、IGMP、AH 與 ESP。
Source IP	本項目可讓您設定套用此規則的來源網路。請使用下拉式選單來選擇下列選項：
ANY	本項目可以讓您套用這項規則到來源網路中的所有電腦，就像那些做為入埠傳輸的網際網路電腦或是所有做為出埠傳輸的本地端網路電腦。
IP Address	本項目可以讓您指定一組 IP 位址，在這組 IP 位址上套用該規則。
IP Address	指定合適的網路位址
Subnet	本項目可讓您包含所有連線到 IP 子網路的電腦。當本選項被選擇，則下列欄位將會變成可以填入數值。
Address	輸入合適的 IP 位址。
Mask	輸入對應的子網路遮罩。
Self(僅適用自我存取規則)	代表路由器本身。
Destination IP	本項目可以讓您設定套用該規則的目的網路。請使用下拉式選單來選擇下列項目：
ANY	本項目可以讓您套用該規則到所有做為入埠傳輸的本地端電腦，或是做為出埠傳輸的網際網路電腦。
IP Address, Subnet	選擇這些項目並如同上述 Source IP 一節中所敘述地一樣輸入相關細節。
Self(僅適用自我存取規則)	代表路由器本身。
Domain	要使本選項發揮作用，使用者的電腦必須使用 RX3141 當作它的 DNS 伺服器。當每次系統重新啓動後，都會清除網域名稱 (Domain name) 變數與相連結的 IP 位址。多重的 ACL 規則可以使用相同的網域名稱與 IP 位址連結。 <ul style="list-style-type: none"> <li>最多可以支援 30 組網域名稱變數。</li> <li>當網路用戶端向 RX3141 提出 DNS 需求時，每個可變動的網域名稱變數與 IP 位址連結會更新。當輸入網址" http://www.yahoo.com.tw" 在您的網頁瀏覽器上時，RX3141 將會更新 www.yahoo.com 的 IP 位址在被防火牆參照的內部資料庫中。</li> </ul>

欄位	描述
	<ul style="list-style-type: none"> <li>· 每個網域名稱變數可以結合最多 256 個 IP 位址。</li> <li>· 萬用字元 “*” 可以讓您使用如以下的例子來快速輸入欲尋找的網域名稱：               <ol style="list-style-type: none"> <li>1. www.google.* : 對應 www.google.com 與 www.google.net , 而不對應 www.google.com.tw 。</li> <li>2. www.google.*.* : 可對應 www.google.com.tw 與 www.google.com.sg , 而不對應 www.google.com 。</li> <li>3. .com.tw : 可對應 www.google.com.tw 與 www.com.tw , 而不可對應 com.tw 。</li> <li>4. *.com : 對應 google.com 與 abc.com , 而不對應 www.google.com , com 。</li> <li>5. * : 可對應任何的網域名稱。</li> <li>6. . (僅一個點) : 可對應任何的網域名稱。</li> </ol> </li> </ul>
Source Port	<p>本項目可以讓您設定套用該規則的來源連接埠。請使用下拉式選單來從下列選項選擇一項您想選擇的設定值：</p>
ANY	若您想將本規則套用到具有任意來源埠號碼的所有應用程式，請選擇本項目。
Single	若您想將本規則套用到具有特定連接埠號碼的一個應用程式，則請選擇本項目。
Port Number	輸入來源連接埠號碼
Range	如果你想要這個規則套用到符合此連接埠範圍的應用程式，請選擇本項目。而選擇本項目後，下列欄位便可以輸入設定數值。
Start Port	輸入連接埠範圍開始的號碼
End Port	輸入連接埠範圍結束的號碼
Destination Port	<p>本項目可以讓您設定套用本規則的目的連接埠。您可以使用下拉式選單來選擇以下選項：</p>
ANY	若您想將本規則套用到具有任意來源埠號碼的所有應用程式，請選擇本項目。
Single, Range	選擇這些項目並如同上述 Source Port 一節中所敘述地一樣輸入相關細節。
ICMP (僅於協定的模式設定為 ICMP 時才可使用)	<p>本項目可以讓您選擇在 ACL 規則中的 ICMP 訊息類型。所支援的 ICMP 訊息類型有：</p> <ul style="list-style-type: none"> <li>· Any(預設值) (Default)</li> <li>· 0：回音答覆 (Echo reply)</li> <li>· 1：類型 1 (Type 1)</li> <li>· 2：類型 2 (Type 2)</li> <li>· 3：資料不能傳達：資料無法傳到目的地 (Dst unreachable : destination unreachable)</li> <li>· 4：降低來源封包速度：降低來源封包速度 (Src quench : source quench)</li> <li>· 5：重新定向 (Redirect)</li> <li>· 6：類型 6 (Type 6)</li> <li>· 7：類型 7 (Type 7)</li> <li>· 8：回音要求 (Echo req)</li> <li>· 9：路由廣播 (Router advertisement)</li> </ul>

欄位	描述
• 10	路由請求 (Router solicitation)
• 11	時間超時：時間超過 (Time exceed : time exceeded)
• 12	參數問題 (Parameter problem)
• 13	時間標記請求 (Timestamp request)
• 14	時間標記回應 (Timestamp reply)
• 15	訊息請求：要求訊息報告 (Info request : Information request)
• 16	回覆訊息：訊息回應 (Info reply : information reply)
• 17	請求遮罩位址：遮罩位址請求 (Addr mask req : address mask request)
• 18	回應遮罩位址：遮罩位址回應 (Addr mask reply : address mask reply)

## 9.4 設定入埠 ACL 規則

透過如圖 9.2 所示，在入埠 ACL 規則設立 ACL 規則，您將可以控制（允許或拒絕）連線到您區域網路電腦的外來存取動作。

在此設定頁面中的選項可以讓您：

- 新增一條規則，並設定該項規則的參數
- 修改已存在的規則
- 刪除已存在的規則
- 檢視已設定的 ACL 規則

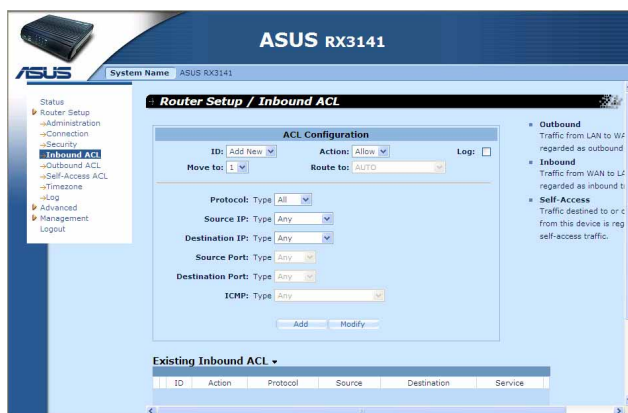


圖9.2 入埠 ACL 規則設定頁面

### 9.4.1 新增入埠 ACL 規則

請依照下面的介紹來新增入埠的 ACL 規則：

1. 開啟出埠 ACL Rule（ACL 規則）設定頁面，如圖9.2 所示，雙按 Router Setup → Inbound ACL 目錄。
2. 從“ID”的下拉式選單中選擇“ADD New”。
3. 在“Action”的下拉式選單中，設定您想要設定的動作（Allow/Deny）。
4. 將變更套用到任一或是所有以下的欄位：來源/目的 IP、來源/目的連接埠、通訊協定、ICMP 訊息類型與記錄。請參閱9.3節中關於這些欄位的解釋。
5. 從“Move to”的下拉式選單中選擇號碼來為這些規則指定優先順序。請注意！這些號碼便是代表優先順序，其中以 1 的優先順序最高。
6. 點選 **Add** 鍵可以建立新的 ACL 規則。新的 ACL 規則稍後會顯示在入埠 ACL 設定頁面中下方的入埠存取控制列表。

圖9.3 顯示如何建立新的規則來允許入埠 HTTP（如 web server）服務。本規則可讓入埠 HTTP 傳輸導向 IP 位址192.168.1.28的主機。請注意新增的 Inbound ACL 規則會顯示在 Existing Inbound ACL 欄裡，如圖 9.4 所示。



圖9.3 入埠 ACL 設定範例

Existing Inbound ACL ▾						
	ID	Action	Protocol	Source	Destination	Service
	1	Allow	TCP	Any	192.168.1.28	80


圖9.4 入埠 ACL 列表範例

### 9.4.2 修改入埠 ACL 規則

請依照以下介紹來修改入埠 ACL 規則：

1. 開啓入埠 ACL Rule（ACL 規則）設定頁面，如圖9.2 所示，雙按 Router Setup → Inbound ACL 目錄。
2. 點選規則中的  圖示來修改入埠 ACL 列表或從"ID"下拉式選單選擇規則編號。
3. 將變更套用到任一或是所有以下的欄位：來源/目的 IP、來源/目的連接埠、通訊協定、ICMP 訊息類型與記錄。請參閱 9.3 節中關於這些欄位的解釋。
4. 點選  鍵來修改 ACL 規則。而稍後 ACL 規則的新設定將會被顯示在入埠 ACL 設定頁面中下方的存取控制列表上。

### 9.4.3 刪除入埠 ACL 規則

如要刪除入埠 ACL 規則，請開啓 Inbound ACL 規則設定頁面，雙按點選 Router Setup → Inbound ACL 目錄，然後要刪除之規則前的  圖示。

### 9.4.4 顯示入埠 ACL 規則

如要檢視既有的 ACL 規則，只要開啓 Router Setup → Inbound ACL 目錄存取入埠 ACL（Inbound ACL Rule）規則設定頁面，現存的入埠 ACL 規則設定項目，則位於設定頁面中的最下方。

## 9.5 設定出埠 ACL 規則

藉由如圖 9.5 所示，在出埠 ACL 規則設定頁面建立 ACL 規則，您可以控制（允許/拒絕）網際網路或您區域網路的外部網路存取。

在這個構造頁裡的選擇允許你：

- 增加並設定此規則的參數
- 修改既有的規則
- 刪除既有的規則
- 檢視已設定的出埠 ACL 規則



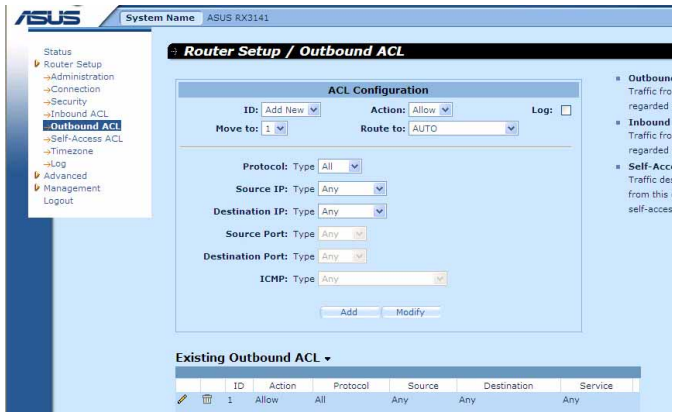


圖9.5 出埠 ACL 設定頁面

### 9.5.1 新增出埠 ACL 規則

爲了增加一個如欲新增出埠 ACL 規則，請依照以下介紹操作：

1. 開啓出埠 ACL Rule（Outbound ACL 規則）設定頁面，如圖 9.5 所示，雙按 Router Setup → Outbound ACL 目錄。
2. 從“ID”下拉式選單選擇“Add New”。
3. 從“Action”下拉式選單選擇您想設定的動作（允許/拒絕）。
4. 從“Move to”的下拉式選單中選擇號碼來爲這些規則指定優先順序。請注意！這些號碼代表修先順序，其中以 1 的優先順序最高。
5. 選擇傳送封包的介面，可以選擇的選項有：AUTO、ppp0 (unnumbered)、ppp1(1<sup>st</sup> PPPoE session)、ppp2(2<sup>nd</sup> PPPoE session)。這些選項可由下拉式選單中加以選擇。若是選擇 AUTO，路由器將基於路由表中的 ACL 規則資訊來導引封包。
6. 將變更套用到任一或是所有以下的欄位：來源/目的 IP、來源/目的連接埠、通訊協定、ICMP 訊息類型與記錄。請參閱 9.3 節中關於這些欄位的解釋。
7. 點選 **Add** 鍵來建立新的 ACL 規則。新的 ACL 規則稍後會顯示在出埠 ACL 規則設定頁面中下方的出埠存取控制列表中。

圖 9.6 顯示如何建立新的規則來允許出埠 HTTP（如 web server）服務。本規則可讓內部 IP 位址 192.168.1.15 的主機之出埠 http 傳輸導向（目的地 Port 80）外部網路的任一主機。請注意新增的 Outbound ACL 規則會顯示在 Existing Outbound ACL 欄裡，如圖 9.7 所示。

圖9.6 出埠 ACL 設定範例

Existing Outbound ACL ▾						
	ID	Action	Protocol	Source	Destination	Service
	1	Allow	All	Any	211.0.0.0/255.0.0.0	Any
	2	Allow	All	Any	*.myserv.net	Any
	3	Allow	All	Any	Any	Any

圖9.7 出埠 ACL 列表範例

## 9.5.2 修改出埠 ACL 規則

1. 開啟出埠 ACL Rule (Outbound ACL 規則) 設定頁面，如圖 9.5 所示，雙按 Router Setup → Outbound ACL 目錄。
2. 點選規則中的 圖示來修改出埠 ACL 列表或從 "ID" 下拉式選單選擇規則編號。
3. 將變更套用到任一或是所有以下的欄位：來源/目的 IP、來源/目的連接埠、通訊協定、ICMP 訊息類型與記錄。請參閱 9.3 節中關於這些欄位的解釋。
4. 點選 鍵來修改 ACL 規則。而稍後 ACL 規則的新設定將會被顯示在出埠 ACL 設定頁面中下方的存取控制列表上。

## 9.5.3 刪除出埠 ACL 規則

如要刪除出埠 ACL 規則，請開啟 Outbound ACL 規則設定頁面，雙按點選 Router Setup → Outbound ACL 目錄，然後要刪除之規則前的 圖示。

## 9.5.4 顯示出埠 ACL 規則

如要檢視既有的 ACL 規則，只要開啟 Router Setup → Outbound ACL 規則設定頁面所示，開啟出埠 ACL 規則設定頁面即可。

## 9.6 設定自我存取 ACL 規則 — (Firewall → Router Setup → Self-Access)

自我存取是針對 RX3141 的存取控制。您可以如圖 9.8 所示，利用自我存取設定頁面來：

- 新增自我存取規則
- 修改既有的自我存取規則
- 刪除既有的自我存取規則
- 觀看既有的自我存取規則

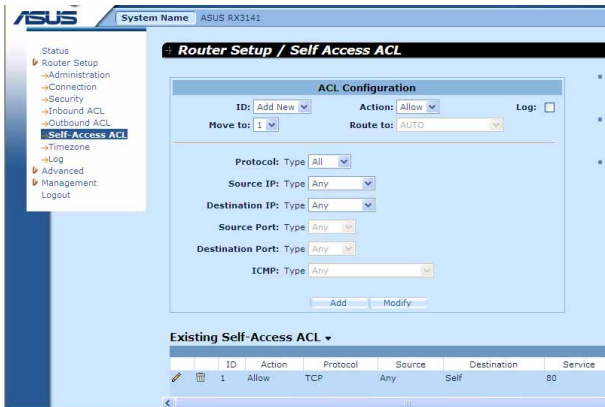


圖9.8 自我存取 ACL 設定頁面

### 9.6.1 新增自我存取規則

如欲新增自我存取規則，請依照以下介紹操作：

1. 開啓 Self-Access 規則設定頁面，如圖 9.8 所示，雙按 Router Setup → Self Access ACL 目錄。
2. 從“ID”下拉式選單選擇“Add New”。
3. 從“Action”下拉式選單選擇您想設定的動作（允許/拒絕）。
4. 從“Move to”的下拉式選單中選擇號碼，來為這些規則指定優先順序。請注意！這些號碼便是代表優先順序，其中以 1 的優先順序最高。
5. 將變更套用到任一或是所有以下的欄位：來源/目的 IP、來源/目的連接埠、通訊協定、ICMP 訊息類型與記錄。請參閱 9.3 節中關於這些欄位的解釋。
6. 點選 **Add** 鍵來建立新的 ACL 規則。新的 ACL 規則稍後會顯示在自我存取規則設定頁面中下方的自我存取控制列表中。

## 例子

圖9.9 顯示讓 TCP port 80之傳輸（如 HTTP 傳輸）自 RX3141通行的自我存取 ACL 設定範例。

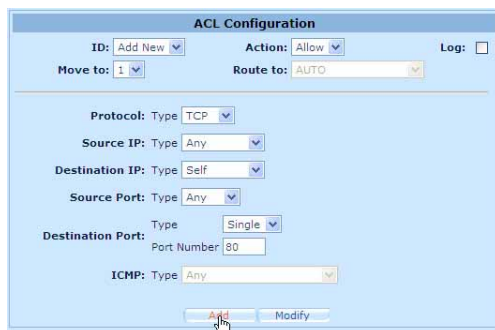




圖9.9 自我存取 ACL 設定範例

## 9.6.2 修改一個自我存取規則

如欲修改自我存取規則，請依照以下介紹操作：

1. 開啓 Self-Access 規則設定頁面，如圖 9.8 所示，雙按 Router Setup → Self Access ACL 目錄。
2. 點選規則中的  圖示來修改自我存取 ACL 列表或從"ID"下拉式選單中既有的自我存取 ACL 列表中選擇自我存取 ACL。
3. 設定您所想要的設定值。
4. 點選  鍵來修改 ACL 規則。而稍後 ACL 規則的新設定將會被顯示在自我存取 ACL 設定頁面中下方的存取控制列表上。

## 9.6.3 刪除一個自我存取規則

如欲刪除自我存取規則，請開啓 Self-Access ACL 規則設定頁面，雙按點選 Router Setup → Self-Access ACL 目錄，然後要刪除之規則前的  圖示。

## 9.6.4 檢視已設定的自我存取規則

如果要檢視自我存取規則，只要藉由開啓 Self-Access ACL 規則設定頁面後，雙按點選 Router Setup → Self-Access ACL 選單來開啓設定頁面即可。


Existing Self-Access ACL ▼							
	ID	Action	Protocol	Source	Destination	Service	
	1	Allow	TCP	Any	Self	80	

圖9.10 檢視自我存取 ACL 設定範例

## 9.7 防火牆登錄 — (Router Setup → Log)

你可以開啓防火牆登錄畫面，雙按點選 Router Setup → Log 選單，來開啓防火牆登錄頁面，並如圖 9.11 所示檢視任何登錄事件。您可以點選登錄頁面下方的 鍵來檢視更新的登錄訊息。

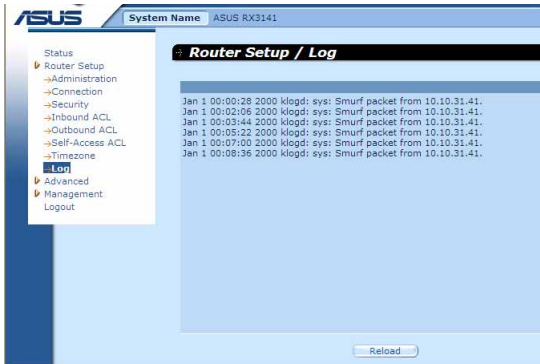


圖9.10 防火牆登錄範例

### 9.7.1 登錄格式

RX3141 支援兩個登錄類型-系統安全登錄和防火牆存取控制登錄，分別以 ” sys ” 及 ” fw ” 兩個關鍵字表示。舉例如下：

系統安全登錄案例：

Jan 1 00:01:22 2000 klogd:sys: TCP XMAS/NULL packet from 192.168.1.100

解說：1月1日 00:01:22 2000 年，指出此時間遭受攻擊事件；klogd: sys，這個攻擊事件被系統安全模組偵測到；TCP XMAS/NULL，所偵測到的攻擊類型；192.168.1.100，攻擊的來源 IP 位址。

登入防火牆存取控制登錄案例：

Jan 1 00:03:11 2000 klogd:fw: OUTBOUND rule=1 allow icmp from 192.168.1.100 to 211.1.1.1 type=8 code=0 id=512

解說：1月1日 00:03:11 2000 年，指出此進入存取的時間；klogd:fw，屬於防火牆存取控制的登錄狀況；OUTBOUND，描述通訊的方向；rule=1，對應到此 IP 訊息的規則號碼；allow，防火牆所取得的動作訊息；icmp，通訊協定的類型；192.168.1.100，通訊的來源 IP；211.1.1.1，通訊的目的地；type=8，ICMP 訊息的類型；code=0，ICMP 通知碼；id=512，ICMP 訊息 ID。

# 10. 虛擬伺服器與特別應用程式

這章節是描述以下的設定步驟：

虛擬伺服器

特別應用

NAT 是用來支援上述應用的技術。

## 10.1 NAT 概述

網路位址轉譯允許使用單一設備，例如RX3141，擔任網際網路（對外網路）與本地網路（私人）的代理。這也就是說 NAT 的 IP 位址可以對外部網路代表內部區域網路一整個群組的電腦。網路位址轉譯（NAT）可以節省廣大網路環境下已註冊之 IP 位址使用，並可以簡化 IP 位址的管理工作。由於 IP 位址的轉譯，NAT 也可以隱蔽網路位址並對區域網路提供某種程度的安全保障。

### 10.1.1 NAPT(Network Address and Port Translation) 或 PAT(Port Address Translation)

NAPT 也稱作 IP 偽裝，這項功能可以將許多內部主機對應到一個有效的對外網際網路位址。這項映射包含有一組用來轉譯的網路連接埠。每一個封包都會透過這個有效的對外網路位址來傳送，而連接埠的號碼也被一組網路連接埠中未使用的連接埠加以轉譯。圖 10.1 顯示所有本地網路的主機透過對應到一個全球通用 IP 位址的方式，和來自未使用的網際連接埠的不同埠號來連結網際網路。

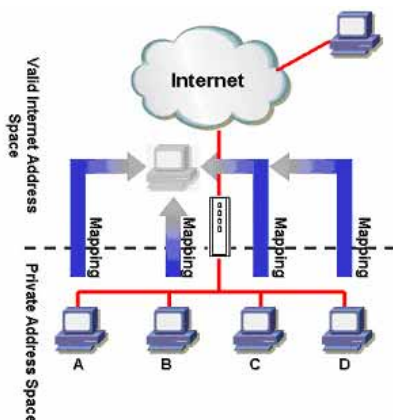


圖10.1 NAPT - 映射任何內部 PC 至單一有效 IP 位址

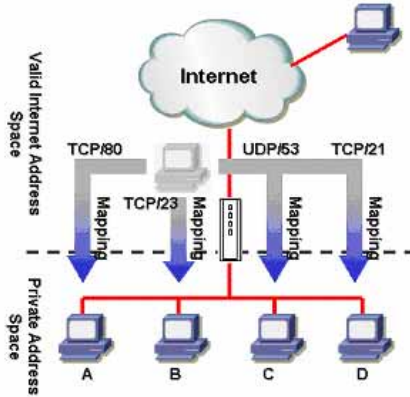


圖10.2 反向 NAT - 由外部進入的封包依照通訊協定、連接埠號碼或 IP 位址，被分配到各內部主機

### 10.1.2 反向NAPT /虛擬伺服器

反向 NAT 也被稱作入埠映射，連接埠映射，或是虛擬伺服器。任何來到 RX3141 的封包，都會依照通訊協定、連接埠號碼或 IP 位址，或依照特定的 ACL 規則被加以分配。當多重服務是由不同的內部主機所負責時，這項功能是相當有用的。圖 10.2 顯示網頁伺服器（TCP/80）是由 PC A 所負責、telnet 服務（TCP/23）為 PC B 所負責、DNS 伺服器（UDP 53）為 PC C 負責，而 FTP 伺服器（TCP/21）則為 PC D 負責。這也就是說，這四種服務的入埠傳輸將會被導向對應這些服務的主機。

## 10.2 設定虛擬伺服器

虛擬伺服器可以讓您設定 10 種對外服務，像是網頁、E-mail、FTP 服務等服務，而這些服務都可以被外來網際網路上的用戶們存取。每一項服務是由一具有靜態 IP 位址的專責伺服器所提供。雖然內部的服務無法為外部使用者所直接使用，但路由器可以辨識提出服務要求的連接埠號碼並將其導向正確的內部伺服器。



RX3141 同一時間只支援一種特定類型的伺服器。

## RX 系列

### 10.2.1 虛擬伺服器參數設定

表格10.1 描述虛擬伺服器的設定參數。

表10.1 虛擬伺服器參數設定

設定	描述
Enabled	從預設的應用程式中選擇一個應用程式。而對應的通訊協定與重新導向的連接埠範圍將會自動被選擇。若您想要自己進行設定，則請選擇“Manual Setting”。若想讓設定的規則生效，則請確認本選項已被勾選。如欲取得預設的應用程式列表，請參照表 10.2。
Protocol	本項目可讓您從下拉式選單中選擇通訊協定類型。本項目可供選擇的項目有 All、TCP、UDP、TCP/UDP，與 ESP。
Redirect Port Range	輸入想要設定的連接埠號。
To IP Address	輸入伺服器的IP 位址。

表10.2 常見應用程式連接埠號列表


應用程式	連接埠號碼
AOE II(伺服器)	2300-2400
AUTH	113
Baldurs Gate II	2300-2400
Battle Isle	3004-3004
Counter Strike	27005-27015
Cu See Me	7648-7648 , 56800,24032
Diablo II	4000-4000
DNS	UDP 53-53
FTP	TCP 21-21
FTP	TCP 20(代數)-21
Gopher	TCP 70-70
HTTP	TCP 80-80
HTTP8080	TCP 8080-8080
HTTPS	TCP 443-443
I-phone 5.0	TCP/UDP 22555-22555
ISAKMP	UDP 500-500
mIrc	6601-700
MSN Messenger	1863 代數
Need for Speed 5	9400-9400
Netmeeting Audio	TCP 1731-1731
Netmeeting Call	TCP 1720-1720
Netmeeting Conference	UDP 49500-49700
Netmeeting File Transfer	TCP 1503-1503
Netmeeting or VOIP	1503-1503 , 1720(代數)



應用程式	連接埠號碼
NEWS	TCP 119-119
PC Anywhere	TCP : 5631
PC Anywhere	TCP : 5631 , UDP : 5632
POP3	TCP 110-110
Powwow Chat	13223-13223
Red Alert II	1234-1237
SMTP	TCP 25-25
Sudden Strike	2300-2400
TELNET	TCP 23-23
Win VNC	UDP 5800-5900

## 10.2.2 虛擬伺服器範例

請依照以下敘述步驟來設定 FTP 伺服器：

1. 開啓 Virtual Server 設定頁面，雙按點選 Advanced → Virtual Server 選單，如圖 10.3 所示開啓虛擬伺服器設定頁面。
2. 從 Enable 的下拉式選單中選擇 FTP，並勾選本選項來讓該設定生效。請注意！通訊協定與重新導向的连接埠範圍會被自動選定。
3. 輸入FTP伺服器的IP 位址。請注意這邊所指的 IP 位址是指私人IP 位址。
4. 點選  鍵來儲存設定值。

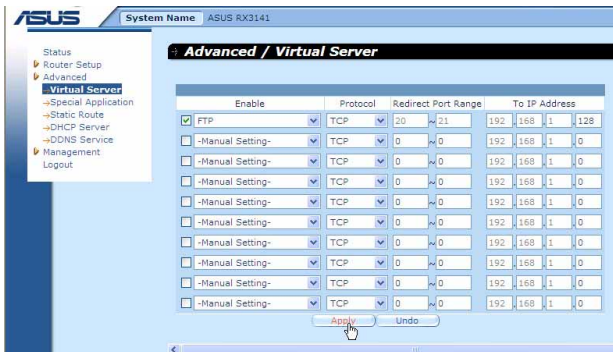


圖10.3 虛擬伺服器範例

5. 爲了安全需求，RX3141 拒絕從外部進入的存取要求，除非針對每一個 Virtual Server 設定來建立一個入埠 ACL 允許外部使用者連入。舉例來說，若您要允許外部網路連入 FTP 伺服器，請開啓如圖 10.4 的設定頁面中的入埠 ACL 規則下定義。

## RX 系列

請注意，此處的目的地 IP 位址與目的地連接埠要填入您在 Virtual Server（虛擬伺服器）設定頁面中的” To IP Address” 及” Redirect Port Range”。如果您想要限制某個特定的 IP 位址進行存取 FTP 伺服器，在入埠的 ACL 規則設定中可變更來源 IP。舉例來說，如果在入埠的 ACL 規則設定中的來源 IP 設為 198.175.2.10，RX3141 將會拒絕此特定 IP 以外的其他外部 IP 進行存取 FTP 伺服器。為了更詳細了解關於入埠的 ACL 規則設定，請參考 9.4 節的說明。

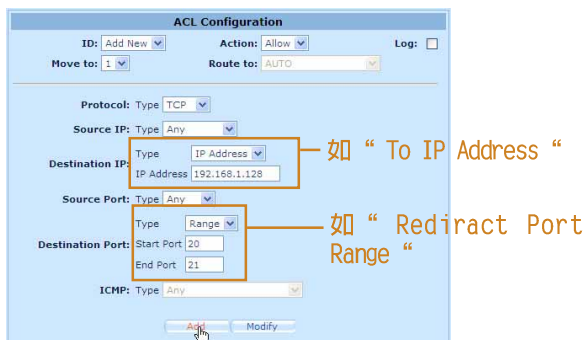


圖10.4 虛擬伺服器案例 - 入埠的 ACL 規則

### 10.3 設定特別應用程式

一些應用程式使用多重 TCP/UDP 連接埠來傳輸資料。由於 NAT 的運作，這些應用程式不能直接透過路由器運作，若要讓特定應用程式正常運作需要進行額外的設定。



無論何時只有一部 PC 可以使用一個特定的應用程式。

#### 10.3.1 特別應用程式設定

表10.3 描述特別應用程式設定中可進行的參數設定。

表 10.3 特別應用參數設定

設定	描述
Enable	從預設應用程式列表選擇一應用程式。對應的通訊協定與重新導向的連接埠範圍會被自動選定。若您想自己進行設定，則請選擇“Manual Setting”。如要讓設定生效，請確定本選項已被勾選。
Application Name	應用程式的辨識名稱。
Outgoing (Trigger) Port Range	當應用程式傳送出埠封包時所使用的連接埠範圍。對外的連接埠號的作用如同一觸發裝置。當路由器偵測到這些連接埠的外送封包，路由器會允許帶有定義在 Incoming Port Range 裡的埠號之入埠封包通過。如欲查看被某些常見應用程式採用的連接埠號列表，請參照表 10.4。
Incoming Port Range	對應入埠封包所使用的連接埠範圍。如欲查看的應用程式連接埠號表，請參照表 10.4。

表 10.4 常見應用程式連接埠號列表

應用程式	對外連接埠號	向內的連接埠範圍
Battle.net	6112	6112
DialPad	7175	51200,51201,51210
ICU II	2019	2000-2038 , 2050-2051 , 2069,2085,3010-3030
MSN Gaming Zone	47624	2300-2400,28800-29000
PC to Phone	12053	12120,12122,24150-24220
Quick Time 4	554	6970-6999
wowcall	8000	4000-4020

### 10.3.2 特別應用程式範例

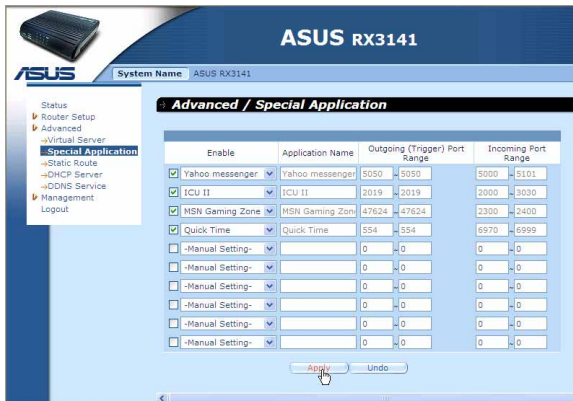



圖10.5 特別應用程式設定頁面

請依照下列敘述步驟步驟來設定 Quick Time 特定應用程式。

1. 藉由點選 **Advanced** → **Special Application** 選單，如圖 10.5 所示開啓特別應用程式設定頁面。
2. 從 **Enabled** 的下拉式選單中選擇 **Quick Time**，並勾選本選項來啓動本項設定。請注意！應用程式名稱、向外與向內的連接埠範圍會被自動選定。
3. 點選 **Apply** 鍵來儲存設定值。

5. RX3141 具備一個預設的出埠 ACL 規則與所有外部的網路連線。這個預設的出埠 ACL 規則，可以允許任何人使用定義在特別應用（Special Application）裡的應用。假如這個就是您所要的，略過這一步。然而，為了安全或其他理由，您可能會要限制只給某一特定使用群組使用此應用，然後設定一個出埠的 ACL 規則控制存取如圖 10.6 所示，這個例子可以讓主控者端透過設定 192.168.1.110 至 192.168.1.115 的 IP 進行限制。

請注意，為了限制存取的動作，預設出埠 ACL 規則設定允許任何人使用在特別應用（Special Application）設定頁面裡定義的任一應用程式。若要刪除預設的出埠 ACL 規則，只需要按下在 ACL 規則設定欄位中的預設 ACL 規則前的  圖示（於 Outbound ACL rule - 出埠的 ACL - 設定頁面中，如圖 10.7 所示）即可。有關出埠的 ACL 規則設定，請參考第 9.5 節的說明。

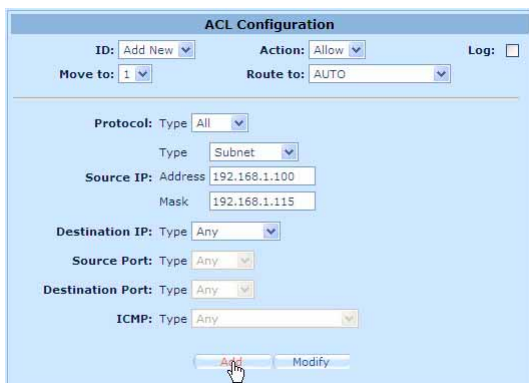


圖10.6 特別應用程式案例





Existing Outbound ACL ▼							
	ID	Action	Protocol	Source	Destination	Service	
	1	Allow	TCP	192.168.1.15	Any	80	
	2	Allow	All	Any	Any	Any	

圖10.7 出埠的 ACL 規則欄

## 11. 系統管理

在本章節中將敘述以下您可以使用的設定管理項目：

- 修改密碼與 System wide 設定。
- 檢視系統資訊
- 修改系統日期與時間
- 重置系統設定
- 重新啓動系統
- 更新韌體
- 備份/還原系統設定

### 11.1 登入密碼與 System-Wide 設定

當您第一次登入系統管理員時，請使用預設的使用者名稱與密碼（admin 與 admin）。



在這裡的使用者名稱與密碼僅可用來登入設定管理員，與您用來登入 ISP 的使用者名稱與密碼是不同的。

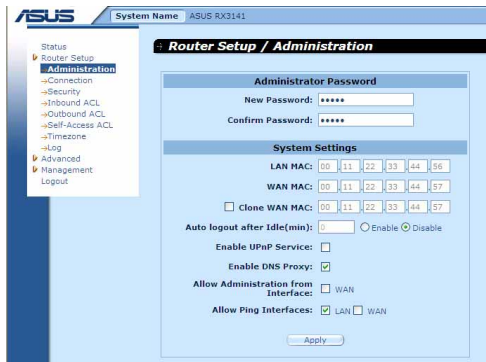



圖11.1 系統管理設定頁面

系統管理設定頁面，如圖 11.1 所示，可讓您變更登入 RX3141 的使用者名稱、密碼與其他通用設定。請依照下列步驟來變更密碼與/或 system-wide 設定：

1. 開啓系統管理設定頁面，雙按點選 Router Setup → Administration 選項，開啓設定頁面。
2. 變更登入密碼
  - a) 在新密碼的輸入欄位輸入新的密碼，並在下一欄位再次輸入密碼做為確認之用。密碼長度最長可以設定 16 個字母。當您再次登入時您必需依照您在此設定的密碼，並需符合大小寫。

3. 複製 MAC 位址供廣域網路 (WAN) 使用。
  - a) 若您先前有在您的 ISP 註冊用來登入網際網路的 MAC 位址，則請在此輸入該註冊的 MAC 位址，否則請保留預設值 — 由出廠設定值指定 MAC 位址供廣域網路 (WAN) 使用。
4. 在閒置一段時間後自動登出：按下” Enabled” 選項與輸入活動時間來建立這項設定；否則就選擇” Disabled” 或在文字欄輸入” 0” 來關閉這個選項。當這個選擇從網頁瀏覽器設定上啟用，接著之後將會自動依照所設定的閒置時間期間，來採自動不預警的執行。若您想繼續設定，您需要再次進入 RX3141 設定頁面。
5. 啟用 uPnP 服務：藉由勾選或取消勾選本選項，來開啓或關閉 uPnP 服務。
6. 開啓 DNS Proxy：藉由勾選或取消勾選本選項，來開啓或關閉 DNS Proxy 服務。
7. 允許自廣域網路 (WAN) 介面進行管理：藉由勾選或取消勾選來開啓或關閉透過廣域網路 (WAN) 連接埠進行遠端管理的功能。
8. 允許 Ping 介面：您可以透過區域網路 (LAN) 或者是廣域網路 (WAN)，來讓 RX3141 允許使用 Ping 的方式檢查。建議您只在區域網路開啓此選項。
9. 點選  鍵來儲存設定值。

## 11.2 檢視系統資訊

系統資訊頁面會顯示自您登入 RX3141 以來的相關資訊。這些資訊包含整體的系統設定值。



圖 11.2 系統狀態頁面

## 11.3 設定日期與時間

RX3141 會紀錄目前的日期與時間，這份資料是用來計算和報告各類資料之用。然而在 RX3141 中並沒有真實時鐘，RX3141 是依靠外部時間伺服器來保持正確的時間。RX3141 可讓您設定最多 3 組的外部時間伺服器。請確定“Enable”的選項已被勾選以便啟動 SNMP 服務（簡易網路時間通訊協定, Simple Network Time Protocol）來保持正確的時間。



變更RX3141上的日期與時間並不會影響您的PC上的時間。

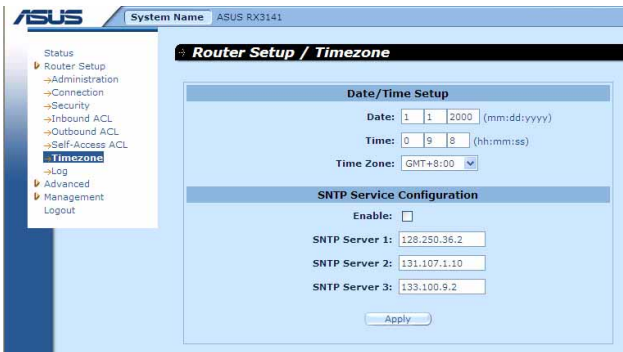


圖 11.3 日期與時間設定頁面

## RX 系列

請依照下列步驟來維持路由器中準確的時間：

1. 開啓 Date and Time 設定頁面，如圖 11.3 所示，雙按點選 Router Setup → Timezone 項目。
2. 從下拉式選單中選擇您所在地的時區。
3. 勾選“Enable”選項來啓動 SNTP（Simple Network Time Protocol）服務。
4. 請爲 SNTP 伺服器輸入 IP 位址，以作爲未來更新系統時間之用。
5. 點選  鍵來儲存設定值。

你也能以手動的方式輸入正確時間，但在系統重新啓動或關閉電源後會重置回預設時間，1/1/2000 00:00:00。

### 11.3.1 檢視系統日期與時間

爲了檢視更新後的系統日期與時間，請登入設定管理員，點選 Router Setup → Timezone 選單。請注意！若是 SNTP 伺服器並未開啓或在系統重新啓動或是電源關閉後沒有重新設定 SNTP 伺服器則系統時間會回復到預設值，1/1/2000 00:00:00。

## 11.4 恢復至出廠預設值

### 11.4.1 使用 GUI 恢復出廠預設值

有時候，你可能想要藉由恢復到出廠預設值來減少因錯誤系統設定所導致的問題。請依照下列步驟來重置系統設定：

1. 登入設定管理員，雙按點選 Management → Factory Reset 選單。接下來，預設值設定頁面便會如圖 11.4 顯示出來。

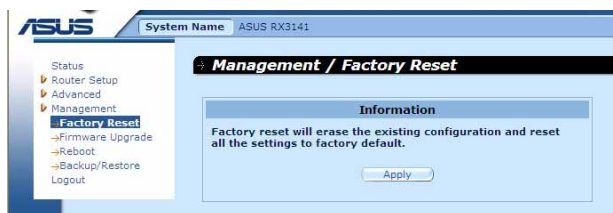


圖 11.4 工廠預設值重置頁面

2. 點選  鍵來讓系統設定值回到出廠預設值。
3. 一選項將會如圖 11.5 所示的請求確認。點選  鍵以繼續，或點選  鍵來取消此動作。





圖 11.5 出廠預設值重置確認視窗

4. RX3141接下來會重新啓動來回復出廠預設值。請注意！如圖 11.6 所示的計時視窗將會出現，以標示系統重置完成尚需的時間。

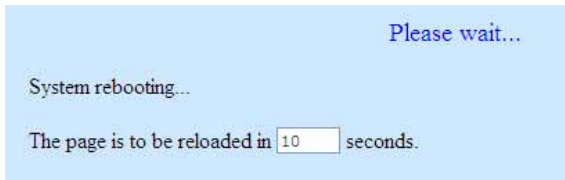


圖 11.6 出廠預設值重置計時秒數

### 11.4.2 使用 Reset 鍵恢復至出廠預設值



有時候您可能發現無法存取 RX3141，如 您忘記您的密碼或是 RX3141 的 IP位址。解決這類狀況的唯一方法就是藉由按下RX3141 上的重置鍵至少 5 秒鐘來將系統設定重置回出廠預設。當進行重置動作並重新啓動 RX3141 後，系統設定便會回復到出廠預設值。

## 11.5 更新韌體

ASUSTeK 會不斷地提供您可使用在 RX3141 上的新版韌體。而所有的系統檔案僅包含一單獨的映象檔。至於韌體的升級，設定管理員提供一種簡易的方式進行升級。如欲升級韌體，請依照下列步驟進行：

1. 藉由點選 Management → Firmware Upgrade 選單，如圖 11.7 所示，開啓更新韌體頁面。

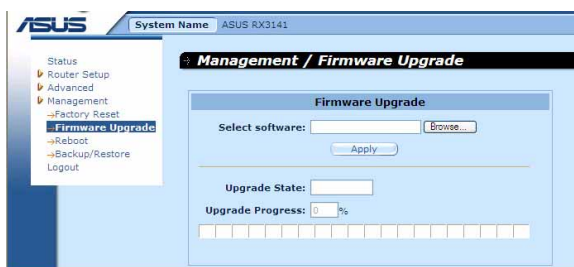


圖 11.7 更新韌體頁面

2. 在選擇韌體欄位中，請輸入韌體檔案所在路徑或是韌體檔案的名稱。除此之外，您也可以點選 **Browse...**（瀏覽）鍵來開啓檔案總管搜尋在您電腦中的韌體映象檔。

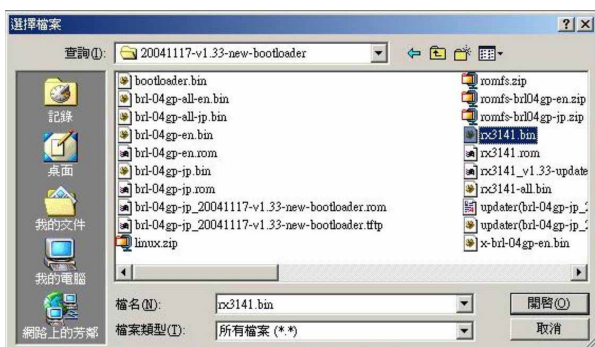


圖11.8 檔案總管選擇畫面

3. 點選 **Apply** 鍵來更新韌體。在更新作業進行前，如下圖所示的對話視窗會出現並詢問是否確定進行韌體更新。請點選 OK 以繼續進行；否則點選 Cancel 鍵來取消此一動作。



圖 11.9 更新韌體確認視窗

4. 當韌體正在進行更新時，如圖 11.10 所示的更新狀態會出現告知您韌體更新的進度。

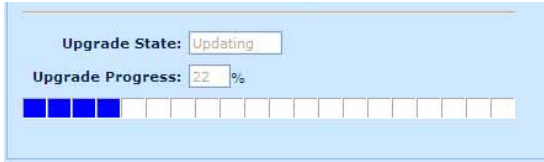


圖 11.10 韌體更新狀態視窗

5. 在韌體更新完成後，如圖 11.11 所示會顯示一時間倒數視窗。當倒數至 0 時，您將會重新連接到 RX3141。而若是 RX3141 沒有自動重新連線，請以手動方式設定您的電腦與 RX3141 間的連線。

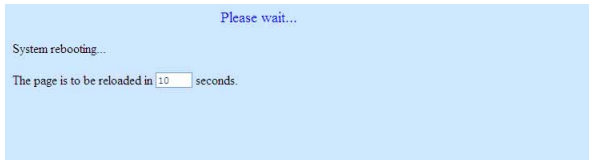



圖 11.11 韌體更新倒數計時視窗

6. 當您重新連線到 RX3141，您可藉由點選 **Status** 選單來檢查韌體是否已正確更新。請注意！您或許需要清除網頁瀏覽器的快取以便檢視系統資訊頁面。請依照以下步驟來清除 Microsoft Internet Explorer 瀏覽器的快取：
- 點選瀏覽器的“工具”選項。
  - 接著點選“網際網路選項”。
  - 點選“刪除檔案”按鍵來清除瀏覽器快取。

## 11.6 重新啟動系統

- 藉由點選 **Management** → **Reboot** 選單，如圖 11.7 所示，開啓重新啟動系統頁面。
- 點選  鍵來重新啟動系統。

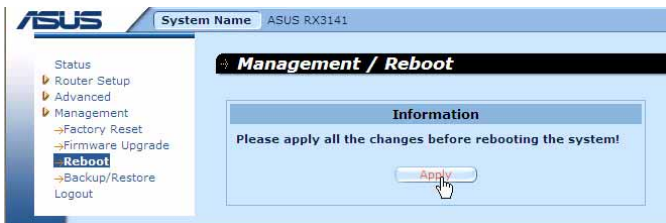


圖 11.12 重新啟動系統頁面

## RX 系列

- 這時會跳出一個對話框，如圖 11.13 所示，按下  鍵後來確認，或者是按下  鍵取消。



圖 11.13 重新啓動系統設定

- 網頁瀏覽器這時將會重新開啓 RX3141 的倒數計時秒數畫面。

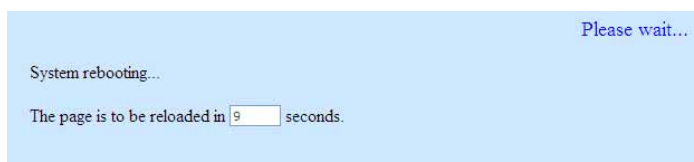


圖 11.14 重新啓動系統更新倒數計時視窗

## 11.7 系統設定管理

### 11.7.1 備份系統設定

請依照下列步驟進行備份系統的設定：

- 開啓 System Configuration Backup/Restore 設定頁面，如圖 11.15 所示，雙按點選 Management → Backup/Restore 選單，開啓設定頁面。

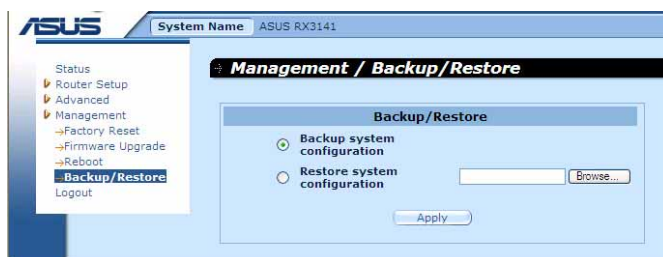


圖 11.15 系統設定備份視窗

- 勾選” Backup system configuration ”選項。
- 按下  按鍵來備份系統設定。
- 若您使用微軟 Windows 系統，會顯示” File Download ”交談視窗，按下  鍵後進行備份，如圖 11.16 所示。

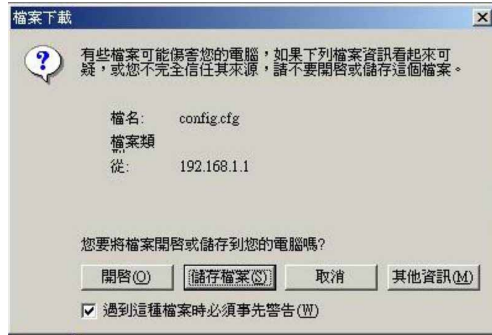



圖 11.16 系統設定備份畫面  
- 檔案下載對話視窗

5. 輸入一個欲備份的檔案名稱，如圖 11.17 所示，然後按下  鍵後繼續。

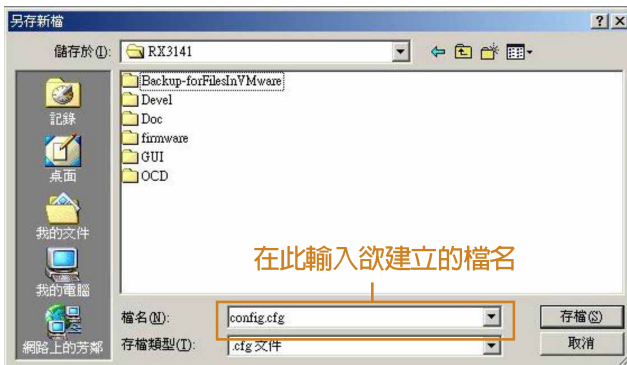


圖 11.17 系統設定備份畫面  
- 儲存檔案的交談框

6. 最後出現一個訊息，如圖 11.18 所示，讓您知道備份的檔案已經成功地儲存到您的電腦中。

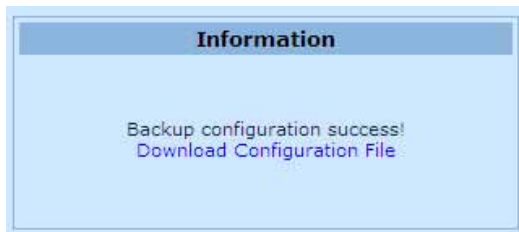


圖 11.18 系統備份設定狀態提示

## 11.7.2 回復系統設定

請依照下列步驟進行備份系統的設定：

1. 開啟 System Configuration Backup/Restore 設定頁面，如圖 11.19 所示，雙按點選 Management → Backup/Restore 選單，開啟設定頁面。

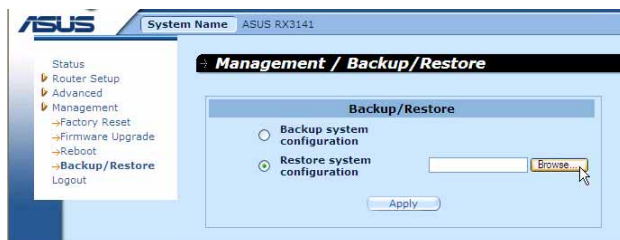


圖 11.19 回復備份系統設定視窗

2. 您可以按下 **Browse...**（瀏覽）鍵來搜尋存在電腦中的備份檔案位置，當您選擇這方式尋找後，就會類似如圖 11.20 所顯示的狀態。當選擇好所要回復的檔案時，按下 **開啓(O)** 鍵繼續。

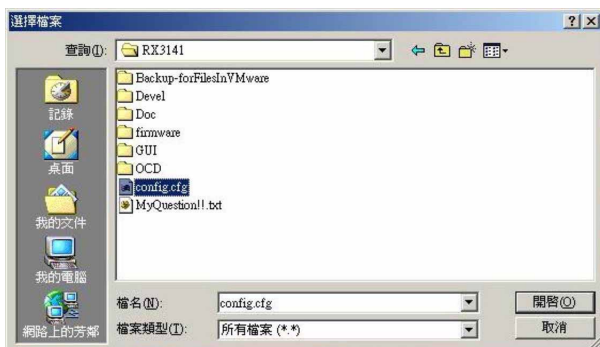


圖 11.20 回復備份系統設定視窗-  
選擇檔案交談視窗

3. 按下 **Apply** 按鈕來回復備份系統設定。
4. 後出現一個訊息，如圖 11.21 所示，讓您知道備份的檔案已經成功地將 RX3141 系統回復。請注意，這時記得重新啓動 RX3141 讓新的設定啓用。

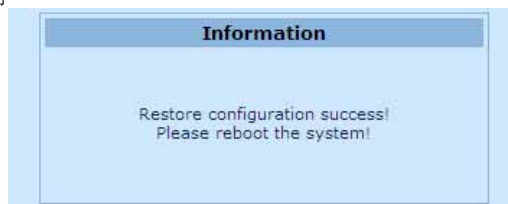


圖 11.21 回復系統備份狀態提示

## 12. IP 位址、網路遮罩，與子網路

### 12.1 IP 位址



- 本節敘述僅關於 Ipv4 位址(version 4 of the Internet Protocol)的範圍，內容並未涵蓋 Ipv6 位址。
- 本節假設您已對二進位數字、位元與位元組有初步的認識。如欲取得關於本主題的相關細節，請參閱附錄 12。

IP 位址，網際網路版本的電話號碼，是用來確認網際網路上獨立的節點（電腦或是其他裝置）。每一組 IP 位址包含四組數字，而每一組數字可由 0 到 255，並以句點分隔，如 20.56.0.211。這些號碼的閱讀方式是由左至右，第一欄位、第二欄位、第三欄位、第四欄位。

書寫 IP 位址的方式，如由句點所分隔的十進位數字被稱作十進位句點標記法。而 IP 位址為 20.56.0.211 在閱讀上便讀作“二十點五十六點零點二一一”。

### 12.2 IP 位址架構

IP 位址有一種類似電話號碼的分級設計。例如，一組 7 位數字的電話號碼起使於一組三位數字的號碼，這組號碼是用來由上千條電話線中進行確認之用。而其他四位數字則是用來確認是該群組中的哪一條特定電話線之用。

簡單來說，一組 IP 位址含有兩種訊息。

- 網路 ID  
在網際網路或內部網路中標示一特定網路
- 主機 ID  
在網路中標示一特定的電腦或裝置

的第一部分每 IP 位址包含網路 ID，並且其餘位址包含主人 ID。網路 ID 的長度取決於網路的種類(看見以後的章節)。

表 12.1 IP 位址架構。

	Field1	Field2	Field3	Field4
A級	網路ID	主機ID		
B級	網路ID		主機ID	
C級	網路ID			主機ID

## RX 系列

---

以下是一些有效的 IP 位址範例：

A 級：10.30.6.125(網路= 10，主機= 30.6.125)

B 級：129.88.16.49(網路= 129.88，主機= 16.49)

C 級：192.60.201.11(網路= 192.60.201，主機= 11)

### 12.3 網路等級

常被使用的三種網路等級分別為等級 A、B 與 C（此外尚有一種等級 D，但屬於特殊使用範圍，不在本節的討論中）。這些等級具有不同的用途與特性。

A 級網路是網際網路中範圍最大的網路，其中每個網路有超過 1600 萬部主機。而此等級的網路最高可存在 126 個，約等於二十億部主機。由於其巨大的容量，這些網路多用於廣域網路（WAN）環境，並被組織為網際網路中的基礎等級，例如您的 ISP。

B 級網路在範圍上較 A 級更小但範圍仍然十分龐大，每個網路可以有超過 65,000 部的主機。而此等級的網路最高可存在 16,384 個。一個 B 級網路可能為較大的組織如商業或政府機構所採用。

C 級網路是三種網路等級中最小的，最多只能容納 254 部主機，但此等級的網路可存在超過 2 百萬個（正確地說是 2,097,152）。連線至網際網路的區域網路大多屬於 C 級網路。

關於 IP 位址的一些重要註記：

- 可由第一欄位輕易決定的等級：

- 欄位 1 = 1-126：A 級

- 欄位 1 = 128-191：B 級

- 欄位 1 = 192-223：C 級

(欄位 1 所顯示的數值不為特別用途保留)

- 一主機 ID 可以具有除了所有欄位皆設為 0 或 255 以外的數值，因為那些數值是有其特殊用途的。

### 12.4 子網路遮罩



一組子網路遮罩看起來像是一般的 IP 位址，但卻包含位元的樣式，此樣式是用以告知 IP 位址的哪一部份是網路 ID，而哪一部份又是主機 ID。位元設為 1 代表“此位元為網路 ID 的一部份”，而設為 0 代表“這是主機 ID 的一部份”。

---



---

子網路遮罩是被用來定義子網路（就是您將網路分為較小的片段）。一組子網路的網路 ID 藉由向主機 ID 位址的一部份“借”一個或更多位元。子網路標示這些主機 ID 位元。

例如，一 C 級網路 192.168.1。將其分做兩個子網路，您會使用以下的子網路遮罩設定：

255.255.255.128

如果我們以二進位方式書寫將更容易瞭解其意義：

11111111. 11111111. 11111111.10000000

像任何 C 級位址一樣，所有欄位 1 到欄位 3 的位元是網路 ID 的一部份。但請注意，網路遮罩如何指定欄位 4 的第一位元也包含其中。當此一多出的位元擁有兩數值（0 與 1），這便代表有兩個子網路。每個子網路在欄位 4 中使用剩下的 7 個位元做為其主機 ID，其範圍是從 0 至 127（除了 0 至 255 是做為 C 級網路位址之用）。

同樣地，如將 C 級網路分為四個子網路，則遮罩為：

255.255.255.192 或 11111111。 11111111. 11111111.11000000

在欄位 4 中兩個多出的位元可以有四組數值（00,01,10,11），因此有四個子網路。每個子網路使用欄位 4 中剩下的六位元做為其主機 ID，範圍由 0 至 63。



有時子網路遮罩不指定任何其他的網路 ID 位元，也因此沒有子網路，像是被稱作預設子網路遮罩的遮罩，這些遮罩有：

A 級：255.0.0.0

B 級：255.255.0.0

C 級：255.255.255.0

這些被叫為預設值，是因為它們是當一個網路是初始設定時被使用，而在當時是沒有子網路的。


---

## 13. 移難排解

本附錄將列出您在安裝或使用 RX3141 時可以遭遇到之問題的解決建議。此外，也將提供使用幾個 IP 公用程式來診斷問題的介紹。

若以下的問題解決建議無法解決您的問題，請與本公司的客戶支援部門聯繫。

問題	檢修建議
LEDs	
當電源開啓後，電源 LED 燈號並未亮起。	請確認您是使用 AC 電源供應器來供給裝置電源，並確認電源供應器一端確實連接到 RX3141，而另一端則確實連接到室內電源插座或電源延長線。
當連接乙太網路線後，Link WAN LED 燈號未亮起。	請確認乙太網路線的一端緊密連接到您的 ADSL 或 Cable 數據機的一端，而另一端則緊密地連接到 RX3141 的 WAN 連接埠。接著請確認您的 ADSL 或 Cable 數據機的電源已開啓。請等待 30 秒鐘來讓 RX3141 與您的寬頻數據機建立連線。
當連接乙太網路線後，LINK LAN LED 燈號未亮起。	確認乙太網路線已緊密連接到您區域網路的集線器或 PC 與連接到 RX3141。並確認 PC 與集線器的電源已開啓。
確認您所使用的乙太網路線符合您的網路傳輸需求。	100Mbit/sec 的網路 (100BaseTx) 應該使用標示 Cat.5 的網路纜線。若使用 10Mbit/sec 的網路連線則可以使用較低傳輸品質的網路纜線。
Internet 連線	
PC 無法連線到 Internet	<p>使用在下一節中會討論到的封包測試公用程式來檢查您的 PC 是否可以連線到 RX3141 的區域網路 IP 位址 (預設值: 192.168.1.1)。</p> <p>若無法連線，請檢查您的網路纜線。</p> <p>如果您把私人 IP 位址靜態配發到電腦 (未註冊的公開網路位址)，請檢查以下幾點：</p> <ul style="list-style-type: none"> <li>檢查電腦上的閘道器 IP 位址是您公開對外的 IP 位址 (請參考快速安裝指南中第二章第二部分關於檢視 IP 資訊的介紹)。若設定並非如此，請更正該位址或設定您的 PC 來自動接收 IP 資訊。</li> <li>請與您的 ISP 確認指定給 PC 使用的 DNS 伺服器位址是有效的。請更正該位址或設定自動接收該項資訊。</li> <li>請確認 RX3141 中的網路位址翻譯規則已正確設定，以便正確翻譯由您內部私人 IP 位置至對外公開的 IP 位址。而配發 IP 位址必需符合 NAT 規則中特定的範圍。或是，也可以設定 PC 來接收由其他裝置所配發的位址 (請參考 3.2 “第二部分 — 設定您的電腦” 一節中的相關介紹)。在預設值中，包含有一 NAT 規則用以在預設位址池中動態指定位址的功能。</li> </ul>
PC 無法顯示網際網路的網頁內容。	確認您的 ISP 所提供的 DNS 伺服器位址是有效的且已正確設定在您的電腦中。您可以使用下一節中將討論的封包探測工具來測試您電腦與 ISP 之 DNS 伺服器間的連線。

設定管理員程式 (Configuration Manager Program)	
你忘記/ 遺失您在設定管理員中的使用者名稱或密碼。	若您不曾變更預設的使用者名稱與密碼，試著在使用者名稱與密碼的欄位輸入“admin”與“admin”。否則，您可以依照 11.4 節中的介紹，進行將裝置重置回出廠預設值的動作。警告：重置動作將會一併清除所有先前的設定，並回復到出廠預設值。
無法由您的瀏覽器進入設定管理員程式。	使用在下一節中，將介紹的封包測試公用程式來檢查您的 PC 與 RX3141 之區域網路連接埠（預設值：192.168.1.1）間的連線是否正常。若無法連線，請檢查乙太網路纜線是否正常。 確認您是使用 Internet Explorer 6.0 或者更新版本的瀏覽器軟體。您的瀏覽器必需支援 Javascript，且瀏覽器也支援 Java 可能也是需要的。 確認 PC 的 IP 位址與 RX3141 的區域網路連接埠是在同一子網路環境中。
在設定管理員所做的設定變更未被保留。	請確定設定後已點選  鍵來儲存變更的設定值。


## 13.1 使用IP 公用程式診斷問題

### 13.1.1 封包探測 (Ping)

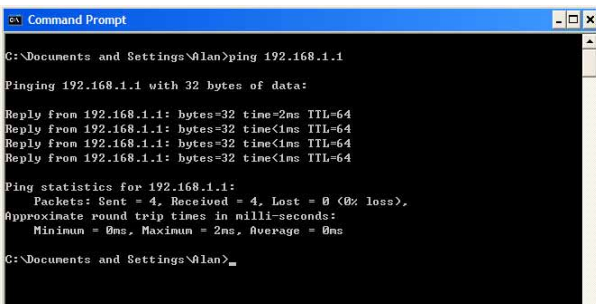
封包探測 (Ping) 是您可以用來檢查您的 PC 是否可以辨識區域網路或網際網路中電腦的一項指令。封包探測指令會傳送訊息至您所指定的電腦主機，若該電腦接收到訊息，便會傳回一回覆訊息。若要使用這項指令，您必需知道您試圖連線之電腦的 IP 位址。

在使用 Windows 作業系統的電腦上，您需要從開始選單中執行封包探測指令。請點選開始選單按鍵，接著請點選“執行”。在接下來的文字選項中，請依照以下例子進行輸入：

Ping 192.168.1.1

點選 。此外，您也可以用任何其他區域網路的 IP 位址或您知道的網際網路 IP 位址，來進行封包探測的測試。

若目標電腦接收到訊息，則如圖 13.1 所示的指令提示視窗會顯示出來。



```

C:\Documents and Settings\Alan>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Documents and Settings\Alan>

```

圖 13.1 使用封包探測公用程式

## RX 系列

若封包探測所送出的訊息不能到達目標電腦，則您將會收到“Request timed out”的訊息。

藉由使用封包探測公用程式，您可以測試 RX3141 的連線路徑（使用預設的區域網路 IP 位址：192.168.1.1 進行探測）或其他您所指定的位址是否連線正常。

你也可以藉由輸入其他外部的 IP 位址來測試網際網路的連線是否正常。舉例來說，您可以輸入 **www.yahoo.com**（216.115.108.243）來進行測試。若您不知道特定網際網路位址的 IP 位址，您則可以使用下一節中會介紹的 nslookup 指令進行測試。

以大多數啓用 IP 功能的作業系統，您可以透過系統管理公用程式來執行相同的封包探測指令。

### 13.1.2 nslookup

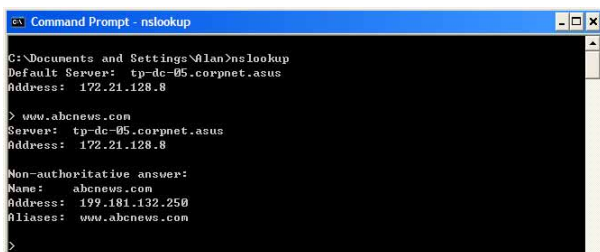
您可以使用 nslookup 指令來決定與網際網路網站名稱相對應關連的 IP 位址。您可指定一般名稱，接著 nslookup 指令會在您的 DNS 伺服器中搜尋該名稱（通常會儲存於您的 ISP 伺服器中）。若該登錄無法在您 ISP 的 DNS 伺服器中找到，則該要求會被轉送到更高等級的伺服器，以此類推，直到該登錄被搜尋到為止。搜尋到之後，伺服器接著會回覆該登錄的對應 IP 位址。

在使用 Windows 作業系統的電腦上，您需要從開始選單中執行 nslookup 指令。請點選開始選單按鈕，接著請點選“執行”。在接下來的文字選項中，請依照以下例子進行輸入：

#### nslookup

輸入完畢請點選 。接著一個包含 (>) 符號的命令提示視窗會出現。在此一命令提示視窗中輸入您感興趣的網際網路位址名稱，例如：**www.absnews.com**。

接著視窗會如圖 13.2 顯示相關連的 IP 位址。



```
Command Prompt - nslookup
C:\Documents and Settings\Alan>nslookup
Default Servers: tp-dc-05.corpnet.asu
Address: 172.21.128.8

> www.absnews.com
Server: tp-dc-05.corpnet.asu
Address: 172.21.128.8

Non-authoritative answer:
Name: absnews.com
Address: 199.181.132.250
Aliases: www.absnews.com

>
```

圖 13.2 使用 nslookup 公用程式

以同一網際網路名稱來說，可能有好幾個相對應的位址。這對於傳輸量大的網站來說是很正常的現象，因為這些網站採用多重、備份伺服器來傳送相同的資訊。

如要退出 nslookup 程式，請在指令提示列輸入 exit 並按下 <Enter> 即可。

- 
- 索引
  - Computers
    - configuring IP information, 10
  - Configuration Manager
    - overview, 17
    - troubleshooting, 72
  - Connectors
    - rear panel, 6
  - Date and time, changing, 61
  - Default configuration, 15
  - Default gateway, 33
  - DHCP
    - defined, 29
    - DHCP Address Table page, 30
    - DHCP client
      - defined, 29
      - DHCP Lease Table page, 31
      - DHCP server
        - defined, 29
        - pools, 29
        - viewing assigned addresses, 31
      - DHCP Server Configuration page, 30
    - Diagnosing problems
      - after installation, 15
    - DNS, 30
    - Dynamically assigned IP addresses, 29
  - Eth-0 interface
    - defined, 16
  - Ethernet cable, 9
  - Features, 1
  - Firmware Upgrade page, 63, 64
  - Firmware upgrades, 63
  - Front panel, 5
  - Gateways
    - in DHCP pools, 30
  - Gateway
    - defined, 33
  - Hardware connections, 9, 10
  - Host ID, 67
  - HTTP DDNS, 38
  - Inbound ACL Configuration page, 45
  - Internet
    - troubleshooting access to, 71
  - IP address
    - in device's routing table, 36
  - IP addresses
    - explained, 67
  - IP configuration
    - static, 13
    - static IP addresses, 13
    - Windows 2000, 11
    - Windows Me, 12
    - Windows NT 4.0, 12
  - IP Configuration
    - Windows XP, 11
  - IP information
    - configuring on LAN computers, 10
    - , 34, 35
  - IP Routes
    - defined, 33
  - LAN IP address, 21
  - specifying, 21
  - LAN network mask, 21
  - LAN subnet mask, 21
  - LEDs, 5
  - troubleshooting, 71
  - Login
    - to Configuration Manager, 17
  - NAT
    - defined, 53
  - NAPT, 53
  - Overload, 53
  - PAT, 53
  - Reverse NAPT, 54
  - Virtual Server, 54
  - Navigating, 18
  - Netmask. See Network mask
  - Network classes, 67
  - Network ID, 67
  - Network interface card, 1
  - Network mask, 68
-

- Network Setup, 21
- Network Setup Configuration page, 22
- Node on network
  - defined, 21
- Notational conventions, 1
- nslookup, 73
- Outbound ACL Configuration page, 47
- Packet
  - filtering, 39
- Pages
  - DHCP Address Table, 30
  - DHCP Lease Table, 31
  - DHCP Server Configuration, 30
  - Firmware Upgrade Upgrade, 63, 64, 34, 35
  - LAN Configuration, 22
  - Routing Configuration, 34, 35
  - System Information, 15
  - User Password Configuration, 59
  - Pages Inbound ACL Configuration, 45
  - Pages Outbound ACL Configuration, 47
- Parts
  - checking for, 3
- Password
  - changing, 59
  - default, 14, 17
  - recovering, 72
- PC configuration, 10
- PC Configuration
  - static IP addresses, 13
- Ping, 72
- Power adapter, 9
- Primary DNS, 27
- Quick Configuration
  - logging in, 13
- Rear Panel, 6
- Routing Configuration page, 34, 35
- Secondary DNS, 27
- Static IP addresses, 13
- Static routes
  - adding, 35
  - Statically assigned IP addresses, 29
- Subnet masks, 68
- System Information page, 15
- System requirements
  - for Configuration Manager, 17
- System requirements:, 1
- Testing setup, 15
- Time and date, changing, 61
- Troubleshooting, 71
- Typographical conventions, 1
- Upgrading firmware, 63
- User Password Configuration page, 59
- Username
  - default, 14, 17
- WAN DHCP, 22
- WAN IP address, 22
- Web browser
  - requirements, 1
  - version requirements, 17
- Web browsers
  - compatible versions, 17
- Windows NT
  - configuring IP information, 12