

# RX3042H

## 使用手冊

Revision 0.8  
2005 年 08 月

---

<b>第一章 簡介</b> .....	<b>1</b>
1.1 特色 .....	1
1.2 系統需求 .....	1
1.3 如何使用本手冊 .....	2
1.3.1 提示符號的說明 .....	2
1.3.2 印刷樣式的說明 .....	2
1.3.3 特別資訊 .....	2
<b>第二章 認識您的 RX3042H</b> .....	<b>3</b>
2.1 零件明細表 .....	3
2.2 硬體功能 .....	3
2.3 軟體功能 .....	3
2.3.1 NAT 功能 .....	3
2.3.2 防火牆功能 .....	4
2.3.2.1 封包檢查 (Stateful Packet Inspection) ...	4
2.3.2.2 封包過濾 (Packet Filtering - ACL) .....	4
2.3.2.3 防範 DoS 攻擊 .....	5
2.3.3 特別資訊 .....	2
2.4 產品概觀 .....	6
2.4.1 前面板 .....	6
2.4.2 後面板 .....	7
2.4.3 底視圖 .....	7
2.5 擺放選項 .....	8
2.5.1 桌面放置 .....	8
2.5.2 壁掛安裝介紹 .....	8
<b>第三章 快速安裝指南</b> .....	<b>9</b>
3.1 Part 1 — 連接硬體 .....	9
3.1.1 Step 1：連接 ADSL 或 Cable Modem .....	9
3.1.2 Step 2：連接電腦或網路 .....	10
3.1.3 Step 3：連接 AC 電源供應器 .....	10
3.1.4 Step 4：開啓 RX3042H、ADSL 或 Cable Modem 的電源 並啓動您的電腦 .....	10
3.2 Part 2 — 設定您的電腦 .....	11

---

3.2.1	在你開始之前 .....	11
3.2.2	安裝 Windows XP 作業系統之個人電腦 .....	12
3.2.3	安裝 Windows 2000 作業系統之個人電腦 .....	12
3.2.4	安裝 Windows 95、98 或 ME 作業系統的個人電腦 ..	13
3.2.5	安裝 Windows NT 4.0 作業系統的工作站 .....	14
3.2.6	指定靜態 IP 位址給您的個人電腦 .....	15
3.3	Part 3 — 快速設定 RX3042H .....	16
3.3.1	設定 RX3042H .....	16
3.3.2	測試您的設定 .....	18
3.3.3	預設路由器設定 .....	18
<b>第四章</b>	<b>使用設定管理員 .....</b>	<b>19</b>
4.1	登入設定管理員 .....	19
4.2	設定頁結構 .....	20
4.2.1	選單導覽 .....	21
4.2.2	通用的按鍵與圖示 .....	21
4.3	系統設定概觀 .....	21
<b>第五章</b>	<b>路由設定 .....</b>	<b>23</b>
5.1	區域網路設定 (LAN Configuration) .....	23
5.1.1	區域網路的 IP 位址 .....	23
5.1.2	區域網路參數設定 .....	23
5.1.3	設定區域網路的 IP 位址 .....	24
5.2	WAN/DMZ 設定 .....	25
5.2.1	廣域網路的連接模式 .....	25
5.2.2	PPPoE .....	25
5.2.2.1	廣域網路的 PPPoE 參數設定 .....	26
5.2.2.2	為廣域網路設定 PPPoE 連線 .....	27
5.2.3	PPPoE unnumbered .....	28
5.2.3.1	廣域網路 PPPoE Unnumbered 參數設定 .....	29
5.2.3.2	設定供廣域網路使用的 PPPoE Unnumbered ..	29
5.2.4	動態 IP (Dynamic IP) .....	30
5.2.4.1	設定供廣域網路使用的動態 IP .....	30
5.2.5	靜態 IP .....	31

---

---

5.2.5.1 WAN 或 DMZ 靜態 IP 參數設定 .....	31
5.2.5.2 WAN 或 DMZ 模式下的靜態 IP 位址 .....	32
5.2.6 PPTP .....	33
5.2.6.1 設定供廣域網路使用的 PPTP 參數 .....	33
5.2.6.2 設定廣域網路模式下的 PPTP .....	32
5.3 WAN Load Balancing 和 Line Back Up .....	35
5.3.1 WAN Load Balancing 和 Line Back Up 設定參數 ..	36
5.3.2 設定 WAN 負載平衡 .....	37
5.3.3 設定 WAN 線上備份 .....	38
<b>第六章 設定 DHCP 伺服器 .....</b>	<b>39</b>
6.1 DHCP (動態主機配置協定) .....	39
6.1.1 何謂 DHCP 伺服器? .....	39
6.1.2 為何要使用 DHCP 伺服器? .....	39
6.1.3 設定 DHCP 伺服器 .....	40
6.1.4 檢視目前指定的 DHCP 位址 .....	41
6.1.5 固定式 DHCP 租約 .....	42
6.1.5.1 進入固定式 DHCP 租約設定畫面 .....	42
6.1.5.2 增加一個固定式 DHCP 租約 .....	42
6.1.5.3 查看固定式 DHCP 租約列表 .....	42
6.2 DNS .....	43
6.2.1 關於 DNS .....	43
6.2.2 分配 DNS 位址 .....	43
6.2.3 設定 DNS 轉送功能 .....	44
<b>第七章 路由 .....</b>	<b>45</b>
7.1 IP 路由概述 .....	45
7.1.1 我需要定義靜態路由嗎? .....	45
7.2 啓用 RIP 的動態路由協定 .....	45
7.2.1 RIP 的相關參數 .....	46
7.2.2 配置 RIP .....	47
7.3 靜態路由 .....	47
7.3.1 靜態路由的參數設定 .....	48
7.3.2 新增靜態路由 .....	48

---

7.3.3 刪除靜態路由 .....	49
7.3.4 觀看靜態路由表 .....	49
<b>第八章 設定 DDNS .....</b>	<b>51</b>
8.1 DDNS 參數設定 .....	52
8.2 設定 HTTP DDNS 用戶端 .....	52
<b>第九章 設定防火牆/NAT 設置 .....</b>	<b>55</b>
9.1 防火牆概述 .....	55
9.1.1 Stateful 封包檢查 .....	55
9.1.2 DoS (阻絕服務) 保護 .....	55
9.1.3 防火牆與存取控制列表 (ACL) .....	56
9.1.3.1 ACL 規則的優先順序 .....	56
9.1.3.2 ACL 規則與連線狀態追蹤 .....	56
9.1.4 預設的 ACL 規則 .....	56
9.2 NAT 概述 .....	57
9.2.1 NAT (Network Address and Port Translation) 或 PAT (Port Address Translation) .....	57
9.2.2 反向 NAT/虛擬伺服器 .....	58
9.3 防火牆設定 .....	58
9.3.1 防火牆參數設定 .....	58
9.3.2 DoS 設定 .....	59
9.3.2.1 DoS 保護參數設定 .....	59
9.3.2.2 進行 DoS 設定 .....	61
9.4 ACL 規則參數設定 .....	61
9.4.1 ACL 規則參數設定 .....	61
9.5 設定 ACL 規則 (Firewall -> ACL) .....	64
9.5.1 新增 ACL 規則 .....	65
9.5.2 修改 ACL 規則 .....	66
9.6 設定 Self-Access ACL 規則 .....	66
9.6.1 新增一個 Self-Access 規則 .....	67
9.6.2 修改 Self-Access ACL 規則 .....	68
9.6.3 刪除 Self-Access ACL 規則 .....	68
9.6.3 顯示 Self-Access ACL 規則 .....	68

---

---

9.7 設定虛擬伺服器 .....	69
9.7.1 虛擬伺服器參數設定 .....	69
9.7.2 虛擬伺服器設定範例 1 - 網頁伺服器 .....	71
9.7.3 虛擬伺服器設定範例 2 - FTP 伺服器 .....	73
9.7.4 虛擬伺服器設定範例 3 - 具備存取控制功能的 FTP 伺服器 .....	73
9.8 特別應用程式設定 .....	75
<b>第十章 系統管理 .....</b>	<b>79</b>
10.1 設定系統服務 .....	79
10.2 登入密碼與系統設定 .....	80
10.2.1 更改密碼 .....	80
10.2.2 設定系統參數 .....	81
10.3 檢視系統資訊 .....	81
10.4 設定日期與時間 .....	82
10.4.1 檢視系統日期與時間 .....	83
10.5 SNMP 設定 .....	83
10.5.1 SNMP 的設定參數 .....	83
10.6 設定日誌 .....	84
10.6.1 使用 Syslog 設定遠端日誌 .....	84
10.6.2 查看系統日誌 .....	85
10.7 系統設定管理 .....	85
10.7.1 將系統設定參數還原至出廠值 .....	85
10.7.2 備份系統設定 .....	87
10.7.3 回復系統設定 .....	88
10.8 更新韌體 .....	89
10.9 重新啟動系統 .....	91
10.10 登出設定管理頁面 .....	92
<b>第十一章 IP 位址、網路遮罩，與子網路 .....</b>	<b>93</b>
11.1 IP 位址 .....	93
11.1.1 IP 位址架構 .....	93
11.2 網路等級 .....	94
11.3 子網路遮罩 .....	94

---

<b>第十二章 移難排解 .....</b>	<b>97</b>
12.1 使用IP 公用程式診斷問題 .....	98
12.1.1 封包探測 (Ping) .....	98
12.1.2 nslookup .....	99

---

## 圖示目錄

圖 2.1	前面板 LED 指示燈	6
圖 2.2	後背板插座	7
圖 3.1	硬體連接示意圖	10
圖 3.2	登入畫面	16
圖 3.3	系統資訊頁面	17
圖 4.1	設定管理員登入畫面	19
圖 4.2	典型的設定管理員畫面	20
圖 4.3	系統資訊頁面	21
圖 5.1	網路設定 - 區域網路設定	24
圖 5.2	網路設定 - 廣域網路設定	25
圖 5.3	WAN - PPPoE 設定	26
圖 5.4	WAN - PPPoE Unnumbered 設定	28
圖 5.5	WAN - 動態 IP (DHCP 用戶端) 設定	30
圖 5.6	WAN - 靜態 IP 設定	31
圖 5.7	WAN - PPTP 設定	34
圖 5.8	負載平衡設定	37
圖 6.1	DHCP 伺服器設定頁面	40
圖 6.2	DHCP 借出列表	41
圖 6.3	固定式 DHCP 租約設定畫面	42
圖 7.1	RIP 設定畫面	46
圖 7.2	靜態路由設定畫面	47
圖 7.3	靜態路由設定	48
圖 7.4	路由範例列表	49
圖 8.1	HTTP DDNS 的網路圖	51
圖 8.2	HTTP DDNS 設定頁面	52
圖 9.1	NAPT - 映射任何內部 PC 至單一有效 IP 位址	57
圖 9.2	反面NAPT - 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	58
圖 9.3	防火牆一般設定畫面	61
圖 9.4	ACL 規則設定頁面	64
圖 9.5	ACL 設定範例	65
圖 9.6	ACL 列表範例	66
圖 9.7	Self-Access 設定頁面	67
圖 9.8	Self-Access 設定範例	68
圖 9.9	虛擬伺服器設定畫面	69
圖 9.10	虛擬伺服器撲拓架構圖	71
圖 9.11	虛擬伺服器設定範例 1 - 網頁伺服器	72
圖 9.12	增加一個新的服務	72
圖 9.13	虛擬伺服器設定範例 2 - FTP 伺服器	73
圖 9.14	虛擬伺服器設定範例 3 - FTP 伺服器	74
圖 9.15	ACL 防火牆虛擬伺服器範例 3 - FTP 伺服器	75
圖 9.16	特別應用程式設定畫面	77
圖 10.1	系統服務設定畫面	79



---

圖 10.2	系統管理設定畫面	80
圖 10.3	系統狀態畫面	81
圖 10.4	日期與時間設定畫面	82
圖 10.5	SNMP 設定畫面	84
圖 10.6	Syslog Server 設定畫面	84
圖 10.7	日誌範例	85
圖 10.8	出廠預設值設定畫面	85
圖 10.9	出廠預設值重置確認視窗	86
圖 10.10	出廠預設值重置計時秒數	86
圖 10.11	備份系統設定畫面	87
圖 10.12	回復備份系統設定畫面	88
圖 10.13	從檔案總管中選擇系統設定檔案	88
圖 10.14	系統設定回復畫面	89
圖 10.15	重新啟動系統更新倒數計時秒數	89
圖 10.16	更新韌體頁面	89
圖 10.17	檔案總管選擇畫面	90
圖 10.18	更新韌體確認視窗	90
圖 10.19	韌體更新狀態視窗	90
圖 10.20	韌體更新倒數計時視窗	91
圖 10.21	重新啟動系統頁面	91
圖 10.22	登出設定的管理畫面	92
圖 10.23	確認關閉 IE 瀏覽器	92
圖 12.1	使用封包探測公用程式	98
圖 12.2	使用 nslookup 公用程式	99

---

## 列表目錄

表 2.1	DoS 攻擊類型防護	5
表 2.2	前面板 LEDs 狀態說明	6
表 2.3	後背板插座與指示燈號說明	7
表 3.1	燈號指示列表	11
表 3.2	預設值摘要	18
表 4.1	常用按鍵與圖示的功能敘述	21
表 5.1	區域網路參數設定	23
表 5.2	廣域網路的 PPPoE 參數設定	26
表 5.3	廣域網路的 PPPoE Unnumbered 參數設定	29
表 5.4	廣域網路靜態 IP 參數設定	32
表 5.5	廣域網路 PPTP 參數設定	33
表 5.6	Load Balancing 和 Line Back Up 的相關參數設定	36
表 6.1	DHCP 參數設定	41
表 6.2	固定式 DHCP 租約的相關參數	42
表 7.1	RIP 的相關參數	46
表 7.2	靜態路由參數設定	48
表 8.1	DDNS 的參數設定	52
表 9.1	防火牆的基本參數設定	59
表 9.2	DoS 攻擊定義	60
表 9.3	ACL 規則參數設定	61
表 9.4	服務的相關參數	63
表 9.5	虛擬伺服器參數設定	69
表 9.6	常見應用程式連接埠列表	70
表 9.7	特別應用參數設定	75
表 9.8	常見應用程式連接埠列表	76
表 10.1	SNMP 相關的參數設定	83
表 11.1	IP 位址架構	93

---

# 第一章 簡介

感謝您選購華碩 RX3042H 路由器！現在，您可以將這台高速頻寬的路由器與您的 ADSL 或 Cable modem 進行連接，盡情享受高速區域網路連線的樂趣。

## 1.1 特色

---

- LAN：4 埠 Gigabit 交換器
- WAN：雙 10/100Base-T 乙太網路埠，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。
- 使用者可設定雙 WAN 或 WAN 並支援 DMZ。
- 可透過如微軟 Internet Explorer 6.0 或更新版本的網路瀏覽器，進行功能與參數設定。

## 1.2 系統需求

---

爲了使用 RX3042H 路由器來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（基於網頁的圖形介面）的設定需要：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 如何使用本手冊

---

### 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，RX3042H 有時會被稱爲“路由器“或“閘道器“。
- 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，“系統（System）”→“網路設定（Network Setup）”，代表雙按點選“系統（System）”選單，接著並點選“網路設定（Network Setup）”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。

---



---

重要: 重點提示說明。

---



---

警告: 禁止不當行為及操作，提醒您進行某一項操作時要注意安全。

---

---

## 第二章 認識您的 RX3042H

---

### 2.1 零件明細表

---

除這份資料之外，RX3042H 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 埠高速乙太網路交換器
- 自動速度協調

#### 廣域網路 (WAN)

- 雙 10/100M 乙太網路埠
- 自動 MDI/MDIX 跳線功能

### 2.3 軟體功能

---

#### 2.3.1 NAT 功能

RX3042H 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 RX3042H 所支援的 NAT 類型。

- **NAPT** (網路位址與連接埠轉譯, Network Address and Port Translation) 一亦被稱做 **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 NAPT — 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 RX3042H 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)

RX3042H 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，讓電腦免於受到威脅。

RX3042H 防火牆 ACL 規則支援：

- 基於目的地與來源 IP 位址、埠號與通訊協議的過濾方式。
- 使用 Wild card 組成過濾規則。
- 過濾規則優先權定義。

### 2.3.2.3 防範 DoS 攻擊

RX3042H 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（偽裝）、LAND、Ping of Death 與所有可能被假定的攻擊。舉例來說，RX3042H 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。下表中所列舉者為 RX3042H 提供的攻擊類型防護/偵查類型。

表 2.1 DoS 攻擊的類型防護

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 掃描進行登入 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 (回應攻擊), Ascend Kill
其他類的攻擊	IP spoofing (偽裝), LAND, Targa, WinNuke

### 2.3.2.4 應用層閘道 (ALG)

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。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。因為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）形式的智慧地用來做應用程式解析封包和打開動態聯繫。RX3042H 路由器的防火牆功能，常用的應用程式如 FTP、H.323、RTSP、Microsoft Games、SIP等，提供 ALG 的一個序號。

### 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 RX3042H 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。

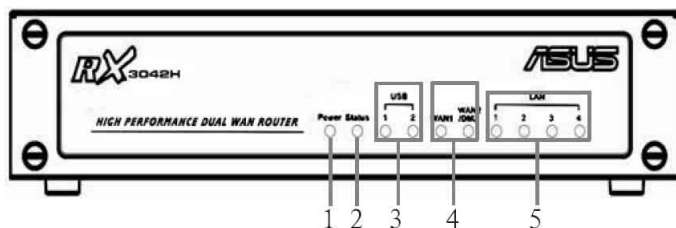


圖2.1 前面板 LED 指示燈

表2.2 前面板 LEDs 狀態說明

LED 標籤	顏色	狀態	標示意義
1	綠色	亮燈	RX3042H 電源已接通
		熄滅	RX3042H 電源未接通
2	綠色		
3	綠色	熄滅	USB 埠已辨識
		亮燈	未偵測到 USB 裝置 偵測到 USB 裝置
4	琥珀色	熄滅	未偵測到連線
		亮燈	偵測到 100Mbps 連線
		閃爍	偵測到 100Mbps 資料傳輸
		亮燈	偵測到 10Mbps 連線
		閃爍	偵測到 10Mbps 資料傳輸
5	琥珀色	熄滅	LAN 埠已辨識
		亮燈	未偵測到連線
		閃爍	偵測到 100Mbps 連線
		閃爍	偵測到 100Mbps 資料傳輸
		亮燈	偵測到 10Mbps 連線
		亮燈	偵測到 10Mbps 資料傳輸
		閃爍	偵測到 10Mbps 資料傳輸



### 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。

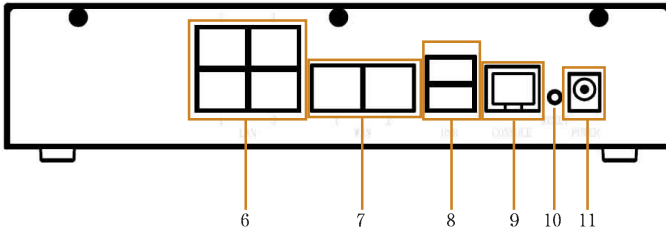
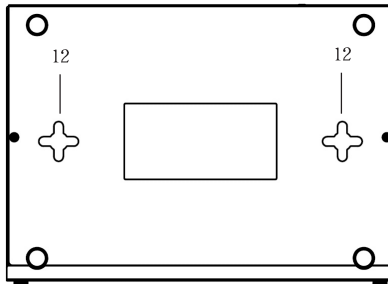


圖2.2 後背板插座

表2.3 後背板插座與指示燈號說明

標籤	標示意義
6	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。
7	WAN 1和 WAN2/ DMZ 雙 WAN 連接埠或一個 WAN 連接埠 + 一個 DMZ 連接埠：連接你的 WAN 端設備，例如ADSL 或 Cable modem 或 DMZ 網路，請注意 DMZ 網路必須連接到標示有 WAN2/DMZ 的連接埠上。
8	USB USB 連接埠：連接到 USB 1.1 或 2.0 裝置
9	Console 不支援
10	RESET 重置按鈕： 1. 重新啟動設備 2. 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。
11	POWER 電源輸入插座：連接產品提供的 AC 電源供應器。

### 2.4.3 底視圖



12. 壁掛插孔：您可以使用這插孔來將 RX3042H 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。

## 2.5 擺放選項

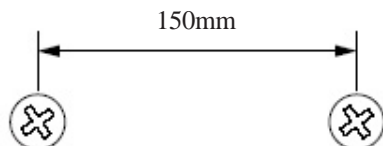
取決於您的環境，您可以為 RX3042H 放置選擇三種支援的方法：平放、壁掛安裝。

### 2.5.1 桌面放置

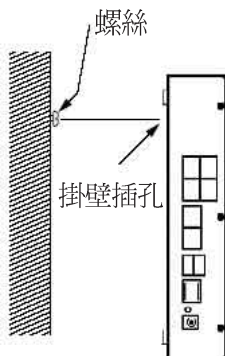
您可將 RX3042H 放置於任何平面上。採用節省空間設計的RX3042H 只需佔用您桌面上的局部空間即可擺放。

### 2.5.2 壁掛安裝介紹

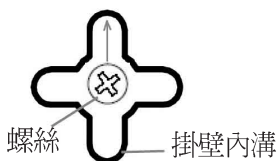
1. 先將兩隻螺絲固定於牆壁上，若您想以前面板或後背板朝上壁掛，則請讓兩隻螺絲相隔約 150 mm。此外，請確認兩隻螺絲是等高的，並請注意在 RX3042H 機身底部是有四個壁掛插孔，您可任意選擇其中兩個插孔進行安裝。



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。



排列成行牆掛在路由器上的兩個螺旋槳槽。



請調動插孔讓牆壁上的兩隻螺絲都可以插入插孔中。

## 第三章 快速安裝指南

本快速安裝指南可以提供將 RX3042H 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 RX3042H 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 4.3 節的說明以確認交換器可以正常運作。

這個迅速的入門指南，假設您已經與您的網際網路服務供應商 (ISP) 建立 ADSL 或者 Cable 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。如需要其他的設定訊息，請參考隨後的章節。

### 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。



**警告：**在你開始之前，為全部設備關掉動力。這些包括您的電腦，您的區域網路中心(如果適用)接通，以及 RX3042H 路由器。

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 RX3042H 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 RX3042H 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。

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 RX3042H、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 RX3042H 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。

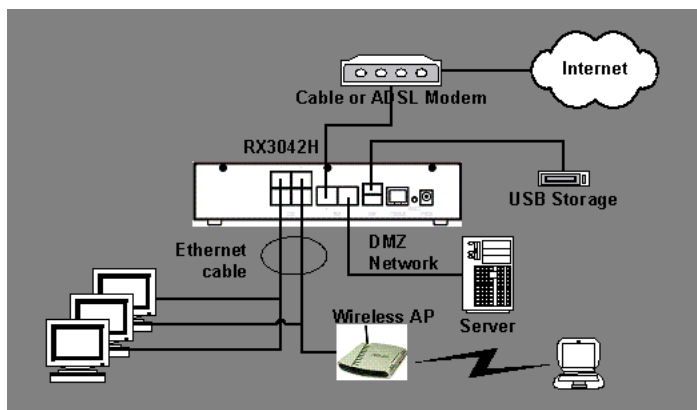


圖3.1 硬體連接示意圖

你應該確認本裝置上的 LED 指示燈如同表格 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 RX3042H 的電源供應器插頭是否妥善地連接在電源插座上。
LAN 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

本快速安裝指南的第 2 部分提供在您的電腦上針對 RX3042H 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，RX3042H 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 RX3042H 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 RX3042H 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 RX3042H，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) 的圖象並選擇 <內容> (通常此圖示會標示為區域連線) 的正確點擊和選擇特性。(經常這張圖象被稱為局部地區連接)。

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。

4. 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。
5. 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，保證檢查箱子在項目左側稱網際協議為傳輸控制協議/網際協議被檢查，並且點選 <特性> 按鈕。
6. 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 協議和如有必要，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。
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。

您可能會看到提示，要求從 Windows 2000 安裝光碟或其他媒體安裝，請依照提示來進行安裝。

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

接下來，請設定您的個人電腦來接受 RX3042H 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 作業系統的個人電腦

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，請尋找起使為“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 協定已被啟用，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啟動您的電腦。

接下來，請設定您的個人電腦來接受 RX3042H 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，請尋找起使為“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 RX3042H 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啟動電腦，則請點選 <確定> 鍵來套用新的設定值並重新啟動電腦。

### 3.2.5 安裝 Windows NT 4.0 作業系統的工作站

首先，檢查 IP 協議，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啟動該通訊協定，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。

6. 點選 <好> 鍵進入下一步，接著若是訊息提示您重新啟動電腦，請點選 <確定> 鍵來重新啟動電腦。接下來請設定您的個人電腦，使其可以接受 RX3042H 所分配的 IP 位址。
7. 開啟控制台視窗，接著請點選網路圖示。
8. 在網路選項中，點選協議標籤頁。
9. 在協議標籤頁中，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 RX3042H 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（通常稱做靜態(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，而您想要每次接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 RX3042H 時，在 192.168.1.0 的網路環境下，您可以指定 192.168.1.0 的 IP 位址給您的 PC，以便建立個人電腦與 RX3042H 之間的連線，在此一網路環境下，在預設的區域網路中，RX3042H 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。



您的個人電腦必須的 IP 位址必需連接於 RX3042H 的區域網路連接埠並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 RX3042H

在第 3 部分中，請您登入成 RX3042H 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 RX3042H 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 RX3042H

請依照下列步驟來設定 RX3042H：

12. 在您進入 RX3042H 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”。
13. 在連接到 RX3042H 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 RX3042H 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

如果你在連接RX3042H 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 RX3042H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 ” OK ” ，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10.2 節的登入密碼和系統設定 ) 。

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 ) 。

The screenshot shows the 'Status' page of the ASUS RX3042H router. The page is titled 'ASUS RX3042H' and 'Status'. It contains the following information:

- General Information:**
  - System Name: RX3042H
  - Firmware Version: 0.53
  - System Time: 18:35:23 5 5 2005
  - Default Gateway: 172.21.150.1
- LAN Information:**
  - IP Address: 192.168.1.1
  - Netmask: 255.255.255.0
  - MAC Address: 00-00-00-04-05-03
- WAN Information:**
  - Connection Mode: DHCP
  - IP Address: 172.21.151.13
  - Netmask: 255.255.254.0
  - Gateway: 172.21.150.1
  - DNS Server1: 172.21.128.8
  - DNS Server2: 172.21.128.9
  - MAC Address: 00-01-02-03-10-FF
- DMZ Information:**
  - Connection Mode: Static
  - IP Address: 192.168.3.1
  - Netmask: 255.255.255.0
  - Gateway: 192.168.3.254
  - DNS Server1: 192.168.3.254
  - DNS Server2: 0.0.0.0
  - MAC Address: 00-00-00-06-07-07

圖3.3 系統資訊頁面

- 請遵照第五章 “ 路由器設定 ” 來為 RX3042H 進行 LAN 與 WAN 的設定。

當您將 RX3042H 完成基本的設定之後，請閱讀以下內容來決定您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 RX3042H 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 12 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，RX3042H 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，請再次參閱第四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	RX3042H 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 RX3042H 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 RX3042H 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

## 第四章 使用設定管理員

RX3042H 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 RX3042H 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 RX3042H 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 RX3042H 上之區域網路 (LAN) 或廣域網路 (WAN) 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。

你可從任何連接於 RX3042H 區域網路 (LAN) 或廣域網路 (WAN) 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 RX3042H 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 RX3042H 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 <OK>。

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 10.2 節登入密碼與系統設定）。

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 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 RX3042H 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。

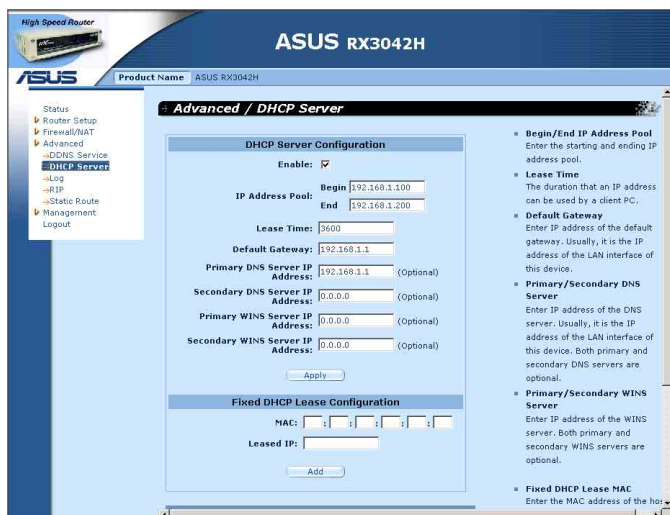





圖4.2 典型的設定管理員頁面







## 4.2.1 選單導覽

- 開啓相關選單的延伸群組：點選選單或是圖示，。
- 收回相關選單的延伸群組：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，。

## 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。
	選擇選項進行編輯。
	刪除已被選擇的選項。

## 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，便是在狀態 (Status) 頁中可取得的範例資訊。

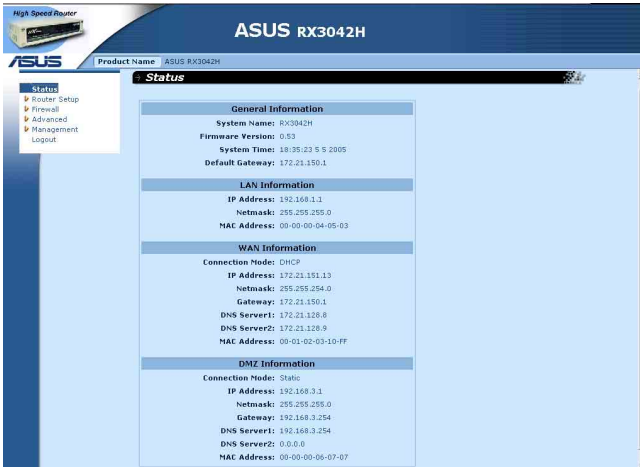


圖 4.3 系統資訊頁面





## 第五章 路由設定

本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 RX3042H 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 RX3042H 處在同一子網路下。RX3042H 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 RX3042H 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	RX3042H 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 RX3042H 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。



圖5.1 網路設定 - 區域網路設定

2. (非必需步驟) 輸入 RX3042H 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。
3. 輸入 RX3042H 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。



7. 若連線超過計時的時間，您只需要重新登入即可繼續進行設定。

## 5.2 WAN/DMZ 設定

本節中將會敘述如何對 RX3042H 連線到您的 ISP 之廣域網路（WAN）或與 DMZ 介面進行相關的設定。在本節中，您將可以學習到如何為您的廣域網路（WAN）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

RX3042H 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。

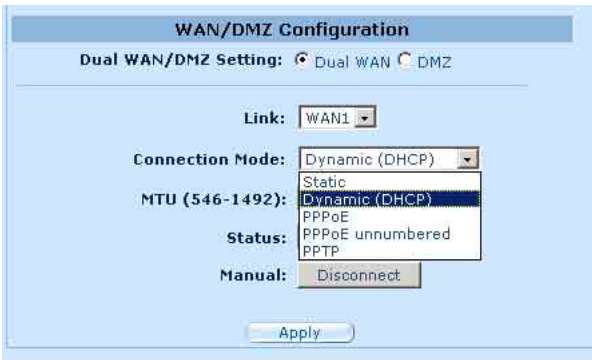


圖5.3 網路設定 - 廣域網路設定

### 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。

**WAN/DMZ Configuration**

Dual WAN/DMZ Setting:  Dual WAN  DMZ

Link:

Connection Mode:

PPPoE Session:   Enable

User Name:

Password:

Service Name:  (Optional)

AC Name:  (Optional)

IP Address:  (Optional)

Primary DNS Server:  (Optional)

Secondary DNS Server:  (Optional)

MTU (546-1492):

Connect on Demand:  Enable  Disable

Disconnect after Idle(min):

Status:

Manual:

圖5.4 WAN — PPPoE 設定

### 5.2.2.1 廣域網路的PPPoE 參數設定

下表描述提供給廣域網路的 PPPoE 連接模式的設定參數。

表 5.2 廣域網路的 PPPoE 參數設定

設定	描述
Link	選擇一個連接埠進行配置，可選擇的選項有 WAN1、WAN2 或 DMZ。
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。

設定	描述
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 和成 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。
MTU	此為您可以指定傳送的封包的最大大小，對於 PPPoE 來說，MTU 值的範圍是從 546 到 1492，預設值為 1492。
Connection on Demand	按下” Enabled” 或” Disabled” 圖示按鍵，就可以啟用或關閉這項功能。
Disconnect after Idle (min)	輸入當無通信量時您想要斷開的非活動時間點。若您建立的數值為 0 時，則表示沒有設定非活動的時間點。請注意 SNTP 服務的動作，可能會干擾這個服務功能的進行。
狀態 (Status)	On : 在 PPPoE 的連線已建立。 Off : 無 PPPoE 的連線建立。 Connecting : RX3042H 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. 選擇一個 WAN 連接埠來進行配置 (WAN1/WAN2) PPPoE 的連線模式。
3. 從 WAN 連線模式的下拉式選單中如圖 5.3，選擇 PPPoE。
4. 從 PPPoE 區段 ID 下拉式選單中選擇 PPPoE 區段 ID。以目前來說，每個 WAN 埠最多支援兩個區段。
5. 輸入由您的 ISP 所提供的使用者名稱與密碼。
6. 若您的 ISP 需要，請輸入服務名稱（非必需）。

7. 如果 ISP 允許您為 WAN 使用同樣的 IP 位址的話，請在 IP 位址欄中輸入。否則，請跳過此項步驟（非必需）。
8. 如果您想使用主要的 DNS 伺服器，請在第一和 / 或第二個 DNS 伺服器輸入 IP 位址。否則，請跳過此項步驟（非必需）。
9. 若需要更改 MTU 值，如果您不清楚填入多少數值，請保留預設值。而對於浮動 IP 來說，MTU 值的範圍是從 546 到 1492，預設值為 1492。
10. 輸入關於“Disconnect after idle (min)”與“Connect on Demand”的適當設定值。
11. 點選  來儲存設定值。

### 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。

The screenshot displays the 'WAN/DMZ Configuration' interface. At the top, it shows 'Dual WAN/DMZ Setting' with radio buttons for 'Dual WAN' (selected) and 'DMZ'. Below this, the 'Link' is set to 'WAN1'. The 'Connection Mode' is set to 'PPPoE unnumbered'. The 'Enable NAPT' checkbox is checked. The 'User Name' field contains 'UserName' and the 'Password' field contains '\*\*\*\*\*'. The 'Service Name' and 'AC Name' fields are empty, with '(Optional)' text to their right. The 'IP Address' field is set to '0.0.0.0'. The 'Unnumbered network address' field is also set to '0.0.0.0'. The 'Unnumbered netmask' field is set to '0.0.0.0'. The 'Primary DNS Server' and 'Secondary DNS Server' fields are both set to '0.0.0.0', with '(Optional)' text to their right. The 'MTU (546-1492)' field is set to '1492'. The 'Connect on Demand' section has radio buttons for 'Enable' and 'Disable', with 'Disable' selected. The 'Disconnect after Idle(min)' field is set to '0'. The 'Status' field is set to 'OFF'. At the bottom, there is a 'Manual' button labeled 'Disconnect' and an 'Apply' button.

圖 5.4 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 連接模式下的無編號參數設定。

表5.3 廣域網路 PPPoE Unnumbered 參數設定

設定	描述
Link	選擇一個連接埠進行配置，可選擇的選項有 WAN1、WAN2 或 DMZ。
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 NAPT	按下這項可以開啓或關閉 NAPT 的功能。
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。
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。
Primary /Secondary DNS Server (第一/第二 DNS 伺服器)	第一和/第二個 DNS 伺服器的 IP 位址可視情況填入，因為 PPPoE 將會採用自動的方式來偵測您的 ISP 所提供的 DNS IP 位址。倘若您想要使用其他的 DNS 伺服器，請在此欄中輸入其 IP 位址。
MTU	您可以指定傳送封包的大小上限，針對 PPPoE 來說，數字 0 表示沒有超過時間。請注意，如果有啓用 SNTP 的話，它會影響這項功能。
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)	輸入當無通信量時您想要斷開的非活動時間點。若您建立的數值為 0 時，則表示沒有設定非活動的時間點。請注意 SNTP 服務的動作，可能會干擾這個服務功能的進行。
狀態 (Status)	On：PPPoE unnumbered 的連線已建立。 Off：無 PPPoE unnumbered 的連線建立。 Connecting：RX3042H 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提供者的 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. 選擇一個 WAN 連接埠來進行配置 (WAN1/WAN2) PPPoE 的連線模式。
3. 從 WAN 連線模式的下拉式選單中如圖5.4，選擇 PPPoE。
4. 如果要使用 NAT 連線的話，請選擇 NAPT。
5. 輸入由您的 ISP 所提供的使用者名稱與密碼。
6. 若您的 ISP 需要，請輸入服務名稱 (非必需)。
7. 輸入 ISP 提供的 IP 位址、unnumbered 網路位址，以及 unnumbered 子網路遮罩。
8. 如果您想使用主要的 DNS 伺服器，請在第一和 / 或第二個 DNS 伺服器輸入 IP 位址。否則，請跳過此項步驟 (非必需)。
9. 若需要更改 MTU 值，如果您不清楚填入多少數值，請保留預設值。而對於浮動 IP 來說，MTU 值的範圍是從 546 到 1492，預設值為 1492。
10. 輸入關於 “Disconnect after idle (min)” 與 “Connect on Demand” 的適當設定值。
11. 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。



The screenshot shows the 'WAN/DMZ Configuration' interface. At the top, there are two radio buttons for 'Dual WAN/DMZ Setting': 'Dual WAN' (selected) and 'DMZ'. Below this, the 'Link' is set to 'WAN1'. The 'Connection Mode' is set to 'Dynamic (DHCP)'. The 'MTU (546-1492)' is set to '1492'. The 'Status' is set to 'OFF'. The 'Manual' setting is set to 'Disconnect'. At the bottom, there is an 'Apply' button.

圖5.5 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

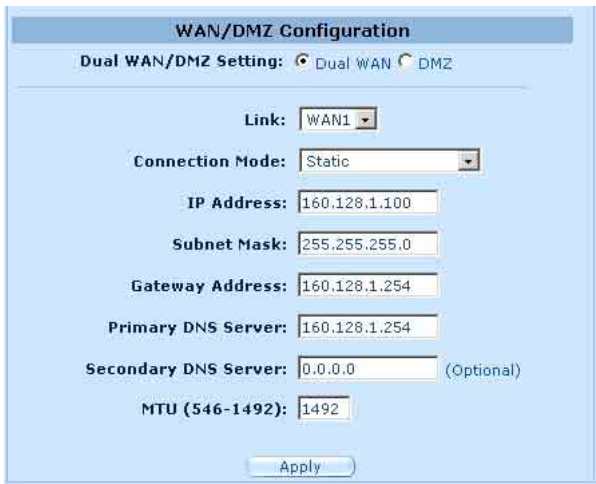
請依照下列介紹來進行動態 IP 設定：

1. 打開 Router Connection 安裝設定頁面，並雙按點選 Router Setup → Connection 選單。



2. 選擇一個 WAN 連接埠來進行配置 (WAN1/WAN2) PPPoE 的連線模式。
3. 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。
4. 若需要更改 MTU 值，如果您不清楚填入多少數值，請保留預設值。而對於浮動 IP 來說，MTU 值的範圍是從 546 到 1492，預設值為 1492。
5. 點選  來儲存設定值。

## 5.2.5 靜態 IP



The screenshot shows the 'WAN/DMZ Configuration' window. At the top, it says 'Dual WAN/DMZ Setting:  Dual WAN  DMZ'. Below this, there are several fields for configuration:

- Link: WAN1 (dropdown menu)
- Connection Mode: Static (dropdown menu)
- IP Address: 160.128.1.100
- Subnet Mask: 255.255.255.0
- Gateway Address: 160.128.1.254
- Primary DNS Server: 160.128.1.254
- Secondary DNS Server: 0.0.0.0 (Optional)
- MTU (546-1492): 1492

At the bottom of the window is an 'Apply' button.

圖5.6 WAN - 靜態 IP 設定

### 5.2.5.1 WAN 或 DMZ 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
Link	選擇一個連接埠進行配置，可選擇的選項有 WAN1、WAN2 或 DMZ。
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 RX3042H 的廣域網路處於相同的子網路下。
第一/第二/ DNS 伺服器 (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。
MTU	您可以指定傳送封包的大小上限，針對靜態 IP 連線而言，MTU 的範圍是從 546 到 1500，預設值為 1500。

### 5.2.5.2 WAN 或 DMZ 模式下的 IP 位址

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. 選擇一個 WAN 連接埠來進行配置（WAN1/WAN2）PPPoE 的連線模式。
3. 從廣域網路（WAN）連線選單的下拉式選單中，如圖 5.6 所示選擇 Static。
4. 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。
5. 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。
6. 輸入由您的 ISP 所提供的閘道器位址。
7. 輸入第一 DNS 伺服器的 IP 位址。本訊息是由您的 ISP 所提供，至於第二 DNS 伺服器 IP 位置則非必需輸入。
8. 若需要更改 MTU 值，如果您不清楚填入多少數值，請保留預設值。而對於浮動 IP 來說，MTU 值的範圍是從 546 到 1500，預設值為 1500。
9. 點選  來儲存設定值。

## 5.2.6 PPTP

一些 ISP 業者則提供使用者透過 PPTP 的方式連線。

### 5.2.6.1 設定供廣域網路使用的 PPTP 參數

表5.5 列出 PPTP 連線模式的相關參數設定。

表5.5 廣域網路 PPTP 參數設定

設定	描述
Link	選擇一個連接埠進行配置，可選擇的選項有 WAN1、WAN2 或 DMZ。
連線模式 (Connection Mode)	從連線模式下拉式選單中選擇 PPTP。
WAN 介面 IP	選擇 WAN IP 位址的配置方式：採用靜態（手動設定 IP 位址）或動態（由 DHCP 伺服器自動產生 IP 位址）。
狀態 (Status)	如果 WAN IP 是由您的 ISP 業者提供的固定 IP，那麼請選擇這個模式來連線。
IP Address	輸入由您的 ISP 業者所提供的 WAN IP 位址。
Subnet Mask	輸入由您的 ISP 業者所提供的 WAN IP 的子網路遮罩位址。
Gateway Address	輸入由您的 ISP 業者所提供的 WAN IP 的閘道器位址。
Dynamic (DHCP) 動態 DHCP	若您的 WAN IP 位址是由 DHCP 伺服器自動產生的而取得的話，請選擇這項連線模式。
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）。
伺服器 IP 位址 (Server IP Address)	輸入 ISP 提供的 PPTP 伺服器 IP 位址。
MTU	您可以指定傳送封包的大小上限，針對 PPTP 來說，MTU 值的範圍是從 546 到 1460，預設值為 1460。
MPPE	MPPE 表示微軟的點對點加密協定 (Microsoft Point-to-Point Encryption protocol)，如果封包欲採用此協定加密的話，請選此項。
Connection on Demand	按下“Enabled”或“Disabled”圖示按鍵，就可以啟用或關閉這項功能。
Disconnect after Idle (min)	輸入當無通信量時您想要斷開的非活動時間點。若您建立的數值為 0 時，則表示沒有設定非活動的時間點。請注意 SNTP 服務的动作，可能會干擾這個服務功能的進行。
狀態 (Status)	On：PPTP 的連線已建立。 Off：無 PPTP 的連線建立。 Connecting：RX3042H 正試圖使用 PPTP 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提供者的 PPTP 連線模式。


The screenshot displays the 'WAN/DMZ Configuration' interface. At the top, 'Dual WAN/DMZ Setting' has 'Dual WAN' selected. Under 'Link', 'WAN1' is chosen. 'Connection Mode' is set to 'PPTP'. The 'WAN Interface Settings' section includes 'WAN Interface IP' set to 'Static', 'IP Address' as '160.128.1.100', 'Subnet Mask' as '255.255.255.0', and 'Gateway Address' as '160.128.1.254'. The 'PPTP Settings' section shows 'User Name' as 'userName', 'Password' as '\*\*\*\*\*', 'Server IP Address' as '160.128.1.10', and 'MTU (546-1492)' as '1492'. 'MPPE' is unchecked. 'Connect on Demand' has 'Disable' selected. 'Disconnect after Idle(min)' is '0', 'Status' is 'OFF', and the 'Manual' button is 'Disconnect'. An 'Apply' button is at the bottom.

圖 5.7 WAN - PPTP 設定

### 5.2.6.2 設定供廣域網路模式下的 PPTP

請依照下列介紹來設定 PPTP 設定：

1. 打開 Router Connection 安裝設定頁面，並雙按點選 Router Setup → Connection 選單。
2. 選擇一個 WAN 連接埠來進行配置（WAN1/WAN2）PPTP 的連線模式。

3. 從廣域網路 (WAN) 連線選單的下拉式選單中，如圖 5.6 所示選擇 PPTP。
4. 選擇取得 WAN IP 的方式：採用靜態或動態。若 ISP 業者提供靜態 (固定) IP 位址，請在 WAN 介面 IP 下拉式功能表中選擇 Static。如果您不能確定，請詢問您的 ISP 業者。
5. 如果您的 WAN IP 為採用手動設定的話，請輸入 IP 位址、子網路遮罩以及閘道器 IP 位址。
6. 輸入由您的 ISP 所提供的使用者名稱與密碼。
7. 輸入由 ISP 所提供的 PPTP 服務器 IP 位址。
8. 若需要更改 MTU 值，如果您不清楚填入多少數值，請保留預設值。而對於浮動 IP 來說，MTU 值的範圍是從 546 到 1460，預設值為 1460。
9. 若傳遞的封包要使用 MPPE 進行加密的話，請選擇 MPPE。
10. 輸入關於 “Disconnect after idle (min)” 與 “Connect on Demand” 的適當設定值。
11. 點選  來儲存設定值。

## 5.3 WAN Load Balancing 和 Line Back Up

在 WAN 連線中，RX3042H 支援 Load Balancing (負載平衡) 與 Line Back Up (線上備份) 的功能。當您要進行這些功能設定時，請進入 Router Connection (路由連線) 設定畫面中，選擇 Dual-WAN 後 (點選 Router Connection -> Connection 選單)，就可以使用這些功能。

透過 RX3042H 上的兩個 WAN 連接埠，WAN 負載平衡功能會根據預設的頻寬需求來處理通訊傳輸。另一項特點是可以支援 WAN 連接埠的故障恢復 (fail-over) 功能，如果 WAN 連線停止傳輸的話，RX3042H 將會把停止傳輸的連接埠上的資料傳輸至另一個連接埠上。

而線上備份則是另一個保持連線至網際網路的功能，當第一個 WAN 埠連線中斷時，網際網路的連線將會自動轉換到另一個 WAN 埠繼續連線。

### 5.3.1 WAN Load Balancing 和 Line Back Up 設定參數

表5.6 列出了 Load Balancing 和 Line Back Up 的相關參數設定。

表5.6 Load Balancing 和 Line Back Up 的相關參數設定

設定	描述
Load Balance (負載平衡)	選擇下面三項的其中一項： Disable：關閉 WAN load balancing 和 line back up 功能。 Auto Mode：如果需要 load balancing 功能的話，請選擇此項。此選項針對 load balancing 有很大的幫助。 Line Back Up：如果需要 line back up 功能的話，請選擇此項。在預設的狀態下，第一個連線則為 WAN1，備份連接的則為 WAN 2。
WAN1/WAN2 頻寬	輸入您想要分配到每個 WAN 埠的傳輸流量大小比例。比例值在 0 與 100% 之間。例如，WAN1 80% 和 WAN2 20%，表示 80% 的流量頻寬分配給 WAN1，而 20% 則分配給 WAN2。
Connectivity Check (連線檢查)	點選 Enabled 或 Disabled 按鈕來開啓或關閉這項功能。這項檢查功能是用來監控 WAN 連接埠的連線狀態。如果關閉此項功能，RX3042H 將不能進行故障回復 (fail-over)。因此，若其中一個 WNA 連接埠停止連線，該連接埠上的資料傳輸就不能轉傳送到正常的連接埠上。所以您應該選擇此項為 Enabled，以確保此功能開啓。但是，如果閘道器或一些特定的網路裝置不想被 Ping 的話，您就需要關閉此項功能。否則，針對 WAN 連線狀態，RX3042H 會做出不正確的判斷，因而可能會影響到負載平衡或線上備份的運作。
Connection Check (連線檢查時間間隔)	RX3042H 檢查 WAN 連線狀態的時間間隔。可填入的數值在 1 到 60 秒之間。
Connection check IP Address (WAN1) (連線檢查 IP 位址 WAN1)	輸入流量經過的特定網路裝置的 IP 位址。此項目為選擇性的填寫，一般來說，您不需要在此項目內填入 IP 位址，除非您知道流量必需經過那個特定的網路裝置。
Connection check IP Address (WAN2) (連線檢查 IP 位址 WAN2)	輸入流量經過的特定網路裝置的 IP 位址。此項目為選擇性的填寫，一般來說，您不需要在此項目內填入 IP 位址，除非您知道流量必需經過那個特定的網路裝置。

## 5.3.2 設定 WAN 負載平衡

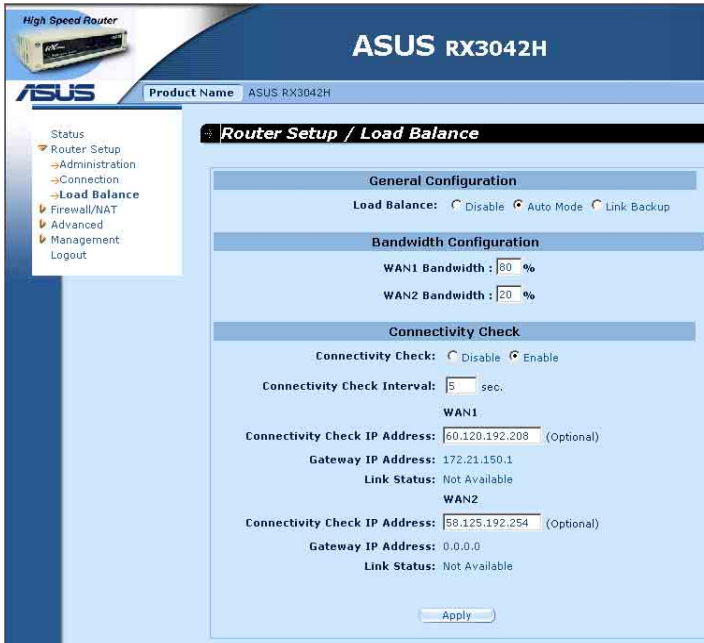



圖5.8 負載平衡設定

請依照下列介紹來設定 WAN 負載平衡設定：

1. 打開 Router Connection 安裝設定頁面，並雙按點選 Router Setup → Load Balancing 選單。
2. 在 Load Balancing 項目中選擇 Auto Mode。
3. 輸入您想要分配的兩個 WAN 埠的傳輸流量大小比例。比例值在 0 到 100% 之間，兩個的總和為 100%。
4. 選擇是否要啓用或關閉連線檢查功能，若此功能啓用的話，請輸入以下的訊息：
  - a) 輸入連線檢查的時間間隔。
  - b) 輸入 WAN1 和 /WAN2 連線檢查的 IP 位址（非必需）。
5. 點選  來儲存設定值。

### 5.3.3 設定 WAN 線上備份

請依照下列介紹來設定 WAN 線上備份 (Line Back Up) 設定：

1. 打開 Router Connection 安裝設定頁面，並雙按點選 Router Setup → Load Balancing 選單。
2. 在 Load Balancing 項目中選擇 Line Backup。
3. 選擇是否要啓用或關閉連線檢查功能，若此功能啓用的話，請輸入以下的訊息：
  - a) 輸入連線檢查的時間間隔。
  - b) 輸入 WAN1 和 /WAN2 連線檢查的 IP 位址 (非必需)。
5. 點選  來儲存設定值。



---

## 第六章 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 RX3042H 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 RX3042H 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 RX3042H 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 RX3042H 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，如下頁圖 6.1 所示，並雙按點選 Advanced → DHCP Server 選單。

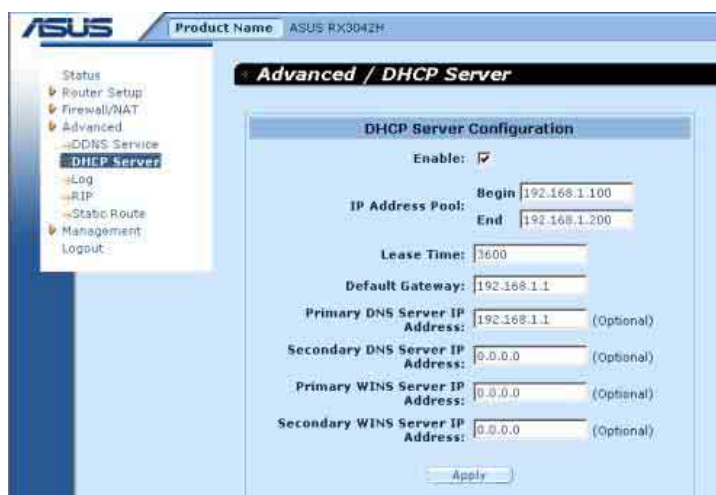


圖6.1 DHCP伺服器設定頁面

2. 輸入IP位址池所需資訊（開始/結束位址），子網路遮罩，IP 借出資訊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6.1 DHCP 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所在區域網路使用的 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 位址之電腦的預設開道器位址。預設的開道器位址是 DHCP 用戶端電腦首先用來連接實際網路裝置的 IP 位址。一般而言，這便是指 RX3042H 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 那裡。但是，您可以輸入 RX3042H 區域網路 IP 位址，來把它當作是 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（因為它有 DSN 代理的功能，可以將 DNS 請求提交給 DNS 伺服器），並回復結果至區域網路的電腦。請注意！無論主要（第一）或次要（第二）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 位址的電腦所使用。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。

3. 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RX3042H 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上方的“Current DHCP Lease Table”連結，如圖 6.2 所示的頁面便會出現。

DHCP 借出（租約）列表將會列出所有借出的 IP 位址與對應的 MAC 位址。

No	IP Address	MAC Address	Start Time	End Time	Client Name
1	192.168.1.100	00:08:a1:18:a5:9b	6 2005/04/23 19:54:07	6 2005/04/23 20:54:07	cc_hsiao_oapc
2	192.168.1.101	00:0c:29:88:f2:90	6 2005/04/23 19:54:45	6 2005/04/23 20:54:45	ac2000

圖6.2 DHCP 借出列表

## 6.1.5 固定式 DHCP 租約

固定式 DHCP 租約主要用在主機需要從 DHCP 伺服器取得固定（靜態）DHCP 位址的情況。首先，您需設定電腦，讓它能夠接收 DHCP 伺服器分配的 DHCP 訊息。

### 6.1.5.1 進入固定式 DHCP 租約設定畫面

進入 Fixed DHCP Lease（固定式 DHCP 租約）設定畫面，如圖 6.3 所示，點選 Advanced -> DHCP Server 選項。

請注意，當您開啓固定式 DHCP 租約設定畫面時，如圖 6.3 所示，可以看到目前使用的借出（租約）列表，會顯示在畫面的下方。

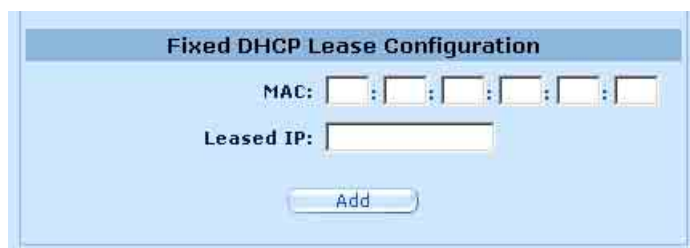


圖 6.3 固定式 DHCP 租約設定畫面

### 6.1.5.2 增加一組固定式 DHCP 租約

若要增加一組 DHCP 固定租約，請依照以下的步驟進行：

1. 點選 Advanced -> DHCP Server 選單，如圖 6.3 所示，打開 Fixed DHCP Lease 設定畫面。
2. 輸入 MAC 位址以及主機所需要的固定（靜態）IP 位址，如表 6.2 所詳細列出的固定式 DHCP 租約相關的設定參數。

表 6.2 固定式 DHCP 租約的相關參數

設定	描述
固定式 DHCP 租約的 MAC 位址 ( Fixed DHCP Lease MAC )	需要從 DHCP 伺服器取得固定 IP 位址裝置的 MAC 位址。
固定式 DHCP 租約的 IP 位址 (Fixed DHCP Lease IP )	從 DHCP 伺服器取得的固定 IP 位址，請注意這個 IP 位址必須是 DHCP IP 池以外的 IP 位址。

### 6.1.5.3 查看固定式 DHCP 租約列表

若您想查看固定式 DHCP 租約，請點選 Advanced -> DHCP Server 選單，就可以開啓固定式 DHCP Lease（租約）列表。

---

## 6.2 DNS

---

### 6.2.1 關於 DNS

網域名稱系統（Domain Name System，DNS）伺服器，提供使用者一個相當便利的網址輸入方式（如“yahoo.com”），這個網址在實際上。等於 Internet 路由中所輸入的 IP 位址。

當電腦使用者在瀏覽器中輸入一個網域名稱，接著電腦會向 DNS 伺服器發出一個請求，來要求取得相對應的 IP 位址。然後 DNS 伺服器會試著在自己的資料庫裡面找尋此網域名稱，若沒找到，則會向更高一等級的 DNS 伺服器提出搜尋的需求。當位址找到之後，伺服器會將找到的 IP 位址傳回給電腦，並同時把它建立在 IP 資料庫裡面，以提供下次能更快速搜尋使用。

### 6.2.2 分配 DNS 位址

多個 DNS 位址是用來防止當某個 DNS 伺服器停止動作或超過負荷時，可以提供替代之用。ISP 一般提供第一（主要）和第二（次要）個 DNS 位址，也有可能提供更多位址。您所上網用的電腦，可經由下面的任一方式來取得 DNS 位址：

- 靜態（固定）：若您的 ISP 提供 DNS 伺服器的位址，您只需要在電腦的 IP 設定中填上即可使用。
- 從 DHCP 伺服器中採動態（浮動）的方式取得：您可以在 RX3042H 的 DHCP 伺服器中設定 DNS 位址，允許 DHCP 伺服器分配 DNS 位址給電腦使用。請參考 6.1.3 節“設定 DHCP 伺服器”，來了解如何設定 DHCP 伺服器。

而您也可以指定 ISP 的 DNS 伺服器的實體位址（在電腦主機上或在 DHCP 伺服器的設定畫面中），或者您也可以指定 RX3042H 的網路連接埠的位址（192.168.1.1）。當您指定網路連接埠的 IP 位址後，這個裝置就有 DNS relay（轉送）的功能，關於這項功能，請參考下一節的介紹。



**注意：**若您在電腦或 DHCP 設定中，指定了實體的 DNS 位址，DNS relay（轉送）功能將不會被啓用。

---

## 6.2.3 設定 DNS 轉送功能

當指定區域網路路由器的網路連接埠的 IP 位址為 DNS 位址後，路由器將會自動地具備 DNS relay (轉送) 功能。也就是說，該裝置本身不是 DNS 伺服器，它只是把網域名稱查詢的請求從區域網路中的電腦傳送到 ISP 的 DNS 伺服器上，以取得反向的數據資料後，再把這些資料轉給電腦。

當具備 DNS 轉送功能時，RX3042H 必須保留 DNS 伺服器的 IP 位址，它可以從以下兩種方式取得位址：

- 從 PPPoE 或動態 IP 連線中取得：若 RX3042H 使用 PPPoE (請參考第 5.2.2 節 PPPoE 或第 5.2.3 節 PPPoE Unnumbered) 或是動態 IP (請參考第 5.2.4 節動態 IP) 連線到 ISP，主要和次要 DNS 位址可以透過 PPPoE 連線來取得。選擇這種方式，最大的好處就是當 ISP 更改它們的 DNS 位址時，您可以不用再重新設定電腦這端或 RX3042H 的設定。
- 設定 RX3042H，如圖 5.3、5.4、5.5 和 5.6 所示，您可以在 WAN 設定畫面中，指定 ISP 提供的 DNS 位址。

請按照以下的步驟，來設定 DNS 轉送：

1. 如圖 6.1 所示，在 DHCP 設定畫面的 DNS 伺服器的 IP 位址欄中，輸入網路 IP。
2. 電腦上的網路設定，使用網路安全路由器上的 DHCP 伺服器所分配的 IP 位址，或者手動將網路上每一部電腦都輸入網路安全路由器的 IP 位址，作為它們的 DNS 伺服器位址。



**注意：**在電腦重新啟動之前，啟用 DNS 轉送前所分配給網路電腦的 DNS 位址，將會一直有效。當您將電腦的 DNS 位址變更成網路 IP 位址時，DNS 轉送才會生效。

而同樣的，在 DNS 轉送功能啟用之後，您在 DHCP 設定或電腦上指定了一個 DNS 位址 (不同於網路 IP 位址)，接著這個位址會取代 DNS 轉送的位址。

## 第七章 路由

您可以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 RX3042H 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？

- 在您的區域網路中的電腦，一組預設的閘道器會將所有網際網路傳輸的資料傳送到 RX3042H 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 RX3042H 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 啓用 RIP 的動態路由協定

RIP（Routing Information Protocol，路由訊息協定）允許在路由器間交換路由訊息；因此，路由可以不用人工操作，即可自動更新。如圖 10.1 所示，您可以在系統服務（System Services）設定畫面中啓動 RIP 的功能。



圖7.1 RIP 設定畫面

## 7.2.1 RIP 相關的參數

以下的列表中列示了 RIP 的相關參數。

表 7.1 RIP 的相關參數

設定	描述
介面 (Interface)	選擇一個路由訊息交換的連接方式，可選擇的有 LAN、WAN1、WAN2、PPPoE1、PPPoE2、PPPoE3，以及 PPPoE4。
路由訊息協定 (RIP)	點選 Enable 或 Disable 按鈕來開啓或關閉“RIP”功能。請注意，您必須先啓用 Management/System Service 設定畫面中的 RIP 服務。
被動模式 (Passive Mode)	若要将 RIP 設定成只能接收其他路由器所發送的訊息，而不能發送訊息的話，請設定啓用這個模式。 若您希望 RIP 模式既能夠接收又能夠發送訊息給其他路由器的話，請關閉 (Disable) 這個模式。
RIP 版本 (發送) (RIP Version (Send))	選擇發送路由訊息的 RIP 版本，有三個版本可供您選擇：版本1、版本2，和兩個同時。
RIP 版本 (接收) (RIP Version (Receive))	選擇接收路由訊息的 RIP 版本，有三個版本可供您選擇：版本1、版本2，和兩個同時。
驗證 (Authentication)	點選 Enable 或 Disable 按鈕來開啓或關閉訊息交換的驗證功能。請注意，所有的路由器交換訊息時，必須使用相同的驗證密碼。
驗證模式 (Authentication)	從下拉是功能列表中，選擇 RIP 的驗證模式。支援 Clear Text 和 MD5 兩種模式。
驗證密碼 (Authentication Key)	輸入路由器交換訊息時，所共同使用的驗證密碼。



## 7.2.2 配置 RIP

請按以下的步驟，來啓用或關閉 RIP：

1. 在 System Service（系統服務）設定畫面中（如圖 10.1 所示），點選 Enable 或 Disable 按鈕，來開啓或關閉 RIP 功能。
2. 在下拉式選單列表中，選擇路由交換的連線介面。
3. 點選 Enable 按鈕來將選擇的連接方式啓用 RIP 功能。
4. 點選 Enable 或 Disable 按鈕，來決定是否啓用被動模式。
5. 接著選擇發送與接收路由訊息的 RIP 版本，有三個版本供您選擇：版本 1、版本 2，以及兩者均可。
6. 點選 Enable 或 Disable 按鈕，來決定是否要啓用驗證功能。
7. 若啓用了驗證功能，接著就必須選擇其中一種驗證模式，並填入驗證密碼（非必需）。
8. 點選  來儲存這些設定。

## 7.3 靜態路由

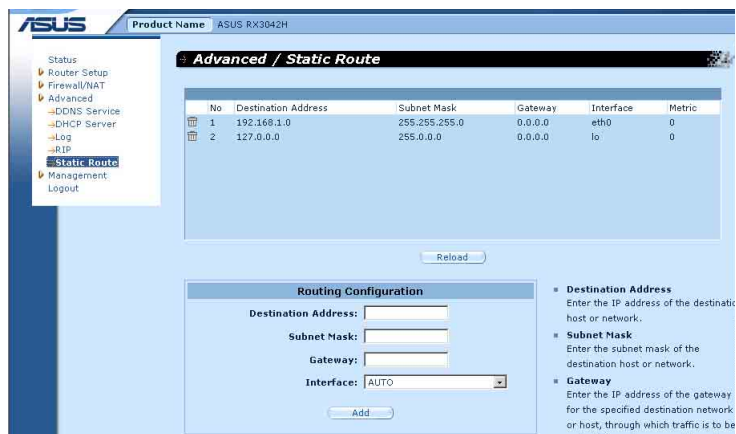


圖7.2 靜態路由設定畫面

### 7.3.1 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 7.2 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。

### 7.3.2 新增靜態路由



圖 7.3 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 7.2 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。

### 7.3.3 刪除靜態路由

No.	Destination Address	Subnet Mask	Gateway	Interface	Metric
1	192.168.1.0	255.255.255.0	0.0.0.0	eth0	0
2	127.0.0.0	255.0.0.0	0.0.0.0	lo	0

圖7.4 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。

### 7.3.4 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 RX3042H 的路由表，請雙按點選 **Advanced** → **Sstatic Route** 選單。接著路由表將會如圖 7.2 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。



## 第八章 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，RX3042H 便會連線到一動態 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（額外的）
- 強制 DNS 更新

### 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。RX3042H 使用 HTTP 來啟動更新作業。RX3042H 支援以下列的服務提供者進行 HTTP DDNS 更新。

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

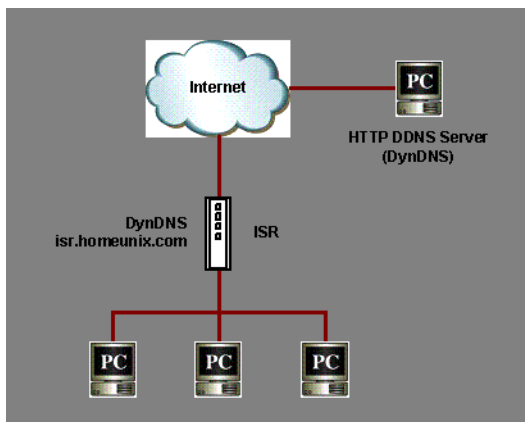


圖 8.1 HTTP DDNS 的網路圖

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。RX3042H 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 的參數設定

欄位	描述
介面	選擇 DDNS 服務所使用的介面。
狀態	顯示 DDNS 的狀態。
DDNS 啟用或關閉	
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 RX3042H 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

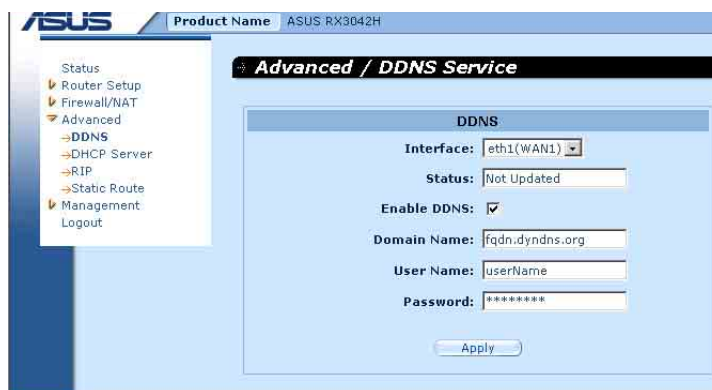



圖8.2 HTTP DDNS設定頁面

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  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。





## 第九章 設定防火牆/NAT 設置

RX3042H 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。

**注意到：** 當你定義一個 ACL 規則，便是指示RX3042H 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 RX3042H 中的 stateful 封包檢查引擎存有一狀態列表，而這份列表是被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啓動時便預設為啓動的。請參閱 9.3.1 “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 RX3042H 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 RX3042H 的防火牆功能被啓動後，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 9.3.1 “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 RX3042H 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，RX3042H 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 至 192.168.1.1。在 RX3042H 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

RX3042H 支援 2 種類型的預設存取規則：

- ACL 規則：用來控制 LAN 和 DMZ 上所有的存取電腦權限，以及控制 LAN 和 DMZ 上所有存取外部網路的電腦的權限。
- Self-Access (自我存取) 規則：作為控制 RX3042H 自身存取動作的用途。

### 預設安全存取規則

- 所有的從外部網路來存取 LAN 和 DMZ 的主機流量都會被阻擋。
- 所有的從 LAN 來的流量都會經由使用 NAT 來存取外部網路。



**注意：**您無需自 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 NAT 概述

網路位址轉譯允許使用單一設備，例如RX3042H，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。

### 9.2.1 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 9.1 顯示所有本地網路的主機透過對應到一個全球通用 IP 位址的方式來連結網際網路，而連接埠號碼與自由的網路連接埠不同。

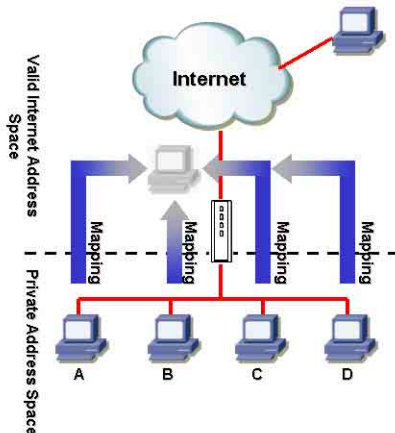


圖 9.1 NAPT - 映射任何內部 PC 至單一有效 IP 位址

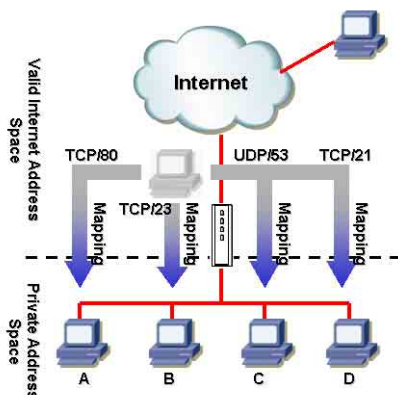


圖 9.2 反向 NAT - 由外部進入的封包依照通訊協定、連接埠號碼或 IP 位址，被分配到各內部主機

## 9.2.2 反向 NAT / 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 RX3042H 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 9.2 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。

## 9.3 防火牆設定

### 9.3.1 防火牆參數設定

表9.1 說明有關防火牆的基本參數設定的相關描述。

表 9.1 防火牆的基本參數設定

欄位	描述
DoS 偵測	勾選或取消勾選本選項來開啓或關閉 DoS 偵測的功能。當 DoS 偵測處於關閉的狀態時，以下的功能也隨之關閉： <ul style="list-style-type: none"> <li>· 狀態封包偵測。</li> <li>· 略過所有的 DoS 攻擊檢查。</li> </ul>
預設的 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 RX3042H 將不會回應遠端嘗試對未開啓的 TCP/UDP 埠的連線。

如欲進行防火牆基本設置，請依照下列介紹進行操作：

1. 開啓 Firewall (防火牆) -> 雙按點選 Setting 設定畫面，如圖 9.3 所示，來開啓此設定頁面。
2. 勾選或取消勾選每一個相對應的選項。
3. 點選  來儲存設定值。

### 9.3.2 DoS 設定

RX3042H 有一攻擊防禦引擎，以提供保護內部網路免於遭受服務中止 (DoS) 攻擊，像是 SYN flooding、IP smurfing、LAND、Ping of Death 與所有封包重組類型的攻擊。這個設定功能，還能丟棄 ICMP 重寄及 IP loose/strict 來源路由封包。此外，它也可以丟棄 ICMP 重新導向與 IP 放鬆/限制路由封包。舉例來說，RX3042H 的防火牆功能，可防範來自“WinNuke”用來癱瘓視窗作業系統的攻擊。同時，RX3042H 防火牆還提供了多種針對普通 Internet 攻擊的保護，如 IP Spoofing、Ping of Death、Land Attack，以及封包重組攻擊。請參考以下的列表 2.1，便是 RX3042H 防火牆可提供保護的 DoS 攻擊類型列表。

#### 9.3.2.1 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。當不能從有效的用戶那裡接收連線時，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，有時也可能是為了半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。
Re-assembly	在攻擊中，攻擊者的 IP 的第二或第三片段，會含有一種混淆的偏移值（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 9.3 所示，開啓 Firewall（防火牆）設定畫面，藉由雙按點選 Firewall → Security 選單，如圖 9.3，來開啓防火牆一般設定畫面。
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。

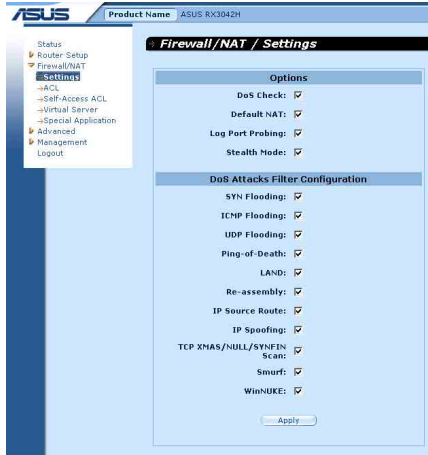


圖9.3 防火牆一般設定畫面

## 9.4 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（Self-Access）ACL 規則的參數設定。

表9.3 ACL 規則參數設定

欄位	描述
	交通方向 - 從下拉式選單列表中选择適當的選項來設定 ACL。 配置雙 WAN 有兩個選項可選：LAN -> WAN 以及 WAN -> LAN。 配置 WAN + DMZ 有六個選項可選：LAN ->WAN, WAN ->LAN, LAN ->DMZ, DMZ ->LAN, WAN ->DMZ 以及 DMZ -> WAN。
ID	
新增	點選本選頁來新增 ACL 規則。
規則編號	從下拉式選單中选择一個規則，並修改它的設定。

欄位	描述
路由	此選項允許您設定本規則的優先等級。RX3042H 防火牆根據規則的優先順序來決定是否讓封包通過。您可以指定規則列表中一個特定數字，來決定規則的優先順序。選項包括：AUTO、eth1 (WAN1)、eth2 (WAN2)、PPP1 (WAN1-unnumbered)、PPP2 (WAN2-unnumbered)、PPP3 (WAN1-PPPoE1)、PPP4 (WAN1-PPPoE2)、PPP5 (WAN2-PPPoE1)、PPP6 (WAN2-PPPoE2)。若 WAN 連接埠設定為 DMZ 模式，則只有 AUTO、eth1、PPP1/3/4。
1 (最初)	本數字代表最高優先的等級。
其他數字	從下拉式列表中選擇一項規則，並修改其屬性。
日誌	勾選此欄可以開啓 ACL 規則的日誌功能，若要關閉這項功能，請消除欄框中的勾選即可。
動作 (Action)	
允許 (Allow)	點選本按鍵來設定 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。
拒絕 (Deny)	點選本按鍵來設定 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。
路由	· 保持 " 自動 " 設定，除非封包將傳送至特定的介面。 在這裡可以選擇 PPPoE unnumbered 或 PPPoE multi-session 需要的路由方式。可選的項目包括 AUTO、PPP1/2 (PPPoE unnumbered)、PPP1/2/3/4 (PPPoE multi-session)。這些選項皆可以從下拉式選單中選擇。如果選擇 " 自動 "，路由器會根據路由列表中的訊息，來替封包進行路由尋址。
NAT	
無	若您不想在 ACL 規則中使用 NAT，請選擇本項目。
IP 位址	若您想外部傳輸使用來源 IP 位址的話，請指定電腦的 IP 位址。請注意此選項已選擇。
IP 位址	輸入 IP 位址
自動	RX3042H 自動地使用傳輸來源 IP 的 IP 位址。請注意，如果 NAT 用於出埠傳輸的話，請選擇此項。
來源網路	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：
任意 (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 位址	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 位址	指定合適的網路位址
子網路	本項目可讓您包括所有連線到 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 (位址)	輸入合適的 IP 位址。
Mask (遮罩)	輸入對應的子網路遮罩。
MAC 位址	本項目可以讓您為套用本規則者指定 MAC 位址。



欄位	描述
Destination IP 本項目可以讓您設定套用該項規則的目的網路。請使用下拉式選單來選擇下列項目：	
ANY (任意)	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。
服務 從下拉式選單中選擇套用該規則的服務。如果所需的服務沒有列出，請點選 " Edit " 按鈕來建立一個新的服務。	
時間 選擇套用規則的時間點。	
啟用	如果您想要在特定的時間啟動 ACL 規則的話，請選擇此項。並將設定欄位中的勾選消除，消除之後就能在任何時間裡面均採用此項規則。
日期和時間	檢查 ACL 規則所需的時間和日期。

表 9.4 服務的相關參數

欄位	描述
服務名稱 輸入一個服務名稱，以區別新的服務。	
協定 從下拉式功能選單中選擇一種協定，可選擇的有：All、TCP、UDP、ICMP、IGMP、AH、ESP，以及 TCP/IP。	
Source Port 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：	
ANY (任意)	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 (單一)	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
Port 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
ICMP (僅於協定的模式設定為 ICMP 時才可使用) 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：	
<ul style="list-style-type: none"> <li>· Any(預設值)</li> <li>· 0：回音答覆</li> <li>· 1：類型 1</li> <li>· 2：類型 2</li> <li>· 3：資料不能傳達：資料無法傳到目的地</li> <li>· 4：Scr 降低：源頭降低</li> <li>· 5：重新定向</li> </ul>	

欄位	描述
	<ul style="list-style-type: none"> <li>• 6：類型 6</li> <li>• 7：類型 7</li> <li>• 8：回音要求</li> <li>• 9：路由廣播</li> <li>• 10：路由請求</li> <li>• 11：時間超時：時間超過</li> <li>• 12：參數問題</li> <li>• 13：穩定時間請求</li> <li>• 14：穩定時間回應</li> <li>• 15：請求報告：要求訊息報告</li> <li>• 16：回覆報告：報告回應</li> <li>• 17：請求遮罩位址：遮罩位址請求</li> <li>• 18：回應遮罩位址：遮罩位址回應</li> </ul>

## 9.5 設定 ACL 規則 (Firewall -> ACL)

透過如圖 9.4 所示，透過 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

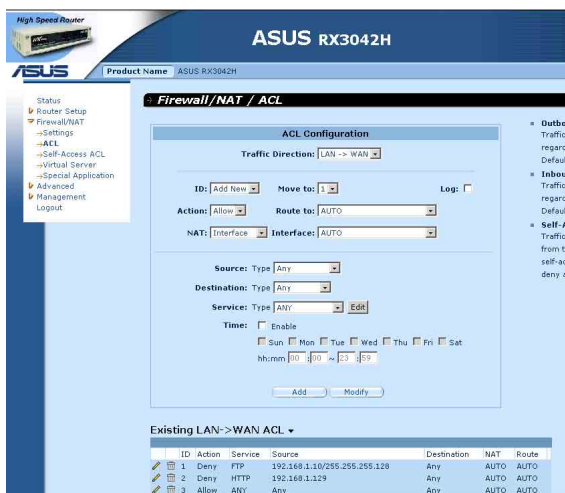


圖 9.4 ACL 規則設定頁面

### 9.5.1 新增 ACL 規則

請依照下面的介紹來新增 ACL 規則：


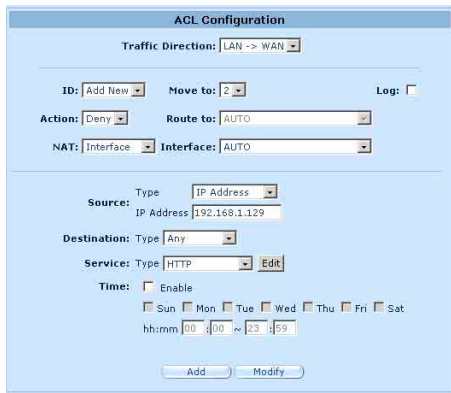
1. 開啟 Firewall 設定頁面，如圖 9.4 所示，雙按 Firewall → ACL 選單。
2. 從 Traffic Direction 下拉式功能表中，選擇一個選項。例如，若您想要建立一個 ACL 來過濾 LAN 到 WAN 的傳輸，請選擇 LAN -> WAN 選項。
3. 從 “ID” 的下拉式選單中選擇 “ADD New”。
4. 在 “Action” 的下拉式選單中，設定您想要設定的動作（Allow/Deny）。
5. 從 “Route to” 的下拉式選單中選擇號碼來為這些規則指定優先順序的介面。若您想要 RX3042H 自動引導傳輸，請選擇 AUTO。
6. 選擇 NAT 類型，並輸入所對應的訊息。
7. 將以下的欄位做變更：來源/目標 IP、來源/目標連接埠、協定、ICMP 訊息類型以及日誌，請參考表 9.3 中，關於這些欄位的詳細說明。
8. 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。
9. 點選  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 9.5 顯示如何建立新的規則來允許 HTTP（如 web server）服務。本規則可讓出埠 HTTP 傳輸導向 IP 位址 192.168.1.129 的主機。



The screenshot shows the "ACL Configuration" window. At the top, "Traffic Direction" is set to "LAN -> WAN". Below that, "ID" is "Add New", "Move to" is "2", and "Log" is unchecked. "Action" is "Deny", "Route to" is "AUTO", and "NAT" is "Interface" with "Interface" set to "AUTO". The "Source" section has "Type" as "IP Address" and "IP Address" as "192.168.1.129". The "Destination" section has "Type" as "Any". The "Service" section has "Type" as "HTTP" and "EdR". The "Time" section has "Enable" checked, and a schedule for "Sun Mon Tue Wed Thu Fri Sat" from "00:00" to "23:59". At the bottom, there are "Add" and "Modify" buttons.

圖 9.5 ACL 設定範例

Existing LAN->WAN ACL ▾							
	ID	Action	Service	Source	Destination	NAT	Route
	1	Deny	FTP	192.168.1.110/255.255.255.128	Any	AUTO	AUTO
	2	Deny	HTTP	192.168.1.129	Any	AUTO	AUTO
	3	Allow	ANY	Any	Any	AUTO	AUTO

圖9.4 ACL 列表範例

## 9.5.2 修改 ACL 規則

請依照以下的步驟，來修改 ACL 規則：

1. 開啓入埠 Firewall/ACL 設定頁面，雙按選擇 ACL 選單。
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。

## 9.5.3 刪除 ACL 規則

如要刪除 ACL 規則，請點選規則前的 圖示。

## 9.5.4 顯示 ACL 規則

如要檢視既有的 ACL 規則，只要開啓 Firewall/ACL → ACL 選單，開啓 ACL 規則設定畫面，然後從 Traffic Direction 下拉式功能表中選擇傳輸的方向。

## 9.6 設定 Self-Access ACL 規則

使用 Self-Access（自我存取）規則來控制對 RX3042H 本身的存取。您可以使用 Self-Access Rule configuration 畫面，如圖 9.7 所示，進行以下的步驟：

- 增加一個 Self-Access 規則
- 修改既有的 Self-Access 規則
- 刪除既有的 Self-Access 規則
- 檢視已設定的 Self-Access 規則

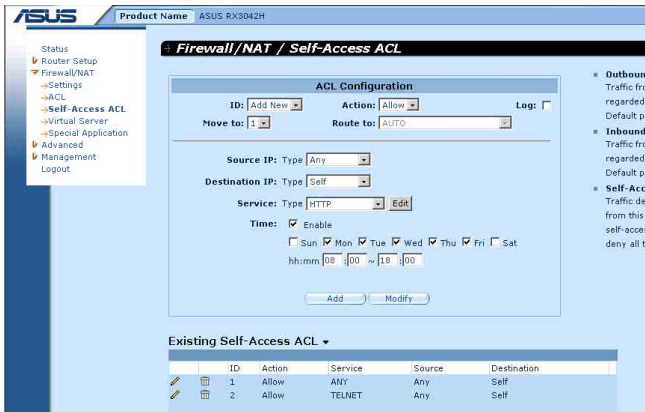


圖9.7 Self-Access ACL 設定頁面

### 9.6.1 新增一個 Self-Access 規則

為了增加一個如欲新增 Self-Access 規則，請依照以下介紹操作：

1. 點選 Firewall/NAT → Self-Access 選項，並進入 Self-Access 規則設定畫面。
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！這些號碼代表修先順序，其中以 1 的優先順序最高。
5. 根據需要來針對下列的欄位進行變更：來源/目的 IP 服務、時間，以及日誌。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 Self-Access ACL 設定頁面中下方的 Self-Access ACL 列表中。

例如：



圖 9.8 顯示了一個允許任何來源到 RX3042H 的 HTTP 傳輸的 Self-Access ACL 配置。



圖9.8 Self-Access 設定範例

## 9.6.2 修改 Self-Access 規則

請按照以下的步驟，來修改一個 Self-Access 規則：



1. 點選 Firewall/NAT → Self-Access 選單，進入 Self-Access ACL 規則設定畫面。
2. 點選規則中的  圖示來修改 Existing Self-Access 表的規則，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、服務、時間，以及日誌。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 Self-Access ACL 設定頁面中下方的 Existing Self-Access ACL 列表中。

## 9.6.3 刪除 Self-Access ACL 規則

如要刪除，請點選規則前的  圖示，刪除 Self-Access 規則。

## 9.6.4 顯示 Self-Access ACL 規則

如要檢視既有的 ACL 規則，只要開啓 Firewall/NAT → Self-Access ACL 規則設定頁面所示，開啓 Self-Access ACL 規則設定頁面即可。

Existing Self-Access ACL ▼					
	ID	Action	Service	Source	Destination
	1	Allow	ANY	Any	Self
	2	Allow	TELNET	Any	Self

## 9.7 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。



RX3042H 同一時間只支援一種特定類型的伺服器。



圖 9.9 虛擬伺服器設定畫面

### 9.7.1 虛擬伺服器參數設定

表 9.5 列出虛擬伺服器的參數設定

表 9.5 虛擬伺服器參數設定

設定	描述
ID	
新增數字	點選此項目來新增一個虛擬伺服器。 從下拉式列表選單中，選擇虛擬伺服器的 ID，更改它的設定。
轉移到	
	此選頁允許您設定虛擬伺服器規則檢查的優先等級。NAT 會依據規則的優先等級，來決定是否對 IP 和 (或) 連接埠進行偵測，您可以指定規則列表中之一特定數字，來決定規則的優先等級。
1 (最初)	本數字代表最高的優先等級。
其他數字	選擇要指定給其他規則的優先等級號碼。
目標 IP	
	此選頁可以讓您設定套用該規則的來源網路。請在下拉式列表中選擇下列選項：

設定	描述
任意 IP 位址	如果虛擬伺服器有已知共用的 IP 位址，請輸入此 IP 位址。
介面	使用已選擇的連線介面的 IP 位址作為目標 IP 位址，可選擇的選項有： eth1 (WAN1) eth2 (WAN2) PPP1 (WAN1 unnumbered) PPP2 (WAN2 unnumbered) PPP3 (WAN1 PPPoE1) PPP4 (WAN1 PPPoE2) PPP5 (WAN2 PPPoE1) PPP6 (WAN2 PPPoE2)
Service	從下拉式選單中選擇一個套用此規則的服務。如果沒有所需的服務，請點選 “Edit” 按鈕來建立一個新的服務。
Redirect IP	輸入您希望的目的地電腦 IP 位址（通常是 LAN 中的伺服器）。例如，如果 LAN 中的網頁伺服器的 IP 位址是 192.168.1.28，請輸入 192.168.1.28。
Redirect Service	從下拉式功能選單中，選擇一個套用此規則的服務，如果沒有所需的服務，請點選 “Edit” 按鈕來建立一個新的服務。
Bypass ACL	若您不希望防火牆控制虛擬伺服器的存取權限的話，請選擇此項目。此項用意是虛擬伺服器將允許所有使用者存取提供的服務。若您希望能控制誰可以存取伺服器的話，請不要選擇此項。請建立一個合適的 ACL 規則來控制存取。

表9.6 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 8080-80880
HTTPS	TCP 443-443
I-phone 5.0	TCP/UDP 22555-22555
ISAKMP	UDP 500-500



應用程式	連接埠號碼
mIRC	66011-700
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)
NEWS	TCP 119-119
PC Anywhere	TCP : 5631
PC Anywhere	TCP : 5631, UDP : 5632
POP3	TCP 110-110
Powwow Chat	13233-13233
Red Alert II	1234-1237
SMTP	TCP 25-25
Sudden Strike	2300-2400
TELNET	TCP 23-23
Win VNC	UDP 5800-5800

## 9.7.2 虛擬伺服器設定範例 1 - 網頁伺服器

圖 9.10 描述的網頁伺服器的網路拓撲架構圖，此伺服器使用 8080 埠來提供 HTTP 服務：

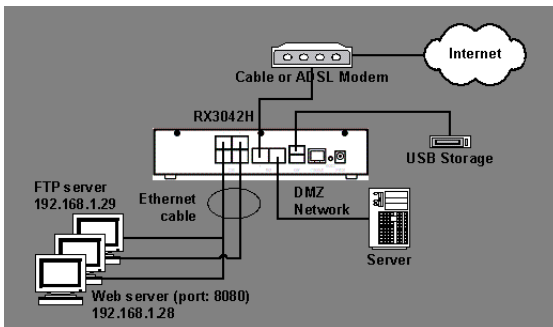


圖 9.10 虛擬伺服器擴拓架構圖

請依照以下敘述步驟來設定 FTP 伺服器：

1. 點選 Firewall/NAT -> Virtual Server 選單，如圖 9.9 所示，進入虛擬伺服器設定畫面。
2. 如圖 9.11 所示，選擇目標 IP 類型及服務類型。

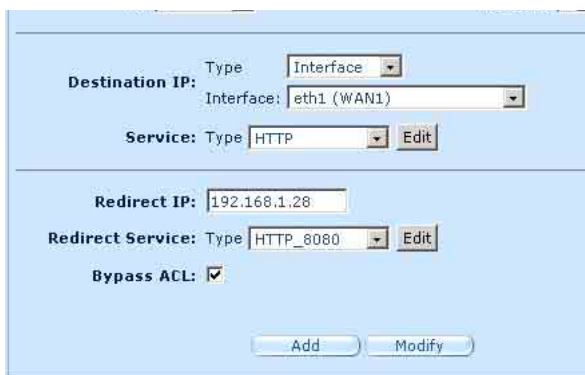


圖 9.11 虛擬伺服器設定範例 1 - 網頁伺服器

3. 把 Redirect IP 框中的 192.168.1.28 作為 IP 位址輸入。
4. 由於網頁伺服器沒有使用標準的 TCP 埠（80 埠），所以必須建立一個新的使用 80 埠的 HTTP 服務。點選 Edit 後，來建立一個新的服務類型。在跳出的服務設定畫面中，如圖 9.12 所示，輸入服務名稱、協定，以及埠的代號，然後點選 **Add**（Add to list）來建立新的服務名稱為 HTTP\_8080，最後點選 Save & Exit 按鈕。

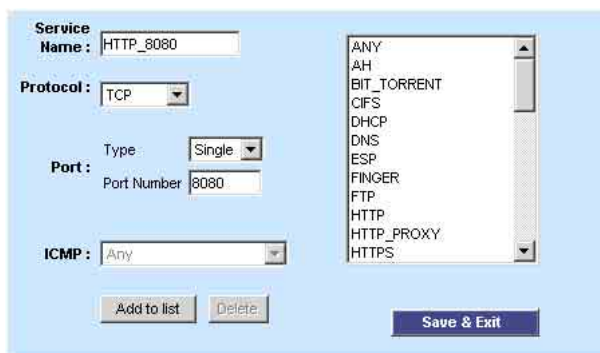


圖9.12 增加一個新的服務

5. 為重新選擇下拉式功能表，選擇 HTTP\_8080。
6. 點選 **Apply** 鍵來儲存設定值。

### 9.7.3 虛擬伺服器設定範例 2 - FTP 伺服器

圖 9.10 描述的網頁伺服器的網路拓撲架構圖，FTP 伺服器使用標準的 FTP 埠來提供 FTP 服務。

請按照以下的步驟，如圖 9.12 所示，來設定 FTP 伺服器。

1. 點選 Firewall/NAT -> Virtual Server 選單，如圖 9.9 所示，進入虛擬伺服器設定畫面。
2. 如圖 9.13 所示，輸入所需的訊息。
3. 點選  來儲存這些設定。

The screenshot shows the 'Virtual Server Configuration' window. At the top, there are two dropdown menus: 'ID:' with the value '1' and 'Move to:' with the value '1'. Below this is a horizontal line. Underneath, there are two rows of configuration options. The first row is for 'Destination IP:', with a 'Type:' dropdown set to 'Interface' and an 'Interface:' dropdown set to 'eth1 (WAN1)'. The second row is for 'Service:', with a 'Type:' dropdown set to 'FTP' and an 'Edit' button. Another horizontal line follows. The third row is for 'Redirect IP:', with a text input field containing '192.168.1.29'. The fourth row is for 'Redirect Service:', with a 'Type:' dropdown set to 'AUTO' and an 'Edit' button. The fifth row is for 'Bypass ACL:', with a checked checkbox. At the bottom of the window, there are two buttons: 'Add' and 'Modify'.

圖9.13 虛擬伺服器設定範例 2 - FTP 伺服器

### 9.7.4 虛擬伺服器設定範例 3 - 具備存取控制功能的 FTP 伺服器

本範例與前面第 9.7.3 一節中所述的” 虛擬伺服器範例 2-FTP 伺服器” 類似，不過本範例還另外具備了由防火牆 ACL 規則提供的存取控制功能。在本範例中，我們將 FTP 的存取範圍限制在 168.192.1.0 的網路區段中。

請按照以下的步驟，來設定這類的 FTP 伺服器。

1. 建立一個 FTP 虛擬伺服器。
  - a) 點選點選 Firewall/NAT -> Virtual Server 選單，如圖 9.9 所示，進入虛擬伺服器設定畫面。
  - b) 如圖 9.13 所示，輸入所需的訊息。
  - c) 確認 Bypass ACL 欄中的勾選為” 未勾選” 的狀態。
  - d) 點選  來儲存這些設定。

Virtual Server Configuration

ID: Add New Move to: 1

Destination IP: Type Interface Interface: eth1 (WAN1)

Service: Type FTP Edit

Redirect IP: 192.168.1.29

Redirect Service: Type AUTO Edit

Bypass ACL:

Add Modify

圖9.14 虛擬伺服器範例 3 - FTP 伺服器

2. 建立一條控制 FTP 伺服器存取範圍的 ACL 規則。
  - a) 點選點選 Firewall/NAT -> Virtual Server 選單，如圖 9.4 所示，進入虛擬伺服器設定畫面。
  - b) 從 Traffic Direction 下拉式選單中選擇 WAN - LAN。
  - c) 從 ID 下拉式選單中選擇 Add New。
  - d) 從 Action 下拉式選單中選擇 Allow。
  - e) 從 Source Type 下拉式選單中選擇 Subnet。
  - f) 在 Source Address 和 Mask 欄中分別輸入 168.1921.28.0 和 255.255.255.0。
  - g) 從 Service Type 下拉式選單中選擇 FTP。
  - h) 在 Move to 下拉式選單中選擇數字來設定規則的優先等級。請注意數字 1 表示最高的優先等級，防火牆會先搜尋比較高的優先等級。
  - i) 點選  來儲存新建立的 ACL 規則。

The screenshot shows the 'ACL Configuration' window. At the top, 'Traffic Direction' is set to 'WAN -> LAN'. Below that, 'ID' is 'Add New', 'Move to' is '1', and 'Log' is unchecked. The 'Action' is set to 'Allow'. The 'Type' is 'Subnet'. The 'Source' is 'Address: 168.192.128.0' and 'Mask: 255.255.255.0'. The 'Destination' is 'Type: Any'. The 'Service' is 'Type: FTP' with an 'Edit' button. The 'Time' section has 'Enable' unchecked, and checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, Sat. The time is set to 'hh:mm 00:00 ~ 23:59'. At the bottom are 'Add' and 'Modify' buttons.

圖9.15 ACL 防火牆虛擬伺服器範例 3 - FTP 伺服器

## 9.8 特別應用程式設定

一些特別的應用程式使用多個 TCP/UDP 埠來傳輸資料，由於 NAT 的緣故，這些程式不能工作，但是透過進行特別應用程式的設定，即能正常運作。



**請注意：**一部電腦一次只能使用一個特別應用程式。

表 9.7 列出了特別應用參數的設定

表 9.7 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。
Tigger Protocol	從下拉式選單中選擇協定類型，可選擇的項目有：TCP、UDP，以及 TCP/UDP。
Outgoing (Trigger) Port Range	當應用程式傳送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 9.8。
Incoming Protocol	對應入埠封包所使用的協定。可選擇的選項有：TCP、UDP，以及 TCP/UDP。

設定	描述
Incoming Port	相應的入埠封包使用的埠範圍，請參考表 9.8 中主要應用程式的連接埠號列表。請注意，連接埠範圍是由一對數字中間加 “—” 所組成，例如 100—200。多個連接埠範圍由逗號所分隔，如 100—200、700—800。
Note	您可以在此輸入關於應用程式的敘述，比如用於區分的應用程式名稱。

表 9.8 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
Yahoo Messenger	5050	5000-5101

## 9.8.2 特別應用程式範例

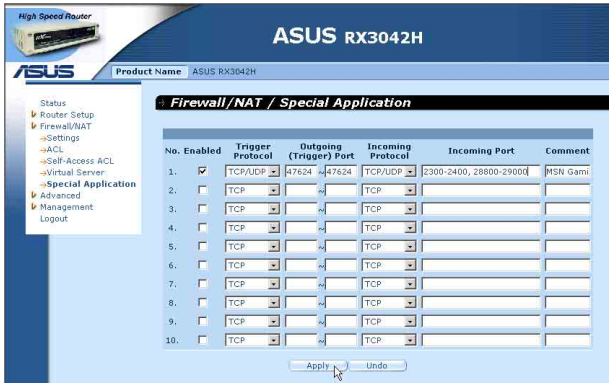


圖 9.16 特別應用程式設定畫面

請依照下列敘述步驟步驟來設定 Quick Time 特定應用程式。

1. 點選 Firewall/NAT -> Special Application 選單，如圖 9.16 所示，進入特別應用程式設定畫面。
2. 點選 Enabled。
3. 從 Trigger Protocol 選單中選擇 TCP/UDP，若您不能確認應用程式是採用 TCP 或 UDP 協定，您可以選擇 TCP/UDP。
4. 輸入 Outgoing (Trigger) 連接埠的範圍，如：47624 - 47624。
5. 從 Outgoing (Trigger) 下拉式列表中選擇 TCP/UDP，若您不能確認應用程式是採用 TCP 或 UDP 協定，您可以選擇 TCP/UDP。
6. 輸入 Incoming Port 連接埠的範圍，如：2300 - 2400 和 28800 - 29000。
7. 在 Comment 欄中，輸入名字 MSN Gaming Zone 以區分程式。
8. 點選  鍵來儲存設定值。





## 第十章 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：

- 設定系統服務
- 修改密碼
- 查看系統訊息
- 修改系統日期與時間
- 設定 SNMP
- 還原系統至出廠預設值
- 備份/還原系統設定
- 重新啓動系統
- 韌體更新

### 10.1 設定系統服務

如圖 10.1 所示，您可以透過系統服務設定，來開啓或關閉 RX3042H 支援的服務。除了 DDNS、SNTP、UPnP，以及 RIP，所有服務都在出廠前已被開啓，請依照以下的步驟來進行：

1. 點選 Management -> System Service 選單，進入系統設定畫面。
2. 點選相對應的 Enable 或 Disable 按鈕來開啓或關閉相對應的服務。
3. 點選  來儲存設定。

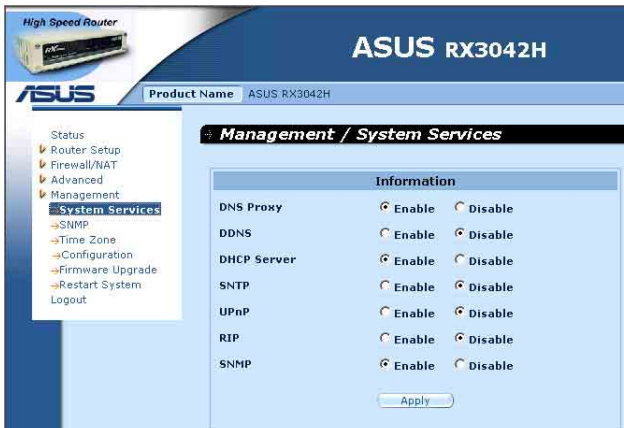


圖 10.1 系統服務設定畫面

## 10.2 登入密碼與系統設定

### 10.2.1 更改密碼

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）。基於安全的緣故，建議您應該更換密碼，以避免其他人更改路由的設定。



**注意：**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10.2 系統管理設定畫面

請依照下列步驟來變更您的密碼：

1. 點選 Router Setup -> Administration 選單，如圖 10.2 所示，開啓系統管理設定畫面。
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. 點選  鍵來儲存設定值。

## 10.2.2 設定系統參數

請依照以下的步驟，來進行變更系統參數設定：

1. 點選 Router Setup -> Administration 選單，如圖 10.2 所示，開啟系統管理設定畫面。
2. 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。
3. 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。
4. 允許 Ping 介面：您可以透過網路（LAN）或廣域網路（WAN），來讓 RX3042H 允許使用 Ping 的方式檢查。建議您僅在網路（LAN）下才開啓這個功能。
5. 點選  鍵來儲存設定值。

## 10.3 檢視系統資訊

當您登錄 RX3042H，系統資訊頁面會顯示自您登入以來的相關資訊，而這些資訊包含整體的系統設定值。



圖 10.3 系統狀態畫面

## 10.4 設定日期與時間

RX3042H 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 RX3042H 中並沒有真實時鐘，RX3042H 是依靠外部時間伺服器來保持正確的時間。RX3042H 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 SNTP 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 RX3042H 上的日期與時間並不會影響您的 PC 上的時間。



圖 10.4 日期與時間設定畫面

請依照下列步驟來維持路由器中準確的時間：

1. 點選 Management -> Zone 選單，來開啓日期與時間設定畫面。
2. 輸入現在的時間和日期。
3. 從下拉式選單中選擇您所在地的時區（Time Zone）。
4. 點選  鍵來儲存設定值。

可按照以下的步驟將真正時間與外部時間伺服器設定同步化：

1. 點選 Management -> Zone 選單，來開啓日期與時間設定畫面。
2. 從下拉式選單中選擇您所在地的時區（Time Zone）。
3. 勾選 “Enable” 選項來啓動 SNTP 服務。
4. 請為 SNTP 伺服器輸入 IP 位址，以作為未來更新系統時間之用。
5. 點選  鍵來儲存設定值。

### 10.4.1 檢視系統日期與時間

爲了檢視更新後的系統日期與時間，請您先登入設定管理員，並點選 Management -> Zone 選單。

## 10.5 SNMP 設定

SNMP (Simple Network Management Protocol, 簡易網路管理協定) 是用來協助網路管理，您可以透過 SNMP 設定畫面來開啓或關閉 SNMP 功能。

### 10.5.1 SNMP 的設定參數

表 10.1 列舉了 SNMP 的相關設定參數。

表 10.1 SNMP 相關的設定參數


設定	描述
SNMP Enable	選擇此項後可以開啓 SNMP 功能，否則為關閉。
RO Community Name	Community string 是一串明顯的字串，用在 SNMP 管理站與 Internet Security Router (網路安全路由器) 之間的密碼。“僅提供讀取” (Read Only, RO) community name 是讓 SNMP 管理站用來接收 Internet Security Router 的設定。
RW Community Name	Community string 是一串明顯的字串，用在 SNMP 管理站與 Internet Security Router (網路安全路由器) 之間的密碼。“提供讀取與寫入” (Read and Write, RW) community name 是讓 SNMP 管理站用來讀取和分配 Internet Security Router 的設定。
Trap Address	Trap message (陷阱訊息) 是 Internet Security Router 傳送給 SNMP 管理站，並告訴它路由器上所發生的狀況。在此欄中輸入 SNMP 管理站的 IP 位址，則可用來接收從 Internet Security Router 發送來的陷阱訊息。

### 10.5.2 設定 SNMP

1. 點選 Management -> SNMP 選單，如圖 10.5 所示，進入 SNMP 設定畫面。



圖 10.5 SNMP 設定畫面

2. 點選 **SNMP Enable**。來開啓 SNMP 功能，反之亦然。
3. 輸入 RO（僅供讀取），以及 RW（可讀可寫入）
4. 輸入用來接收 RX3042H 傳送來的 trap 訊息的 SNMP 管理站的 IP 位址。
5. 點選  鍵來儲存設定值。

## 10.6 設定日誌

日誌的訊息資料是存放在動態記憶體中，當系統重新開啓後則會消失。如果要保存日誌記錄的訊息內容，您就需要進行安裝一個日誌伺服器（syslog server），讓 RX3042H 傳送日誌訊息給伺服器來記錄。

### 10.6.1 使用 Syslog Server 設定遠端日誌



圖 10.6 Syslog Server 設定畫面

1. 如圖 10.6 所示，點選 Management -> Log 選單，來開啓日誌的設定畫面。
2. 點選 Enable Remote Log 欄來啓用遠端日誌功能。
3. 在 Syslog Server IP Address 欄中輸入 syslog server 的 IP 位址。
4. 點選  鍵來儲存設定值。

## 10.6.2 查看系統日誌

您可以點選 Firewall/NAT -> Log 選單，來開啓防火牆日誌畫面。圖 10.7 顯示一個日誌的範本，您可以點選畫面下方的 Reload 按鈕來查看更新的日誌訊息，若要刪除日誌訊息，只需要點選 Clear Log 按鈕。

```

May 19 19:47:21 kernel: fw: SELF rule=1 allow udp from 172.21.150.29 to 172.21.151.255 sport=138 dport=138
May 19 19:47:25 kernel: fw: SELF rule=1 allow icmp from 192.168.1.1 to 192.168.1.11 type=8 code=0 id=155
May 19 19:47:29 kernel: fw: SELF rule=1 allow udp from 172.21.151.15 to 172.21.151.255 sport=5003 dport=5003
May 19 19:47:31 kernel: fw: SELF rule=1 allow udp from 172.21.150.12 to 172.21.151.255 sport=138 dport=138
May 19 19:47:31 kernel: fw: SELF rule=1 allow udp from 172.21.151.15 to 172.21.151.255 sport=138 dport=138
May 19 19:47:32 kernel: fw: SELF rule=1 allow udp from 172.21.150.35 to 172.21.151.255 sport=138 dport=138
May 19 19:47:40 kernel: fw: SELF rule=1 allow udp from 172.21.150.22 to 172.21.151.255 sport=138 dport=138
May 19 19:47:43 kernel: fw: SELF rule=1 allow udp from 172.21.150.26 to 172.21.151.255 sport=138 dport=138
May 19 19:47:43 kernel: fw: SELF rule=1 allow udp from 172.21.150.8 to 172.21.151.255 sport=138 dport=138
May 19 19:47:44 kernel: fw: SELF rule=1 allow udp from 172.21.150.10 to 172.21.151.255 sport=138 dport=138
May 19 19:47:44 kernel: fw: SELF rule=1 allow udp from 172.21.150.34 to 172.21.151.255 sport=138 dport=138
May 19 19:47:54 kernel: fw: SELF rule=1 allow udp from 172.21.151.9 to 172.21.151.255 sport=138 dport=138
May 19 19:47:54 kernel: fw: SELF rule=1 allow udp from 172.21.151.36 to 172.21.151.255 sport=138 dport=138
May 19 19:47:56 kernel: fw: SELF rule=1 allow udp from 172.21.150.28 to 172.21.151.255 sport=138 dport=138

```

圖 10.7 日誌範例

## 10.7 系統設定管理

### 10.7.1 將系統設定參數還原至出廠值

有時候會遇到爲了解決因不正確的設定而引起的問題，而想將系統設定的參數還原到出廠預設值，當需要做這樣動作時，請按照以下的步驟來進行：

1. 如圖 10.8 所示，點選 Management -> Configuration -> Factory Default 選單，來進入出廠預設值設定畫面。

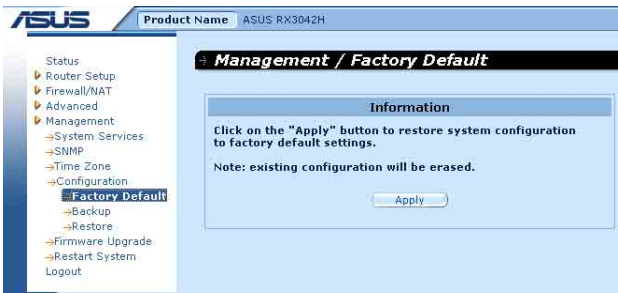


圖 10.8 出廠預設值設定畫面

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 10.9 所示的請求確認。點選  鍵以繼續，或點選  鍵來取消此動作。



圖 10.9 出廠預設值重置確認視窗

4. RX3042H 接下來會重新啓動來回復出廠預設值。請注意！如圖 10.10 所示的計時視窗將會出現，以標示系統重置完成尚須的時間。



圖 10.10 出廠預設值重置計時秒數



有時候您可能發現無法存取 RX3042H，如 您忘記您的密碼或是 RX3042H 的 IP 位址 > 解決這類狀況的唯一方法就是藉由按下 RX3042H 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 RX3042H 後，系統設定便會回復到出廠預設值。

---



## 10.7.2 備份系統設定

請依照以下的步驟，來進行備份系統設定：


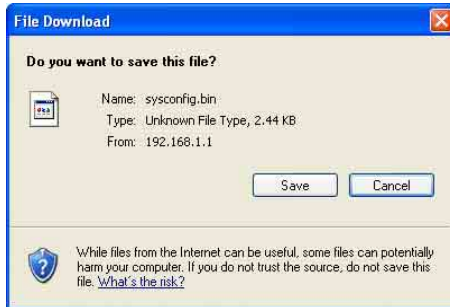
1. 點選 Management -> Configuration -> Backup 選單，來進入系統備份設定畫面。
2. 點選  按鈕來備份系統設定。

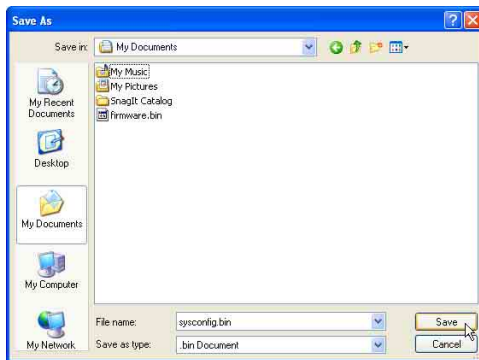


圖 10.11 備份系統設定畫面

3. 點選  鍵來備份系統設定。



4. 點選  鍵來進行備份的系統檔案建立。



### 10.7.3 回復系統設定

請依照下列步驟進行回復系統的設定：

1. 點選 Management -> Configuration -> Restore 選單，開啓系統回復設定畫面。



圖 10.12 回復備份系統設定畫面

2. 在 Configuration File 欄中輸入您想要回復的系統設定檔案的路徑、名字；或者是您也可以點選 Browse... 按鈕來尋找檔案，接著會跳出如圖 10.13 的視窗讓您選擇所要回復的設定檔案。

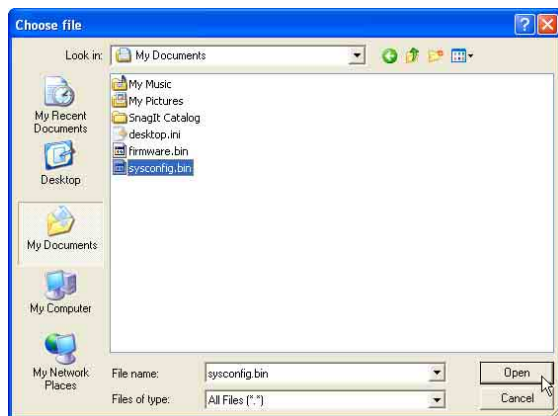


圖 10.13 從檔案總管中選擇系統設定檔案

3. 按下 **Apply** 按鍵來回復備份系統設定。然後會跳出一個訊息，如下圖所示的交談框，詢問您是否回復系統設定。點選 **OK** 繼續，若不要繼續則點選 **Cancel** 中斷此次的動作。請注意，這時記得重新啓動 RX3042H 讓新的設定啓用。



圖 10.14 系統設定回復畫面

4. 如圖 10.15 所示，網頁瀏覽器這時將會重新開啓 RX3042H 的倒數計時秒數畫面。當秒數倒數至零秒時，將會重新開啓 RX3042H，若沒有自動連線的話，您也可以採用手動來進行連線。

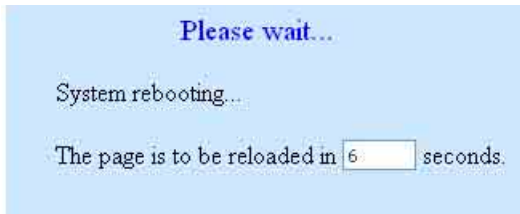


圖 10.15 重新啓動系統更新倒數計時視窗

## 10.8 更新韌體

ASUSTeK 會不斷地提供您可使用在 RX3042H 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 System → Firmware Upgrade 選單，如圖 10.16 所示，開啓更新韌體頁面。



圖 10.16 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  鍵來開啓檔案總管搜尋在您電腦中的韌體映象檔。

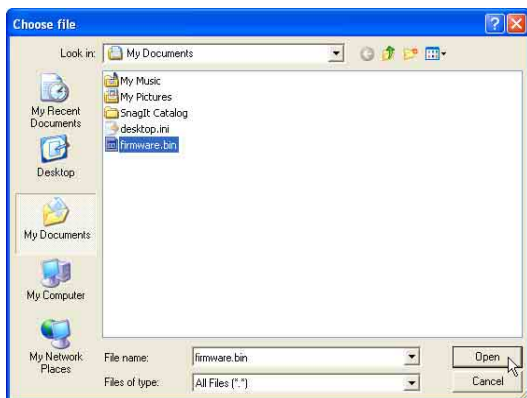


圖10.17 檔案總管選擇畫面

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 10.18 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 10.19 韌體更新狀態視窗

5. 在韌體更新完成後，如圖 10.20 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 RX3042H。而若是 RX3042H 沒有自動重新連線，請以手動方式設定您的電腦與 RX3042H 間的連線。

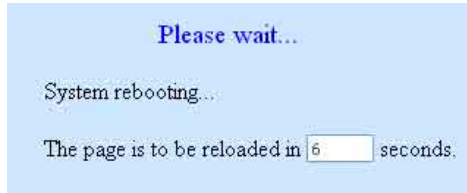


圖 10.20 韌體更新倒數計時視窗

6. 當您重新連線到 RX3042H，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：
  - a) 點選瀏覽器的“工具”選項。
  - b) 接著點選“網際網路選項”。
  - c) 點選“刪除檔案”按鈕來清除瀏覽器快取。

## 10.9 重新啓動系統

1. 點選 Management -> Restart System 選單，如圖 10.21 所示，開啓重新啓動系統頁面。
2. 點選  鍵來重新啓動系統。

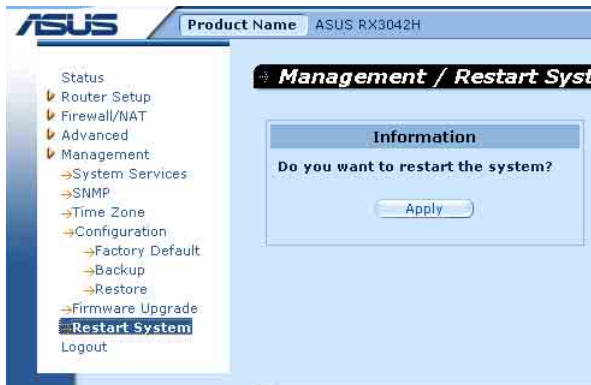


圖 10.21 重新啓動系統頁面

## 10.10 登出設定管理頁面

如果您要登出設定的管理畫面，請先點選 **Logout** 選項，然後再點選 **Apply** 按鈕來退出此畫面，如圖 10.22 所示。若您使用的是 **IE** 瀏覽器，請注意會跳出如圖 10.23 所示的視窗，詢問您是否確認要關閉瀏覽器，按 **Yes** 按鈕之後就可關閉。

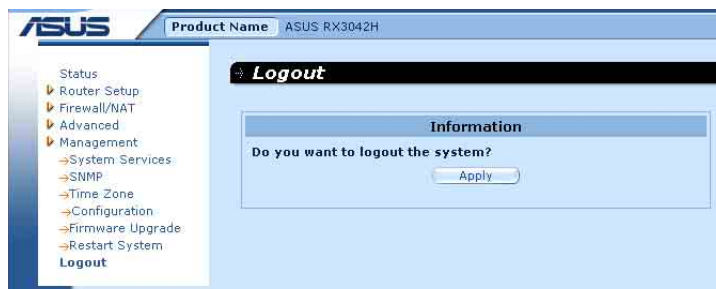


圖 10.22 登出設定的管理畫面



圖 10.23 確認關閉 IE 瀏覽器

# 第十一章 IP 位址、網路遮罩，與子網路

## 11.1 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。

在本章節中，我們假設您已經掌握了一些基本知識，如二進位數字、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。請參考附錄 11。

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——”。

### 11.1.1 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 的長度取決于網路的種類（參考以下的章節）。

表 11.1 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

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)

## 11.2 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 (field 1) 輕易決定的等級：

- 欄位 1 (field 1) = 1-126：A 級
- 欄位 1 (field 1) = 128-191：B 級
- 欄位 1 (field 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。

## 11.3 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。當此一出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。




## 第十二章 移難排解

本附錄將列出您在安裝或使用 RX3042H 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 RX3042H，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 數據機的乙太網路連接埠，而另一端則緊密地接到 RX3042H 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 RX3042H 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 RX3042H。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 RX3042H 的區域網路 IP 位址 (預設值：192.168.1.1)。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 RX3042H 中的網路位址轉譯規則已正確設定，以便正確轉譯由您內部私人 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)	
您忘記/ 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 RX3042H 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 RX3042H 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。


## 12.1 使用 IP 公用程式診斷問題

### 12.1.1 封包探測 (Ping)

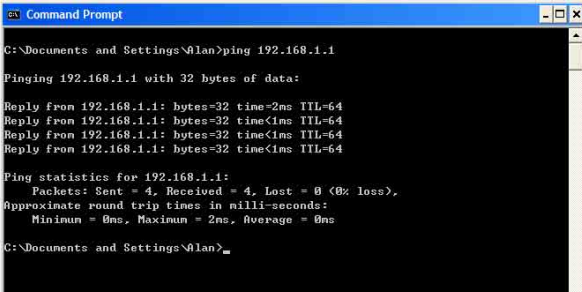
封包探測 (Ping) 是您可以用來檢查您的 PC 是否可以辨識區域網路或網際網路中電腦的一項指令。封包探測指令會傳送訊息至您所指定的電腦主機，若該電腦接收到訊息，便會傳回一回覆訊息。若要使用這項指令，您必需知道您試圖連線之電腦的 IP 位址。

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：

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 12.1 使用封包探測公用程式

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RX3042H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。

您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。

### 12.1.2 nslookup

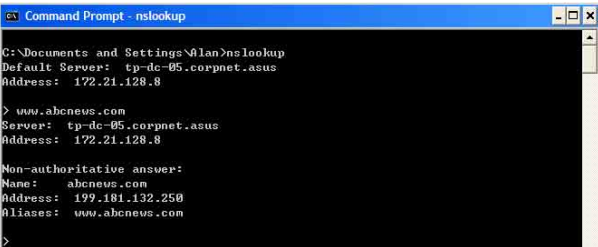
您可以使用nslookup指令來決定與網際網路網站名稱相對應關連的IP位址。您可指定一般名稱，接著nslookup指令會到您的DNS伺服器中搜尋該名稱（通常會儲存於您的ISP伺服器中）。若該登錄無法在您ISP的DNS伺服器中找到，則該要求會被轉送到更高等級的伺服器，以此類推，直到該登錄被搜尋到為止。搜尋到之後，伺服器接著會回覆該登錄的對應IP位址。

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12.2所顯示相關連的IP位址。



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

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

Non-authoritative answer:
Name: abcnews.com
Address: 199.181.132.250
Aliases: www.abcnews.com
>
```

圖 12.2 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。

