



**Vigor 3300 系列**  
**Broadband VoIP/Security/Load Balance 路由器**  
**使用手冊**

版本: 1.0

日期: 2005/12/15

## 關於本手冊

本手冊旨在協助用戶使用 Vigor 3300 系列路由器。本手冊包含的資訊可以根據需要進行改動，恕不另行通知。如果有任何疑問，請隨時透過 E-mail，傳真，電話等聯繫方式與我們的支援部門聯繫。想瞭解最新的產品資訊和功能，請參觀我們的網站 [www.draytek.com.tw](http://www.draytek.com.tw)。

## 版權資訊

版權所有© 2005 本手冊的內容受到版權保護，未經版權所有人的允許，本手冊內容的一部分或是全部皆不得重製、轉送、儲存、或轉譯為任何語言。

## 商標

DrayTek 是居易科技公司商標，Vigor 系列產品為居易科技登記的註冊商標，本手冊中所提及之其他產品商標分別為各所有公司所擁有。

## 目標讀者

本手冊提供支援予 Vigor 3300 安裝和使用人員。

## 居易科技保修聲明

對於任何由於工藝和產品缺陷造成的故障，我們對購買者提供三年免費保修，保修時間自用戶購買路由器之日起。請妥善保管發票，發票將作為購買日期證明。

在保修期內，如果我們認定產品故障為設計或工藝缺陷所造成，我們將免費維修或更換產品或部件。一旦產品被自行改動，錯誤使用，外力損壞或者在錯誤的工作環境下使用，將不再享受免費保修服務。

本保修協定所針對物件不包括那些銷售商所附帶的軟體，不影響產品功能的損壞也不在保修條款之列。我們保留隨時修改手冊和線上文字檔案而不進行任何形式的通知權利。

## 成為註冊用戶

請存取 [www.draytek.com.tw](http://www.draytek.com.tw) 進行線上註冊，也可以填寫註冊卡並寄送到卡背面印刷的地址，我們會不定期向註冊用戶發送產品資訊的更新。

## 警告

更換並使用錯誤的電池有爆炸危險，請根據當地的環境條例處理廢舊電池。

## 安全須知

### 安全須知

#### 使用環境

- 確保路由器的交流電源電壓範圍在 90-240V 之間，路由器應該在溫度 0 到 50 °C 以及相關濕度 10%到 90%之間的環境中使用。
- 請不要將路由器直接暴露在日光或其他熱源下，電子器件有可能被直射日光或熱源破壞。

#### 安裝

- 在開啓電源之前，請閱讀安裝手冊。
- 請將路由器電源連接至帶有安全保護的插線板。
- 路由器最好安置在空氣流通較好的地方。
- 請勿在危險的工作環境下進行工作。
- 請確保電源接地，並儘量避免路由器在潮濕的環境中工作。
- 當安裝或移除底盤，更換保險絲時，請關閉路由器電源。
- 請不要將路由器放置在潮濕的環境中，例如浴室一樣的環境。
- 請勿在閃電時進行線路連接。
- 如果您要將路由器移除，請遵守當地的環境保護相關條例進行操作。

#### 維護

用戶可以在必要時更換保險絲。其他元件必須由指定的維修機構進行修理。請勿自行打開和修理設備。

保險絲必須是：250VAC，1A

## 歐洲地區(EC)宣告

居易公司宣告 Vigor3300 系列路由器完全符合 R&TTE Directive 99/5/EC 中的基本要求及相關的規定，Vigor3300 系列的 ISDN 介面主要是針對遍及歐洲地區的 ISDN 網路而設計

## 客戶支援

請在聯繫客戶支援人員之前準備好以下資訊。

- 產品型號和序列號
- 保修訊息
- 收到產品的時間
- 產品配置
- 軟體版本
- 問題簡單描述
- 您試圖解決問題的步驟以及相關的 Syslog 日誌資訊

客戶支援和銷售代表的聯繫資訊分別為 [support@draytek.com.tw](mailto:support@draytek.com.tw) 和 [sales@draytek.com.tw](mailto:sales@draytek.com.tw)。

本頁留白

# 目錄

<b>第 1 章</b> .....	<b>9</b>
<b>序言和安裝</b> .....	<b>9</b>
1.1 序言.....	9
1.2 硬體連接和 LED 狀態.....	10
1.3 硬體安裝.....	13
<b>第 2 章</b> .....	<b>17</b>
<b>管理員密碼設置</b> .....	<b>17</b>
2.1 序言.....	17
2.2 修改管理員密碼.....	18
<b>第 3 章</b> .....	<b>21</b>
<b>快速設置</b> .....	<b>21</b>
3.1 序言.....	21
3.2 WAN 設定.....	21
3.3 LAN 介面設置 .....	26
<b>第 4 章</b> .....	<b>31</b>
<b>系統設置</b> .....	<b>31</b>
4.1 Status(狀態) .....	31
4.2 Time(時間設定) .....	34
4.3 Syslog (紀錄設定).....	36
4.4 Access Control(連線控制設定) .....	37
4.5 Reboot(重新啓動設定) .....	38
4.6 Firmware Upgrade(軟體升級設定).....	39
4.7 Diagnostic Tools(診斷工具).....	41
4.8 Configuration(設定).....	44
<b>第 5 章</b> .....	<b>47</b>
<b>網路設置</b> .....	<b>47</b>
5.1 WAN 和網際網路連線設定 .....	47
5.2 LAN 設定 .....	53
5.3 Load Balance Policy(負載平衡策略設定).....	57

5.4 High Availability(高可用性設定).....	59
<b>第 6 章</b> .....	<b>63</b>
<b>高級設置</b> .....	<b>63</b>
6.1 Static Route(靜態路由設定).....	63
6.2 NAT 設定.....	64
6.3 Port Block(埠阻擋設定).....	70
6.4 UPnP 設置.....	72
6.5 DDNS 設定.....	74
6.6 RADIUS 設置.....	77
6.7 Call Schedule(撥號計畫時間表設定).....	78
<b>第 7 章</b> .....	<b>83</b>
<b>防火牆設置</b> .....	<b>83</b>
7.1 序言.....	83
7.2 防火牆設定概述.....	84
7.3 IP Filter (IP 過濾設定).....	85
7.4 DoS(拒絕服務攻擊設定).....	89
7.5 URL(過濾設定).....	92
<b>第 8 章</b> .....	<b>101</b>
<b>QoS 設置</b> .....	<b>101</b>
8.1 序言.....	101
8.2 Imcoming/Outgoing Class Setup(傳入/傳出分類設置).....	101
8.3 Incoming/Outgoing Class Filter (傳入/傳出分類過濾設置).....	102
<b>第 9 章</b> .....	<b>107</b>
<b>VPN(虛擬專用網路)與遠程連線設置</b> .....	<b>107</b>
9.1 序言.....	107
9.2 IPSec 設定.....	108
9.3 PPTP 設定.....	118
<b>第 10 章</b> .....	<b>121</b>
<b>VoIP 設置</b> .....	<b>121</b>
10.1 序言.....	121
10.2 VoIP 協議設置.....	122

10.3 Port Settings(電話號碼設定) .....	124
10.4 Speed Dial(快速撥號設置) .....	128
10.5 Advanced Speed Dial(進階快速撥號設置).....	128
10.6 Miscellaneous(其他設定).....	130
10.7 Tone Settings(語音設定).....	130
10.8 QoS 設定 .....	131
10.9 NAT Traversal (NAT 穿越設置) .....	132
10.10 Incoming Call Barring(來電撥入限制).....	133
10.11 Status(連接狀態) .....	135
10.12 Call History(呼叫歷史記錄) .....	136

本頁留白

---

# 第 1 章

## 序言和安裝

---

### 1.1 序言

Vigor3300 整合了豐富的功能，包括 NAT、防火牆、VPN、內容過濾、頻寬管理、安全的無線通訊和 VoIP 功能，給您的公司在商業上的成功提供保障。Vigor3300 系列的各種應用場景可參照圖 1-1。

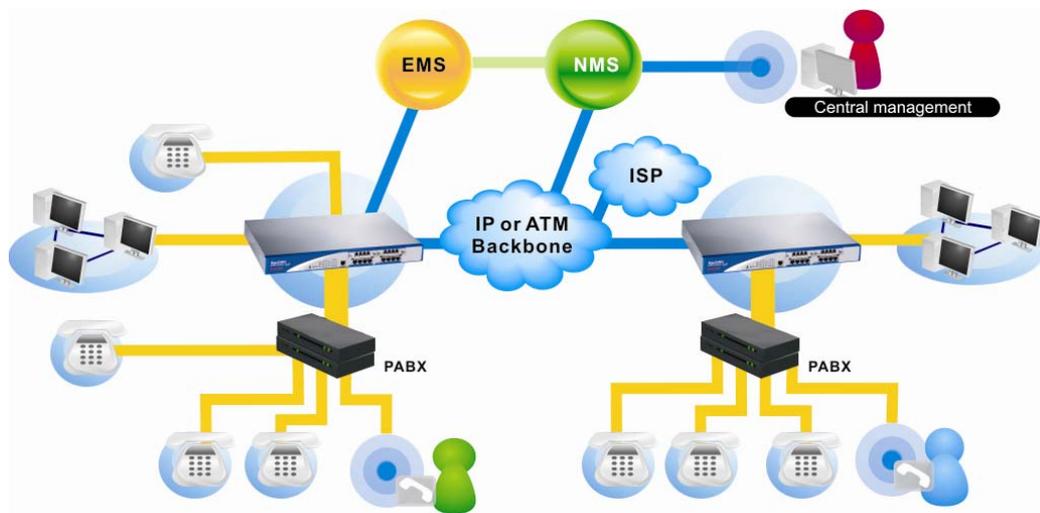


圖 1-1 Vigor3300 系列的應用

首先，虛擬專用網路(VPN)是一個私有網路的擴展，它包括來自共用或公眾網路，比如 Internet 上的連接。VPN 連接可允許透過共用 Internet 網路的 2 台電腦之間發送資料，來仿效點對點私有連接的一些特性。

DrayTek Vigor3300 系列路由器的 VPN 支援 Internet 工業標準，提供給客戶一個開放且可互操作的 VPN 解決方案，比如 Internet 協議安全(IPSec)和點對點隧道協議(PPTP)等。Vigor3300 系列最多可支援 128 個通道。

Internet 語音，通常被稱為 Voice over Internet Protocol (VoIP)，它是透過寬頻 Internet 連接的方式打電話，從而替代使用常規的電話線路的一種技術。有些 VoIP 服務只允許和使用相同服務的人通話，但是另外一些服務允許撥打任何有電話號碼的人，無論這個號碼是本地、長途、移動或國際號碼。同樣的，一些服務只能在您電腦或特定的 VoIP 電話上運作，而另外一些服務允許您透過一塊介面卡來使用傳統的電話機。

因為 Internet 語音是數位的，VoIP 服務的優點在於它可以提供一些新功能和服務，這些功能和服務在傳統電話上是沒有的。如果有一條寬頻連接 Internet，您甚至不需要支付額外的費用打電話。

您可以無限時地和世界上的任何人通話（條件是另外一個人也連接 Internet）。您也可以

在同一時間和許多人說話而無需額外的費用。

最重要的一點是 Vigor3300 系列整合了含有 QoS 的 VoIP 功能。即時應用比如語音應用，有別於傳統的應用，它有著不同的特性和需求。因為它們是基於即時的功能，當傳輸語音封包發生延遲的時候，語音應用只能容忍很小的語音變化。語音資料流程同樣不能忍受封包丟失和抖動，它們會降低傳輸到接受端用戶的語音品質。在 IP 上傳輸語音最有效的方式是這個裝置需要有低延時且可靠的封包傳送能力。Vigor3300 系列提供了一種方法來實施優先順序服務，這項服務滿足了對語音封包傳遞的迫切需要。

接下來的內文將會著重描述 Vigor3300 的安裝和配置。

## 1.2 硬體連接和 LED 狀態

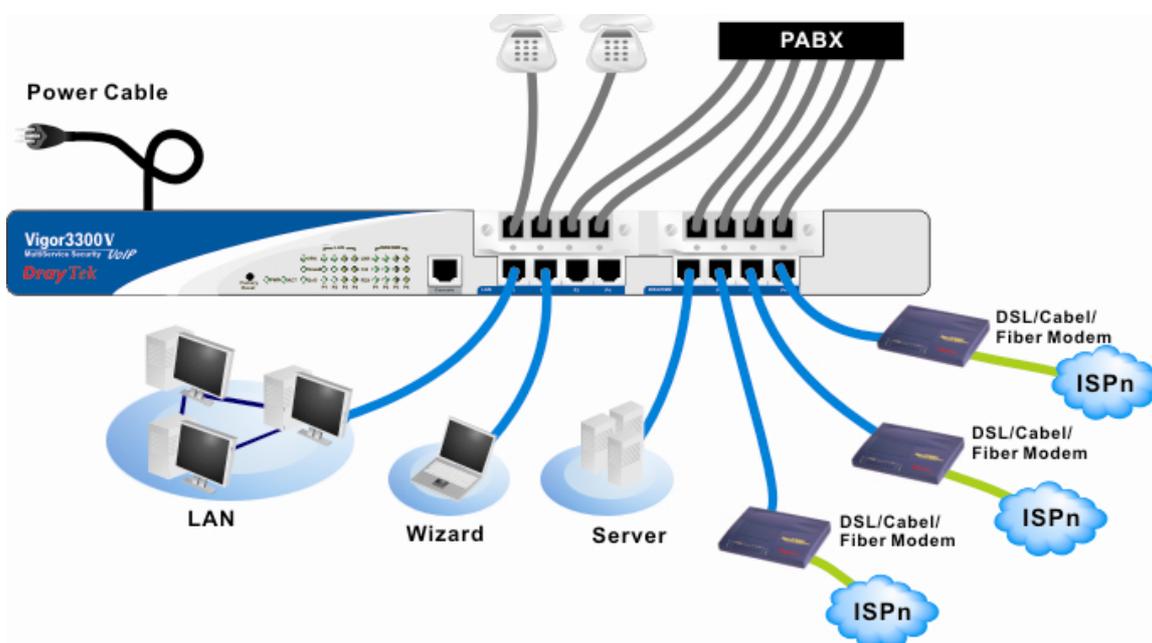


圖 1-2 Vigor3300 系列網路連接

Vigor 3300V 最多可支援 4 個 WAN 介面。用戶可以選擇使用 DMZ 以應用到任何一個 WAN 介面上。對於其他 WAN 介面，用戶可以連接這些連接埠到自己的 ISP 上，Vigor3300 系列支援在這些 WAN 介面上的負載平衡，這個優勢是使資料流程能穿過每一個 WAN 介面，從而使系統能到達最大的性能。

此外，Vigor3300V 同時在 WAN 介面支援備份功能，用戶可以選擇一個處於非活動狀態的 WAN 介面作為從介面，目的是當主介面在連接出現問題時，可利用此從介面來代替主介面。

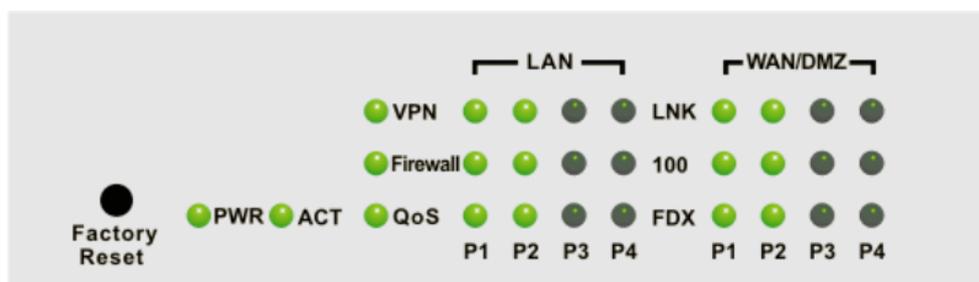
表 1-1 Vigor3300 連接

連接埠	類型，顏色	連接到...	備註
電源線	黑色	交流電源插座	90-264VAC

連接埠	類型，顏色	連接到...	備註
端端 (Console)	RS232， 灰色	PC RS232 連接埠 進行測試	--
乙太網路(LAN)	RJ-45， 藍色	交換機或集線器	--
乙太網路(DMZ)	RJ-45， 藍色	伺服器	
乙太網路(WAN1)	RJ-45， 藍色	DSL/Cable/Fiber Modem	--
乙太網路(WAN2)	RJ-45， 藍色	DSL/Cable/Fiber Modem	
乙太網路(WAN3)	RJ-45， 藍色	DSL/Cable/Fiber Modem	--
乙太網路(WAN4)	RJ-45， 藍色	DSL/Cable/Fiber Modem	

用戶可以透過幾個步驟來完成連接。首先，連接 Vigor3300 背面的電源線到電源插座，連好後 PWR LED 燈會亮。然後，當系統自我測試完成後，ACT 燈號會開始閃爍。接著將您的電腦以藍色 RJ-45 纜線連接到 Vigor3300 的任何一個 LAN 連接埠上，此時 LAN 的 LED 燈會閃爍。此外 Vigor3300 提供了 ISDN、VPN、Firewall、QoS 和 4 個 WAN 連接埠的 LED 指示燈，所有 LED 指示燈顯示在圖 1-3，這些燈號的功能將於表 1-2 中說明。

面板 LED 與連接器：



For Vigor3300/3300V



For Vigor3300B+

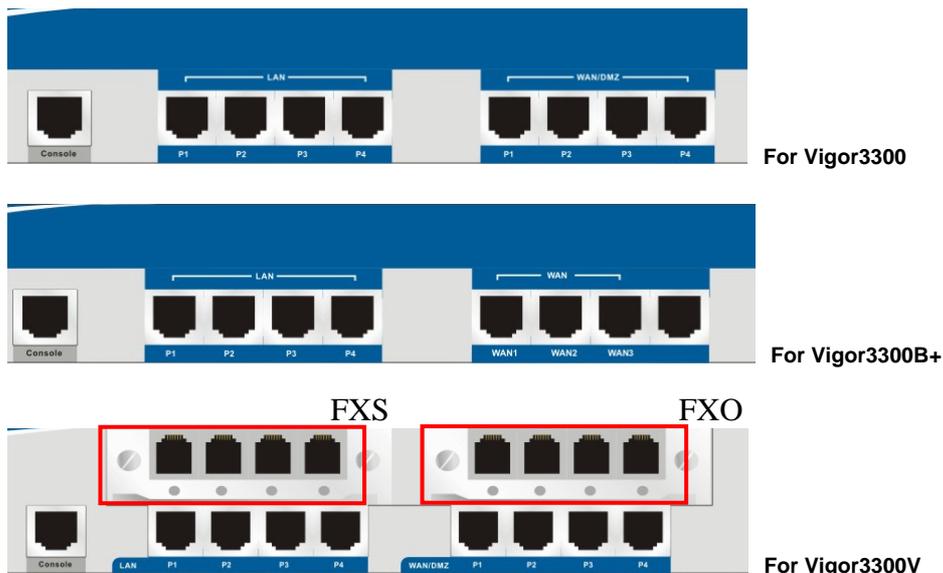


圖 1-3 Vigor3300 指示燈與面版圖

表 1-2 Vigor3300 前面板 LED 以及說明

LED	指示燈色	說明	備註	
PWR	綠色	電源開啓	90-264VAC	
	關閉	電源關閉		
ACT	綠色	閃動表示路由器處於工作狀態	--	
	關閉	當系統關閉時		
WAN/ DMZ	LNK	綠色	乙太網連接已建立	Px: P1 , P2 , P3 , P4
		關閉	無連接	
	100M	綠色	乙太網速度連接速度為 100M	
		關閉	乙太網速度連接速度為 10M	
	FDX	綠色	乙太網傳輸模式為全雙工	
		關閉	乙太網傳輸模式為半雙工	
LAN	LNK	綠色	Px 乙太網連接已經建立	Px: P1、P2、P3、P4
		關閉	Px 無乙太網連接	
	100M	綠色	Px 乙太網速度為 100M	
		關閉	Px 乙太網速度為 10M	
	FDX	綠色	Px 乙太網埠傳輸模式為全雙工	
		關閉	乙太網傳輸模式為半雙工	
VPN	綠色	VPN 功能正在使用	V3300B 無此模	

	關閉	VPN 功能未使用	組
Firewall	綠色	正在使用防火牆功能	
	關閉	防火牆功能未開啓	
QoS	綠色	QoS 正在使用	V3300B 無此模 組
	關閉	QoS 功能未使用	

## 1.3 硬體安裝

從圖 1.4 中，我們可以看到 Vigor3300 系列有很多介面。在 Vigor3300 系列裡，每一款型號，都支援一套不同的介面。Vigor3300V 支援 4 個區域網路端、4 個廣域網路介面以及一到兩個可擴展的 VoIP 通道(每個通道皆具有 4 個連接埠)。

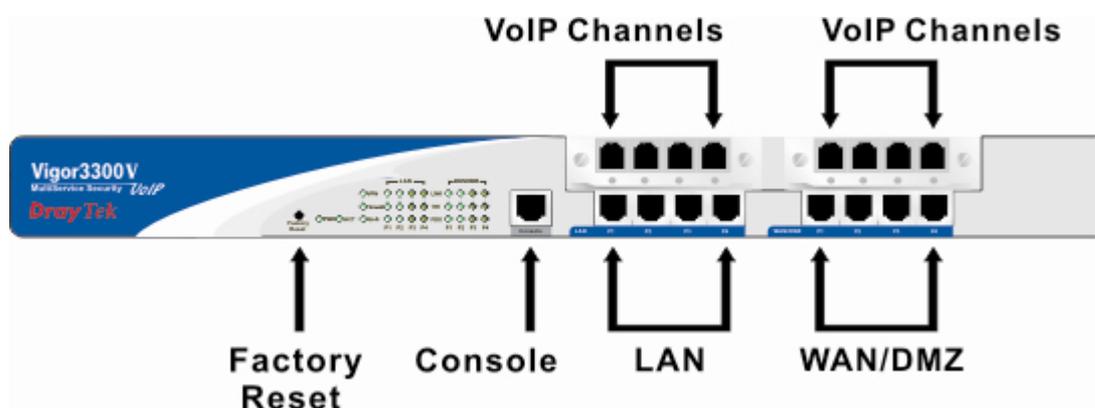


圖 1-4 硬體安裝

### 1.3.1 連接器和介面描述

#### RS232 連接器

RJ45 連接頭允許進行基礎系統配置和控制功能。在初始化安裝階段，此連接器乃是用來初始化 Vigor3300。圖 1-5 顯示 RJ45 的介面可藉由纜線轉換成 RS232 介面，RJ45 連接頭連接到 Vigor3300 上的控制台介面，同時 RS232 DB9 連接到電腦上的連接埠端。控制台介面的預設設置是“每秒位數 57600，無奇偶，資料位元 8，停止位元 1。”

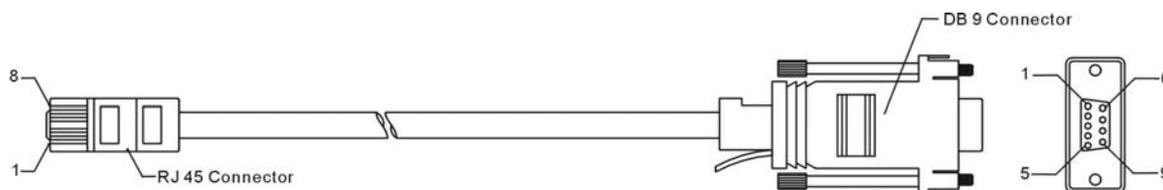


圖 1-5 控制台管理連接線

此連接器輸出針腳列表如下。

表 1-3 RS232 連接器針腳定義

RJ45	DB9	Signal
X	1	CD
3	2	TD
6	3	RD
7	4	DTR
5	5	GND
2	6	DSR
8	7	RTS
1	8	CTS
X	9	RI

### 標準的 10/100 Base-T 乙太網路介面連接器

RJ45 連接頭提供基本的 10/100 Base-T 乙太網路介面，此介面支援 MDI/MDIX 自動檢測兩邊是否直接連線或者使用交叉 RJ45 纜線。這些纜線用於廣域網路、區域網路和 DMZ 介面。

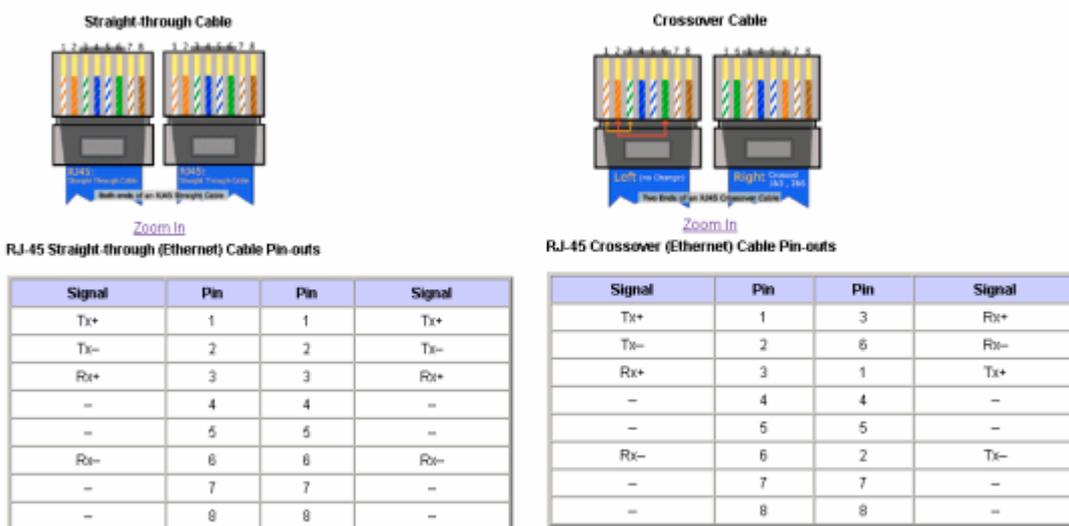


圖 1-6 相容直通線或交叉線

### 1.3.2 底盤連接

#### 底盤上架

Vigor3300 可以安裝到 19 或 23 英寸的支架上。在 19 英寸的支架上使用標準的托架，在 23 英寸支架上用大的托架。19、23 英寸支架上用的托架如圖 1-7 所示。

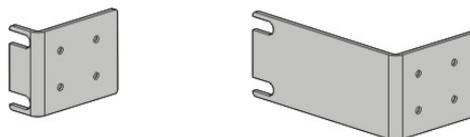


圖 1-7 19 和 23 英寸支架的托架

圖 1-8、1-9 顯示出將托架裝上底盤為 19、23 英寸的支架上。另一面的支架安裝過程同樣可參考此圖。

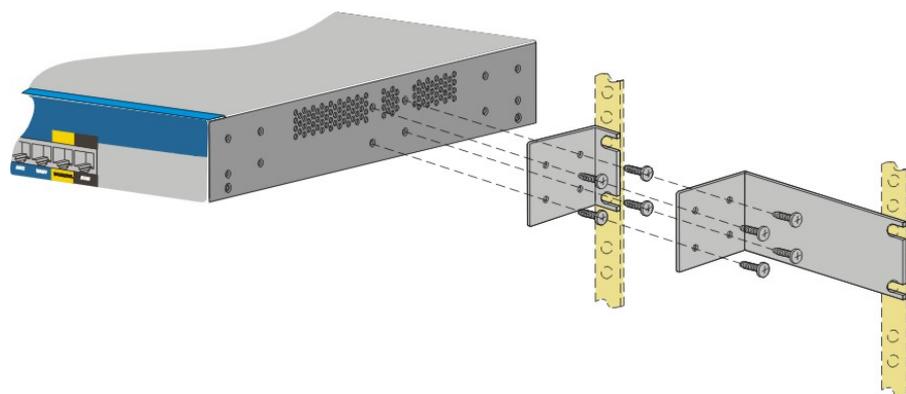


圖 1-8 19、23 英寸支架的托架安裝

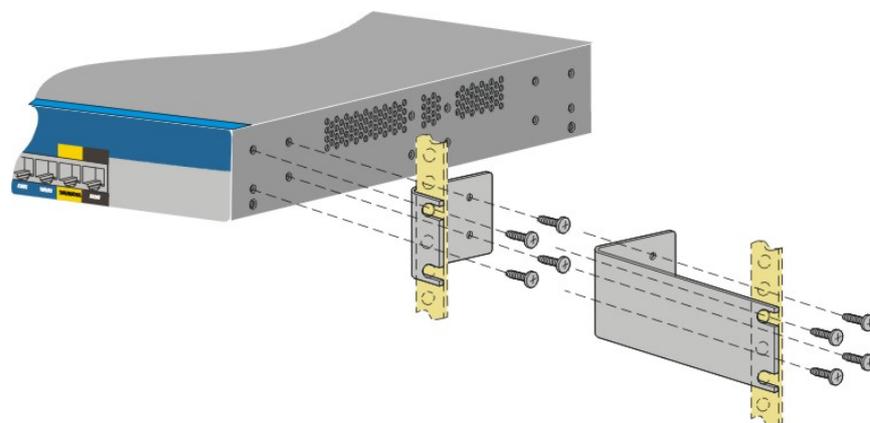


圖 1-9 19、23 英寸支架的托架安裝

該如何將底盤安裝到支架上呢？在托架安裝好以後，Vigor3300 底盤可以用 2 個螺絲一邊一個安裝到支架上去。

### 桌面型安裝

在 Vigor3300 包中有橡皮腳支援桌面安裝。這些橡皮腳目的是為了增加空氣迴旋和減少不必要的桌面摩擦。

交流電插頭和接地連接在後面板上，參閱圖 1-10。

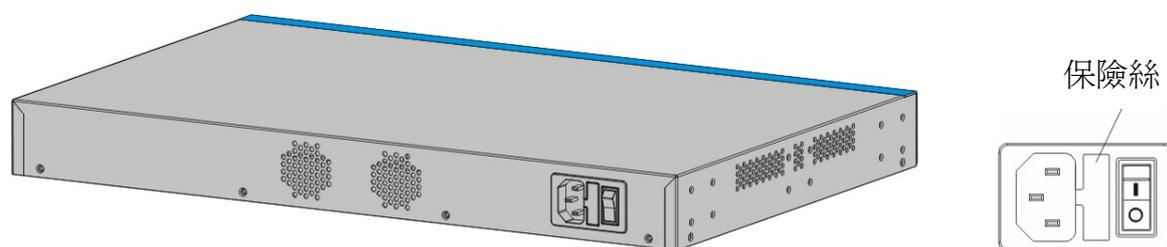


圖 1-10 後面板和交流電源輸入

本頁留白

# 第 2 章

## 管理員密碼設置

### 2.1 序言

Vigor3300 系列可以透過 WEB 方式進行配置和管理，而不需使用額外的軟體工具。本章，我們將介紹如何設置管理員密碼。在 **System** 組中，按 **Change Password** 選項，就可以修改管理員密碼。

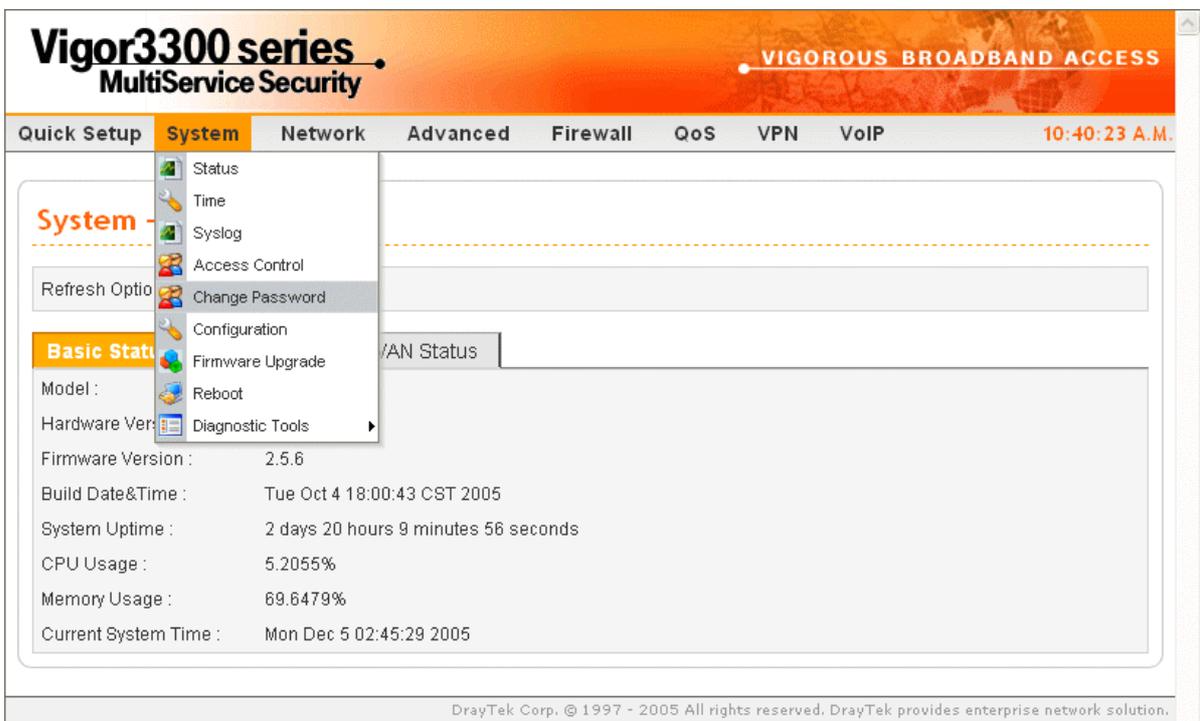


圖 2-1 系統

選擇 **Change Password** 選項，將顯示如下頁面：

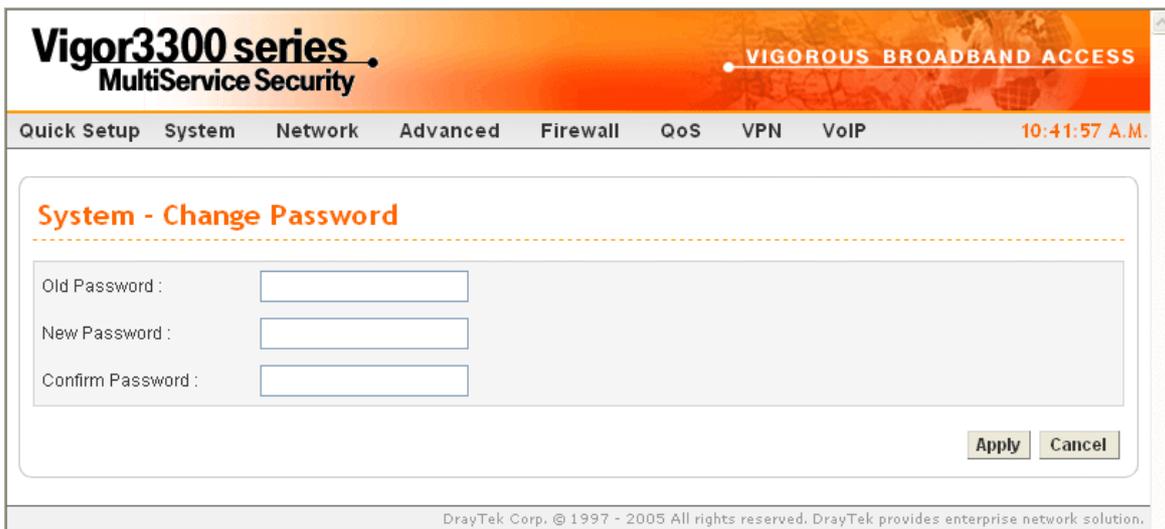


圖 2-2 System 組下的管理員密碼

## 2.2 修改管理員密碼

鑒於安全考慮，我們強烈推薦您為路由器設置密碼，Vigor3300 系列的預設用戶名為“draytek”，密碼為“1234”。您可利用 **System→Change Password** 的方式修改預設密碼。

按 **Change Password**，將顯示如下頁面：

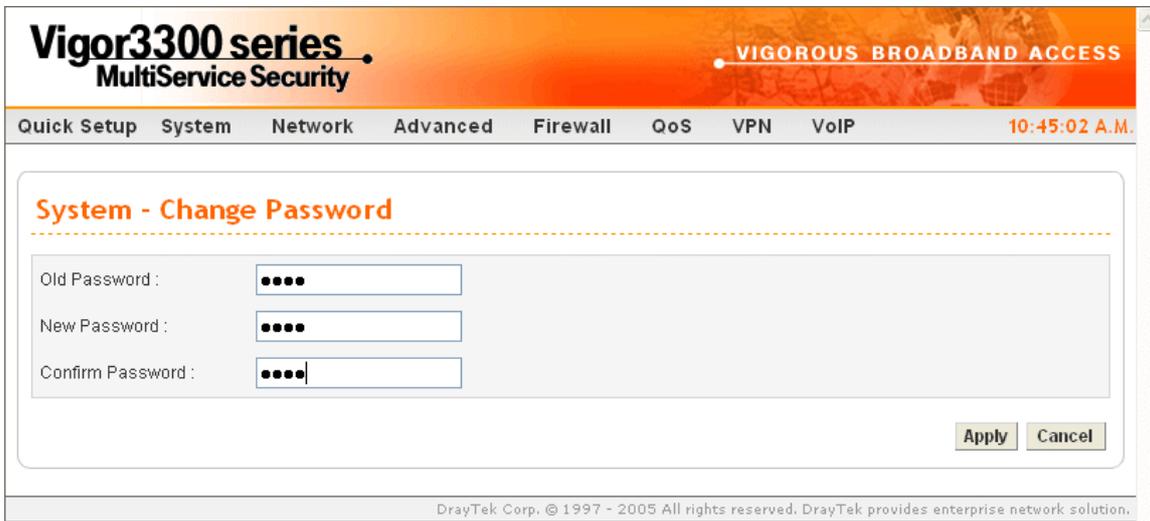


圖 2-3 管理員密碼設置

Old Password (舊密碼)	輸入目前管理員密碼。如果這是第一次設置密碼，請輸入預設值“1234”。
New Password (新密碼)	輸入一個新的管理員密碼。
Confirm Password(確認密碼)	再次輸入新密碼以確認。

請按 **Apply (應用)** 將這些設置應用到 Vigor3300 設備。在您按 **Apply** 後，登錄介面將會彈出，您必須使用新密碼再次進入系統配置。



圖 2-4 登錄介面

本頁留白

# 第 3 章

## 快速設置

### 3.1 序言

本章將詳細介紹快速設置。快速設置可以簡單地對 Vigor3300 基本使用環境進行設置。它包含 WAN 和 LAN 介面設置兩個部分。如果您的 Vigor3300 用於高速 NAT 環境，這些設置將使您的安裝和配置更為快速。

### 3.2 WAN 設定

在快速設置中，您可以配置多種 Internet 連線方式（如：靜態、DHCP、PPPoE 或 PPTP）。對多數用戶來說，Internet 連線是主要的應用，本路由器支援乙太 Internet 連線。接下來的部分，將詳細介紹幾種不同的寬頻連線配置。

本小節介紹第一個 WAN 介面（WAN1）的全部設置。

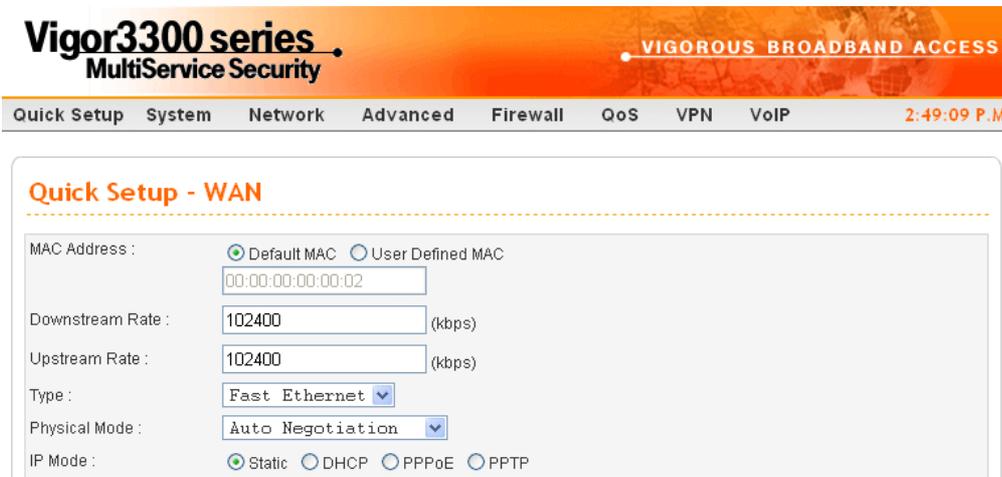


圖 3-1 快速設置

MAC 地址	
Default MAC (路由器預設)	使用出廠設置的路由器預設 MAC 位址。
User Defined MAC (用戶定義)	使用用戶自定義的 MAC 位址。
Downstream Rate (下傳速率)	為此 WAN 介面分配下傳資料的速率。路由器預設值為 102400 kbps (100 兆)。此一設定對 Vigor3300 下傳資料 Cache 調節很重要。如果您使用下傳速率為

	2Mbps 的 DSL 服務，那麼下傳速率設置是 2Mbps。
Upstream Rate (上傳速率)	為此 WAN 介面分配上傳資料的速率。預設值為 102400 kbps (100 兆)。這一設置對 Vigor3300 上傳資料 Cache 調節和權重 (Weighting) 設置來說，同上一設定一樣重要。如果您使用的是上傳速率為 2Mbps 的 DSL 服務，那麼上傳速率設置是 2Mbps。
Type(類型)	選擇此 WAN 介面的連接類型。
Physical Mode (實體模式)	選擇此 WAN 介面的連接速度模式。有 <b>Auto Negotiation</b> 、 <b>Full Duplex</b> 、 <b>Half Duplex</b> 和 10M 或 100M 速度供選擇。 
IP Mode (IP 模式)	為 WAN 介面選擇一種產生 IP 組資訊的模式。有四種 Internet 連線模式，分別為： <b>Static</b> 、 <b>DHCP</b> 、 <b>PPPoE</b> 和 <b>PPTP</b> 。在此頁面中您可以配置 WAN 介面為： <b>Static</b> (固定 IP 位址)、 <b>DHCP</b> (動態 IP 位址)、 <b>PPPoE</b> 或 <b>PPTP</b> 。多數 cable 使用者將使用 DHCP 模式從 cable 前端系統獲得一個公用 IP 位址。

### 3.2.1 靜態設置

您可以為 WAN 介面手動設置一個 IP 位址並透過重新啓動來使設置生效。

圖 3-2 靜態設置

IP Address (IP 地址)	為 WAN 介面分配一個本地 IP 位址。
Subnet Mask (子網路遮罩)	為 WAN 介面指定一個子網路遮罩值。
Default Gateway (預設閘道)	設置閘道的本地 IP 位址。
Primary DNS (首選 DNS)	設置首選 DNS 的本地 IP 位址。
Secondary DNS (備用 DNS)	設置備用 DNS 的本地 IP 位址。
IP Alias List (IP 別名列表)	為此介面設定其他可用的 IP 位址。

完成 WAN 介面設置後，用戶可按 **Next>>** (下一步>>) 進入 LAN 介面設置。

### 3.2.2 DHCP 用戶端設置

此功能可從 Internet 上的 DHCP 伺服器自動獲得一個 IP 位址。將 WAN 介面設置為一個 DHCP 用戶端後，它將從 DHCP 伺服器或 DSL modem 取得一個 IP 位址。

用戶選擇此模式後可以不用進行其他設定。

**Quick Setup - WAN**

MAC Address :  Default MAC  User Defined MAC

Downstream Rate :  (kbps)

Upstream Rate :  (kbps)

Type :

Physical Mode :

IP Mode :  Static  DHCP  PPPoE  PPTP

**Static/DHCP Configuration** | PPPoE/PPTP Configuration

IP Address :  Host Name :

Subnet Mask :  Domain Name :

Default Gateway :  (Host Name and Domain Name are required for some ISPs.)

Primary DNS :

Secondary DNS :

**IP Alias List**

1.	<input type="text"/>	2.	<input type="text"/>
3.	<input type="text"/>	4.	<input type="text"/>
5.	<input type="text"/>	6.	<input type="text"/>
7.	<input type="text"/>	8.	<input type="text"/>

**Next >>**

圖 3-3 DHCP 配置

完成 WAN 介面設置後，用戶可按 **Next>>** (下一步>>) 進入 LAN 介面設置。

### 3.2.3 DSL Modem PPPoE 設置

多數 DSL modem 用戶會用到此設置，所有本地用戶可共用一個 PPPoE 連接來存取 Internet。

下圖僅為範例，您的 DSL 服務供應商會提供特定的設定資料。按 PPPoE 進入如下頁面：

**Quick Setup - WAN**

MAC Address :  Default MAC  User Defined MAC

Downstream Rate :  (kbps)

Upstream Rate :  (kbps)

Type :  ▾

Physical Mode :  ▾

IP Mode :  Static  DHCP  PPPoE  PPTP

Static/DHCP Configuration | **PPPoE/PPTP Configuration**

User Name :

Password :

Authentication :  ▾

Service Name :

PPTP Local Address :

PPTP Subnet Mask :

PPTP Remote Address :

**Next >>**

圖 3-4 PPPoE 配置

<b>User Name</b> (用戶名稱)	鍵入本地 ISP (Internet 服務供應商) 提供的有效用戶名。
<b>Password</b> (密碼)	鍵入由本地 ISP 提供的有效密碼。
<b>Authentication</b> (認證)	選擇 <b>PAP</b> 或 <b>CHAP</b> 協議以獲得最佳相容性。預設值為 <b>PAP</b> 。

完成 WAN 介面設定後，用戶可按 **Next>>** (下一步>>) 進入 LAN 介面設置。

### 3.2.4 DSL Modem PPTP 設置

此模式可讓用戶從 ISP (Internet 服務供應商，具備 PPTP 服務的 DSL modem) 取得 IP 分組資訊。下圖僅為範例，您的 DSL 服務供應商會提供特定的設定資料。

**Quick Setup - WAN**

MAC Address :  Default MAC  User Defined MAC

Downstream Rate :  (kbps)

Upstream Rate :  (kbps)

Type :  ▼

Physical Mode :  ▼

IP Mode :  Static  DHCP  PPPoE  PPTP

Static/DHCP Configuration | **PPPoE/PPTP Configuration**

User Name :

Password :

Authentication :  ▼

Service Name :

PPTP Local Address :

PPTP Subnet Mask :

PPTP Remote Address :

**Next >>**

圖 3-5 PPTP 配置

PPTP Local Address (PPTP 本地地址)	為 PPTP 指定一個本地 IP 位址。
PPTP Subnet Mask (PPTP 遮罩)	為 PPTP 的 IP 位址指定相應的網路遮罩。
PPTP Remote Address (PPTP 遠程地址)	指定 PPTP 伺服器的遠端 IP 地址。

完成 WAN 介面設置後，用戶可按 **Next>>** (下一步>>) 進入 LAN 介面設置。

### 3.3 LAN 介面設置

在 Vigor3300 系列的快速設置 LAN 介面設置介面中，為本地用戶或 NAT 用戶提供了 IP 地址/子網路遮罩設置。若要應用至其他公用網域上的用戶，您需要向您的本地 ISP (Internet 服務供應商) 申請到可路由的子網路。其他本地 PC 必須將路由器的 IP 位址設置為預設閘道，當連接至 ISP 的 DSL 連線建立時，本地 PC 將直接路由到 Internet。同時您也可以使用這一 IP 位址/子網路遮罩來連接到其他本地用戶 (PC)。

LAN 介面設置有以下三種應用供您設置。

- IP 配置
- 第一子網 DHCP 伺服器
- 第二子網 DHCP 伺服器

### 3.3.1 IP 配置

**Network - LAN**

**IP Configuration** | 1st DHCP Server | 2nd DHCP Server

**For NAT Usage**

1st IP Address :

1st Subnet Mask :

**For IP Routing Usage**

Enable  Disable

2nd IP Address :

2nd Subnet Mask :

WAN Interface :

圖 3-6 LAN 介面設置

在 Vigor3300 系列路由器中，LAN 介面設置介面提供了以下幾個 IP 位址設置。IP 地址/子網路遮罩是提供給本地用戶或 NAT 用戶的。若要允許公網用戶，您需要向您的 ISP（Internet 服務供應商）申請一個可路由的子網路。其他本地 PC 的預設閘道 IP 位址應該設為 Vigor3300 的 IP 地址。當到 ISP 的 DSL 連接建立後，所有本地 PC 將直接路由到 Internet。同時，您可以使用這一 IP 位址/子網路遮罩來連接到其他本地用戶（PC）。在此設置也面中您將看到 RFC-1918 中定義的本地 IP 地址。通常我們為路由器選擇使用 192.168.1.0/24 子網路。

<b>For NAT Usage</b>	
1 <sup>st</sup> IP Address (第一子網 IP 位址)	連接到本地網路所使用的本地私有網路 IP 位址，預設值為 192.168.1.1。
1 <sup>st</sup> Subnet Mask (子網路遮罩)	本地網路的網路遮罩，預設值為 255.255.255.0。
<b>For IP Routing Usage</b>	
Enable/Disable (啓用/關閉)	選擇 Enable(啓用)以啓用此功能。 選擇 Disable(關閉)以關閉此功能。
2 <sup>nd</sup> Subnet Mask (第二子網 IP 地址)	可路由介面的 IP 位址。
2 <sup>nd</sup> Subnet Mask (子網路遮罩)	可路由子網的遮罩。
WAN Interface (WAN 介面)	選擇需用之 WAN 連接埠。

按 **Apply(完成)**，將出現重新啓動提示頁面並重新啓動路由器。

### 3.3.2 DHCP 伺服器設定

DHCP 即動態主機配置協定(Dynamic Host Configuration Protocol)，它將自動為所有配置為 DHCP 用戶端的本地用戶分配相應的 IP 設置，請參看下圖進行 DHCP 伺服器設置。

DNS 即功能變數名稱系統(Domain Name System)，所有 Internet 主機必須對應一個唯一的 IP 位址，同時它們需要具備一個容易被人記住的名字，如 www.yahoo.com。DNS 伺服器將名字轉換為對應的 IP 位址。

注意：如果首選 DNS 地址是空的，路由器會將自己的 IP 地址指定為本地用戶的 DNS 代理伺服器，並維護一個 DNS Cache。如果功能變數名稱的 IP 位址已存於 DNSCache，那麼路由器將直接處理功能變數名稱，否則，路由器將透過可用的 WAN 連接(如 DSL/Cable)向上傳遞 DNS 請求傳送至外部 DNS 伺服器。

#### 第一子網 DHCP 伺服器設定

圖 3-7 第一子網 DHCP 伺服器設定

<b>Status(狀態)</b>	選擇 Enable 以啓動此功能；選擇 Disable 以關閉此功能；選擇 Relay Agent 啓動此功能。
<b>Start IP(起始 IP)</b>	設定起始 IP 位址。
<b>End IP(終止 IP)</b>	設定結束 IP 位址。
<b>Primary DNS (首選 DNS)</b>	指定首選 DNS 的 IP 地址。

<b>Secondary DNS</b> (備用 DNS)	指定備用 DNS 的 IP 地址。
<b>Lease Time(租約期期間)</b>	指定上述 IP 地址連線所使用的期間。
<b>WAN Interface</b> (WAN 介面)	指定 WAN 介面。
<b>DHCP Server IP Address</b> (DHCP 伺服器位址)	設定 DHCP 伺服器位址。

按 **Apply(完成)**，將出現重新啓動提示頁面並重新啓動路由器。

### 第二子網 DHCP 伺服器設置定

Vigor3300 系列路由器支援備用 DHCP 伺服器功能。

**Network - LAN**

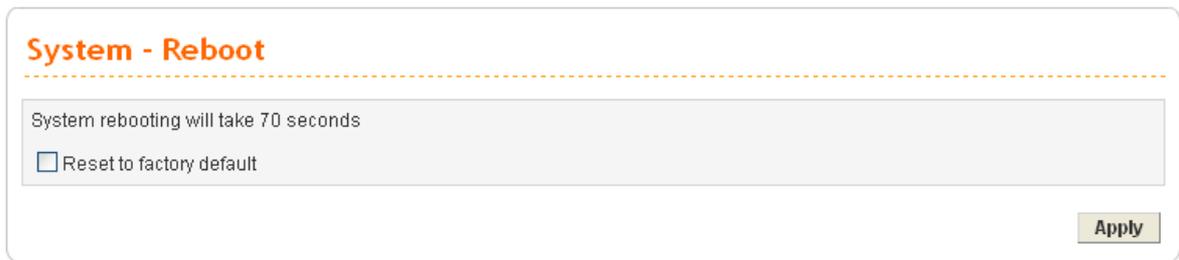
IP Configuration	1st DHCP Server	2nd DHCP Server
Start IP Address :	<input type="text" value="192.168.2.10"/>	
IP Pool Size :	<input type="text" value="100"/>	
<b>MAC Address List (MAC Address Format xx:xx:xx:xx:xx:xx)</b>		
1.	<input type="text" value="00:21:33:47:56:23"/>	2. <input type="text"/>
3.	<input type="text"/>	4. <input type="text"/>
5.	<input type="text"/>	6. <input type="text"/>
7.	<input type="text"/>	8. <input type="text"/>
9.	<input type="text"/>	10. <input type="text"/>

**Apply** **Cancel**

圖 3-8 備用 DHCP 伺服器設置

<b>Start IP Address</b> (起始 IP 位址)	設定 IP Pool 的起始 IP 位址。
<b>IP Pool Size</b> (IP Pool 大小)	指定 IP Pool 中連續 IP 位址的數目。
<b>MAC Address List</b> (Mac 地址列表)	可指定最多 10 個 MAC 地址，一旦 MAC 地址與列表符合，即可獲得 IP 位址分組資訊。

按 **Apply(完成)**，將出現重新啓動提示頁面並重新啓動路由器。



The image shows a web interface for system rebooting. At the top, the title "System - Reboot" is displayed in orange text. Below the title, a dashed orange line separates it from a grey box containing the text "System rebooting will take 70 seconds". Underneath this, there is a checkbox labeled "Reset to factory default". In the bottom right corner of the interface, there is a button labeled "Apply".

圖 3-9 系統重新啓動

按 **Apply(完成)** 並重新啓動 Vigor3300 以使用新的配置。

# 第 4 章

## 系統設置

### 4.1 Status(狀態)

狀態功能提供一些關於 Vigor3300 具有價值的系統資訊，當然，用戶也能夠在此頁面查看網際網路的連線狀態。

按 **System >> Status(系統->狀態)**。

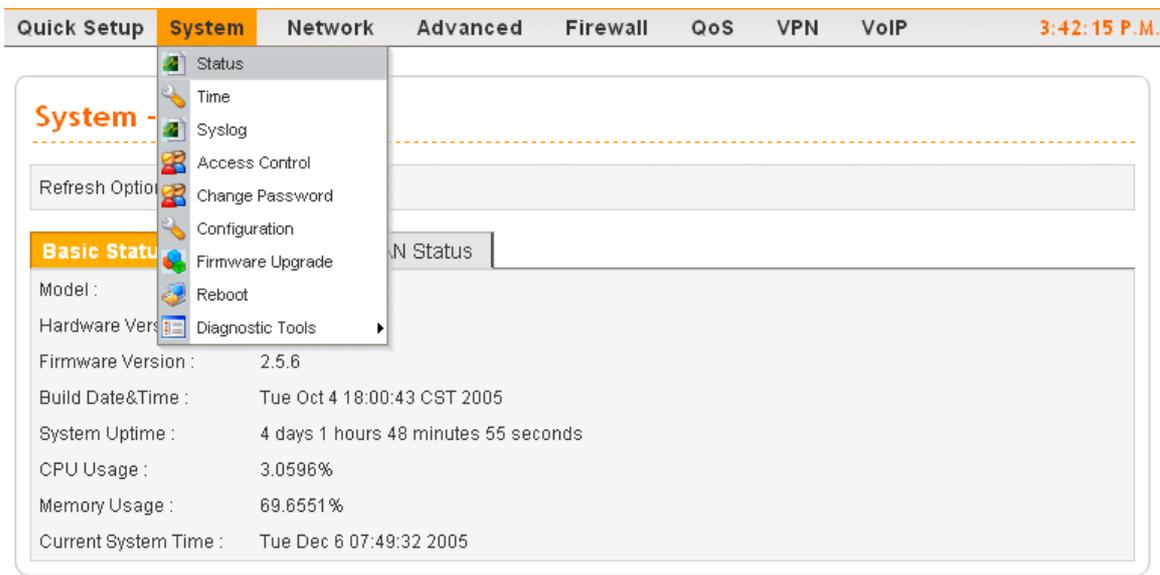


圖 4-1 狀態頁面

按 **Status(狀態)**，將會進入如下提示頁面。

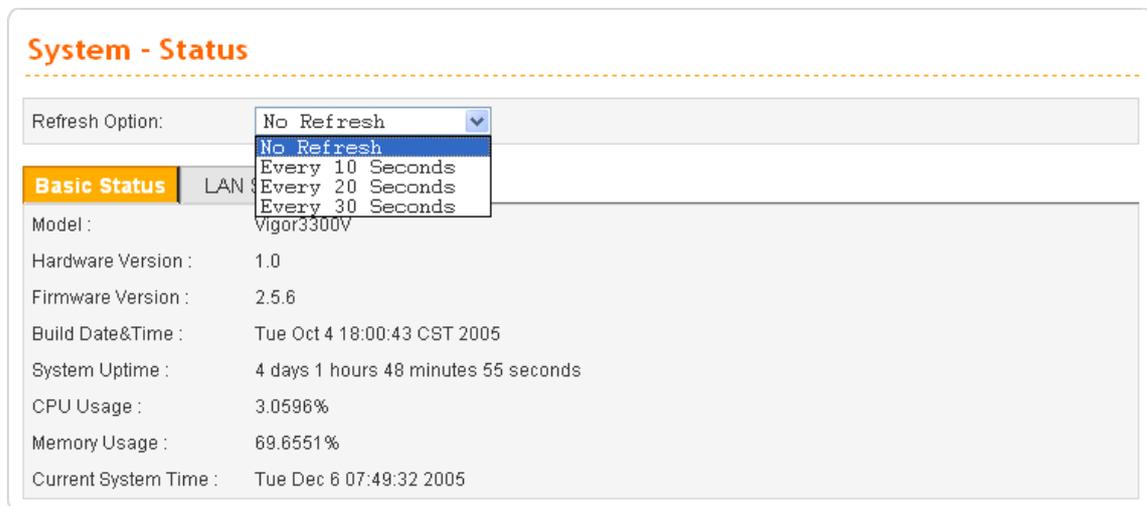


圖 4-2 系統狀態

狀態頁面包括三個部分，他們是基本狀態、LAN 狀態、WAN 狀態。

<b>Refresh Option</b> (更新選項)	您將可以選擇自動更新或者不更新頁面資訊。 有如下四個選項 —— <b>No Refresh(不更新)</b> ： 頁面資訊鎖定。 <b>Every 10 Seconds(每 10 秒)</b> ： 每隔 10 秒更新頁面。 <b>Every 20 Seconds(每 20 秒)</b> ： 每隔 20 秒更新頁面。 <b>Every 30 Seconds(每 30 秒)</b> ： 每隔 30 秒更新頁面。
---------------------------------	--

#### 4.1.1 Basic Status(基本狀態)

基本狀態提供用戶使用型號、硬體版本、韌體版本、建立日期時間、CPU 使用率、記憶體使用率以及目前系統使用的時間等等路由器基本資訊。

圖 4-3 基本狀態

Model(型號)	路由器的型號名稱
Hardware Version(硬體版本)	路由器的硬體版本
Firmware Version(韌體版本)	路由器的韌體版本
Build Date&Time(建立時間)	韌體的製作日期
System Uptime(系統運行時間)	路由器已正常運行的時間
CPU Usage (CPU 使用率)	CPU 的平均使用率
Memory Usage(記憶體使用率)	記憶體的平均使用率
Current System Time (目前系統時間)	系統目前的真實時間

### 4.1.2 LAN Status (LAN 狀態)

此一頁面提供區域網路設定的狀態訊息。

圖 4-4 LAN 狀態

IP Address(IP 地址)	LAN 介面的 IP 位址
MAC Address (MAC 地址)	LAN 介面的 MAC 位址
High Availability Status (高可用性狀態)	當系統高可用性功能開啓時，功能的狀態有如下兩個選項： 支配：Vigor3300 在高可用性中處於支配角色。 從屬：Vigor3300 在高可用性中處於從屬角色。
RX Packets(接收封包)	LAN 介面接收的全部封包數量。
TX Packets(傳送封包)	LAN 介面發送的全部封包數量。

### 4.1.3 WAN Status (WAN 狀態)

此一頁面提供廣域網路設定的狀態訊息。

System - Status	
Refresh Option:	No Refresh
Basic Status	LAN Status
<b>WAN Status</b>	
<b>WAN1 :</b>	<b>WAN2 :</b>
IP Address :	172.16.3.229
MAC Address :	00:00:00:00:00:02
Primary DNS :	168.95.1.1
Secondary DNS :	168.95.192.1
Gateway :	172.16.3.1
RX Packets :	1423069
TX Packets :	154067
Connection Status :	connected
Up Time :	4 days 2 hours 13 minutes 32 seconds
<b>WAN3 :</b>	<b>WAN4 :</b>
IP Address :	
MAC Address :	00:00:00:00:00:04
Primary DNS :	
Secondary DNS :	
Gateway :	
RX Packets :	
TX Packets :	
Connection Status :	
Up Time :	

圖 4-5 WAN 狀態

這裡展示了 4 個 WAN 介面的一些基本資訊。

IP Address (IP 地址)	WAN 介面的 IP 位址
MAC Address (MAC 地址)	WAN 介面的 MAC 位址
Primary DNS (首選 DNS 伺服器)	分配的首選 DNS 地址
Secondary DNS (備用 DNS 伺服器)	分配的備用 DNS 地址
Gateway(閘道)	分配的預設閘道的地址
RX Packets(接收封包)	各個 WAN 介面接收的全部封包數量
TX Packets(發送封包)	各個 WAN 介面發送的全部封包數量
Connection Status (連接狀態)	顯示 WAN 介面的狀態，包括連線(connected)和斷線(disconnected)。 <b>Connected</b> ：當路由器在“負載平衡”或“備份”功能開啓時路由器能夠與閘道溝通狀態。若是此介面是唯一的工作介面，那麼它將永遠顯示連線。
Up Time(保持時間)	顯示開始後的連線時間。

## 4.2 Time(時間設定)

路由器透過 NTP (網路時間協定)用戶端從時間伺服器獲得時間基礎。由於一些基於時間的功能(比如計畫任務、URL 目錄過濾)，系統時間需要預先正確設置好，典型的 NTP 設置會利用多個時間伺服器和不同的網路路徑，以期獲得高精確度和可靠性。

Vigor3300 可與指定的時間伺服器或遠端管理主機進行同步化作業。

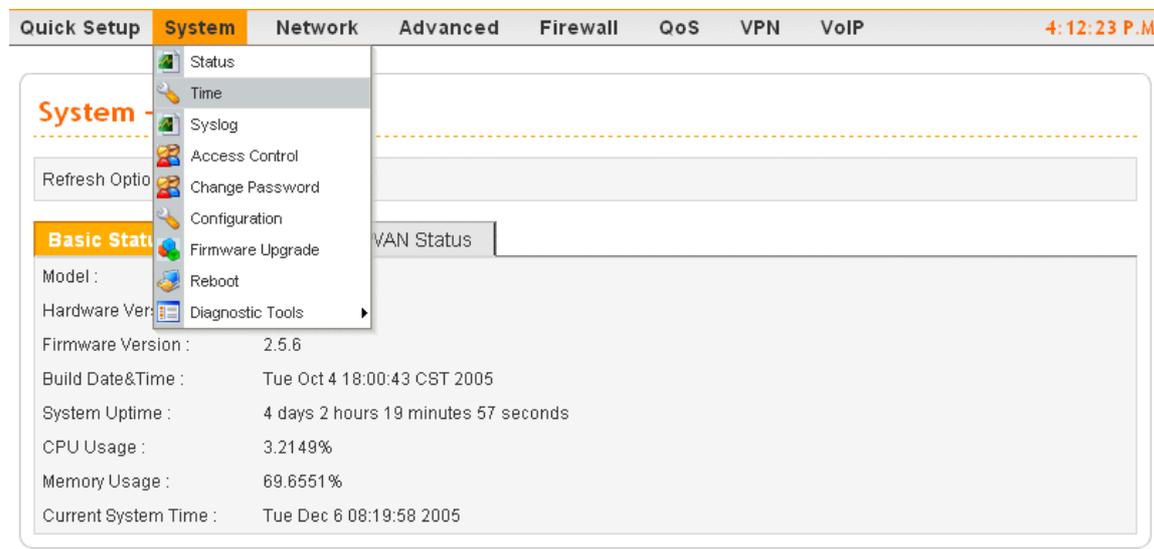


圖 4-6 時間設置

按 **System >> Time(系統 >> 時間)**，將會進入如下頁面。

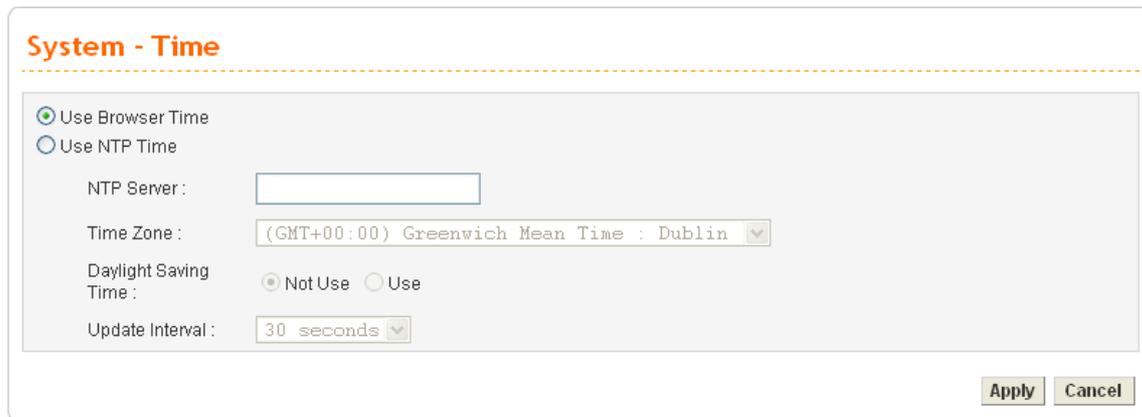


圖 4-7 時間設置

Use Browser Time (遠程管理員校時)	按此選項，從遠端管理主機來調整時間。
Use NTP Time (由 NTP 伺服器校時)	按此選項，從 NTP 伺服器來調整時間。
NTP Server (NTP 伺服器)	指派一個 NTP 伺服器的 IP 位址或功能變數名稱。
Time Zone(時區)	選擇 Vigor3300 所在地的時區。
Daylight Saving Time	選擇 <b>Use</b> 以啟動此功能。

(日光節約時制)	
Update Interval (更新時間間隔)	選擇向 NTP 伺服器更新時間資訊的間隔。

按 **Apply(完成)** 以使設置生效。

### 4.3 Syslog (紀錄設定)

Vigor3300 系列支援系統紀錄 (syslog) 功能用以記錄非正常的狀況。路由器會發送 Syslog 封包到 Internet 上的 syslog 伺服器，這樣，管理員就可以監測發生在 Vigor3300 上的反常事件了。

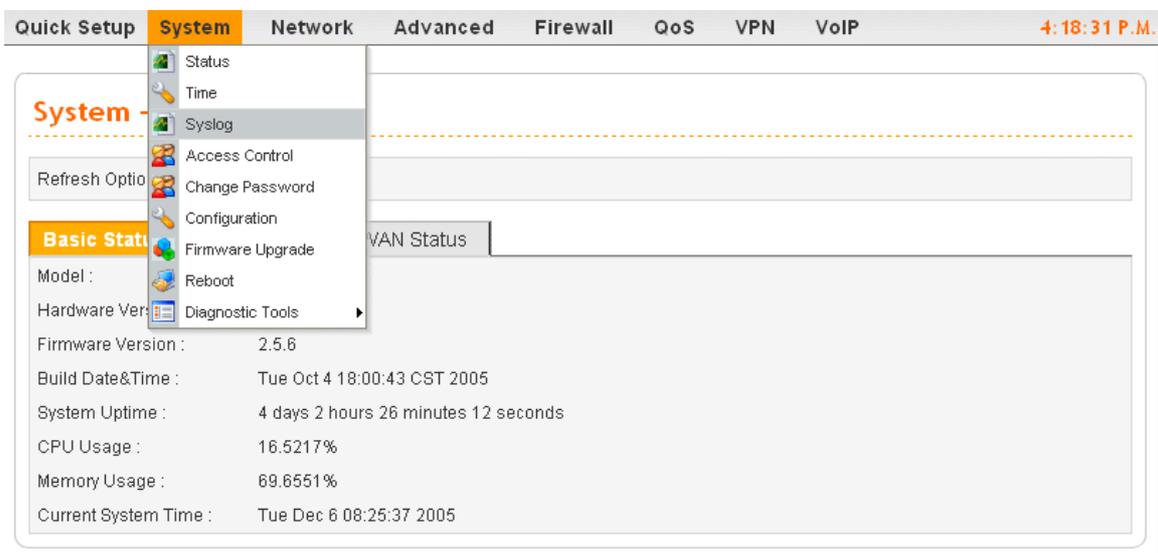


圖 4-8 日誌位置

按 **System >> Syslog(系統 >>紀錄)**，將會進入如下提示頁面。

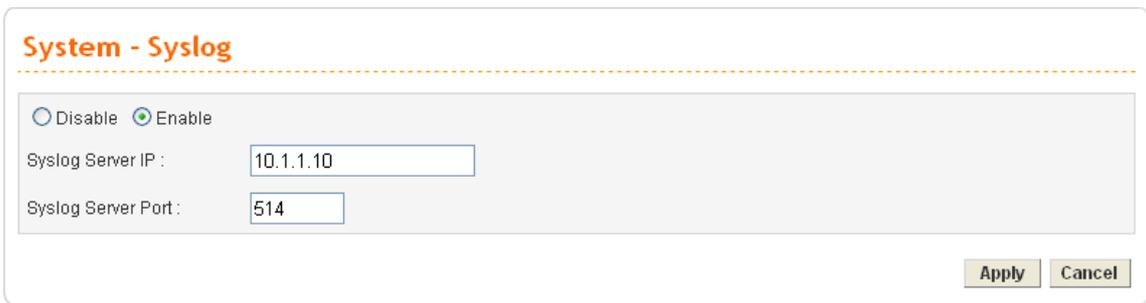


圖 4-9 日誌設置

Disable/Enable (啓動/關閉)	按 <b>Enable</b> 以啓動功能； <b>Disable</b> 則是關閉此功能。
Syslog Server IP (系統紀錄伺服器 IP)	指派的 syslog 伺服器 IP 地址。如果用戶指派的 IP 是“0.0.0.0”，syslog 功能將被關閉，也就是說 Vigor3300

	不會向 syslog 伺服器發送 syslog 封包。
Syslog Server Port (紀錄伺服器埠)	為 Syslog 協議指派一個埠號。

按 **Apply(完成)** 以使設置生效。

## 4.4 Access Control(連線控制設定)

連線控制可以防止由病毒而引起的 ICMP 封包攻擊。當 LAN 內有蠕蟲類型病毒時，您可以關閉 LAN 內的 ping 功能。這一機制可以預防病毒的傳播。然而，我們不推薦在正常情況下使用此設置，因為它也會阻擋正當的請求封包。

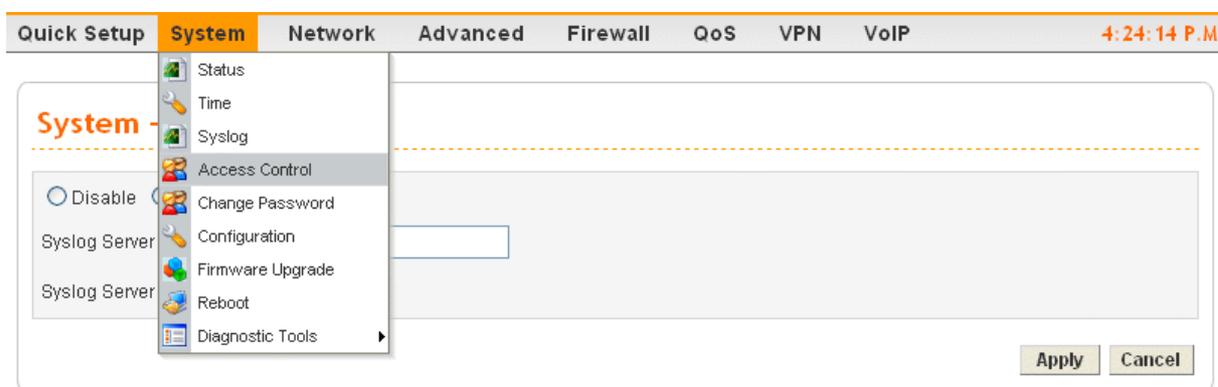


圖 4-10 連線控制位置

按 **System>>Access Control(系統 >>連線控制)**，將會進入如下提示頁面。

### System - Access Control

---

**Management Access Control**  
 Allow Management from the WAN  
 Disable     Enable All     Enable User Defined WAN IP  
 Allowed IP1:   
 Allowed IP2:   
 Allowed IP3:

**Management Port**  
 Default Ports (HTTP Port:80 Telnet Port:23)     User Defined Ports  
 HTTP Port:   
 Telnet Port:

**PING Restriction**  
 Disable PING from the LAN  
 Disable PING from the WAN

圖 4-11 連線控制設置

Management Access Control(允許從網際網路管理路由器)	
Disable(關閉)	關閉所有 WAN 介面的管理功能。
Enable All(全部啟動)	開啓所有 WAN 介面的管理功能。
Enable User Defined WAN IP (允許用戶定義 WAN ) IP	用戶可以指派 3 個 IP 位址用於 WAN 介面管理。
Management Port (管理埠)	
Default Ports(預設埠)	使用 Http 及 Telnet 的預設值。(Http:80 ; Telnet: 23)
User Defined Ports (用戶自定義埠)	讓用戶自行指定 HTTP 及 Telnet 埠值。
PING Restriction (限制 PING)	
Disable PING from the LAN(關閉來自 LAN 端的 PING)	選擇此選項以拒絕所有來自 LAN 的 ICMP 封包
Disable PING from the WLAN(禁止來自 WAN 端的 PING)	選擇此選項以拒絕所有來自 WAN 的 ICMP 封包

按 **Apply(完成)** 以使設置生效。

## 4.5 Reboot(重新啟動設定)

用 Web 介面來重新啟動 Vigor3300。



圖 4-12 重新啟動位置

按 **System >> Reboot(系統>>重新啟動)**，將會進入如下提示頁面。用戶可以選擇重新啟動 Vigor3300 時，保存現有設置或者回復至出廠設置。

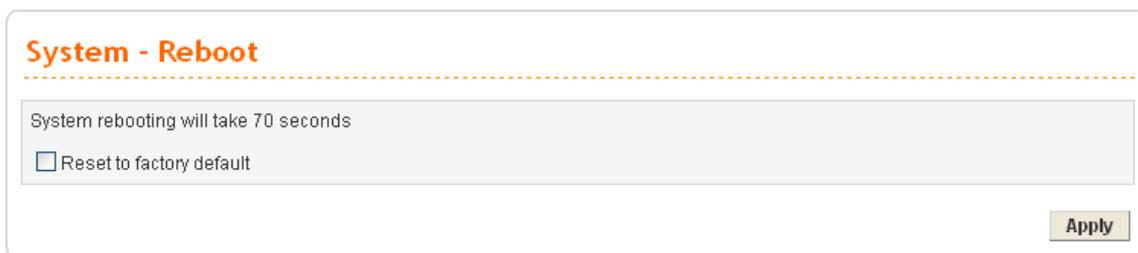


圖 4-13 重新啓動設置

按 **Apply(完成)**以重新啓動整個系統，一般需要 70 多秒以完成整個重新啓動步驟。

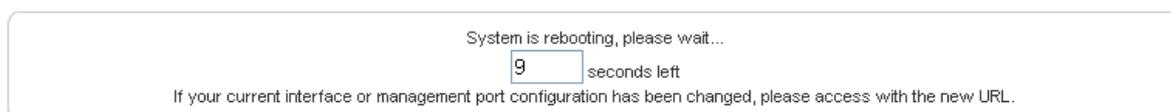


圖 4-14 重新啓動倒計時

## 4.6 Firmware Upgrade(軟體升級設定)

Vigor3300 提供下列升級方法。在升級前，您需要先在本地主機上安裝 Router Tools，包括 Firmware Upgrade Utility。下面步驟可以幫助您進行韌體升級。

### 由 web 介面升級韌體

Vigor3300 支援 web 介面升級韌體

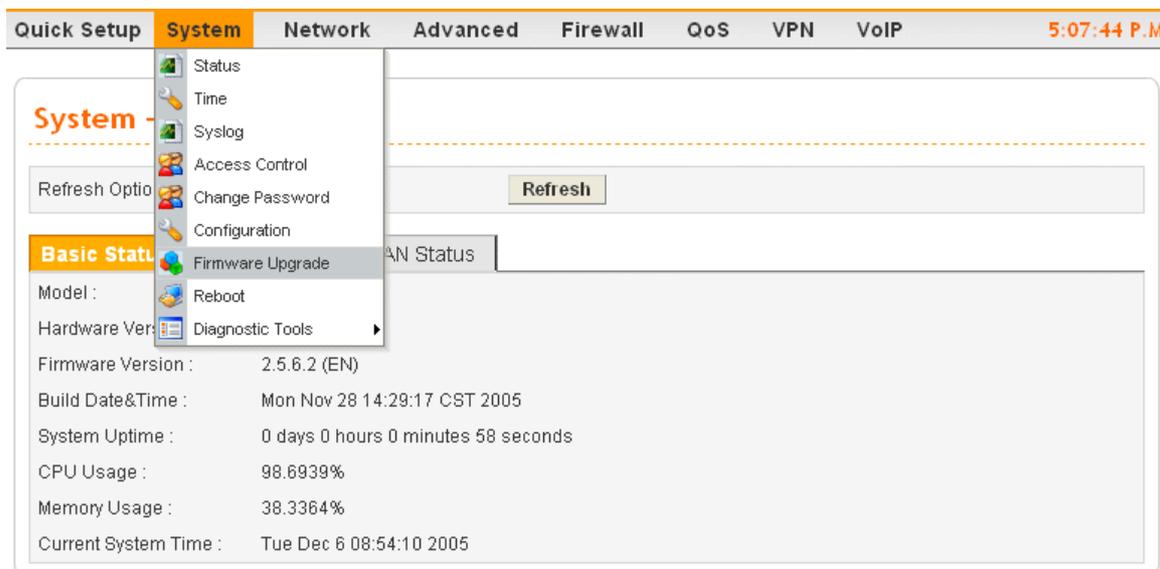


圖 4-15 韌體升級位置

按 **System >>Firmware Upgrade(系統>>韌體升級)**。

圖 4-16 韌體升級設置

Location(地址)	按 <b>Local</b> 或者 <b>Remote</b> 選項，以選擇升級方式。 <b>Local</b> ：從本地的 TFTP 伺服器升級韌體。 <b>Remote</b> ：從遠端的 TFTP 伺服器升級韌體。
Firmware(韌體)	在按 <b>瀏覽</b> 後，找出韌體所在路徑。
TFTP Server IP (TFTP 伺服器 IP)	為遠端升級的 TFTP 伺服器指派的 IP 地址。

注意：本例是在 Windows 環境中設定，在此步驟用戶需要等待 3 至 5 分鐘，然後再次重新啓動系統。

1. 從 DrayTek 的主力站點 [www.draytek.com.tw](http://www.draytek.com.tw)（或者本地的 DrayTek 站點）或 FTP 站點 [ftp.draytek.com](http://ftp.draytek.com) 下載最新的韌體。將韌體保存在本地主機上。
2. 按**瀏覽**定位韌體的位置並按 **Apply(完成)**。升級程序開始進行，並在進度條上會顯示出目前狀態。一旦升級完成，大約 30 秒後，路由器將可恢復正常(亦即在 Vigor3300 的面板上的 ACT 燈持續正常閃爍)。

注意：用戶在此步驟中必須等待 3 到 5 分鐘，然後重新啓動系統。

3. 按 **Apply(完成)**以開始升級步驟。

#### 從控制台介面升級韌體

注意：本例在 Windows 環境中設定。

1. 按上面提到的方法從 DrayTek 的網站和 FTP 站點下載最新的韌體。
2. 透過控制台連接，把 Vigor3300 和 DB9 的 RJ45 控制台埠連到主機的 RS232 連接器上。控制台埠的預設值為“串列傳輸速率 57600，無奇偶校驗，8 位元資料位元，1 位元停止位。”

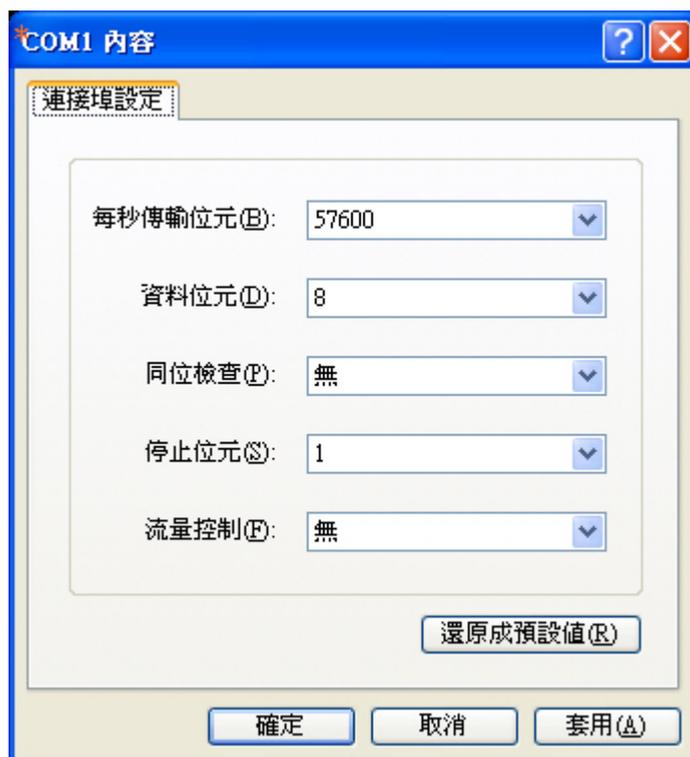


圖 4-17 從控制台埠升級韌體

3. 開啓 Vigor3300，並在系統完全重新啓動前在 PC 上按下 ENTER。Vigor3300 將會處於等待 TFTP 載入狀態，會有如下資訊顯示。  

```
*****
* DrayTek V3300 Bootloader *
*****
Press [ENTER] key within 5 sec. to download image...1
Current LAN IP is 192.168.1.1
New IP:
Prepare downloading
```
4. 鍵入圖形的名稱並在 PC 上執行 TFTP 用戶端，會有如下資訊顯示。  

```
TFTP -i 192.168.1.1 PUT [Vigor3300 image file name]
```
5. 升級步驟完成後，系統會自動進行重新啓動。

## 4.7 Diagnostic Tools(診斷工具)

在有些情況下，用戶需要知道一些有關 Vigor3300 的資訊，比方說一些靜態或動態的資料庫或者一些路由資訊等等。Vigor3300 提供 4 種功能以幫助用戶檢視這些資訊，可使客戶更加便利的瞭解到目前路由和網際網路狀態。

Vigor3300 上有 4 個選項，接下來的章節將會提出更詳細的描述。用戶可以充分瞭解關於路由、ARP、DHCP 和 NAT 功能的一些資訊。

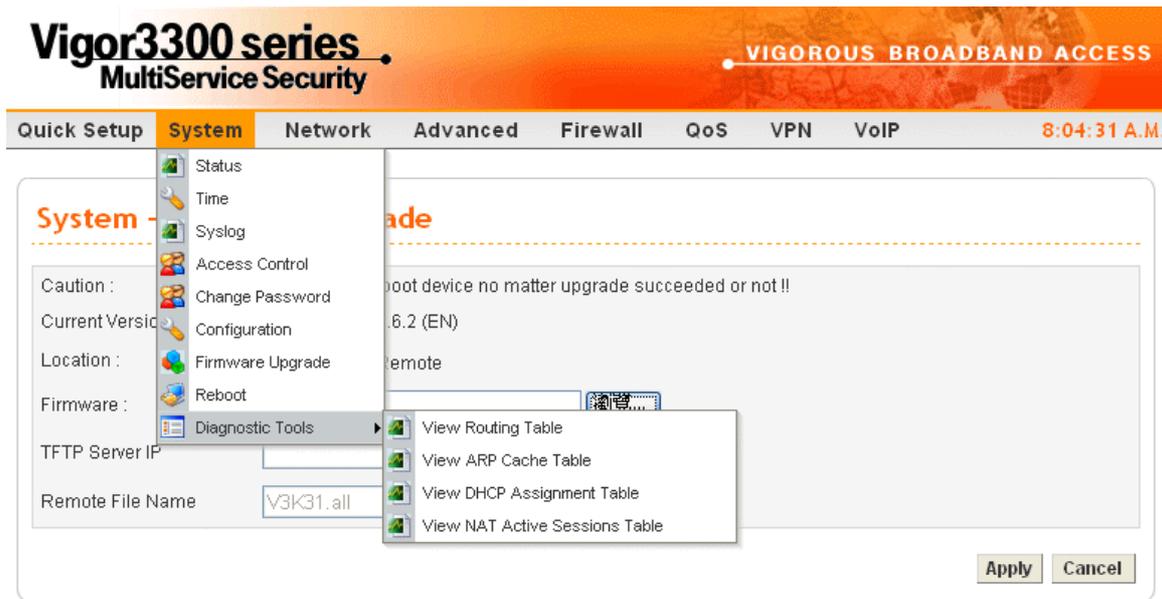


圖 4-18 診斷工具功能

#### 4.7.1 View Routing Table(查看路由表)

此頁列舉在頁面上的 Vigor3300 的路由表。目標指目標 IP 位址，閘道指預設閘道，標記指狀態，介面則是 eth0 指 LAN 介面，eth1 指 WAN 介面。

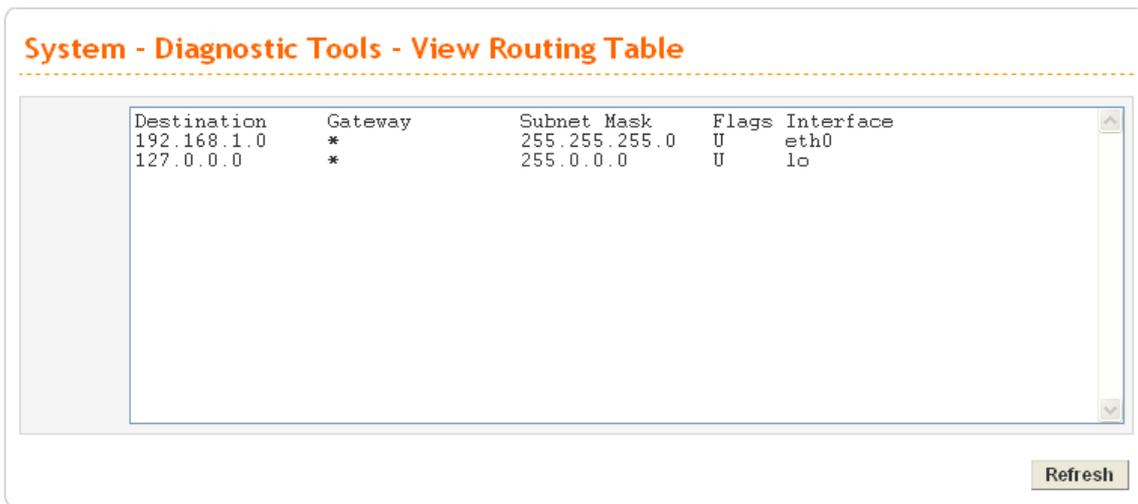
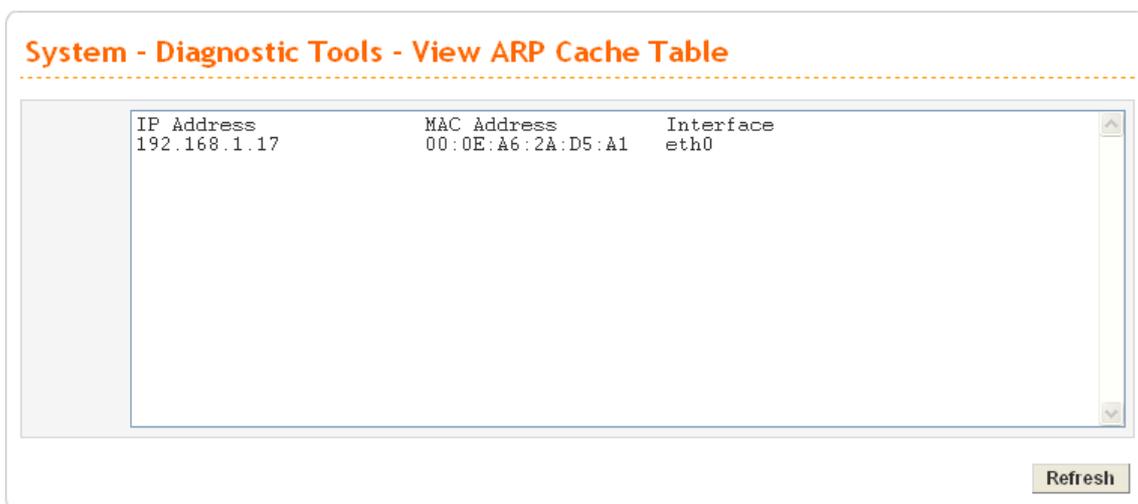


圖 4-19 查看路由表

#### 4.7.2 View ARP Cache Tabel (查看 ARP Cache 表)

此頁列舉 Vigor3300 上的 ARP Cache 表。

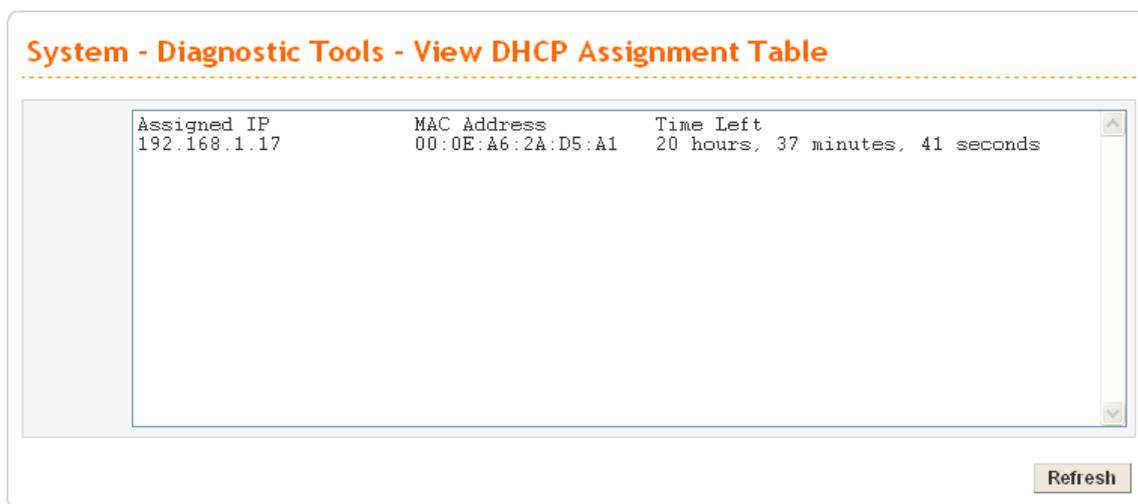


IP Address	MAC Address	Interface
192.168.1.17	00:0E:A6:2A:D5:A1	eth0

圖 4-20 查看 ARP Cache 表

### 4.7.3 View DHCP Assignment Table(查看 DHCP 分配表)

此頁列舉 Vigor3300 上的 DHCP 分配表。



Assigned IP	MAC Address	Time Left
192.168.1.17	00:0E:A6:2A:D5:A1	20 hours, 37 minutes, 41 seconds

圖 4-21 查看 DHCP 分配表

### 4.7.4 View NAT Active Sessions Table(查看 NAT 活動對話表)

此頁列舉 Vigor3300 上的現行活動的 NAT 對話表。

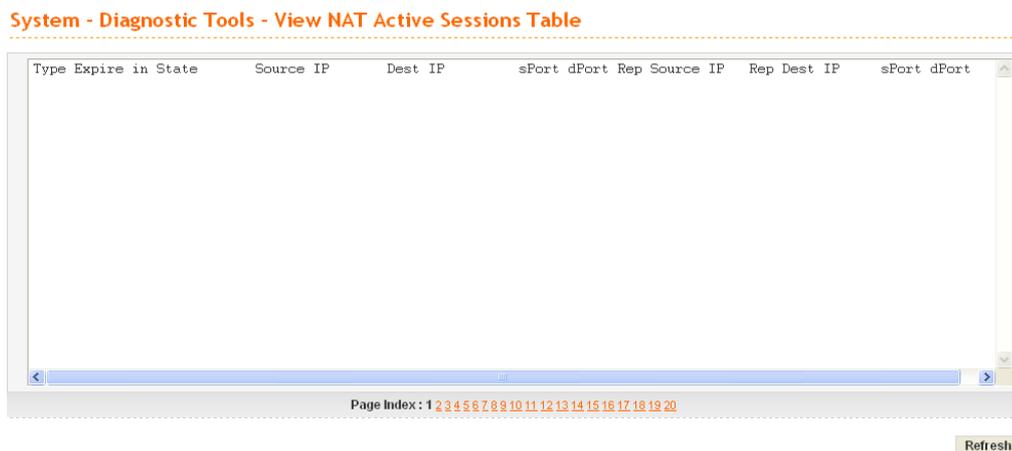


圖 4-22 查看 NAT 活動對話表

## 4.8 Configuration(設定)

當用戶完成設置後，Vigor3300 提供一個功能用以儲存這些設置。這樣一來，用戶在下次設置路由器時，只需要直接讀取存儲的設定，重新啓動一次路由器即可恢復設定。

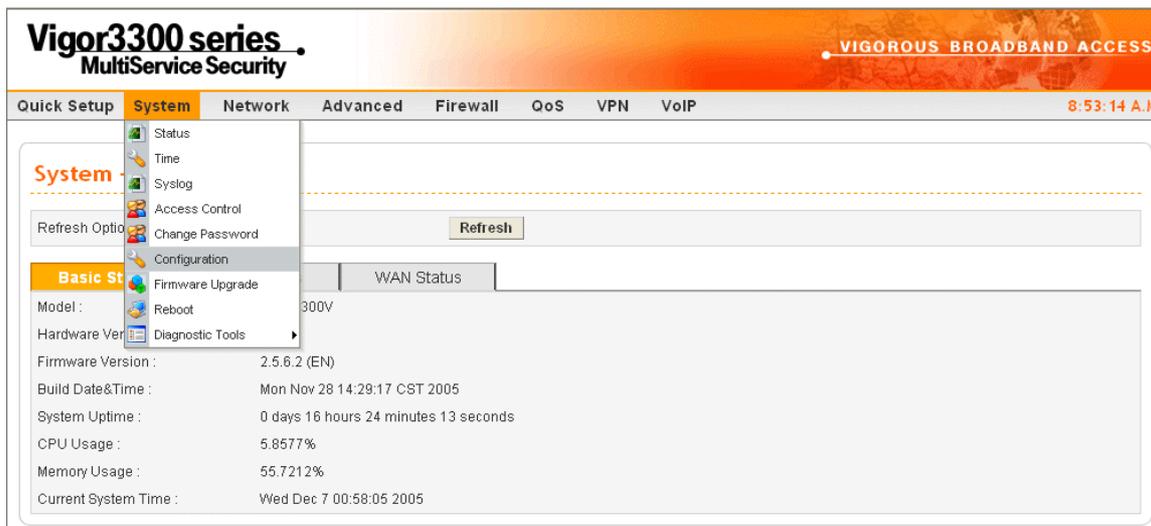


圖 4-23 配置

按 **System>> Configuration(系統>>設定)**，將會顯示如下提示頁面。



圖 4-24 設置

<b>Restore(恢復)</b>	
<b>Select a configuration file(選擇配置檔)</b>	指派一個檔從主機上傳到路由器。
<b>Backup(備份)</b>	
<b>Backup configuration Push Backup button (備份配置檔 按備份按鈕)</b>	可從路由器傳送一個檔到主機上。預設檔案名為“v3300.cfg”。

本頁留白

# 第 5 章

## 網路設置

在網路組中，您可以設置路由器以連線網際網路的 WAN 和 LAN 介面。

### 5.1 WAN 和網際網路連線設定

用戶可以設置 WAN 介面，以便在 Internet 環境中應用。Vigor3300 系列支援 4 個 WAN 介面，每個 WAN 介面都有相同的設置頁面。

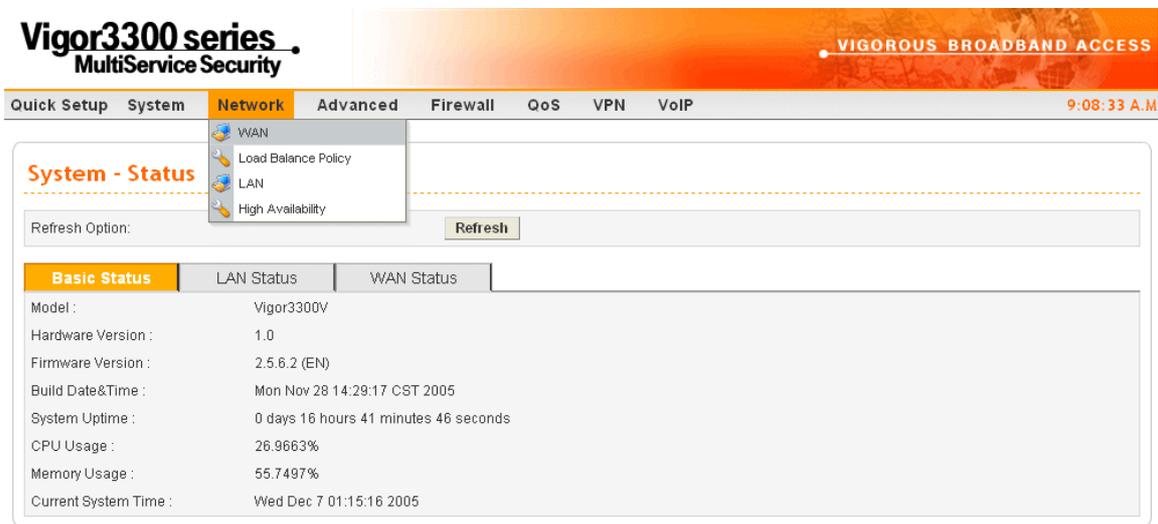


圖 5-1 網路功能表位置

按 **Network>>WAN(網路>>WAN)**，將會顯示如下頁面：

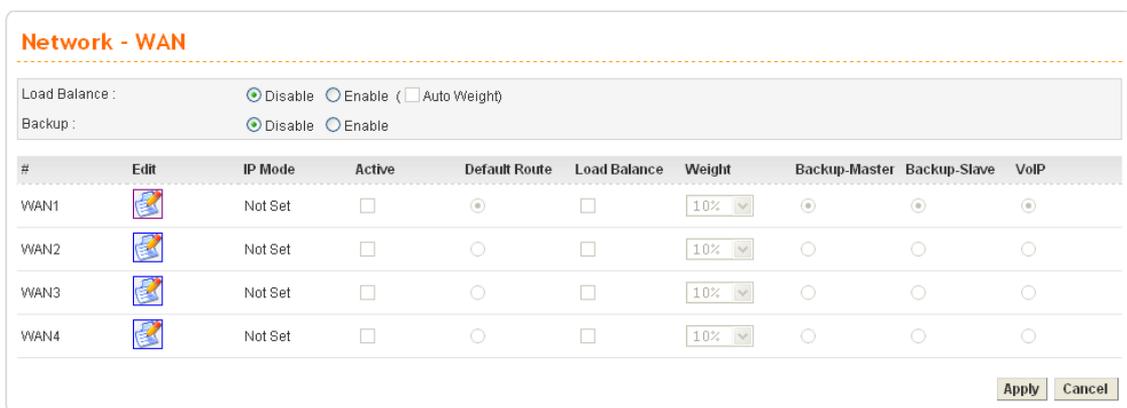


圖 5-2 WAN 介面

**Load Balance**  
(負載平衡)

用戶可以“**Enable(啓動)**”或者“**Disable(關閉)**” WAN 端的負載平衡。並且它允許用戶選擇 **Auto Weight(自動)**

	權重調整)，不過只有在選擇“啓用”的情況下。
<b>Backup(備份)</b>	用戶可以“ <b>Enable(啓動)</b> ”或者“ <b>Disable(關閉)</b> ”WAN 端的備份功能。
<b>Edit(編輯)</b>	按此圖示可進入相應的 WAN 端設置頁面。
<b>IP Mode(IP 模式)</b>	顯示目前 WAN 介面的設置模式。 有 4 個選項 – Static, DHCP, PPPoE, PPTP
<b>Active(啓用)</b>	按此選項以啓動此 WAN 介面。
<b>Default Route (預設路由)</b>	按此選項，以選擇此 WAN 介面作為預設路由介面。
<b>Load Balance (負載平衡)</b>	按此選項以選擇此 WAN 介面加入負載平衡組。
<b>Weight(權重)</b>	選擇此 WAN 介面的在負載平衡中的載荷值，範圍從 10% 到 90%。
<b>Backup-Master(主備份)</b>	按此選項以選擇此 WAN 介面作為主介面。
<b>Backup-Slave(從備份)</b>	按此選項以選擇此 WAN 介面作為副介面。
<b>VoIP</b>	按此選項以選擇此 WAN 介面作為 VoIP 預設介面。

對於大多數用戶，網際網路連線是個主要的應用。Vigor3300 系列支援寬頻網際網路連線並提供超過一個的 WAN 介面。接下來的部分會給出詳細的寬頻連線方法的說明。

按“**Edit(編輯)**”圖示以進入每個 WAN 介面設置頁面。

**Network - WAN - WAN1 - Fast Ethernet**

MAC Address :  Default MAC  User Defined MAC

Downstream Rate :  (kbps)

Upstream Rate :  (kbps)

Type :

Physical Mode :

IP Mode :  Static  DHCP  PPPoE  PPTP

**Static/DHCP Configuration** | PPPoE/PPTP Configuration

IP Address :  Host Name :

Subnet Mask :  Domain Name :

Default Gateway :  (Host Name and Domain Name are required for some ISPs.)

Primary DNS :

Secondary DNS :

**Connection Detection**

Detect Type :

Detect Interval(sec) :

Max Unreply Times :

Detect Destination Host : (IP or Domain Name)

**IP Alias List**

1.	<input type="text"/>	2.	<input type="text"/>
3.	<input type="text"/>	4.	<input type="text"/>
5.	<input type="text"/>	6.	<input type="text"/>
7.	<input type="text"/>	8.	<input type="text"/>

圖 5-3 WAN 介面設置

MAC Address (MAC 地址)	
<b>Default MAC (路由器預設)</b>	使用存在路由器的原始 MAC 位址。
<b>User Defined MAC (戶定義)</b>	使用用戶自定義的 MAC 位址。
<b>Downstream Rate (下傳速率)</b>	指定 WAN 介面的下傳速率。預設值是 102400kbps (100Megabit)。此設定對於 Vigor3300 的下傳 Cache 調整非常重要。如果您使用 2Mbps 的 DSL 下傳速率，那麼下傳速率設置為 2Mbps。
<b>Upstream Rate (上傳速率)</b>	指定 WAN 介面的上傳速率。預設值是 102400kbps，設定對於 Vigor3300 上傳 Cache 調整以及載荷設置，如同上面一樣重要。如果您使用 2Mbps 的 DSL 上傳速率，那麼上傳速率設置為 2Mbps。
<b>Type(類型)</b>	選擇 WAN 介面的連接類型。
<b>Physical Mode</b>	選擇 WAN 介面的連接速度模式。有自動協商，全雙工，半雙工，以及 10M 和 100M 速度選項。

(實體模式)	
<b>IP Mode (IP 模式)</b>	選擇 WAN 介面的生成 IP 資訊的模式。共有 4 種可用的 Internet 連線方式， <b>Static</b> 、 <b>DHCP</b> 、 <b>PPPoE</b> 以及 <b>PPTP</b> 。在此頁面，您可以為 WAN 介面設置靜態、DHCP、PPPoE 以及 PPTP 等模式。大部分的 Cable 用戶會用 DHCP 模式以便從系統來取得一個公用網 IP。

在連接到寬頻連線設備前，例如，DSL/Cable modem，對於路由器，您必須知道 ISP 提供的是那種服務。接下來的部分為您介紹 4 個廣泛使用的寬頻連線服務。大多數情況下，您可以從 ISP 那裡得到一個 DSL/Cable modem。路由器可以被連接到寬頻設備上（即 DSL/Cable），並以 NAT 或 IP 路由器工作方式連線 Internet。

### 5.1.1 Static Configuration(靜態 IP 設定)

用戶可以手動設置某個 WAN 介面的 IP 資訊。

圖 5-4 靜態 IP 設置

<b>IP Address(IP 地址)</b>	指派 WAN 介面位址。
--------------------------	--------------

<b>Subnet Mask</b> (子網路遮罩)	指派 WAN 介面的子網路遮罩。
<b>Default Gateway</b> (預設閘道)	指派閘道 IP 地址。
<b>Primary DNS</b> (首選 DNS)	指派首選 DNS 的 IP 地址。
<b>Secondary DNS</b> (備用 DNS)	指派備用 DNS 的 IP 地址。
<b>IP Alias List</b> (IP 別名列表)	指派在此介面中其他可以使用的 IP 位址。

按 **Apply(完成)** 並重新啓動系統。

### 5.1.2 DHCP 用戶端設定

設置 WAN 介面作為 DHCP 用戶端，這樣 Vigor3300 將會向 DHCP 伺服器或者 DSL modem 自動申請 IP 網路設定。如果用戶選擇此模式，則無需進行其他設置。

**Network - WAN - WAN1 - Fast Ethernet**

---

MAC Address :  Default MAC  User Defined MAC

Downstream Rate :  (kbps)

Upstream Rate :  (kbps)

Type :  ▼

Physical Mode :  ▼

IP Mode :  Static  DHCP  PPPoE  PPTP

---

**Static/DHCP Configuration** | PPPoE/PPTP Configuration

IP Address :  Host Name :

Subnet Mask :  Domain Name :

Default Gateway :  (Host Name and Domain Name are required for some ISPs.)

Primary DNS :

Secondary DNS :

---

**Connection Detection**

Detect Type :  ▼

Detect Interval(sec) :

Max Unreply Times :

Detect Destination Host : (IP or Domain Name)

---

**IP Alias List**

1. <input type="text"/>	2. <input type="text"/>
3. <input type="text"/>	4. <input type="text"/>
5. <input type="text"/>	6. <input type="text"/>
7. <input type="text"/>	8. <input type="text"/>

圖 5-5 DHCP 設定

按 **Apply(完成)**，並重新啓動系統。

### 5.1.3 DSL Modem 的 PPPoE 設定

大部分的 DSL 用戶都會使用此模式，所有的本地用戶共用一個 PPPoE 連接至 Internet，用戶只要輸入 ISP 業者提供的設定資料即可。

The screenshot shows the configuration interface for Network - WAN - WAN1 - Fast Ethernet. The 'IP Mode' is set to PPPoE. The 'PPPoE/PPTP Configuration' tab is active, showing fields for User Name, Password, Authentication (set to PAP), Service Name, PPTP Local Address, PPTP Subnet Mask, and PPTP Server Address. The 'Connection Detection' section shows Detect Interval set to 10 and Max Unreply Times set to 2. Buttons for Apply, Reset, and Cancel are at the bottom right.

圖 5-6 PPPoE 設定

<b>User Name(用戶名)</b>	指派 ISP 提供用戶名。
<b>Password(密碼)</b>	指派 ISP 提供的對應用戶名的密碼。
<b>Authentication(認證)</b>	選擇 <b>PAP</b> or <b>CHAP</b> 協議將有更好的相容性。預設值為 <b>PAP</b> 。

按 **Apply(完成)**，並重新啓動系統。

### 5.1.4 DSL Modem 的 PPTP 設定

下列設定頁面僅僅作為示範參考，您的服務供應商應該提供給您正確的設置。

**Network - WAN - WAN1 - Fast Ethernet**

MAC Address :  Default MAC  User Defined MAC

Downstream Rate :  (kbps)

Upstream Rate :  (kbps)

Type :

Physical Mode :

IP Mode :  Static  DHCP  PPPoE  PPTP

Static/DHCP Configuration | **PPPoE/PPTP Configuration**

User Name :  PPTP Local Address :

Password :  PPTP Subnet Mask :

Authentication :  PPTP Server Address :

Service Name :

**Connection Detection**

Detect Interval :

Max Unreply Times :

圖 5-7 PPTP 設定

<b>User Name(用戶名)</b>	指派 ISP 提供用戶名。
<b>Password(密碼)</b>	指派 ISP 提供的對應用戶名的密碼。
<b>Authentication(認證)</b>	選擇 <b>PAP</b> or <b>CHAP</b> 協議將有更好的相容性。預設值為 <b>PAP</b> 。
<b>PPTP Local Address (PPTP 本地地址)</b>	指派 PPTP 的本地 IP 地址。
<b>PPTP Subnet Mask (PPTP 網路遮罩)</b>	指派 PPTP 的網路遮罩值。
<b>PPTP Server Address (PPTP 伺服器位址)</b>	指派 PPTP 伺服器的遠端 IP 地址。

按 **Apply(完成)**，並重新啟動系統。

## 5.2 LAN 設定

本節將詳細解釋 LAN 介面的設定。



圖 5-8 LAN 功能表位置

按 **Network >> LAN(網路)>>LAN**，將會顯示如下頁面。

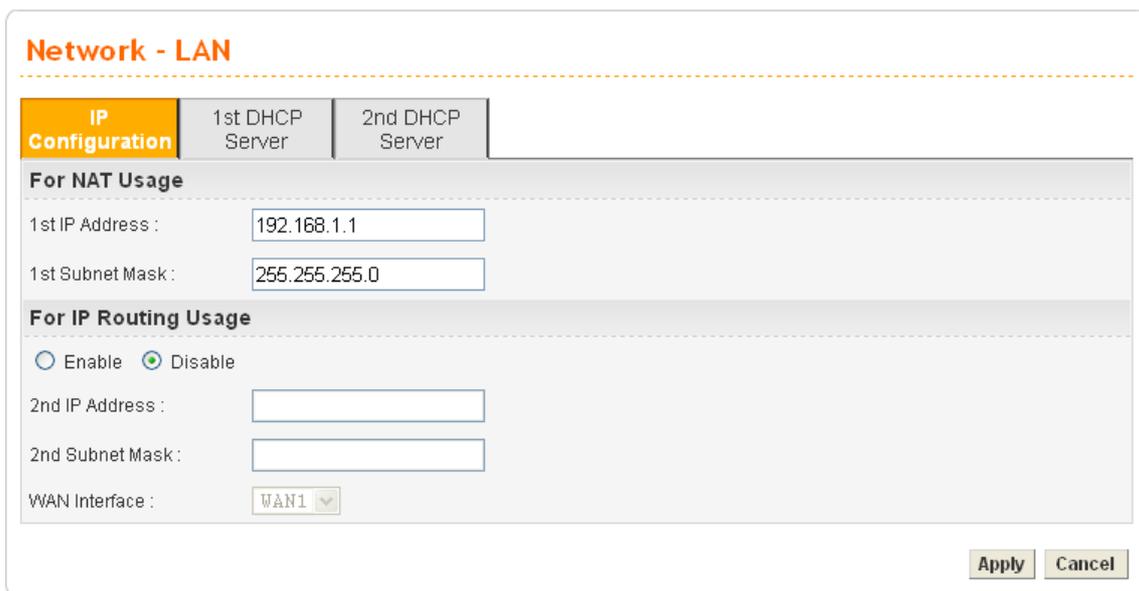


圖 5-9 LAN 設定

此頁面有 3 個選項卡，分別為：

- IP 配置
- 第一子網 DHCP 伺服器
- 第二子網 DHCP 伺服器

### 5.2.1 IP 設定

按 IP 設定，將會顯示如下頁面：

The screenshot shows the 'Network - LAN' configuration page. It has three tabs: 'IP Configuration' (selected), '1st DHCP Server', and '2nd DHCP Server'. Under 'For NAT Usage', there are input fields for '1st IP Address' (192.168.1.1) and '1st Subnet Mask' (255.255.255.0). Under 'For IP Routing Usage', there are radio buttons for 'Enable' and 'Disable' (selected), and input fields for '2nd IP Address' and '2nd Subnet Mask'. A 'WAN Interface' dropdown menu is set to 'WAN1'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

圖 5-10 IP 設定

在 Vigor3300 路由器中，有一些如下表顯示的 IP 位址設置。IP 位址/子網路遮罩可供本地用戶或者 NAT 用戶使用，要啓用路由子網路，您需要從 ISP 獲得一個可路由的子網路。本地主機的預設開道的 IP 地址應設為 Vigor3300 的 IP 地址。當建立起與 ISP 的 DSL 連接後，每個本地 PC 都將直接路由到 Internet。同樣的，您也可以使用 IP 位址/子網路遮罩來連接到其他的本地主機，在此頁面上，您可以看到在 RFC-1918 定義的私人網域位址範圍，通常我們使用 192.168.1.1/24 這個子網域。

For NAT Usage (NAT 應用)	
<b>1<sup>st</sup> IP Address</b> (第一子網 IP 位址)	本地子網的第一 IP 位址，預設值是 192.168.1.1。
<b>1<sup>st</sup> Subnet Mask</b> (第一子網路遮罩)	本地子網的第一網路遮罩，預設值是 255.255.255.0。
For IP Routing Usage (IP 路由應用)	
<b>Enable/Disable</b>	按“啓用”來啓用此功能。 按“關閉”來關閉此功能。
<b>2<sup>nd</sup> IP Address</b> (第二子網 IP 地址)	第二子網的 IP 地址。
<b>2<sup>nd</sup> Subnet Mask</b> (第二子網路遮罩)	第二子網的網路遮罩。

按應用並重新啓動系統。

### 5.2.2 1<sup>st</sup> DHCP Server(第一子網 DHCP 伺服器設定)

Vigor3300 系列支援兩個 DHCP 伺服器。

DHCP 是 Dynamic Host Configuration Protocol 的簡稱，它會自動分配相關的 IP 設定給本地 DHCP 客戶，請參考下列圖片來設置 DHCP 伺服器。

The screenshot shows the 'Network - LAN' configuration interface. It has three tabs: 'IP Configuration', '1st DHCP Server' (selected), and '2nd DHCP Server'. Under '1st DHCP Server', there are radio buttons for 'Status' (Enable, Disable, Relay Agent), with 'Enable' selected. Below are input fields for 'Start IP' (192.168.1.10), 'End IP' (192.168.1.254), 'Primary DNS', 'Secondary DNS', 'Lease Time (Min)' (1440), and 'Gateway IP (Optional)'. A 'Relay Agent' section follows, with a 'WAN Interface' dropdown set to 'WAN1' and a 'DHCP Server IP Address' field. 'Apply' and 'Cancel' buttons are at the bottom right.

圖 5-11 1<sup>st</sup> DHCP 伺服器設置

<b>Status(狀態)</b>	按 <b>Enable(啓動)</b> 以啓動此功能。 按 <b>Disable(關閉)</b> 以關閉此功能。 按 <b>Relay Agent</b> 以啓動此功能。
<b>Start IP(起始 IP)</b>	設定起始 IP 位址。
<b>End IP(終止 IP)</b>	設定結束 IP 位址。
<b>Primary DNS (首選)DNS</b>	設定首選 DNS 的 IP 位址。
<b>Secondary DNS (備用 DNS)</b>	設定備用 DNS 的 IP 位址。
<b>Lease Time(租約期間)</b>	設定上述 IP 地址連線所使用的期間。
<b>Gateway IP (Optional) (閘道 IP 位址選項功能)</b>	設定閘道 IP 位址。
<b>WAN Interface (WAN 介面)</b>	設定 Relay Agent 的 WAN 介面。
<b>DHCP Server IP Address (DHCP 伺服器位址)</b>	設定 DHCP 伺服器位址。

注意：如果首選 DNS 和備用 DNS 都是空白的，那麼路由器會將自己的 IP 地址指派給本地用戶作為 DNS 代理伺服器，並保持著 DNS Cache。如果一個功能變數名稱的 IP 位址已經在 DNSCache 內的話，路由器會立刻解析功能變數名稱。否則，路由器會把 DNS 請求封包發送給透過 WAN 連接(比如 DSL/Cable 連線)的外部 DNS 伺服器。

按 **Apply(完成)**並重新啟動系統。

### 5.2.3 2<sup>nd</sup> DHCP Server(第二子網 DHCP 伺服器設定)

Vigor3300 支援第二子網 DHCP 伺服器。

The screenshot shows the 'Network - LAN' configuration page. It has three tabs: 'IP Configuration', '1st DHCP Server', and '2nd DHCP Server' (which is selected). Below the tabs are the following fields:

- Start IP Address: [input field]
- IP Pool Size: [input field]
- MAC Address List (MAC Address Format xx:xx:xx:xx:xx:xx): A table with 10 rows and 2 columns for MAC addresses.

At the bottom right, there are 'Apply' and 'Cancel' buttons.

圖 5-12 第二子網 DHCP 伺服器設定

<b>Start IP Address (起始 IP 位址)</b>	設定起始 IP 位址。
<b>IP Pool Size (IP Pool 大小)</b>	設定一個數字，指定連續 IP 的數量。
<b>MAC Address List (MAC 地址列表)</b>	設定 10 個 MAC 位址。一旦某個 MAC 位址符合此表所列的位址，它將獲得相應的 IP 位址資訊。

按 **Apply(完成)**並重新啟動系統。

## 5.3 Load Balance Policy(負載平衡策略設定)

Vigor3300 支援負載平衡，此功能會指定一個或者一段子網的主機使用某個 WAN 介面，而不受任何負載平衡帶來的影響。



圖 5-13 負載平衡策略

按 **Network>>Load Balance Policy(網路>>負載平衡策略)**，將會顯示出如下頁面。

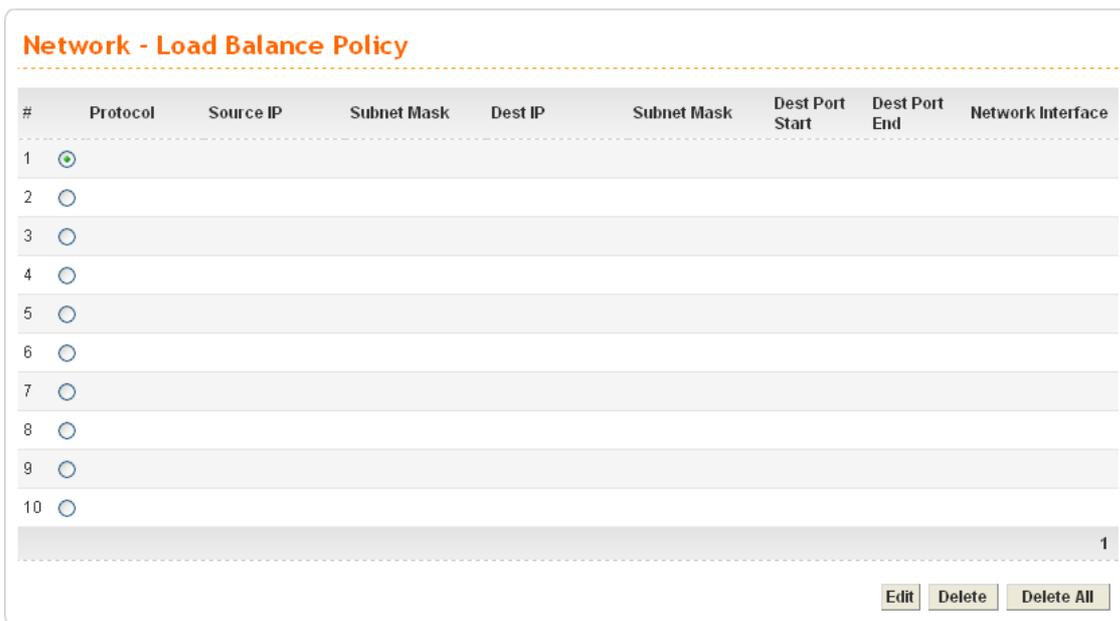


圖 5-14 負載平衡策略表

按第一個項目按鈕，在按下 **Edit(編輯)** 按鈕，可顯示如下頁面。

**Network - Load Balance Policy - Edit**

1

Protocol: TCP

Source IP / Subnet Mask: 192.168.5.1 / 255.255.255.0

Dest IP / Subnet Mask: 192.168.5.100 / 255.255.255.0

Dest Port Range: 100 - 200

Network Interface: WAN1

Apply Cancel

圖 5-15 負載平衡策略 – 編輯

<b>Protocol(協議)</b>	選擇一個協議。
<b>Source IP(來源 IP)</b>	指定一個 IP 位址，用以檢測所有接收封包內的源 IP 位址。
<b>Subnet Mask (子網路遮罩)</b>	指定一個子網路遮罩值。
<b>Dest Port Range(目的埠號範圍)</b>	指定起始和結束埠號。
<b>Network Interface (網路介面)</b>	選擇將要發送到的介面。

按 **Apply(完成)** 以增加或修改該項內容。

此外，按某個項目按鈕，再按刪除，將會顯示出如下提示頁面。



圖 5-16 負載平衡策略 – 刪除

按 **確定**，即可將此項目將從表內刪除。

按 **Delete All(全部刪除)**，系統將刪除此頁面中全部的內容。

## 5.4 High Availability(高可用性設定)

高可用性 (HA) 是關於電腦系統資源的可用性，是有關系統元件出現故障後情況處理的技術。

這並不是一個特殊的技術，但是其目的是在於特殊的商業需求，一個高可用性解決方案的複雜性，取決於公司的可用性需求以及業務可以接受的系統中斷次數。

在某種情況下，系統被設置為提供幾乎全天候可用。這種系統一般都有冗餘的硬體及軟體，使得系統在故障的情況下仍然可用。設計完善的高可用性系統不會只有單一的故障點，任何出現故障的硬體或軟體都會有相同類型的冗餘元件。

當故障發生時，與此同時的進程會交由後備元件進行處理，此過程會保留系統大部分的資源，並復原部分失敗的操作，令系統在幾微秒內恢復正常，高可用性系統可以讓用戶在不知道的情況下完成故障修復操作。

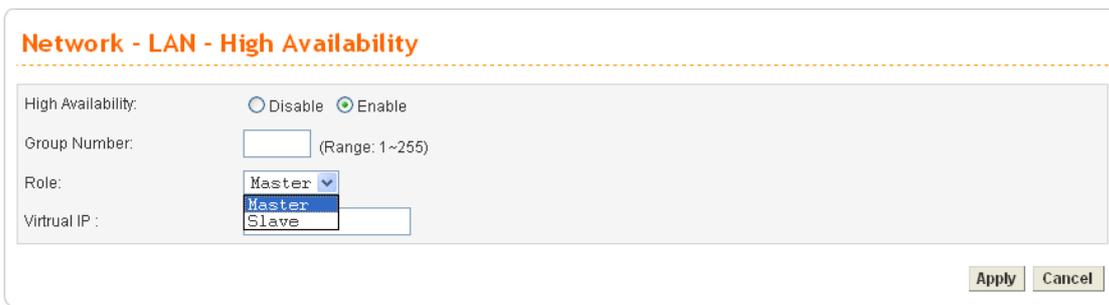
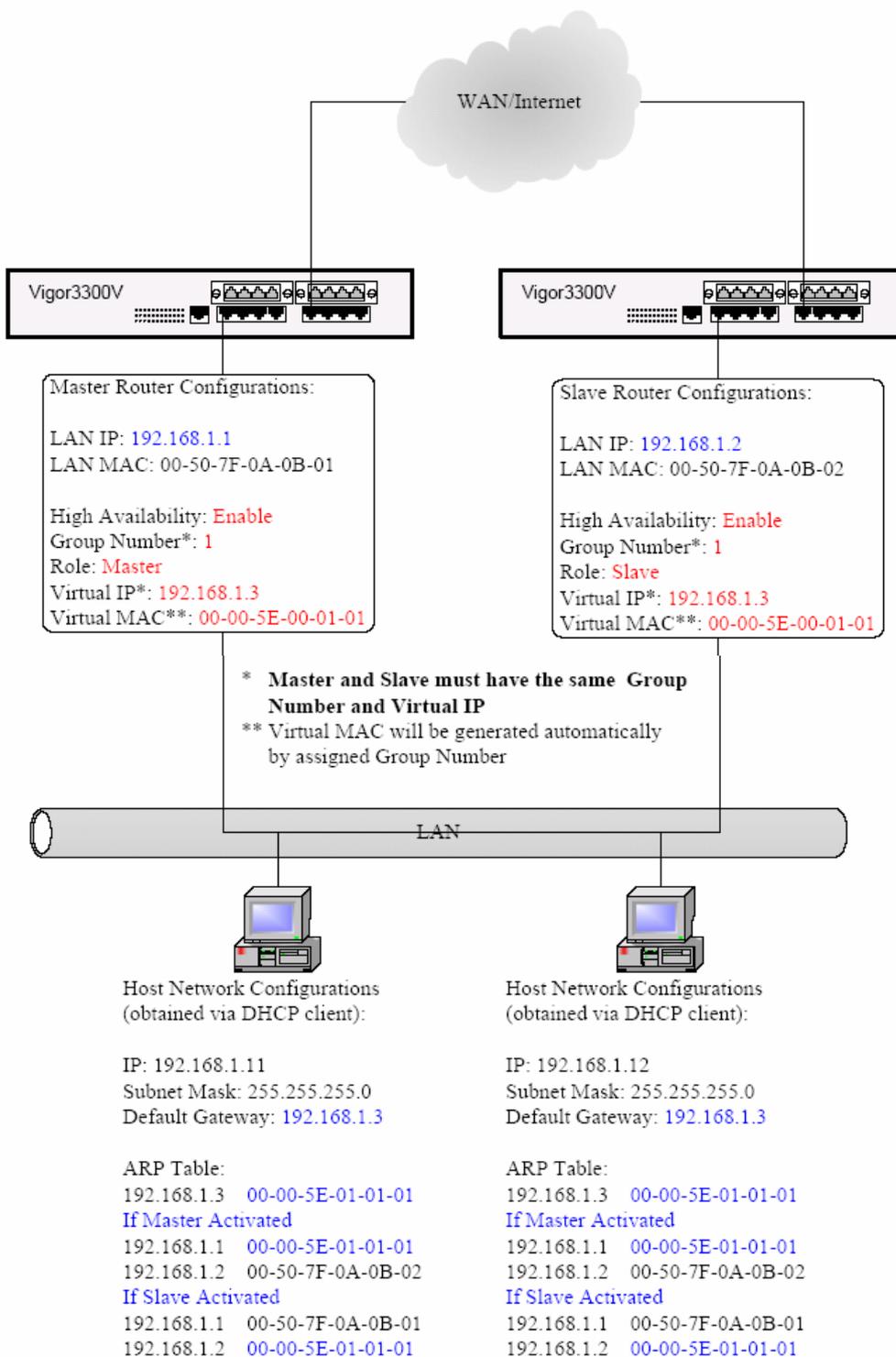


圖 5-17 高可用性設置

<b>High Availability (高可用性)</b>	按 <b>Enable(啓動)</b> 或者 <b>Disable(關閉)</b> 定是否使用此功能。
<b>Group Number (組數)</b>	指派一個組編號，範圍是 1 到 255。
<b>Role(角色)</b>	選擇在高可用性功能內的角色。有如下兩個選項 主：作為主路由器 從：作為從屬路由器 主路由器的優先順序更高
<b>Virtual IP(虛擬 IP)</b>	指派一個虛擬 IP

請按 **Apply(完成)**以使設定生效。



本頁留白

# 第 6 章

## 高級設置

### 6.1 Static Route(靜態路由設定)

用戶可以使用靜態路由功能來指定靜態路由資訊。

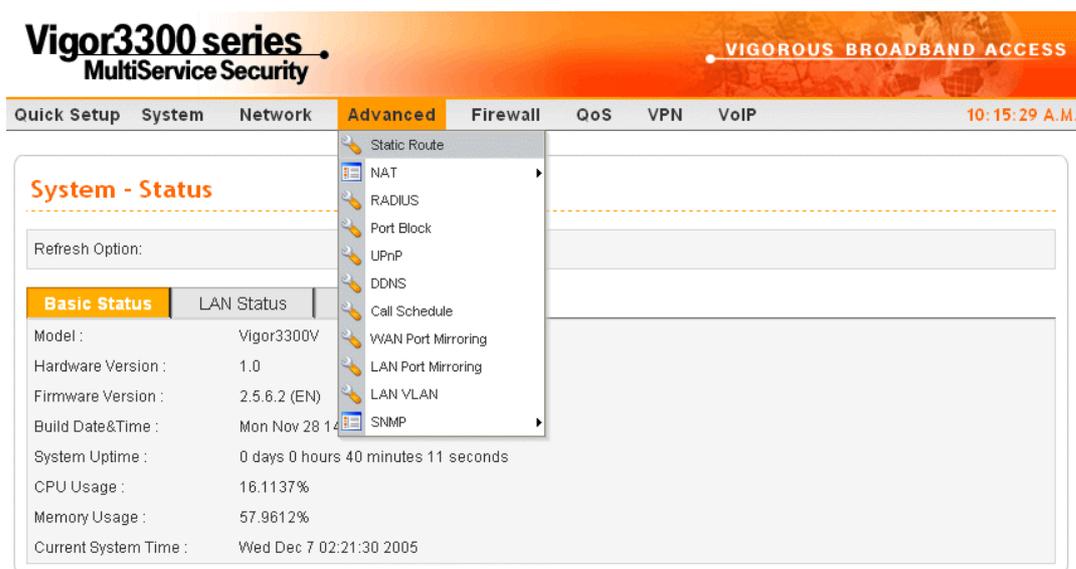


圖 6-1 靜態路由

按 **Advanced>>Static Route(高級>>靜態路由)**，將顯示下面的設置頁面。

Advanced - Static Route				
#	Network Interface	Destination IP	Gateway IP	Mask
1	<input checked="" type="radio"/>			
2	<input type="radio"/>			
3	<input type="radio"/>			
4	<input type="radio"/>			
5	<input type="radio"/>			
6	<input type="radio"/>			
7	<input type="radio"/>			
8	<input type="radio"/>			
9	<input type="radio"/>			
10	<input type="radio"/>			
				1

圖 6-2 靜態路由表

### 6.1.1 Edit(編輯)

按 **Edit(編輯)**可在靜態路由表中新增或編輯一個項目。

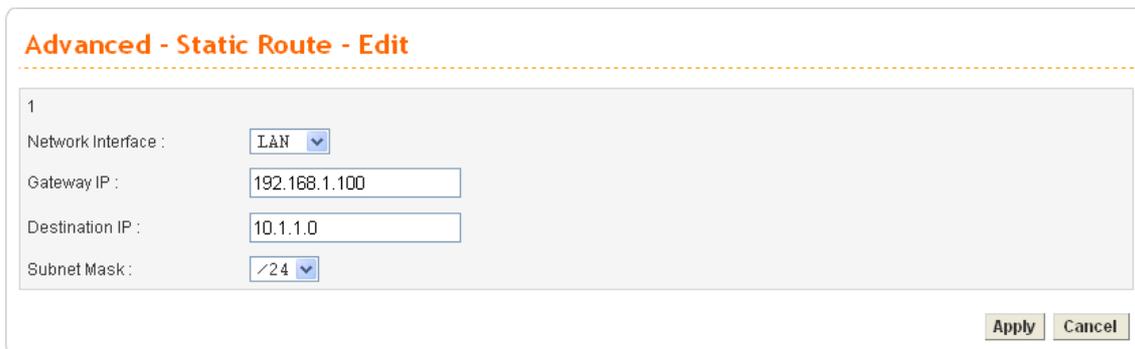


圖 6-3 編輯

<b>Network Interface</b> (網路介面)	選擇發送去目的地的網路介面。它包括 LAN，WAN1~WAN4。
<b>Gateway IP(閘道 IP)</b>	指定閘道的 IP。
<b>Destination IP</b> (目的 IP)	指定目的 IP。
<b>Subnet Mask</b> (子網路遮罩)	指定目的地 IP 的子網路遮罩

按 **Apply(完成)**以完成設置。

### 6.1.2 Delete(刪除)

按 **Delete(刪除)**以刪除路由表中的一個項目。



圖 6-4 刪除選項

請先檢查表中的內容並確認是否要刪除此項目。當用戶想要執行編輯或刪除操作時，用戶必須按項目按鈕再按 **Delete(刪除)**按鈕，然後按**確定**完成刪除。

## 6.2 NAT 設定

NAT（網路位址轉換）是用來映射一個或多個 IP 位址以及服務埠到不同服務的方法。它

使 LAN 中擁有私有網路 IP 的多個電腦能夠轉換到公網 IP 位址以便節省公網 IP 地址的資源。它同時也充當了一個“保安”的角色用來隱藏的 PC 的真實 IP 來防止 Internet 上的駭客攻擊。Vigor3300 預設情況下啓用 NAT 並用靜態，PPPoE，或 DHCP 的機制從 ISP 獲得一個能夠路由的 IP 位址。Vigor3300 根據 RFC-1918 定義的私有網路 IP 來指定私有網路的 IP 位址，並且將私有網路的 IP 位址轉換為一個能夠路由的 IP 位址以實現 Internet 存取。

按 **Advanced>>NAT(高級設置>>NAT)**，將顯示如下頁面。

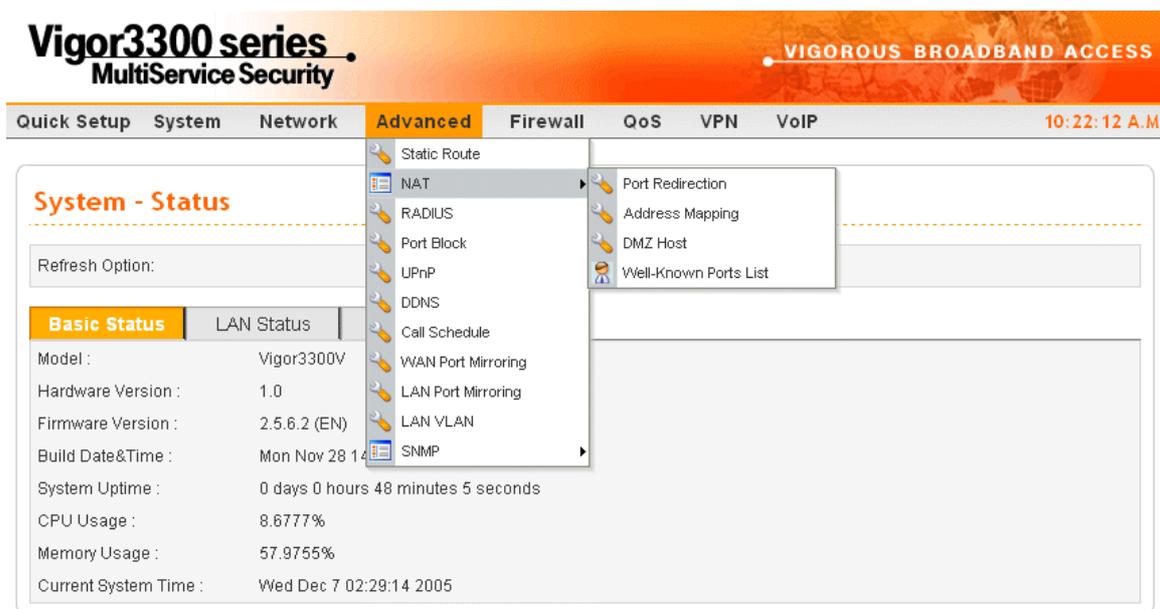


圖 6-5 NAT 功能

### 6.2.1 Port Redirection(埠號重定向設定)

Port Redirection 用來開放內部的伺服器到網際網路或是為內部主機開放指定的埠。Internet 上的主機可以用 WAN IP 位址來存取內部的服務，例如 FTP，WWW 等。下面的例子顯示如何開放 FTP 伺服器到公網。內部的 FTP server 是運行在 192.168.1.2 的一臺本地的主機上。如果埠滿足表中定義的埠，資料封包將轉發到指定的內網主機。用戶也可以進行不同埠之間的轉換。

按 **Advanced>>NAT>> Port Redirection(高級設置>>NAT>>埠號重定向)**，將顯示如下頁面。

#	Comment	Protocol	Public Port Start	Public Port End	Private IP	Private Port Start	Private Port End	Use IP Alias	WAN Interface	IP Alias
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

圖 6-6 NAT-埠號重定向設置

按 **Edit(編輯)** 以新增或修改一條規則。

圖 6-7 編輯一條新規則

<b>Comment(註解)</b>	輸入此項設定相關註解。
<b>Protocol(協議)</b>	指定 TCP 或 UDP 協議。
<b>Public Port Range (公用埠號範圍)</b>	指定起始埠號。
<b>Private IP (私有 IP)</b>	區域網路的 IP 地址。
<b>Private Port Range (私有埠號範圍)</b>	指定本地埠號範圍。
<b>Use IP Alias</b>	選擇 <b>Disable(關閉)</b> 則使用 WAN 介面，

(使用 IP 別名)	選擇 <b>Enable(啓動)</b> 則使用 IP 別名位址。
<b>WAN Interface (WAN 介面)</b>	用戶可以從下拉視窗中選擇一個 WAN 介面。
<b>IP Alias (IP 別名)</b>	用戶可以從下拉視窗中選擇一個分配給 WAN 介面的 IP 別名地址。

按 **Apply(完成)**結束設定。

注意：埠號重定向只對外部用戶有效，內部的用戶不能透過存取外部公有 IP 的方法來存取內部的伺服器，內部的用戶只能透過私有的 IP 來存取內部的伺服器，或者你可以在 Windows 的 hosts 檔中設置一個 alias，只要重定向你所需要的埠號即可，不要重新定向所有的埠號，以免 NAT 固有防火牆功能受到影響。

另外，用戶可以按 **Delete(刪除)**來刪除 NAT 項目。

## 6.2.2 Address Mapping(位址映射設定)

如果您有一組靜態的 IP 位址，那您就能使用位址映射的功能在 Vigor3300 上為特定的一台或多台指定 NAT 使用的公網位址，下面的內容告訴您如何設置位址映射。

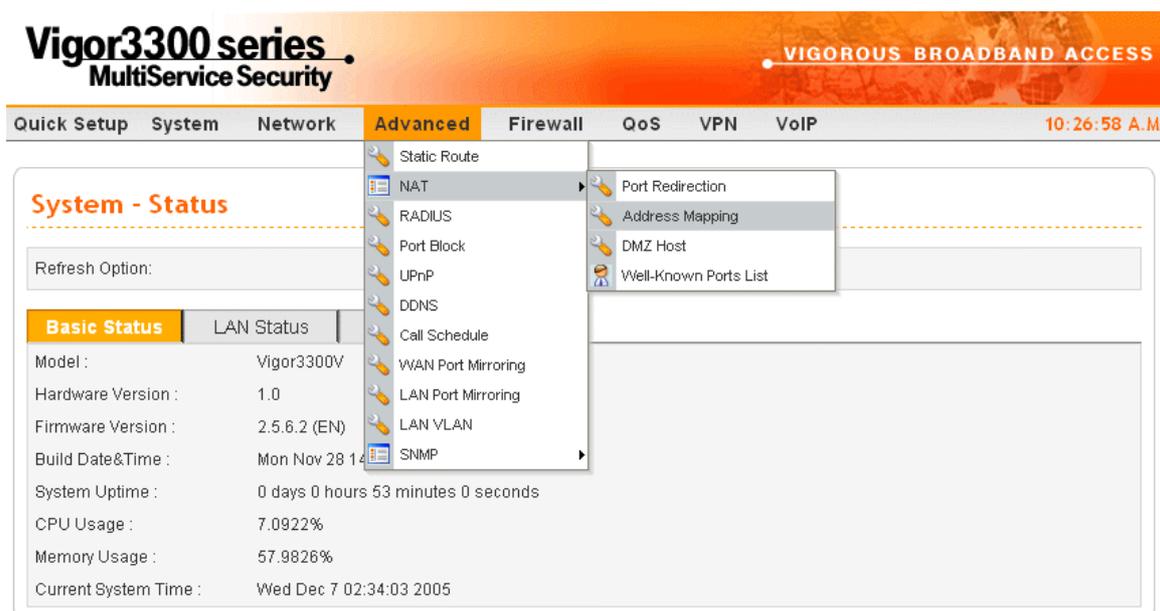


圖 6-8 NAT-位址映射

按 **Advanced>>NAT>>Address Mapping(高級>>NAT>>位址映射)**，將顯示如下頁面。

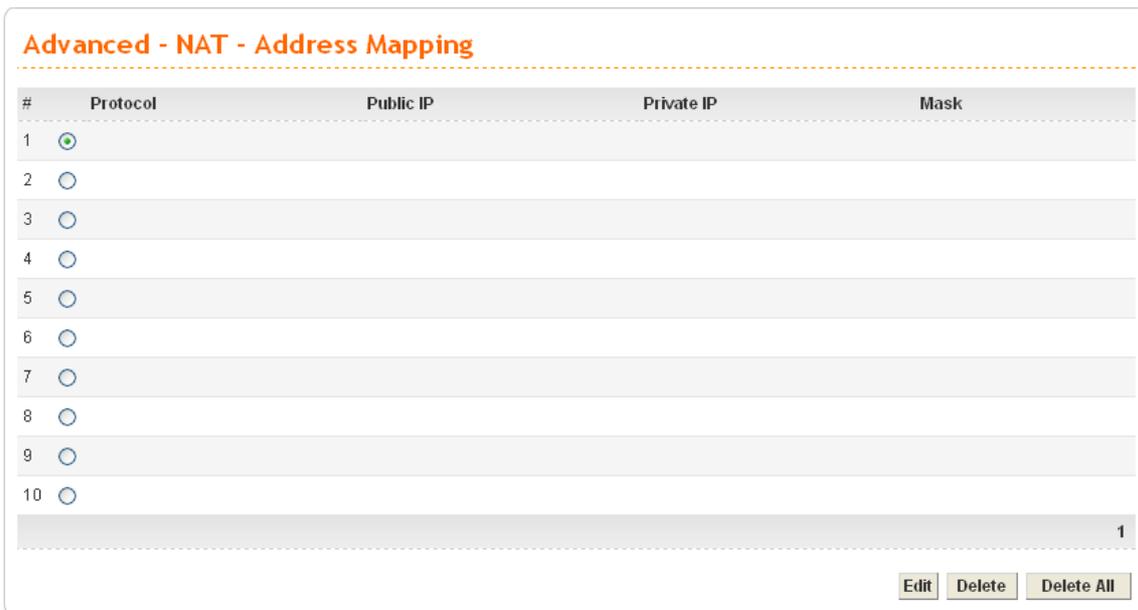


圖 6-9 NAT-位址映射設定

按 **Edit(編輯)** 來新增或者修改一條規則。

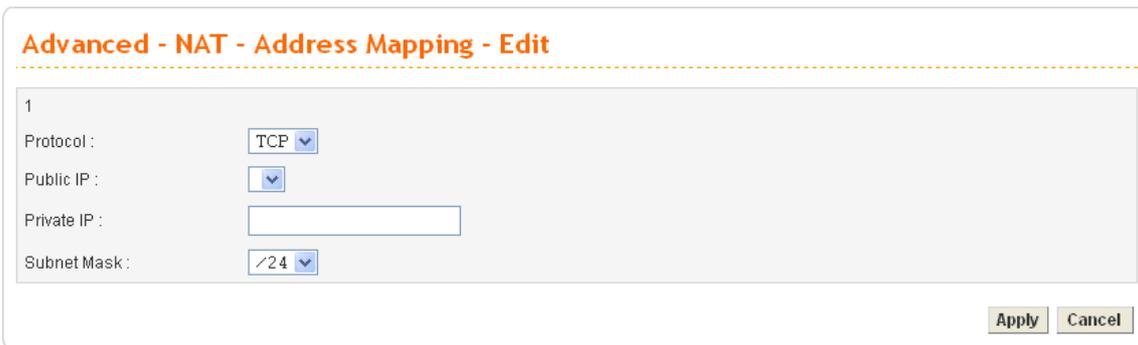


圖 6-10 在位址映射中編輯新規則

<b>Protocol(協議)</b>	指定要求檢查的協議類型。
<b>Public IP(公用 IP)</b>	如果來源 IP 可以滿足私有 IP 中設置的話，請使用此 IP 來改變資料封包的來源 IP 位址。
<b>Private IP(私有 IP)</b>	指定用來比較的 IP 位址或者子網路。當資料封包的來源位址符合該處設定時，則使用“公用 IP”指定的 WAN IP 作為資料封包的來源位址，以進行 NAT 轉換。
<b>Subnet Mask (子網路遮罩)</b>	選擇一個遮罩值。

按 **Apply(完成)** 以結束設置。

另外，用戶可按 **Delete(刪除)** 來刪除 NAT 項目。

### 6.2.3 DMZ 主機設定

在電腦網路中，DMZ 是一個介於公司私有網路和外部公有網路之間的中性區域的主機或小型網路，可防止外部用戶直接存取公司內部的伺服器。DMZ 為選項設定，並有接近防火牆一樣的安全性，也能做為代理伺服器。

在一個典型的小型公司的 DMZ 設置中，一個主機將接受來自私有網路內部用戶的存取請求來存取 Web 站點或其他公網上可以存取的公司。然後 DMZ 主機在公網上發起相應的請求，但是 DMZ 主機不能向私有網路初始請求，它只有轉發的功用。

公司外部的公網用戶只能存取 DMZ 主機，DMZ 比較典型的應用是建構公司的 Web 網頁以便於所有的外部網路能夠存取。如果外部用戶突破 DMZ 主機的安全防線，Web 網頁將會被破壞，但公司其他資訊並不會因此而暴露出去。

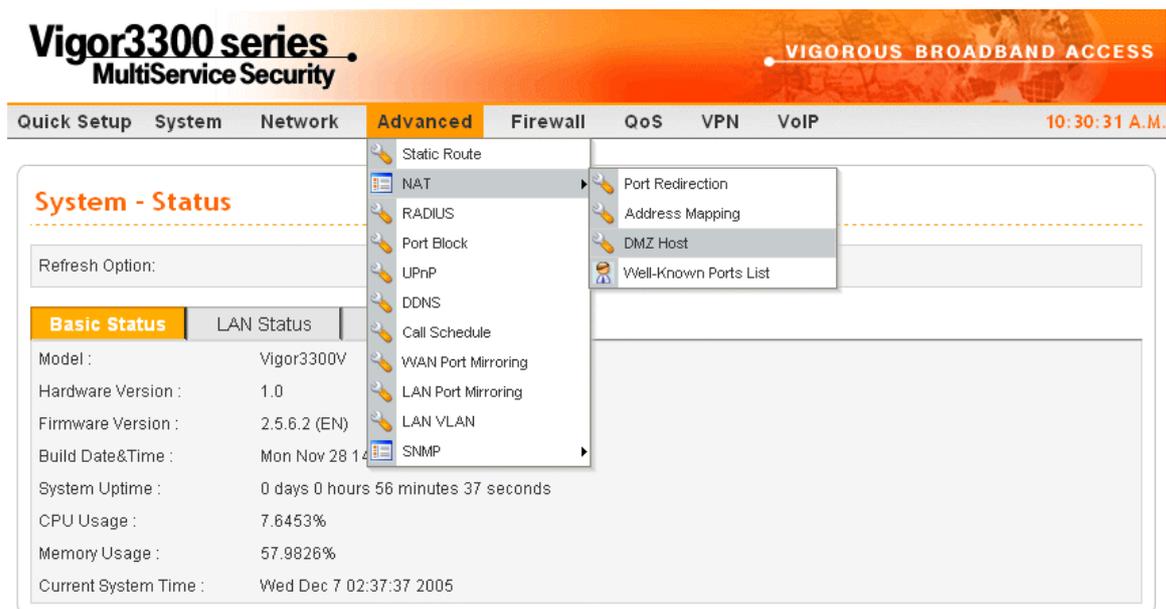


圖 6-11 DMZ 主機

按 **Advanced>>NAT>>DMZ Host**(高級>>NAT>>DMZ 主機)，將會顯示如下頁面。

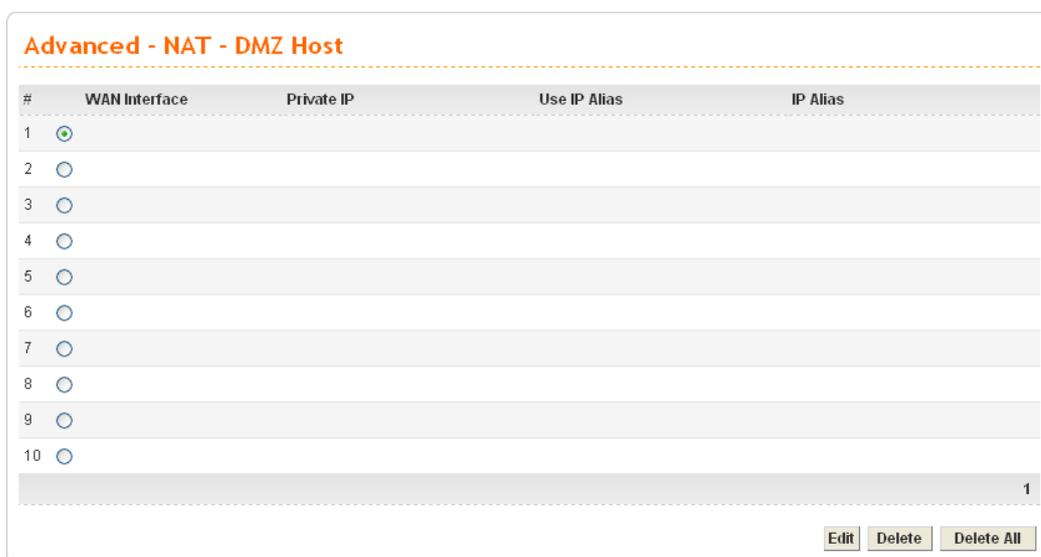


圖 6-12 DMZ 主機表

按 **Edit(編輯)** 新增一個新項目到 DMZ 主機表中。

圖 6-13 DMZ 主機 – 編輯

<b>WAN Interface (WAN 介面)</b>	選擇一個 WAN 介面。
<b>Private IP(私有 IP)</b>	指定 DMZ 可以被外部存取的 IP 位址。
<b>Use IP Alias(用 IP 別名)</b>	選擇 <b>Disable(關閉)</b> 則使用 WAN 介面， 選擇 <b>Enable(啓動)</b> 則使用 IP 別名位址。
<b>IP Alias (IP 別名)</b>	在 WAN 設定頁面的 IP 別名列表中選擇一個 IP 位址。

按 **Apply(完成)** 以結束設置。

按 **Delete(刪除)** 來刪除 DMZ 主機表中的項目。

圖 6-14 DMZ 主機 – 刪除

若您確定刪除，按**確定**以執行刪除動作。

## 6.3 Port Block(埠阻擋設定)

埠阻擋功能能讓用戶設置一些埠號，如果外部網路的埠號與這些指定的埠號相同，這些網路資料將被丟棄。這個功能的優點在於能夠過濾一些不必要的資料或者是 Internet 上的攻擊資料。

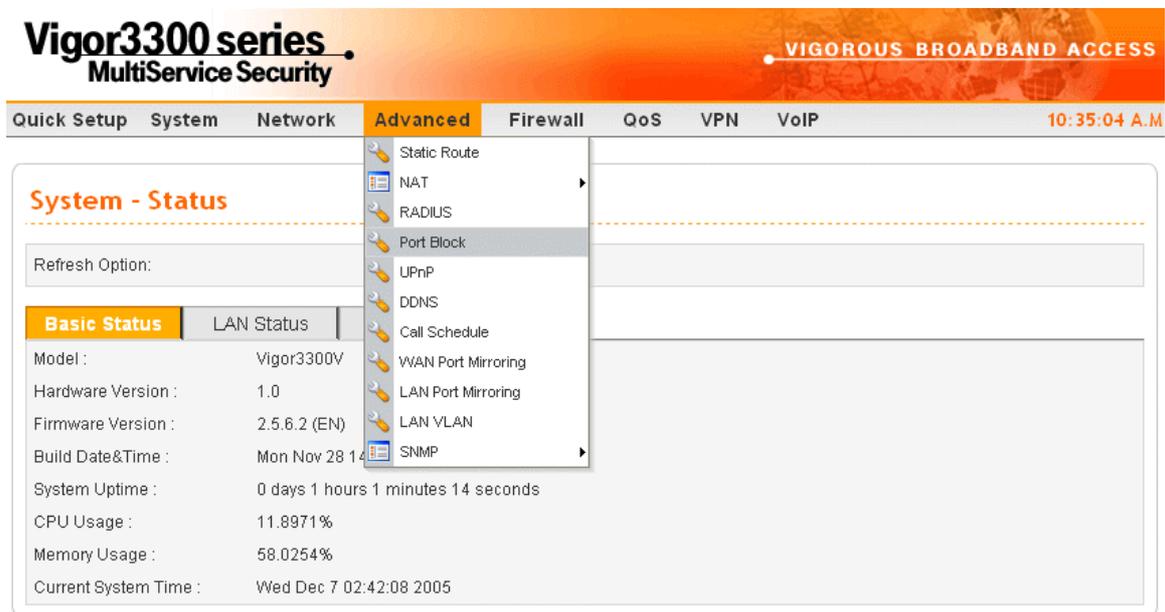


圖 6-15 埠阻擋

Vigor3300 系列支援阻擋 10 個埠號，按 **Port Block(埠阻擋)**，將會顯示如下頁面：

Index	Status	Port Number
1.	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	123
2.	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	568
3.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
4.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
5.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
6.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
7.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
8.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
9.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
10.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	

圖 6-16 埠阻擋設定

<b>Index(索引號)</b>	索引編號。
<b>Status(狀態)</b>	用戶能關閉或是啟動被選擇的項目。
<b>Port Number(埠號)</b>	指定一個被系統阻擋的埠。

按 **Apply(完成)** 來完成設置。

## 6.4 UPnP 設置

UPnP（通用即插即用）協定服務於網路中的即插即用設備，Windows 的即插即用系統為某些 PC 設備提供了此功能。

對於 NAT 路由器，Vigor3300 上的 UPnP 的主要作用是“NAT 穿越”，它意味著防火牆內部的應用程式自動開放埠來穿透路由器，這種機制比路由器自己指定開放埠更加具可行性。而且，用戶也不必用手工設置埠映射或是 DMZ。

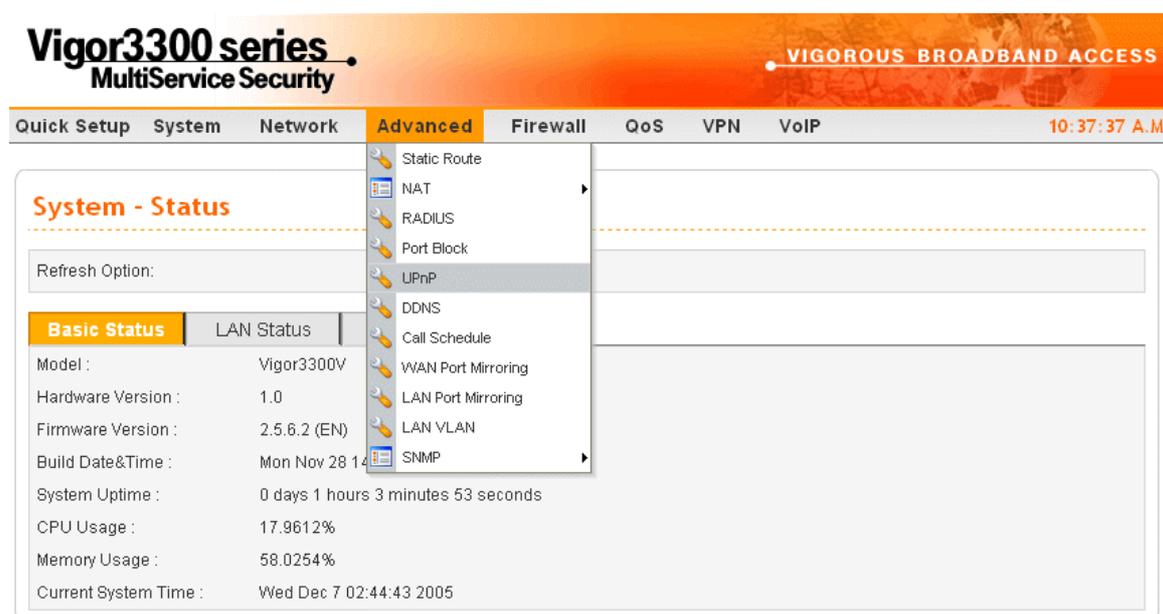


圖 6-17 UPnP

由於使用了 UPnP 功能，Vigor3300 為 Windows XP 用戶提供了便捷的 MSN Messenger 的聲音，視頻和消息的通訊功能，按 UPnP，將會顯示下面的頁面。

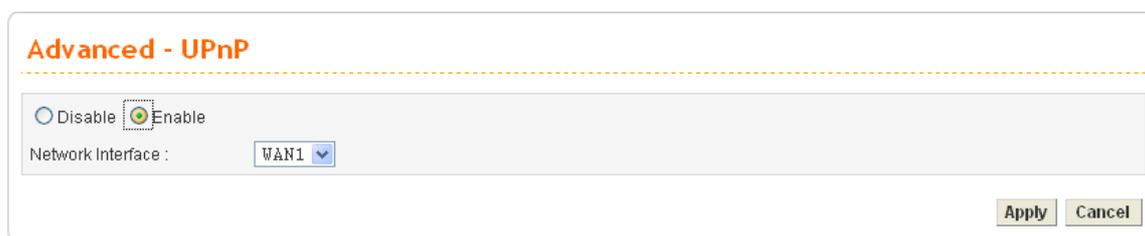


圖 6-18 UPnP 設置

Disable/Enable	點單按鈕來關閉或啓用 UPnP 功能。
網路介面	選擇使用 UPnP 的 WAN 介面。

按 **Apply(完成)** 以完成設置。

在 Windows XP 的網路連接中按 Router 上的 IP Broadband Connection，可以查看連接狀態或控制狀態，如圖 6-19。

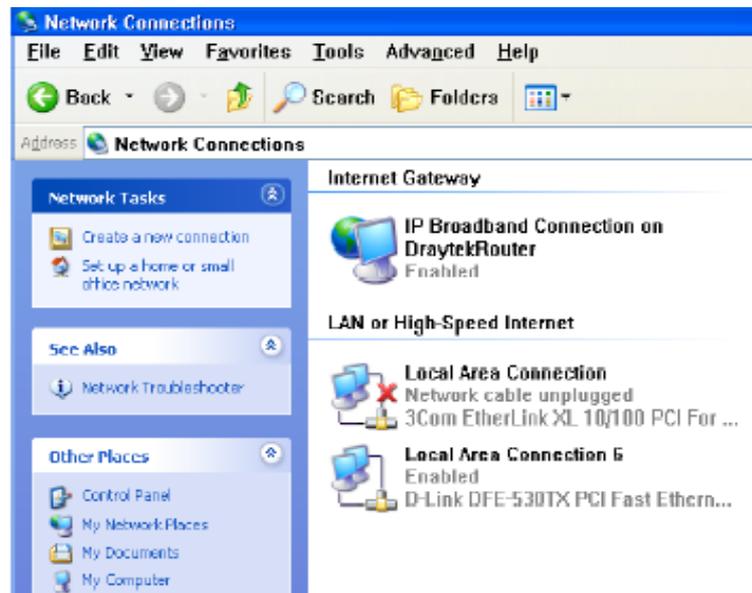


圖 6-19 Windows 網路連接

NAT 的穿越特徵將使您更加方便的啓用應用程式的多媒體功能，沒有 UPnP，您將不得不設置埠映射或手工做其他類似的設置。下面的範例圖是一個例子。



圖 6-20 連接狀態

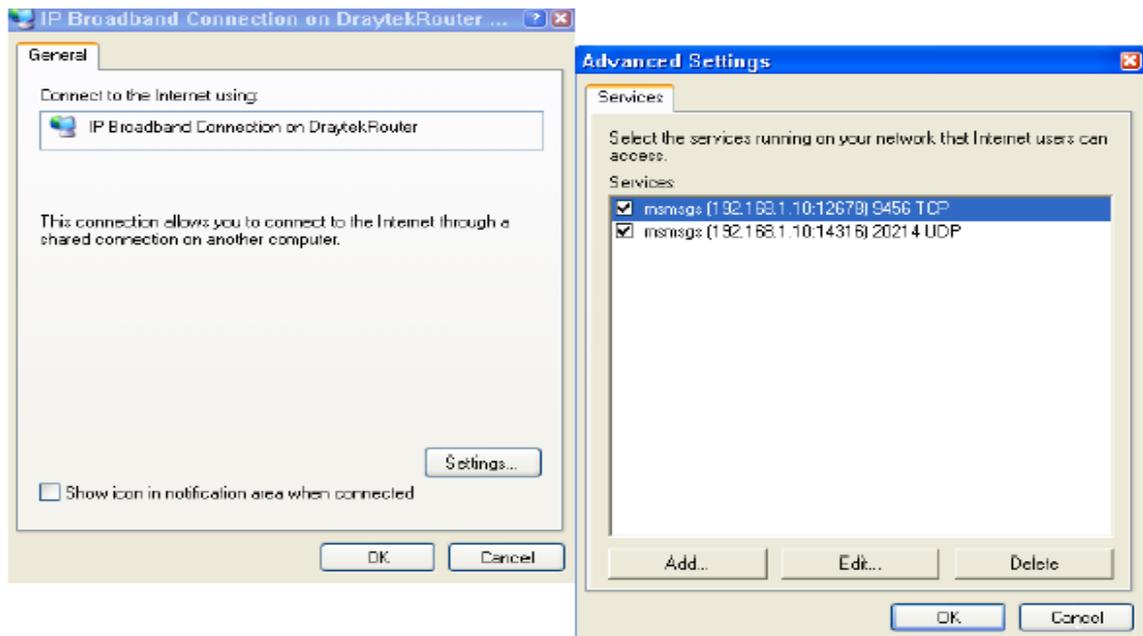


圖 6-21 UPnP 設置

Vigor3300 的 UPnP 功能可以讓支援 UPnP 的應用程式（例如 MSN Messenger）發現外部路由器 IP 位址並為路由器配置埠映射。最後，路由器的 UPnP 工具會重新定向外部埠的資料到內部埠以滿足應用程式的需要。

## 6.5 DDNS 設定

動態 DNS 功能允許路由器到指定的動態 DNS 伺服器即時更新 WAN 介面的線上 IP 位址，這些 WAN 的 IP 位址由 ISP 或 DHCP 分配，一旦路由器上線，你就能用註冊的功能變數名稱從 Internet 上存取路由器或是內部的虛擬伺服器。對動態 IP 的用戶來說，DDNS 是非常受歡迎的，這些動態 IP 的用戶一般是從他們的 ISP 那裡接收動態、改變頻繁的 IP 位址。

在你設置動態的 DNS 功能之前，你必須從動態 DNS 服務供應商那裡預定一個免費的功能變數名稱。路由器支援最多 10 個帳戶，並支援下面的 DNS 服務供應商：

[www.dynsns.org](http://www.dynsns.org)，[www.no-ip.com](http://www.no-ip.com)，[www.dtdns.com](http://www.dtdns.com)，[www.changeip.com](http://www.changeip.com)，[www.dynamic-nameserver.com](http://www.dynamic-nameserver.com)。您應該進入其網站去註冊屬於自己的路由器功能變數名稱。

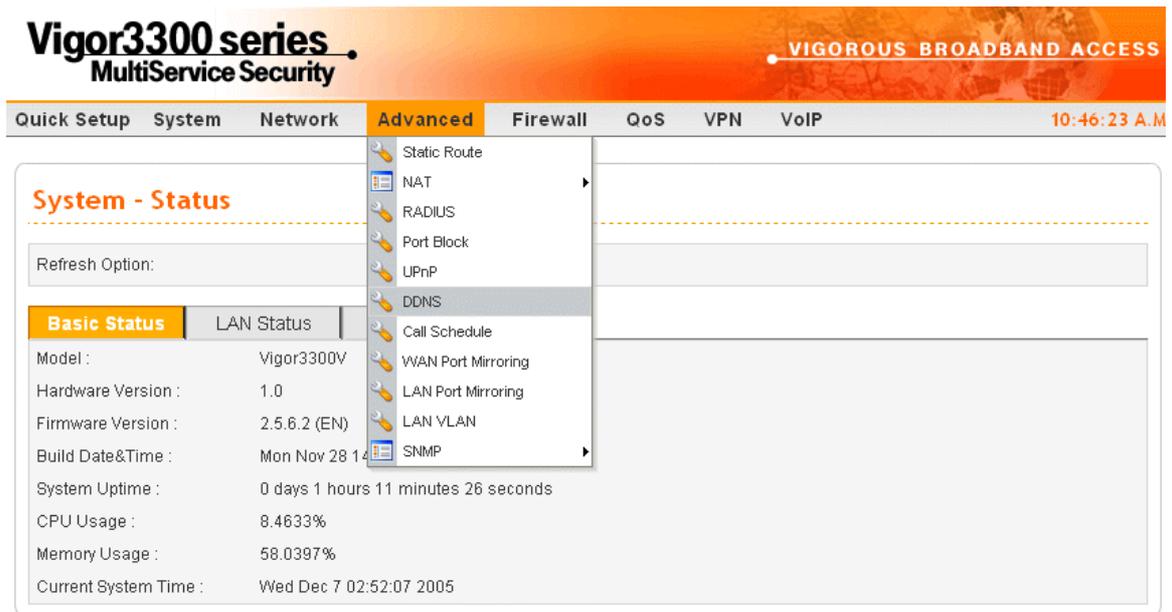


圖 6-22 DDNS

按 DDNS，將顯示如下頁面。

The screenshot shows the 'Advanced - DDNS' configuration page. It features a table with the following columns: #, Domain Name, Server Provider, Server Type, Active, and Status. The table contains 10 rows of data, all with 'dyndns.org' as the domain name and 'dynamic' as the server type. The 'Active' column is set to 'disable' for all entries, and the 'Status' column shows 'Not Connected' for all. A 'Refresh' button is located at the bottom right of the table.

#	Domain Name	Server Provider	Server Type	Active	Status
1	dyndns.org	dyndns.org	dynamic	disable	Not Connected
2	dyndns.org	dyndns.org	dynamic	disable	Not Connected
3	dyndns.org	dyndns.org	dynamic	disable	Not Connected
4	dyndns.org	dyndns.org	dynamic	disable	Not Connected
5	dyndns.org	dyndns.org	dynamic	disable	Not Connected
6	dyndns.org	dyndns.org	dynamic	disable	Not Connected
7	dyndns.org	dyndns.org	dynamic	disable	Not Connected
8	dyndns.org	dyndns.org	dynamic	disable	Not Connected
9	dyndns.org	dyndns.org	dynamic	disable	Not Connected
10	dyndns.org	dyndns.org	dynamic	disable	Not Connected

圖 6-23 DDNS 表

按 **Refresh(更新)**以重新顯示整個頁面資訊。

按對應編號以修改 DDNS 表中該對應項目的設定。

**Advanced - DDNS Setting**

Status :  Disable  Enable

Interface :

Server Provider :

Server Type :

Domain Name :

Login Name :

Login Password :

Wild Card :  Disable  Enable

Backup MX :  Disable  Enable

Mail Extender :

圖 6-24 DDNS 設置

<b>Status(狀態)</b>	按 <b>Disable(關閉)</b> 來關閉該功能。 按 <b>Enable(啓動)</b> 來啓動該功能。
<b>Interface(介面)</b>	從 WAN1 到 WAN4 中選擇一個 DDNS 對應的介面。
<b>Service Provider (服務供應商)</b>	指定一個提供商來支援 DDNS 服務。Vigor3300 預設支援 5 個功能變數名稱提供商。
<b>Server Type(伺服器類型)</b>	選擇靜態，動態或定制。
<b>Domain Name(網域名稱)</b>	指定可以存取的網域名稱。
<b>Login Name(登錄名)</b>	指定登錄到 DDNS 伺服器的名字。
<b>Login Password (登錄密碼)</b>	指定登錄到 DDNS 伺服器的密碼。
<b>Wild Card</b>	按 <b>Disable(關閉)</b> 來關閉該功能。 按 <b>Enable(啓動)</b> 來啓動該功能。
<b>Backup MX</b>	按 <b>Disable(關閉)</b> 來關閉該功能。 按 <b>Enable(啓動)</b> 來啓動該功能。
<b>Mail Extender</b>	指定一個郵件位址。

附註：並不是所有的動態 DNS 提供商都支援 Wild Card 和 Backup MX 功能，請自其網站獲得更詳細的資訊。

如果您的主郵件伺服器因為某種原因無法上線的話，Backup MX 將提供給您第二個郵件伺服器來保留 email。一旦你恢復連線，你的 email 將遞送給您。

按 **Apply(完成)**以完成設定。

**Advanced - DDNS**

#	Domain Name	Server Provider	Server Type	Active	Status
1	draytek	dyndns.org	dynamic	enable	Not Connected
2		dyndns.org	dynamic	disable	Not Connected
3		dyndns.org	dynamic	disable	Not Connected
4		dyndns.org	dynamic	disable	Not Connected
5		dyndns.org	dynamic	disable	Not Connected
6		dyndns.org	dynamic	disable	Not Connected
7		dyndns.org	dynamic	disable	Not Connected
8		dyndns.org	dynamic	disable	Not Connected
9		dyndns.org	dynamic	disable	Not Connected
10		dyndns.org	dynamic	disable	Not Connected

[Refresh](#)

圖 6-25 DDNS 表

## 6.6 RADIUS 設置

RADIUS 是安全的伺服器/用戶端驗證協定，並被 ISP 廣泛使用於其他的遠端存取服務，RADIUS 是驗證並授權撥號和隧道用戶的最常見的方法。內建的 RADIUS 用戶端功能允許你擴充遠端撥入用戶的帳號到 RADIUS 的伺服器上，你的用戶帳號不會僅僅局限於內建的帳號，它也能讓你在網路裡集中管理遠端存取的驗證。

Radius 是管理遠端用戶驗證和計帳的伺服器，主要用於 ISP，不過它也被用於需要集中管理驗證和計帳服務的網路上。Radius 支持廣泛的驗證機制，用戶可以透過直接回答終端伺服器的登錄/密碼提示，使用 PAP 或 CHAP 協定等方式來提供驗證資料。

Vigor3300 為用戶提供 Radius 設定，我們可配置一些驗證資訊讓 Radius 伺服器來進行驗證，在 Vigor 3300 中只適用於 VPN>>PPTP 功能。

**Vigor3300 series**  
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network **Advanced** Firewall QoS VPN VoIP 10:51:48 A.M

**System - Status**

Refresh Option:

**Basic Status** LAN Status

Model : Vigor3300V  
Hardware Version : 1.0  
Firmware Version : 2.5.6.2 (EN)  
Build Date&Time : Mon Nov 28 14:00:00 2005  
System Uptime : 0 days 1 hours 17 minutes 42 seconds  
CPU Usage : 29.8701 %  
Memory Usage : 58.0468 %  
Current System Time : Wed Dec 7 02:58:16 2005

- Static Route
- NAT
- RADIUS**
- Port Block
- UPnP
- DDNS
- Call Schedule
- WAN Port Mirroring
- LAN Port Mirroring
- LAN VLAN
- SNMP

圖 6-26 Radius

按 **Advanced>>Radius**，將顯示如下頁面。

圖 6-27 Radius 設置

<b>Disable/Enable</b>	按 <b>Disable(關閉)</b> 以關閉此功能。 按 <b>Enable(啟動)</b> 來啟動該功能。
<b>Server IP Address</b> (伺服器 IP 地址)	指定 Radius 伺服器的 IP 地址。
<b>Destination Port(目的埠)</b>	指定 Radius 功能使用的目標埠。
<b>Shared Secret(共用密鑰)</b>	為伺服器指定一個驗證的代碼。
<b>Confirm Shared Secret</b> (重新輸入共用密鑰)	重新輸入共用密鑰中的內容。
<b>WAN Interface</b> (WAN 介面)	指定將要使用的 WAN 介面

按 **Apply(完成)**以完成設定。

## 6.7 Call Schedule(撥號計畫時間表設定)

撥號計畫時間表用配置檔的設置來控制路由器的撥號或連接管理連線或斷線的時間，在配置撥號計畫時間表功能前，用戶必須正確的設置時間，並為 Internet 存取的配置或 LAN-to-LAN 的配置安排時間表。

Vigor 3300 支援配置大量的撥號計畫時間表配置。

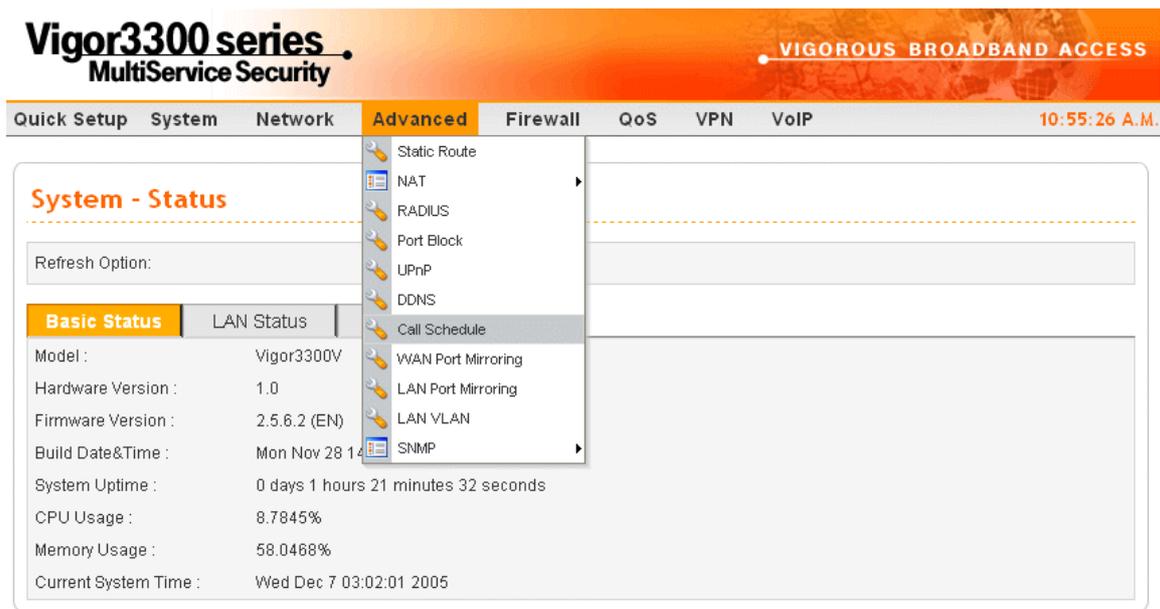


圖 6-28 撥號計畫時間表

按 **Call Schedule**(撥號計畫時間表)，將顯示如下頁面。

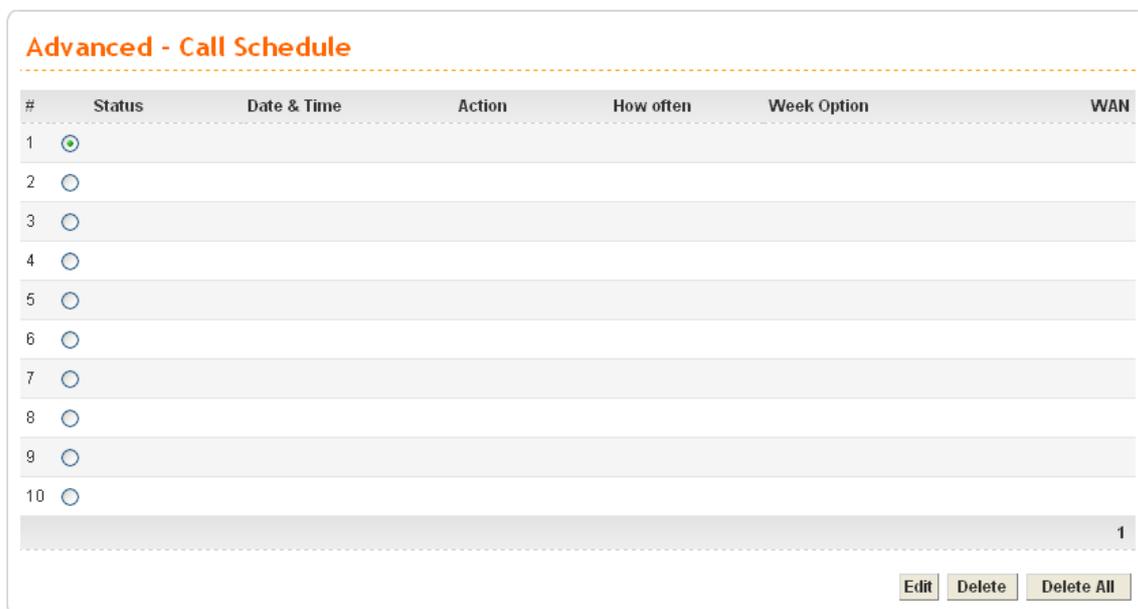


圖 6-29 撥號計畫時間表設置

### 6.7.1 Edit(編輯)

按 **Edit**(編輯)新增一項記錄。

**Advanced - Call Schedule - Edit**

Disable  Enable

Start Date :      2005 - 12 - 7 (Year - Month - Date)

Start Time :      00 : 00 (Hour : Minute)

Action :             Force Down  Force On

How often :         Once  Weekdays

Monday  Tuesday  Wednesday  Thursday  Friday  Saturday  Sunday

Network Interface

圖 6-30 撥號計畫時間表- 編輯

<b>Disable/Enable</b>	按 Disable(關閉)以關閉此功能。 按 Enable(啓動)以啓動此功能。
<b>Start Date(開始日期)</b>	指定開始的日期。
<b>Start Time(開始時間)</b>	指定開始的時間。
<b>Action(動作)</b>	Force Down(強制斷線)代表強制網路離線。 Force On(強制連線)則表示強制聯網。
<b>How often(使用頻率)</b>	Once(一次)代表只使用一次。 Weekdays(日期)則表示用戶可以選擇一周的某幾天。
<b>Network Interface (網路介面)</b>	選擇將要應用的 WAN 介面。

按 **Apply**(完成)以完成設置。

### 6.7.2 Delete(刪除)

按 **Delete**(刪除)以刪除一個選取項目。

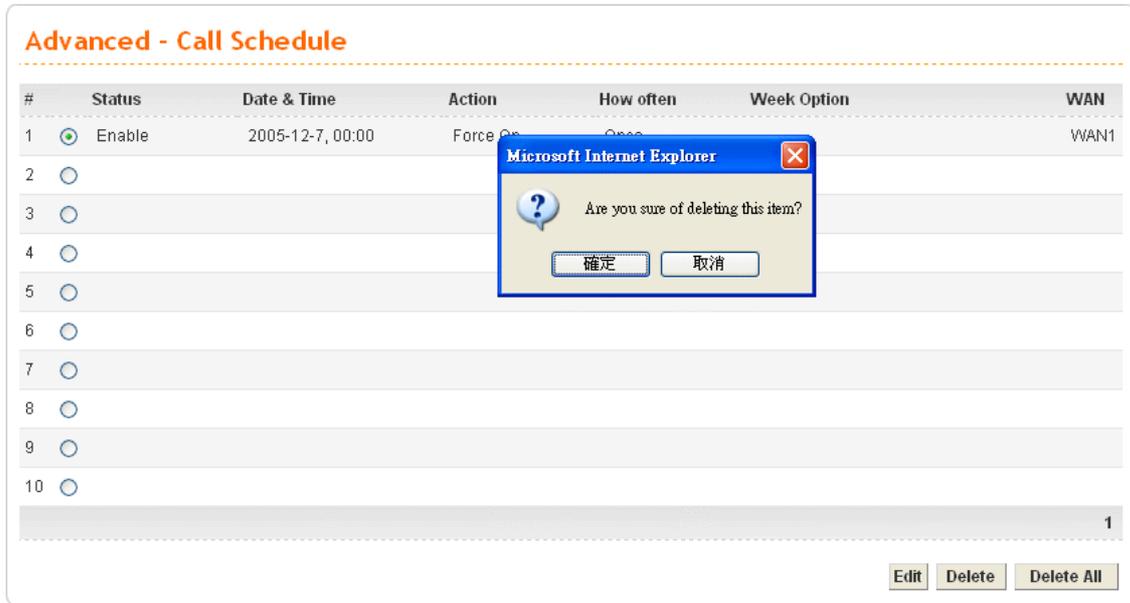


圖 6-31 撥號計畫時間表 – 刪除

按 **Apply(確定)**以完成刪除。

本頁留白

# 第 7 章

## 防火牆設置

### 7.1 序言

Vigor 的防火牆設置主要包含資料封包過濾、拒絕服務(DoS)防禦和 URL (Universal Resource Locator 統一資源定位)內容過濾工具。防火牆功能不僅可保護您的內部網路免受來自外部的攻擊，也提供了一種方法來限制本地網路的用戶存取 Internet。並且，它能夠過濾掉一些特殊的資料封包，防止它們觸發路由器進行撥號連接。

資料封包過濾功能包含兩種類型的過濾：呼叫過濾和數據過濾。呼叫過濾用於那些企圖建立一條從區域網路端到 Internet 的連接的用戶。在 WAN 連接已經建立的時候，資料過濾用來決定哪些種類的 IP 資料封包被允許透過路由器。

當一個外出的資料封包將要被路由到 WAN 時，IP 過濾將決定該資料封包是否應該被轉到呼叫過濾或資料過濾。

- 如果 WAN 連結還沒建立，資料封包將進入呼叫過濾；如果該資料封包不被允許觸發路由器撥號，它將被丟棄。否則將發起一個連接來建立 WAN 連接。
- 如果 WAN 連結已經建立，資料封包將透過資料過濾。如果該資料封包類型被設置為阻擋型態，該資料封包將被丟棄，否則它將被發送到 WAN 介面。相反地，如果一個資料封包從 WAN 介面進入，它將直接透過資料過濾。若是該資料封包類型被設置為阻擋型態，則該資料將被丟棄，否則就被發送到內部網路。過濾結構如圖 7-1 所示。

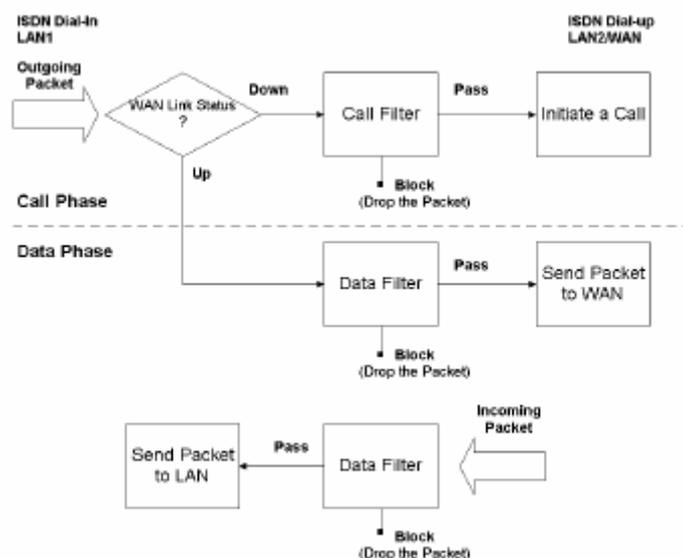


圖 7-1 資料封包過濾功能的過濾結構

在啓用防火牆功能的 IP 過濾前，用戶必須創建一組過濾設定，該組包含許多過濾規則。過濾規則可以連結到子組中以便進行進一步的過濾處理，這些設定組將排列並維護過濾規則。您必須選擇一個起始組並指派其他組作為下一個組，或在過濾規則裡分支到另一個組，原理如圖 7-2 所示。

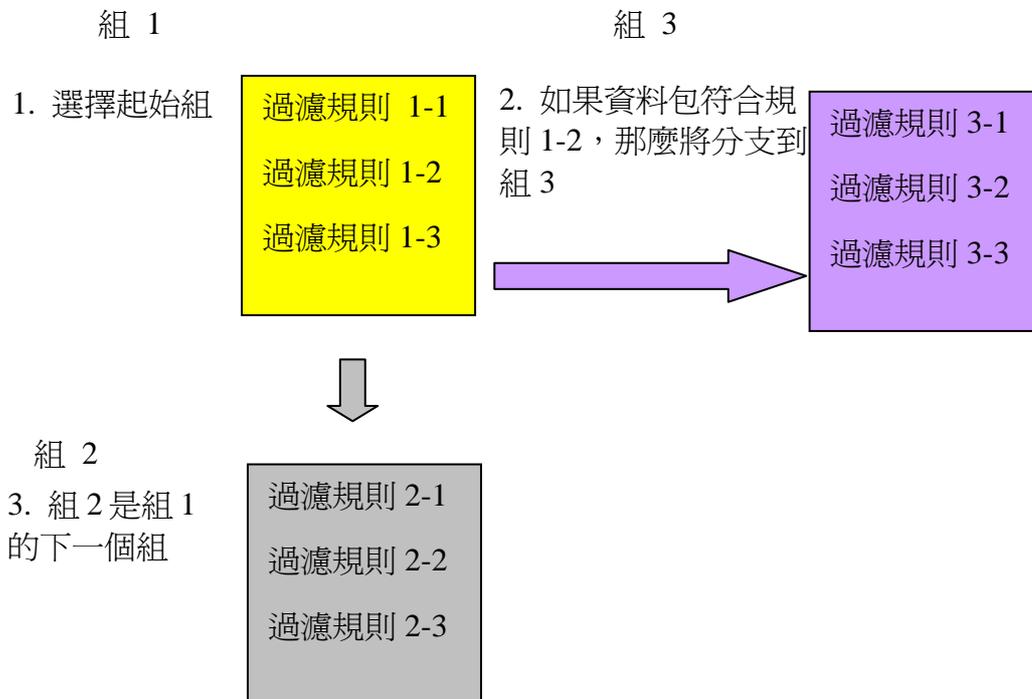


圖 7-2 過濾規則組的原理

## 7.2 防火牆設定概述

以下部分將介紹如何配置防火牆，在 Web 配置介面按防火牆，您可以看到 IP 過濾，DoS 和 URL 過濾。首先您必須在 IP 過濾 > 組列表裡建立至少一個設定組，然後您就能夠啓用資料過濾並在基本設置裡選擇起始過濾組。DoS 防禦功能能夠偵測並減輕 DoS 攻擊，URL 過濾則提供了阻擋不恰當網站的能力，以保護在學校或家裡的小孩。

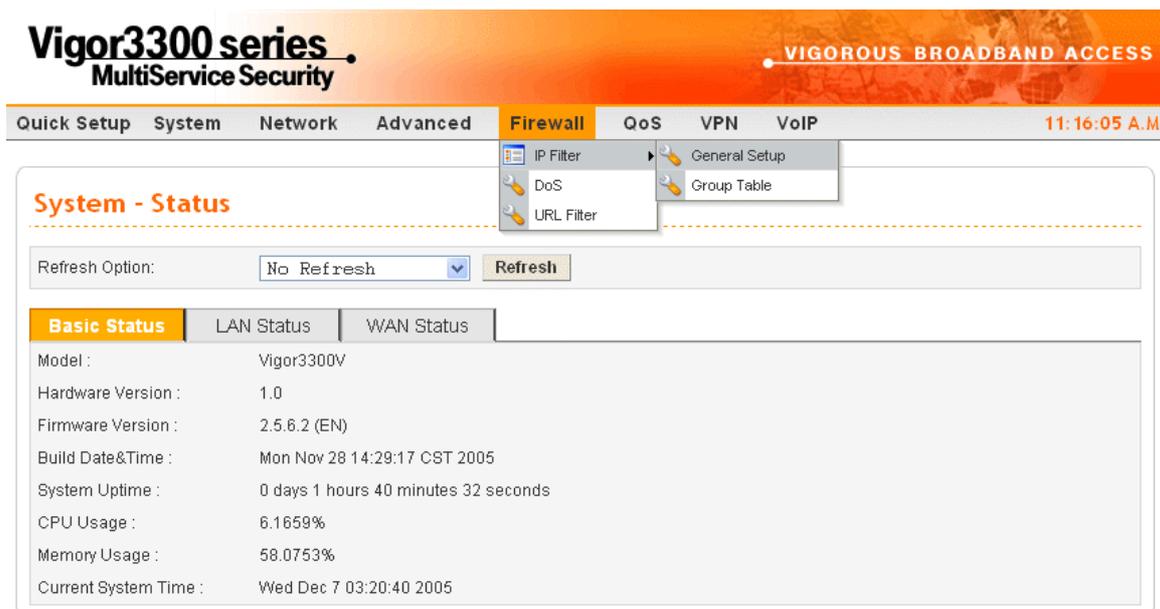


圖 7-3 防火牆位置

## 7.3 IP Filter (IP 過濾設定)

以下部分詳細解釋了 IP 過濾功能。

### 7.3.1 General Setup(基本設定)

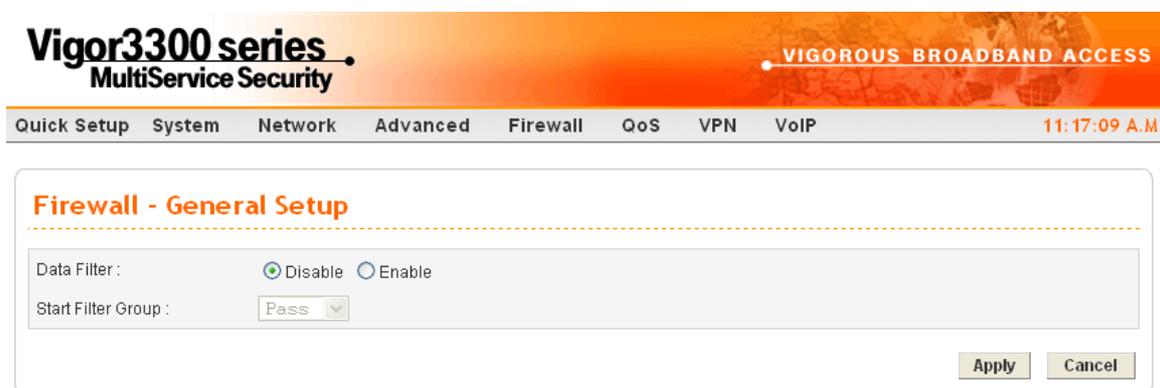


圖 7-4 基本設定

<b>Data Filter</b> (數據過濾)	選擇 <b>Disable(關閉)</b> 或 <b>Enable(啓用)</b> 。如果有多於一個組時，該功能是可選擇的。
<b>Start Filter Group</b> (起始過濾組)	選擇過濾啓動的第一組。在此列表裡的組必須預先配置。

## 7.3.2 Group Table(組列表設定)

按“組列表”，將顯示以下頁面。

IP Filter Group Table			
Index	Group Name	Next Group	Comment
1	Pass	Block	Group for pass rules
2	Block	none	Group for block rules

Add Edit Delete

圖 7-5 組列表配置

按 **Add(新增)**以新增一個新的組。在 **Group Name(組名稱)**、**Next Group(下一組)**和 **Comment(注意)**欄裡填入相應的資訊，然後按 **Apply(完成)**以保存設定，或按 **Cancel(取消)**以放棄設定。

Group Name :

Next Group Name :

Comment :

Apply Cancel

圖 7-6 IP 過濾表 – 新增

<b>Group Name(組名)</b>	為組指定一個名稱。
<b>Next Group Name (下一組名稱)</b>	下一組指示了資料封包在和目前規則組比較完成後下一個將要比較的 IP 過濾規則組。
<b>Comment(注意)</b>	規則組別的注意事項。

按 **Apply(完成)**以完成設定。

按 **Edit(編輯)**以修改 IP 過濾表格配置，您就能更改該螢幕的任意設定。

Group Name :

Next Group Name :

Comment :

Apply Cancel

圖 7-7 IP 過濾表 – 編輯

注意：在編輯模式下用戶不能修改組名欄位。

按 **Apply(完成)**以完成設定。

按 **Delete(刪除)**以移除 IP 過濾表格配置裡某組設定。



圖 7-8 IP 過濾表 – 刪除

注意：如果該項目已經被指定為啟動組，我們就不能刪除該項目，除非我們在基本設定頁面裡關閉資料過濾功能。

### 7.3.3 新增過濾規則設置(找不到可設定之處)

當您新增一組防火牆設定名稱之後，請按該新名稱之索引號碼，進入如下畫面。

Firewall - IP Filter Table

Group Name :

Next Group Name :

Comment :

按下 **Add Rule(新增規則)**按鈕開啓過濾規則設定頁面。

圖 7-9 IP 過濾配置

<b>Source(來源)</b>	
<b>IP(來源 IP)</b>	該欄指定了將被該過濾規則應用到的一個源 IP 位址。在一個特殊的 IP 位址前放置一個符號“!”將防止該規則被應用到該 IP 地址。它等同於邏輯操作符 NOT。
<b>Subnet Mask (子網路遮罩)</b>	該項目為源 IP 指定子網路遮罩。
<b>Port(來源埠)</b>	該項目為源 IP 指定埠。
<b>Destination (目的)</b>	
<b>IP(來源 IP)</b>	該欄指定了將被該過濾規則應用到的一個目標 IP 位址。在一個特殊的 IP 位址前放置一個符號“!”將可防止該規則被應用到該 IP 地址。它等同於邏輯操作符 NOT。
<b>Subnet Mask (子網路遮罩)</b>	該欄指定了該過濾規則將要應用到的目標 IP 列的子網路遮罩。
<b>Port(目的埠)</b>	該項目為目標 IP 指定埠。
<b>Group Name(組名)</b>	該名稱指定了目前規則所屬的組。
<b>Protocol(協議)</b>	該項目指定了該過濾規則使用的協定。
<b>Direction(方向)</b>	該項目設置了資料流程的方向，進入資料封包為 IN，外出資料封包為 OUT，同時兩個方向為 Any。
<b>Fragement(碎片)</b>	指定了一個對分片的資料封包行為。有如下三個選項。 <b>忽略</b> ：指定了在該過濾規則裡沒有分片選項。 <b>非分片</b> ：將此規則應用到未分片的資料封包。 <b>分片</b> ：將此規則應用到分片的資料封包。
<b>Action(啓用)</b>	選此項目以啓用該功能。

<b>Block or Pass</b> (阻擋或通過)	<p>指定了對符合規則的資料封包將要採取的操作。有如下三個選項。</p> <p><b>阻擋</b>：符合該規則的資料封包將被立刻丟棄。</p> <p><b>通過</b>：符合該規則的資料封包將可立刻通過。</p> <p><b>如無其他符合則阻擋</b>：一個符合目前規則，而不符合進一步深層規則的資料封包將被丟棄。</p> <p><b>如無其他符合則通過</b>：一個符合目前規則，而不符合進一步深層規則的資料封包則可通過。</p>
<b>Next Group Name</b> (下一組名)	<p>選擇下一個規則組的名稱。如果您在“阻擋或透過”裡選擇了<b>如無其他符合則阻擋</b>或<b>如無其他符合則透過</b>，資料封包將在下一個組裡與其他規則進行比較。但是如果您選擇了<b>阻擋</b>或<b>透過</b>，該設定將被忽略。</p>

## 7.4 DoS(拒絕服務攻擊設定)

DoS 防禦功能幫助您偵測並減輕 DoS 攻擊，攻擊包括淹沒類型的攻擊和弱點攻擊。淹沒類型的攻擊企圖耗盡您系統的資源，而弱點攻擊試圖透過攻擊協定或作業系統的弱點以使系統癱瘓。

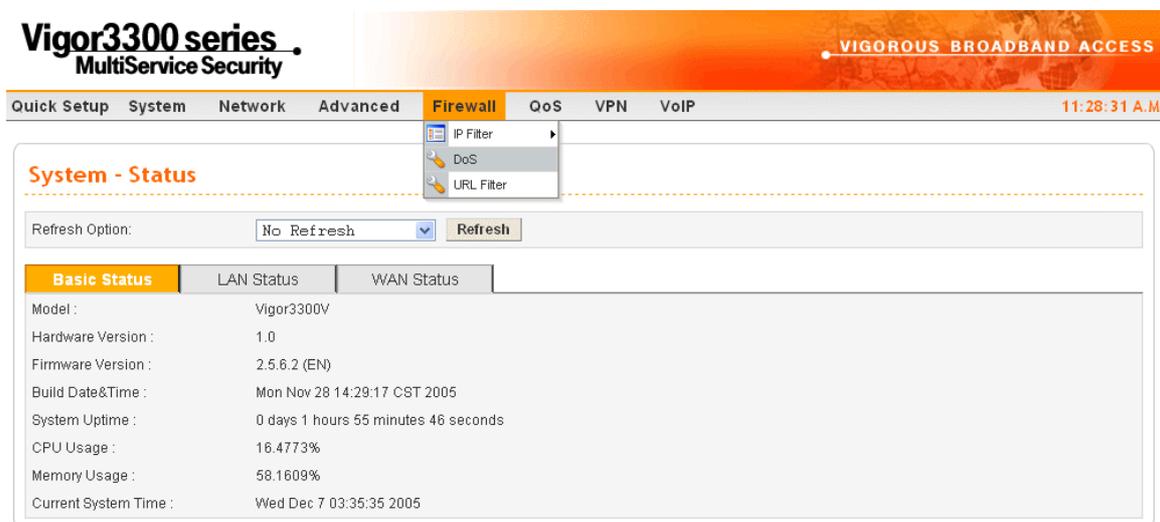


圖 7-10 DoS 位置

按 DoS 項目，將顯示以下頁面。

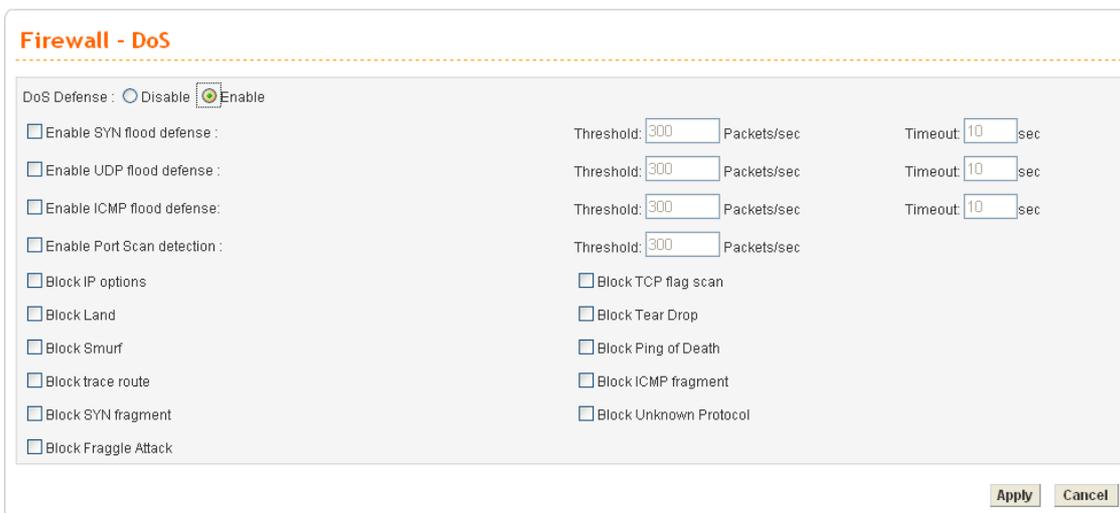


圖 7-11 DoS 設定

DoS 防禦機根據攻擊信號資料庫檢查每一個進入的資料封包，任何可能使安全區域裡的主機癱瘓的資料封包將被阻擋，DoS 防禦機也監控傳輸行為，任何違反 DoS 配置的異常狀況都將被報告出來，系統將執行相應的防禦功能以減輕攻擊。

下面將更詳細地說明如何應用 Web 配置工具來設置 DoS 防禦，這是 IP 過濾的子功能，共有 15 種防禦功能可應用於 DoS 防禦設置。DoS 防禦功能預設值是關閉的。此外，一旦 DoS 防禦功能被啟用，在某些功能裡存在的 threshold 和 timeout 預設值被分別設置為每秒和每 10 秒有 300 資料封包，對 DoS 防禦功能裡每個項目的簡短描述如下所示。

<b>DoS Defense(DoS 防禦)</b>	選擇 <b>Enable(啟動)</b> 以啟用 DoS 防禦功能。
<b>Enable SYN flood defense (啟用 SYN flood 防禦)</b>	勾選該核取方塊以啟用 SYN flood 防禦功能。如果來自 Internet 的 TCP SYN 資料封包數量超過用戶定義的臨界值，路由器將在用戶定義的 timeout 期間強制任意丟棄後續的 TCP SYN 資料封包。它的主要目標是保護路由器，防止那些企圖耗盡路由器有限資源的 TCP SYN 資料封包。threshold 和 timeout 的預設值分別為每秒和每 10 秒有 300 資料封包。
<b>Enable UDP flood defense (啟用 UDP flood 防禦)</b>	勾選該核取方塊以啟用 UDP flood 防禦功能。一旦來自 Internet 的 UDP 資料封包超過用戶定義的臨界值，路由器將在用戶定義的 timeout 期間強制丟棄所有後續的 TCP SYN 資料封包。threshold 和 timeout 的預設值被分別設置每秒和每 10 秒有 300 資料封包。
<b>Enable ICMP flood defense (啟用 ICMP flood 防禦)</b>	勾選該核取方塊以啟用 ICMP flood 防禦功能。與 UDP flood 防禦功能類似，一旦來自 Internet 的 ICMP echo 請求超過用戶定義的臨界值(預設值是 300 資料封包每秒)，路由器將在一段時間裡(預設是 10 秒)丟棄來自 Internet 的 ICMP echo 請求。
<b>Enable Port Scan defense</b>	勾選此核取方塊以啟用 Port Scan detection 功能。埠掃描攻擊發生時，透過發送包含不同埠號的資料封包嘗試掃

<b>(啓用 Port Scan detection)</b>	描可用的服務，當一個埠將響應時表明該服務可用。要檢查此類探測行爲，請在您的路由器裡勾選核取方塊以啓用 Port Scan detection 功能。如果埠掃描速度(資料封包每秒)超過用戶定義的臨界值，路由器將識別此攻擊並報告一個警告資訊。路由器設置臨界值預設爲每秒 300 資料封包，以偵測這種掃描活動。
<b>Block IP Option (阻擋 IP 選項)</b>	勾選此核取方塊以啓用阻擋 IP 選項功能。路由器將忽略任何 IP 選項域出現在資料封包頭的 IP 資料封包。IP 選項爲主機提供了一種發送某些重要資訊的方法，譬如安全性、分隔、TCC(封閉用戶組)參數、一連串 Internet 位址和路由資訊。外部可以分析此資訊以瞭解您私有網路的詳細情況。
<b>Block Land(阻擋 Land)</b>	勾選此核取方塊以強制路由器抵禦 Land 攻擊。Land 攻擊將結合了 SYN 攻擊技術與 IP 欺騙，當一個攻擊者發送包含那些受害者的相同來源位址和目標位址以及埠號欺騙的 SYN 資料封包時，Land 攻擊就發生了。
<b>Block Smurf (阻擋)Smurf</b>	勾選此核取方塊以啓用阻擋 Smurf 功能，路由器將拒絕任何目標位址是廣播位址的 ICMP echo 請求。
<b>Block trace router (阻擋 trace route)</b>	勾選此核取方塊以啓用此功能，路由器將不會轉發任何追蹤路由的資料封包。
<b>Block SYN fragment (阻擋 SYN 碎片)</b>	勾選此核取方塊以啓用阻擋 SYN 碎片功能，任何包含 SYN 標誌以及更多分段位元(MF)設定的資料封包將被丟棄。
<b>Block Fraggle Attack (阻擋 Fraggle 攻擊)</b>	勾選此核取方塊以啓用阻擋 fraggle 攻擊功能，任何來自 Internet 的廣播 UDP 資料封包將被阻擋。
<b>Block TCP flag scan (阻擋 TCP flag scan)</b>	勾選此核取方塊以啓用阻擋 TCP flag scan 功能，任何包含異常標誌設定的 TCP 資料封包將被丟棄。那些掃描活動包括 no flag scan、FIN without ACK scan、SYN FIN scan、Xmas scan 以及 full Xmas scan。
<b>Block Tear Drop (阻擋 Tear Drop)</b>	勾選此核取方塊以啓用阻擋 Tear Drop 功能，攻擊者生成一系列 IP 片斷，這些 IP 片斷的偏移欄位彼此重疊。當這些 IP 片斷到達目標主機進行重組的時候，某些系統就會崩潰、當掉或重新啓動。路由器將阻擋任何實現此攻擊活動的資料封包。
<b>Block Ping of Death (阻擋 Ping of Death)</b>	勾選此核取方塊以啓用阻擋 Ping of Death 功能，當接收到超過最大長度的 ICMP 資料封包時，很多機器都會崩潰。要避免此類攻擊，路由器被設計爲有能力丟棄任何長度超過 1024 位元組的分段 ICMP 資料封包。
<b>Block ICMP fragment (阻擋 ICMP fragment)</b>	勾選此核取方塊以啓用阻擋 ICMP fragment 功能，任何包含更多分段位元設定的 ICMP 資料封包將被丟棄。

<b>Block Unknown Protocol (阻擋 Unknown Protocol)</b>	勾選此核取方塊以啓用阻擋 Unknown Protocol 功能，單獨的資料封包有一個協定區域用以指出上層運行的協議類型。但是目前大於 100 的協議類型是保留的且沒有被定義出來，因此路由器應該有能力偵測並拒絕此類資料封包。
---	--

按應用以完成該設定。

## 7.5 URL(過濾設定)

### 7.5.1 序言

Internet 包含廣泛的資源，其中一些資源可能是攻擊性的，在某些國家甚至是違法的。不像傳統的媒體，Internet 沒有任何明顯的工具來隔離基於 URL 字串或內容的資源。URL 內容過濾系統被視為一種工具，它爲了限制存取一些特殊的資源，將提供等同於物理隔離的網路空間。透過評定一個站點爲“令人討厭的”，並拒絕把它顯示在用戶的電腦螢幕上，URL 內容過濾工具可以被用來防止小孩看到一些他們的父母認爲是“令人討厭的”資源。在阻止存取方面，URL 內容過濾工具擔當自動化形式的便利店職員，他們拒絕向中學生出售成人雜誌，URL 內容過濾工具也被企業用來防止員工存取與工作無關的或被認爲是不恰當的 Internet 資源。

URL 內容過濾這個名稱來自檢查 URL 字串的內容，傳統的防火牆檢查資料封包區域基於主要 TCP/IP，而 URL 內容過濾檢查 URL 字串或 TCP/IP 資料封包的負載。在路由器裡，URL 內容過濾工具檢查 URL 字串和一些藏在 TCP 資料封包負載裡的 HTTP 資料。

### 7.5.2 URL 內容過濾概述

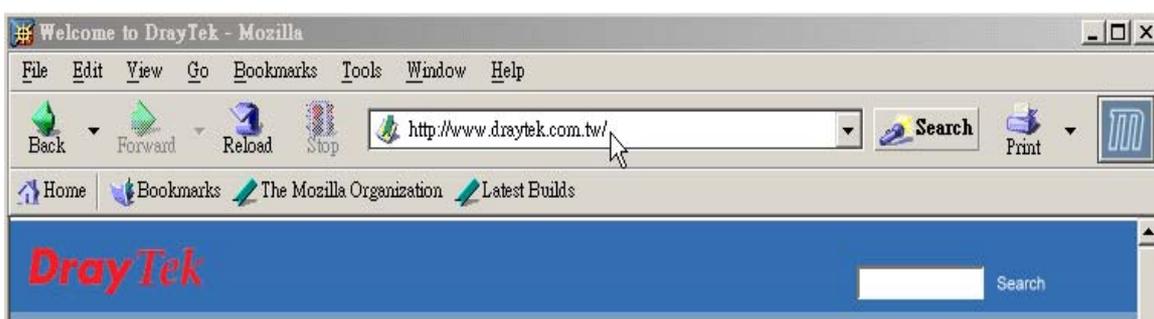


圖 7-12 URL 過濾實例

這一系列的寬頻安全路由器裡的 URL 內容過濾工具根據關鍵字列表檢查從內部發起的 HTTP 請求裡的每個 URL 字串。如果整個或部分 URL 字串(譬如，http://www.draytek.com 如圖 7-12 所示) 符合任意啓用的關鍵字，與它關聯的 HTTP 請求將被路由器阻擋。任何嘗試檢索惡意代碼的請求都將被系統丟棄。

URL 內容過濾工具防止用戶存取不恰當的 web 站點，它們的 URL 字串被識別爲禁止存

取的。注意在存取一個 web 頁面之前，您必須首先清除您的瀏覽器的 Cache，以便 URL 內容過濾工具能正確地工作。

### 7.5.3 URL 內容過濾配置

以下部分介紹了用於設定 URL 內容過濾工具的 web 配置，包括特殊的配置資訊和它們具有的任何限制。

路由器支援的 URL 內容過濾工具由 URL 連線控制、IP 位址連線控制、限制 WEB 功能、例外網路類別、和過濾時間表功能組成。URL 連線控制的目標是控制存取 web 站點的權利，方法是根據用戶定義的關鍵字檢查 URL 字串；限制網路功能是要阻擋隱藏在 Web 頁面裡的惡意代碼，譬如 Java Applet、Active X、Cookies、代理伺服器、壓縮檔和可執行檔。為了控制使用頻寬，它也能阻擋所有從 Web 頁面下載的多媒體檔。

IP 位址連線控制這個功能被用來防止那些不適當的站點，可以透過在 URL 位址欄裡直接使用 IP 位址存取，即使它們的 URL 字串匹配用戶定義的關鍵字。例外網路類別這個功能允許管理員指定某一個組的主機不受 URL 連線控制的限制。這個組的主機可以定義為一組 IP 位址或子網。最後路由器支援過濾時間表功能以控制什麼時候應該執 URL 內容過濾工具，現在請繼續閱讀每個項目用法的具體說明。



圖 7-13 URL 過濾

選擇 URL 過濾專案，將顯示以下頁面。

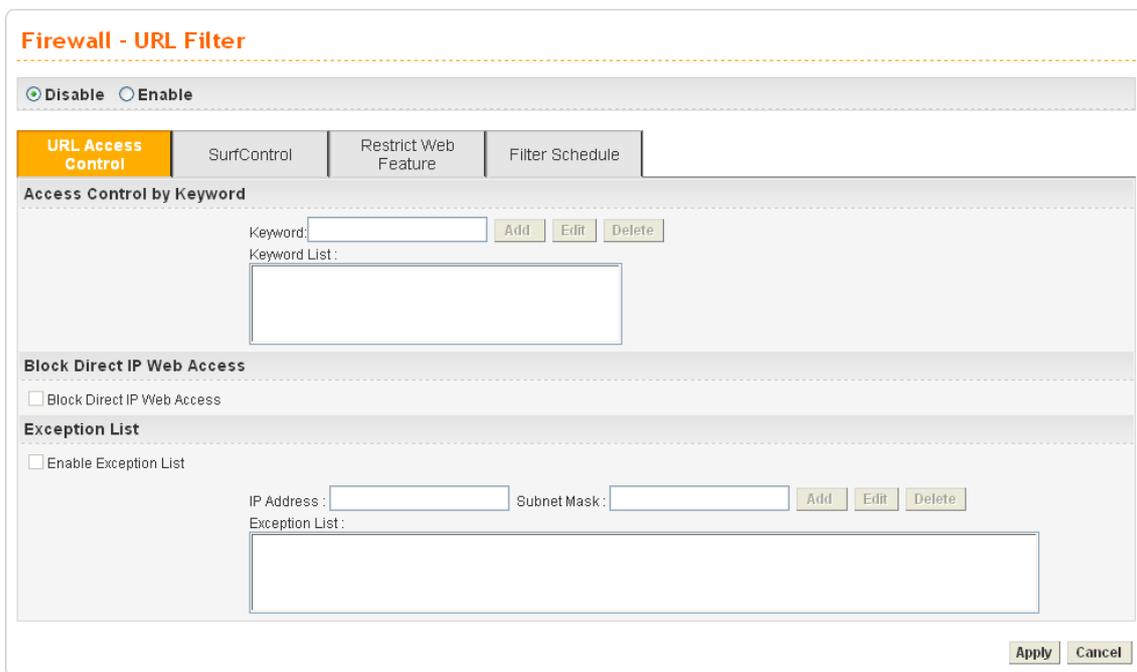


圖 7-14 URL 過濾 – URL 連線控制

**URL Access Control (URL 連線控制設定)**

<b>Access Control by Keyword(透過關鍵字進行連線控制)</b>	
<b>Keyword(關鍵字)</b>	關鍵字可以是一個名詞，名詞的一部分，或一個完整的 URL 字串。在一個框架裡的多個關鍵字由空格，逗號或分號進行分隔。每個框架的最大長度是 32 個字元。指定好關鍵字後，如果 web 站點的整個或部分 URL 字串匹配任意一個用戶定義的關鍵字，路由器都將拒絕對它們的存取權利。必須要注意的是，阻擋關鍵字列表越簡單，路由器的效率將更高。
<b>Keyword List (關鍵字列表)</b>	包含每個關鍵字框架的組列表。
<b>Block Direct IP Web Access(禁止使用 IP 存取網站)</b>	
<b>Block Direct IP Web Access (禁止使用 IP 存取網站)</b>	勾選核取方塊以啓用該功能，它將拒絕任何直接使用 IP 位址進行網路衝浪的活動。
<b>Exception List(例外列表)</b>	
<b>Enable Exception List (允許例外列表)</b>	用來指定一些特殊的 IP 地址或子網，以便它們不受 <b>URL 連線控制</b> 的限制。用戶必須勾上此核取方塊以啓用該功能。
<b>IP Address (IP 地址)</b>	指派一個 IP 位址。
<b>Subnet Mask (子網路遮罩)</b>	指派一個子網路遮罩值。
<b>Exception List</b>	包含每個 IP 位址的組列表。

(例外 IP 列表)	
------------	--

*實例* – 如果您想要過濾任何 URL 字串包含“sex”，“fuck”，“gun”，或“drug”的 web 站點，您應該將這些關鍵字新增到框架裡。所以，如果 web 站點關聯的 URL 字串裡包含任何一個列表裡的關鍵字，系統都將自動拒絕對它們的存取。考慮用戶嘗試存取 `www.backdoor.net/images/sex /p_386.html` 的情況，路由器將斷開此連接，因為該站點是被禁止的。但是，用戶可以存取 web 站點 `www.backdoor.net/firewall/forum/d_123.html`。此外，URL 內容過濾工具也允許您在阻擋關鍵字列表裡指定一個完整的 URL 字串(譬如，“`www.whitehouse.com`”和“`www.hotmail.com`”)或 URL 字串的一部分(譬如，“`yahoo.com`”)。因此，路由器將識別被禁止的 URL 並透過切斷相應的連接來為這些 web 站點執行阻擋動作。

## SurfControl 設定

Access Control by Category (透過類型進行連線控制)	
<b>CPA Server (CPA 伺服器)</b>	選擇 Disable(關閉)或 Enable(啓用)。
<b>Select a CPA Server (選擇一個 CPA 伺服器)</b>	選擇一個功能變數名稱作為 CPA 伺服器。
<b>Permitted Categories list (允許分類列表)</b>	它顯示了一個來自選定的 CPA 伺服器的可能的類別。這些類別是一直准許存取的。
<b>Forbidden Categories List (被禁止的分類列表)</b>	這些選定的類別是一直禁止存取的。
<b>URL</b>	指派一個 URL 功能變數名稱。
<b>Option(選項)</b>	有兩個選項為“拒絕”或“允許”。
<b>例外的 URL 列表</b>	關於每個 URL 記錄的組列別。

## Restrict Web Feature(約束網路特徵設定)

提供保護機制以禁止從 web 頁面下載惡意代碼將是很有價值的，這些惡意代碼可能嵌入在某些可執行物件裡，譬如 ActiveX、Java Applet、壓縮檔、可執行檔、代理伺服器和多媒體。如果它們已經從網站上被下載下來，將會對用戶的系統帶來威脅，譬如，ActiveX 物件可以從 WEB 頁面被下載和操作，如果該 ActiveX 物件本身存在某些惡意代碼，它可

能會擁有對用戶的系統不受限的存取權利。

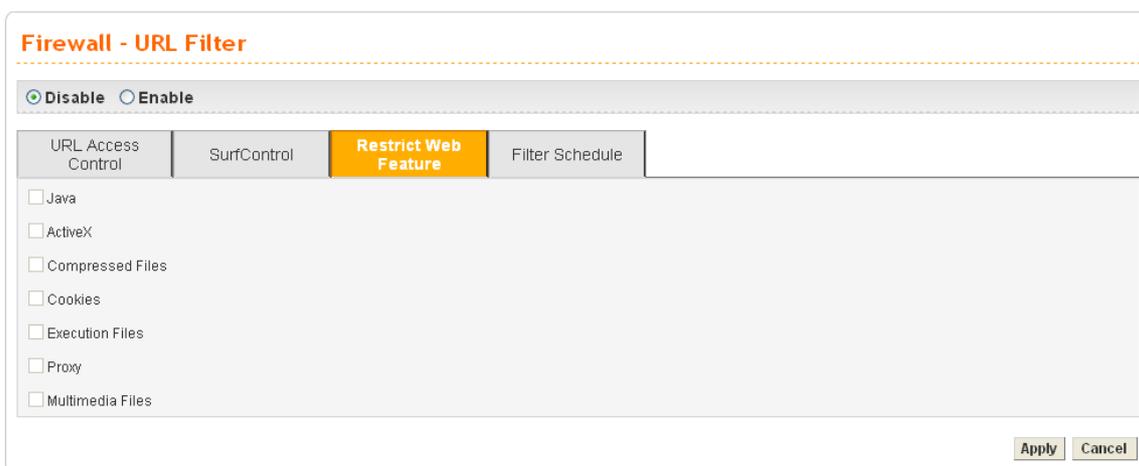


圖 7-15 URL 過濾 – 約束網路特徵

<b>Java</b>	勾選核取方塊以啓用阻擋 Java 物件工具，路由器將丟棄來自 Internet 的 Java 對象。
<b>ActiveX</b>	勾選核取方塊以啓用阻擋 ActiveX 物件工具。任何來自 Internet 的 ActiveX 物件將被拒絕。
<b>Compressed File (壓縮檔)</b>	有一個核取方塊可以用來選擇啓用阻擋壓縮檔功能，它能防止某些人下載任何壓縮檔。以下列表顯示了可以被路由器阻擋的壓縮檔類型： .zip、.rar、.arj、.ace、.cab、.sit 要啓用該功能，勾選核取方塊，即可啓用該功能。
<b>Cookie</b>	勾選核取方塊以啓用阻擋 Cookie 傳輸。 路由器將過濾掉來自任何網站的 cookie。
<b>Execution Files (可執行檔)</b>	與上面的功能類似，勾選核取方塊以啓用阻擋執行檔功能，從而拒絕任何從 Internet 下載執行檔的行為。要啓用該功能，請勾選核取方塊。路由器將阻擋有以下副檔名地檔： .exe、.com、.scr、.pif、.bas、.bat、.inf、.reg 一個 Netscape 引入的所謂的 <i>cookie</i> 特性允許您密切注視 HTTP 的每個線程的請求和回應行為。許多 web 站點用它們來創建有狀態地線程，以便能追蹤 Internet 用戶。但這樣將會破壞用戶的隱私，因此路由器提供了 <i>Cookies 過濾工具</i> ，允許您過濾 cookie 傳輸。同樣地，路由器也允許您過濾掉所有與代理相關的傳輸，以支援更強的安全。
<b>Proxy (代理伺服器)</b>	勾選核取方塊以啓用阻擋代理伺服器傳輸。 路由器將過濾掉來自任何網站的代理伺服器。
<b>Multimedia File(多媒體)</b>	勾選核取方塊以啓用阻擋多媒體傳輸。 路由器將過濾掉來自任何網站的多媒體。

### Filter Schedule(過濾時間表設定)

指定何時執行 URL 內容過濾工具。

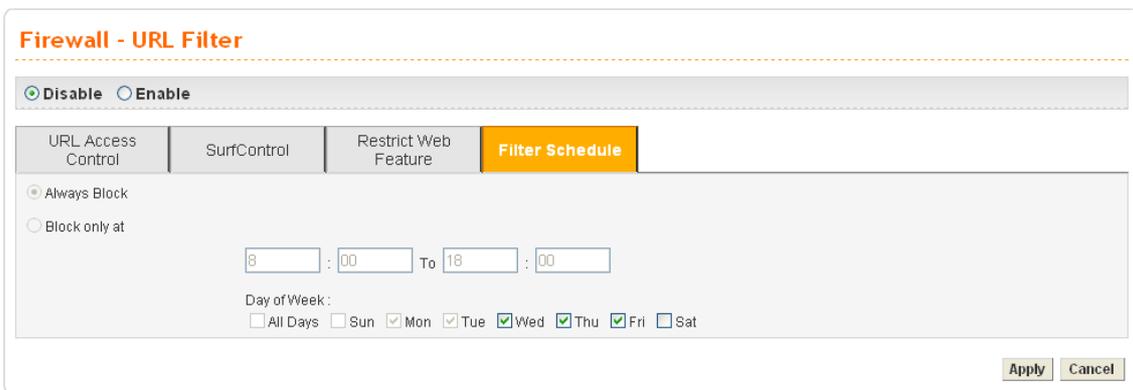


圖 7-16 URL 過濾 – 過濾時間

<b>Always Block</b> (總是阻擋)	選擇該設定以便 URL 內容過濾工具能在任何時候執行。
<b>Block only at</b> (只遮罩於)	指定一天中適當的一段時間 - 從 <i>H1:M1</i> 到 <i>H2:M2</i> 。 <i>H1</i> 和 <i>H2</i> 代表小時， <i>M1</i> 和 <i>M2</i> 代表分鐘。
<b>Day of Week</b> (每週設置)	指定一周當中哪幾天應該應用 URL 內容過濾工具。路由器支援兩個互斥的選項，也就是每天和一周中的某幾天。如果您希望 URL 內容過濾工具整周都啓用，您應該勾選“每天”核取方塊。否則，您應該明確指定一周裡有哪幾天。譬如，如果您想要 URL 內容過濾工具從週一到週三工作，那麼您應該選定合適的核取方塊(星期一、星期二和星期三)。一周剩下日子裡 URL 內容過濾工具將不運作。預設值從 8:00 到 18:00，星期一到星期五。

#### 7.5.4 警告資訊

當一個 HTTP 請求被拒絕，您的瀏覽器將顯示 一個警告頁面，如下圖所示。

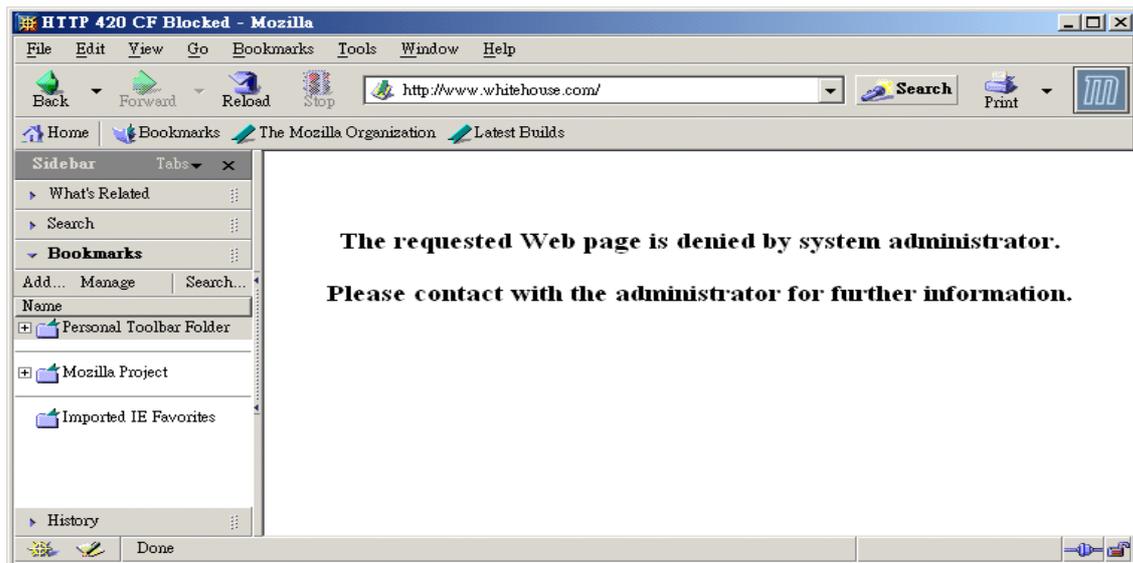


圖 7-17 警告資訊

本頁留白

# 第 8 章

## QoS 設置

### 8.1 序言

Vigor3300 系列路由器的 QoS (Quality of Service) 功能，允許網路管理者在各種類型的網路通信中即時地監控、分析和分配網路頻寬。因此，即時程式將不會受網路存取或其他的非關鍵應用軟體影響，例如檔傳輸，相比之下，如果沒有 QoS 控制功能，有限的頻寬資源就無法分配給網路或伺服器，來支援那些即時和關鍵性的網路應用程式正常運作像是 VoIP(Voice over IP)和線上遊戲應用程式等。因此，我們相信 QoS 功能將是網路舞臺上的一個重要焦點。此外，在設計 Vigor3300 系列路由器的 QoS 功能控制模組時，我們已經考慮將支援 DSCP(Differentiated Service Code Point)功能的代碼加入。

本章節詳細說明了 QoS 功能，以及在主功能表中如何配置 QoS 功能的具體細節。

Vigor3300 系列路由器的 QoS 功能的傳入和傳出功能是獨立的，也就是說，用戶可以自由配置傳入或傳出而不必擔心出現衝突。

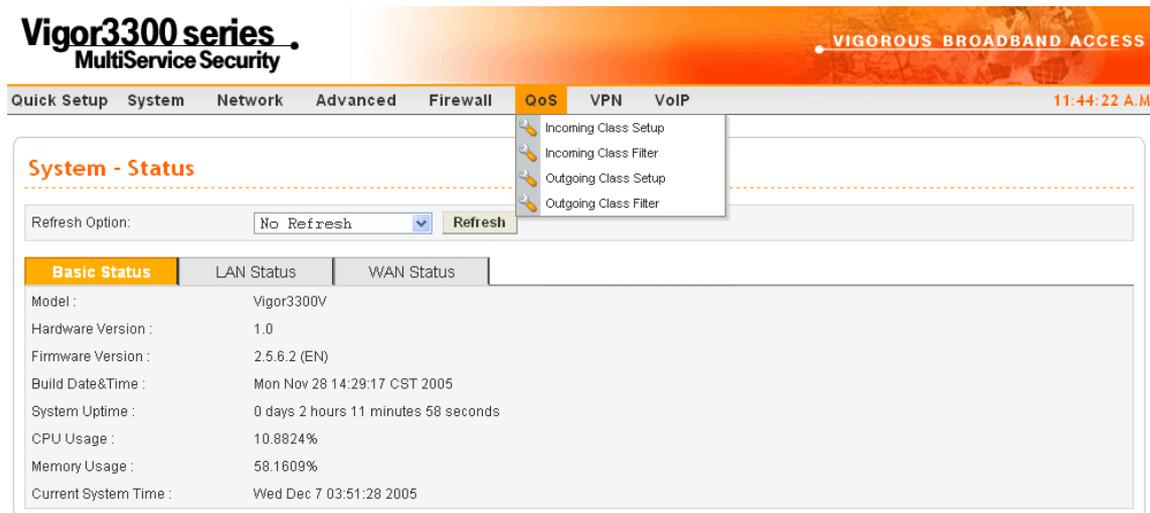


圖 8-1 QoS 功能

### 8.2 Incoming/Outgoing Class Setup(傳入/傳出分類設置)

該部分描述了如何配置傳入/傳出分類。

### QoS - Incoming Class Setup

Disable     Enable

Index	Class Name	Bandwidth
1.	<input type="text" value="learning"/>	<input type="text" value="25"/> %
2.	<input type="text"/>	<input type="text"/> %
3.	<input type="text"/>	<input type="text"/> %
4.	<input type="text"/>	<input type="text"/> %
5.	<input type="text"/>	<input type="text"/> %
6.	<input type="text"/>	<input type="text"/> %
7.	<input type="text"/>	<input type="text"/> %
8.	others	<input type="text"/> %

### QoS - Outgoing Class Setup

Disable     Enable

Index	Class Name	Bandwidth
1.	<input type="text"/>	<input type="text" value="25"/> %
2.	<input type="text"/>	<input type="text"/> %
3.	<input type="text"/>	<input type="text"/> %
4.	<input type="text"/>	<input type="text"/> %
5.	<input type="text"/>	<input type="text"/> %
6.	<input type="text"/>	<input type="text"/> %
7.	<input type="text"/>	<input type="text"/> %
8.	others	<input type="text"/> %

圖 8-2 分類配置

<b>Disable/Enable</b>	按 <b>Enable(啓動)</b> 或者 <b>Disable(關閉)</b> QoS 功能。
<b>Index(索引)</b>	每個分類的索引號。
<b>Class Name(類名)</b>	賦予每個分類一個名字。
<b>Bandwidth(頻寬)</b>	一個百分比數字。

提供了最多 8 個分類可以設置。所有分類的頻寬總和必須為 100%。第 1 至 7 分類之外的剩餘頻寬分配給第 8 分類(other)，以便保證總和為 100%。請按應用按鈕保存設置。

## 8.3 Incoming/Outgoing Class Filter (傳入/傳出分類過濾設置)

描述如下：

### QoS - Incoming Class Filter

Priority	Source IP	Destination IP	Service Type Status	DiffServ CodePoint Status	Class
1	<input checked="" type="radio"/>				
2	<input type="radio"/>				
3	<input type="radio"/>				
4	<input type="radio"/>				
5	<input type="radio"/>				
6	<input type="radio"/>				
7	<input type="radio"/>				
8	<input type="radio"/>				
9	<input type="radio"/>				
10	<input type="radio"/>				

Edit Delete Delete All

### QoS - Outgoing Class Filter

Priority	Source IP	Destination IP	Service Type Status	DiffServ CodePoint Status	Class
1	<input checked="" type="radio"/>				
2	<input type="radio"/>				
3	<input type="radio"/>				
4	<input type="radio"/>				
5	<input type="radio"/>				
6	<input type="radio"/>				
7	<input type="radio"/>				
8	<input type="radio"/>				
9	<input type="radio"/>				
10	<input type="radio"/>				

Edit Delete Delete All

圖 8-3 分類過濾配置

用戶可以按 **Edit(編輯)** 按鈕來編輯應用於該分類的過濾條件，按 **Edit(編輯)** 按鈕，將進入編輯頁面。

### QoS - Incoming Class Filter - Edit

Source IP:	<input type="text"/>	<input type="text" value="/24"/>
Destination IP:	<input type="text"/>	<input type="text" value="/24"/>
Service Type Status:	<input checked="" type="radio"/> Basic <input type="radio"/> Advanced <input type="radio"/> None	
Service Type:	<input type="text" value="AUTH(TCP:113)"/>	
Protocol:	<input type="text" value="TCP"/>	
Port:	<input type="text"/>	
DiffServ CodePoint Status:	<input checked="" type="radio"/> Basic <input type="radio"/> Advanced <input type="radio"/> None	
DiffServ CodePoint Type:	<input type="text" value="BE"/>	
DiffServ CodePoint:	0x <input type="text"/> (Hex)	
Class:	<input type="text" value="undefined"/>	

Apply Cancel

**QoS - Outgoing Class Filter - Edit**

Source IP:  /24

Destination IP:  /24

Service Type Status:  Basic  Advanced  None

Service Type: AUTH(TCP:113)

Protocol: TCP

Port:

DiffServ CodePoint Status:  Basic  Advanced  None

DiffServ CodePoint Type: BE

DiffServ CodePoint: 0x (Hex)

Class: undefined

Apply Cancel

圖 8-4 分類過濾編輯

<b>Source IP(來源 IP)</b>	來源 IP 地址（含子網路遮罩）。
<b>Destination IP(目的 IP)</b>	目的 IP 位址（含子網路遮罩）。
<b>Service Type Status (服務類型狀態)</b>	有 3 種選項供選擇： Basic(基本) - 用戶可以配置“服務類型”項。 Advanced(高級) - 用戶可以配置“協定”、“埠”項。 None(無) - 用戶無需配置。
<b>Service Type(服務類型)</b>	支援超過 35 種類型。請按網頁進行瀏覽。
<b>Protocol(協議)</b>	支援 3 種類型協定，包括：TCP，UDP，TCP/UDP。
<b>Port(埠)</b>	埠號。
<b>DiffServ CodePoint Status (DiffServ CodePoint 狀態)</b>	有 3 種選項，如下： Basic(基本)-用戶可以配置“DiffServ CodePoint 狀態”項； Advanced(高級)-用戶可以配置“DiffServ CodePoint”項； None(無)-用戶無需配置。
<b>DiffServ CodePoint Type (DiffServ CodePoint 類型)</b>	支援超過 21 種類型，見表 10-5。
<b>DiffServ CodePoint</b>	十六進位數字。
<b>Class(類)</b>	選擇一個分類以便使用這些過濾條件。

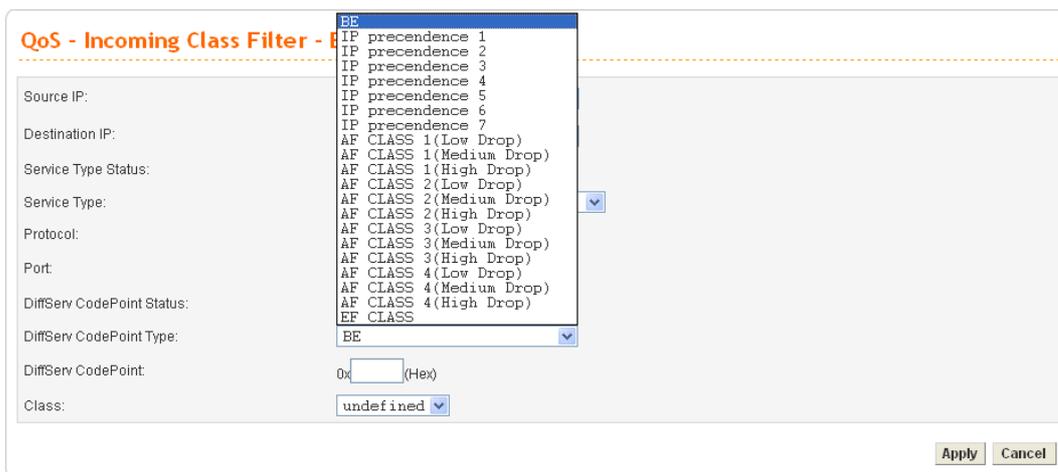


圖 8-5 DiffServ CodePoint 類型表

請按 **Apply(完成)** 按鈕保存設置。

本頁留白

## VPN(虛擬專用網路)與遠程連線設置

---

### 9.1 序言

虛擬專用網路是透過 Internet 對專用網路的拓展，VPN 使您能夠在公眾網上模擬點對點的專用網路連接進行資料傳輸。

VPN 連接類型分為兩種：遠端用戶連線 VPN 和區域網路到區域網路 VPN(LAN-to-LAN VPN)。“遠端用戶連線”允許遠端用戶(NAT 路由器或電腦)透過 Internet 撥入到 VPN 路由器以存取該路由器後的網路資源；LAN-to-LAN VPN 則用來連接兩個獨立的網路以共用網路資源。例如，總公司的網路可以存取分公司的網路，反之亦然。

Vigor 3300 系列寬頻安全路由器採用的 VPN 技術遵循 Internet 工業標準，提供用戶通用的 VPN 解決方案，例如 Internet 安全協議 (IPSec)。目前僅 Vigor 3300，Vigor3300V 路由器提供支援此種功能。

IPSec 是 IP 網路的安全體系，IPSec 提供 IP 層的安全服務，用戶可以選擇安全協定，決定密碼演算法以及加入任意的安全密鑰來實現 IPsec 安全服務。IPSec 可以用來保護主機之間的一個或多個“路徑”，也可以用來保護多個主機之間的“路徑”，同樣支援對主機和閘道之間的路徑保護。

IPSec 服務能夠提供包括存取控制、無連接方式資料完整性、資料源認證、抗重播(replay)保護(序列完整性(sequence integrity)的一個組成部分)、保密性和有限傳輸流保密性在內的服務。這些目標都是透過兩個傳輸安全協議 - 頭部認證(AH)、封裝安全負載(ESP)以及透過密鑰管理過程和協議的使用來完成的。

Vigor3300 系列支援 ESP Tunnel 模式，使用 IKE 進行密鑰管理。Internet 密鑰交換協議 (IKE)，是 IPSec 體系結構中一個重要的協定，由 Oakley、SKEME 的一部分構成的混合協議，與 ISAKMP 聯合使用以獲得 ISAKMP 所需的密鑰，以及生成 IPsec DOI 的 AH 和 ESP 安全關聯。

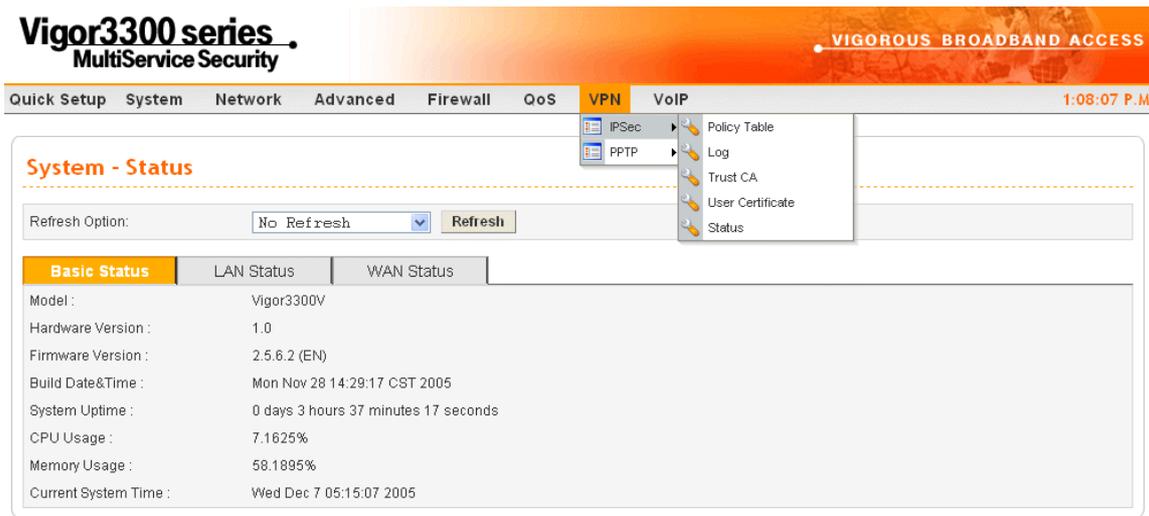


圖 9-1 VPN

VPN 功能表給用戶提供了兩種選擇。我們將在下面的部分進行詳細介紹。

## 9.2 IPsec 設定

### 9.2.1 Policy Table(策略表設定)

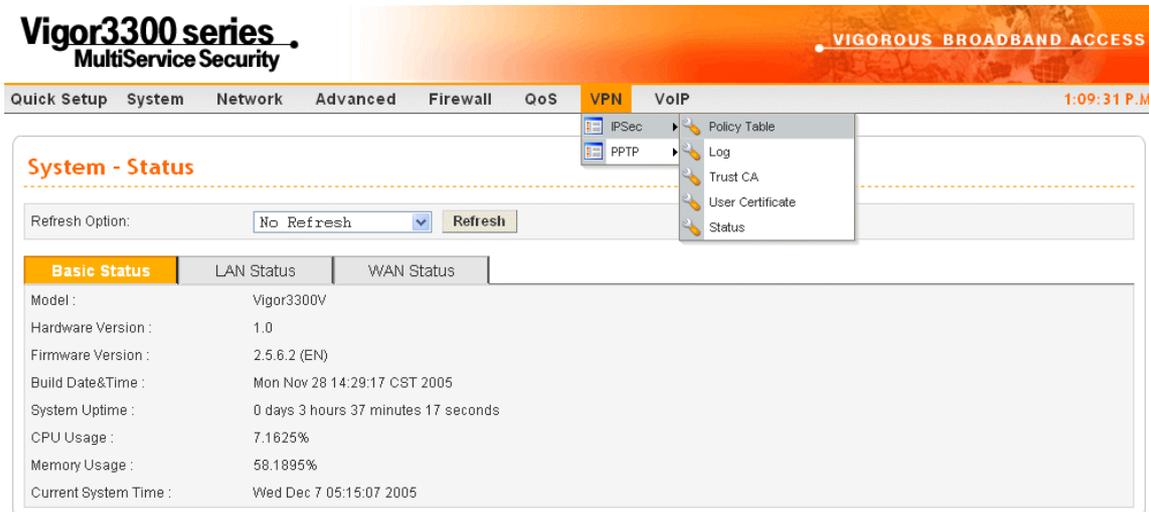


圖 9-2 VPN 策略表

要建立 VPN IPsec 策略，請依次按 **VPN >>IPSec>>Policy Table**，如下圖。

**VPN - IPSec - Policy Table**

#	Connection Name	Local Subnet	Remote Gateway	Remote Subnet	Interface	Admin Status	Operational Status	Action
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

Refresh Edit Delete Delete All

圖 9-3 VPN 策略表

圖中有四個按鈕 –

<b>Refresh(更新)</b>	按此按鈕以更新整個頁面資訊。
<b>Edit(編輯)</b>	按此按鈕以設置一個策略。
<b>Delete(刪除)</b>	按此按鈕以刪除已設置的策略。
<b>Delete All(全部刪除)</b>	按此按鈕以刪除全部策略。

請選擇一個記錄，按編輯以創建一個新的 IPSec 通道，如圖 8-4。

**Default(預設設定)**

**VPN - IPSec Tunnel**

Default | Advanced

**Basic**

Name :

Authentication : Preshared Key ▾

Preshared Key :

Security Protocol : ESP ▾

Admin Status : Enable ▾

**Local Gateway**

WAN Interface : WAN1 ▾

Local Certificate :

Security Gateway : default

Network IP / Subnet Mask :  /

Next hop : default

**Remote Gateway**

Remote ID :

DHCP-over-IPSec : OFF ▾

Security Gateway :  (\*0.0.0.0\* for dynamic client)

Network IP / Subnet Mask :  /  (\*0.0.0.0/32\* for dynamic client)

Apply Cancel

圖 9-4 IPSec 通道設置

<b>Basic(基本設置)</b>	
<b>Name(名稱)</b>	VPN 連接的標識名稱，例如“VPN1”。此名稱對於所有的 VPN 策略來說必須獨特唯一的，最大長度為 20 個字元，不能包含空字元。
<b>Authentication(認證)</b>	選擇一個認證選項。預共用密鑰或 RSA 簽名。
<b>Preshared Key(預共用密鑰)</b>	指定一個共用密鑰進行兩端的認證。該密鑰不能包含任何空字元，最大長度為 40 個字元。
<b>Security Protocol (安全協議)</b>	目前的版本僅支持 ESP。ESP 數據將被加密和認證，我們支援 DES、3DES、AES 3 種加密方法以及不加密。
<b>Admin Status (管理狀態)</b>	設置管理狀態。如果設置為 Enable(啓用)，此策略將被啓用並等待遠端發起 IKE 協商及顯示連接記錄(log)。選擇 Disable(關閉)則該策略被停止使用，選擇 <b>始終保持</b> 則 VPN 將會自動連線。 建議使用“始終保持”以保持 VPN tunnel 在一直線上。
<b>Local Gateway(本地閘道)</b>	
<b>WAN Interface (WAN 介面)</b>	選擇一個 WAN 介面。
<b>Local Certificate (本地證書)</b>	如果在“認證”選項處選擇了“RSA 簽名”，則可以在此處進行選擇，其中的選項來自於用戶的證書檔。
<b>Security Gateway (安全閘道)</b>	本地閘道的公網介面 IP 位址。也可以指定關鍵字“default”來表示預設路由介面的位址。
<b>Network IP/Subnet Mask 網路 IP 位址/子網遮罩</b>	本地網路 IP 位址/子網遮罩。
<b>Next Hop</b>	下一個 IP 地址。也可以指定關鍵字“default”表述預設路由介面的下一跳位址。
<b>Remote Gateway(遠端閘道)</b>	
<b>Remote ID(遠端 ID)</b>	指定遠端 ID。
<b>DHCP-Over-IPSec</b>	選擇“OFF”以關閉此功能。 選擇“ON”以啓用此功能。
<b>Security Gateway (安全閘道)</b>	指定遠端客戶/閘道的 IP 位址，此處為強制設置。如果對端位址為動態分配的 IP 位址，則設置為 0.0.0.0。
<b>Network IP/Subnet Mask 網路 IP 位址/子網遮罩</b>	遠端子網，例如 192.158.2.0/24，如果遠端閘道 IP 位址為 0.0.0.0，此處可以忽略。不過您必須指定其為 0.0.0.0/32。

## Advanced(高級設定)

**VPN - IPsec Tunnel**

Default **Advanced**

**IKE Phase1(main mode)**

Key lifetime : 480 minutes

Proposal : des-md5-modp768 des-sha-modp768 3des-md5-modp768 3des-sha-modp1024

**IKE Phase2(quick mode)**

Key lifetime : 60 minutes

Proposal : des-md5 des-sha1 3des-md5 3des-sha1

PFS (Perfect Forward Secrecy)

**Dead Peer Detection**

Status :  Disable  Enable

Delay : 30 seconds

Timeout : 120 seconds

Apply Cancel

圖 9-5 VPN 高級設定

<b>IKE Phase1 (主模式)</b>	
<b>IKE Lifetime (密鑰存活時間)</b>	定義 IKE 第一階段密鑰從建立安全關聯到再次協商的時間，可接受範圍是 5 到 480 分鐘（8 小時）。
<b>Proposal(提議)</b>	IKE 第一階段協商的提議加密/認證方法，可接受以下組合： <i>加密機制</i> 可以為 DES/3DES/AES <i>認證方法</i> 可以為 MD5/SHA1 <i>DH 組</i> - 可以為 MODP768/MODP1024/MODP1536.
<b>IKE Phase2 (快速模式)</b>	
<b>IKE Lifetime (密鑰存活時間)</b>	定義第二階段密鑰從建立關聯到重新協商的時間，可接受範圍是 5 到 1440 分鐘（24 小時）。
<b>Proposal(提議)</b>	IKE 第二階段協商的提議加密/認證方法，可接受以下組合。 <i>加密機制</i> - 可以為 NULL/DES/3DES/AES.
<b>PFS</b>	勾選以啓用此功能。
<b>Dead Peer Detection(斷線檢測)</b>	
<b>Delay(延時)</b>	保持線上計時器，當 tunnel 空閒時，路由器週期性的發出 Hello 資訊。設置為 0 則關閉此機制。如果要啓用此功能，則建議值為 30 秒。
<b>Timeout(超時)</b>	超時計時器。超過指定的時間沒有收到回應則表明 tunnel 已中斷，設置為 0 值則關閉此機制，如果要啓用此功能，則建議值為 120 秒。

按 **Apply(完成)**以完成 IPsec 策略設置，將新增新的記錄到策略表。

**VPN - IPsec - Policy Table**

#	Connection Name	Local Subnet	Remote Gateway	Remote Subnet	Interface	Admin Status	Operational Status	Action
1	Research	172.16.3.228/32	172.16.2.1	172.16.2.15/32	WAN1	enable	down	<a href="#">Initiate</a>
2								
3								
4								
5								
6								
7								
8								
9								
10								

1

圖 9-6 VPN 策略表

比較重要的選項被匯總到 IPsec 策略表中，運行狀態反映 tunnel 的目前狀態。“UP” 值表明 IPsec 通道已經建立，“down” 值表明沒有 tunnel 建立，其他值表示 tunnel 的一些特殊狀態。

如果要本地開道初始化一個 IKE 連接，也就是說，發出 IKE 主模式的第一個 IKE 消息，可以按“Initiate”超連結開始 IKE 協商。在協商過程中，可以按下“Refresh”顯示所有策略的最新狀態。如果一段時間之後運行狀態仍然是“down”，可以按 **Initiate** 重試。

### 9.2.2 Log (日誌)

**VPN>>IPsec>>Log** 可用來查看或監控 VPN tunnel 狀態，以提供足夠的資訊幫助用戶解決一些設置問題，在目前版本中，系統將保留最新的 100 個消息，可以透過按 **Clear** 以清除日誌，VPN 日誌如下圖。

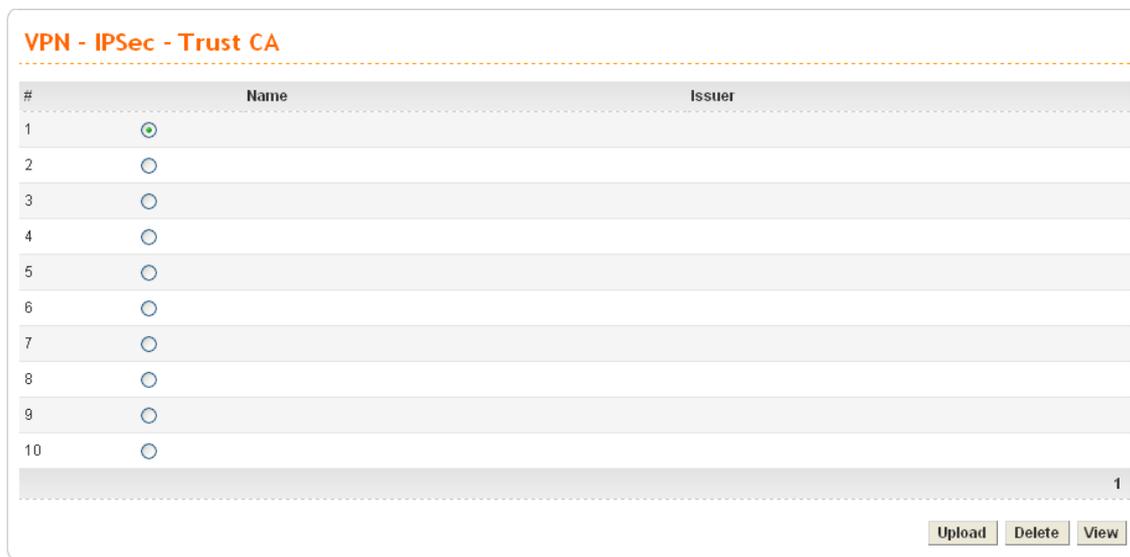
**VPN - IPsec - Log**

#	Date/Time	Description
1	---	No log data

圖 9-8 VPN 日誌資訊

### 9.2.3 Trust CA 設置

按 **VPN>>IPSec>>Trust CA**，將顯示如下頁面。



#	Name	Issuer
1	<input checked="" type="radio"/>	
2	<input type="radio"/>	
3	<input type="radio"/>	
4	<input type="radio"/>	
5	<input type="radio"/>	
6	<input type="radio"/>	
7	<input type="radio"/>	
8	<input type="radio"/>	
9	<input type="radio"/>	
10	<input type="radio"/>	

1

Upload Delete View

圖 9-9 VPN IPSec Trust CA 設置

選擇想要新增的項目(請按數字旁的按鈕)，然後按 **Upload(上傳)** 按鈕，會出現如下頁面。



VPN - IPSec - Trust CA # 1 - Upload

Upload CA Certificate

Upload File  瀏覽...

Apply Cancel

圖 9-10 VPN IPSec Trust CA – 上傳

按**瀏覽**找到所需的檔案，稍後再按下 **Apply(完成)**，系統及開始上傳此檔。

### 9.2.4 User Certificate(用戶證書)

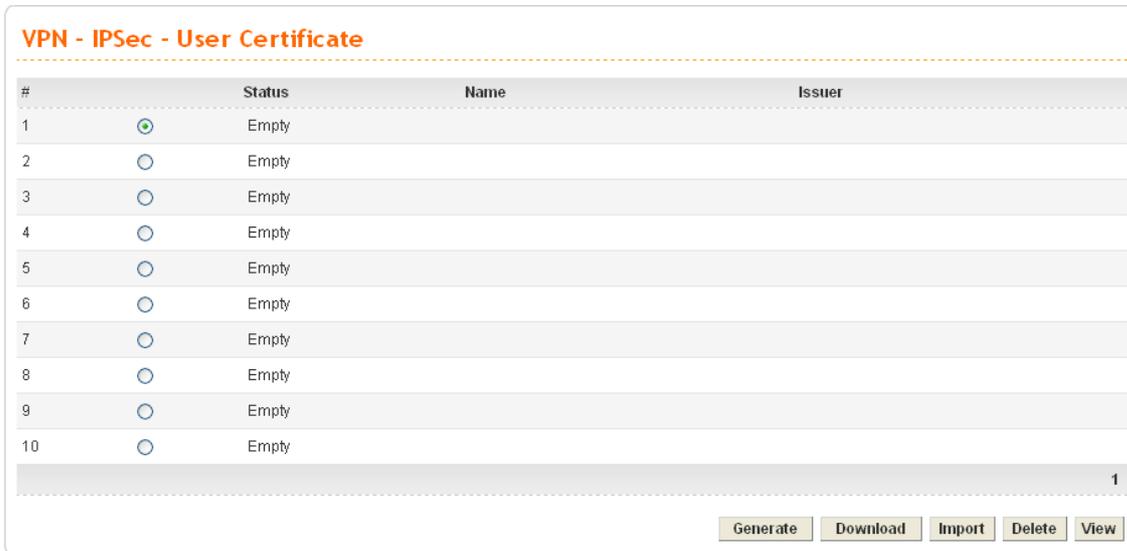


圖 9-11 VPN IPsec 用戶證書

共有以下五個按鈕 –

<b>Generate(生成)</b>	生成一個新的用戶證書項。
<b>Download(下載)</b>	下載一個由路由器生成的證書檔存儲到本地主機。
<b>Import(輸入)</b>	從伺服器導入一個證書檔。
<b>Delete(刪除)</b>	刪除指定項。
<b>View(查看)</b>	顯示指定項的設置

#### Generate(生成設定)

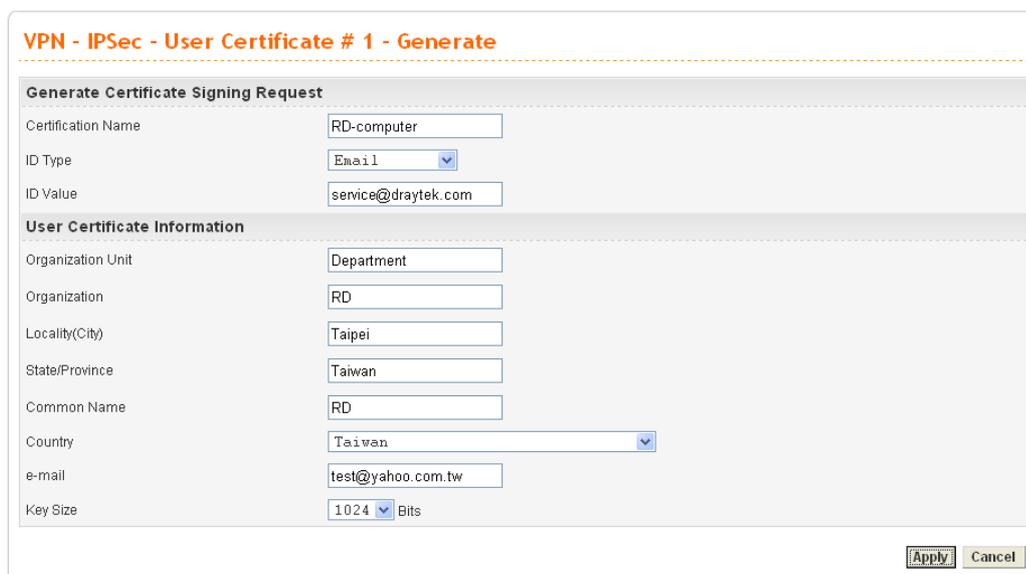


圖 9-12 VPN IPsec 用戶證書 – 生成

<b>Generate Certificate Signing Request(生成證書簽名請求)</b>	
<b>Certification Name</b> (證書名稱)	給證書指定名稱。
<b>ID Type</b> (ID 類型)	為該項選擇一個類型模式。共有三種模式供選擇 – <b>功能變數名稱:</b> 透過功能變數名稱認證。 <b>IP:</b> 透過 IP 地址認證。 <b>Email:</b> 透過 email 地址認證。
<b>ID Value (ID 值)</b>	指定一個 ID 值。
<b>User Certificate Information(用戶證書資訊)</b>	
<b>Organization Unit</b> (組織機構)	指定組織機構。
<b>Organization(組織)</b>	指定組織。
<b>Locality(City)/地點(城市)</b>	指定城市名稱。
<b>State/Province(州/省)</b>	指定州/省名稱。
<b>Common Name</b> (普通名稱)	指定普通名稱。
<b>Country(國家)</b>	指定國家名稱。
<b>e-mail</b>	指定 email。
<b>Key Size(密鑰大小)</b>	選擇密鑰大小。支援以下三種類型 – 1024 位 1536 位 2048 位

### Download(下載證書)

此功能用來導出路由器生成的證書檔到本地電腦。該檔必須移動到認證伺服器上進行驗證。



圖 9-13 VPN IPsec 用戶證書 – 下載

選擇儲存路徑並保存。

### Import(導入設置)



圖 9-14 VPN IPsec 用戶證書 – 導入

從本地電腦選擇一個證書檔，按 **Apply(完成)**以完成此操作。

## Delete(刪除設置)

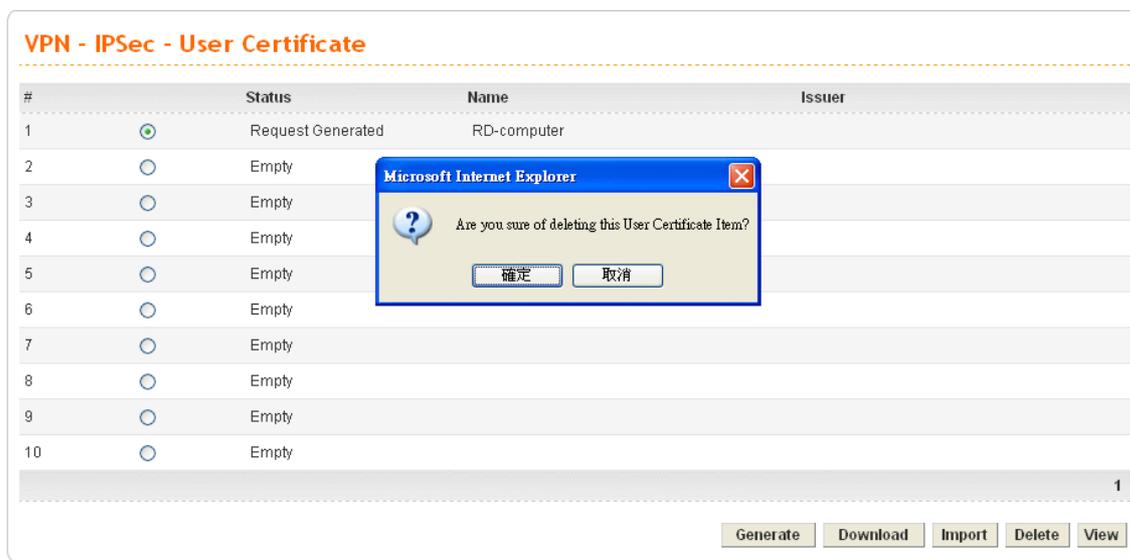


圖 9-15 VPN IPsec 用戶證書 – 刪除

選擇一個要從表中刪除的項目。

## View(查看)

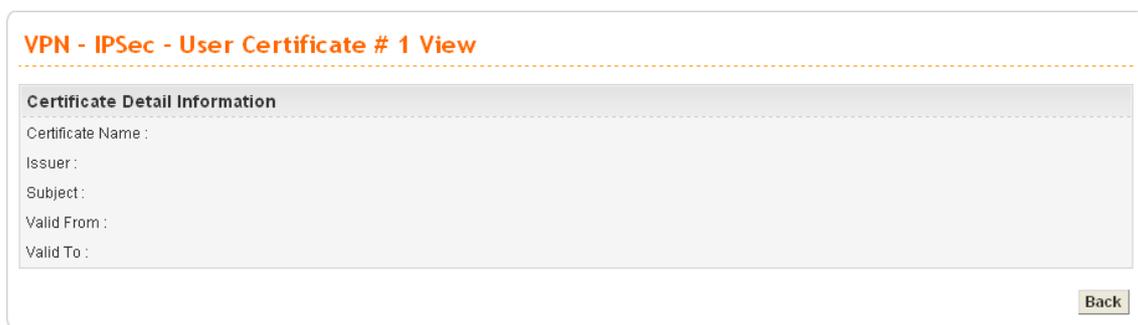


圖 9-16 VPN IPsec 用戶證書 – 查看

顯示選定證書的相關資訊。

## 9.2.5 Status(連接狀態)

按 VPN>>IPsec>>Status，會顯示以下頁面。



圖 9-17 VPN 連接狀態圖

## 9.3 PPTP 設定

### 9.3.1 General Setup(基本設定)

Vigor3300 系列支援 VPN - PPTP 設置。

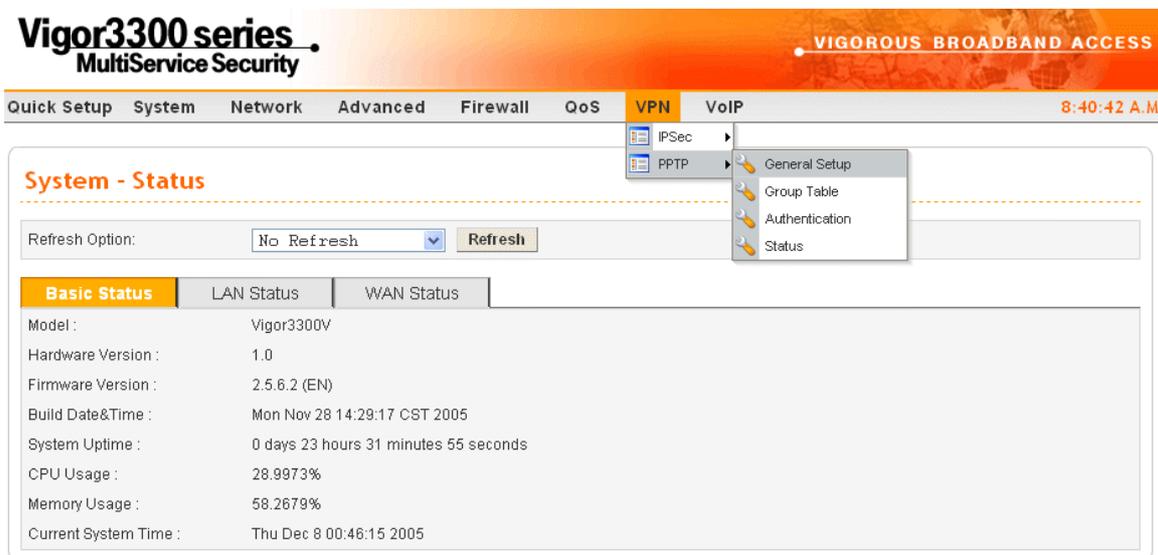


圖 9-18 VPN PPTP

### General Setup(基本設定)

按 **VPN >> PPTP>>General Setup**，將顯示如下網頁。

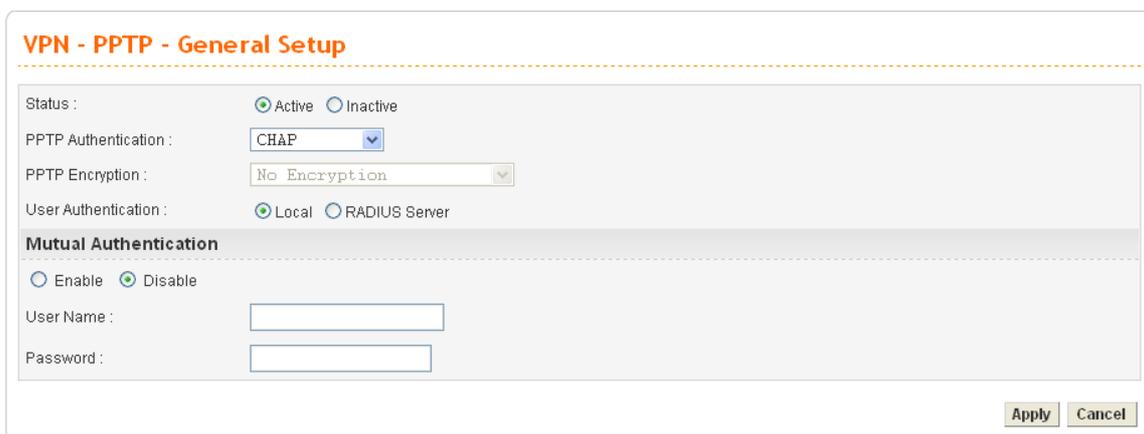


圖 9-19 PPTP 基本設定

<b>Status(狀態)</b>	按 <b>Enable(啓動)</b> 以啓用此功能。 按 <b>Disable(關閉)</b> 關閉此功能。
<b>PPTP Authentication (PPTP 認證)</b>	用戶可以選擇四種認證模式中的一種，預設設置爲 <b>CHAP</b> 。

<b>PPTP Encryption (PPTP 加密)</b>	用戶可以選擇三種認證模式中的一種。
<b>User Authentication (用戶認證)</b>	按 <b>Local(本地)</b> 可從本地主機認證。 按 <b>Radius Server(Radius 伺服器)</b> 可從 Radius 伺服器認證。
<b>Mutual Authentication(雙向認證)</b>	
<b>Status(狀態)</b>	按 <b>Enable(啓動)</b> 以啓用此功能。 按 <b>Disable(關閉)</b> 關閉此功能。
<b>User Name(用戶名)</b>	指定用戶名。
<b>Password(密碼)</b>	指定密碼。

### Group Table(組列表設定)

Vigor3300 系列路由器支援最多四組設置。

**VPN - PPTP - Group Table**

Group	Start IP	Subnet Mask	Accessed IP	Subnet Mask
A	<input type="text" value="192.168.1.224"/>	<input type="text" value="/28"/>	<input type="text"/>	<input type="text" value="/24"/>
B	<input type="text"/>	<input type="text" value="/24"/>	<input type="text"/>	<input type="text" value="/24"/>
C	<input type="text"/>	<input type="text" value="/24"/>	<input type="text"/>	<input type="text" value="/24"/>
D	<input type="text"/>	<input type="text" value="/24"/>	<input type="text"/>	<input type="text" value="/24"/>

圖 9-20 PPTP 組設定

<b>Start IP(起始 IP)</b>	指定起始 IP 位址。
<b>Subnet Mask (子網路遮罩)</b>	為起始 IP 設置子網路遮罩。
<b>Accessed IP (連線 IP)</b>	指定連線 IP 地址。
<b>Subnet Mask (子網路遮罩)</b>	為連線 IP 位址設置子網路遮罩。

## Authentication(認證設定)

#	User Name	Group
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

1

圖 9-21 PPTP 認證設定

此頁顯示 User Name(用戶名稱)和 Group(組別)訊息。用戶可以選擇一項然後按 **Edit(編輯)** 以新增一個新的項目。

1

User Name :

User Password :

Group :

圖 9-22 PPTP 認證－編輯項

<b>User Name(用戶名)</b>	指定用戶名。
<b>User Password(用戶密碼)</b>	指定密碼。
<b>Group(組別)</b>	選擇所屬的組別。

按 **Apply(完成)**以完成設置。

## Status(連接狀態)

#	Index	Remote IP	Assigned IP	User	Byte In	Byte Out	Up Time

圖 9-23 連接狀態

該頁面顯示 PPTP 連接的相關資訊，每隔 10 秒鐘系統將會自動更新此頁一次。

# 第 10 章

## VoIP 設置

### 10.1 序言

Voice over Internet Protocol (VoIP)是一個新興技術，可以使用戶透過 Internet 而不是常規的電話線路撥打電話，從而大量節省用戶的通話開支。Vigor 3300 可以根據您的需要設置 4 個或者 8 個 FXS/FXO 介面，連接語音交換機，支援群組通話，為中小型企業提供經濟的語音電話解決方案。結合 EMS(網元管理系統)可以使用戶更方便的控制 Vigor 3300。

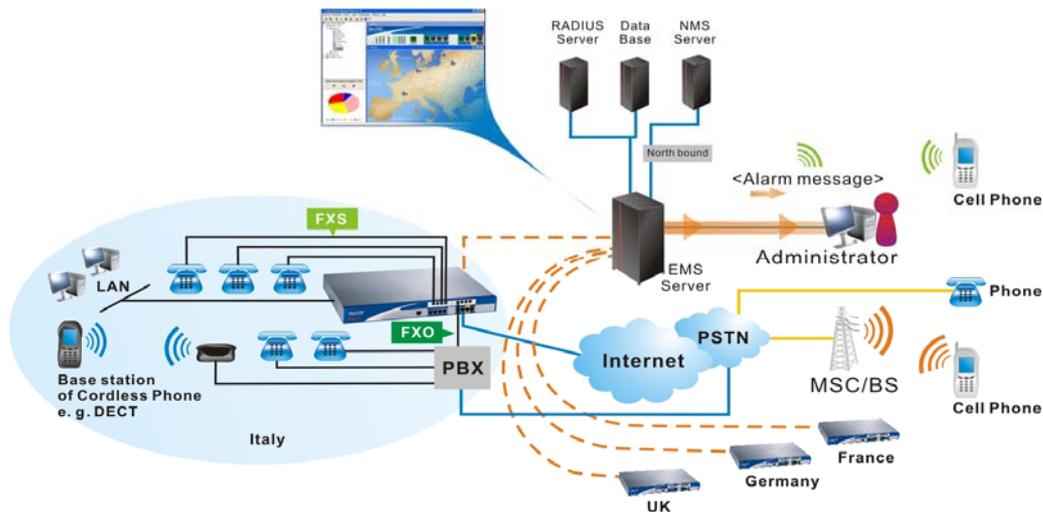


圖 10-1 Vigor 3300 VoIP 使用環境

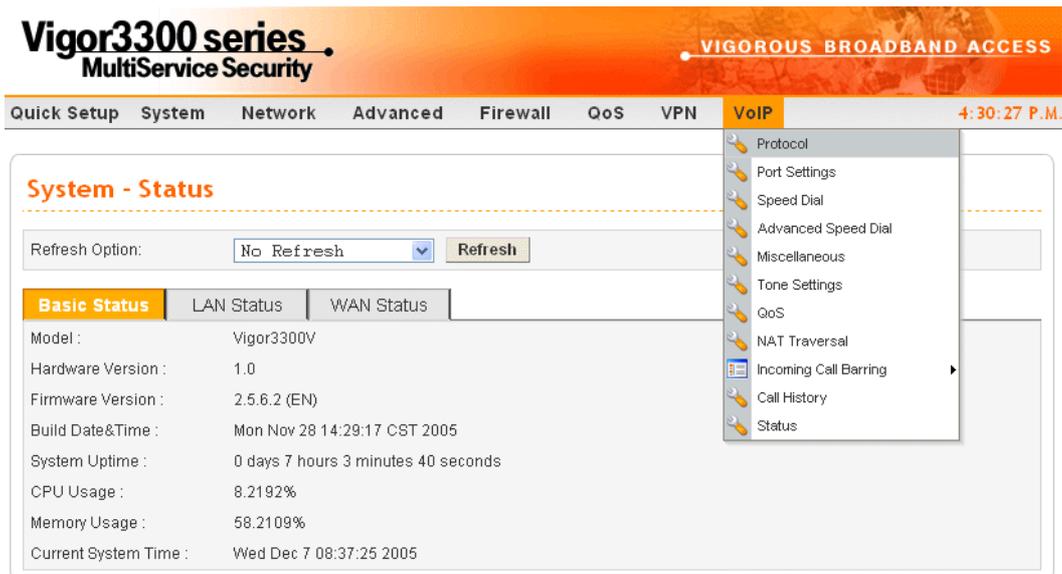


圖 10-2 VoIP 功能展示

## 10.2 VoIP 協議設置

按 **VoIP>>Protocol**，現如下圖所示配置頁面。

**VoIP - Protocol**

Select Protocol :  SIP  MGCP

**SIP Configuration** | MGCP Configuration

SIP Local Port :

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	5060	<input type="text"/>	5060	300	<input type="text"/>
2.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	5060	<input type="text"/>	5060	300	<input type="text"/>
3.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	5060	<input type="text"/>	5060	300	<input type="text"/>
Example			iptel	iptel.org		iptel.org			iptel.org

圖 10-3 VoIP 協定設置頁面

Vigor 3300 VoIP 功能使用兩種協定：SIP 以及 MGCP，預設值為 **SIP**。

### 10.2.1 SIP Configuration (SIP 設定)

Vigor3300 可以同時支援 3 個 SIP 註冊服務商。

**VoIP - Protocol**

Select Protocol :  SIP  MGCP

**SIP Configuration** | MGCP Configuration

SIP Local Port :

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	5060	<input type="text"/>	5060	300	<input type="text"/>
2.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	5060	<input type="text"/>	5060	300	<input type="text"/>
3.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	5060	<input type="text"/>	5060	300	<input type="text"/>
Example			iptel	iptel.org		iptel.org			iptel.org

圖 10-4 SIP 設定

**SIP 本地埠** –設定一個本地發送 SIP 資訊的埠，預設為 5060

<b>Active(啓用)</b>	用戶勾選此選項來啓動對應的 SIP 設定。
<b>Outbound Proxy</b>	如果用戶選擇此選項，則所有的 SIP 語音資料封包將被發

(外出代理)	送到該 SIP 代理。
<b>Proxy Name</b> (代理名稱)	設定該 SIP Proxy 的名稱。
<b>Proxy Address</b> (代理位址)	設定該 SIP Proxy 的 IP 位址。
<b>Proxy Port(代理埠)</b>	設定該 SIP Proxy 的接收埠。
<b>Registrar Addr.</b> (註冊地址)	設定 SIP 註冊伺服器的 IP 位址或功能變數名稱。
<b>Registrar Port(註冊埠)</b>	設定 SIP 註冊伺服器的接收埠。
<b>Expires (秒)</b>	設定每隔多少秒, Vigor 3300 向註冊伺服器發送註冊申請。
<b>Domain(網域)</b>	設定該 SIP 域的 IP 位址或者功能變數名稱。

按 **Apply(完成)**，完成設定。

注意：如果用戶在 VoIP IP 地址欄選擇 LAN/VPN，我們建議用戶不要啓動所有的 SIP Proxy 選項，以保證 VoIP 的網路連接。

## 10.2.2 MGCP Configuration (MGCP 設定)

**VoIP - Protocol**

Select Protocol:  SIP  MGCP

**SIP Configuration** | **MGCP Configuration**

MGCP Local Port:

MGCP Call Agent Address:

MGCP Call Agent Port:

EndPoint Name Style:  aaln/#@[ip\_addr]  mac\_addr/#@[ip\_addr]  aaln/#@mac\_addr

Wild-carded RSIP:  Each endpoint sends its own RSIP  Send only one wild RSIP

**Apply** **Cancel**

圖 10-5 MGCP 設定

<b>MGCP Local Port</b> (MGCP 本地埠)	為 MGCP 本地終端設置一個 UDP 埠。
<b>MGCP Call Agent Address</b> (MGCP 電話代理位址)	設定呼叫代理伺服器的 IP 位址。
<b>MGCP Call Agent Port</b> (MGCP 電話代理埠)	設定呼叫代理伺服器的 UDP 接收埠。
<b>EndPoint Name Style</b> (終端名稱類型)	用戶可以填寫三種格式的名稱： aaln/#@[ip_addr]

	mac_addr/#@[ip_addr] aaln/#@mac_addr
<b>Wild-carded RSIP</b>	用戶有兩種選擇： 每個終端發送自己的 RSIP 設定。 僅發送一個 wild RSIP 。

## 10.3 Port Settings(電話號碼設定)

這裡需要進行兩部分的設置。

### 10.3.1 設定電話號碼

按 **VoIP >>Port Settings**，出現如下圖所示配置頁面。

VoIP - Port Settings							
Phone Number	Group						
#	Edit	Type	Active	Group	Username	Proxy	Codec
1		FXS	V	1	1001		G.729A-8kbps
2		FXS	V	2	1002		G.729A-8kbps
3		FXS	V	3	1003		G.729A-8kbps
4		FXS	V	4	1004		G.729A-8kbps
5		FXS	V	5	1005		G.729A-8kbps
6		FXS	V	6	1006		G.729A-8kbps
7		FXS	V	7	1007		G.729A-8kbps
8		FXS	V	8	1008		G.729A-8kbps

圖 10-6 設定電話號碼

有以下內容需要用戶自行設定：Type(類型)、Active(啓用)、Group(組別)、Username(用戶名)、Proxy(代理)和 Codec 設定。

按編輯圖示，進入下一層設定頁面：

**VoIP - Port Settings - Port1 - Edit**

---

**Port 1 (FXS)**

Disable  Enable  
 Username:   
 Password:   
 Display Name:   
 Proxy Server:   
 VoIP IP Address:

**Hotline**

Hotline Number to Internet:   
 Hotline Number to PBX / PSTN:

**FXO**

Manual Disconnection:

**Codec**

Preferred Codec:   
 Codec Rate:  (ms)  
 Codec VAD:  Disable  Enable

**CAS**

RX Gain:  (Range: -32 ~ 31)  
 TX Gain:  (Range: -32 ~ 31)

**FAX**

FAX Mode:   
 FAX Bypass Codec:   
 FAX Bypass Codec Rate:  (ms)

**DTMF**

DTMF Relay:  Disable  RFC2833  SIP INFO

**Call Forwarding**

Disable  
 Call forwarding all calls  
 Call forwarding busy  
 Call forwarding no answer after  rings (Range:1~10)

SIP URL  (Example: 8001@iptel.org)

圖 10-7 設置電話號碼

<b>Port 1(埠 1 (FXS))</b>	
<b>Disable/Enable</b>	按 <b>Enable(啓動)</b> 啓動該埠； 按 <b>Disable(關閉)</b> 關閉該埠。
<b>Username(用戶名)</b>	設置電話號碼。
<b>Password (密碼)</b>	設置密碼。
<b>Display Name (顯示名稱)</b>	設置來電顯示號碼。
<b>Proxy Server (代理伺服器)</b>	設定 SIP Proxy 伺服器。
<b>VoIP IP Address</b>	設定 call in/out 之介面。
<b>Hotline</b>	
<b>Hotline Number to</b>	爲 FXO/FXS 功能設置一個號碼，當有電話自 Internet 撥

<b>Internet</b>	入時，路由器會自動撥接此號碼。
<b>Hotline Number to PBX/PSTN</b>	為 FXO 功能設置一個號碼，當有電話透過 <b>PBX/PSTN</b> 撥入時，路由器會自動撥接此號碼。此設置只對 FXO 功能生效。
<b>FXO</b>	
<b>Manual Disconnection</b>	按下此鈕可將此電話埠之電話斷線。
<b>Codec</b>	
<b>Preferred Codec</b>	選擇語音資料採用的編碼。不同編碼佔用不同的頻寬。
<b>Codec Rate(編碼頻率)</b>	選擇每個封包包含的多少時間的語音資訊。
<b>Codec VAD</b>	按 <b>Enable(啓動)</b> 啓動此功能。 按 <b>Disable(關閉)</b> 關閉此功能。
<b>CAS</b>	
<b>RX Gain</b>	為 RX 設定一個增益值，預設為 0，選擇範圍從-32 到 31。
<b>TX Gain</b>	為 TX 設定一個增益值，預設為 0，選擇範圍從-32 到 31。
<b>FAX</b>	
<b>FAX Mode (FAX 模式)</b>	選擇 FAX 功能的模式，共有以下三種模式可以選擇： <b>Transparent</b> ：如果編碼選擇 G.711，推薦您使用此模式 <b>T.38 Relay</b> ：預設設定 <b>Bypass</b> ：如果用戶選擇此項，則 Vigor 3300 將會啓用下面的兩個設置- FAX Bypass Codec 和 FAX Bypass Codec Rate。
<b>FAX Bypass Codec</b>	如果 FAX 被設定為 Bypass 模式，選擇一個使用的選項。
<b>FAX Bypass Codec Rate</b>	如果 FAX 被設定為 Bypass 模式，選擇一個使用的速率。
<b>DTMF</b>	
<b>DTMF Relay</b>	選擇一個 DTMF 功能使用的選項，共三種： 關閉 RFC2833 SIP INFO
<b>Call Forwarding</b>	
<b>Call forwarding all calls</b>	將所有 VoIP 來電自動轉接至指定接受號碼。
<b>Call forwarding busy</b>	當接收處忙碌時，則將所有 VoIP 來電自動轉接至指定接受號碼。
<b>Call forwarding no answer after ....rings</b>	當來電響了幾聲之後(響鈴次數自行定義)仍無接聽時，自動轉接到指定接收號碼。
<b>SIP URL</b>	指定轉接號碼。

按 **Apply(完成)** 完成設置。

注意：內部埠分別被定義為“01 “，” 02 “……用戶可以直接撥打內線號碼來接通內線電話。如果用戶需要使用 FAX 功能，建議您對兩端的 Vigor 3300 的 FAX 功能進行同樣的設置。如果用戶在 FAX 模式裡選擇“Transparent” 或者“T.38” 選項，FAX 功能將使用 Codec field 設置的參數。

下表為應用表 –

<b>Codec</b>	FAX 模式可以使用。
<b>G.711U</b> <b>G.711A</b>	Transparent , T.38 , Bypass
<b>G.729A</b> <b>G.723.1</b> <b>G.725</b>	T.38 , Bypass

### 10.3.2 Group(組群設定)

群組電話功能對於公司的語音服務是非常重要的，用戶可以撥打一個號碼與一組人員進行通話。當 Vigor 3300 接到撥向組中第一個號碼的電話時，則同時撥通所有包含在該組的電話，並提供語音服務。對於用戶來說，只需要記住公司的一個電話號碼即可，透過啓用此功能，4 或 8 個 VoIP 埠都會使用第一個電話設定作為自己的電話號碼。

用戶最多可以設置 8 個組別，每個介面只能屬於一組而無法同時被分配到兩組中。

**VoIP - Port Settings**

Phone Number **Group**

Group :  Disable  Enable

Group	Port							
	1	2	3	4	5	6	7	8
1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>				
7	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>					
8	<input type="radio"/>	<input checked="" type="radio"/>						

**Incomming Call Rings**

Rings all ports in the group  Rings the first available port

Default Group Apply Cancel

圖 9-8 組群設定

注意：每個組有一個預設的主介面，如果該組包含多於一個介面，所有其他介面的設定必須服從主介面的設定，主介面必須被分配在相應的組群之中。

## 10.4 Speed Dial(快速撥號設置)

此功能允許用戶透過撥打一個簡單的號碼來接通特定的通話物件，Vigor 3300 系列路由器支援最多 30 個快速撥號號碼。按 **VoIP >> Speed Dial (VoIP >> 快速撥號)**，出現如下圖所示頁面：

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>

Example 101                      101@iptel.org

1 2 3 4 5 6 7 8 9 10 >

圖 9-9 快速撥號設置

<b>Speed Dial Phone Number</b> (快速撥號的電話號碼)	設置一個快速撥號號碼。
<b>Speed Dial Destination</b> (快速撥號目的地址)	設置該號碼對應的目標位址。
<b>Memo(備註)</b>	紀錄有關該號碼之注意事項。

按 **Apply(完成)**完成設置。

## 10.5 Advanced Speed Dial(進階快速撥號設置)

按 **VoIP>> Advanced Speed Dial**，出現如下圖所示配置頁面：

**VoIP - Advanced Speed Dial**

#	Prefix	Strip Length	Append	Destination	Memo
1	<input checked="" type="radio"/>				
2	<input type="radio"/>				
3	<input type="radio"/>				
4	<input type="radio"/>				
5	<input type="radio"/>				
6	<input type="radio"/>				
7	<input type="radio"/>				
8	<input type="radio"/>				
9	<input type="radio"/>				
10	<input type="radio"/>				

1

<b>Index No. (#索引號碼)</b>	代表快速撥號設定組。
<b>Strip Length (Strip 長度)</b>	顯示預備刪除之號碼長度(字數)。
<b>Append</b>	顯示預備增添之號碼數字。
<b>Destination</b>	顯示目的 IP/domain 位址。
<b>Memo(備註)</b>	紀錄有關該號碼之注意事項。

欲進行進階快速撥號前，請按任一索引號碼進入設定畫面。

**VoIP - Advanced Speed Dial - Edit**

1

Prefix :

Strip Length:

Append :

Destination :

Memo :

<b>Prefix</b>	設定前置碼的內容作為比對用途，例如您輸入 3，即表示所有前置號碼有 3 的帳號都符合條件。
<b>Strip Length</b>	輸入預備刪除之號碼長度(字數)，例如您輸入 3，即表示所有符合條件的帳號前三碼都會被刪除。
<b>Append</b>	輸入預備增添之號碼數字，例如您輸入 3，即表示所有符合條件的帳號前面都將加入 3。
<b>Destination</b>	輸入目的 IP/domain。

<b>Memo(備註)</b>	紀錄有關該號碼之注意事項。
-----------------	---------------

## 10.6 Miscellaneous(其他設定)

按 **VoIP>>Miscellaneous (VoIP>>其他設置)**，出現如下圖所示設定頁面：

圖 9-10 其他設定

<b>RTP Starting Port (RTP 起始埠)</b>	設定 RTP 資料封包發送時採用的起始埠。
<b>T.38 Starting Port (T.38 起始埠)</b>	設定 T.38 資料封包發送時採用的起始埠，預設值為 49170。
<b>T.38 Redundancy number (T.38 Redundancy 數)</b>	為 T.38 協議設置 redundancy 數。
<b>Dialing Completion Timeout</b>	撥號等待時間，若超過此處所訂立的時間秒數，系統立即將隻前所撥打之號碼送出。
<b>VOIP TOS</b>	設定 VoIP 數據包的 TOS 值，預設值為 0xa0。
<b>FXO auto disconnection if no packet is received in ...</b>	設定限制時間內若無收到任何封包則關閉 FXO 功能。

按 **Apply(完成)**完成設定。

## 10.7 Tone Settings(語音設定)

此頁用來設置語音頻率。按 **VoIP>>Tone Settings (VoIP>>語音設定)**，出現如下圖所示設定頁面：

**VoIP - Tone Settings**

Region:  Caller ID Type:

Tone Classification	Low Frequency(Hz)	High Frequency(Hz)	Ton1 (10msec)	Toff1 (10msec)	Ton2 (10msec)	Toff2 (10msec)
Dial tone	<input type="text" value="350"/>	<input type="text" value="440"/>	<input type="text" value="500"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Ringing tone	<input type="text" value="440"/>	<input type="text" value="480"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="200"/>	<input type="text" value="400"/>
Busy tone	<input type="text" value="480"/>	<input type="text" value="620"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="50"/>	<input type="text" value="50"/>
Congestion tone	<input type="text" value="480"/>	<input type="text" value="620"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="25"/>	<input type="text" value="25"/>

圖 10-11 語音設定

<b>Region(地域)</b>	設置用戶所在國家。另有一個 <b>用戶定義</b> 模式可以選擇。
<b>Call ID Type (呼叫者 ID 類型)</b>	如果用戶選擇 <b>用戶定義</b> 模式，用戶可以設置該值。如果用戶選擇了國家名稱，則該選項已經被設置。

共有四種語音資訊(撥號音、震鈴音、佔線音、壅塞音)用戶可以定義以下類型。

撥號音- 當用戶拿起電話，聽到的聲音。

震鈴音- 當撥通對方電話時，聽到的聲音。

佔線音- 如果對方占線，聽到的聲音。

壅塞音- 一段忙音後聽到的聲音。

<b>Low Frequency(低頻 (Hz))</b>	設置低頻率值（單位為赫茲）。
<b>High Frequency(高頻 (Hz))</b>	設置高頻率值（單位為赫茲）。
<b>Ton1(10msec)</b>	首次響鈴持續的時間（單位為 10 毫秒）。
<b>Toff1(10msec)</b>	首次響鈴後的靜默時間（單位為 10 毫秒）。
<b>Ton2(10msec)</b>	第二次響鈴持續的時間。
<b>Toff2(10msec)</b>	第二次響鈴後的靜默時間。

## 10.8 QoS 設定

按 **VoIP>>QoS**，出現如下圖所示設定頁面：

**VoIP - QoS**

Disable (non-guaranteed voice quality, higher data throughput)

Enable (guaranteed voice quality, normal data throughput)

Apply Cancel

圖 10-12 QoS 設定

狀態	用戶可以關閉或普通 QoS 以及嚴格 QoS 功能。
----	----------------------------

注意：這裡的 Quality of Service (QoS)功能只對 VoIP 生效，當用戶啓用此功能，Vigor 3300 將優先處理 VoIP 資料封包，從而保證通話品質。

按應用完成設置。

## 10.9 NAT Traversal (NAT 穿越設置)

對於基於公網 IP 傳送的多媒體資訊來說，NAT 後方此類應用正面對著 NAT 穿越的難題。Vigor 3300 在為 NAT 或防火牆後的用戶提供安全的連接的同時，還加入了對 NAT 穿越功能的支援。解決了這一問題，用戶可以大範圍的部署透過 Internet 連接的語音或者多媒體服務。Vigor 3300 支援此功能，從而保證 VoIP 功能即使在 NAT 後面也可以正常工作。

**VoIP - NAT Traversal**

**NAT Traversal**

Disable

Manually Input NAT IP Address

NAT IP Address : 127.0.0.1

Auto Discover NAT IP Address

Semi-auto, need to config NAT

Full-auto, no need to config NAT

STUN Local Port : 3478

STUN Server Address : stun.fwdnet.net

STUN Server Port : 3478

**Symmetric Media**

Disable symmetric RTP and T.38

Enable symmetric RTP and T.38

**NAT Status**

NAT Type: N/A, Local IP Address: 172.16.3.229, WAN IP Address: 172.16.3.229

Apply Cancel

圖 10-13 NAT 穿越設置

有三個選項可供用戶選擇：**Disable(關閉)**、**Manually Input NAT IP Address(手工輸入 NAT IP 位址)**和 **Auto Discover NAT IP Address(自動偵測 NAT IP 位址)**。

<b>Disable(關閉)</b>	如果 Vigor 3300 具有公眾網 IP，則可以關掉此功能。
--------------------	----------------------------------

<b>Manually Input NAT IP Address(手工輸入 NAT IP 位址)</b>	
<b>NAT IP Address (NAT IP 地址)</b>	如果用戶的 Vigor 3300 在 NAT 後，同時 NAT 設備具有靜態的公網 IP，則在此輸入該 IP 位址。
<b>Auto Discover NAT IP Address(自動偵測 NAT IP 位址)</b>	
<b>STUN Local Port (STUN 本地埠)</b>	設定 STUN 的本地埠。
<b>STUN Server Address (STUN 伺服器地址)</b>	設定 STUN 伺服器的 IP 位址。
<b>STUN Server Port (STUN 伺服器埠)</b>	設定 STUN 伺服器的埠。
<b>Symmetric Media</b>	
<b>Disable symmetric RTP and T.38</b>	關閉此一功能。
<b>Enable symmetric RTP and T.38</b>	啓用此一功能。

注意：“自動偵測 NAT IP 位址”選項只有當 Vigor 3300 在轉址後，且 NAT 器件使用動態公網 IP 時才有效，同時該功能必須配合 Internet 上的一台 STUN 伺服器才能工作。STUN 是一個應用層協議，用來告訴私有網路裡的 Vigor 3300 被 NAT 以後的 IP 地址，STUN 伺服器配合 Vigor 3300 才能使 Vigor 3300 的 STUN 功能正常使用。

## 10.10 Incoming Call Barring(來電撥入限制)

此功能用來對 VoIP 來電進行篩選，用戶可以設置規則，由路由器對來電進行拒接或透過的操作。用戶可以設置 5 個篩選組，預設的情形為所有的 VoIP 來電都可透過。

### 10.10.1 Set(設定)

**VoIP - Incoming Call Barring - Set**

**Barring Class**  
 Allow only calls from speed dial entries

**Match Method**

Name:  Disable  Enable  
 Remind: match username in speeddial destination

IP/Domain:  Disable  Enable  
 Remind: match hostname in speeddial destination

**Speed Dial Entries**  
 From: 1 To: 150

Apply Cancel

圖 10-14 設定

<b>Barring Class</b> (限制類別)	有五個選項供用戶選擇： 允許所有的電話號碼。 僅允許列表中的電話 僅允許快速撥號項目中電話號碼 拒絕在拒絕列表中的電話號碼 拒絕所有撥入電話。
<b>Match Method(匹配方法)</b>	
<b>Name(名稱)</b>	選擇 <b>Disable(關閉)</b> 則不檢查“快速撥號”中的名稱欄。 選擇 <b>Enable(啓動)</b> 則檢查“快速撥號”中名稱一欄。
<b>IP/Domain</b>	選擇 <b>Disable(關閉)</b> 則不檢查“快速撥號”中的 IP/ Domain 名稱欄。 選擇 <b>Enable(啓動)</b> 則檢查“快速撥號”中的 IP/ Domain 名稱欄。
<b>Speed Dial Entries</b> (快速撥號項目)	設置檢查快速撥號號碼的範圍，預設值為從 1 到 30。

### 10.10.2 Allow List(允許列表)

**VoIP - Incoming Call Barring - Allow List**

#	Name	IP/Domain
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
Example	John	192.168.1.1 or iptel.org

1 2 3 4 5 6

圖 10-15 允許列表設定

<b>Name(名稱)</b>	設定該項的名稱。
<b>IP/Domain</b>	設定該項的 IP 位址或功能變數名稱。 如果對方已經註冊了 SIP 帳號，則填入 SIP 代理伺服器的功能變數名稱；如果對方沒有註冊 SIP 帳號，則填入對方的靜態 IP 位址或動態功能變數名稱。

注意：Vigor3300 系列路由器支援 30 個允許列表。

### 10.10.3 Deny List (拒絕列表)

**VoIP - Incoming Call Barring - Deny List**

#	Name	IP/Domain
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
Example	John	192.168.1.1 or iptel.org

1 2 3 4 5 6

圖 10-16 拒絕列表設置

<b>Name(名稱)</b>	設置該拒絕項的名稱。
<b>IP/Domain</b>	設置該拒絕項的 IP 位址或者功能變數名稱。 如果對方已經註冊了 SIP 帳號，則填入 SIP 代理伺服器的功能變數名稱；如果對方沒有註冊 SIP 帳號，則填入對方的靜態 IP 位址或動態功能變數名稱。

注意：Vigor3300 系列路由器支援 30 個拒絕列表。

## 10.11 Status(連接狀態)

按 **VoIP>>Status(VoIP>>連接狀態)**，出現如下圖所示配置頁面：

**VoIP - Status**

Refresh Option:

#	Register Status	Call Status	Call Type	Caller Number	Callee Number	Start Time	Remote RTP Address	Remote RTP Port	RTP Statistic	Codec Type	Packet Period	VAD	DTMF Relay
1		Idle											
2		Idle											
3		Idle											
4		Idle											
5		Idle											
6		Idle											
7		Idle											
8		Idle											

\* PS: Packets Sent, OS: Octets Sent, PR: Packets Received, OR: Octets Received, PL: Packets Lost, JI: Interarrival Jitter Estimate(ms), LA: Avg TX Delay(ms)

圖 10-17 VoIP 連接狀態

該頁可以顯示每個介面通話狀態的一些資訊。

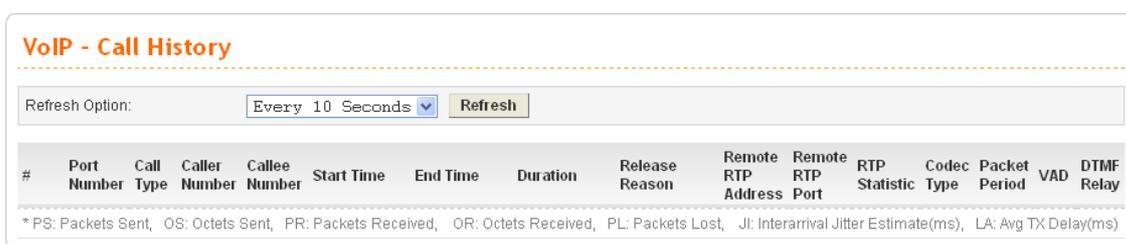
<b>Refresh Option (更新選項)</b>	選擇更新項目然後按 <b>Refresh(更新)</b> 按鈕更新本頁訊息。
------------------------------	--

<b>Register Status</b> (註冊狀態)	介面的註冊狀態
<b>Call Status</b> (呼叫狀態)	介面的通話狀態
<b>Call Type</b> (撥號類型)	顯示撥入或者撥出。
<b>Caller Number</b> (撥出號碼)	顯示呼叫號碼。
<b>Callee Number</b> (被呼叫號碼)	顯示被呼叫號碼。
<b>Start Time</b> (開始時間)	顯示通話開始時間
<b>Remote RTP Address</b> (遠端 RTP 地址)	顯示通話對方 IP 位址。
<b>Remote RTP Port</b> (遠端 RTP 埠)	顯示通話對方埠。
<b>RTP Statistic</b>	
<b>Codec Type</b> (編碼類型)	顯示通話資料編碼類型。
<b>Packet Period</b> (封包週期)	顯示每個 VoIP 資料封包的採集時間。
<b>VAD</b>	顯示 VAD 狀態。
<b>DTMF Relay</b>	顯示 DTMF 狀態。

用戶可以按 **Refresh(更新)**來更新以上資訊，路由器會每隔 10 秒鐘自動更新該資訊。

## 10.12 Call History(呼叫歷史記錄)

此頁顯示所有歷史通話記錄的資訊。



**VoIP - Call History**

Refresh Option:

#	Port Number	Call Type	Caller Number	Callee Number	Start Time	End Time	Duration	Release Reason	Remote RTP Address	Remote RTP Port	RTP Statistic	Codec Type	Packet Period	VAD	DTMF Relay
---	-------------	-----------	---------------	---------------	------------	----------	----------	----------------	--------------------	-----------------	---------------	------------	---------------	-----	------------

\* PS: Packets Sent, OS: Octets Sent, PR: Packets Received, OR: Octets Received, PL: Packets Lost, JI: Interarrival Jitter Estimate(ms), LA: Avg TX Delay(ms)

圖 10-18 VoIP 連接歷史記錄狀態

<b>Refresh Option</b> (更新選項)	選擇更新項目然後按 <b>Refresh(更新)</b> 按鈕更新本頁訊息。
<b>Port Number</b> (埠號)	顯示撥打 VoIP 的埠號。
<b>Call Type</b> (撥號類型)	顯示撥入或者撥出。
<b>Caller Number</b> (撥出號碼)	顯示主叫號碼。

<b>Callee Number</b> (被呼號碼)	顯示被叫號碼。
<b>Start Time</b> (開始時間)	顯示通話開始時間。
<b>End Time</b> (終止時間)	顯示通話結束時間。
<b>Duration</b> (持續時間)	顯示通話持續時間。
<b>Release Reason</b> (釋放原因)	顯示斷開電話的原因。
<b>Remote RTP Address</b> (遠端 RTP 地址)	顯示通話對方 IP 位址。
<b>Remote RTP Port</b> (遠端 RTP 埠)	顯示通話對方埠。
<b>RTP Statistic</b> (RTP 統計)	顯示 RTP 統計資訊。
<b>Codec Type</b> (編碼類型)	顯示通話資料編碼類型。
<b>Packet Period</b> (封包週期)	顯示每個 VoIP 資料封包的採集時間。
<b>VAD</b>	顯示 VAD 狀態。
<b>DTMF Relay</b>	顯示 DTMF 狀態。

用戶可以按 **Refresh**(更新)來更新以上資訊，路由器會每隔 10 秒鐘自動更新該資訊。