Multi Homing Gateway

使 用 手 冊

Doc. No.:120602-05

目　　錄

第一章 系統管理 ---------- 5

管理員 7

系統設定 11

時間設定 18

Multiple NAT 19

駭客預警 24

指定路由表 26

動態 IP 位址 30

DNS 代理伺服器 32

動態 DNS 36

軟體更新 41

第二章 介面位址 ---------- 43

內部網路介面位址 44

外部網路介面位址 45

第三章 位址表 ---------- 55

內部網路 56

內部網路群組 60

外部網路 64

外部網路群組 68

第四章 服務表 ---------- 73

基本服務 74

自訂服務 75

服務群組 82

第五章 排程表 ---------- 87

第六章 管制條例 ---------- 93

內部至外部 95

外部至內部 102

第七章 虛擬私有網路 109
自動加密驗證 110
PPTP 伺服器 115
PPTP 用戶端 121
第八章 內容管制 127
網站管制 128
Script 管制 133
第九章 虛擬伺服器 135
IP 對映 137
虛擬伺服器 1/2/3/4 141
虛擬伺服器服務 146
第十章 監控記錄 153
流量監控 154
事件監控 157
監控報告 160
第十一章 警示記錄 163
流量警示 164
事件警示 167
第十二章 流量統計 171
流量統計 172
第十三章 系統狀態 175
介面狀態 176
ARP 表 178
DHCP 用戶表 179

操作範例 181

1. 內部至外部管制條例 181
2. 管制條例與位址表應用 184
3. 虛擬伺服器設定 187
4. 虛擬私有網路應用 191

第一章

系 統 管 理

所謂的系統管理，廣義的定義是指進出路由分配器系統的權限、路徑位址與監控等各種相關設定的管理，在本單元中則定義爲管理員、系統設定與軟體更新的設定與管理。

路由分配器的管理由系統主管理員設定。系統主管理員可增加修改系統的各項設定，監控系統狀態，而其他管理員（管理員名稱由系統主管理員設定）僅能讀取系統各項設定資料，不能予以更改。在本【系統管理】單元中：

【管理員】：系統主管理員，可依需求新增與變更次管理員人數與名單，或更改次管理員的密碼。

【系統設定】：系統主管理員，可經由此功能，將先前儲存的路由分配器系統各單元設定檔，匯出至用戶端硬碟中備份；或將備份的設定檔匯入至路由分配器系統以修正/更改路由分配器設定；以及將路由分配器設定恢復至原出廠設定值。同時，系統主管理員也可利用此單元中的【E-Mail 設定】功能，設定路由分配器在遭受駭客侵入時，即時自動傳送警訊通知系統管理員,紀錄經由【到路由分器封包】設定此功能會將路由分配器的所有進出封包均紀錄下來方便進行管制, 【重新啓動路由分配器】可以重新開機啓動路由分配器。

【時間設定】：可將路由分配器的系統時間設定爲與內部使用者電腦或外部時間伺服器電腦時間同步。

【Multiple NAT】：內部網路可支援多個區段的網路位址。

【駭客預警】：建立路由分配器各項偵測功能。系統管理員可利用此功能設

定，啓動路由分配器自動偵測功能，當系統發生異常現象時，路由分配器將會發出電子郵件警告系統管理員，同時將警告訊息顯示在【警示記錄】之【事件警示】視窗中。

【指定路由表】：系統管理員於此單元中，定義企業網路架構內之內部網路或外部網路，在資料封包傳遞至某特定網域時，所設定之閘道位址。

【動態 IP 位址】：系統管理員於此單元中，定義、開啓動態 IP 位址（DHCP）組態的各項參數位址與功能。

【DNS 代理伺服器】：系統管理員可利用此 DNS 代理伺服器功能，指定公司內部伺服器的網域名稱對應到內部及非軍事區，電腦或伺服器的 IP 位址。

【動態 DNS】：可讓浮動 IP 使用者做即時更新 DNS 與 IP 對映的功能。【管理位址】：此功能可設定被允許進入防火牆設定畫面的網路位址，經由此功能，非設定條例所允許的網路位址在企圖連線防火牆的介面位址時，都將被系統認定爲不可信任之網路位址而將其阻擋掉。

【軟體更新】：使用者可至本公司網站上，下載最新、功能更強的軟體程式，系統主管理員可利用本功能，更新路由分配器軟體，幫助您將路由分配器發揮最大效用。

路由分配器之【管理員】功能設定

步驟**1.** 在左方的功能選項中，點選【系統管理】功能，進入【管理員】設定視窗。*（如圖 1-1）*

圖 1-1 點選【系統管理】之【管理員】功能設定選項

步驟**2.** 【管理員】表格說明：

- 管理員名稱：admin 爲本路由分配器預設系統管理員名稱無法刪除。
- 權限：本路由分配器管理員的使用權限。可分爲主管理員與次管理員。
- 組態：管理員之組態設定。點選表格下方【變更】功能修改主/次管理員密碼，或點選【刪除】功能以刪除次管理員。
- 管理員：系統主管理員。主管理員之系統使用權限爲【讀/寫】，亦即可更改系統設定、監控系統狀態、新增、刪除次管理員等。
- 次管理員：次管理員。次管理員名稱由主管理員設定，其系統使用權限爲【讀】，所有次管理員只能讀取系統狀態、監控系統狀態，無法更改任何系統設定值。

變更主/次管理員密碼

步驟**1.** 在【管理員】的表格中，找到欲變更設定的管理員名稱，對應至右方【變更】欄，點選【修改】。*（如圖 1-1）*

步驟**2.** 在【變更管理員密碼】視窗中。鍵入下列資料：

- 密碼：鍵入原使用密碼。
- 新密碼：鍵入新密碼。
- 確認密碼：鍵入與上列新密碼欄一致的字串。*（如圖 1-2）*

步驟**3.** 點選【確認】修改密碼，或點選【取消】取消變更設定。

圖 1-2 變更管理員密碼

新增次管理員

步驟**1.** 在【管理員】設定視窗中，點選螢幕下方【新增次管理員】功能按鈕。*(如圖 1-1)*

步驟**2.** 在【新增管理員】視窗中，鍵入以下資料：*(如圖 1-3)*

- 次管理員名稱：鍵入欲新增之次管理員名稱。
- 密碼：鍵入密碼。
- 確認密碼：鍵入與上列密碼欄一致的字串。

步驟**3.** 點選【確定】以登錄使用者，或點選【取消】取消新增管理員。

圖 1-3 新增次管理員

刪除次管理員

步驟**1.** 在【管理員】的表格中，找到欲變更設定的管理員名稱，對應至右方的【變更】欄，點選【刪除】。*(如圖 1-1)*

步驟**2.** 螢幕上會立即產生【刪除管理員】的確認對話框。*(如圖 1-4)*

步驟**3.** 依照對話框所示，點選【確定】刪除該次管理員，或點選【取消】取消刪除。

圖 1-4 刪除次管理員

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【系統設定】，進入【系統設定】工作視窗。*（如圖 1-5）*

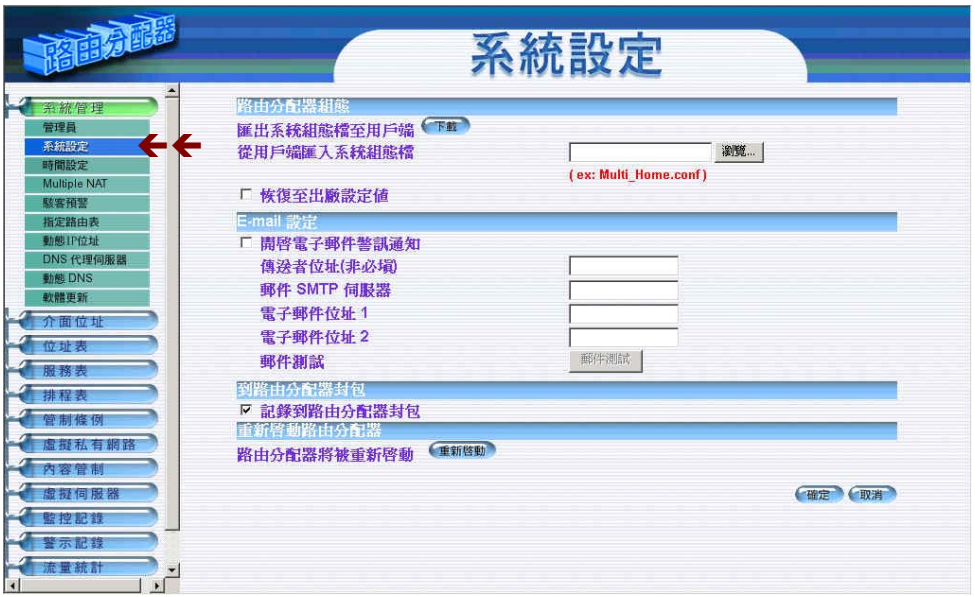

圖 1-5 【系統管理】功能之【系統設定】工作視窗

匯出路由分配器組態設定檔

步驟**1.** 先點選左方功能選項中的【系統管理】，接著點選下方的【系統設定】，進入【系統設定】工作視窗。*（如圖 1-5）*

步驟**2.** 在【系統設定】視窗中，點選【路由分配器組態】下【匯出路由分配器組態設定檔】右方的【下載】功能按鈕 。

步驟**3.** 在出現【檔案下載】視窗中，選擇【將這個檔案儲到磁碟】，按下確定，接著指定匯出檔案所要儲存的目的位置，再按下【確定】。路由分配器設定檔即會複製至指定儲存位置。*（如圖 1-6）*

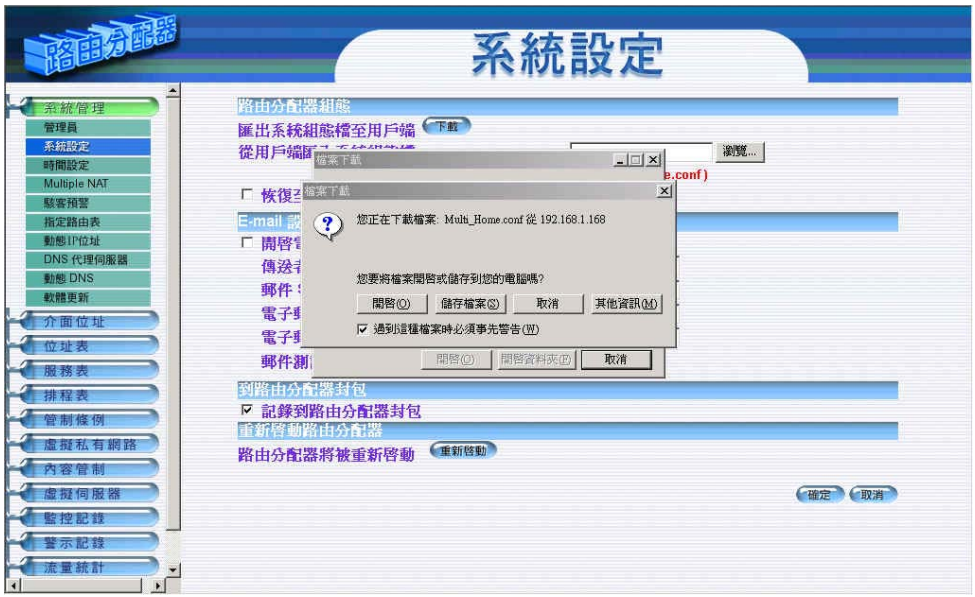

圖 1-6 擇匯出檔案所要儲存的目的位置

匯入路由分配器組態設定檔

步驟**1.** 先點選左方功能選項的【系統管理】，接著點選下方的【系統設定】，進入【系統設定】工作視窗。*（如圖 1-5）*

步驟**2.** 在【系統設定】視窗中，點選【路由分配器組態】下【匯入路由分配器組態設定檔】右方的【瀏覽】功能按鈕。

步驟**3.** 在出現的【選擇檔案】視窗中，選擇之前編輯儲存的路由分配器設定檔所在的目錄位置，選擇檔名後，再點選【開啓】。*（如圖 1-7）*

步驟**4.** 點選螢幕右下方【確定】按鈕，將檔案匯入至路由分配器。

圖 1-7 匯入檔案所在目錄位置與檔名

恢復原出廠設定值

步驟**1.** 先點選左方功能選項的【系統管理】，接著點選下方的【系統設定】，進入【系統設定】工作視窗。*（如圖 1-5）*

步驟**2.** 在【系統設定】視窗中，勾選【路由分配器組態】下【恢復原出廠設定值】。

步驟**3.** 點選螢幕右下方【確定】按鈕。恢復路由分配器原出廠時的設定值。*（如圖 1-8）*

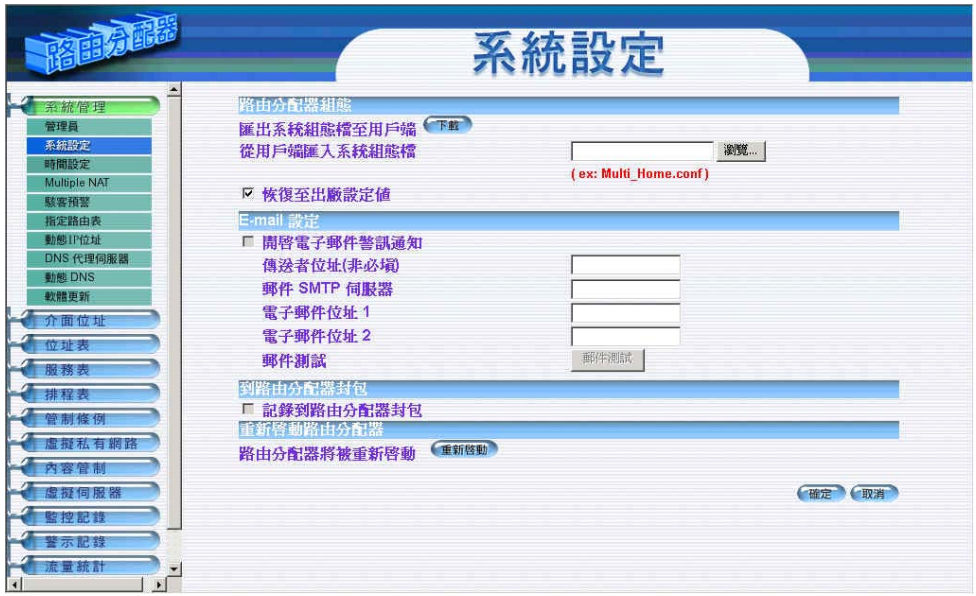

圖 1-8 勾選【恢復原出廠設定值】

設定即時警訊通知

步驟**1.** 先點選左方功能選項的【系統管理】，接著點選下方的【系統設定】，進入【系統設定】工作視窗。*（如圖 1-5）*

步驟**2.** 勾選【**E-Mail 設定**】下之【啓動 E-mail 警訊通知】。開啓此功能後，本路由分配器系統在任何時候遭受駭客侵入或出現緊急事件時，將自動且即時傳送警訊通知系統管理員。（各種駭客攻擊偵測，可於【系統管理】之【駭客預警】功能設定。）

步驟**3.** 傳送者位址(非必填)：在空格中可輸入傳送者的名稱或電子郵件。

步驟**4.** 郵件 SMTP 伺服器：在空格中輸入遞送電子郵件的 SMTP 伺服器 IP 位址。

步驟**5.** 電子郵件位址 1：在空格內輸入第一位接受警訊通知的電子郵件位址。

步驟**6.** 電子郵件位址 2：在空格內輸入第二位接受警訊通知的電子郵件位址。

步驟**7.** 郵件測試：點選旁邊【**郵件測試**】可測試電子郵件位址 1
電子郵件位址 2 ,輸入的電子郵件是否能正確收到警訊

步驟**8.** 點選螢幕右下方【確定】設定警訊傳送功能。*（如圖 1-9）*

圖 1-9 啓路由分配器即時傳送警訊功能

設定到路由分配器封包

步驟**1.** 先點選左方功能選項的【系統管理】，接著點選下方的【系統設定】，進入【系統設定】工作視窗。*（如圖 1-5）*

步驟**2.** 勾選【記錄到路由分配器封包】。開啓此功能後，本路由分配器系統在任何時候會將進出路由分配器的封包紀錄下來，供系統系統管理員使用。*（如圖 1-10）*

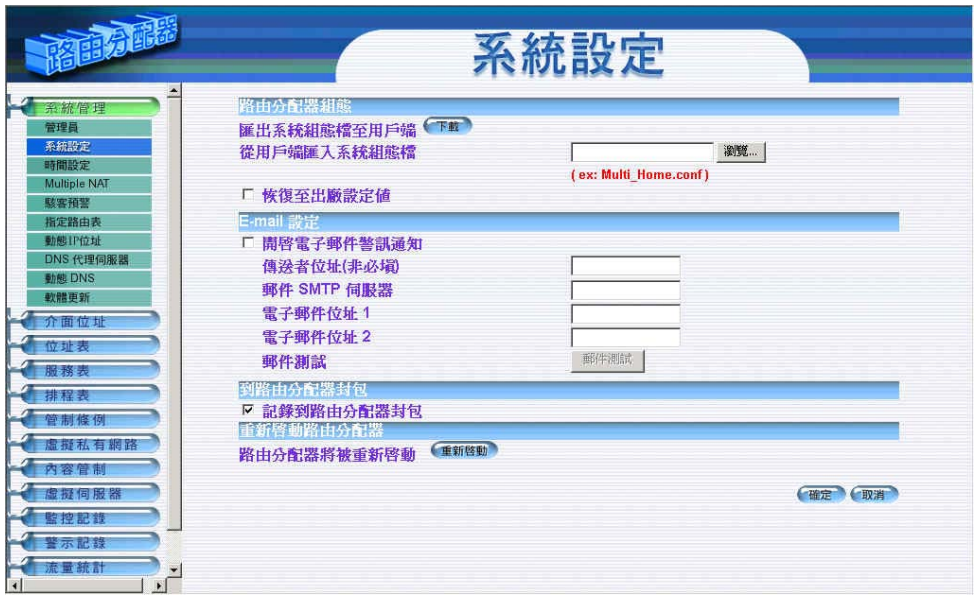

圖 1-10 開啓到路由分配器封包功能

設定路由分配器重新啓動

步驟**1.** 先點選左方功能選項的【系統管理】，接著點選下方的【系統設定】，進入【系統設定】工作視窗。*（如圖 1-5）*

步驟**2.** 路由分配器重新啓動：點選旁邊**【重新啓動】**

步驟**3.** 螢幕上會立即產生【你確定要重新啓動】的確認對話框。

步驟**4.** 依照對話框所示，點選【確定】重新啓動路由分配器，或點選【取消】取消刪除。*（如圖 1-11）*

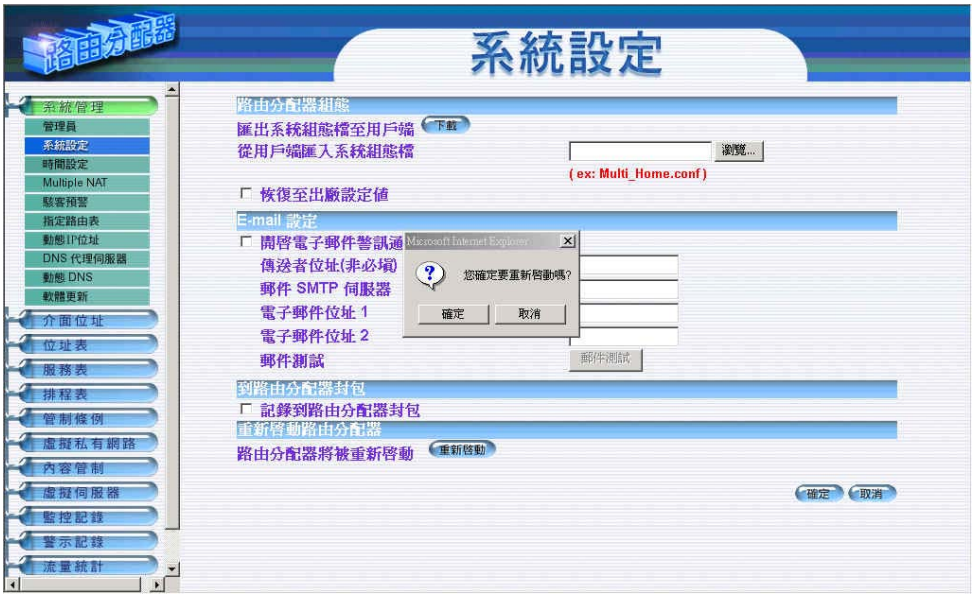

圖 1-11 開啓路由分配器重新啓動功能

系統時間設定

可將路由分配器的系統時間設定與內部使用者電腦或外部時間伺服器電腦時間同步。

步驟**1.** 先點選左方功能選項的【系統管理】，接著點選下方的【時間設定】，進入【時間設定】工作視窗。*（如圖 1-12）*

步驟**2.** 勾選【開啓與外部時間伺服器同步】。

步驟**3.** 可點選下拉式選單設定與 GMT 相差時間(以小時爲單位)。

步驟**4.** 可輸入外部時間伺服器網路位址。

步驟**5.** 可設定路由分配器的系統時間每隔多少時間與外部時間伺服器自動更新路由分配器的系統時間，也可選擇輸入 0 表示不自動更新。

步驟**6.** 點選系統時間與此用戶電腦同步【**同步**】,則路由分配器的系統時間會與此用戶電腦的時間同步。

步驟**7.** 點選螢幕右下方【確定】設定功能。*（如圖 1-12）*

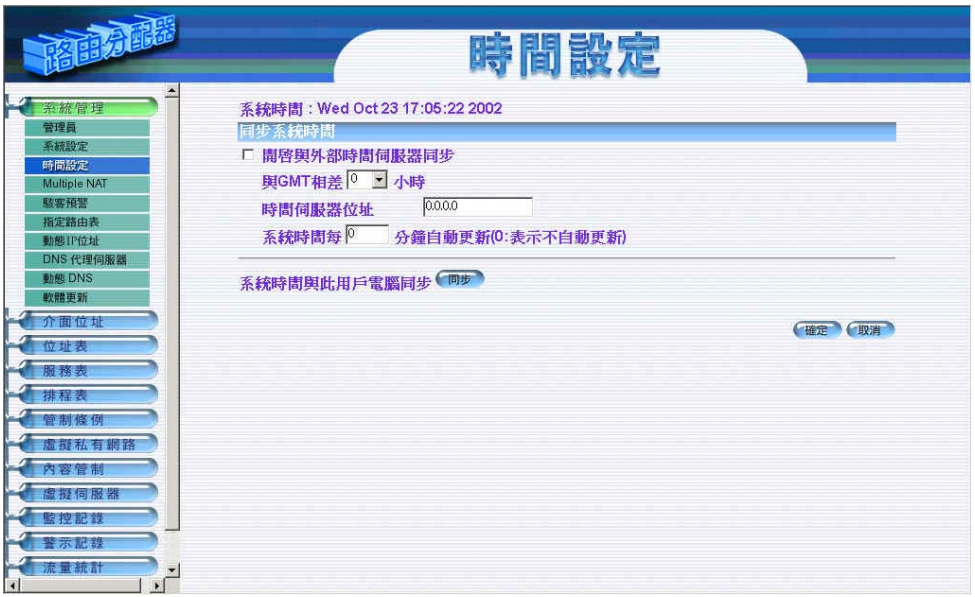

圖 1-12 系統時間設定

Multiple NAT 功能設定

可讓內部網路設定多個網段位址，並可經由不同的外部位址與網際網路建立連線。

例如：公司的專線申請到多個真實 IP 位址 168.85.88.0/24，公司內部也分爲許多的部門，研發部、客服部、業務部、採購部、會計室等，爲了方便管理可將各部門以不同 IP 網段來區分。設定方式如下：

1.研發部網段 192.168.1.11/24(Internal) ←→ 168.85.88.253(External)
2.客服部網段 192.168.2.11/24(Internal) ←→ 168.85.88.252(External)
3.業務部網段 192.168.3.11/24(Internal) ←→ 168.85.88.251(External)
4.採購部網段 192.168.4.11/24(Internal) ←→ 168.85.88.250(External)
5.會計室網段 192.168.5.11/24(Internal) ←→ 168.85.88.249(External)

第 1 項在介面位址設定時就設定好了，其他 4 項就必須新增在 Multiple NAT，設定完成後每個部門就會從不同的外部 IP 位址出去，各部門的電腦設定如下

客服部　IP 位址　　：192.168.2.1
　　子網路遮罩：255.255.255.0
　　預設閘道　：192.168.2.11

其他部門也是按照所屬之區段來設定，這就是 Multiple NAT 的功能。

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【Multiple NAT】，進入【Multiple NAT】工作視窗。*（如圖 1-13）*

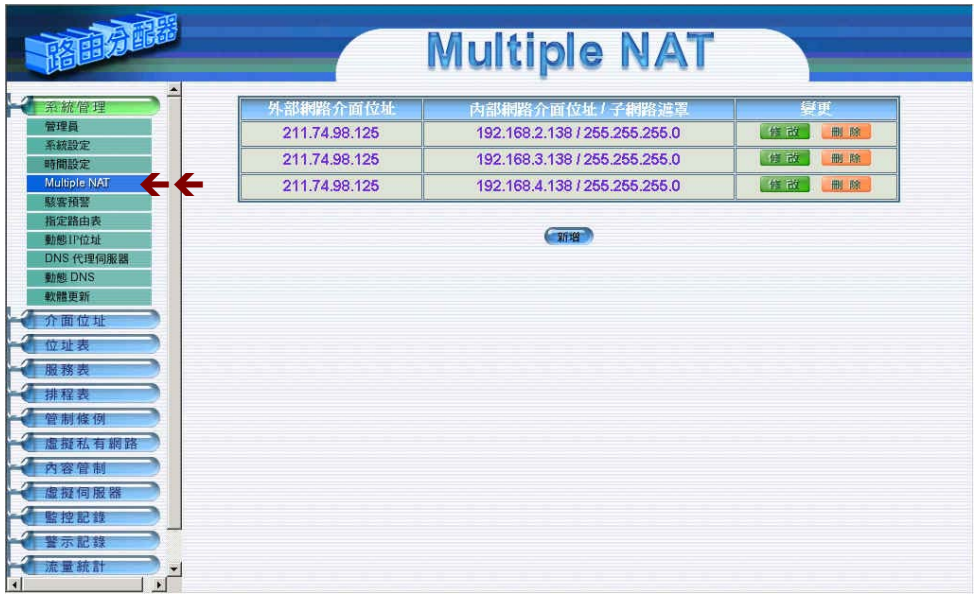

圖 1-13　進入 Multiple NAT 功能設定

Multiple NAT 工作視窗名詞定義：

- 外部網路介面位址：外部網路之 IP 位址。
- 內部網路介面位址/子網路遮罩：內部網路之 IP 位址及遮罩。
- 變更：變更網路管制中各項設定值。點選【修改】，可修改網路管制各項參數；點選【刪除】，可刪除該項設定。

新增 Multiple NAT

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【Multiple NAT】，進入【Multiple NAT】工作視窗。*（如圖 1-13）*

步驟**2.** 點選下方【新增】網路管制功能按鈕。

步驟**3.** 在新視窗網站名稱空欄中，鍵入 IP 位址。*（如圖 1-14）*

- 外部網路介面位址 ： 選擇外部網路之 IP 位址。
- 外部網路介面位址 ： 鍵入內部網路之 IP 位址。
- 子網路遮罩：鍵入內部網路的子網路遮罩。

步驟**4.** 點選【確定】新增 Multiple NAT，或【取消】取消新增。

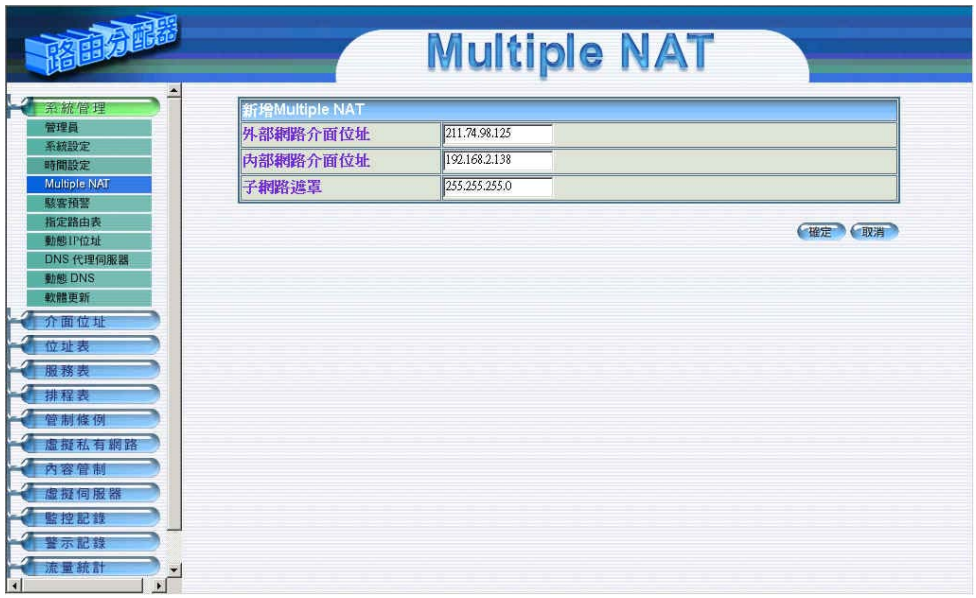

圖 1-14　新增 Multiple NAT

變更 Multiple NAT

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【Multiple NAT】，進入【Multiple NAT】工作視窗。*（如圖 1-13）*

步驟**2.** 在【Multiple NAT】的表格中，找到欲變更設定的 IP 位址，對應至右方【變更】欄，點選【修改】。

步驟**3.** 在【修改 Multiple NAT】視窗中，鍵入新的 IP 位址。*（如圖 1-15）*

步驟**4.** 點選螢幕下方【確定】按鈕，變更設定，或 點選【取消】取消變更。

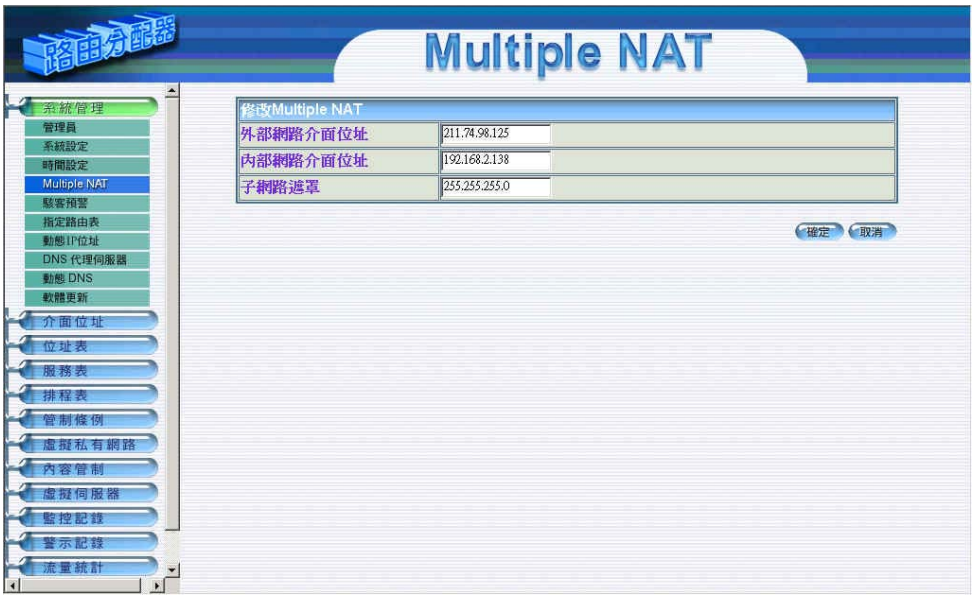

圖 1-15　變更 Multiple NAT

移除 Multiple NAT

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【Multiple NAT】，進入【Multiple NAT】工作視窗。*（如圖 1-13）*

步驟**2.** 在【Multiple NAT】的表格中，找到欲刪除設定的 IP 位址，對應至右方【變更】欄，點選【刪除】。

步驟**3.** 在【確定刪除】對話框中，點選【確定】按鈕，移除設定，或 點選【取消】取消移除。*（如圖 1-16）*

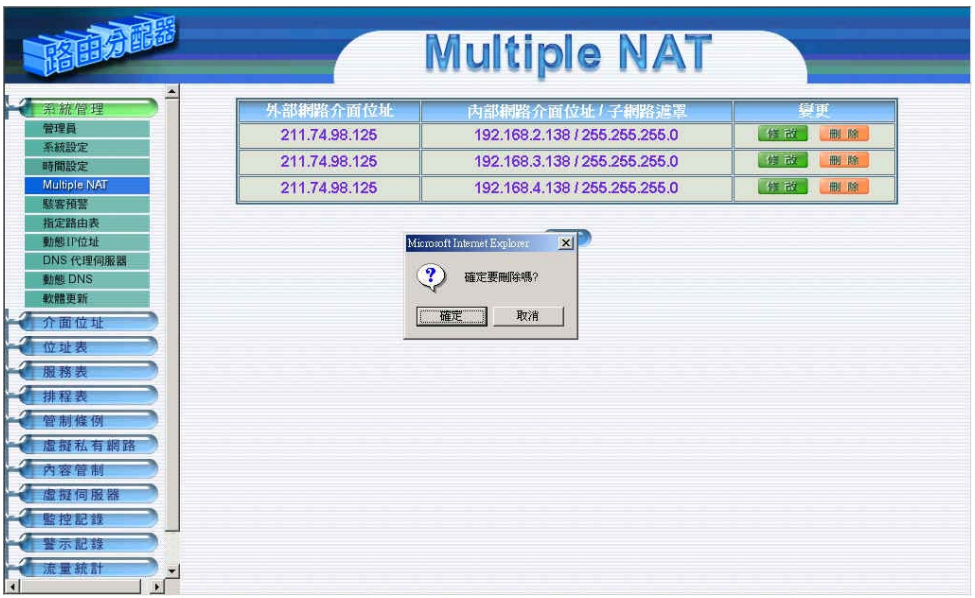

圖 1-16　移除 Multiple NAT

駭客預警功能設定

步驟**1.** 在左方的功能選項中，點選【系統管理】功能，再點選【駭客預警】次功能選項。*（如圖 1-17）*

步驟**2.** 【駭客預警】各項偵測功能說明 *（如圖 1-17）*

圖 1-17 設定路由分配器各項偵測功能

- 偵測 SYN 攻擊：偵測當駭客連續送出TCP SYN資料封包給伺服器，企圖將伺服器連線（Connection ）資源耗光，使其他使用者無法連線成功的狀況。勾選此項後，系統管理員可於右方【允許SYN最大流量】空格中，定義每秒可通過路由分配器的最大封包數(Pkts/Sec)。
- 偵測 ICMP 流量：偵測當駭客連續發出PING的資料封包，且是以廣播方式（Broadcast）送給網路內每部機器的狀況。勾選此項後，系統管理員可於【允許ICMP最大流量】空格中，定義每秒可通過路由分配器的最大封包數(Pkts/Sec)。
- 偵測 UDP 流量：同ICMP Flood。勾選此項後，系統管理員可於【允許UDP最大流量】空格中，定義每秒可通過路由分配器的最大封包

數(Pkts/Sec)。

- 偵測 Ping of Death 攻擊：偵測當駭客送出的PING資料封包帶有大量垃圾資料，導致某些系統收到這些資料後產生不良反應，如：執行效率變慢，或系統毀壞必須重新開機，才可正成運作的狀況。
- 偵測 IP Spoofing 攻擊：偵測當駭客僞造成合法的使用者企圖穿越路由分配器入侵系統。
- 偵測 Port Scan 攻擊：偵測當駭客連續發出掃瞄偵測伺服器開放的埠號（Port ID），當伺服器對某些Port的偵測有反應時，駭客即可針對此Port攻擊的狀況。
- 偵測 Tear Drop 攻擊：偵測當IP資料封包在傳送過程中會被分段切割，而在目的地組合起來。如果攻擊者送出自訂的封包，強迫分段成爲負值的長度，有些系統會將此負值誤認爲很大的數值，而將大量的資料複製進系統，導致系統損毀、停機或重新開機的狀況。
- 過濾 IP Route 選擇：IP封包中有個選項，可以指定封包回傳時所用的目的位址，且此位址可與IP封包標頭中的來源位址不同。駭客可利用此種封包僞裝的IP位址進入網域中，並將網域中的資料回傳給駭客。勾選這個功能，可以阻擋使用此種選項的IP封包。
- 偵測 Land 攻擊：有些系統接收到來源位址與目的位址相同，來源埠號與目的埠號相同，且TCP封包標頭中的「SYN」標記又被設定時，會因此處理不當而當機。勾選這個功能即可偵測此種不正常的封包。

步驟**3.** 勾選各項偵測功能後，點選螢幕左下方【確定】按鈕。

完成此部分設定後，當系統偵測到任何異常現象時，會立即將警告訊息顯示在【警示記錄】之【事件警示】視窗中。系統管理員亦可於【系統設定】中開啓電子郵件警訊通知功能，路由分配器將會自動發出電子郵件警告系統管理員。

【指定路由表】設定功能

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【指定路由表】，進入【指定路由表】工作視窗。*（如圖 1-18）*

圖 1-18 【指定路由表】功能設定

步驟**2.** 指定路由表工作視窗的表格名詞定義：

- 介面位址：目的網域所屬區域，爲內部網路、外部網路或區域網路。
- 目的位址：連結目的網域之 IP 位址。
- 子網路遮罩：連結目的網域之子網路遮罩。
- 閘道位址：連結目的網域之閘道位址。
- 變更：變更路由表中各項設定值。點選【修改】，可修改指定路由表各項參數資訊；點選【刪除】，可刪除該項設定。

新增網路閘道

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【新增】按鈕，進入【指定路由表】工作視窗。*（如圖 1-18）*

步驟**2.** 在【新增網路閘道】視窗中，鍵入欲新增網路閘道的目的位址、子網路遮罩、閘道位址等資料。*（如圖 1-19）*

步驟**3.** 在介面位址的下拉選單中，選擇欲連結的目的網域所屬區域（內部網路、外部網路）。

步驟**4.** 點選【確定】新增所指定的網路閘道，或點選【取消】取消設定。

圖 1-19 新增指定路由閘道

變更指定路由表中的網路閘道設定

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【指定路由表】，進入【指定路由表】工作視窗。*（如圖 1-18）*

步驟**2.** 在【指定路由表】的表格中，找到欲修改的網路名稱，對應至右方【變更】欄，點選【修改】。

步驟**3.** 在出現的【變更指定路徑】的視窗中，填入各項欲變更的路徑位址。

步驟**4.** 點選【確定】修改該指定網路區域，或點選【取消】取消修改。*（如圖 1-20）*

圖 1-20　變更指定路由表中的閘道設定

刪除指定路由表中的閘道設定

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【指定路由表】，進入【指定路由表】工作視窗。*（如圖 1-18）*

步驟**2.** 在【指定路由表】的表格中，找到欲移除的網路名稱，對應至右方【變更】欄，點選【刪除】。

步驟**3.** 在出現的【變更指定路徑】的視窗中，填入各項欲變更的路徑位址。*（如圖 1-21）*

步驟**4.** 在【確定移除】對話框中點選螢幕左下方【確定】執行刪除設定，或點選【取消】取消刪除。

圖 1-21 刪除指定路由表中的閘道設定

動態 IP 位址功能設定

若是內部網路電腦要從路由分配器取得固定 IP，須先至【位址表】的【內部網路】功能中，設定該電腦的 MAC 位址與欲配發的 IP 位址，並勾選下方的【從路由分配器取得固定 IP 位址】。

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【動態 IP 位址】，進入【動態 IP 位址】工作視窗。*（如圖 1-22）*

圖 1-22 動態 IP 位址設定

步驟**2.** 動態 IP 位址設定資訊：

- 子網域 ： 內部網路所屬網域。
- 子網路遮罩 ： 內部網路所屬網域遮罩。
- 閘道位址: 內部網路預設閘道。
- 廣播位址: 內部網路所屬網域廣播位址。

啓動動態 IP 位址功能

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【動態 IP 位址】，進入【動態 IP 位址】工作視窗。*（如圖 1-22）*

步驟**2.** 勾選【啓動動態 DHCP 伺服器】。並鍵入下列資訊 *（如圖 1-23）*

- 網域名稱：鍵入內部私有網域名稱。
- DNS 伺服器 ： 鍵入欲配發 DNS 伺服器之 IP 位址。
- 用戶 IP 位址範圍 1：於左邊欄位鍵入第一組可使用的起始 IP 位址；於右邊欄位鍵入第一組可使用的結束 IP 位址。
- 用戶 IP 位址範圍 2：於左邊欄位鍵入第二組可使用的起始 IP 位址；於右邊欄位鍵入第二組可使用的結束 IP 位址。（須爲同一網域）

步驟**3.** 點選【確定】執行動態 IP 位址支援功能，或【取消】取消啓動動態 IP 位址功能。

圖 1-23 啓動動態 IP 位址功能

DNS 代理伺服器功能設定

使用者自行架設伺服器，且已申請合法網域名稱，為使內部網路電腦可使用該網域名稱來連結此伺服器，必須先於此功能中將網域名稱對映至該伺服器在路由分配器後的虛擬 IP 位址。且內部網路電腦必須將其 DNS 伺服器設定值定義為在路由分配器【系統管理】介面位址中的「內部網路介面ＩＰ位址」。

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【DNS 代理伺服器】，進入【DNS 代理伺服器】工作視窗。*（如圖 1-24）*

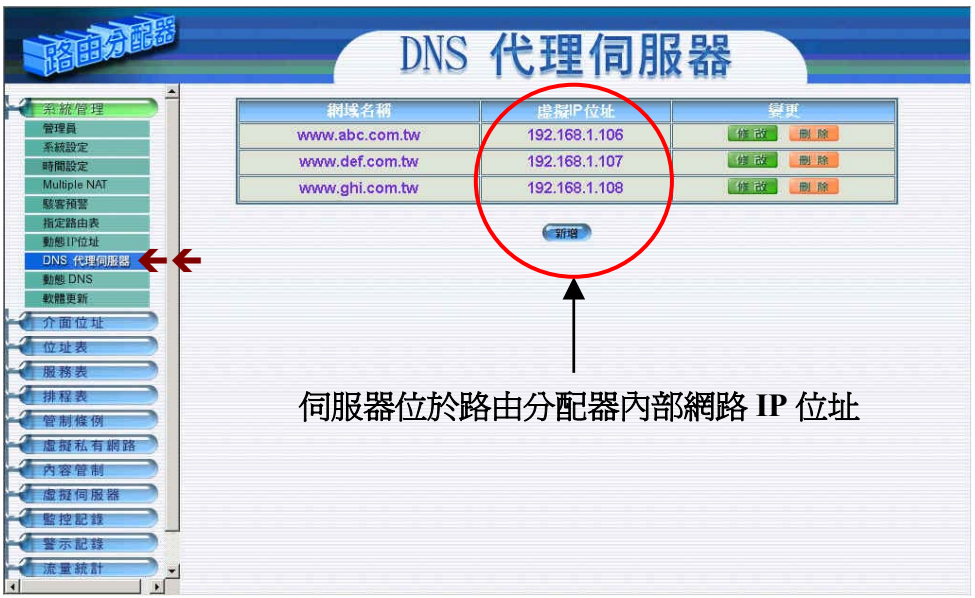

圖 1-24　DNS 代理伺服器功能

DNS 代理伺服器設定資訊：

- 網域名稱：內部或非軍事區內電腦的網域名稱位址。
- 虛擬 IP 位址：該網域名稱所對映之內部或非軍事區虛擬 IP 位址。
- 變更：變更 DNS 代理伺服器中各項設定值。點選【修改】，可修改 DNS 代理伺服器各項參數；點選【刪除】，可刪除該項設定。

要使用路由分配器的 DNS 伺服器功能，使用者 PC 端的第一個（主）DNS 伺服器一定要指向路由分配器的 IP，也就是電腦端所設定的預設閘道（Gateway）。

新增 DNS 代理伺服器

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【DNS 代理伺服器】，進入【DNS 代理伺服器】工作視窗。*（如圖 1-24）*

步驟**2.** 點選下方【新增】DNS 代理伺服器功能按鈕。

步驟**3.** 在【新增 DNS 代理伺服器】視窗中，鍵入相關參數。*（如圖 1-25）*

- 網域名稱：鍵入網域名稱。
- 虛擬 IP 位址 ： 鍵入該網域名稱所對映之虛擬 IP 位址。

步驟**4.** 點選【確定】新增 DNS 代理伺服器，或【取消】取消新增。

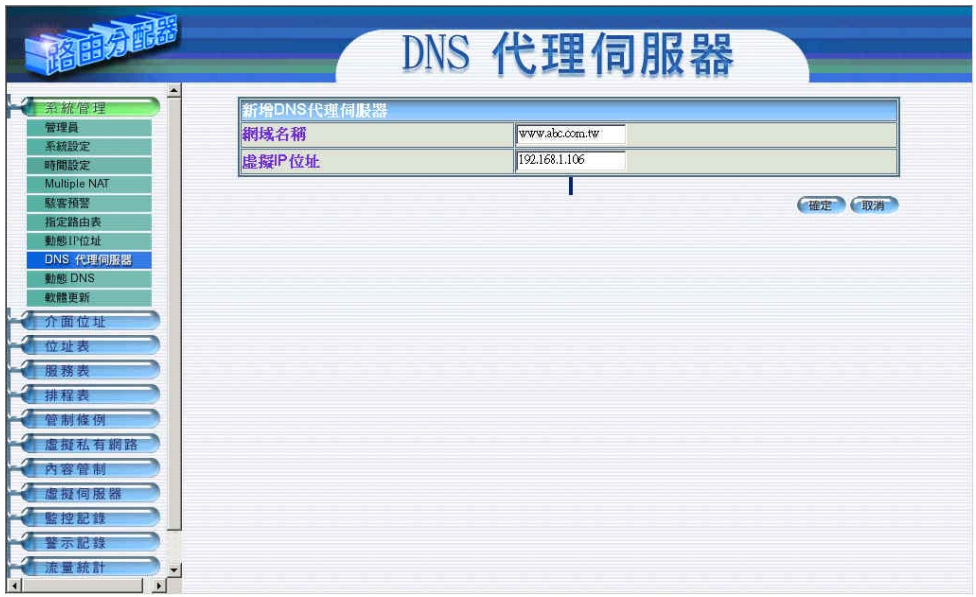

圖 1-25　新增 DNS 代理伺服器

變更 DNS 代理伺服器

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【DNS 代理伺服器】，進入【DNS 代理伺服器】工作視窗。*（如圖 1-24）*

步驟**2.** 在【DNS 代理伺服器】的表格中，找到欲變更設定的網域名稱，對應至右方【變更】欄，點選【修改】。

步驟**3.** 在【修改 DNS 代理伺服器】視窗中，鍵入各項欲變更參數。*（如圖 1-26）*

步驟**4.** 點選螢幕下方【確定】按鈕，變更設定，或 點選【取消】取消變更。

圖 1-26　變更 DNS 代理伺服器

刪除 DNS 代理伺服器

步驟**1.** 在左方的功能選項中，點選【系統管理】功能，再點選【DNS 代理伺服器】次功能選項。*（如圖 1-24）*

步驟**2.** 在【DNS 代理伺服器】的表格中，找到欲刪除設定的網域名稱，對應至右方【變更】欄，點選【刪除】。

步驟**3.** 在【確定移除】DNS 代理伺服器對話框中，點選【確定】按鈕，移除設定，或 點選【取消】取消移除。*（如圖 1-27）*

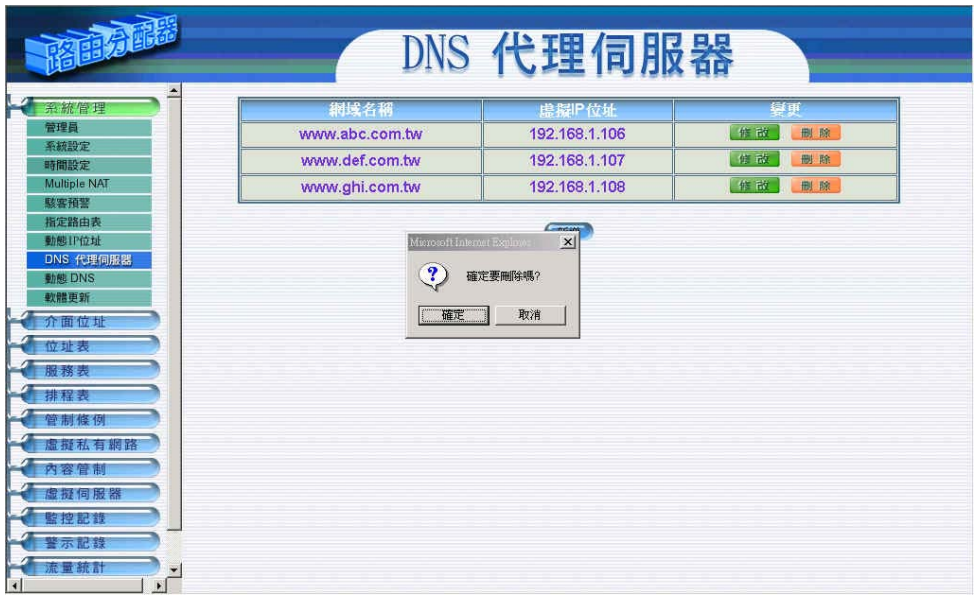

圖 1-27　移除 DNS 代理伺服器

動態 DNS 功能設定

設定動態 DNS，可讓使用浮動 IP 的使用者直接透過路由分配器就可以與提供動態 DNS 的服務網站做動態 DNS 與 IP 位址的對映。

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【動態 DNS】，進入【動態 DNS】工作視窗。*（如圖 1-28）*

圖 1-28 動態 DNS 功能設定

步驟**2.** 動態 DNS 工作視窗名詞定義：

- !：更新狀態。【連線中；連線時間逾時，更新失敗；更新成功；不明的錯誤】
- 網站名稱：申請的網站名稱。
- 外部網路位址：外部網路介面現在的 IP 位址。
- 變更：變更動態 DNS 中各項設定值。點選【修改】，可修改動態 DNS 各項參數；點選【刪除】，可刪除該項設定。

步驟**3.** 動態 DNS 使用方法：

路由分配器裡提供三家的服務廠商，使用者必須先到該網站註冊後才可使用此功能，其使用規章請參閱該服務商網站。

如何註冊：於左方功能選項，先點選【系統管理】，接著點選下方的【動態 DNS】，進入【動態 DNS】工作視窗，再按下新增按鈕，在服務提供者的右方，按下註冊去即出現該服務商的網站，註冊辦法請自行參閱網站說明。*（如圖 1-29）*

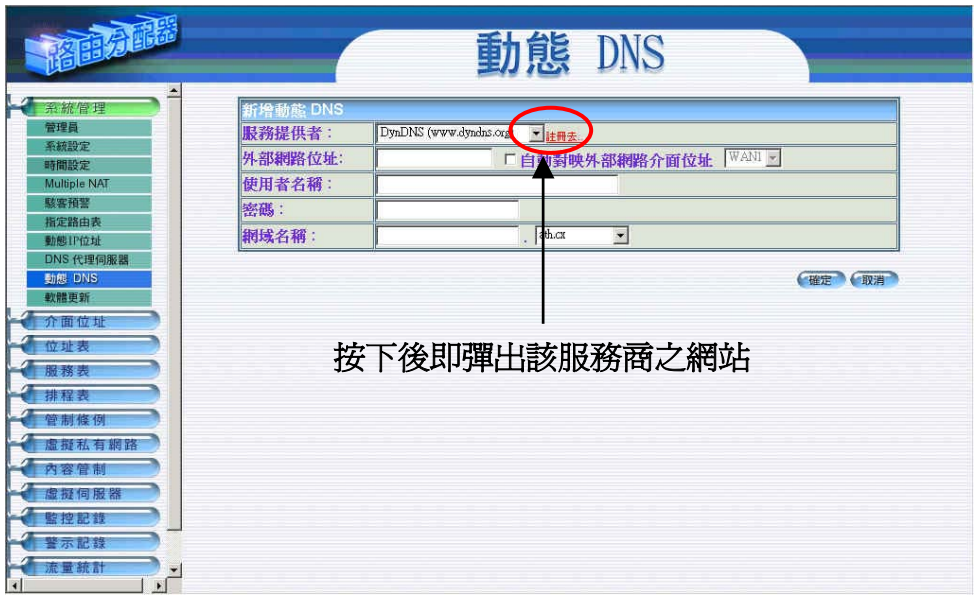

圖 1-29　動態 DNS 功能設定

新增動態 DNS

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【動態 DNS】，進入【動態 DNS】工作視窗。*（如圖 1-27）*

步驟**2.** 點選下方【新增】動態 DNS 功能按鈕。

步驟**3.** 在新視窗空欄中，鍵入相關資訊。*（如圖 1-30）*

- 服務提供者：選擇服務提供廠商。
- 註冊去：到該服務廠商之網站。
- 外部網路位址：路由分配器外部介面位址之 IP。
- 自動對映外部網路介面位址：自動將外部介面位址填入
- 選擇對應的外部網路爲 WAN 1 / 2。
- 使用者名稱：申請時所註冊的帳號。
- 密碼：申請時所註冊的密碼。
- 網域名稱/網域：申請時所註冊的名稱及網域。

步驟**4.** 點選【確定】新增動態 DNS，或【取消】取消新增。

圖 1-30 新增動態 DNS

變更動態 DNS

步驟**1.** 於左方功能選項，先點選【系統管理】，接著點選下方的【動態 DNS】，進入【動態 DNS】工作視窗。*（如圖 1-28）*

步驟**2.** 在【動態 DNS】的表格中，找到欲變更設定的項目，對應至右方【變更】欄，點選【修改】。

步驟**3.** 在【修改動態 DNS】視窗中，鍵入新的資訊。*（如圖 1-31）*

步驟**4.** 點選螢幕下方【確定】按鈕，變更設定，或 點選【取消】取消變更。

圖 1-31 變更動態 DNS

移除動態 DNS

步驟**1.** 在左方的功能選項中，點選【系統管理】功能，再點選【動態 DNS】次功能選項。*（如圖 1-28）*

步驟**2.** 在【動態 DNS】的表格中，找到欲刪除設定的動態 DNS，對應至右方【變更】欄，點選【刪除】。

步驟**3.** 在【確定刪除】動態 DNS 對話框中，點選【確定】按鈕，移除設定，或 點選【取消】取消移除。*（如圖 1-32）*

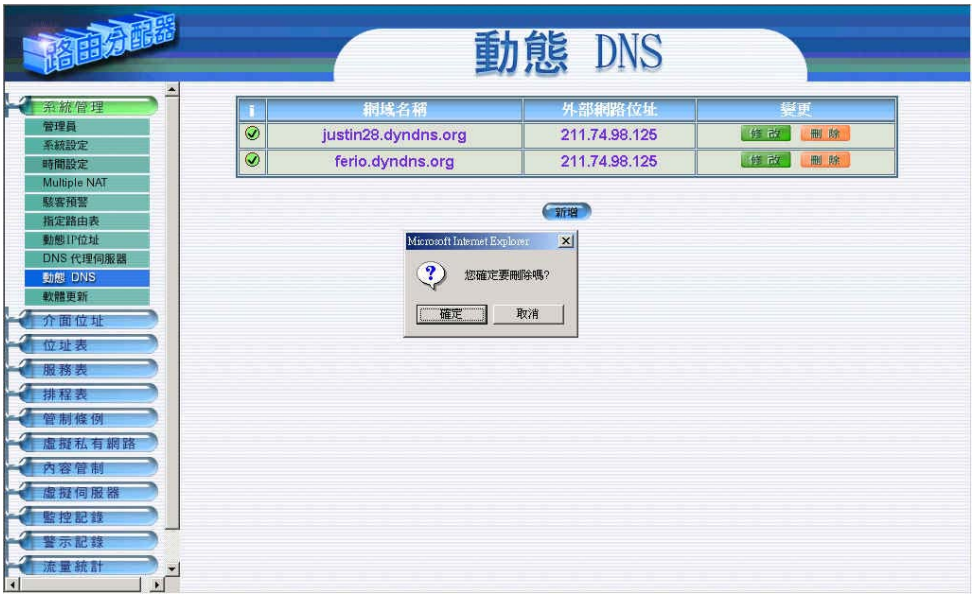

圖 1-32 移除動態 DNS

軟體更新

升級路由分配器軟體，請先至本公司網站免費下載最新版本軟體，再依下列步驟更新。更新後，無須重新設定路由分配器系統設定值。

步驟**1.** 由螢幕上【軟體版本】資訊中，獲知目前軟體使用版本號碼。再經由瀏覽器至本公司網站取得最新軟體版本訊息，並將更新程式下載儲存至伺服器的硬碟中。

步驟**2.** 先點選左方功能選項的【系統管理】，接著點選下方的【軟體更新】，進入【軟體更新】工作視窗。*（如圖 1-33）*

步驟**3.** 點選【瀏覽】，於【選擇檔案】視窗中，選擇最新的軟體版本檔案名稱。

步驟**4.** 點選螢幕右下方【確定】功能按鈕，執行軟體自動更新升級。

圖 1-33 路由分配器軟體更新

軟體更新需 3 分鐘的時間，更新後系統將會自動重新開機。

第二章

介 面 位 址

介面位址包括了路由分配器系統的內部網路,及外部網路等設定值。這些設定值在設定後會儲存在介面位址檔裡。

在本【介面位址】單元中：系統管理員於此單元中，依照所選擇的 ISP 網路連線方式，定義企業網路架構內的內部網路、外部網路、周圍網路的 IP 位址、子網路遮罩、閘道位址等介面位址。

內部網路介面位址設定

步驟**1.** 在左方的功能選項中，點選【介面位址】功能，再點選【內部網路】次功能選項。*（如圖 2-1）*

步驟**2.** 鍵入內部網路之各項介面位址設定：

- IP 位址： 鍵入內部網路之 IP 位址。
- 子網路遮罩： 鍵入內部網路之子網路遮罩。
- 開啓：是否開啓 Ping / WebUI 等功能

步驟**3.** 將所有介面位址設定好後，點選螢幕右下方【確定】按鈕。

圖 2-1 內部網路介面位址設定

如果路由分配器新的 Internal IP Address 不是 192.168.1.1，則系統主管理員必須更改 PC 端的 IP Address，並重新開機才能使新的 IP 位址生效。例如：路由分配器新的 Internal IP Address 是 172.16.0.1，則在 Browser 的網址欄位上輸入新的 Internal IP Address 172.16.0.1，與路由分配器重新連線。

外部網路介面設定

步驟**1.** 在左方的功能選項中，點選【介面位址】功能，再點選【外部網路】次功能選項。*（如圖 2-2）*

步驟**2.** 在負載模式下，點選下拉是選單可選擇

自動分配：路由分配器依照外部網路下載頻寬,
會自動依頻寬分配對外網路下載比例。
(適用不相同下載頻寬的使用者)

循環分配：路由分配器強制採用 1:1 循環分配網路下載連線。
(適用相同下載頻寬的使用者)

依照連線數：路由分配器依照使用者設定的 **飽和連線數** 來分配對外網路連線。

- 外部網路介面：爲外部網路介面 1 / 2
- 連線模式：顯示目前外部網路介面連線模式
  PPPoE 設定 (ADSL 撥接使用者)
  自動取得 IP 位址 (纜線數據機使用者)
  指定 IP 位址 (固接式或 ADSL 專線使用者)
- IP 位址：顯示目前外部網路介面連線的 IP 位址
- 飽和連線數：設定外部網路連線數量,使用連線達設定值時即循環進入下一個外部網路連線
- 開啓功能：顯示是否勾選 Ping / WebUI 等功能
- 變更：修改外部網路介面設定
- 優先權：設定外部網路介面的優先使用權

圖 2-2　外部網路介面位址設定

PPPoE 設定 (ADSL 撥接使用者)

步驟**1.** 在左方的功能選項中，點選【介面位址】功能，再點選【外部網路】次功能選項,再點選外部網路介面 2 中變更修改。*（如圖 2-2）*

步驟**2.** 點選【PPPoE 設定 (ADSL 撥接使用者)】次功能選項。*（如圖 2-3）*

- 測試連線 IP 位址或網址：本路由分配器系統會自動發出偵測封包給使用者設定的 IP 位址或網址，已確認連線狀態是否正常。如使用者設定的 IP 位址或網址未有回應，本路由分配器將會重新進行連線動作，確保連線狀態正常。
- 目前狀態：本路由分配器系統會自動偵測並顯現目前網路連線狀態（連線中或斷線）。
- IP 位址：顯示 ISP 配發的外部的 IP 位址。
- 使用者名稱：ISP 配發的帳號名稱。
- 密碼：ISP 配發帳號的密碼。
- 服務:：某些 ISP 會要求輸入，請自行參見您的 ISP 設定說明書。
- 由 ISP 提供的 IP 位址：勾選動態 IP；或是勾選固定 IP，並鍵入該固定 IP 位址。
- 下載頻寬：輸入連線下載最大頻寬
- 上傳頻寬：輸入連線上傳最大頻寬
- 自動連線：勾選此項，當有封包到外部網路時時，將會自動連線上網。
- 閒置？分鐘自動斷線：原出廠值設定爲 0 分鐘。您可自行設定爲網路閒置時，自動斷線的時間，若設定值定爲”0”，即表示永遠維持連線狀態。選擇計時制的用戶，最好設定自動斷線時間，以節省連線費用。
- Ping：勾選此項，允許遠端用戶 Ping 外部網路介面位址。
- WebUI：勾選此項，允許遠端用戶使用 HTTP 連線至路由分配器設定畫面。

步驟**3.** 將所有參數設定好後，點選螢幕右下方【確定】按鈕。

圖 2-3 PPPoE 設定(ADSL 撥接使用者)設定

自動取得 IP 位址(纜線數據機使用者)

步驟**1.** 在左方的功能選項中，點選【介面位址】功能，再點選【外部網路】次功能選項,再點選外部網路介面 2 中變更修改。*（如圖 2-2）*

步驟**2.** 點選外部網路下方【自動取得 IP 位址(纜線數據機使用者)】。*（如圖 2-4）*

- 測試連線 IP 位址或網址：本路由分配器系統會自動發出偵測封包給使用者設定的 IP 位址或網址，已確認連線狀態是否正常。如使用者設定的 IP 位址或網址未有回應，本路由分配器將會重新進行連線動作，確保連線狀態正常。
- IP 位址：顯示 ISP 配發的外部的 IP 位址。
- MAC 位址 (某些 ISP 要求輸入)：某些 ISP 需輸入 MAC 位址。
- 用戶名稱 (某些 ISP 要求輸入)：某些 ISP 要求輸入配發的帳號名稱。
- 網域名稱：某些 ISP 要求輸入的網域名稱
- 下載(上傳)頻寬：輸入連線下載(上傳)最大頻寬
- 更新:：要求重新取得外部 IP 位址。
- 釋放:：要求釋放已取得外部 IP 位址。
- Ping：勾選此項，允許遠端用戶 Ping 外部網路介面位址。
- WebUI：勾選此項，允許遠端用戶使用 HTTP 連線至路由分配器設定畫面。

步驟**3.** 將所有參數設定好後，點選螢幕右下方【確定】按鈕。

圖 2-4 自動取得 IP 位址(纜線數據機使用者)設定

指定 IP 位址(固接或 ADSL 專線使用者)

步驟**1.** 在左方的功能選項中，點選【介面位址】功能，再點選【外部網路】次功能選項,再點選外部網路介面 2 中變更修改。*（如圖 2-2）*

步驟**2.** 點選外部網路下方【指定 IP 位址 (固接式或 ADSL 專線使用者)】。*（如圖 2-5）*

- 測試連線 IP 位址或網址：本路由分配器系統會自動發出偵測封包給使用者設定的 IP 位址或網址，已確認連線狀態是否正常。如使用者設定的 IP 位址或網址未有回應，本路由分配器將會重新進行連線動作，確保連線狀態正常。
- IP 位址：鍵入 ISP 配發的固定 IP 位址。
- 子網路遮罩 鍵入 ISP 配發的子網路遮罩。
- 預設閘道：鍵入 ISP 配發的預設閘道位址。
- DNS 伺服器 1/2：鍵入 ISP 所配發的 DNS 1/2 伺服器位址。(*詳見附註)*
- 下載頻寬：輸入連線下載最大頻寬
- 上傳頻寬：輸入連線上傳最大頻寬
- Ping：勾選此項，允許遠端用戶 Ping 外部網路介面位址。
- WebUI：勾選此項，允許遠端用戶使用 HTTP 連線至路由分配器設定畫面。

步驟**3.** 將所有介面位址設定好後，點選螢幕右下方【確定】按鈕。

圖 2-5 指定 IP 位址(固接或 ADSL 專線使用者)設定

若自行架設 DNS 伺服器，需先至【虛擬伺服器】功能中，將原先 DNS 伺服器的真實 IP 位址對應至內部 DNS 伺服器的虛擬 IP 位址，而在此處 DNS 伺服器位址中，則必需鍵入內部伺服器的虛擬 IP 位址。

外部網路介面 2 設定方法

步驟**1.** 在左方的功能選項中，點選【介面位址】功能，再點選【外部網路】次功能選項,再點選外部網路介面 2 中變更修改。*（如圖 2-2）*

設定外部網路介面 2 時,需將外部網路 2 〔開啓〕 方可進行設定...其餘設定均同外部網路設定方法。（如圖 2-6）

圖 2-6 外部網路 2 設定方法

第三章

位 址 表

本路由分配器在此單元中提供系統主管理員，定義內部網路、內部網路群組、外部網路、外部網路群組、周圍網路、周圍網路群組的介面位址。

【位址表】紀錄的 IP 位址可能是一個主機 IP 位址，也可能是一個網域多個 IP 位址。系統管理員可以自行設定一個易辨識的名字代表此一 IP 位址。基本上 IP 位址根據不同的網路區可分爲三種：內部網路 IP 位址(Internal IP Address) ，外部網路 IP 位址(External IP Address)和非軍事區網路 IP 位址(DMZ IP Address)。當系統管理員欲將不同 IP 位址封包的過濾規則，加入相同管制條例時，可先將這些 IP 位址建立一個「內部網路群組」或是「外部網路群組」，以簡化設立管制條例工作程序。

如何運用位址表

有了易辨識的 IP 位址的名稱後，同時位址群組名稱也已顯示在位址表上，系統管理員在設定管制條例時，就可選用此位址表名稱，套用在管制條例的來源位址(Source Address)或目的位址(Destination Address)。所以位址表的設定應該在管制條例的設定之前，如此在設定管制條例時，才可在位址表中挑出正確的 IP 位址名稱。

位址表之【內部網路】功能

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【內部網路】次功能選項。*（如圖 3-1）*

圖 3-1 內部網路位址功能設定

步驟**2.** 內部網路工作視窗之表格名詞定義：

- 名稱：內部網路電腦名稱。
- IP：內部網路電腦 IP 位址。
- 子網路遮罩：子網路遮罩。
- MAC 位址：內部網路電腦 IP 位址對應的 MAC 位址。
- 變更：變更內部網路中各項設定值。點選【修改】，可修改內部網路各項參數資訊；點選【刪除】，可刪除該項設定。

在內部網路視窗中，若是某個位址表成員已被加入管制條例或網路群組之中。則在【變更】欄位中，將會出現【使用中】文字，無法進行修改或刪除的變更設定。

新增內部網路位址

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【內部網路】次功能選項。*（如圖 3-1）*

步驟**2.** 點選【新增】功能按鈕。

步驟**3.** 在新視窗中，鍵入新內部網路之網路名稱、IP 位址、子網路遮罩、MAC 位址等各項參數值。*（如圖 3-2）*

步驟**4.** 勾選【從路由分配器取得固定 IP 位址】，可使此 MAC 位址每次皆取得同一 IP 位址。

步驟**5.** 點選螢幕下方【確定】按鈕，新增指定的內部網路，或點選【取消】取消設定。

圖 3-2 新增內部網路位址

若欲使用【從路由分配器取得固定 IP 位址】功能，必須先鍵入 MAC 位址，此功能才可生效。

變更內部網路位址

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【內部網路】次功能選項。*（如圖 3-1）*

步驟**2.** 在【內部網路】的表格中，找到欲變更設定的網路名稱，對應至右方【變更】欄，點選【修改】。

步驟**3.** 在新的【變更位址】視窗中，鍵入各項欲變更的路徑位址。*（如圖 3-3）*

步驟**4.** 點選螢幕下方【確定】按鈕，變更設定，或點選【取消】取消變更。

圖 3-3 變更路由分配器各項偵測功能

移除內部網路位址

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【內部網路】次功能選項。*（如圖 3-1）*

步驟**2.** 在【內部網路】的表格中，找到欲變更設定的網路名稱，對應至右方【變更】欄，點選【刪除】。

步驟**3.** 在【確定刪除】內部網路位址對話框中，點選【確定】按鈕，移除設定，或 點選【取消】取消移除。*（如圖 3-4）*

圖 3-4 移除內部網路位址設定

內部網路群組功能設定

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【內部網路群組】次功能選項。*（如圖 3-5）*

圖 3-5 內部網路群組功能設定

步驟**2.** 內部網路群組工作視窗之表格名詞定義：

- 名稱：內部網路群組名稱。
- 成員：該群組成員。
- 變更：變更內部網路群組中各項設定值。點選【修改】，可修改內部網路群組各項參數資訊；點選【刪除】，可刪除該群組。

在【內部網路群組】工作視窗中，若是某個網路群組已被加入管制條例中，【變更】欄中會出現【使用中】文字，而無法進行修改或刪除設定。需先至管制條例刪除該項設定，才可進行變更設定。

新增內部網路群組

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【內部網路群組】次功能選項。*（如圖 3-5）*

步驟**2.** 在內部網路群組視窗中，點選【新增】內部網路群組功能按鈕。

步驟**3.** 在出現的新增群組視窗中*（如圖 3-6）*

可選取的位址：顯示內部網路所有組員名單。
被選取的位址：顯示登錄至新群組的組員名單。

- 名稱：鍵入新群組名稱。
- 新增組員：由【可選取的位址】選單中，點選欲登錄之組員名稱，再點選【加入＞＞】，將該成員加入新群組組員名單中。
- 移除組員：在【被選取的位址】選單中，點選欲移除之組員名稱，再點選【＜＜刪除】，將該組員由群組中移除。

步驟**4.** 點選【確定】執行新增群組；或點選【取消】取消新增。

圖 3-6 新增內部網路群組

變更內部網路群組設定

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【內部網路群組】次功能選項。*（如圖 3-5）*

步驟**2.** 在內部網路群組視窗中，找到欲變更設定的網路群組名稱，對應至右方【變更】欄，點選【修改】。

步驟**3.** 在出現的變更群組視窗中*（如圖 3-7）*

- 名稱：鍵入新群組名稱。
- 新增組員：由【可選取的位址】選單中，點選欲登錄之組員名稱，再點選【加入＞＞】，將該成員加入新群組組員名單中。
- 移除組員：在【被選取的位址】選單中，點選欲移除之組員名稱，再點選【＜＜刪除】，將該組員由群組中移除。

步驟**4.** 點選【確定】執行變更群組；或點選【取消】取消變更。

圖 3-7 變更網路群組設定

移除內部網路群組

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【內部網路群組】次功能選項。*（如圖 3-5）*

步驟**2.** 在【內部網路群組】的表格中，找到欲移除的內部網路群組，對應至右方【變更】欄，點選【刪除】。

步驟**3.** 在【確定移除】內部網路群組對話框中，點選【確定】按鈕，移除設定，或點選【取消】取消移除。*（如圖 3-8）*

圖 3-8 移除內部網路群組

外部網路功能設定

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【外部網路】次功能選項。*（如圖 3-9）*

圖 3-9 外部網路設定功能

步驟**2.** 外部網路工作視窗之表格名詞定義：

- 名稱：外部網路名稱。
- IP 位址/子網路遮罩：連結目的網域之 IP 位址與子網路遮罩。
- 變更：變更外部網路中各項設定值。點選【修改】，可修改外部網路各項參數；點選【刪除】，可刪除該項設定。

在外部網路視窗中，若是某個位址表成員已被加入管制條例或網路群組之中，【變更】欄中會出現【使用中】文字，無法進行修改或刪除的變更設定。

新增外部網路位址

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【外部網路】次功能選項。*（如圖 3-9）*

步驟**2.** 點選【新增】外部網路位址功能按鈕。

步驟**3.** 在新視窗中，鍵入新外部網路各項參數值。*（如圖 3-10）*

步驟**4.** 點選螢幕下方【確定】按鈕，新增指定外部網路，或點選【取消】取消設定。

圖 3-10 新增外部網路位址

變更外部網路位址

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【外部網路】次功能選項。*（如圖 3-9）*

步驟**2.** 在【外部網路】的表格中，找到欲變更設定的網路名稱，對應至右方【變更】欄，點選【修改】。

步驟**3.** 在新的【變更位址】視窗中，鍵入各項欲變更的路徑位址。*（如圖 3-11）*

步驟**4.** 點選螢幕下方【確定】按鈕，變更設定，或 點選【取消】取消變更。

圖 3-11 變更外部網路位址

移除外部網路位址

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【外部網路】次功能選項。*（如圖 3-1）*

步驟**2.** 在【外部網路】的表格中，找到欲變更設定的網路名稱，對應至右方【變更】欄，點選【刪除】。

步驟**3.** 在【確定移除】外部網路位址對話框中，點選【確定】按鈕，移除設定，或 點選【取消】取消移除。*（如圖 3-12）*

圖 3-12 移除外部網路位址

外部網路群組功能設定

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【外部網路群組】次功能選項。*（如圖 3-13）*

圖 3-13 外部網路群組功能設定

步驟**2.** 外部網路群組工作視窗之表格名詞定義：

- 名稱：外部網路群組名稱。
- 成員：該群組成員。
- 變更：變更外部網路群組中各項設定值。點選【修改】，可修改外部網路群組各項參數；點選【刪除】，可刪除該群組。

在【外部網路群組】工作視窗中，若是某個網路群組已被加入管制條例中，在【變更】欄會出現【使用中】文字，無法進行修改或刪除的變更設定，需先至管制條例移除該向設定，才可進行變更設定。

新增外部網路群組

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【外部網路群組】次功能選項。*（如圖 3-13）*

步驟**2.** 在外部網路群組視窗中，點選【新增】外部網路群組功能按鈕。

步驟**3.** 在出現的新增群組視窗中*（如圖 3-14）*

可選取的位址：顯示外部網路所有組員名單。
被選取的位址：顯示登錄至新群組的組員名單。

- 名稱：鍵入新群組名稱。
- 新增組員：由【可選取的位址】選單中，點選欲登錄之組員名稱，再點選【加入＞＞】，將該成員加入新群組組員名單中。
- 移除組員：在【被選取的位址】選單中，點選欲移除之組員名稱，再點選【＜＜刪除】，將該組員由群組中移除。

步驟**4.** 點選【確定】執行新增群組；或點選【取消】取消新增。

3-14 新增外部網路群組

變更外部網路群組設定

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【外部網路群組】次功能選項。*（如圖 3-13）*

步驟**2.** 在外部網路群組視窗中，找到欲變更設定的網路群組名稱，對應至右方【變更】欄，點選【修改】。

步驟**3.** 在出現的變更群組視窗中*（如圖 3-15）*

- 名稱：鍵入新群組名稱。
- 新增組員：由【可選取的位址】選單中，點選欲登錄之組員名稱，再點選【加入＞＞】，將該成員加入新群組組員名單中。
- 移除組員：在【被選取的位址】選單中，點選欲移除之組員名稱，再點選【＜＜刪除】，將該組員由群組中移除。

步驟**4.** 點選【確定】執行變更群組；或點選【取消】取消變更。

3-15 變更外部網路群組設定

移除外部網路群組

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【外部網路群組】次功能選項。*（如圖 3-13）*

步驟**2.** 在【外部網路群組】的表格中，找到欲移除的外部網路群組，對應至右方【變更】欄，點選【刪除】。

步驟**3.** 在【確定移除】外部網路群組對話框中，點選【確定】按鈕，移除設定，或點選【取消】取消移除。*（如圖 3-16）*

圖 3-16 移除外部網路群組

第四章

服 務 表

TCP 協定和 UDP 協定提供各種不同的服務，每一個服務都有一個 TCP 埠(TCP Port)號碼或 UDP 埠號碼代表，如 TELNET(23)，FTP(21)，SMTP(25)，POP3(110)，…等。本產品的服務包含兩個部分 ： 基本服務表和自訂服務表，比較常用的 TCP 服務或 UDP 服務已預告定義在基本服務表，此類服務不能修改也不可移除。另外使用者也可依自己的需求到自訂服務表設定適當 TCP 埠和 UDP 埠號碼。在自訂服務時，客戶端埠(Client Port)設定的區間一般爲 1024：65535，伺服器端埠(Server Port)號碼則是設定在 0:65535 之間。

本路由分配器在此單元中，將一些常用的網路服務列入各項表列的服務選單中（基本服務、自訂服務與服務群組）。系統主管理員只需依照下列操作說明，將網路協定與出入埠號碼定義在各種網路通訊應用中，用戶端即可與各種不同伺服器連線，傳輸資料。

如何運用服務表

系統管理員可以在【服務表】的【服務群組】選項中，新增服務群組名稱，將要提供的服務包含進去。有了服務群組的功能，管理員在制訂管制條例時可以簡化許多流程。例如，有 10 個不同 IP 位址可以對伺服器存取 5 個不同的服務，如 HTTP、FTP、SMTP、POP3 和 TELNET，如果不使用服務群組的功能，總共需制定 10x5=50 條管制條例，但使用服務群組名稱套用在服務選項上，則只需一條管制條例即可達到 50 條管制條例的功能。

服務表之【基本服務】功能

步驟**1.** 在左方的功能選項中，點選【服務表】功能，再點選【基本服務】次功能選項。*（如圖 4-1）*

圖 4-1 基本服務表

步驟**2.** 基本服務表視窗表格內圖示與名詞名稱定義：

圖示	說明
TCP	TCP 服務，如：FTP、FINGER、HTTP、 、HTTPS 、IMAP、SMTP、POP3、ANY、AOL、BGP、GOPHER、InterLocator、IRC、L2TP、LDAP、NetMeeting、NNTP、PPTPReal、 Media、RLOGIN、SSH、TCP ANY、TELNET、VDO Live、WAIS、WINFRAME、X-WINDOWS 等。
UDP	UDP 服務，如：IKE、DNS、NTP、IRC、RIP、SNMP、SYSLOG、TALK、TFTP、UDP-ANY、UUCP 等。
ICMP	ICMP 服務，如：PING、TRACEROUTE 等。

自訂服務功能設定

步驟**1.** 在左方的功能選項中，點選【服務表】功能，再點選【自定服務】次功能選項。*（如圖 4-2）*

圖 4-2 自訂服務功能設定

步驟**2.** 內部網路工作視窗之表格名詞定義：

- 服務名稱：自訂服務項目名稱。
- 通訊協定：【基本設定】中所使用的網路協定。如 TCP、UDP，或其他（請選擇代碼）。
- 用戶端：自定服務項目中之用戶端的出入埠範圍。

  在用戶端兩個空格內輸入的 port 號如爲不同埠號，則是開啓埠號爲兩個空格內輸入 port 號的中間範圍。

  在用戶端兩個空格內輸入的 port 號如爲相同埠號，則是開啓埠號爲同一個 port 號
- 伺服器端：自定服務項目中之伺服器端的出入埠範圍。

  在伺服器端兩個空格內輸入的 port 號如爲不同埠號，則是開啓埠號爲兩個空格內輸入 port 號的中間範圍。

在伺服器端兩個空格內輸入的 port 號如爲相同埠號，則是開啓埠號爲同一個 port 號

- 變更：變更服務表中各項設定值。點選【修改】，可修改服務表各項參數；點選【刪除】，可刪除該項設定。

在自訂服務工作視窗中，若是某個服務已被加入管制條例或服務群組之中。【變更】欄會出現【使用中】，而無法進行修改或刪除的變更設定，需先至管制條例或服務群組中，移除該項設定，才可執行變更。

新增自訂服務

步驟**1.** 在左方的功能選項中，點選【服務表】功能，再點選【自訂服務】次功能選項。*（如圖 4--2）*

步驟**2.** 在【自訂服務】表格中，點選【新增服務】功能按鈕。

步驟**3.** 在出現的新增服務視窗中 *（如圖 4-3）*

- 服務名稱：輸入新服務名稱。
- 通訊協定：勾選【基本設定】中所使用的網路協定。如 TCP、UDP，或其他（請選擇代碼）。
- 用戶端： 輸入新服務之用戶端的出入埠範圍。
  在用戶端兩個空格內輸入的 port 號如爲不同埠號，則是開啓埠號爲兩個空格內輸入 port 號的中間範圍。
  在用戶端兩個空格內輸入的 port 號如爲相同埠號，則是開啓埠號爲同一個 port 號
- 伺服器端：輸入新服務之伺服器端的出入埠範圍。
  在伺服器端兩個空格內輸入的 port 號如爲不同埠號，則是開啓埠號爲兩個空格內輸入 port 號的中間範圍。
  在伺服器端兩個空格內輸入的 port 號如爲相同埠號，則是開啓埠號爲同一個 port 號

步驟**4.** 點選【確定】執行新增服務；或點選【取消】取消新增。

圖 4-3 新增自訂服務

變更自訂服務

步驟**1.** 在左方的功能選項中，點選【服務表】功能，再點選【自訂服務】次功能選項。*（如圖 4-2）*

步驟**2.** 在【自訂服務】視窗中，找到欲變更設定的服務名稱，對應至右方【變更】欄，點選【修改】。

步驟**3.** 在出現的變更群組視窗中 *（如圖 4-4）*

- 服務名稱：輸入新服務名稱。
- 通訊協定：勾選【基本設定】中所使用的網路協定。如 TCP、UDP，或其他（請選擇代碼）。
- 用戶端： 輸入新服務之用戶端的出入埠範圍。
  在用戶端兩個空格內輸入的 port 號如爲不同埠號，則是開啓埠號爲兩個空格內輸入 port 號的中間範圍。
  在用戶端兩個空格內輸入的 port 號如爲相同埠號，則是開啓埠號爲同一個 port 號
- 伺服器端：輸入新服務之伺服器端的出入埠範圍。
  在伺服器端兩個空格內輸入的 port 號如爲不同埠號，則是開啓埠號爲兩個空格內輸入 port 號的中間範圍。
  在伺服器端兩個空格內輸入的 port 號如爲相同埠號，則是開啓埠號爲同一個 port 號

步驟**4.** 點選【確定】執行變更服務；或點選【取消】取消變更。

圖 4-4 變更自訂服務

移除自訂服務

步驟**1.** 在左方的功能選項中，點選【服務表】功能，再點選【自訂】次功能選項。*（如圖 4-2）*

步驟**2.** 在【自訂服務】視窗表格中，找到欲變更設定的服務名稱，對應至右方【變更】欄，點選【刪除】。

步驟**3.** 在【刪除服務】確定對話框中，點選【確定】按鈕，移除設定，或 點選【取消】取消移除。*（如圖 4-5）*

圖 4-5 移除自訂服務

服務群組功能設定

步驟**1.** 在左方的功能選項中，點選【服務表】功能，再點選【服務群組】次功能選項。*（如圖 4-6）*

圖 4-6 服務群組功能設定

步驟**2.** 服務群組工作視窗之表格名詞定義：

- 群組名稱：所有已設定之服務群組名稱。
- 服務名稱：該服務群組服務項目。
- 變更：變更服務群組中各項設定值。點選【修改】，可修改服務群組各項參數；點選【刪除】，可刪除該群組。

在【服務群組】工作視窗中，若是某個服務群組已被加入管制條例中，則在【變更】欄會出現【使用中】，而無法進行修改或移除的變更設定，需先至管制條例中，移除該項設定，才可執行變更。

新增服務群組

步驟**1.** 在左方的功能選項中，點選【服務表】功能，再點選【服務群組】次功能選項。*（如圖 4-6）*

步驟**2.** 在服務群組視窗中，點選【新增服務群組】功能按鈕。

步驟**3.** 在出現的服務群組視窗中 *（如圖 4-7）*

可選取的服務：顯示所有有效的服務項目。
被選取的服務：顯示針對新增服務群組所選擇的服務項目。

- 名稱：鍵入新服務群組名稱。
- 新增服務項目：在【可選取的服務】選單中，點選欲增加的服務項目名稱，再點選【加入＞＞】，將該服務項目加入新群組。
- 移除服務項目：在【被選取的服務】欄位中，點選欲移除之服務項目名稱，再點選【＜＜刪除】，將該服務項目自群組中移除。

步驟**4.** 點選【確定】執行新增群組；或點選【取消】取消新增。

圖 4-7 新增服務群組

變更服務群組

步驟**1.** 在左方的功能選項中，點選【服務表】功能，再點選【服務群組】次功能選項。*（如圖 4-6）*

步驟**2.** 在內部網路群組視窗中，找到欲變更設定的網路群組名稱，對應至右方【變更】欄，點選【修改】。

步驟**3.** 在出現的變更群組視窗中 *（如圖 4-8）*

- 名稱：鍵入新群組名稱。
- 新增組員：由【可選取的服務】選單中，點選欲登錄之組員名稱，再點選【加入＞＞】，將該成員加入新群組組員名單中。
- 移除組員：在【被選取的服務】選單中，點選欲移除之組員名稱，再點選【＜＜刪除】，將該組員由群組中移除。

步驟**4.** 點選【確定】執行變更群組；或點選【取消】取消變更。

圖 4-8 變更服務群組

刪除服務群組

步驟**1.** 在左方的功能選項中，點選【服務表】功能，再點選【服務群組】次功能選項。*（如圖 4-6）*

步驟**2.** 在【服務群組】的表格中，找到欲移除的服務群組，對應至右方【變更】欄，點選【刪除】。

步驟**3.** 在【確定刪除】服務群組確認對話框中，點選【確定】按鈕，移除設定，或 點選【取消】取消移除。*（如圖 4-9）*

圖 4-9 移除服務群組

第五章

排 程 表

本路由分配器在此單元中提供系統主管理員，在排程表中定義網路系統連結與執行的時間區段，以便在【管制條例】或【網站管制】功能中，選擇特定時間內開放資料封包的出入或限制網站瀏覽。利用排程表的自動執行功能，系統管理員可以節省許多時間，同時讓網路系統發揮最大的效能。

如何運用排程表

系統管理員可利用排程表功能，設定系統在多個不同的時間區段內，自動執行設定封包流向的【管制條例】或限制網站瀏覽的【網站管制】功能。

排程表功能設定

步驟**1.** 在左方的功能選項中，點選【排程表】功能。*（如圖 5-1）*

圖 5-1 排程表功能設定

步驟**2.** 排程表工作視窗之表格名詞定義：

- 排程名稱：管理者所定義之排程表名稱。
- 變更：變更排程表中各項設定值。點選【修改】，可修改排程表各項參數；點選【刪除】，可刪除該項設定。

在排程表工作視窗中，若是某個排程已被加入【管制條例】或【網站管制】之中。【變更】欄會出現【使用中】，而無法進行修改或刪除的變更設定，需先至【管制條例】或【網站管制】中，移除該項設定，才可執行變更。 。

新增排程表

步驟**1.** 在左方的功能選項中，點選【排程表】功能。*（如圖 5-1）*

步驟**2.** 點選【新增】功能按鈕。

步驟**3.** 在出現的【新增排程表】視窗中 *（如圖 5-2）*

- 排程名稱：輸入新排程名稱。
- 時段：在每週特定日期的表格內，於【起始時間】與【結束時間】的下拉選單中，點選有效執行的時間範圍。

步驟**4.** 點選【確定】執行新增排程表；或點選【取消】取消新增。

圖 5-2 新增排程表

制定排程表時，【起始時間】欄位，必須小於【結束時間】欄位，否則無法進行新增或修改的設定。

變更排程表

步驟**1.** 在左方的功能選項中，點選【排程表】功能。*（如圖 5-1）*

步驟**2.** 在【排程表】視窗中，找到欲變更設定的排程表名稱，對應至右方【變更】欄，點選【修改】。

步驟**3.** 在出現的變更群組視窗中，鍵入新排程表名稱，並設定排程表時間範圍 *（如圖 5-3）*

步驟**4.** 點選【確定】執行變更；或點選【取消】取消變更。

圖 5-3 變更排程表

移除排程表

步驟**1.** 在左方的功能選項中，點選【排程表】功能。*（如圖 5-1）*

步驟**2.** 在【排程表】視窗表格中，找到欲變更設定的排程表名稱，對應至右方【變更】欄，點選【刪除】。

步驟**3.** 在【刪除排程表】確定對話框中，點選【確定】按鈕，移除設定，或點選【取消】取消移除。*（如圖 5-4）*

圖 5-4 移除排程表

第六章

管 制 條 例

路由分配器經由管制條例的參數設定，可以控管資料封包的過濾規則。管制條例的參數包含有來源位址、目的位址、服務、管制動作、流量監控、流量統計、及自動排程流量警示等。系統管理員可以由這些參數，管理、設定不同出入埠間的資料傳送以及服務項目，哪些網路物件、網路服務或應用程式的封包該予以攔截或放行。

本路由分配器依據不同來源位址的資料封包，將管制條例設定功能區分爲下列六項，以便利系統主管理員，針對不同資料封包的來源 IP、來源埠、目的 IP、目的埠制訂管制規則。

（一）【內部至外部】：來源網路區是在內部網路區，目的網路區是在外部網路區。系統管理員在此功能中，訂定內部網路至外部網路間所有封包的管制、服務項目的管制規則。

（二）【外部至內部】：來源網路區是在外部網路區，目的網路區是在內部網路區。系統管理員在此功能中，訂定外部網路至內部網路間所有封包的管制、服務項目的管制規則。

如何運用管制條例

管制條例所需設定的參數包含有：來源網路、目的網路、服務項目、管制動作、紀錄、統計、流程和流量警示值。其中，來源網路和目的網路和 IP 位址對映的名稱必需先在【位址表】定義。而服務項目，若屬於【基本服務】項目中，則可直接使用，如果是屬於自訂服務，則必須先在【服務表】中的【自訂服務】定義其服務項目名稱和其對映的埠號(Port Number)。

在制定【至內部網路】條例時，它的目的位址爲 1 對 1 對映的 IP 位址或是虛擬伺服器 IP 位址，此部分需在【虛擬伺服器】項目中定義，而非在【位址表】制定。

管制條例操作指引

步驟**1.** 至【位址表】中，定義來源網路與目的網路的名稱、位址。

步驟**2.** 至【服務表】中，定義服務項目。

步驟**3.** 至【虛擬伺服器】中，定義對映 IP 或虛擬伺服器名稱位址。（此步驟僅於定義【至內部網路】需操作。）

步驟**4.** 於本單元【管制條例】設定各項參數。

內部至外部管制條例功能設定

步驟**1.** 在左方的功能選項中，點選【管制條例】功能，再點選【內部至外部】次功能選項。*（如圖 6-1）*

圖 6-1 內部網路至外部網路功能設定

步驟**2.** 管制條例表格說明（由內部網路至外部網路）：

- 編號：所設定之管制條例編號，此處編號由 1 開始。
- 來源網路：已於【位址表】之【內部網路】功能中所指定的內部網路位址，或所有內部網路位址。
- 目的網路：已於【位址表】之【外部網路】功能中所指定的外部網路位址，或所有外部網路位址。
- 服務名稱：指定外部網路伺服器提供的服務項目。
- 管制動作：指定內、外部網路進出路由分配器資料封包的准許與拒絕動作。
- 監控功能：指定內、外部網路進出路由分配器資料封包的各種監控功能。第一欄爲流量監控功能，第二欄爲流量統計功能，第三欄爲排程表功能，第四欄爲流量警示功能，第五欄爲頻寬管理功能。當

該欄出現圖示即表示該項監控功能已啓動，反之，若未有任何圖示，則監控功能未開啓。（圖示說明如下方表格。）

- 變更：變更內部網路中各項設定值。點選【修改】，可修改內部網路各項參數資訊；點選【刪除】，可刪除該項設定。
- 移動：該項管制條例之編號排列次序。由下拉選單中點選編號，可移動該項管制條例次序。

管制條例圖示說明：

圖 示	名 稱	說　　明
	准許	准許指定的所有內部到外部網路資料封包進出。
	監控	准許指定的內部到外部網路 1 資料封包進出。
	監控	准許指定的內部到外部網路 2 資料封包進出。
	拒絕	拒絕指定的所有內部到外部網路資料封包進出。
	監控	流量、事件監控功能已開啓。
	統計	流量統計功能已開啓。
	排程	已啓動排程表所制訂時間範圍內自動執行功能。
	警示	流量、事件警示功能已開啓。

備註：

1. 檢視系統之流量、事件監控紀錄 ，點選螢幕左方【監控功能】選項，系統使用與操作方式，請翻閱第八章。
2. 檢視系統之警示記錄 ，點選螢幕左方【警示記錄】選項，系統使用與操作方式，請翻閱第九章。
3. 檢視系統之流量統計紀錄 ，點選螢幕左方【流量統計】選項，使用與操作方式，請翻閱第十章。
4. 路由分配器自動執行時間範圍之排程 ，修改排程時間，點選螢幕左方【排程表】選項，使用與操作方式，請翻閱第五章。

新增內部至外部管制條例

步驟**1.** 在左方的功能選項中，點選【管制條例】功能，再點選【內部至外部】次功能選項。*（如圖 6-1）*

步驟**2.** 在【內部至外部】視窗中，點選【新增管制條例】功能按鈕。

步驟**3.** 在出現的【新增管制條例】視窗中，鍵入下列相關參數*（如圖 6-2）*

圖 6-2 新增內部網路至外部網路管制條例

- 來源網路位址：由下拉選單中點選內部網路名稱。
  此部分下拉選單所顯示的內部網路名稱爲：【位址表】之【內部網路】所設定的內部網路位址。若要新增選項需至【位址表】之【內部網路】功能視窗中設定，此處無法新增。
- 目的網路位址：由下拉選單中點選外部網路名稱。
  此部分下拉選單所顯示的外部網路名稱爲：【位址表】之【外部網路】所設定的內部網路位址。若要新增選項需至【位址表】之【外部網路】功能視窗中設定，此處無法新增。
- 服務名稱：由下拉選單中點選服務功能。此部分下拉選單所顯示的

服務功能項目爲：(一)【服務表】中的【基本服務】功能，如：ANY、AOL、AUTH.....等多項服務可供選擇；(二) 系統管理員已於【服務表】之【自訂服務】或【服務群組】所定義之服務功能項目。

- 管制動作：由下拉選單中點選指定的內、外部網路資料封包進出的准許或拒絕。可選擇【允許】；或【拒絕】。
- 流量監控：勾選【啓動】，開啓流量監控記錄功能。
- 流量統計：勾選【啓動】，開啓流量統計功能。
- 自動排程：在下拉選單中，點選已於【排程表】設定之排程表名稱，可開啓此項管制條例在特定時間範圍自動有效執行的功能。
- 最高流量警示值：設定進出資料封包之最高流量（KBytes/Sec）警示值。此警示記錄將記錄於【警示記錄】之【流量警示】中。

步驟**4.** 點選螢幕下方【確定】按鈕，新增指定的內部網路，或點選【取消】取消設定。

若要變更本單元【內部至外部】表格內管制條例次序，可於表格右方【移動】欄，下拉選單中點選編號，即可移動該項管制條例。

變更內部至外部管制條例

步驟**1.** 在左方的功能選項中，點選【管制條例】功能，再點選【內部至外部】次功能選項。*（如圖 6-1）*

步驟**2.** 在【內部至外部】視窗中，找到欲變更設定的網路區域名稱，對映至右方【變更】欄，點選【修改】。

步驟**3.** 在出現的【變更管制條例】視窗中，鍵入下列相關參數*（如圖 6-3）*

圖 6-3 變更內部網路至外部網路管制條例

- 來源網路位址：由下拉選單中點選內部網路名稱。
  此部分下拉選單所顯示的內部網路名稱爲：【位址表】之【內部網路】所設定的內部網路位址。
- 目的網路位址：由下拉選單中點選外部網路名稱。
  此部分下拉選單所顯示的外部網路名稱爲：【位址表】之【外部網路】所設定的外部網路位址。

- 服務名稱：由下拉選單中點選新服務項目。
- 管制動作：由下拉選單中點選指定的內、外部網路資料封包進出的

准許或拒絕。

- 流量監控：勾選【啓動】，開啓流量監控功能。
- 流量統計：勾選【啓動】，開啓流量統計功能。
- 自動排程：在下拉選單中，點選已於【排程表】設定之排程表名稱，可開啓此項管制條例在特定時間範圍自動有效執行的功能。
- 警示功能：設定進出資料封包之最高流量（KBytes/Sec）警示值。

步驟**4.** 點選螢幕下方【確定】按鈕，變更指定的至外部網路管制條例，或點選【取消】取消變更。

若要變更或新增下拉選單的選項，需至各選項的原始設定單元重新設定。

- *來源網路→【位址表】之【內部網路】;*
- *目的網路→【位址表】之【外部網路】;*
- *服務表內的服務名稱→【服務表】之【基本服務】、【自訂服務】或【服務群組】。*

移除內部至外部管制條例

步驟**1.** 在左方的功能選項中，點選【管制條例】功能，再點選【內部至外部】次功能選項。*（如圖 6-1）*

步驟**2.** 在【內部至外部】視窗中，找到欲變更設定的網路區域名稱，對映至右方【設定】欄，點選【刪除】。

步驟**3.** 在【移除管制條例】確定對話框中，點選【確定】按鈕移除設定，或點選【取消】取消移除。*（如圖 6-4）*

圖 6-4 移除內部網路至外部網路管制條例

外部至內部管制條例功能設定

在設定外部至內部管制條例時，必須在【虛擬伺服器】中，先設定好各項參數。虛擬伺服器設定請參考第八章。

步驟**1.** 在左方的功能選項中，點選【管制條例】功能，再點選【外部至內部】次功能選項。*（如圖 6-5）*

圖 6-5 外部網路至內部網路管制條例功能設定

步驟**2.** 管制條例表格說明（由外部網路至內部網路）：

- 編號：所設定之管制條例編號，此處編號由 1 開始。
- 來源網路位址：已於【位址表】之【外部網路】功能中所指定的外部網路位址，或所有外部網路位址。
- 目的網路位址：已於【虛擬伺服器】之【IP 對映】或【虛擬伺服器 1/2/3/4】功能中所指定的 IP 對映網路位址，或虛擬伺服器網路位址。
- 服務名稱：虛擬伺服器（或 IP 對映）提供的服務項目。
- 管制動作：指定外部網路 1/2、虛擬伺服器（或 IP 對映）進出路由分配器資料封包的准許與拒絕動作。
- 監控功能：指定外部網路 1/2、虛擬伺服器（或 IP 對映）進出路由

分配器資料封包的各種監控功能。第一欄爲流量監控功能，第二欄爲流量統計功能，第三欄爲排程表功能，第四欄爲流量警示功能，第五欄爲頻寬管理功能。當該欄出現圖示即表示該項監控功能已啓動，反之，若未有任何圖示，則監控功能未開啓。（圖示說明如下方表格。）

- 變更：變更至內部網路中各項管制條例設定值。點選【修改】，可修改各項相關參數值；點選【刪除】，可刪除該項設定。
- 移動：該項管制條例之編號排列次序。由下拉選單中點選編號，可移動該項管制條例次序。

管制條例圖示說明：

圖 示	名 稱	說　　明
	准許	准許指定的所有外部到內部網路資料封包進出。
	監控	准許指定的外部網路 1 到內部資料封包進出。
	監控	准許指定的外部網路 2 到內部資料封包進出。
	拒絕	拒絕指定的所有外部到內部網路資料封包進出。
	監控	流量、事件監控功能已開啓。
	統計	流量統計功能已開啓。
	排程	已啓動排程表所制訂時間範圍內自動執行功能。
	警示	流量、事件警示功能已開啓。

備註：

1. 檢視系統之流量、事件監控紀錄 ，點選螢幕左方【監控功能】選項，系統使用與操作方式，請翻閱第八章。
2. 檢視系統之警示記錄 ，點選螢幕左方【警示記錄】選項，系統使用與操作方式，請翻閱第九章。
3. 檢視系統之流量統計紀錄 ，點選螢幕左方【流量統計】選項，使用與操作方式，請翻閱第十章。
4. 路由分配器自動執行時間範圍之排程 ，修改排程時間，點選螢幕左方【排程表】選項，使用與操作方式，請翻閱第五章。

新增外部至內部管制條例

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【外部至內部】次功能選項。*（如圖 6-5）*

步驟**2.** 在【外部至內部】視窗中，點選【新增管制條例】功能按鈕。

步驟**3.** 在出現的【新增管制條例】視窗中，鍵入下列相關參數*（如圖 6-6）*

圖 6-6 新增外部網路至內部網路管制條例

- 來源網路位址：由下拉選單中點選外部網路名稱。
  此部分下拉選單所顯示的外部網路名稱爲：已在【位址表】之【外部網路】所設定的外部網路位址。若要新增需至【位址表】之【外部網路】功能視窗中設定，此處無法新增。
- 目的網路位址：由下拉選單中點選內部網路名稱。
  此部分下拉選單所顯示的內部網路名稱爲：已在【虛擬伺服器】之【IP 對映】或【虛擬伺服器 1/2/3/4】，所設定的 IP 對映網路位址，或虛擬伺服器網路位址。若要新增選單內的選項需至【虛擬伺服器】功能視窗中設定（新增方法請詳見第七章虛擬伺服器），此處無法新

增。

- 服務名稱：由下拉選單中點選服務項目。
  此部分下拉選單所顯示的服務項目爲：系統管理員已在【虛擬伺服器】之【IP 對映】或【虛擬伺服器 1/2/3/4】，所定義之該 IP 對映，或該虛擬伺服器的服務項目。若要新增或修改選單內的服務項目選項，需至【虛擬伺服器】工作視窗中設定（新增方法請詳見第七章虛擬伺服器），此處無法修改。
- 管制動作：由下拉選單中點選指定的外部網路 1/2、虛擬伺服器（或 IP 對映）資料封包進出的准許或拒絕。可選擇【准許】；或【拒絕】。
- 流量監控：勾選【啓動】，開啓流量監控功能。
- 流量統計：勾選【啓動】，開啓流量統計功能。
- 自動排程：在下拉選單中，點選已於【排程表】設定之排程表名稱，可開啓此項管制條例在特定時間範圍自動有效執行的功能。
- 流量警示：設定進出資料封包之最高流量（KBytes/Sec）警示值。

步驟**4.** 點選【確定】執行新增群組；或點選【取消】取消新增。

若要變更本單元【外部至內部】表格內管制條例次序，可於表格右方【次序】欄，下拉選單中點選編號，即可移動該項管制條例。

變更外部至內部管制條例

步驟**1.** 在左方的功能選項中，點選【管制條例】功能，再點選【外部至內部】次功能選項。*（如圖 6-5）*

步驟**2.** 在【外部至內部】視窗中，找到欲變更設定的網路區域名稱，對映至右方【設定】欄，點選【變更】。

步驟**3.** 在出現的【變更管制條例】視窗中，鍵入各項欲變更之參數值*（如圖 6-7）*

圖 6-7 變更外部網路至內部網路管制條例

- 來源網路：由下拉選單中點選已在【位址表】之【外部網路】所設定的外部網路位址名稱。
- 目的網路：由下拉選單中點選已在【虛擬伺服器】之【IP 對映】或【虛擬伺服器 1/2/3/4】，所設定的 IP 對映網路位址，或虛擬伺服器網路位址名稱。
- 服務名稱：由下拉選單中點選已在【虛擬伺服器】之【IP 對映】或【虛擬伺服器 1/2/3/4】，所定義之該 IP 對映，或該虛擬伺服器的服務項目。

- 管制動作：由下拉選單中點選指定的外部網路、虛擬伺服器（或 IP 對映）資料封包進出的准許或拒絕。
- 流量監控：勾選【啓動】，開啓流量監控功能。
- 流量統計：勾選【啓動】，開啓流量統計功能。
- 自動排程：在下拉選單中，點選已於【排程表】設定之排程表名稱，可開啓此項管制條例在特定時間範圍自動有效執行的功能。
- 流量警示：設定進出資料封包之最高流量（KBytes/Sec）警示值。

步驟**4.** 點選【確定】執行變更管制條例；或點選【取消】取消變更。

若要變更或新增下拉選單的選項，需至各選項的原始設定單元重新設定。

- *來源網路→【位址表】之【外部網路】;*
- *目的網路→【位址表】之【內部網路】;*
- *服務項目→【虛擬伺服器】之【IP 對映】或【虛擬伺服器 1/2/3/4】提供的服務項目。*

移除外部至內部管制條例

步驟**1.** 在左方的功能選項中，點選【管制條例】功能，再點選【外部至內部】次功能選項。*（如圖 6-5）*

步驟**2.** 在【外部至內部】視窗中，找到欲變更設定的網路區域名稱，對映至右方【設定】欄，點選【移除】。

步驟**3.** 在【移除管制條例】確定對話框中，點選【確定】按鈕，移除設定，或點選【取消】取消移除。*（如圖 6-8）*

圖 6-8 移除外部網路至內部網路管制條例

第七章

虛 擬 私 有 網 路

本路由分配器採 VPN 方式建立安全與私密的網路通訊服務，結合遠端用戶認證辨識系統，以整合企業的各個遠地網路與全球外勤人員遠地個人電腦，提供公司企業與遠端使用者一個安全便利的網路加密方式， 讓企業在網際網路上傳遞資料時，得到最佳的效能及保密效果，更節省管理者管理太多鑰匙的麻煩。

本路由分配器 VPN 驗證功能爲【自動加密驗證】。

【自動加密驗證】: 系統管理員可於此單元以自動加密功能建立連線兩端以固定標準方式交換網路加密鑰匙碼，並設定 IPSec Lifetime（加密鑰匙更新週期），亦可以 Perfect Forward Secrecy（進階加密）功能，啓動路由分配器系統自動隨機選取更新無法被判讀入侵的加密鑰匙碼。

【PPTP 伺服器】: 系統管理員可於此單元建立 VPN-PPTP 伺服器的相關功能設定。

【PPTP 用戶端】: 系統管理員可於此單元建立 VPN-PPTP 用戶端的相關功能設定。

如何運用網路驗證

建立虛擬私有網路驗證 Virtual Private Network (VPN)，無須至【管制條例】設定，只需依照下列步驟，設定 VPN 名稱、來源端網路位址、目的端網路位址與認證與加密模式，即可爲連線兩端建立安全保密的網路通訊。

自動加密驗證功能設定

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【自動加密驗證】次功能選項。*（如圖 7-1）*

圖 7-1 自動加密驗證功能設定

步驟**2.** 【自動加密驗證】視窗表格內圖示與名詞名稱定義：

- 名稱：定義虛擬私有網路（VPN）驗證通道名稱。此名稱必須是唯一且不可重複。
- 閘道 IP 位址：目的端網路介面位址。
- 目的端子網路：目的端子網路位址。
- PSK/RSA：加密模式（PSK 或 RSA），此加密鑰匙需至少 128 位元以上。
- 狀態：連接或斷線。
- 設定：變更服務表中各項設定值。點選【變更】，可修改自動加密之　各項參數；點選【刪除】，可刪除該項設定；點選【連線】，啓動與目的端連線；點選【斷線】，關閉與目的端加密連線功能。

新增自動加密驗證

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【自動加密驗證】次功能選項。*（如圖 7-2）*

步驟**2.** 在【自動加密驗證】視窗中，點選下方【新增】按鈕。

步驟**3.** 在【虛擬私有網路自動金鑰管理通道】視窗中，鍵入下列參數 *（如圖 7-2）*

圖 7-2 新增自動加密

- 名稱：定義 VPN 驗證通道名稱。此名稱必須是唯一且不可重複。
- 從來源位址：
  1. 勾選來源網路位址：（內部網路或非軍事區網路）。
  2. 使用介面：選擇 WAN 1 / 2 / 3 / 4(外部網路介面位址 1 / 2 / 3 / 4)。
  3. 鍵入來源網路之子網路位址與遮罩位址。
- 到目的位址：勾選目的端（遠端）網路連線方式並鍵入其 IP 位址。

1. 遠端閘道—固定 IP：使用固定 IP 者，請勾選此項，並鍵入目的端網路閘道位址與其子網路位址與遮罩。
2. 遠端閘道—動態 IP：使用動態 IP 者，請勾選此項，並鍵入目的端子網路位址與遮罩位址。
3. 遠端用戶端程式—固定 IP 或動態 IP：與遠端用戶電腦直接作加密連線請勾選此項。

- 認證方法：在下拉選單中選擇認證方法（Preshare）。目前提供選擇 Preshare 認證方法，並需於下方【加密金鑰】空欄中，鍵入加密金鑰密碼（此加密鑰匙需至少 128byte 長度以上）。
- 加密或認證：勾選加密或認證方式（ESP 加密或認證）。一般預設爲 ESP 加密方式。
- 進階加密：Perfect Forward Secrecy，勾選此項功能，在路由分配器系統自動產生加密鑰匙碼時，將會自動選擇一組完全獨立、無法以邏輯規律性判別獲得的隨機選取加密鑰匙碼，可增加路由分配器安全加密功能。
- 加密金鑰更新週期：鍵入加密鑰匙的使用有效時間（單位：秒），原系統設定值爲 28800 秒（8 小時）。在有效期過後，需重新制訂一組新加密鑰匙碼。
- 自動排程：選擇是否加入排程表的時間管理。

步驟**3.** 點選【確定】執行新增加密驗證；或點選【取消】取消新增。

變更自動加密驗證

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【自動加密驗證】次功能選項。*（如圖 7-1）*

步驟**2.** 在【自動加密驗證】視窗中，找到欲變更設定的虛擬私有網路（VPN）名稱，對應至右方【設定】欄，點選【變更】。

步驟**3.** 在【虛擬私有網路自動金鑰管理通道】視窗中，鍵入欲變更的各項參數值。

步驟**4.** 點選【確定】執行變更；或點選【取消】取消變更。*（如圖 7-3）*

圖 7-3 變更自動加密驗證設定

連接/斷線/移除自動加密驗證

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【自動加密驗證】次功能選項。*（如圖 7-1）*

步驟**2.** 連接/斷線：在【自動加密驗證】視窗表格中，找到欲設定連接/斷線的名稱，對應至右方【設定】欄，點選【連接】或【斷線】。更改設定後，可由左方【狀態】欄檢視設定是否已變更完成。

步驟**3.** 移除：在【自動加密驗證】視窗表格中，找到欲移除設定的虛擬私有網路驗證（VPN）名稱，對應至右方【設定】欄，點選【移除】。

步驟**4.** 在【移除自動加密驗證】確定對話框中，點選【確定】按鈕，移除設定，或 點選【取消】取消移除。*（如圖 7-4）*

圖 7-4 移除自動加密驗證

PPTP 伺服器設定

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【PPTP 伺服器】次功能選項。*（如圖 7-5）*

圖 7-5 PPTP 伺服器設定

- PPTP 伺服器：可設定開啓或關閉
- 用戶端 IP 範圍 **192.26.145.1-254**：可設定 PPTP 用戶端連入分配的網路位址範圍。
- 使用者名稱：PPTP 用戶端連入時所使用的名稱。
- 用戶端 IP 位址：PPTP 用戶端連入 PPTP 伺服器時，所使用的用戶端網路位址。
- 連線歷時：顯示目前 PPTP 用戶端與 PPTP 伺服器連線時間。
- 連線狀況：顯示目前 PPTP 用戶端與 PPTP 伺服器連線狀況。
- 設定：變更服務表中各項設定值。點選【變更】，可修改 PPTP 伺服器之各項參數；點選【刪除】，可刪除該項設定。

修改 PPTP 伺服器設定

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【PPTP 伺服器】次功能選項。*（如圖 7-5）。*

步驟**2.** 在【用戶端 IP 範圍】視窗中，點選右方【修改】按鈕。

步驟**3.** 在【修改伺服器設定】視窗中，鍵入下列參數*（如圖 7-6）*：

圖 7-6 修改 PPTP 伺服器設定

- 關閉 PPTP：可點選關閉 PPTP 伺服器。
- 啓動 PPTP：可點選啓動 PPTP 伺服器。
  1.加密認證設定爲關閉。
  2.用戶端 IP 範圍：可輸入 PPTP 用戶端連入 PPTP 伺服器所分配的 IP 網路位址範圍。
- 閒置時間：可設定超過閒置時間範圍將自動斷線。
- 自動排程：可選擇是否加入時間排程。

步驟**2.** 點選【確定】執行新增；或點選【取消】取消新增。

新增 PPTP 伺服器

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【PPTP 伺服器】次功能選項。*（如圖 7-5）。*

步驟**2.** 在【PPTP 伺服器】視窗中，點選下方【新增】按鈕。

步驟**3.** 在【PPTP 伺服器】視窗中，鍵入下列參數

- 使用者名稱：定義 PPTP 用戶端名稱。此名稱必須是唯一且不可重複。
- 密碼：定義 PPTP 用戶端密碼。
- 遠端用戶端：

  1.可勾選 只對單一電腦作連線

  2.可勾選 對整個網域中的電腦作連線

  IP 位址：輸入 PPTP 用戶端整個網域 IP 位址

  子網路遮罩：輸入 PPTP 用戶端子網路遮罩
- 用戶端的 IP 位址：

  1.使用配給的 IP 範圍：勾選 PPTP 用戶端連入時自動分配網路位址。

  2.使用特定 IP 位址： 勾選 PPTP 用戶端連入時使用鍵入網路位址。

步驟**4.** 點選【確定】執行變更；或點選【取消】取消變更。*(如圖 7-7)。*

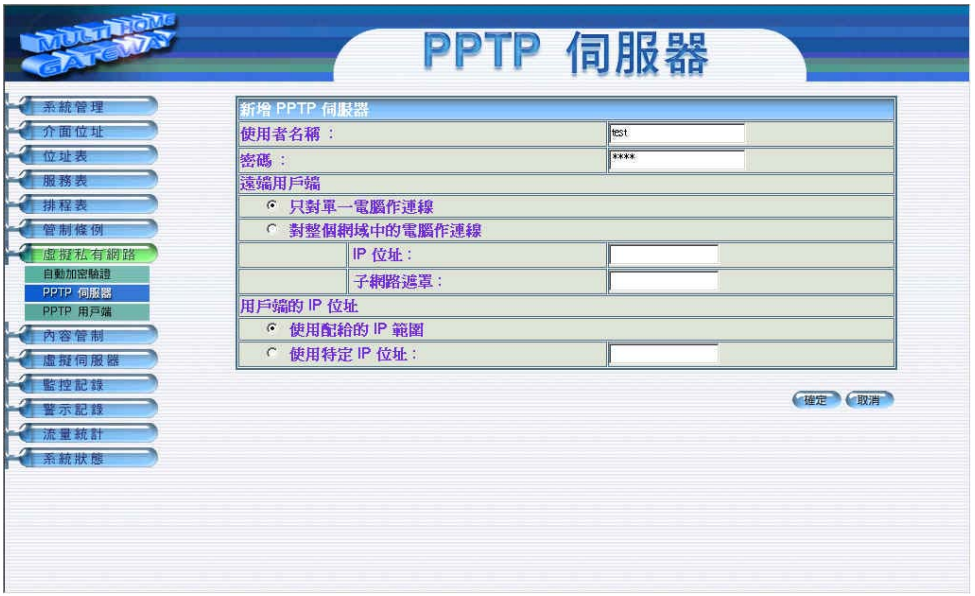

圖 7-7 新增 PPTP 伺服器

修改 PPTP 伺服器

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【PPTP 伺服器】次功能選項。*（如圖 7-5）。*

步驟**2.** 在【PPTP 伺服器】視窗中，找到欲變更設定的 PPTP 伺服器名稱，對應至右方【設定】欄，點選【變更】。

步驟**3.** 在【PPTP 伺服器】視窗中，鍵入下列參數。

步驟**4.** 點選【確定】執行修改；或點選【取消】取消新增。*（如圖 7-8）*

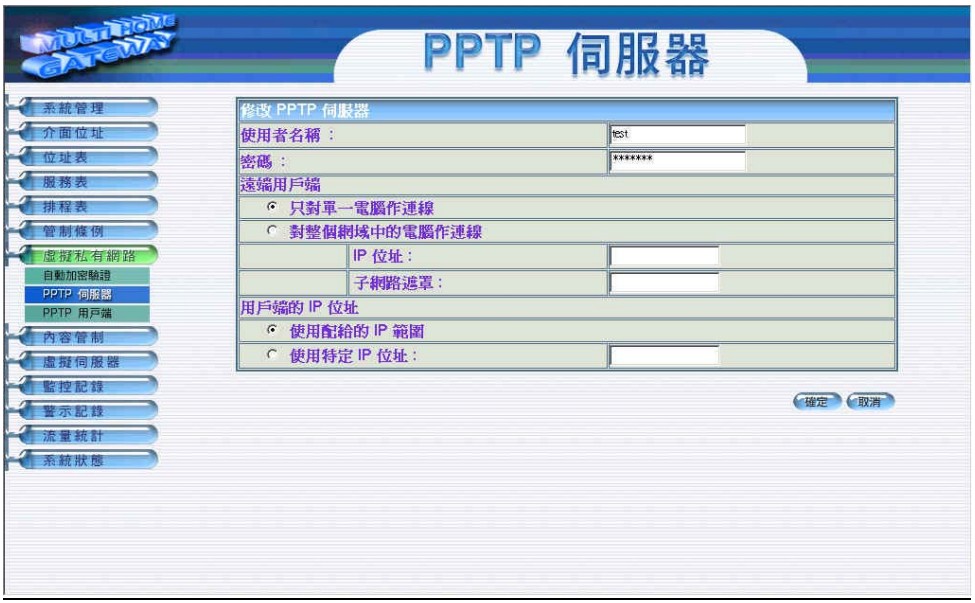

圖 7-8 修改 PPTP 伺服器

移除 PPTP 伺服器

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【PPTP 伺服器】次功能選項。*(如圖 7-5)。*

步驟**2.** 移除：在【PPTP 伺服器】視窗表格中，找到欲移除設定的 PPTP 伺服器名稱，對應至右方【設定】欄，點選【移除】。

步驟**3.** 在【移除 PPTP 伺服器】確定對話框中，點選【確定】按鈕，移除設定，或 點選【取消】取消移除。*(如圖 7-9)。*

圖 7-9 移除 PPTP 伺服器圖

PPTP 用戶端

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【PPTP 用戶端】次功能選項。*(如圖 7-10)。*

圖 7-10 PPTP 用戶端

- 使用者名稱：PPTP 用戶端連入時所使用的名稱。
- 伺服器位址：PPTP 用戶端連入 PPTP 伺服器網路位址。
- 連線歷時：顯示目前 PPTP 用戶端與 PPTP 伺服器連線時間。
- 連線狀況：顯示目前 PPTP 用戶端與 PPTP 伺服器連線狀況。
- 設定：變更服務表中各項設定值。點選【連線】連線可使 PPTP 用戶端與 PPTP 伺服器端進行連線，點選【變更】，可修改 PPTP 伺服器之各項參數；點選【刪除】，可刪除該項設定。

新增 PPTP 用戶端

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【PPTP 用戶端】次功能選項。*（如圖 7-10）。*

步驟**2.** 在【PPTP 用戶端】視窗中，點選下方【新增】按鈕。

步驟**3.** 在【PPTP 用戶端】視窗中，鍵入下列參數

- 使用者名稱：定義 PPTP 用戶端名稱。此名稱必須是唯一且不可重複。
- 密碼：定義 PPTP 用戶端密碼。
- 伺服器位址：請鍵入預連線 PPTP 伺服器外部網路位址。
- 遠端伺服器：

  1.可勾選 只對單一電腦作連線。

  2.可勾選 對整個網域中的電腦作連線。

  IP 位址：輸入 PPTP 伺服器端整個網域 IP 位址。

  子網路遮罩：輸入 PPTP 伺服器子網路遮罩。
- 當封包傳送時自動連線：可點選封包傳送時自動與 PPTP 伺服器連線。
- 閒置時間：可設定超過閒置時間範圍將自動斷線。
- 自動排程：可選擇是否加入時間排程。

步驟**4.** 點選【確定】執行變更；或點選【取消】取消變更。*(如圖 7-11)。*

圖 7-11 新增 PPTP 用戶端

修改 PPTP 用戶端

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【PPTP 用戶端】次功能選項。*（如圖 7-10）。*

步驟**2.** 在【PPTP 用戶端】視窗中，找到欲變更設定的 PPTP 用戶端名稱，對應至右方【設定】欄，點選【變更】。

步驟**3.** 在【PPTP 用戶端】視窗中，鍵入所修改的參數。

步驟**4.** 點選【確定】執行修改；或點選【取消】取消新增。*（如圖 7-12）*

圖 7-12 修改 PPTP 用戶端

移除 PPTP 用戶端

步驟**1.** 在左方的功能選項中，點選【虛擬私有網路】功能，再點選【PPTP 用戶端】次功能選項。*(如圖 7-10)。*

步驟**2.** 移除：在【PPTP 用戶端】視窗表格中，找到欲移除設定的 PPTP 用戶端名稱，對應至右方【設定】欄，點選【移除】。

步驟**3.** 在【移除 PPTP 用戶端】確定對話框中，點選【確定】按鈕，移除設定，或 點選【取消】取消移除。*(如圖 7-13)。*

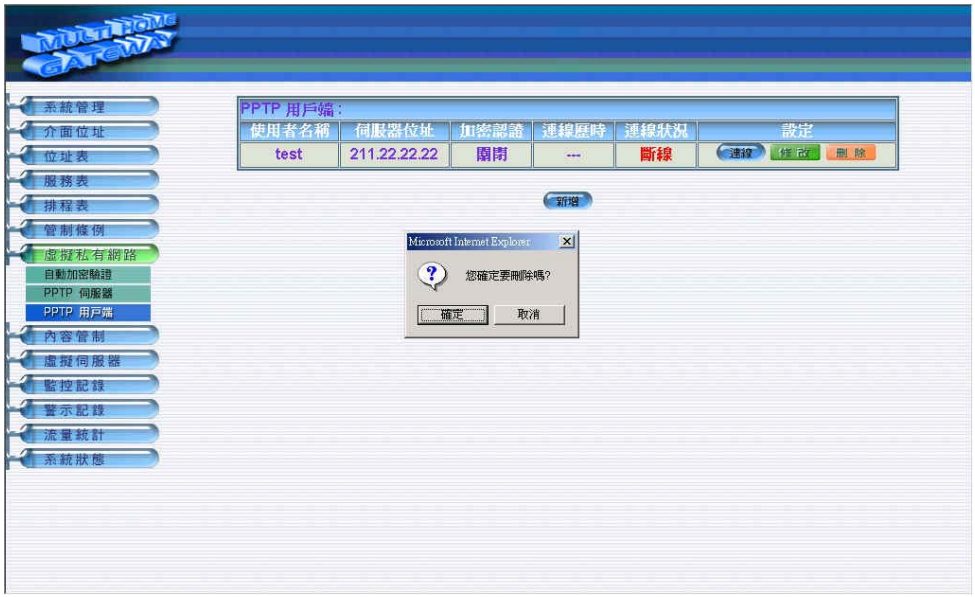

圖 7-13 移除 PPTP 用戶端

第八章

內 容 管 制

內容管制分爲「網站管制」與「Script 管制」兩種。

（一）【網站管制】：系統管理員可使用完整網域名稱、關鍵字、萬用字元（〝～〝及〝＊〞）針對特定網站作「開放」或「限制」進入的制訂。

（二）【Script 管制】：管制 Popup、ActiveX、Java、Cookie「開放」或「限制」進入。

如何運用內容管制

系統管理員可使用完整網域名稱、關鍵字、萬用字元（〝～〝及〝＊〞）針對特定網站作「開放」或「限制」進入的制訂。

網站管制功能設定

設定管制的網站，系統管理員可使用完整網域名稱、關鍵字、萬用字元（〝～〞及〝＊〞）針對特定網站作「開放」或「限制」進入的制訂。

步驟**1.** 於左方功能選項，先點選【系統組態】，接著點選下方的【網站管制】，進入【網站管制】工作視窗。*（如圖 8-1）*

圖 8-1 進入網站管制功能設定

步驟**2.** 網站管制工作視窗名詞定義：

- 網站名稱：受到路由分配器管制進入或僅開放進入的網域名稱。
- 排程表：可利用排程表來管制何時禁止或開放。
- 變更：變更網站管制中各項設定值。點選【修改】，可修改網站管制各項參數；點選【刪除】，可刪除該項設定。

步驟**3.** 網站管制使用方法：

符號說明：〝～〞表示開放；〝＊〞表示萬用字元。

限制無法進入特定網站：在新增網站管制功能的網站名稱中，鍵入欲

禁止網站的「完整網域名稱」、或「關鍵字」。如：www.yahoo.com 或 yahoo。

僅開放特定網站可進入：

1. 先將欲開放網站一一加入網站管制中，新增時，必須於「完整網域名稱」、或「關鍵字」前加入表示開放進入的符號〝～〞。(如：～www.yahoo.com 或～yahoo)。
2. 在所有欲開放的網站設定完成後，於最後一條欲開放的網站管制後，新增一條全部禁止的指令，亦即在網站名稱中，僅鍵入〝＊〞。
   *注意！*此全部禁止的指令必須永遠放置於最後。*(如下圖)*
3. 若欲新增開放網站，必須先將全部禁止指令移除，再鍵入新網域名稱，完成後，再重新加入全部禁止指令。

新增網站管制

步驟**1.** 於左方功能選項，先點選【內容管制】，接著點選下方的【網站管制】，進入【網站管制】工作視窗。*（如圖 8-1）*

步驟**2.** 點選下方【新增】網站管制功能按鈕。

步驟**3.** 在新視窗網站名稱空欄中，鍵入欲管制進入的網址或關鍵字。*（如圖 8-2）*

步驟**4.** 在排程表下拉選單中，點選欲指定的排程表。

步驟**5.** 點選【確定】新增網站管制，或【取消】取消新增。

圖 8-2 新增網站管制

變更網站管制

步驟**1.** 於左方功能選項，先點選【內容管制】，接著點選下方的【網站管制】，進入【網站管制】工作視窗。*（如圖 8-1）*

步驟**2.** 在【網站管制】的表格中，找到欲變更設定的網站名稱，對應至右方【變更】欄，點選【修改】。

步驟**3.** 在【修改網站管制】視窗中，鍵入新網站的網址，或點選新排程表。*（如圖 8-3）*

步驟**4.** 點選螢幕下方【確定】按鈕，變更設定，或 點選【取消】取消變更。

圖 8-3 變更網站管制

移除網站管制

步驟**1.** 在左方的功能選項中，點選【內容管制】功能，再點選【網站管制】次功能選項。*（如圖 8-1）*

步驟**2.** 在【網站管制】的表格中，找到欲刪除設定的網站名稱，對應至右方【變更】欄，點選【刪除】。

步驟**3.** 在【確定刪除】網站管制對話框中，點選【確定】按鈕，移除設定，或 點選【取消】取消移除。*（如圖 8-4）*

圖 8-4 移除網站管制

Script 管制功能設定

步驟**1.** 在左方的功能選項中，點選【內容管制】功能，再點選【Script 管制】次功能選項。*（如圖 8-1）*

步驟**2.** 【Script 管制】各項偵測功能說明*（如圖 8-5）*

圖 8-5 設定路由分配器各項偵測功能

- Popup 管制：可阻擋自動彈跳出的視窗。
- ActiveX 管制：可阻擋 ActiveX 封包。
- Java 管制：可阻擋 Java 封包。
- Cookie 管制：可阻擋 Cookie 封包。

步驟**3.** 勾選各項偵測功能後，點選螢幕右下方【確定】按鈕。

完成此部分設定後，當系統偵測到管制現象時，路由分配器將會自動阻檔。

第九章

虛 擬 伺 服 器

路由分配器將企業內部網路與網際網路(Internet) 分隔成內部網路與外部網路，因IP位址已不夠分配，企業內的內部網路爲了有足夠的IP位址分配給每一台電腦，大都是將電腦設定成私有IP位址 (Private IP Address)，透過路由分配器的NAT (Network Address Translation) 功能，轉換成真實IP位址(Real IP Address)，如果對外提供服務的伺服器是置於內部網路時，它的私有IP位址將無法讓外部的使用者直接連線使用。

對於此類問題，可使用本路由分配器的虛擬伺服器功能得以解決，所謂虛擬伺服器是將路由分配器外部介面子網路的一個真實IP位址設成虛擬伺服器IP位址，藉由路由分配器IP轉換的功能，將外部使用者尋求服務的連線，由虛擬伺服器IP位址轉換成內部網路實際提供服務伺服器的私有IP位址。

虛擬伺服器還擁有一項特色，一對多的對映功能，即一個外部介面的虛擬伺服器 IP 位址可對映到四部提供相同服務的內部網路伺服器的私有 IP 位址，因虛擬伺服器提供負載平衡(Load Balance)功能，可將尋求服務的連線，依權值比重分配給內部網路的伺服器群組，如此可減少伺服器的負載，降低當機的風險，提高伺服器的工作效率。

於本章節，將針對【IP 對映】、【虛擬伺服器 1/2/3/4】作詳細的介紹與使用說明：

【IP 對映】：因爲內部網路是透過 NAT（Network Address Translation）機制轉換的私有 IP 位址，如果伺服器放於內部網路時，它的 IP 位址是屬於私有 IP（Private IP）位址；外部網路的使用者無法直接連上其私有 IP 位址，必須先連接上外部介面子網路真實 IP（Real IP）位址，再由真實 IP 位址對映到內部網路私有 IP 位址，對映的方式有「IP 對映」與「虛擬伺服器」兩項。「IP 對映」是一對一對映，即一個外部介面真實 IP 位址的所有服務，對映到一個內部網路私有 IP 位址。

【虛擬伺服器 1/2/3/4】：虛擬伺服器是一對多對映，即一個外部介面真實 IP 位址，對映到 1～4 個內部網路私有 IP 位址，並提供【服務表】中基本服務之項目。

如何運用虛擬伺服器

虛擬伺服器和IP對映是因NAT轉換機制而產生IP位址對映方式，他們是運用於【管制條例】中【至內部網路】的管制條例，虛擬伺服器和IP對映兩者功能相當類似，都是以真實IP位址對映到私有IP位址（和NAT轉換方式相反）實際的伺服器是放在私有IP位址上，但是它們之間仍有些差異性存在：

- 虛擬伺服器可以對映到內部多台伺服器，IP對映只能對映到一台內部伺服器，並且虛擬伺服器有負載平衡（Load Balance）功能，將服務的連線對映到不同的伺服器主機。
- 虛擬伺服器址能對映內部實際伺服器某一種服務項目，而IP對映可對映到實際伺服器所有服務。

無論是 IP 對映或是虛擬伺服器，都是運用將外部介面虛擬伺服器的 IP 位址轉換成內部網路實際提供服務的伺服器的私有 IP 位址的功能，使得外部網路的使用者可藉由與虛擬伺服器的 IP 位址尋求服務連線而順利的使用內部網路的伺服器。

IP 對映功能設定

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【IP 對映】次功能選項。*（如圖 9-1）*

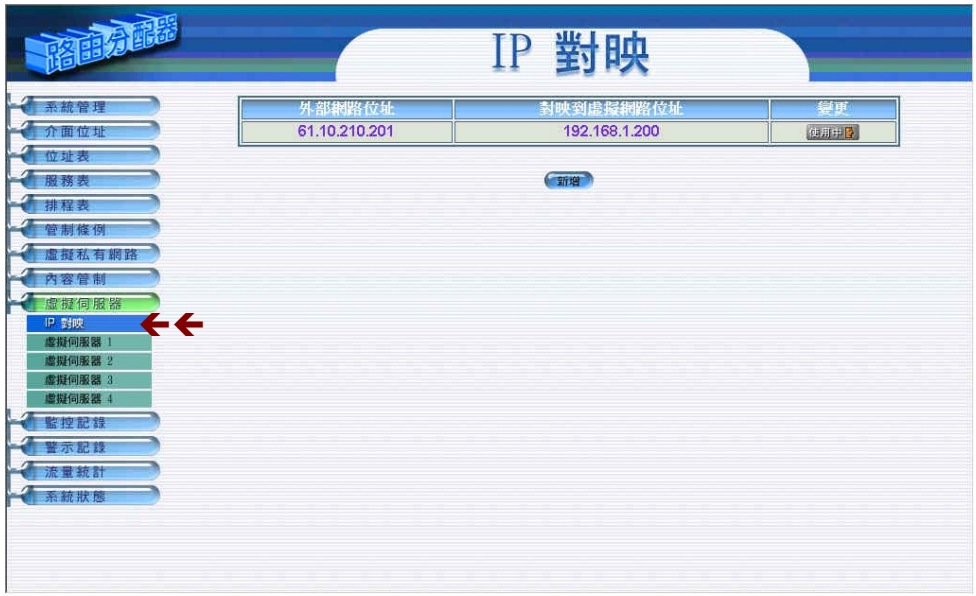

圖 9-1 IP 對映功能設定

步驟**2.** IP 對映表格說明：

- 外部網路位址：外部網路 IP 位址。
- 對映到虛擬網路位址：該外部網路對映至伺服器內之虛擬網路所指定的 IP 位址。
- 變更：變更 IP 對映各項設定值。點選【修改】，可修改 IP 對映各項參數；點選【刪除】，可刪除該項設定。

新增 IP 對映

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【IP 對映】次功能選項。*（如圖 9-1）*

步驟**2.** 在 IP 對映視窗中，點選【新增】功能按鈕。

步驟**3.** 在出現的新增 IP 對映視窗中，鍵入下列相關參數*（如圖 9-2）*

- 外部網路位址：可鍵入外部網路位址。
- Assist：可直接了解目前外部網路 1/2 的 IP 位址。
- 對映到虛擬網路位址：鍵入該外部網路對映至虛擬網路的指定 IP 位址。

步驟**4.** 點選螢幕下方【確定】按鈕，新增指定的 IP 對映，或點選【取消】取消新增。

圖 9-2　新增 IP 對映

變更 IP 對映

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【IP 對映】次功能選項。*（如圖 9-1）*

步驟**2.** 在【IP 對映】視窗中，找到欲變更設定的 IP 對映，對映至右方【變更】欄，點選【修改】。

步驟**3.** 在出現的【修改 IP 對映】視窗中，鍵入欲變更的參數值*（如圖 9-3）*

步驟**4.** 點選螢幕下方【確定】按鈕，變更指定的 IP 對映設定，或點選【取消】取消設定。

圖 9-3 變更 IP 對映

若在【外部至內部網路】管制條例中的目的位址，已設定某 IP 對映，則無法對該條 IP 對映作變更之動作。

移除 IP 對映

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【IP 對映】次功能選項。*（如圖 9-1）*

步驟**2.** 在【IP 對映】視窗中，找到欲變更設定的 IP 對映列，對映至右方【變更】欄，點選【刪除】。

步驟**3.** 在【移除 IP 對映】確定對話框中，點選【確定】按鈕，移除設定，或點選【取消】取消移除。*（如圖 9-4）*

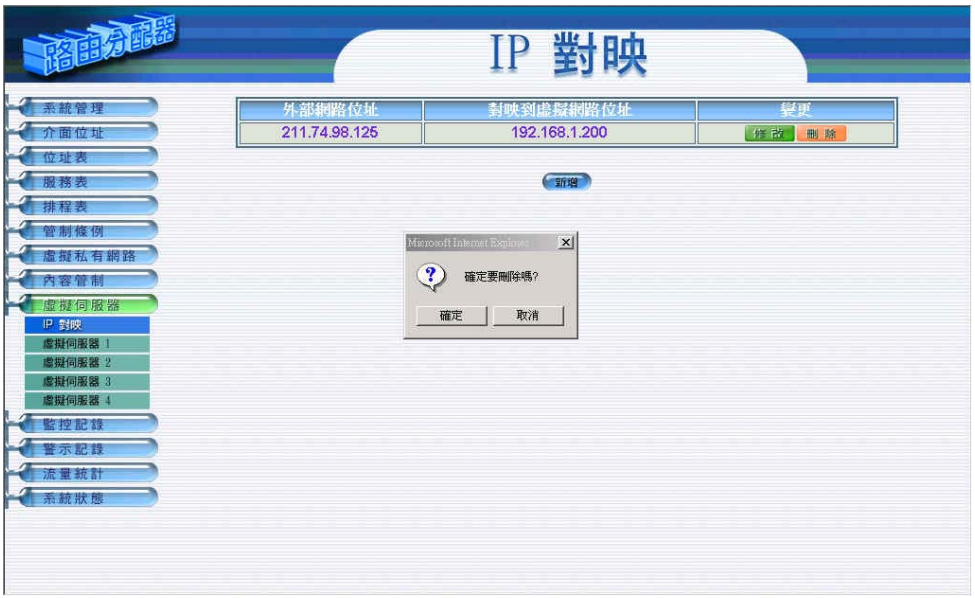

圖 9-4　移除 IP 對映

虛擬伺服器 1/2/3/4 功能設定

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【虛擬伺服器 1/2/3/4】次功能選項。*（如圖 9-5）*

圖 9-5 虛擬伺服器功能設定

步驟**2.** 虛擬伺服器視窗內名詞定義說明：

- 虛擬伺服器 IP：此虛擬伺服器所設定的外部網路 IP 位址。若尚未設定，可點選【選擇】功能按鈕，即可新增新虛擬伺服器位址，若欲變更，則直接點選該【虛擬伺服器 IP 位址】後，鍵入新 IP 位址。
- 服務名稱：此虛擬伺服器所提供的服務項目名稱。
- 埠號:此虛擬伺服器所提供的服務項目所代表之 TCP 埠號碼或 UDP 埠號碼。
- 伺服器 IP 位址：此虛擬伺服器所對映的虛擬網路 IP 位址。
- 變更：變更虛擬伺服器之各項服務設定值。點選【修改】，可修改 IP 對映各項參數；點選【刪除】，可刪除該項設定。

本虛擬伺服器功能提供四個外部介面真實 IP 位址，亦即最多可設定四個虛擬伺服器（由次功能選項之虛擬伺服器 1/2/3/4 中設定）。系統管理員可點選虛擬伺服器 1/2/3/4 工作視窗中，【虛擬伺服器 IP 位址】新增或變更虛擬伺服器之 IP 位址；新增或變更該虛擬伺服器服務設定，則點選下方【新增服務】功能按鈕。

新增虛擬伺服器

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【虛擬伺服器 1（或 2、3、4）】次功能選項。*（如圖 9-5）*

步驟**2.** 在【虛擬伺服器 1（或 2、3、4）】視窗中，點選【虛擬伺服器 IP】功能按鈕。

步驟**3.** 在【新增虛擬伺服器 IP】視窗，由【虛擬伺服器 IP】鍵入可使用外部網路 IP 位址。*（如圖 9-6）*

步驟**4.** 點選【確定】執行新增虛擬伺服器；或點選【取消】取消新增。

9-6 新增虛擬伺服器

變更虛擬伺服器 IP 位址

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【虛擬伺服器 1（或 2、3、4）】次功能選項。*（如圖 9-5）*

步驟**2.** 在【虛擬伺服器 1（或 2、3、4）】視窗中，點選【虛擬伺服器 IP】功能按鈕。

步驟**3.** 在【變更虛擬伺服器】視窗，由【虛擬伺服器 IP】所使用外部網路 IP 位址中， 變更 IP 位址。*（如圖 9-7）*

步驟**4.** 點選【確定】執行變更虛擬伺服器 IP 位址；或點選【取消】取消變更。

圖 9-7 變更虛擬伺服器 IP 位址

移除虛擬伺服器 IP 位址

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【虛擬伺服器 1（或 2、3、4）】次功能選項。*（如圖 9-5）*

步驟**2.** 在【虛擬伺服器 1（或 2、3、4）】視窗中，點選【虛擬伺服器 IP】功能按鈕。

步驟**3.** 在【變更虛擬伺服器】視窗，由【虛擬伺服器 IP】，清除 IP 位址。*（如圖 9-9）*

步驟**4.** 點選【確定】執行移除虛擬伺服器 IP 位址；或點選【取消】取消變更。

圖 9-9　移除虛擬伺服器 IP 位址

虛擬伺服器服務設定

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【虛擬伺服器 1（或 2、3、4）】次功能選項。*（如圖 9-5）*

步驟**2.** 在【虛擬伺服器 1（或 2、3、4）】視窗中，點選虛擬伺服器表格下方【新增】功能按鈕。

步驟**3.** 在【虛擬伺服器組態】設定對話框中*（如圖 9-9）*

圖 9-9 新增虛擬伺服器服務

- 虛擬伺服器 IP：顯示此虛擬伺服器所設定的外部網路 IP 位址。
- 服務名稱埠號：此虛擬伺服器所提供的服務項目的代碼。
- 服務名稱：此虛擬伺服器所提供的服務項目。在此下拉選單內所列的服務項目名稱，皆爲【服務表】內基本服務所定義。
- 編號：伺服器編號。
- 內部網路 IP：此虛擬伺服器所對映的內部伺服器 IP 位址。最多可設定 4 台電腦的 IP 位址，可達到負載平衡的功能。

新增虛擬伺服器服務設定

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【虛擬伺服器 1（或 2、3、4）】次功能選項。*（如圖 9-5）*

步驟**2.** 在【虛擬伺服器 1（或 2、3、4）】視窗中，點選虛擬伺服器表格下方【新增服務】功能按鈕。

步驟**3.** 在【虛擬伺服器組態】對話框中，鍵入下列參數*（如圖 9-10）*

圖 9-10 新增虛擬伺服器服務

- 虛擬伺服器 IP：鍵入此虛擬伺服器所設定的外部網路 IP 位址。
- 服務名稱埠號：無須填寫，點選下方服務項目時，系統會直接顯示該服務項目代碼。
- 服務名稱：點選下拉選單內所列服務項目名稱，此部分表單內容皆爲【服務表】之【基本服務】所定義之服務項目。
- 內部網路 IP：此虛擬伺服器所對映的內部伺服器 IP 位址。最多可設定 4 台電腦的 IP 位址，可達到負載平衡的功能。

步驟**4.** 點選【確定】執行新增虛擬伺服器服務；或點選【取消】取消新增。

系統主管理員可依需求，點選【虛擬伺服器】工作視窗中的【新增服務】控制按鈕，增加虛擬伺服器的服務項目，並在設定【管制條例】前，完成所有虛擬伺服器必須提供的服務項目。否則，於管制條例的服務名稱中將不會顯現，而無法選擇。

變更虛擬伺服器服務設定

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【虛擬伺服器 1（或 2、3、4）】次功能選項。*（如圖 9-5）*

步驟**2.** 在【虛擬伺服器 1（或 2、3、4）】視窗中，由顯示該虛擬伺服器服務項目的表格中，找到欲變更設定的服務名稱，對映至右方【變更】欄，點選【修改】。

步驟**3.** 在【變更虛擬伺服器】視窗，鍵入欲變更的參數值*（如圖 9-11）*

圖 9-11 變更虛擬伺服器服務設定

- 外部網路：鍵入此虛擬伺服器所設定的外部網路 IP 位址。
- 服務埠：無須填寫，點選下方服務項目時，系統會直接顯示該服務項目代碼。
- 服務名稱：點選下拉選單內所列服務項目名稱，此部分表單內容皆爲【服務表】之【基本服務】所定義之服務項目。
- 內部網路 IP：輸入此虛擬伺服器所對映的內部網路 IP 位址。最多可設定四組 IP 位址。

步驟**4.** 點選【確定】執行變更虛擬伺服器服務；或點選【取消】取消變更。

若在【管制條例】中的目的網路，已設定某條虛擬伺服器，則無法對該條虛擬伺服器作變更動作。須先移除該項設定，才可執行變更設定。

移除虛擬伺服器服務設定

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【虛擬伺服器 1（或 2、3、4）】次功能選項。*（如圖 9-5）*

步驟**2.** 在【虛擬伺服器 1（或 2、3、4）】視窗中，由虛擬伺服器服務項目的表格中，找到欲變更設定的服務名稱，對映至右方【變更】欄，點選【刪除】。

步驟**3.** 在【刪除虛擬伺服器】視窗，點選【確定】執行刪除虛擬伺服器 IP 位址；或點選【取消】取消刪除。*（如圖 9-12）*

圖 9-12　移除虛擬伺服器服務設定

若在【管制條例】中的目的網路，已設定某條虛擬伺服器，則無法對該條虛擬伺服器作變更之動作。須先移除該項設定，才可執行變更設定。

第十章

監 控 記 錄

監控記錄爲所有符合【管制條例】的連線記錄，分爲流量監控與事件監控兩種，流量監控的參數是在制定管制條例時同時設定，流量監控詳細記錄每條管制條例資料封包連線內容，包含此封包的連線起始時間、封包來源位址、目的位址、服務項目及處置方式。事件監控則記錄路由分配器系統組態參數值(System Configurations)更改內容，包含更改者、更改時間、修改的參數，從什麼 IP 位址登入…等。

本路由分配器提供之「流量監控」與「事件監控」功能，爲針對系統管理員所指定的「來源位址」與「目的位址」進行「服務項目」及「處置方式」的記錄，讓系統管理員掌握路由分配器系統狀況。同時，本路由分配器亦提供系統管理員將各種記錄下載備份。

（一）【流量監控】系統管理員可在流量監控記錄裡，查詢目前進出路由分配器各個連線狀態，包括：連線起始時間、來源位址、目的位址與處置方式等。並每隔一段時間，將流量監控記錄儲存備份，再刪除線上記錄，讓線上維持最新記錄。
（二）【事件監控】當路由分配器偵測到系統發生某些事件時，系統管理員可經由此事件監控功能，瞭解事件發生的時間詳細說明，並將其下載備份。
（三）【監控報告】：系統管理員可利用此功能，設定系統自動發出 E-mail 提醒管理員流量監控與事件監控的記錄，也可利用遠端記錄即時接收路由分配器的監控報告。

如何運用監控記錄

系統管理員可利用監控記錄，監控網路的使用情形，以作爲網路管理的依據。

流量監控功能

步驟**1.** 在左方的功能選項中，點選【監控記錄】功能，再點選【流量監控】次功能選項。*（如圖 10-1）*

時間	來源位址	目的位址	協定 & 埠號	處置方式
Sep 5 15:07:09	192.168.1.200	168.95.1.1	UDP : 53	ACCEPT
Sep 5 15:07:09	192.168.220.200	192.168.220.1	TCP : 80	ACCEPT
Sep 5 15:07:09	192.168.220.200	192.168.220.1	TCP : 80	ACCEPT
Sep 5 15:07:09	192.168.220.200	192.168.220.1	TCP : 80	ACCEPT
Sep 5 15:07:09	192.168.220.200	192.168.220.1	TCP : 80	ACCEPT
Sep 5 15:07:09	192.168.1.200	168.95.1.1	UDP : 53	ACCEPT
Sep 5 15:07:09	192.168.220.200	192.168.220.1	TCP : 80	ACCEPT
Sep 5 15:07:09	192.168.1.200	168.95.1.1	UDP : 53	ACCEPT
Sep 5 15:07:09	192.168.1.200	168.95.1.1	UDP : 53	ACCEPT
Sep 5 15:07:09	192.168.220.200	192.168.220.1	TCP : 80	ACCEPT
Sep 5 15:07:09	192.168.220.200	192.168.220.1	TCP : 80	ACCEPT
Sep 5 15:07:08	192.168.220.200	192.168.220.1	TCP : 80	ACCEPT
Sep 5 15:07:08	192.168.1.200	168.95.1.1	UDP : 53	ACCEPT
Sep 5 15:07:08	192.168.220.200	192.168.220.1	TCP : 80	ACCEPT
Sep 5 15:07:08	192.168.1.200	168.95.1.1	UDP : 53	ACCEPT
Sep 5 15:07:08	192.168.1.200	168.95.1.1	UDP : 53	ACCEPT
Sep 5 15:07:08	192.168.220.200	192.168.220.1	TCP : 80	ACCEPT
Sep 5 15:07:08	192.168.220.200	192.168.220.1	TCP : 80	ACCEPT
Sep 5 15:07:08	192.168.220.200	192.168.220.1	TCP : 80	ACCEPT

圖 10-1 流量監控功能

步驟**2.** 流量監控視窗名詞名稱定義：

- 下拉選單：點選下拉選單所顯示的連線時間，以檢視於該連線時間之流量狀態。點選【上一頁】，檢視其他連線時間之流量狀態。點選【下一頁】，回到原流量監控畫面。
- 時間：此監控記錄發生的連線起始時間（月/日/時/分/秒）。
- 來源位址：來源端使用者的 IP 位址與協定埠號碼。
- 目的位址：目的端的 IP 位址與協定埠號碼。
- 協定與埠號：服務項目名稱與服務埠。
- 處置方式：ACCEPT 表示允許通過，DROP 表示禁止通過。

下載流量監控記錄

步驟**1.** 在左方的功能選項中，點選【監控記錄】功能，再點選【流量監控】次功能選項。*（如圖 10-1）*

步驟**2.** 在【流量監控】視窗中，點選螢幕下方【下載監控記錄】功能按鈕。

步驟**3.** 在【檔案下載】對話框，將該流量監控記錄儲存至指定的硬碟目錄位置*（如圖 10-2）*

圖 10-2 下載流量監控記錄

清除流量監控記錄

步驟**1.** 在左方的功能選項中，點選【監控記錄】功能，再點選【流量監控】次功能選項。*（如圖 10-1）*

步驟**2.** 在【流量監控】視窗中，點選螢幕下方【清除記錄】功能按鈕。

步驟**3.** 在【清除記錄】確認視窗中，點選【確定】執行清除記錄；或點選【取消】取消清除。*（如圖 10-3）*

圖 10-3 清除流量監控記錄

事件監控功能

步驟**1.** 在左方的功能選項中，點選【監控記錄】功能，再點選【事件監控】次功能選項。*（如圖 10-4）*

圖 10-4 事件監控功能

步驟**2.** 事件監控視窗名詞名稱定義：

- 時間：此連線發生的起始時間。
- 事件：此連線發生時間的事件說明。

下載事件監控記錄

步驟**1.** 在左方的功能選項中，點選【監控記錄】功能，再點選【事件監控】次功能選項。*（如圖 10-4）*

步驟**2.** 在【事件監控】視窗中，點選螢幕下方【下載監控記錄】功能按鈕。

步驟**3.** 在【檔案下載】對話框，將該事件監控記錄儲存至指定的硬碟目錄位置*（如圖 10-5）*

圖 10-5 下載事件監控記錄

清除事件監控記錄

步驟**1.** 在左方的功能選項中，點選【監控記錄】功能，再點選【事件監控】次功能選項。*（如圖 10-4）*

步驟**2.** 在【事件監控】視窗中，點選螢幕下方【清除記錄】功能按鈕。

步驟**3.** 在【清除記錄】確認視窗中，點選【確定】執行清除記錄；或點選【取消】取消清除。*（如圖 10-6）*

圖 10-6 清除事件監控記錄

監控報告功能

步驟**1.** 在左方的功能選項中，點選【監控記錄】功能，再點選【監控報告】次功能選項。*（如圖 10-7）*

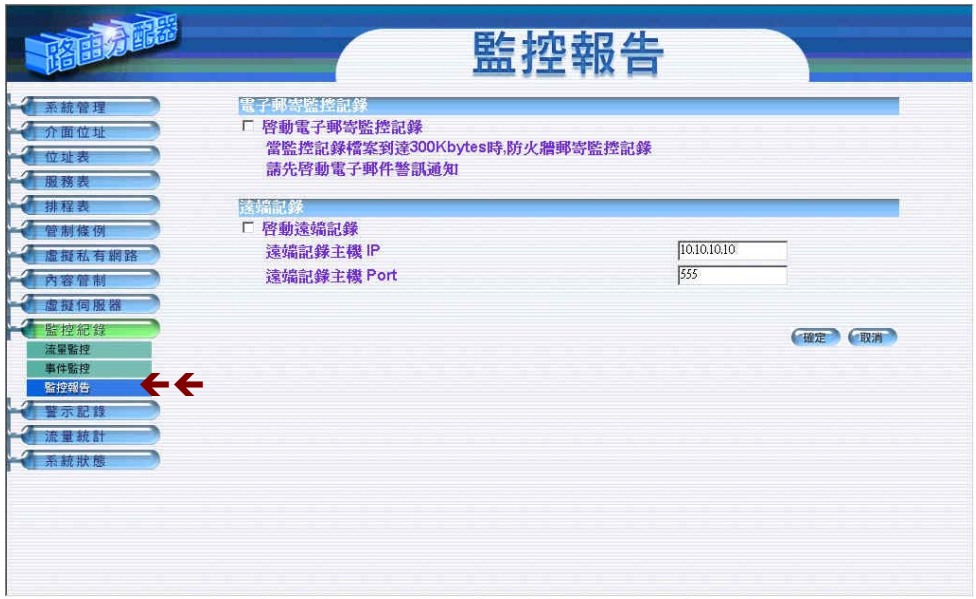

圖 10-7 監控報告

步驟**2.** 【監控報告】視窗名詞名稱定義：

- 電子郵寄監控記錄：當監控記錄檔案到達 300Kbytes 時，路由分配器將會以電子郵件方式發出流量監控與事件監控記錄通知系統管理員。

  ※請注意：啓動此功能必須先於系統管理的系統設定填入 E-mail。
- 遠端記錄：設定此功能，系統會將流量監控與事件監控記錄同步傳送至此設定的 IP 位址的主機電腦。（該主機必須爲提供 Syslog 功能之伺服主機）

欲重新起始連線監控記錄，在【連線記錄】工作視窗中。點選右方【重新設定】功能按鈕，連線監控功能即由設定時即時啓動。

啓動電子郵件與遠端監控記錄

步驟**1.** 在左方的功能選項中，點選【監控記錄】功能，再點選【監控報告】次功能選項。*（如圖 10-7）*

步驟**2.** 開啓電子郵寄監控記錄功能：請先於選單【系統管理】的【系統設定】中的【E-mail 設定】，勾選【開啓電子郵件警訊通知】並鍵入欲接收監控記錄之電子郵件位址，點選【確定】後再於【監控記錄】的【監控報告】勾選【啓動電子郵寄監控記錄】，最後點選螢幕右下方【確定】按鈕。*（如圖 10-8）*

步驟**3.** 啓動遠端記錄：勾選【啓動遠端記錄】，並於下方【遠端記錄主機 IP】空欄中，鍵入提供接收記錄監控的主機 IP 位址與 Port number 後，點選螢幕右下方【確定】按鈕。*（如圖 10-8）*

圖 10-8　啓動電子郵件監控記錄

取消電子郵件與遠端監控記錄

步驟**1.** 在左方的功能選項中，點選【監控記錄】功能，再點選【監控報告】次功能選項。*（如圖 10-7）*

步驟**2.** 取消電子郵寄監控記錄：取消勾選【啓動電子郵寄監控記錄】功能，點選螢幕右下方【確定】按鈕。*（如圖 10-8）*

步驟**3.** 取消遠端記錄：取消勾選【啓動遠端記錄】功能，並點選螢幕右下方【確定】按鈕。*（如圖 10-9）*

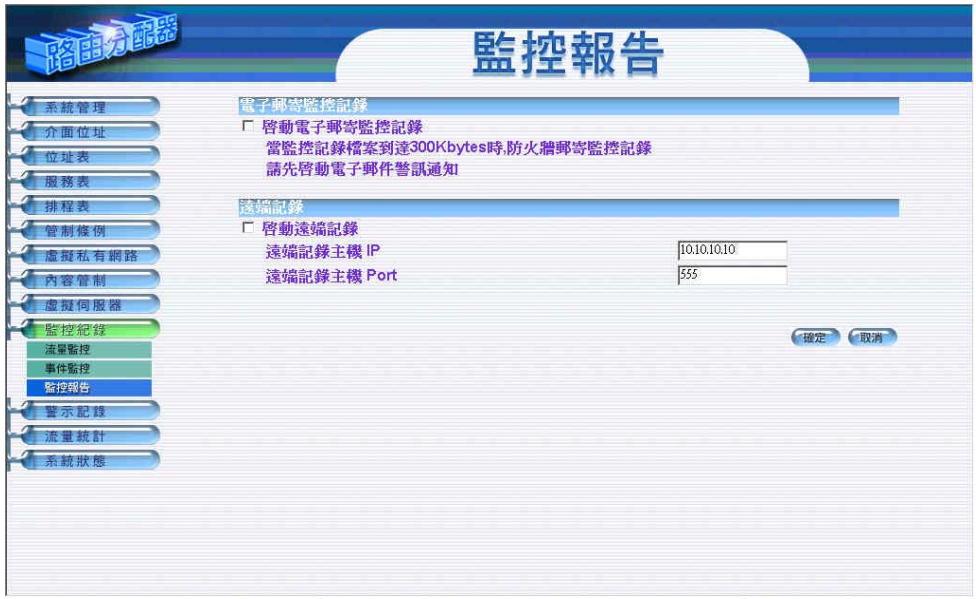

圖 10-9　取消電子郵件監控記錄

第十一章

警 示 記 錄

警示記錄分爲「流量警示」與「事件警示」兩種。

（一）【流量警示】：在制定管制條例時須先設定流量警示值，系統每隔一段時間會檢查經過管制條例的資料量是否超過警示值，如果超過警示值，系統會將其記錄在流量警示檔案。

（二）【事件警示】：當路由分配器偵測出網路正受到駭客惡意攻擊時，系統會將攻擊資料寫入事件警示檔，並發出 E-mail 通知管理員採取警急措施。

如何運用警示記錄

系統管理員可利用「警示記錄」功能，查詢進出路由分配器「來源位址」、「目的位址」、「網路服務」以及網路繁忙狀況。每隔一段時間，系統主管理員可將「流量警示記錄」與「事件警示記錄」儲存備份，再刪除線上記錄，讓線上維持最新網路狀態記錄。

流量警示功能

步驟**1.** 在左方的功能選項中，點選【警示記錄】功能，再點選【流量警示】次功能選項。*（如圖 11-1）*

圖 11-1 流量警示功能

步驟**2.** 流量警示視窗，表格內數值顯現目前系統連線的狀態。

- 時間：連結起始至結束的時間（起始時間 月/日/時/秒 至 結束 時/秒）。
- 來源位址：來源端網路位址。
- 目的位址：目的端網路位址。
- 服務名稱：服務項目名稱。
- 網路流量：網路流量（Kbytes/Sec）。

下載流量警示記錄

步驟**1.** 在左方的功能選項中，點選【警示記錄】功能，再點選【流量警示】次功能選項。*（如圖 11-1）*

步驟**2.** 在【流量警示】視窗中，點選螢幕下方【下載監控記錄】功能按鈕。

步驟**3.** 在【檔案下載】對話框，將該流量警示記錄儲存至指定的硬碟目錄位置*（如圖 11-2）*

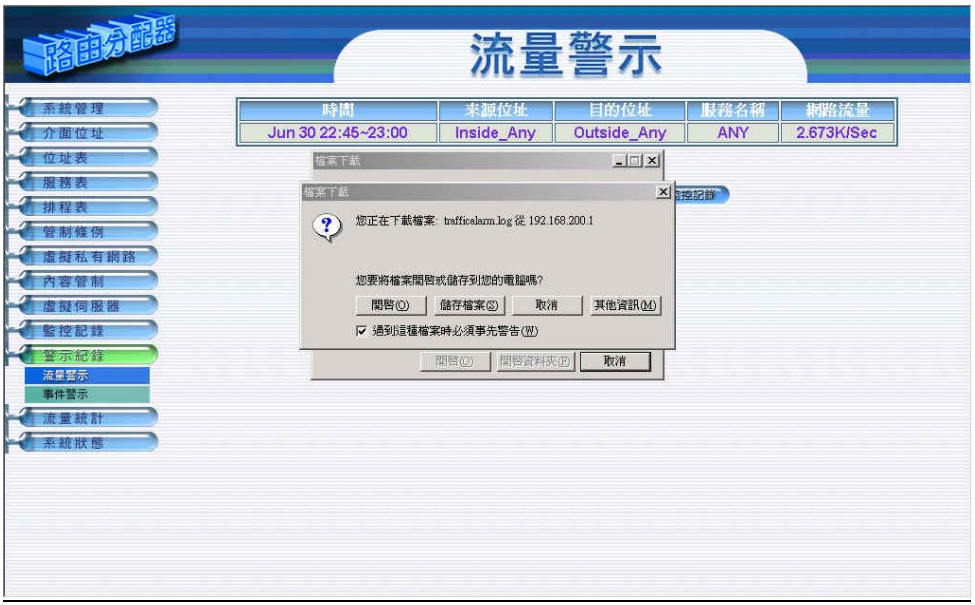

圖 11-2 下載流量警示記錄

清除流量警示記錄

步驟**1.** 在左方的功能選項中，點選【警示記錄】功能，再點選【流量警示】次功能選項。*（如圖 11-1）*

步驟**2.** 在【流量警示】視窗中，點選螢幕下方【清除記錄】功能按鈕。

步驟**3.** 在【清除記錄】確認視窗中，點選【確定】執行清除記錄；或點選【取消】取消清除。*（如圖 11-3）*

圖 11-3 清除流量警示記錄

事件警示功能

步驟**1.** 在左方的功能選項中，點選【警示記錄】功能，再點選【事件警示】次功能選項。*（如圖 11-4）*

圖 11-4 事件警示記錄功能

步驟**2.** 在【事件警示】視窗中，表格內數值顯現目前系統連線狀態

- 下拉選單：可點選下拉選單所顯示的事件警示發生時間，以檢視於該連線時間警示說明。點選【上一頁】，檢視其他連線時間之事件警示。點選【下一頁】，回到原事件警示畫面。
- 時間：事件發生的連線時間（月/日/時/秒）。
- 事件：事件說明。

下載事件警示記錄

步驟**1.** 在左方的功能選項中，點選【警示記錄】功能，再點選【事件警示】次功能選項。*（如圖 11-4）*

步驟**2.** 在【事件警示】視窗中，點選螢幕下方【下載記錄】功能按鈕。

步驟**3.** 在【檔案下載】對話框，將該事件警示記錄儲存至指定的硬碟目錄位置*（如圖 11-5）*

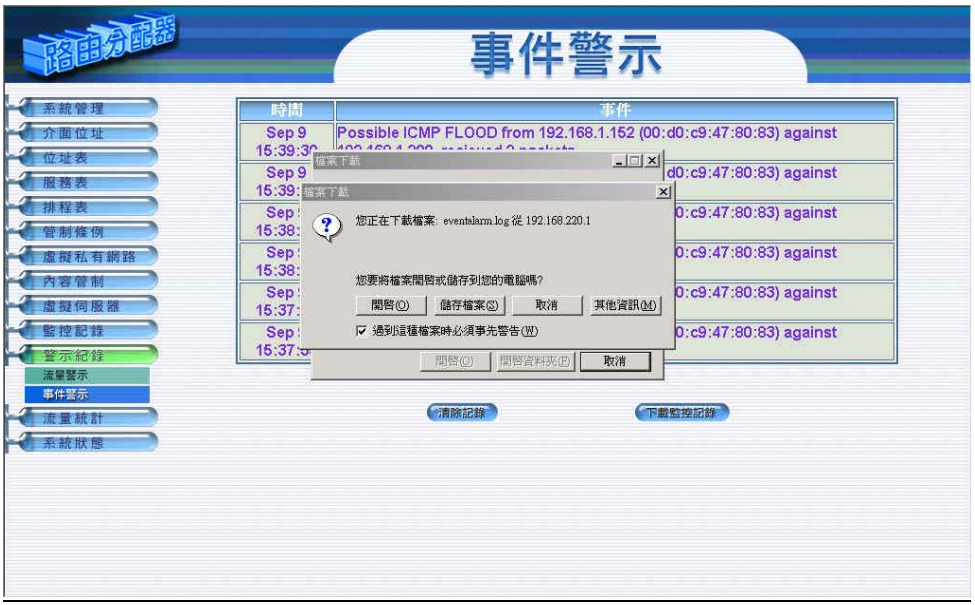

圖 11-5 下載事件警示記錄

清除事件警示記錄

步驟**1.** 在左方的功能選項中，點選【警示記錄】功能，再點選【事件警示】次功能選項。*（如圖 11-4）*

步驟**2.** 在【事件警示】視窗中，點選螢幕下方【清除記錄】功能按鈕。

步驟**3.** 在【清除記錄】確認視窗中，點選【確定】執行清除記錄；或點選【取消】取消清除。*（如圖 11-6）*

圖 11-6 清除事件警示記錄

第十二章

流 量 統 計

「流量統計」即爲所有符合【管制條例】的封包記錄的統計資料。

系統管理員可運用流量統計功能，查詢路由分配器針對【管制條例】內之「來源網路」、「目的網路」、「網路服務」與管制動作等各連線進出路由分配器的「封包」、「傳輸量」流量統計，以提供系統管理員監控網路系統流量狀況，查看網路繁忙狀況。

如何運用流量統計

系統管理員需先至【管制條例】中，設定欲統計流量的網路位址，以經由「流量統計」功能得知目前網路的使用狀況，作爲網路管理的依據。

流量統計功能

步驟**1.** 在左方的功能選項中，點選【流量統計】功能。*（如圖 12-1）*

圖 12-1 流量警示功能

步驟**2.** 流量統計視窗，表格內數值顯現目前系統連線流量。

- 來源/目的 位址：來源/目的 端網路位址。
- 服務名稱：服務項目名稱。
- 管制動作：來源端網路位址、目的端網路位址進出路由分配器資料封包的准許與拒絕動作。
- 時間：檢視分別以分、時、日爲時間單位的流量統計。

若欲使用【流量統計】，系統管理員須先至【管制條例】功能設定中，在指定的網路位址，啓動【流量統計】功能。

檢視流量統計

步驟**1.** 在左方的功能選項中，點選【流量統計】功能。*（如圖 12-1）*

步驟**2.** 在【流量統計】視窗中，找到欲檢視的網路區域名稱，對應至右方【檢視】欄：點選【分】，可檢視以每分鐘（min）爲單位的流量統計圖表；點選【時】，可檢視以每小時(hour)爲單位的流量統計圖表；點選【日】，可檢視以日（day）爲單位的流量統計圖表。

步驟**3.** 流量統計圖表*（如圖 12-2）*

- 縱座標：網路流量（Kbytes/Sec）。
- 橫座標：時間（時/分/日）。

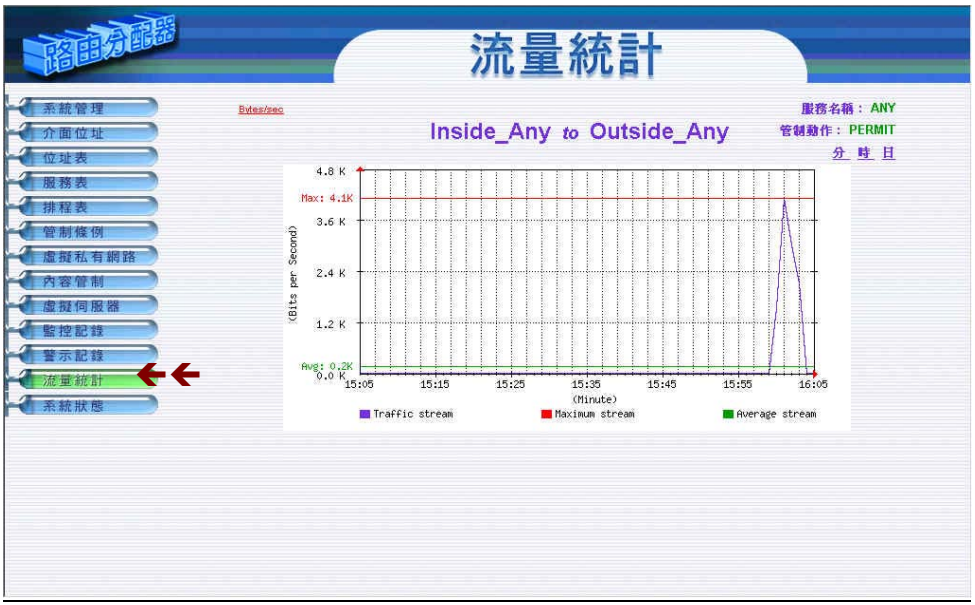

圖 12-2 檢視流量統計

第十三章

系 統 狀 態

使用者可隨時由系統狀態中，得知目前網路連線，如區域網路與外部網路的 IP 位址、子網路遮罩、預設閘道、DNS 伺服器連線 IP 位址等各項資訊。

（一）【介面位址】：目前網路伺服器所設的介面位址資訊。

（二）【ARP 表】：將 MAC 網卡位址轉譯爲 IP 位址。

（三）【DHCP 用戶表】：記錄 DHCP 用戶 IP 位址與 MAC 位址及其租約時間等資訊。

介面狀態功能

步驟**1.** 在左方的功能選項中，點選【系統狀態】功能，再點選【介面狀態】次功能選項。*（如圖 13-1）*

圖 13-1 介面狀態功能

步驟**2.** 【介面狀態】視窗內，顯現目前系統連線之介面位址。

- 系統開機歷時：路由分配器開機歷時時間。

內部網路介面位址（Internal Interface）

- MAC 位址：網路卡識別號碼。
- IP 位址/子網路遮罩: 內部網路 IP 位址/內部網路子網路遮罩。
- MTU：Maximum Transmission Unit。
- 接收封包數, 錯誤封包數：顯示接收封包數,顯示接收錯誤封包數。
- 傳送封包數, 錯誤封包數：顯示傳送封包數,顯示傳送錯誤封包數。
- Ping, WebUI, :

  顯示 Ping 到路由分配器外部網路介面位址功能使用狀態。

  顯示 WebUI 外部網路介面位址連線至路由分配器功能使用狀態。

外部網路介面位址 1 (ADSL 撥接/固接 專線使用者或纜線數據機使用者)

- MAC 位址：網路卡識別號碼。
- IP 位址/子網路遮罩：外部網路 IP 位址/外部網路子網路遮罩。
- 預設閘道：顯示外部通訊閘的位址。
- MTU：Maximum Transmission Unit。
- 接收封包數, 錯誤封包數：顯示接收封包數,顯示接收錯誤封包數。
- 傳送封包數, 錯誤封包數：顯示傳送封包數,顯示傳送錯誤封包數。
- Ping, WebUI,：

  顯示 Ping 到路由分配器外部網路介面位址功能使用狀態,

  顯示 WebUI 外部網路介面位址連線至路由分配器功能使用狀態,

外部網路介面位址 2 (ADSL 撥接/固接 專線使用者或纜線數據機使用者)

- 使用模式：可選擇啓用或是關閉
- MAC 位址：網路卡識別號碼。
- IP 位址/子網路遮罩：外部網路 IP 位址/外部網路子網路遮罩。
- 預設閘道：顯示外部通訊閘的位址。
- MTU：Maximum Transmission Unit。
- 接收封包數, 錯誤封包數：顯示接收封包數,顯示接收錯誤封包數。
- 傳送封包數, 錯誤封包數：顯示傳送封包數,顯示傳送錯誤封包數。
- Ping, WebUI,：

  顯示 Ping 到路由分配器外部網路介面位址功能使用狀態,

  顯示 WebUI 外部網路介面位址連線至路由分配器功能使用狀態,

ARP 表

步驟**1.** 在左方的功能選項中，點選【系統狀態】功能，再點選【ARP 表】次功能選項。*（如圖 13-3）*

圖 13-3 ARP 表

步驟**2.** 【ARP 表】工作視窗內表格名詞定義：

- IP 位址 ： 內部網路 IP 位址。
- MAC 位址：網路卡識別號碼。
- 介面位址：內部網路 IP 位址所屬之介面位址。

DHCP 用戶表

步驟**1.** 在左方的功能選項中，點選【系統狀態】功能，再點選【DHCP 用戶表】次功能選項。*（如圖 13-4）*

圖 13-4 DHCP 用戶表

步驟**2.** 【DHCP 用戶表】工作視窗內表格名詞定義：

- IP 位址：動態 IP 位址。
- MAC 位址：連接動態 IP 位址的 MAC 位址。
- 租用時間：動態位址租用的(起始時間 / 結束時間)（年/月/日/時/分/秒）。

操 作 範 例

操作範例 1

以【管制條例】的制定流程爲範例，讓內部網路的所有 IP 位址都可以連線到網際網路。

步驟**1.** 在左方的功能選項中，點選【管制條例】功能，再點選【內部至外部】次功能選項。

步驟**2.** 在【內部至外部】視窗中，點選【新增】功能按鈕。

步驟**3.** 在出現的【新增管制條例】視窗中，鍵入相關參數 *（如圖 ex1-1）*

步驟**4.** 點選螢幕下方【確定】按鈕，新增指定的內部網路。

圖 ex1-1　新增內部至外部管制條例

操作範例 2

本範例讓公司內部的 IP 位址只能連到 kino 的網站的操作說明，制定流程爲【位址表】至【管制條例】。

步驟**1.** 在左方的功能選項中，點選【位址表】功能，再點選【外部網路】次功能選項。

步驟**2.** 點選【新增】外部網路位址功能按鈕。

步驟**3.** 在新視窗中，鍵入新外部網路各項參數值。*（如圖 ex2-1）*

步驟**4.** 點選螢幕下方【確定】按鈕，新增指定外部網路。

圖 ex2-1　新增外部網路位址

步驟**5.** 在左方的功能選項中，點選【管制條例】功能，再點選【內部至外部】次功能選項。

步驟**6.** 在【內部至外部】視窗中，點選【新增】功能按鈕。

步驟**7.** 在出現的【新增管制條例】視窗中，鍵入相關參數*（如圖 ex2-2）*。

步驟**8.** 點選螢幕下方【確定】按鈕，新增指定的內部網路。

圖 ex2-2　新增內部至外部管制條例

操作範例 3

本範例將以使用【ＩＰ對映】來制定【外部至內部】網路，達到將伺服器架在公司內部(Internal 區)，現在要使外界的使用者，透過 IP 對應來使用伺服器的功能。其制定流程爲由【虛擬伺服器】至【管制條例】。

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【IP 對映】次功能選項。

步驟**2.** 在 IP 對映視窗中，點選【新增】功能按鈕。

步驟**3.** 在出現的新增 IP 對映視窗中，鍵入相關參數*（如圖 ex3-1）*

步驟**4.** 點選螢幕下方【確定】按鈕，新增指定的 IP 對映。

圖 ex3-1　新增 IP 對映

步驟**5.** 出現以下畫面，表示完成 IP 對映的設定。*（如圖 ex3-2）*

圖 ex3-2 新增 IP 對映

步驟**6.** 在左方的功能選項中，點選【管制條例】功能，再點選【外部至內部】次功能選項。*（如圖 ex3-3）*

步驟**7.** 在【外部至內部】視窗中，點選【新增】功能按鈕。

圖 ex3-3 管制條例的外部至內部視窗

步驟**8.** 在出現的【新增管制條例】視窗中，鍵入相關參數後，點選【確定】執行新增群組。*（如圖 ex3-4）*

圖 ex3-4　新增管制條例

步驟**9.** 開放所有的服務項目（ＡＮＹ），設定及完成。*（如圖 ex3-5）*

圖 ex3-5　開放所有服務項目

操作範例 4

本範例將公司的伺服器放在【外部網路】，開放給內部和外部所有ＩＰ位址使用，來制定【管制條例】。其制定流程爲由【虛擬伺服器】至【管制條例】。

步驟**1.** 在左方的功能選項中，點選【虛擬伺服器】功能，再點選【虛擬伺服器 1】次功能選項。進入【虛擬伺服器 1】工作視窗。*（如圖 ex4-1）*

步驟**2.** 點選螢幕上方的【選擇】控制按鈕。

圖 ex4-1　進入虛擬伺服器視窗

步驟**3.** 在【新增虛擬伺服器 IP】視窗中，選擇虛擬伺服器 IP 位址後，點選下方【確定】按鈕。*（如圖 ex4-2）*

圖 ex4-2　新增虛擬伺服器

步驟**4.** 新增虛擬伺服器 IP 後，再接著點選螢幕下方的【新增】控制按鈕。

（如圖 ex4-3）

圖 ex4-3　新增虛擬伺服器服務設定

步驟**5.** 依照伺服器所提供的服務項目，設定好各項參數後，按【確定】。
（如圖 ex4-4）

圖 ex4-4　設定虛擬伺服器

步驟**6.** 出現下列畫面，即表示【虛擬伺服器 1】部分設定完成。*（如圖 ex4-5）*

圖 ex4-5　完成虛擬伺服器設定

步驟**7.** 再到【管制條例】裡的【外部至內部】工作視窗。*（如圖 ex4-7）*

步驟**8.** 點選螢幕下方的【新增】控制按鈕。

圖 ex4-7　進入管制條例之外部至內部視窗

步驟**9.** 在【新增管制條例】設定各項參數，完成後按【確定】。*（如圖 ex4-8）*

圖 ex4-8　新增管制條例

操作範例 5

本範例以 Windows2000 平台操作。假設甲公司 192.168.10.100 要向乙公司 192.168.100.100 做【虛擬私有網路】連線並下載其分享檔案，而 192.168.10.100 的預設閘道爲自己網域的 192.168.10.1，以下設定步驟：

步驟**1.** 進入甲公司防火牆預設位址 192.168.10.1，在左方的功能選項中，點選【虛擬私有網路】功能，再點選【自動加密驗證】次功能選項。*（如圖 ex5-1）*

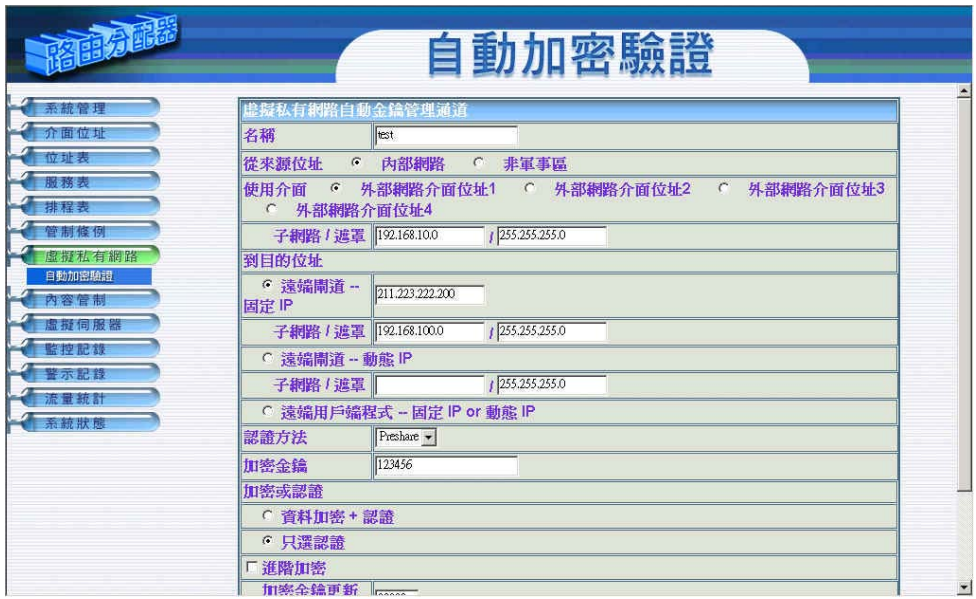

圖 ex5-1 先進入防火牆預設位址，設定自動加密驗證

步驟**2.** 再於乙公司 192.168.100.1 位址設定 VPN。*（如圖 ex5-2）*

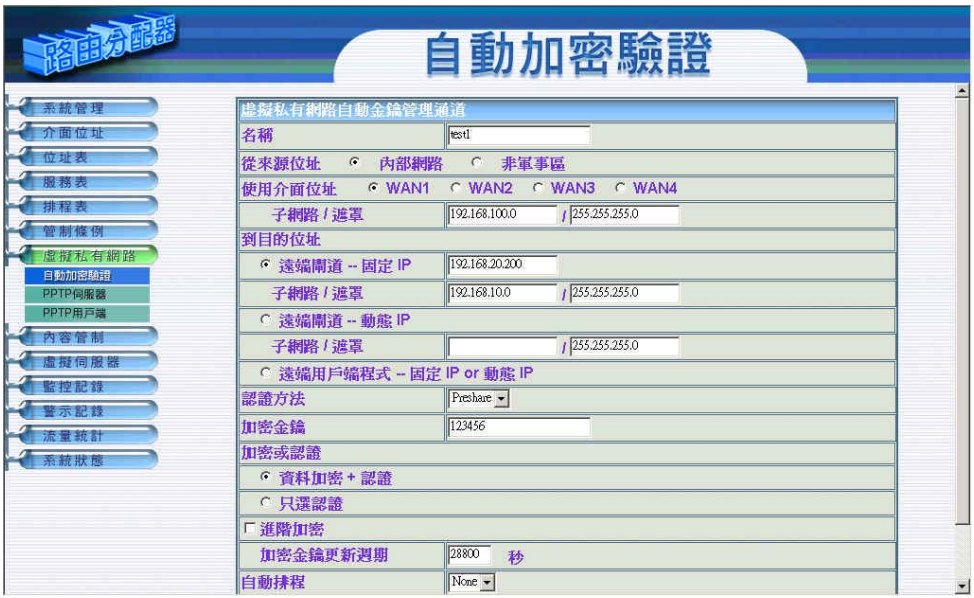

圖 ex5-2 再進入 192.168.2.1，設定 VPN

步驟**3.** 在【開始】功能表下，選擇【設定】中的【控制台】。*（如圖 ex5-3）*

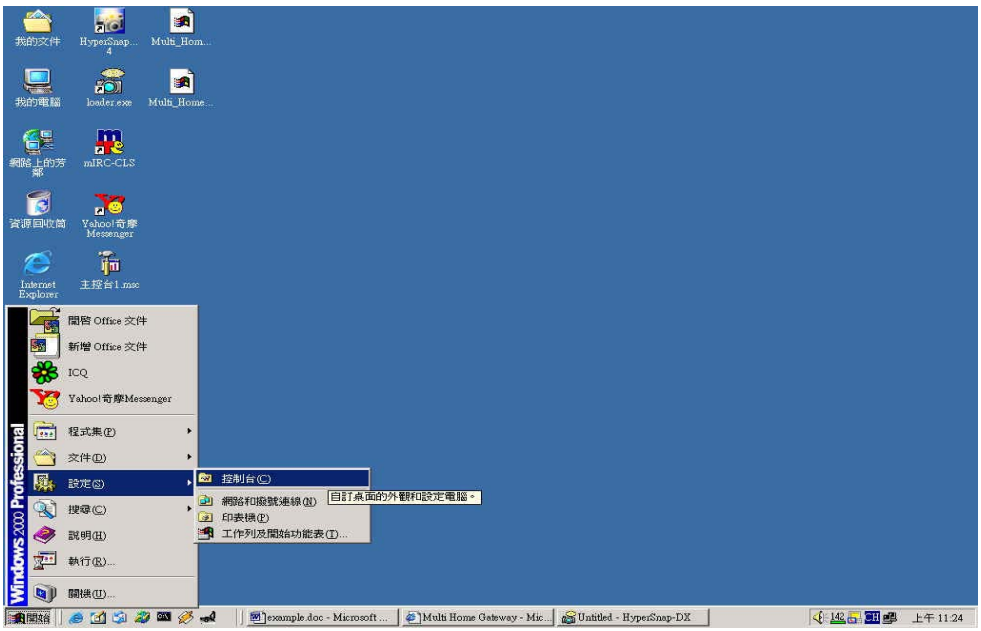

圖 ex5-3 依步驟開啓控制台

步驟**4.** 在【控制台】視窗中，開啓【網路和撥號連線】。*（如圖 ex5-4）*

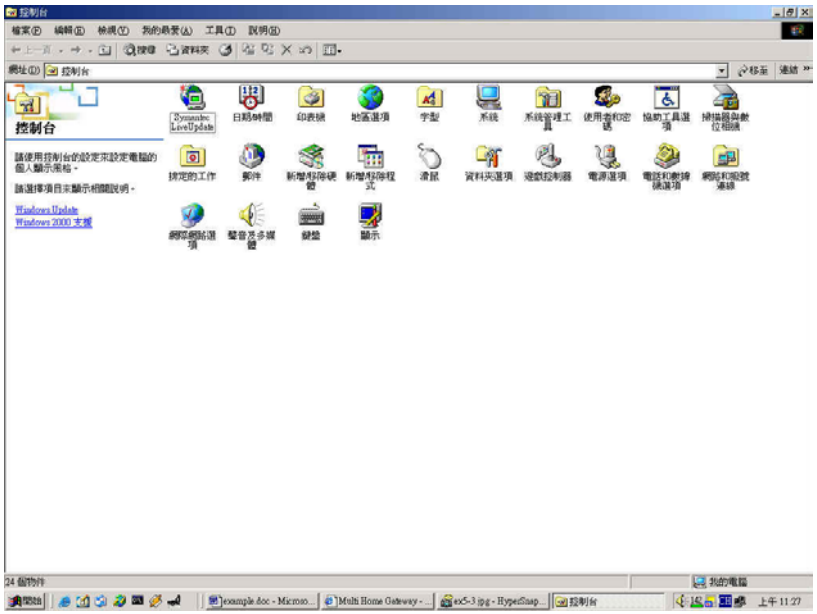

圖 ex5-4 開啓網路和撥號連線

步驟**5.** 在【網路和撥號連線】視窗中，選擇【區域連線】後，按一下滑鼠右鍵，點選【內容】。*（如圖 ex5-5）*

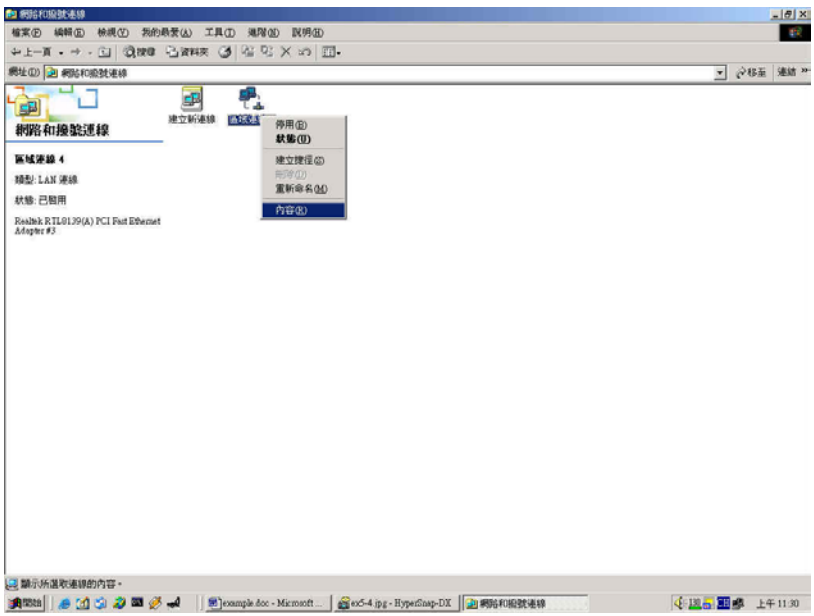

圖 ex5-5 開啓區域連線的內容

步驟**6.** 在【區域連線內容】視窗中，選定【TCP/IP】，接著點選下方【內容】選項。*（如圖 ex5-6）*

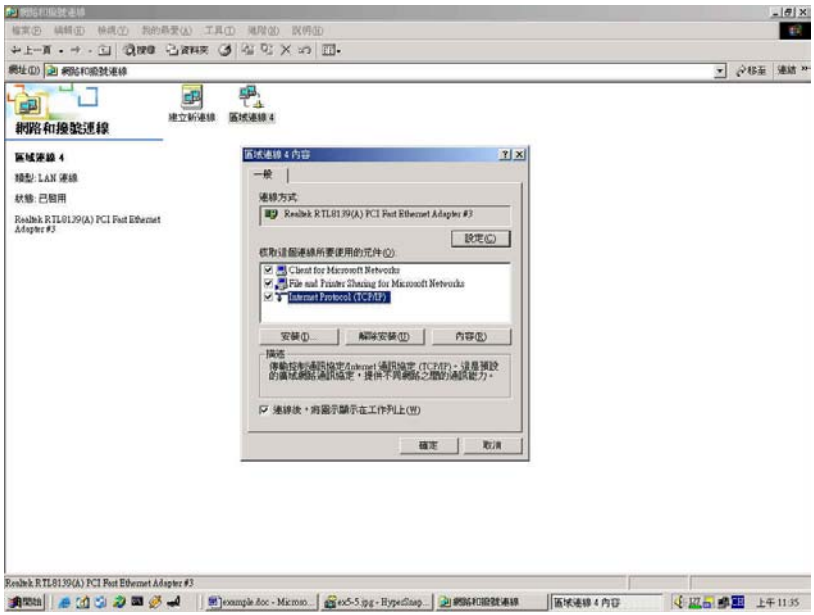

圖 ex5-6 開啓 TCP/IP 的內容

步驟**7.** 【TCP/IP 內容】視窗中，點選【進階】。*（如圖 ex5-7）*

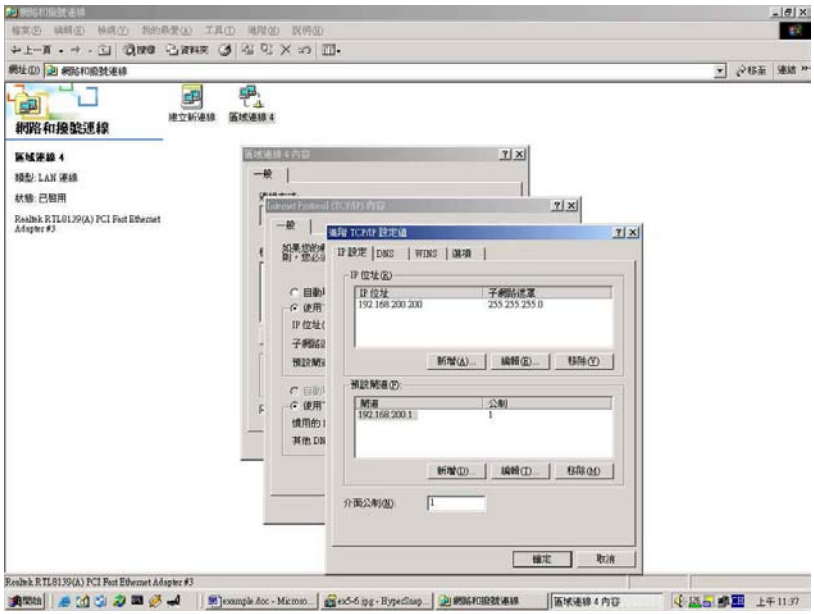

圖 ex5-7 進入 TCP/IP 的進階設定

步驟**8.** 在【進階 TCP/IP 設定值】視窗中，選擇【WINS】，再點選下方【新增】功能*（如圖 ex5-8）*

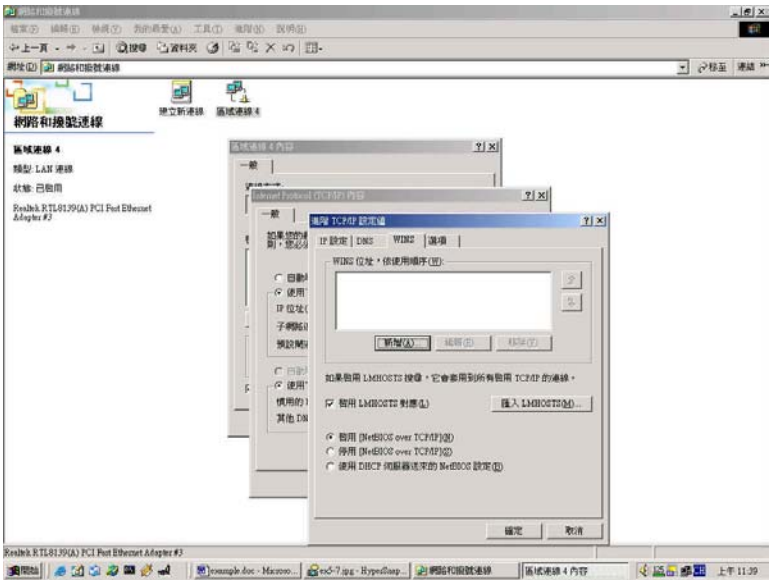

圖 ex5-8 再進入 192.168.2.100，設定 VPN

步驟**9.** 在【TCP/IP WINS 伺服器】視窗中，填入 192.168.100.100（亦即對方的 IP address）後，點選【新增】。*（如圖 ex5-9）*

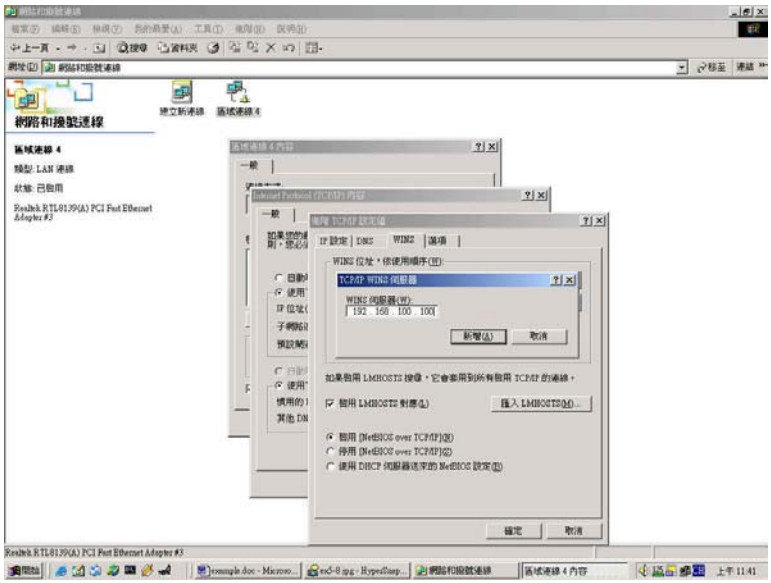

圖 ex5-9 新增 192.168.100.100 伺服器

步驟**10.** 完成新增後，點選『確定』，接著依序點選【確定】離開此設定畫面。
（如圖 ex5-10）

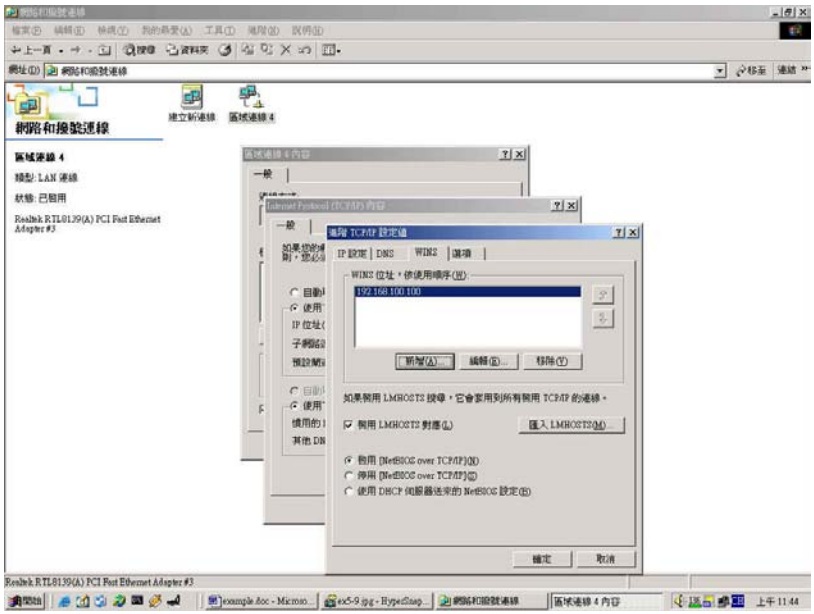

圖 ex5-10 確定新增 192.168.100.100 後，點選確定，離開設定

步驟**11.** 設定完成後，啓動 VPN 連線，並確認雙方已經建立連線。（可用”ping”指令）以確定連線與否。

步驟**12.** 在連線到 192.168.100.100 的分享檔案前，必須先知道對方的電腦名稱才可連線，重複步驟 1 至 3，開啓【控制台】。

步驟**13.** 在【控制台】視窗中，點選【系統】。

步驟**14.** 在【系統內容】視窗中，選擇【網路識別】，找到『完整電腦名稱』，如：nusoft41。*（如圖 ex5-11）*

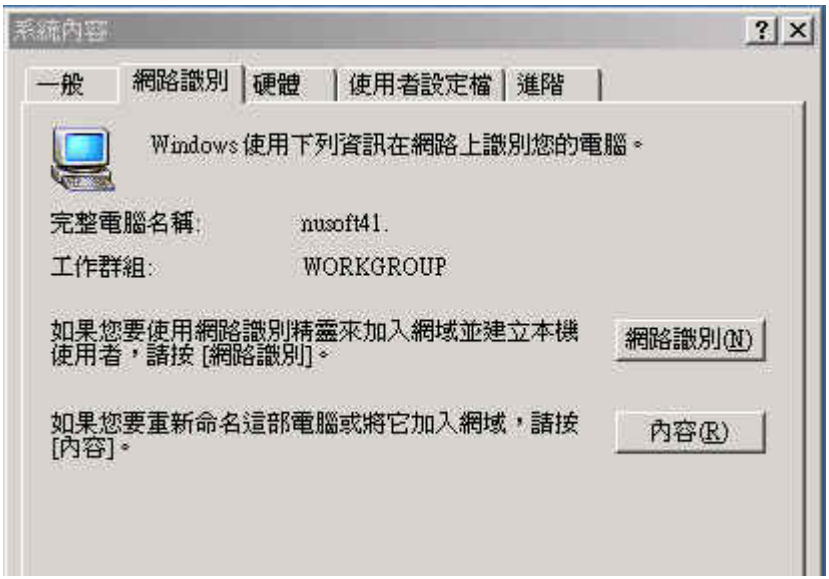

圖 ex5-11 由網路識別，查詢完整電腦名稱

步驟**15.** 在桌面上用滑鼠的右鍵點選【網路上的芳鄰】，選擇【尋找電腦】。*（如圖 ex5-12）*

圖 ex5-12 開啓尋找電腦功能

步驟**16.** 在【尋找電腦】的欄位內，輸入對方的電腦名稱如：nusoft41。點選【立即搜尋】。

步驟**17.** 待搜尋結果出現 nusoft41 即表示已正確連結到 192.168.100.100，即可開始作檔案的存取了。*（如圖 ex5-13）*

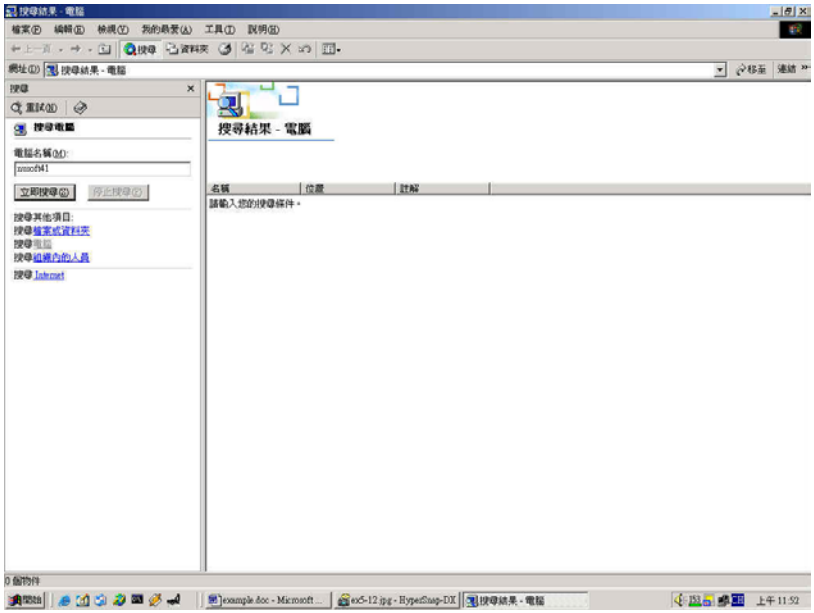

圖 ex5-13 找到欲連線的電腦名稱，即可開始連線作業。