

# **Bandwidth Management**

使用手册

# 目 錄

系统管理.....	1
管理员.....	3
频宽管理器之【管理员】功能设定.....	3
变更主/次管理员密码.....	4
新增次管理员.....	5
删除次管理员.....	6
系统设定.....	7
系统设定.....	7
汇出频宽管理器组态设定档.....	8
汇入频宽管理器组态设定档.....	9
恢复原出厂设定值.....	10
设定实时警讯通知.....	11
设定 Web 管理(外部网络接口).....	12
设定 MTU.....	13
重新激活频宽管理器.....	15
时间设定.....	16
系统时间设定.....	16
语言版本.....	17
语言版本设定.....	17
管理地址.....	18
管理地址功能设定.....	18
新增管理地址.....	19
变更管理地址.....	20
移除管理地址.....	21
Multiple NAT.....	22
Multiple NAT 功能设定.....	22
新增 Multiple NAT.....	24
变更 Multiple NAT.....	25
移除 Multiple NAT.....	26

骇客预警.....	27
骇客预警功能设定.....	27
指定路由表设定功能.....	29
新增网络网关.....	30
变更指定路由表中的网络网关设定.....	31
删除指定路由表中的网关设定.....	32
动态 IP 地址.....	33
动态 IP 地址功能设定.....	33
激活动态 IP 地址功能.....	34
动态 DNS.....	35
动态 DNS 功能设定.....	35
新增动态 DNS.....	37
移除动态 DNS.....	39
注销频宽管理器.....	40
注销频宽管理器设定.....	40
软件更新.....	41
介面位址.....	42
内部网络.....	43
键入内部网络之各项接口地址设定.....	43
外部网络.....	44
ADSL 拨接使用者之接口地址设定.....	44
自动取得 IP 地址(缆线调制解调器使用者).....	46
指定 IP 地址(固接式或 ADSL 专线使用者).....	48
位址表.....	50
内部网络.....	51
地址表之【内部网络】功能.....	51
变更内部网络地址.....	54
移除内部网络地址.....	55
内部网络群组.....	56
内部网络群组功能设定.....	56
新增内部网络群组.....	57

变更内部网络群组设定.....	58
移除内部网络群组.....	59
外部网络.....	60
外部网络功能设定.....	60
变更外部网络地址.....	62
移除外部网络地址.....	63
外部网络群组.....	64
外部网络群组功能设定.....	64
变更外部网络群组设定.....	66
移除外部网络群组.....	67
服务表.....	68
基本服务.....	69
服务表之【基本服务】功能.....	69
自订服务.....	70
自订服务功能设定.....	70
新增自订服务.....	72
变更自订服务.....	74
移除自订服务.....	76
服务群组.....	77
服务群组功能设定.....	77
新增服务群组.....	78
变更服务群组.....	79
删除服务群组.....	80
排程表.....	81
排程表功能设定.....	82
新增排程表.....	83
变更排程表.....	84
移除排程表.....	85
频宽表.....	86
频宽表功能设定.....	87
新增频宽表功能.....	88



修改频宽表功能.....	89
移除频宽表功能设定.....	90
管制条例.....	91
内部至外部.....	93
内部至外部管制条例功能设定.....	93
新增内部至外部管制条例.....	95
变更内部至外部管制条例.....	97
移除内部至外部管制条例.....	99
外部至内部管制条例功能设定.....	100
外部至内部.....	103
新增外部至内部管制条例.....	103
变更外部至内部管制条例.....	105
移除外部至内部管制条例.....	107
内容管制.....	108
网站管制.....	109
网站管制功能设定.....	109
新增网站管制.....	111
变更网站管制.....	112
移除网站管制.....	113
一般管制.....	114
一般管制功能设定.....	114
虚拟伺服器.....	115
IP 对映.....	117
IP 对映功能设定.....	117
新增 IP 对映.....	118
变更 IP 对映.....	119
虚拟服务器.....	121
虚拟服务器 1/2/3/4 功能设定.....	121
新增虚拟服务器.....	123
变更虚拟服务器 IP 地址.....	124
移除虚拟服务器 IP 地址.....	125

虚拟服务器服务设定.....	1 2 6
新增虚拟服务器服务设定.....	1 2 7
变更虚拟服务器服务设定.....	1 2 9
移除虚拟服务器服务设定.....	1 3 1
监控记录.....	1 3 2
流量监控.....	1 3 3
流量监控功能.....	1 3 3
下载流量监控记录.....	1 3 4
清除流量监控记录.....	1 3 5
事件监控.....	1 3 6
事件监控功能.....	1 3 6
下载事件监控记录.....	1 3 7
清除事件监控记录.....	1 3 8
联机纪录.....	1 3 9
联机纪录功能.....	1 3 9
下载联机记录.....	1 4 0
清除联机记录.....	1 4 1
监控报告.....	1 4 2
监控报告功能.....	1 4 2
激活电子邮件与远程监控记录.....	1 4 3
取消电子邮件与远程监控记录.....	1 4 4
警示记录.....	1 4 5
流量警示.....	1 4 6
流量警示功能.....	1 4 6
下载流量警示记录.....	1 4 7
清除流量警示记录.....	1 4 8
事件警示功能.....	1 4 9
下载事件警示记录.....	1 5 0
清除事件警示记录.....	1 5 1
统计报告.....	1 5 2
内部至外部.....	1 5 4

内部至外部统计报告.....	154
外部至内部.....	161
外部至内部统计报告.....	161
流量统计.....	168
外部网络流量.....	169
外部网络流量统计功能.....	169
检视外部网络流量统计.....	170
管制条例流量.....	171
管制条例流量功能.....	171
检视管制条例流量.....	172
系统状态.....	173
接口状态.....	174
接口状态功能.....	174
ARP 表.....	176
DHCP 用户表.....	177
操作范例.....	178
内部至外部管制条例.....	178
管制条例与地址表应用.....	179
虚拟服务器设定.....	181
架设服务器于内部网络.....	184
设定频宽表于内部网络.....	189
设定频宽表于外部网络.....	192

# 系统管理

所谓的系统管理，广义的定义是指进出频宽管理器系统的权限、路径地址与监控等各种相关设定的管理，在本单元中则定义为管理员、系统设定与软件更新的设定与管理。

频宽管理器的管理由系统主管管理员设定。系统主管管理员可增加修改系统的各项设定，监控系统状态，而其它管理员（管理员名称由系统主管管理员设定）仅能读取系统各项设定资料，不能予以更改。在本【系统管理】单元中：

**【管理员】：**系统主管管理员，可依需求新增与变更次管理员人数与名单，或更改次管理员的密码。

**【系统设定】：**系统主管管理员，可经由此功能，将先前储存的频宽管理器系统各单元设定文件，汇出至客户端硬盘中备份；或将备份的设定档汇入至频宽管理器系统以修正/更改频宽管理器设定；以及将频宽管理器设定恢复至原出厂设定值。同时，系统主管管理员也可利用此单元中的**【E-Mail 设定】**功能，设定频宽管理器在遭受骇客侵入时，实时自动传送警讯通知系统管理员,纪录经由**【到路由分器封包】**设定此功能会将频宽管理器的所有进出封包均纪录下来方便进行管制，**【重新激活频宽管理器】**可以重新开机激活频宽管理器。

**【语言版本】：**本软件提供中文与英文两种语言版本，使用者可依个人使用的语言，于此单元中进行软件语言设定。

**【时间设定】：**可将频宽管理器的系统时间设定为与内部使用者计算机或外部时间服务器计算机时间同步。

**【Multiple NAT】：**内部网络可支持多个区段的网络地址。

**【管理地址】:** 让系统管理者仅允许设定 内 / 外 部网络地址, 来进行管理接口管理设定。

**【骇客预警】:** 建立频宽管理器各项侦测功能。系统管理员可利用此功能设定, 激活频宽管理器自动侦测功能, 当系统发生异常现象时, 频宽管理器将会发出电子邮件警告系统管理员, 同时将警告讯息显示在**【警示记录】**之**【事件警示】**窗口中。

**【指定路由表】:** 系统管理员于此单元中, 定义企业网络架构内之内部网络或外部网络, 在资料封包传递至某特定网域时, 所设定之网关地址。

**【动态 IP 地址】:** 系统管理员于此单元中, 定义、开启动态 IP 地址 (DHCP) 组态的各项参数地址与功能。

**【动态 DNS】:** 可让浮动 IP 使用者做实时更新 DNS 与 IP 对映的功能。**【管理地址】:** 此功能可设定被允许进入频宽管理器设定画面的网络地址, 经由此功能, 非设定条例所允许的网络地址在企图联机频宽管理器的接口地址时, 都将被系统认定为不可信任之网络地址而将其阻挡掉。

**【注销频宽管理器】:** 此功能提供管理人员在设定或观察频宽管理器时, 因故离开设定画面, 可利用此功能强制系统将此联机信道断线以防止意图破坏人士之可乘之机。

**【软件更新】:** 使用者可至本公司网站上, 下载最新、功能更强的软件程序, 系统主管理员可利用本功能, 更新频宽管理器软件, 帮助您将频宽管理器发挥最大效用。

## 管理员

### 频宽管理器之【管理员】功能设定

系统主管理员，可依需求新增与变更次管理员人数与名单，或更改次管理员的密码。



图 1-1 点选【系统管理】之【管理员】功能设定选项

【管理员】表格说明：

- 管理员名称：**admin** 为本频宽管理器预设系统管理员名称无法删除。
- 权限：本频宽管理器管理员的使用权限。可分为主管理员与次管理员。
- 组态：管理员之组态设定。点选表格下方【变更】功能修改主/次管理员密码，或点选【删除】功能以删除次管理员。
- 管理员：系统主管理员。主管理员之系统使用权限为【读/写】，亦即可更改系统设定、监控系统状态、新增、删除次管理员等。
- 次管理员：次管理员。次管理员名称由主管理员设定，其系统使用权限为【读】，所有次管理员只能读取系统状态、监控系统状态，无法更改任何系统设定值。

## 变更主/次管理员密码

步驟1. 在【管理员】的表格中，找到欲变更设定的管理员名称，对应至右方【变更】栏，点选【修改】。(如图1-1)

步驟2. 在【变更管理员密码】窗口中。键入下列资料：

- 密码：键入原使用密码。
- 新密码：键入新密码。
- 确认密码：键入与上列新密码栏一致的字符串。(如图1-2)

步驟3. 点选【确认】修改密码，或点选【取消】取消变更设定。



图 1-2 变更管理员密码

## 新增次管理员

步驟1. 在【管理员】设定窗口中，点选屏幕下方【新增次管理员】功能按钮。

(如图 1-1)

步驟2. 在【新增管理员】窗口中，键入以下资料：(如图 1-3)

- 次管理员名称：键入欲新增之次管理员名称。
- 密码：键入密码。
- 确认密码：键入与上列密码栏一致的字符串。

步驟3. 点选【确定】以登录使用者，或点选【取消】取消新增管理员。



图 1-3 新增次管理员



## 删除次管理员

- 步驟1. 在【管理员】的表格中，找到欲变更设定的管理员名称，对应至右方的【变更】栏，点选【删除】。(如图 1-1)
- 步驟2. 屏幕上会立即产生【删除管理员】的确认对话框。(如图 1-4)
- 步驟3. 依照对话框所示，点选【确定】删除该次管理员，或点选【取消】取消删除。



图 1-4 删除次管理员

## 系统设定

系统管理员，可经由此功能，将先前储存的频宽管理器系统各单元设定文件，汇出至客户端硬盘中备份；或将备份的设定档汇入至频宽管理器系统以修正/更改频宽管理器设定；以及将频宽管理器设定恢复至原出厂设定值。同时，系统管理员也可利用此单元中的【E-Mail 设定】功能，设定频宽管理器在遭受骇客侵入时，实时自动传送警讯通知系统管理员,纪录经由【到路由分器封包】设定此功能会将频宽管理器的所有进出封包均纪录下来方便进行管制，【重新激活频宽管理器】可以重新开机激活频宽管理器。

步骤1. 于左方功能选项，先点选【系统管理】，接着点选下方的【系统设定】，进入【系统设定】工作窗口。(如图1-5)

The screenshot shows the 'System Settings' (系統設定) window of the Bandwidth Manager (頻寬管理器). The left sidebar contains a menu with the following items: 系統管理 (System Management), 系統設定 (System Settings), 管理設定 (Management Settings), 管理基本 (Management Basic), 管理位置 (Management Location), Multiple NAT, 駭客防禦 (Hack Defense), 自定义路由表 (Custom Routing Table), 自定义IP地址 (Custom IP Address), 自定义DNS (Custom DNS), 自定义管理地址 (Custom Management Address), 自定义更新 (Custom Update), 介面位置 (Interface Location), 位置表 (Location Table), 策略表 (Policy Table), 带宽表 (Bandwidth Table), 管理策略 (Management Policy), 内容管制 (Content Control), 策略记录 (Policy Log), 警告记录 (Warning Log), 流量统计 (Traffic Statistics), 系统功能 (System Function). The 'System Management' (系統管理) item is selected, and the 'System Settings' (系統設定) item is highlighted with two red arrows. The main content area is titled '系統設定' and includes the following sections: 1. 頻寬管理器組態 (Bandwidth Manager Configuration): 匯出系統組態檔至用戶端 (Download) [Download], 從用戶端匯入系統組態檔 (Import) [Browse...], (ex: bandwidth.conf),  恢復至出廠設定值 (Restore to factory settings). 2. E-mail 設定 (E-mail Settings):  開啟電子郵件警訊通知 (Enable email notification), 備送者位址(非必填) (Sender address) [ ], 郵件 SMTP 伺服器 (SMTP server) [ ], 電子郵件位址 1 (Email address 1) [ ], 電子郵件位址 2 (Email address 2) [ ], 郵件測試 (Test) [Test]. 3. Web 管理(外部網路介面) (Web Management): HTTP 埠號 (Port) [80]. 4. MTU 設定 (MTU Settings): MTU (MTU) [1500]. 5. 到頻寬管理器封包 (To Bandwidth Manager Packets):  記錄到頻寬管理器封包 (Log packets to bandwidth manager), 重新啟動頻寬管理器 (Restart Bandwidth Manager), 頻寬管理器將被重新啟動 (Bandwidth manager will be restarted) [Restart]. At the bottom right, there are buttons for 確定 (OK) and 取消 (Cancel).

图 1-5 【系统管理】功能之【系统设定】工作窗口

## 匯出頻寬管理器組態設定檔

使用本功能,可以将频宽管理器组态设定档案,汇出储存到磁盘上。

**步驟1.** 在【系统设定】窗口中, 点选【频宽管理器组态】下【汇出频宽管理器组态设定档】右方的【下载】功能按钮。

**步驟2.** 在出现【档案下载】窗口中, 选择【将这个档案储到磁盘】, 按下确定, 接着指定汇出档案所要储存的目的位置, 再按下【确定】。频宽管理器设定档即会复制至指定储存位置。(如图1-6)



图 1-6 择汇出档案所要储存的目的位置

## 汇入频宽管理器组态设定档

使用本功能,可以将磁盘上的频宽管理器组态设定档案,汇入至本频宽管理器。

**步骤1.** 在【系统设定】窗口中,点选【频宽管理器组态】下【汇入频宽管理器组态设定档】右方的【浏览】功能按钮。

**步骤2.** 在出现的【选择档案】窗口中,选择之前编辑储存的频宽管理器设定文件所在的目录位置,选择文件名后,再点选【开启】。(如图 1-7)

**步骤3.** 点选屏幕右下方【确定】按钮,将档案汇入至频宽管理器。

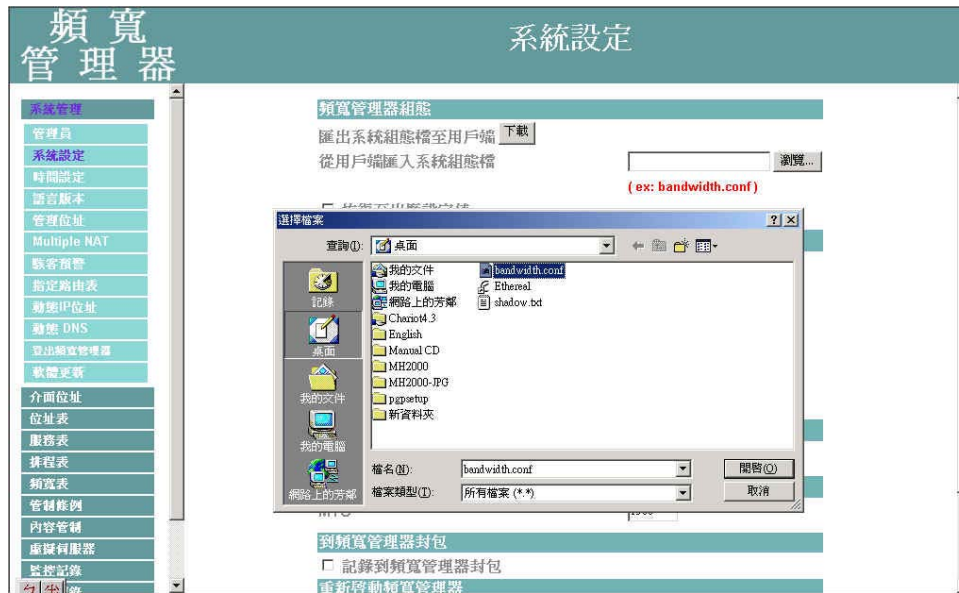


图 1-7 汇入档案所在目录位置与文件名

## 恢复原出厂设定值

使用本功能,会将频宽管理器恢复到出厂时的默认值

步驟1. 在【系统设定】窗口中,勾选【频宽管理器组态】下【恢复原出厂设定值】。

步驟2. 点选屏幕右下方【确定】按钮。恢复频宽管理器原出厂时的设定值。(如图1-8)



图 1-8 勾选【恢复原出厂设定值】

## 设定实时警讯通知

开启此功能后，本频宽管理器系统在任何时候遭受骇客侵入或出现紧急事件时，将自动且实时传送警讯通知系统管理员。（各种骇客攻击侦测，可于【系统管理】之【骇客预警】功能设定。）

**步骤1.** 勾选【E-Mail 设定】下之【激活 E-mail 警讯通知】。开启此功能后，本频宽管理器系统在任何时候遭受骇客侵入或出现紧急事件时，将自动且实时传送警讯通知系统管理员。（各种骇客攻击侦测，可于【系统管理】之【骇客预警】功能设定。）

**步骤2.** 传送者地址(非必填)：在空格中可输入传送者的名称或电子邮件。

**步骤3.** 邮件 SMTP 服务器：在空格中输入递送电子邮件的 SMTP 服务器 IP 地址。

**步骤4.** 电子邮件地址 1：在空格内输入第一位接受警讯通知的电子邮件地址。

**步骤5.** 电子邮件地址 2：在空格内输入第二位接受警讯通知的电子邮件地址。

**步骤6.** 邮件测试：点选旁边【邮件测试】可测试电子邮件地址 1 电子邮件地址 2 ,输入的电子邮件是否能正确收到警讯

**步骤7.** 点选屏幕右下方【确定】设定警讯传送功能。(如图 1-9)



图 1-9 激活频宽管理器实时传送警讯功能

## 設定 Web 管理(外部网络接口)

提供系统管理员在任何地方进行远程管理功能，并可以改变进行远程管理频宽管理器时所使用的埠号。

步驟**1**. 設定 **Web 管理(外部网络接口)**。提供系统管理员在任何时候改变频宽管理器的远程管理所使用的埠号。(如图 1-10)



图 1-10 設定 Web 管理

## 設定 MTU

提供系統管理員在任何時候改變頻寬管理器的進出封包長度。

步驟**1**. **MTU 設定**。輸入需要改變的封包長度。(如圖 1-11)



圖 1-11 設定 MTU



## 设定记录到频宽管理器封包

此功能可以设定将目的 IP 或来源 IP 经过频宽管理器所有进出封包都纪录下来

步骤**1.** 勾选【记录到频宽管理器封包】。开启此功能后，本频宽管理器系统在任何时候会将目的 IP 或来源 IP 为频宽管理器的封包纪录下来，供系统系统管理员浏览。(如图 1-12)



图 1-12 激活记录到频宽管理器封包的功能

## 重新激活频宽管理器

使用本功能会重新将频宽管理器激活(重开机)

步驟**1.** 频宽管理器重新激活：点选旁边【**重新激活**】

步驟**2.** 屏幕上会立即产生【您确定要重新激活】的确认对话框。

步驟**3.** 依照对话框所示，点选【**确定**】重新激活频宽管理器，或点选【**取消**】取消重新激活频宽管理器。(如图1-13)



图 1-13 重新激活频宽管理器

## 时间设定

### 系统时间设定

可将频宽管理器的系统时间设定与内部使用者的计算机或是外部时间服务器的时间同步。

勾选【开启与外部时间服务器同步】。

步骤1. 可点选下拉式选单设定与 GMT 相差时间(以小时为单位)。

步骤2. 可输入外部时间服务器网络地址。

步骤3. 可设定频宽管理器的系统时间每隔多少时间与外部时间服务器自动更新频宽管理器的系统时间，也可选择输入 0 表示不自动更新。

点选 系统时间与此用户计算机同步【同步】按键,则频宽管理器的系统时间会与管理频宽管理器的客户端计算机的时间同步。



图 1-14 系统时间设定

## 语言版本

### 语言版本设定

本功能可更换频宽管理器设定画面的语言版本

步驟**1.** 勾选所欲使用的语言版本（繁体中文/简体中文或英文）。

步驟**2.** 點選【确定】更换软件的语言版本，或點選【取消】取消设定。



图 1-15 频宽管理器软件语言版本设定

## 管理地址

### 管理地址功能设定

可让系统管理者仅允许设定的 内 / 外 部网络地址，来进行频宽管理器的管理设定。(如图1-16)



图 1-16 管理地址

## 新增管理地址

步驟1. 點選下方【新增】功能按鈕。

步驟2. 在新窗口網站名稱空欄中，鍵入內部或外部 IP 地址。 (如圖 1-17)

- IP 地址: 鍵入 內 / 外 部网络之 IP 地址。
- 子网掩碼: 鍵入 內 / 外 部网络的子网掩碼。
- Ping: 勾选此项, 允许远程用户 Ping 外部网络接口地址。
- WebUI: 勾选此项, 允许远程用户使用 HTTP 联机至频宽管理器设定画面。

步驟3. 點選【確定】新增管理地址，或【取消】取消新增。



The screenshot shows the '頻寬管理器' (Bandwidth Manager) web interface. The main title is '管理位址' (Management Address). On the left is a navigation menu with various system management options. The main content area displays the '新增管理位址' (Add Management Address) form with the following fields:

新增管理位址	
IP 位址	61.22.22.22
子網路遮罩	255.255.255.255
服務選項:	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> WebUI
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 1-17 新增管理地址

## 變更管理地址

- 步驟**1.** 在【管理位址】的表格中，找到欲變更設定的 IP 地址，對應至右方【變更】欄，點選【修改】。
- 步驟**2.** 在【修改管理地址】窗口中，鍵入新的 IP 地址。（*如圖 1-18*）
- 步驟**3.** 點選螢幕下方【確定】按鈕，變更設定，或點選【取消】取消變更。



圖 1-18 變更管理地址

## 移除管理地址

- 步驟1. 在【管理位址】的表格中，找到欲刪除設定的 IP 地址，對應至右方【變更】欄，點選【刪除】。
- 步驟2. 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1-19](#)）



圖 1-19 移除管理地址



## Multiple NAT

### Multiple NAT 功能设定

可让内部网络设定多个网段地址，并可经由不同的外部地址与网际网络建立联机。

例如：公司的专线申请到多个真实 IP 地址 168.85.88.0/24，公司内部也分为许多的部门，研发部、客服部、业务部、采购部、会计室等，为了方便管理可将各部门以不同 IP 网段来区分。设定方式如下：

- 1.研发部网段 192.168.1.11/24(Internal)  $\leftrightarrow$  168.85.88.253(External)
- 2.客服部网段 192.168.2.11/24(Internal)  $\leftrightarrow$  168.85.88.252(External)
- 3.业务部网段 192.168.3.11/24(Internal)  $\leftrightarrow$  168.85.88.251(External)
- 4.采购部网段 192.168.4.11/24(Internal)  $\leftrightarrow$  168.85.88.250(External)
- 5.会计室网段 192.168.5.11/24(Internal)  $\leftrightarrow$  168.85.88.249(External)

第 1 项在接口地址设定时就设定好了，其它 4 项就必须新增在 Multiple NAT，设定完成后每个部门就会从不同的外部 IP 地址出去，各部门的计算机设定如下

客服部 IP 地址 : 192.168.2.1  
子网掩码: 255.255.255.0  
预设网关 : 192.168.2.11

其它部门也是按照所属之区段来设定，这就是 Multiple NAT 的功能。

Multiple NAT 工作窗口名词定义：

- 外部网络接口地址：外部网络之 IP 地址。
- 内部网络接口地址/子网掩码：内部网络之 IP 地址及屏蔽。
- 变更：变更网络管制中各项设定值。点选【修改】，可修改网络管制各项参数；点选【删除】，可删除该项设定。

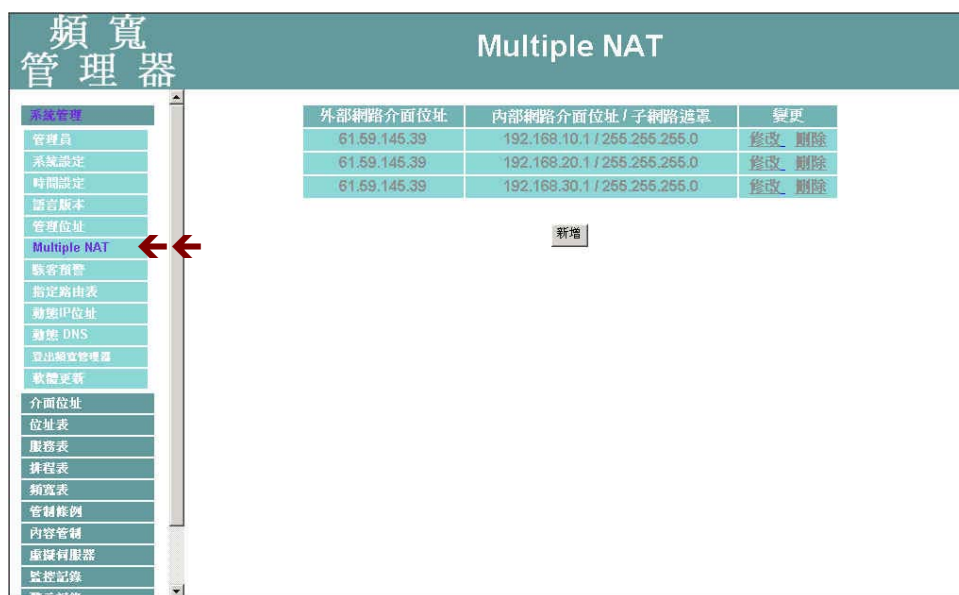


图 1-20 进入 Multiple NAT 功能设定

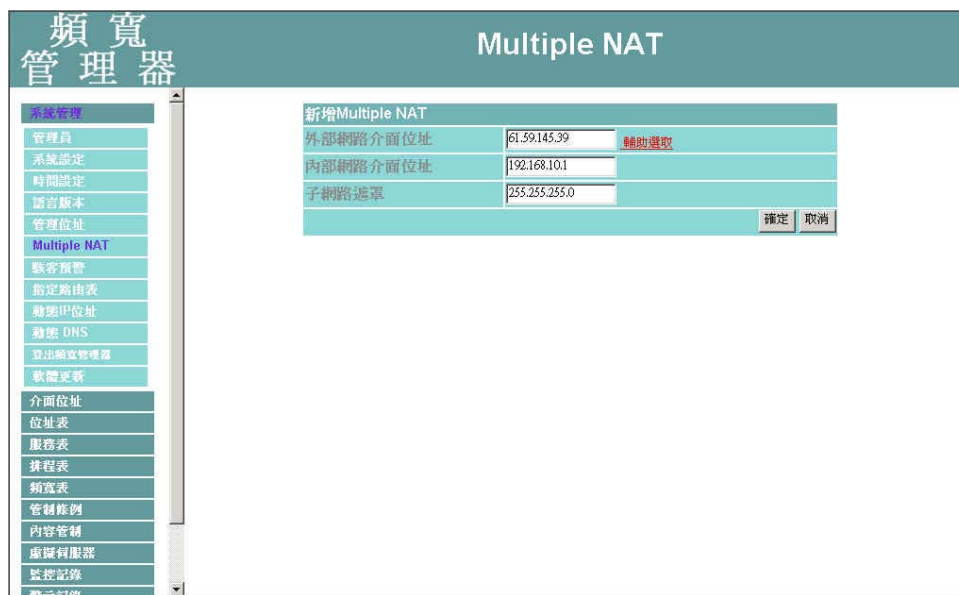
## 新增 Multiple NAT

步驟1. 點選下方【新增】网络管制功能按钮。

步驟2. 在新窗口网站名称空栏中，键入 IP 地址。（如图 1-21）

- 外部网络接口地址：选择外部网络之 IP 地址。
- 外部网络接口地址：键入内部网络之 IP 地址。
- 子网掩码：键入内部网络的子网掩码。

步驟3. 點選【确定】新增 Multiple NAT，或【取消】取消新增。



The screenshot shows a web-based network management interface. The main title is '頻寬管理器' (Bandwidth Manager) and the sub-title is 'Multiple NAT'. On the left is a navigation menu with various system management options. The main content area displays a form for adding a new Multiple NAT rule. The form has three input fields: '外部網路介面地址' (External Network Interface Address) with the value '61.59.145.39' and a '輔助選擇' (Auxiliary Selection) button; '內部網路介面地址' (Internal Network Interface Address) with the value '192.168.10.1'; and '子網路遮罩' (Subnet Mask) with the value '255.255.255.0'. At the bottom right of the form are '確定' (OK) and '取消' (Cancel) buttons.

新增Multiple NAT	
外部網路介面地址	61.59.145.39 <span>輔助選擇</span>
內部網路介面地址	192.168.10.1
子網路遮罩	255.255.255.0
<span>確定</span> <span>取消</span>	

图 1-21 新增 Multiple NAT

## 變更 Multiple NAT

- 步驟**1.** 在【Multiple NAT】的表格中，找到欲變更設定的 IP 地址，對應至右方【變更】欄，點選【修改】。
- 步驟**2.** 在【修改 Multiple NAT】窗口中，鍵入新的 IP 地址。（[如圖 1-22](#)）
- 步驟**3.** 點選螢幕下方【確定】按鈕，變更設定，或點選【取消】取消變更。

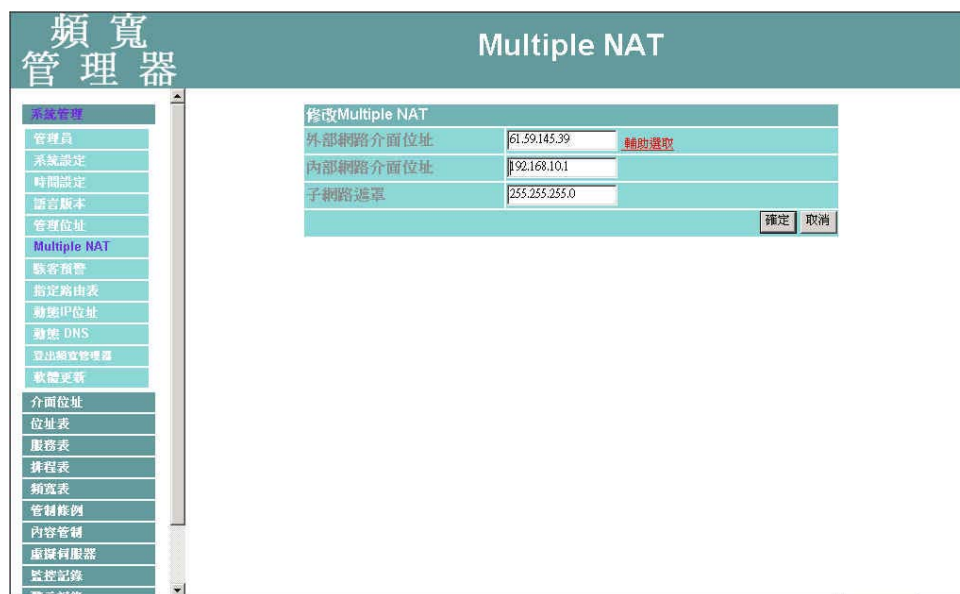


圖 1-22 變更 Multiple NAT

## 移除 Multiple NAT

- 步驟1. 在【Multiple NAT】的表格中，找到欲删除设定的 IP 地址，对应至右方【变更】栏，点选【删除】。
- 步驟2. 在【确定删除】对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。（如图 1-23）

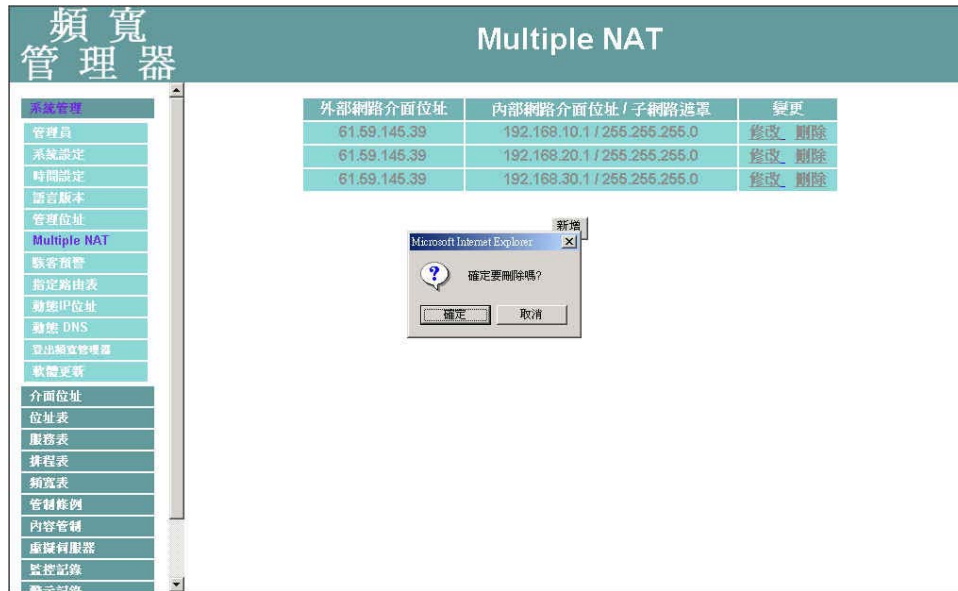


图 1-23 移除 Multiple NAT

## 骇客预警

### 骇客预警功能设定

完成此部分设定后,当系统侦测到任何异常现象时,会立即将警告讯息显示在【警示记录】之【事件警示】窗口中。系统管理员亦可于【系统设定】中开启电子邮件警讯通知功能,频宽管理器将会自动发出电子邮件警告系统管理员。

步骤1. 【骇客预警】各项侦测功能说明 (如图1-24)

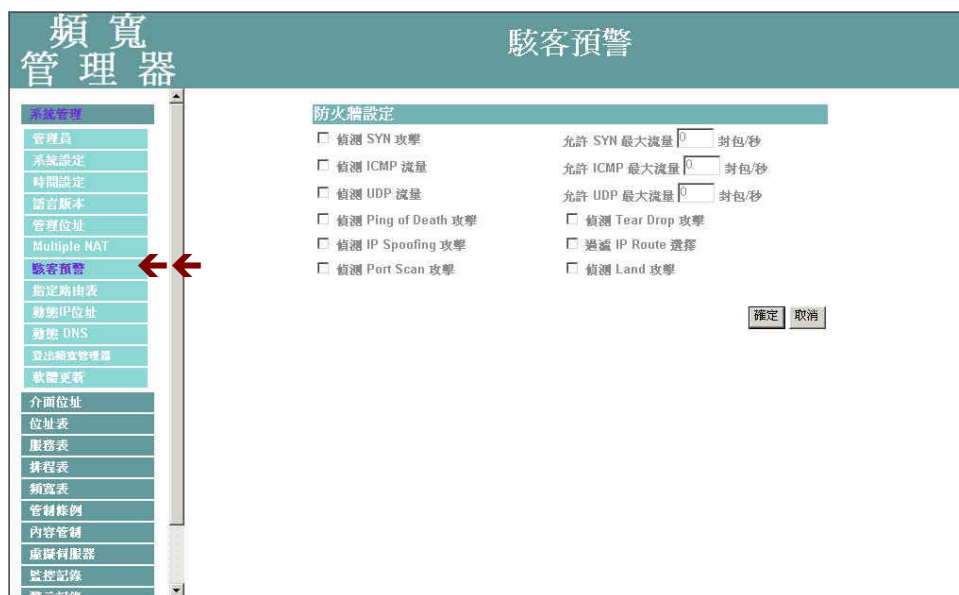


图 1-24 设定频宽管理器各项侦测功能

- 侦测 SYN 攻击: 侦测当骇客连续送出TCP SYN资料封包给服务器,企图将服务器联机 (Connection ) 资源耗光,使其它使用者无法联机成功的状况。勾选此项后,系统管理员可于右方【允许SYN最大流量】空格中,定义每秒可通过频宽管理器的最大封包数(Pkts/Sec)。
- 侦测 ICMP 流量: 侦测当骇客连续发出PING的资料封包,且是以广播方式 (Broadcast) 送给网络内每部机器的状况。勾选此项后,系统管理员可于【允许ICMP最大流量】空格中,定义每秒可通过频宽管理器的最大封包数( Pkts/Sec)。
- 侦测 UDP 流量: 同ICMP Flood。勾选此项后,系统管理员可于【允

许UDP最大流量】空格中，定义每秒可通过频宽管理器的最大封包数(Pkts/Sec)。

- 侦测 Ping of Death 攻击：侦测当骇客送出的PING资料封包带有大量垃圾资料，导致某些系统收到这些资料后产生不良反应，如：执行效率变慢，或系统毁坏必须重新开机，才可正成运作的状况。
- 侦测 IP Spoofing 攻击：侦测当骇客伪造成合法的使用者企图穿越频宽管理器入侵系统。
- 侦测 Port Scan 攻击：侦测当骇客连续发出扫描侦测服务器开放的埠号（Port ID），当服务器对某些Port的侦测有反应时，骇客即可针对此Port攻击的状况。
- 侦测 Tear Drop 攻击：侦测当IP资料封包在传送过程中会被分段切割，而在目的地组合起来。如果攻击者送出自订的封包，强迫分段成为负值的长度，有些系统会将此负值误认为很大的数值，而将大量的资料复制进系统，导致系统损毁、停机或重新开机的状况。
- 过滤 IP Route 选择：IP封包中有个选项，可以指定封包回传时所用的目的位址，且此地址可与IP封包标头中的来源地址不同。骇客可利用此种封包伪装的IP地址进入网域中，并将网域中的资料回传给骇客。勾选这个功能，可以阻挡使用此种选项的IP封包。
- 侦测 Land 攻击：有些系统接收到来源位址与目的位址相同，来源端口号与目的埠号相同，且TCP封包标头中的「SYN」标记又被设定时，会因此处理不当而当机。勾选这个功能即可侦测此种不正常的封包。

**步骤3.** 勾选各项侦测功能后，点选屏幕左下方【确定】按钮。



完成此部分设定后，当系统侦测到任何异常现象时，会立即将警告讯息显示在【警示记录】之【事件警示】窗口中。系统管理员亦可用于【系统设定】中开启电子邮件警讯通知功能，频宽管理器将会自动发出电子邮件警告系统管理员。

## 指定路由表

### 指定路由表设定功能

系统管理员于此单元中，定义企业网络架构内之内部网络或外部网络，在资料封包传递至某特定网域时，所设定之网关地址。



图 1-25 【指定路由表】功能设定

步驟1. 指定路由表工作窗口的表格名词定义：

- 接口地址：目的网域所属区域，为内部网络、外部网络或局域网络。
- 目的位址：连结目的网域之 IP 位址。
- 子网掩码：连结目的网域之子网掩码。
- 网关地址：连结目的网域之网关地址。
- 变更：变更路由表中各项设定值。点选【修改】，可修改指定路由表各项参数信息；点选【删除】，可删除该项设定。



## 新增网络网关

- 步驟1. 在【新增网络网关】窗口中，键入欲新增网络网关的目的位址、子网掩码、网关地址等资料。(如图1-26)
- 步驟2. 在接口地址的下拉选单中，选择欲连结的目的网域所属区域（内部网络、外部网络）。
- 步驟3. 點選【确定】新增所指定的网络网关，或點選【取消】取消设定。



图 1-26 新增指定路由网关

## 变更指定路由表中的网络网关设定

- 步驟1. 在【指定路由表】的表格中，找到欲修改的网络名称，对应至右方【变更】栏，点选【修改】。
- 步驟2. 在出现的【变更指定路径】的窗口中，填入各项欲变更的路径地址。
- 步驟3. 点选【确定】修改该指定网络区域，或点选【取消】取消修改。(如图 1-27)



图 1-27 变更指定路由表中的网关设定

## 删除指定路由表中的网关设定

- 步驟1. 在【指定路由表】的表格中，找到欲移除的网络名称，对应至右方【变更】栏，点选【删除】。
- 步驟2. 在出现的【变更指定路径】的窗口中，填入各项欲变更的路径地址。（如图1-28）
- 步驟3. 在【确定移除】对话框中点选屏幕左下方【确定】执行删除设定，或点选【取消】取消删除。



图 1-28 删除指定路由表中的网关设定

## 动态 IP 地址

### 动态 IP 地址功能设定

若是内部网络计算机要从频宽管理器取得固定 IP，须先至【地址表】的【内部网络】功能中，设定该计算机的 MAC 地址与欲配发的 IP 地址，并勾选下方的【从频宽管理器取得固定 IP 地址】。

步骤1. 于左方功能选项，先点选【系统管理】，接着点选下方的【动态 IP 地址】，进入【动态 IP 地址】工作窗口。(如图 1-29)



图 1-29 动态 IP 地址设定

步骤2. 动态 IP 地址设定信息:

- 子网域：内部网络所属网域。
- 子网掩码：内部网络所属网域屏蔽。
- 网关地址: 内部网络预设网关。
- 广播地址: 内部网络所属网域广播地址。

## 激活动态 IP 地址功能

步驟1. 勾选【激活动态 DHCP 服务器】。并键入下列信息 (如图 1-30)

- 网域名称: 键入内部私有网域名称。
- DNS 服务器 1: 键入欲配发 DNS 服务器 1 之 IP 地址。
- DNS 服务器 2: 键入欲配发 DNS 服务器 2 之 IP 地址。
- WINS 服务器 1: 键入欲配发 WINS 服务器 1 之 IP 地址。
- WINS 服务器 2: 键入欲配发 WINS 服务器 2 之 IP 地址。
- 用户 IP 地址范围 1: 于左边字段键入第一组可使用的起始 IP 地址; 于右边字段键入第一组可使用的结束 IP 地址。
- 用户 IP 地址范围 2: 于左边字段键入第二组可使用的起始 IP 地址; 于右边字段键入第二组可使用的结束 IP 地址。(须为同一网域)
- 租约时间: 为动态 IP 的设定租约时间。

步驟2. 点选【确定】执行动态 IP 地址支持功能, 或【取消】取消激活动态 IP 地址功能。

The screenshot shows a web-based configuration interface for '動態IP位址' (Dynamic IP Address). The interface is divided into a left sidebar menu and a main configuration area. The sidebar menu includes options like '系統管理', '管理員', '系統設定', '時間設定', '語言版本', '管理位址', 'Multiple NAT', '數客預覽', '指定路由表', '動態IP位址', '動態DNS', '退出網管管理員', '軟體更新', '介面位址', '位址表', '服務表', '排程表', '頻寬表', '管轄權例', '內容管制', '虛擬伺服器', '監控記錄', and '顯示幫助'. The main configuration area is titled '動態IP位址' and contains the following settings:

動態IP位址			
子網路	192.168.1.0	子網路遮罩	255.255.255.0
閘道位址	192.168.1.1	廣播位址	192.168.1.255

Below the table, there is a checkbox labeled '啓動DHCP伺服器' which is checked. The configuration options include:

- 網域名稱: [Empty text box]
- DNS伺服器 1: [192.175.55.244]
- DNS伺服器 2: [Empty text box]
- WINS伺服器 1: [Empty text box]
- WINS伺服器 2: [Empty text box]
- 用戶IP位址範圍1: [192.168.1.2] 到 [192.168.1.100]
- 用戶IP位址範圍2: [192.168.1.150] 到 [192.168.1.200]
- 租用時間: [24] 小時

At the bottom right, there are two buttons: '確定' (OK) and '取消' (Cancel).

图 1-30 激活动态 IP 地址功能

## 动态 DNS

### 动态 DNS 功能设定

定动态 DNS，可使用浮动 IP 的使用者直接透过频宽管理器就可以与提供动态 DNS 服务的服务器联机，做浮动 IP 地址与网域名称( Domain Name )的对映。

步驟1. 于左方功能选项，先点选【系统管理】，接着点选下方的【动态 DNS】，进入【动态 DNS】工作窗口。(如图 1-31)



图 1-31 动态 DNS 功能设定

步驟2. 动态 DNS 工作窗口名词定义：

- !: 更新状态。【🔄 联机中, 😊 更新成功, 😞 更新失败, 🤔 不明的错误】
- 网域名称：申请的网域名称。
- 外部网络地址：外部网络接口现在的 IP 地址或是使用者设定的 IP 地址。
- 变更：变更动态 DNS 中各项设定值。点选【修改】，可修改动态 DNS 各项参数；点选【删除】，可删除该项设定。

### 步驟3. 动态 DNS 使用方法：

频宽管理器里提供九家的服务厂商，使用者必须先到该网站注册后才可使用此功能，其使用规章请参阅该服务商网站。

如何注册：于左方功能选项，先点选【系统管理】，接着点选下方的【动态 DNS】，进入【动态 DNS】工作窗口，再按下新增按钮，在服务提供者的右方，按下注册去即出现该服务商的网站，注册办法请自行参阅网站说明。(如图 1-32)

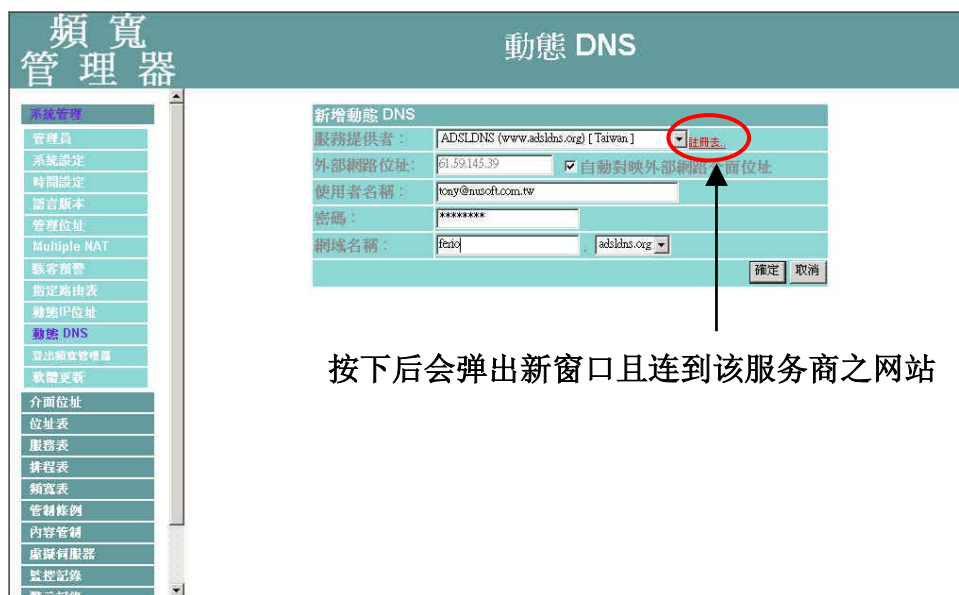


图 1-32 动态 DNS 功能设定

## 新增动态 DNS

步驟1. 點選下方【新增】动态 DNS 功能按钮。

步驟2. 在新窗口空栏中，键入相关信息。（如图 1-33）

- 服务提供者：选择服务提供厂商。
- 注册去：到该服务厂商之网站。
- 外部网络地址：频宽管理器外部接口地址之 IP（可自行输入或勾选自动对映外部网络接口地址）。
- 自动对映外部网络接口地址：自动将外部接口地址填入
- 使用者名称：申请时所注册的帐号。
- 密码：申请时所注册的密码。
- 网域名称/网域：申请时所注册的名称及网域。

步驟3. 點選【确定】新增动态 DNS，或【取消】取消新增。

頻寬管理器

動態 DNS

新增動態 DNS

服務提供者：ADSLDNS (www.adslbbs.org) [ Taiwan ] 註冊去

外部網路位址：61.59.145.39 自動對映外部網路介面位址

使用者名稱：tony@msoft.com.tw

密碼：\*\*\*\*\*

網域名稱：ferio adslbbs.org

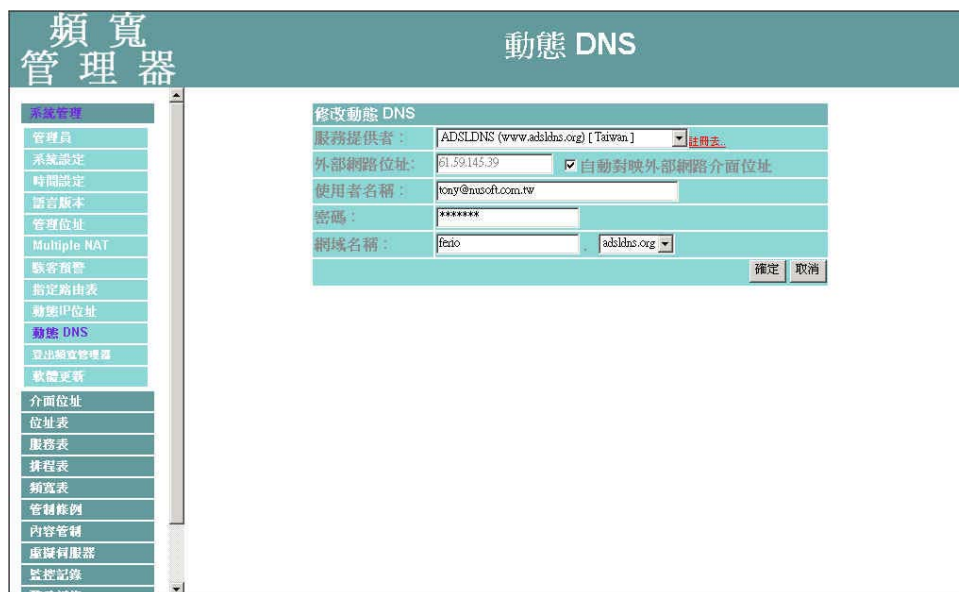
確定 取消

图 1-33 新增动态 DNS



## 变更动态 DNS

- 步驟**1.** 在【动态 DNS】的表格中，找到欲变更设定的项目，对应至右方【变更】栏，点选【修改】。
- 步驟**2.** 在【修改动态 DNS】窗口中，键入新的信息。（如图1-34）
- 步驟**3.** 点选屏幕下方【确定】按钮，变更设定，或点选【取消】取消变更。



The screenshot shows a web-based network management interface titled "頻寬管理器" (Bandwidth Manager) and "動態 DNS" (Dynamic DNS). On the left is a navigation menu with various system management options. The main area displays the "修改動態 DNS" (Modify Dynamic DNS) form. The form includes the following fields:

修改動態 DNS	
服務提供者:	ADSLDNS (www.adslDNS.org) [ Taiwan ] <a href="#">註冊表...</a>
外部網路位址:	61.59.145.39 <input checked="" type="checkbox"/> 自動對映外部網路介面位址
使用者名稱:	lony@mssoft.com.tw
密碼:	*****
網域名稱:	fecio . adslDNS.org
<input type="button" value="確定"/> <input type="button" value="取消"/>	

图 1-34 变更动态 DNS

## 移除动态 DNS

- 步驟1. 在【动态 DNS】的表格中，找到欲删除设定的动态 DNS，对应至右方【变更】栏，点选【删除】。
- 步驟2. 在【确定删除】动态 DNS 对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。（如图 1-35）



图 1-35 移除动态 DNS

## 注销频宽管理器

### 注销频宽管理器设定

防止管理人员在设定或观察频宽管理器时，因故离开设定画面，而造成意图破坏人士之可乘之机，频宽管理器提供此【注销频宽管理器】功能，让设定者在执行此功能后强制系统将此联机信道断线，以防止不明人士进入频宽管理器破坏。

步骤1. 在左方的功能选项中，点选【注销频宽管理器】功能。(如图1-36)。

步骤2. 点选【确定】执行注销频宽管理器功能，或点选【取消】取消注销。



图 1-36 注销频宽管理器设定

## 软件更新

升级频宽管理器软件，请先至本公司网站免费下载最新版本软件，再依下列步骤更新。更新后，无须重新设定频宽管理器系统设定值。

**步骤1.** 由屏幕上【软件版本】信息中，获知目前软件使用版本号码。再经由浏览器至本公司网站取得最新软件版本讯息，并将更新程序下载储存至服务器的硬盘中。

**步骤2.** 先点选左方功能选项的【系统管理】，接着点选下方的【软件更新】，进入【软件更新】工作窗口。(如图1-37)

**步骤3.** 点选【浏览】，于【选择档案】窗口中，选择最新的软件版本文件名称。

**步骤4.** 点选屏幕右下方【确定】功能按钮，执行软件更新升级。



图 1-37 频宽管理器软件更新



软件更新需3分钟的时间，更新后系统将会自动重新开机。

## 介面位址

接口地址包括了频宽管理器系统的内部网络,及外部网络等设定值。这些设定值在设定后会储存在接口地址文件里。

在本【接口地址】单元中：系统管理员于此单元中，依照所选择的 ISP 网络联机方式，定义企业网络架构内的内部网络、外部网络、周围网络的 IP 地址、子网掩码、网关地址等接口地址。



## 外部网络

### ADSL 拨接使用者之接口地址设定

外部网络接口地址 PPPoE (External Interface)

步驟**1**. 勾选外部网络下方【ADSL 拨接使用者 (PPPoE Enable)】。(如图 2-2)。

步驟**2**. 键入外部网络之各项接口地址设定：

頻寬管理器 介面位址

系統管理  
介面位址  
位址表  
服務表  
算數表  
類列表  
管制條例  
內容管理  
庫管理  
庫管理  
警告記錄  
統計報告  
流量統計  
系統狀態

內部網路介面位址  
C Transparent 模式  
NAT 模式  
IP 位址 192.168.1.1  
子網路遮罩 255.255.255.0  
開啓  Ping  WebUI

外部網路介面位址  
PPPoE 設定 (ADSL 撥接使用者) ←←←  
C 自動取得 IP 位址 (動態寬頻使用者)  
C 指定 IP 位址 (固定式或 ADSL 專線使用者)  
目前狀態 連線 [連線] [斷線]  
IP 位址 211.74.99.18  
使用者名稱 0368723  
密碼 \*\*\*\*\*  
由 ISP 提供的 IP 位址  
C 動態  
C 固定  
IP 位址  
子網路遮罩  
預設開道  
下載頻寬 512 Kbps (最大 10 Mbps)  
上傳頻寬 64 Kbps (最大 10 Mbps)  
 自動連線  
間置 0 分鐘自動斷線 (0: 表示不斷線)  
開啓  Ping  WebUI  
[確定] [取消]

图 2-2 ADSL 拨接使用者接口地址设定

- 目前状态：本频宽管理器系统会自动侦测并显现目前网络联机状态（联机中或断线）。
- IP 地址：使用者计算机的 IP 地址。
- 使用者名称：ISP 配发的帐号名称。
- 密码：ISP 配发帐号的密码。
- 由 ISP 提供的 IP 地址：勾选动态 IP；或是勾选固定 IP，并键入该固定 IP 地址。

- 上传频宽/下载频宽：使用者向 ISP 单位所申请的线路频宽。(上传频宽/下载频宽 最大可设定值为 10Mbps)
- 自动联机：勾选此项，当有封包到外部网络时时，将会自动联机上网。
- 闲置？分钟自动断线：原出厂值设定为 0 分钟。您可自行设定为网络闲置时，自动断线的时间，若设定值定为”0”，即表示永远维持联机状态。选择计时制的用户，最好设定自动断线时间，以节省联机费用。
- Ping：勾选此项，激活频宽管理器允许所有外部网络接口地址 Ping。
- WebUI：勾选此项，激活藉由允许外部网络接口地址联机至频宽管理器设定画面。

**步驟3.** 将所有接口地址设定好后，点选屏幕右下方【确定】按钮。



## 自动取得 IP 地址(缆线调制解调器使用者)

### 自动取得 IP 地址(缆线调制解调器使用者)

**步骤1.** 勾选外部网络下方【自动取得 IP 地址(缆线调制解调器使用者)】。*(如图 2-3)。*

**步骤2.** 键入外部网络之各项接口地址设定：

- IP 地址：显示 ISP 配发的外部的 IP 地址。
- MAC 地址 (某些 ISP 要求输入)：某些 ISP 需输入 MAC 地址。
- 用户名称 (某些 ISP 要求输入)：某些 ISP 要求输入配发的帐号名称。
- 网域名称：某些 ISP 要求输入的网域名称
- 上传频宽/下载频宽：使用者向 ISP 单位所申请的线路频宽。(上传频宽/下载频宽 最大可设定值为 10Mbps)
- 更新：：要求重新取得外部 IP 地址。
- 释放：：要求释放已取得外部 IP 地址。
- Ping：勾选此项，允许远程用户 Ping 外部网络接口地址。
- WebUI：勾选此项，允许远程用户使用 HTTP 联机至频宽管理器设定画面。

步驟3. 将所有参数设定好后，点选屏幕右下方【确定】按钮。

頻寬管理器

介面位址

系統管理  
介面位址  
位址表  
服務表  
排程表  
頻寬表  
管制條例  
內容管制  
虛擬伺服器  
監控記錄  
警告記錄  
統計報告  
流量統計  
系統狀態

內部網路介面位址

Transparent 模式

NAT 模式

IP 位址

子網路遮罩

開啓  Ping  WebUI

外部網路介面位址

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

MAC 位址 (某些ISP要求輸入)

用戶名稱 (某些ISP要求輸入)

網域名稱

下載頻寬  Kbps (最大 10 Mbps)

上傳頻寬  Kbps (最大 10 Mbps)

開啓  Ping  WebUI

图 2-3 自动取得 IP 地址(缆线调制解调器使用者)设定

## 指定 IP 地址(固接式或 ADSL 专线使用者)

指定 IP 地址(固接或 ADSL 专线使用者)

步驟**1.** 勾选外部网络下方【指定 IP 地址(固接式或 ADSL 专线使用者)】。

(如图 2-4)。

步驟**2.** 键入外部网络之各项接口地址设定：

- IP 地址：键入 ISP 配发的固定 IP 地址。
- 子网掩码 键入 ISP 配发的子网掩码。
- 预设网关：键入 ISP 配发的预设网关地址。
- DNS 服务器 1/2：键入 ISP 所配发的 DNS 1/2 服务器地址。(详见附注)
- 上传频宽/下载频宽：使用者向 ISP 单位所申请的线路频宽。(上传频宽 / 下载频宽 最大可设定值为 10Mbps)
- Ping：勾选此项，允许远程用户 Ping 外部网络接口地址。
- WebUI：勾选此项，允许远程用户使用 HTTP 联机至频宽管理器设定画面。

步驟**3.** 将所有接口地址设定好后，点选屏幕右下方【确定】按钮。

頻寬管理器

介面位址

系統管理  
介面位址  
位址表  
服務表  
排程表  
頻寬表  
管制條例  
內容管制  
虛擬伺服器  
監控記錄  
警告記錄  
統計報告  
流量統計  
系統狀態

內部網路介面位址

Transparent 模式

NAT 模式

IP 位址

子網路遮罩

開啓  Ping  WebUI

外部網路介面位址

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 地址 (固接式或 ADSL 專線使用者) ← ←

IP 位址

子網路遮罩

預設閘道

DNS 伺服器 1

DNS 伺服器 2

下載頻寬  Kbps (最大 10 Mbps)

上傳頻寬  Kbps (最大 10 Mbps)

開啓  Ping  WebUI

確定 取消

图 2-4 指定 IP 地址(固接或 ADSL 专线使用者)设定



若自行架设 DNS 服务器，需先至【虚拟服务器】功能中，将原先 DNS 服务器的真实 IP 地址对应至内部 DNS 服务器的虚拟 IP 地址，而在此处 DNS 服务器地址中，则必需键入内部服务器的虚拟 IP 地址。

# 位 址 表

本频宽管理器在此单元中提供系统主管理员，定义内部网络、内部网络群组、外部网络、外部网络群组的接口地址。

【地址表】纪录的 IP 地址可能是一个主机 IP 地址，也可能是一个网域多个 IP 地址。系统管理员可以自行设定一个易辨识的名字代表此一 IP 地址。基本上 IP 地址根据不同的网络区可分为二种：内部网络 IP 地址(Internal IP Address)，外部网络 IP 地址(External IP Address)。当系统管理员欲将不同 IP 地址封包的过滤规则，加入相同管制条例时，可先将这些 IP 地址建立一个「内部网络群组」或是「外部网络群组」，以简化设立管制条例工作程序。



## 如何运用地址表

有了易辨识的 IP 地址的名称后，同时地址群组名称也已显示在地址表上，系统管理员在设定管制条例时，就可选用此地址表名称，套用在管制条例的来源地址(Source Address)或目的位址(Destination Address)。所以地址表的设定应该在管制条例的设定之前，如此在设定管制条例时，才可在地址表中挑出正确的 IP 地址名称。

## 内部网络

### 地址表之【内部网络】功能

步驟1. 在左方的功能选项中，點選【地址表】功能，再點選【内部网络】次功能选项。（如图3-1）



图 3-1 内部网络地址功能设定

步驟2. 内部网络工作窗口之表格名词定义：

- 名称：内部网络地址名称。
- IP：内部网络 IP 地址。
- 子网掩码：子网掩码。
- MAC 地址：内部网络 IP 地址对应的 MAC 地址。
- 变更：变更内部网络中各项设定值。點選【修改】，可修改内部网络各项参数信息；點選【删除】，可删除该项设定。



在内部网络窗口中，若是某个地址表成员已被加入管制条例或网络群组之中。则在【变更】字段中，将会出现【使用中】文字，无法进行修改或删除的变更设

定。

## 新增内部网络地址

- 步驟1. 點選【新增】功能按鈕。
- 步驟2. 在新窗口中，鍵入內部網路之網路地址名稱、IP 地址、子網掩碼、MAC 地址等各項參數值。（[如圖 3-2](#)）
- 步驟3. 勾選【從頻寬管理器取得固定 IP 地址】，可使此 MAC 地址每次皆取得同一 IP 地址。
- 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。

新增位址	
名稱	Test
IP	192.168.1.2
子網路遮罩	255.255.255.255
MAC 位址	00:50:BF:16:EA:CE <input type="button" value="填入使用者的MAC位址"/>
<input checked="" type="checkbox"/> 從防火牆取得固定IP位址	
<input type="button" value="確定"/> <input type="button" value="取消"/>	

圖 3-2 新增內部網路地址



若欲使用【從頻寬管理器取得固定 IP 地址】功能，必須先鍵入 MAC 地址，此功能才可生效。



## 变更内部网络地址

- 步驟1. 在【内部网络】的表格中，找到欲变更设定的网络名称，对应至右方【变更】栏，点选【修改】。
- 步驟2. 在新的【变更地址】窗口中，键入各项欲变更的资料。（如图3-3）
- 步驟3. 点选屏幕下方【确定】按钮，变更设定，或点选【取消】取消变更。

图 3-3 变更内部网络地址设定

## 移除内部网络地址

步驟1. 在【内部网络】的表格中，找到欲变更设定的网络名称，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定删除】内部网络地址对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。（如图3-4）



图 3-4 移除内部网络地址设定

## 内部网络群组

### 内部网络群组功能设定

步驟1. 在左方的功能选项中，点选【地址表】功能，再点选【内部网络群组】次功能选项。（如图3-5）



图 3-5 内部网络群组功能设定

步驟2. 内部网络群组工作窗口之表格名词定义：

- 名称：内部网络群组名称。
- 成员：该群组成员。
- 变更：变更内部网络群组中各项设定值。点选【修改】，可修改内部网络群组各项参数信息；点选【删除】，可删除该群组。



在【内部网络群组】工作窗口中，若是某个网络群组已被加入管制条例中，【变更】栏中会出现【使用中】文字，而无法进行修改或删除设定。需先至管制条例删除该项设定，才可进行变更设定。

## 新增内部网络群组

步驟1. 在内部网络群组窗口中，点选【新增】内部网络群组功能按钮。

步驟2. 在出现的新增群组窗口中 (如图3-6)

可选取的地址：显示内部网络所有组员名单。

被选取的地址：显示登录至新群组的组员名单。

- 名称：键入新群组名称。
- 新增组员：由【可选取的地址】选单中，点选欲登录之组员名称，再点选【加入>>】，将该成员加入新群组组员名单中。
- 移除组员：在【被选取的地址】选单中，点选欲移除之组员名称，再点选【<<删除】，将该组员由群组中移除。

步驟3. 点选【确定】执行新增群组；或点选【取消】取消新增。

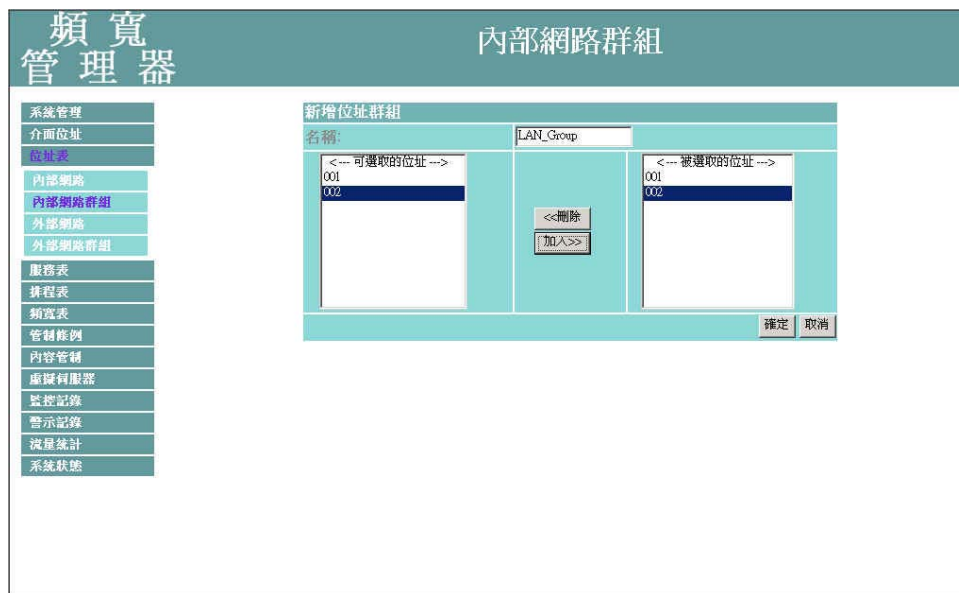


图 3-6 新增内部网络群组

## 变更内部网络群组设定

步驟**1.** 在内部网络群组窗口中，找到欲变更设定的网络群组名称，对应至右方【变更】栏，点选【修改】。

步驟**2.** 在出现的变更群组窗口中 (如图 3-7)

- 名称：键入新群组名称。
- 新增组员：由【可选择的地址】选单中，点选欲登录之组员名称，再点选【加入>>】，将该成员加入新群组组员名单中。
- 移除组员：在【被选择的地址】选单中，点选欲移除之组员名称，再点选【<<删除】，将该组员由群组中移除。

步驟**3.** 点选【确定】执行变更群组；或点选【取消】取消变更。

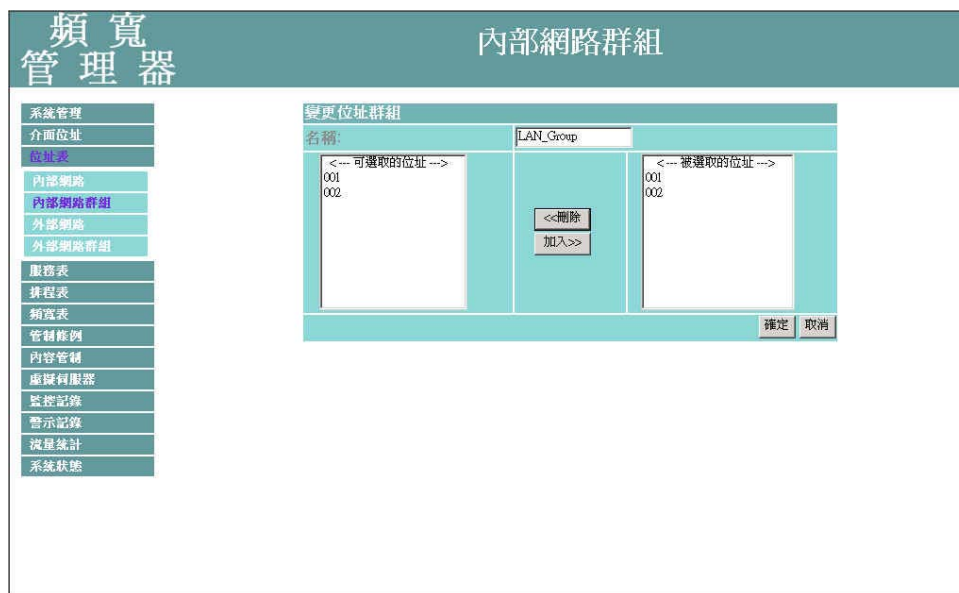


图 3-7 变更网络群组设定

## 移除内部网络群组

- 步驟1. 在【内部网络群组】的表格中，找到欲移除的内部网络群组，对应至右方【变更】栏，点选【删除】。
- 步驟2. 在【确定移除】内部网络群组对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。（如图3-8）



图 3-8 移除内部网络群组

## 外部网络

### 外部网络功能设定

步驟1. 在左方的功能选项中，点选【地址表】功能，再点选【外部网络】次功能选项。（如图3-9）



图 3-9 外部网络设定功能

步驟2. 外部网络工作窗口之表格名词定义：

- 名称：外部网络地址名称。
- IP 地址/子网掩码：连结目的网域之 IP 位址与子网掩码。
- 变更：变更外部网络中各项设定值。点选【修改】，可修改外部网络各项参数；点选【删除】，可删除该项设定。



在外部网络窗口中，若是某个地址表成员已被加入管制条例或网络群组之中，【变更】栏中会出现【使用中】文字，无法进行修改或删除的变更设定。

## 新增外部网络地址

- 步驟1. 點選【新增】外部网络地址功能按钮。
- 步驟2. 在新窗口中，键入外部网络各项参数值。（如图3-10）
- 步驟3. 點選屏幕下方【确定】按钮，新增外部网络地址，或點選【取消】取消设定。



The screenshot displays the 'External Network' configuration page within the 'Bandwidth Manager' interface. The page title is '外部網路' (External Network). On the left, there is a navigation menu with the following items: 系統管理 (System Management), 介面位址 (Interface Address), 位址表 (Address Table), 內部網路 (Internal Network), 內部網路群組 (Internal Network Group), 外部網路 (External Network), 外部網路群組 (External Network Group), 服務表 (Service Table), 排程表 (Schedule Table), 頻寬表 (Bandwidth Table), 管制條例 (Control Policy), 內容管制 (Content Control), 虛擬伺服器 (Virtual Server), 監控記錄 (Monitoring Record), 警示記錄 (Alert Record), 流量統計 (Traffic Statistics), and 系統狀態 (System Status). The main content area is titled '新增位址' (Add Address) and contains a form with the following fields:

新增位址	
名稱 (Name)	006
IP	202.1.237.23
子網路遮罩 (Subnet Mask)	255.255.255.255
<input type="button" value="確定"/> <input type="button" value="取消"/>	

图 3-10 新增外部网络地址



## 变更外部网络地址

- 步驟1. 在【外部网络】的表格中，找到欲变更设定的网络名称，对应至右方【变更】栏，点选【修改】。
- 步驟2. 在新的【变更地址】窗口中，键入各项欲变更的资料。（如图3-11）
- 步驟3. 点选屏幕下方【确定】按钮，变更设定，或点选【取消】取消变更。

變更位址	
名稱	006
IP	202.1.237.23
子網路遮罩	255.255.255.255

图 3-11 变更外部网络地址

## 移除外部网络地址

步驟1. 在【外部网络】的表格中，找到欲变更设定的网络名称，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定移除】外部网络地址对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。（如图3-12）



图 3-12 移除外部网络地址

## 外部网络群组

### 外部网络群组功能设定

步驟1. 在左方的功能选项中，点选【地址表】功能，再点选【外部网络群组】次功能选项。（如图3-13）

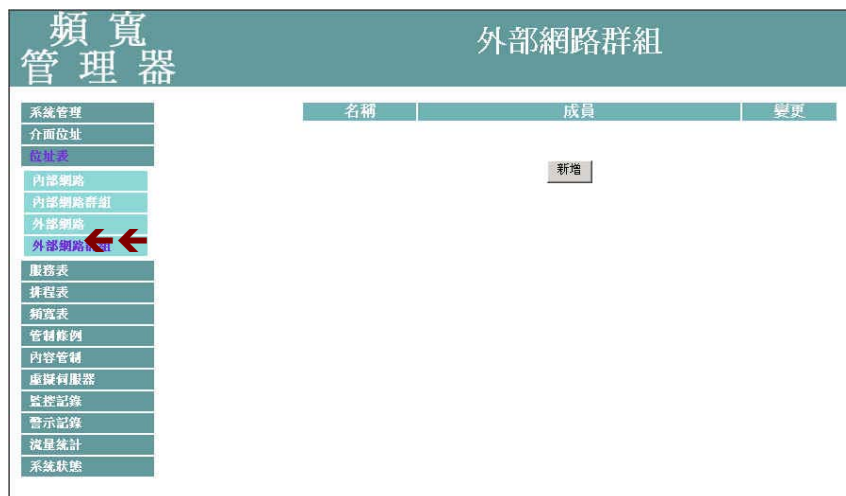


图 3-13 外部网络群组功能设定

步驟2. 外部网络群组工作窗口之表格名词定义：

- 名称：外部网络群组名称。
- 成员：该群组成员。
- 变更：变更外部网络群组中各项设定值。点选【修改】，可修改外部网络群组各项参数；点选【删除】，可删除该群组。



在【外部网络群组】工作窗口中，若是某个网络群组已被加入管制条例中，在【变更】栏会出现【使用中】文字，无法进行修改或删除的变更设定，需先至管制条例移除该向设定，才可进行变更设定。

## 新增外部网络群组

步驟1. 在外部网络群组窗口中，點選【新增】外部网络群组功能按钮。

步驟2. 在出现的新增群组窗口中 (如图3-14)

可选取的地址：显示外部网络所有组员名单。

被选取的地址：显示登录至新群组的组员名单。

- 名称：键入外部网络群组名称。
- 新增组员：由【可选取的地址】选单中，點選欲登录之组员名称，再點選【加入>>】，将该成员加入新群组组员名单中。
- 移除组员：在【被选取的地址】选单中，點選欲移除之组员名称，再點選【<<删除】，将该组员由群组中移除。

步驟3. 點選【确定】执行新增群组；或點選【取消】取消新增。



3-14 新增外部网络群组

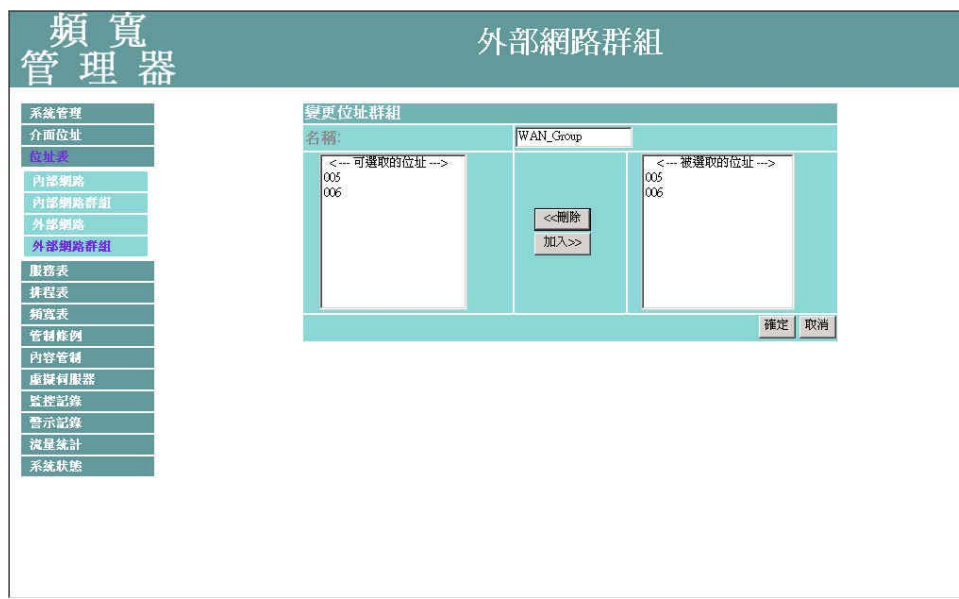
## 变更外部网络群组设定

步驟1. 在外部网络群组窗口中，找到欲变更设定的网络群组名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在出现的变更群组窗口中 (如图 3-15)

- 名称：键入新群组名称。
- 新增组员：由【可选项的地址】选单中，点选欲登录之组员名称，再点选【加入>>】，将该成员加入新群组组员名单中。
- 移除组员：在【被选中的地址】选单中，点选欲移除之组员名称，再点选【<<删除】，将该组员由群组中移除。

步驟3. 点选【确定】执行变更群组；或点选【取消】取消变更。



3-15 变更外部网络群组设定

## 移除外部网络群组

- 步驟1. 在【外部网络群组】的表格中，找到欲移除的外部网络群组，对应至右方【变更】栏，点选【删除】。
- 步驟2. 在【确定移除】外部网络群组对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。（如图3-16）



图 3-16 移除外部网络群组

# 服务表

TCP 协议和 UDP 协议提供各种不同的服务，每一个服务都有一个 TCP 端口 (TCP Port) 号码或 UDP 端口号码代表，如 TELNET(23)，FTP(21)，SMTP(25)，POP3(110)，... 等。本产品的服务包含两个部分：基本服务表和自订服务表，比较常用的 TCP 服务或 UDP 服务已预告定义在基本服务表，此类服务不能修改也不可移除。另外使用者也可依自己的需求到自订服务表设定适当 TCP 端口和 UDP 端口号码。在自订服务时，客户端埠(Client Port)设定的区间预设 1024: 65535，服务器端端口(Server Port)号码则是在 0:65535 之间。

本频宽管理器在此单元中，将一些常用的网络服务列入各项表列的服务选单中（基本服务、自订服务与服务群组）。系统主管理员只需依照下列操作说明，将网络协议与出入端口号码定义在各种网络通讯应用中，客户端即可与各种不同服务器联机，传输资料。



## 如何运用服务表

系统管理员可以在【服务表】的【服务群组】选项中，新增服务群组名称，将要提供的服务包含进去。有了服务群组的功能，管理员在制订管制条例时可以简化许多流程。例如，有 10 个不同 IP 地址可以对服务器存取 5 种不同的服务，如 HTTP、FTP、SMTP、POP3 和 TELNET，如果不使用服务群组的功能，总共需制定  $10 \times 5 = 50$  条管制条例，但使用服务群组名称套用在服务选项上，则只需一条管制条例即可达到 50 条管制条例的功能。

## 基本服务

### 服务表之【基本服务】功能

步骤1. 在左方的功能选项中，点选【服务表】功能，再点选【基本服务】次功能选项。（如图4-1）



图 4-1 基本服务表

步骤2. 基本服务表窗口表格内图标与名词名称定义：

图标	说明
	TCP 服务，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 服务，如：IKE、DNS、NTP、IRC、RIP、SNMP、SYSLOG、TALK、TFTP、UDP-ANY、UUCP 等。
	ICMP 服务，如：PING、TRACEROUTE 等。



## 自订服务

### 自订服务功能设定

步驟1. 在左方的功能选项中，点选【服务表】功能，再点选【自订服务】次功能选项。(如图4-2)



图 4-2 自订服务功能设定

步驟2. 内部网络工作窗口之表格名词定义：

- 服务名称：自订服务项目名称。
- 通讯协议：【基本设定】中所使用的网络协议。如 TCP、UDP，或其它（请选择代码）。
- 客户端：自定服务项目中之客户端的出入埠范围。  
在客户端两个空格内输入的 port 号如为不同埠号，则是开启埠号为两个空格内输入 port 号的中间范围。  
在客户端两个空格内输入的 port 号如为相同埠号，则是开启埠号为同一个 port 号

- 服务器端：自定服务项目中之服务器端的出入埠范围。  
在服务器端两个空格内输入的 port 号如为不同埠号，则是开启埠号为两个空格内输入 port 号的中间范围。  
在服务器端两个空格内输入的 port 号如为相同埠号，则是开启埠号为同一个 port 号
- 变更：变更服务表中各项设定值。点选【修改】，可修改服务表各项参数；点选【删除】，可删除该项设定。



在自订服务工作窗口中，若是某个服务已被加入管制条例或服务群组之中。【变更】栏会出现【使用中】，而无法进行修改或删除的变更设定，需先至管制条例或服务群组中，移除该项设定，才可执行变更。

## 新增自订服务

步驟1. 在【自订服务】表格中，点选【新增服务】功能按钮。

步驟2. 在出现的新增服务窗口中 (如图4-3)

- 服务名称：输入新服务名称。
- 通讯协议：勾选【基本设定】中所使用的网络协议。如 TCP、UDP，或其它（请选择代码）。
- 客户端： 输入新服务之客户端的出入埠范围。  
在客户端两个空格内输入的 port 号如为不同埠号，则是开启埠号为两个空格内输入 port 号的中间范围。  
在客户端两个空格内输入的 port 号如为相同埠号，则是开启埠号为同一个 port 号
- 服务器端：输入新服务之服务器端的出入埠范围。  
在服务器端两个空格内输入的 port 号如为不同埠号，则是开启埠号为两个空格内输入 port 号的中间范围。  
在服务器端两个空格内输入的 port 号如为相同埠号，则是开启埠号为同一个 port 号

步驟3. 點選【確定】執行新增服務；或點選【取消】取消新增。

頻寬  
管理器
自訂服務

- 系統管理
- 介面位址
- 位址表
- 服務表
- 基本服務
- 自訂服務
- 服務群組
- 排程表
- 頻寬表
- 管制條例
- 內容管制
- 虛擬伺服器
- 警告記錄
- 流量統計
- 系統狀態

新增自訂服務

服務名稱：

#	通訊協定	用戶端	伺服器端
1	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	4661 : 4665
2	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
3	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
4	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
5	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
6	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
7	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0
8	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> Other	1024 : 65535	0 : 0

图 4-3 新增自订服务

73

## 变更自订服务

**步骤1.** 在【自订服务】窗口中，找到欲变更设定的服务名称，对应至右方【变更】栏，点选【修改】。

**步骤2.** 在出现的变更群组窗口中 (如图 4-4)

- 服务名称：输入新服务名称。
- 通讯协议：勾选【基本设定】中所使用的网络协议。如 TCP、UDP，或其它（请选择代码）。
- 客户端： 输入新服务之客户端的出入埠范围。
  - 在客户端两个空格内输入的 port 号如为不同埠号，则是开启埠号为两个空格内输入 port 号的中间范围。
  - 在客户端两个空格内输入的 port 号如为相同埠号，则是开启埠号为同一个 port 号
- 服务器端： 输入新服务之服务器端的出入埠范围。
  - 在服务器端两个空格内输入的 port 号如为不同埠号，则是开启埠号为两个空格内输入 port 号的中间范围。
  - 在服务器端两个空格内输入的 port 号如为相同埠号，则是开启埠号为同一个 port 号

步驟3. 點選【確定】執行變更服務；或點選【取消】取消變更。



图 4-4 变更自订服务

## 移除自订服务

- 步驟1. 在【自订服务】窗口表格中，找到欲变更设定的服务名称，对应至右方【变更】栏，点选【删除】。
- 步驟2. 在【删除服务】确定对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。(如图4-5)

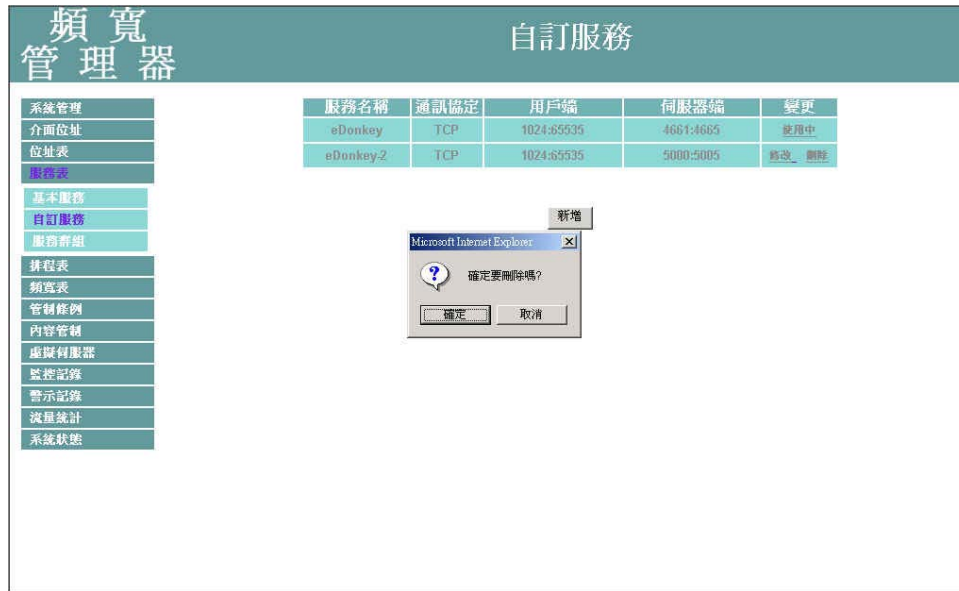


图 4-5 移除自订服务

## 服务群组

### 服务群组功能设定

步驟1. 在左方的功能选项中，点选【服务表】功能，再点选【服务群组】次功能选项。(如图4-6)



图 4-6 服务群组功能设定

步驟2. 服务群组工作窗口之表格名词定义：

- 群组名称：所有已设定之服务群组名称。
- 服务名称：该服务群组服务项目。
- 变更：变更服务群组中各项设定值。点选【修改】，可修改服务群组各项参数；点选【删除】，可删除该群组。



在【服务群组】工作窗口中，若是某个服务群组已被加入管制条例中，则在【变更】栏会出现【使用中】，而无法进行修改或移除的变更设定，需先至管制条例中，移除该项设定，才可执行变更。



## 新增服务群组

步驟1. 在服务群组窗口中，点选【新增服务群组】功能按钮。

步驟2. 在出现的服务群组窗口中 (如图4-7)

可选取的服务：显示所有有效的服务项目。

被选取的服务：显示针对新增服务群组所选择的服务项目。

- 名称：键入新服务群组名称。
- 新增服务项目：在【可选取的服务】选单中，点选欲增加的服务项目名称，再点选【加入>>】，将该服务项目加入新群组。
- 移除服务项目：在【被选取的服务】字段中，点选欲移除之服务项目名称，再点选【<<删除】，将该服务项目自群组中移除。

步驟3. 点选【确定】执行新增群组；或点选【取消】取消新增。



图 4-7 新增服务群组

## 变更服务群组

步驟**1.** 在内部网络群组窗口中，找到欲变更设定的网络群组名称，对应至右方【变更】栏，点选【修改】。

步驟**2.** 在出现的变更群组窗口中（如图4-8）

- 名称：键入新群组名称。
- 新增组员：由【可选取的服务】选单中，点选欲登录之组员名称，再点选【加入>>】，将该成员加入新群组组员名单中。
- 移除组员：在【被选取的服务】选单中，点选欲移除之组员名称，再点选【<<删除】，将该组员由群组中移除。

步驟**3.** 点选【确定】执行变更群组；或点选【取消】取消变更。



图 4-8 变更服务群组

## 删除服务群组

- 步驟1. 在【服务群组】的表格中，找到欲移除的服务群组，对应至右方【变更】栏，点选【删除】。
- 步驟2. 在【确定删除】服务群组确认对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。(如图4-9)



图 4-9 移除服务群组

# 排 程 表

本频宽管理器在此单元中提供系统主管理员，在排程表中定义网络系统连结与执行的时间区段，以便在【管制条例】或【网站管制】功能中，选择特定时间内开放资料封包的出入或限制网站浏览。利用排程表的自动执行功能，系统管理员可以节省许多时间，同时让网络系统发挥最大的效能。



## 如何运用排程表

系统管理员可利用排程表功能，设定系统在多个不同的时间区段内，自动执行设定封包流向的【管制条例】或限制网站浏览的【网站管制】功能。

## 排程表功能设定

步驟1. 在左方的功能选项中，点选【排程表】功能。(如图5-1)



图 5-1 排程表功能设定

步驟2. 排程表工作窗口之表格名词定义：

- 排程名称：管理者所定义之排程表名称。
- 变更：变更排程表中各项设定值。点选【修改】，可修改排程表各项参数；点选【删除】，可删除该项设定。



在排程表工作窗口中，若是某个排程已被加入【管制条例】或【网站管制】之中。【变更】栏会出现【使用中】，而无法进行修改或删除的变更设定，需先至【管制条例】或【网站管制】中，移除该项设定，才可执行变更。。

## 新增排程表

步驟1. 點選【新增】功能按鈕。

步驟2. 在出現的【新增排程表】窗口中 (如圖 5-2)

- 排程名稱：輸入新排程名稱。
- 時段：在每周特定日期的表格內，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3. 點選【確定】執行新增排程表；或點選【取消】取消新增。

星期	時段	
	起始時間	結束時間
星期一	All day	All day
星期二	08:00	20:00
星期三	All day	All day
星期四	08:00	19:00
星期五	All day	All day
星期六	Disable	Disable
星期日	Disable	Disable

圖 5-2 新增排程表



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

## 變更排程表

- 步驟**1.** 在【排程表】窗口中，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**2.** 在出現的變更群組窗口中，鍵入新排程表名稱，並設定排程表時間範圍（[如圖 5-3](#)）
- 步驟**3.** 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【排程表】窗口表格中，找到欲变更设定的排程表名称，对应至右方【变更】栏，点选【删除】。
- 步驟2. 在【删除排程表】确定对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。(如图 5-4)



图 5-4 移除排程表



# 频 宽 表

频宽管理器经由频宽表的参数设定，可以控管内部网络对外部网络的上传下载频宽。

管理人员可依据外部网络所能使用的频宽，来做设定

**下载频宽：** 设定 保证频宽 及 最大频宽

**上传频宽：** 设定 保证频宽 及 最大频宽

**优先权：** 设定 上传 或 下载 未设定使用的频宽分配优先权

本频宽管理器依据不同频宽表，来设定对外的频宽，并藉由管制条例选择适合的频宽表设定加以控管，可有效分配频宽，且便利系统主管理员，针对所能使用的频宽达到最佳的使用。

## 频宽表功能设定

步驟1. 在左方的功能选项中，点选【频宽表】功能选项。（如图6-1）



图 6-1 频宽表功能

步驟2. 频宽表表格说明

- 名称：所设定之频宽表名称。
- 下载频宽：所设定的**下载频宽**内 保证频宽 及 最大频宽。
- 上传频宽：所设定的**上传频宽**内 保证频宽 及 最大频宽。
- 优先权：设定 上传 或 下载 未使用的频宽分配优先权。
- 变更：变更内部网络中各项设定值。点选【修改】，可修改内部网络各项参数信息；点选【删除】，可删除该项设定。

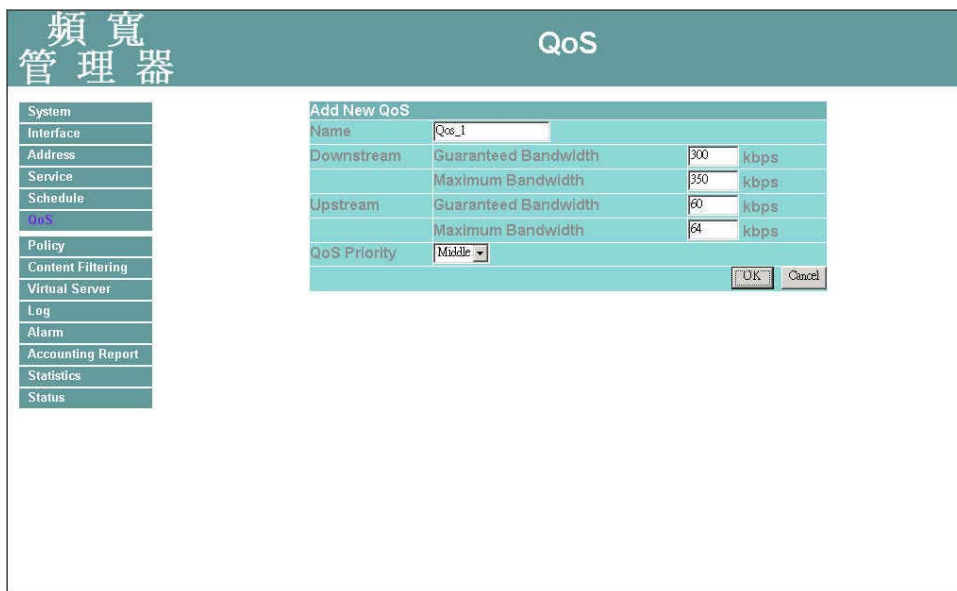
## 新增频宽表功能

步驟1. 點選屏幕下方【新增】按鈕，新增指定的频宽表。

步驟2. 频宽表表格说明

- 名称：所设定之频宽表名称。
- 下载频宽：所设定的**下载频宽**内 保证频宽 及 最大频宽。
- 上传频宽：所设定的**上传频宽**内 保证频宽 及 最大频宽。
- 优先权：设定 上传 或 下载 未使用的频宽分配优先权。

步驟3. 點選屏幕右方【确定】按钮，新增指定的频宽表。 (如图6-2)



The screenshot shows a web-based interface for QoS management. On the left is a navigation menu with items: System, Interface, Address, Service, Schedule, QoS, Policy, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, and Status. The main area is titled 'QoS' and contains a 'Add New QoS' dialog box. The dialog box has the following fields and values:

Add New QoS	
Name	Qos_1
Downstream	Guaranteed Bandwidth: 300 kbps
	Maximum Bandwidth: 350 kbps
Upstream	Guaranteed Bandwidth: 60 kbps
	Maximum Bandwidth: 64 kbps
QoS Priority	Middle
[OK] [Cancel]	

图 6-2 新增频宽表功能

## 修改频宽表功能

步驟1. 點選屏幕右方【變更】按鈕，變更指定的频宽表。

步驟2. 频宽表表格说明

- 名称：所设定之频宽表名称。
- 下载频宽：所设定的**下载频宽**内 保证频宽 及 最大频宽。
- 上传频宽：所设定的**上传频宽**内 保证频宽 及 最大频宽。
- 优先权：设定 上传 或 下载 未使用的频宽分配优先权。

步驟3. 點選屏幕右方【确定】按钮，變更指定的频宽表。 (如图6-3)

The screenshot displays the 'Bandwidth Management' interface with a 'QoS' sub-section. A 'Modify QoS' dialog box is open, showing the following configuration:

Downstream	
Guaranteed Bandwidth	300 kbps
Maximum Bandwidth	350 kbps

Upstream	
Guaranteed Bandwidth	60 kbps
Maximum Bandwidth	64 kbps

QoS Priority: Middle

Buttons: OK, Cancel

Left sidebar menu items: System, Interface, Address, Service, Schedule, QoS (highlighted), Policy, Content Filtering, Virtual Server, Log, Alarm, Accounting Report, Statistics, Status.

图 6-3 修改频宽表功能

## 移除频宽表功能设定

- 步驟**1.** 在【频宽表】窗口中，找到欲变更设定的网络区域名称，对映至右方【设定】栏，点选【移除】。
- 步驟**2.** 在【移除频宽表】确定对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。（如图6-4）



图 6-4 移除频宽表功能设定

# 管制条例

频宽管理器经由管制条例的参数设定，可以控管资料封包的过滤规则。管制条例的参数包含有来源地址、目的地址、服务、管制动作、流量监控、流量统计、及自动排程流量警示等。系统管理员可以由这些参数，管理、设定不同出入口间的资料传送以及服务项目，哪些网络对象、网络服务或应用程序的封包该予以拦截或放行。

本频宽管理器依据不同来源地址的资料封包，将管制条例设定功能区分为下列六项，以便利系统管理员，针对不同资料封包的来源 IP、来源埠、目的 IP、目的端口制订管制规则。

- (一) **【内部至外部】**：来源网络地址是在内部网络区，目的网络地址是在外部网络区。系统管理员在此功能中，订定内部网络至外部网络间所有封包的管制、服务项目的管制规则。
- (二) **【外部至内部】**：来源网络地址是在外部网络区，目的网络地址是在内部网络区。系统管理员在此功能中，订定外部网络至内部网络间所有封包的管制、服务项目的管制规则。



## 如何运用管制条例

管制条例所需设定的参数包含有：来源网络、目的网络、服务项目、管制动作、流量监控、流量统计、自动排程、流量警示值和频宽管理。其中，来源网络和目的网络和IP 地址对映的名称必需先在【地址表】定义。而服务项目，若属于【基本服务】项目中，则可直接使用，如果是属于自订服务，则必须先在【服务表】中的【自订服务】定义其服务项目名称和其对映的埠号(Port Number)。

在制定【至内部网络】条例时，它的目的地址为 1 对 1 对映的 IP 地址或是虚拟服务器 IP 地址，此部分需在【虚拟服务器】项目中定义，而非在【地址表】制定。



### 管制条例操作指引

- 步驟1. 至【地址表】中，定义来源网络与目的网络的名称、地址。
- 步驟2. 至【服务表】中，定义服务项目。
- 步驟3. 至【虚拟服务器】中，定义对映 IP 或虚拟服务器名称地址。（此步骤仅于定义【至内部网络】需操作。）
- 步驟4. 于本单元【管制条例】设定各项参数。

## 内部至外部

### 内部至外部管制条例功能设定

来源网络地址是在内部网络区，目的网络地址是在外部网络区。系统管理员在此功能中，订定内部网络至外部网络间所有封包的管制、服务项目的管制规则。

**步骤1.** 在左方的功能选项中，点选【管制条例】功能，再点选【内部至外部】次功能选项。（如图 7-1）



图 7-1 内部网络至外部网络功能设定

**步骤2.** 管制条例表格说明（由内部网络至外部网络）：








- 编号：所设定之管制条例编号，此处编号由 1 开始。
- 来源网络：已于【地址表】之【内部网络】功能中所指定的内部网络地址，或所有内部网络地址。
- 目的网络：已于【地址表】之【外部网络】功能中所指定的外部网络地址，或所有外部网络地址。
- 服务名称：指定外部网络服务器提供的服务项目。
- 管制动作：指定内、外部网络进出频宽管理器资料封包的准许与拒



绝动作。

- **监控功能：**指定内、外部网络进出频宽管理器资料封包的各种监控功能。第一栏为流量监控功能，第二栏为流量统计功能，第三栏为排程表功能，第四栏为流量警示功能，第五栏为频宽管理功能。当该栏出现图标即表示该项监控功能已激活，反之，若未有任何图标，则监控功能未开启。（图标说明如下方表格。）
- **变更：**变更内部网络中各项设定值。点选【修改】，可修改内部网络各项参数信息；点选【删除】，可删除该项设定。
- **移动：**该项管制条例之编号排列次序。由下拉选单中点选编号，可移动该项管制条例次序。

### 管制条例图标说明：

图 示	名 称	说 明
	准许	准许指定的所有内部到外部网络资料封包进出。
	拒绝	拒绝指定的所有内部到外部网络资料封包进出。
	监控	流量、事件监控功能已开启。
	统计	流量统计功能已开启。
	排程	已激活排程表所制订时间范围内自动执行功能。
	警示	流量、事件警示功能已开启。
	频宽	频宽管理功能已开启。
<b>备注：</b> <ol style="list-style-type: none"> <li>1. 检视系统之流量、事件监控纪录，点选屏幕左方【监控功能】选项，系统使用与操作方式，请翻阅第十章。</li> <li>2. 检视系统之警示记录，点选屏幕左方【警示记录】选项，系统使用与操作方式，请翻阅第十一章。</li> <li>3. 检视系统之流量统计纪录，点选屏幕左方【流量统计】选项，使用与操作方式，请翻阅第十二章。</li> <li>4. 频宽管理器自动执行时间范围之排程，修改排程时间，点选屏幕左方【排程表】选项，使用与操作方式，请翻阅第五章。</li> <li>5. 频宽管理器自动执行频宽管理，修改频宽管理，点选屏幕左方【频宽表】选项，使用与操作方式，请翻阅第六章。</li> </ol>		

## 新增内部至外部管制条例

步驟1. 在【内部至外部】窗口中，点选【新增管制条例】功能按钮。

步驟2. 在出现的【新增管制条例】窗口中，键入下列相关参数（如图7-2）

頻寬管理器		內部至外部	
系統管理	新增管制條例	來源網路位址	Inside_Any
介面位址		目的網路位址	Outside_Any
位址表		服務名稱	ANY
服務表		管制動作	允許
排程表		流量監控	<input type="checkbox"/> 開啓
頻寬表		流量統計	<input type="checkbox"/> 開啓
管制條例		自動排程	None
內部至外部		最高流量警示值	0.0 KBytes/Sec
外部至內部		頻寬管理	None
內容管制			確定 取消
虛擬伺服器			
監控記錄			
警告記錄			
流量統計			
系統狀態			

图 7-2 新增内部网络至外部网络管制条例

- 来源网络地址：由下拉选单中点选内部网络名称。  
此部分下拉选单所显示的内部网络名称为：【地址表】之【内部网络】所设定的内部网络地址。若要新增选项需至【地址表】之【内部网络】功能窗口中设定，此处无法新增。
- 目的网络地址：由下拉选单中点选外部网络名称。  
此部分下拉选单所显示的外部网络名称为：【地址表】之【外部网络】所设定的内部网络地址。若要新增选项需至【地址表】之【外部网络】功能窗口中设定，此处无法新增。
- 服务名称：由下拉选单中点选服务功能。此部分下拉选单所显示的服务功能项目为：（一）【服务表】中的【基本服务】功能，如：ANY、AOL、AUTH.....等多项服务可供选择；（二）系统管理员已于【服务表】之【自订服务】或【服务群组】所定义之服务功能项目。

- 管制动作：由下拉选单中点选指定的内、外部网络资料封包进出的准许或拒绝。可选择【允许】；或【拒绝】。
- 流量监控：勾选【激活】，开启流量监控记录功能。
- 流量统计：勾选【激活】，开启流量统计功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 最高流量警示值：设定进出资料封包之最高流量（KBytes/Sec）警示值。此警示记录将记录于【警示记录】之【流量警示】中。
- 频宽管理：设定频宽管理功能是否在此项管制条例有效执行的功能。

**步骤3.** 点选屏幕下方【确定】按钮，新增指定的内部网络，或点选【取消】取消设定。



若要变更本单元【内部至外部】表格内管制条例次序，可于表格右方【移动】栏，下拉选单中点选编号，即可移动该项管制条例。

## 变更内部至外部管制条例

步驟1. 在【内部至外部】窗口中，找到欲变更设定的网络区域名称，对映至右方【变更】栏，点选【修改】。

步驟2. 在出现的【变更管制条例】窗口中，键入下列相关参数 (如图 7-3)

頻寬管理	
系統管理	變更管制條例
介面位址	來源網路位址: Inside_Any
位址表	目的網路位址: Outside_Any
服務表	服務名稱: ANY
排程表	管制動作: 允許
頻寬表	流量監控: <input checked="" type="checkbox"/> 開啓
管制條例	流量統計: <input checked="" type="checkbox"/> 開啓
內部至外部	自動排程: True
外部至內部	最高流量警示值: 0.0 KBytes/Sec
內容管制	頻寬管理: 512
虛擬伺服器	確定 取消
監控記錄	
警示記錄	
流量統計	
系統狀態	

图 7-3 变更内部网络至外部网络管制条例

- 来源网络地址：由下拉选单中点选内部网络名称。  
此部分下拉选单所显示的内部网络名称为：【地址表】之【内部网络】所设定的内部网络地址。
- 目的网络地址：由下拉选单中点选外部网络名称。  
此部分下拉选单所显示的外部网络名称为：【地址表】之【外部网络】所设定的外部网络地址。
- 服务名称：由下拉选单中点选新服务项目。
- 管制动作：由下拉选单中点选指定的内、外部网络资料封包进出的准许或拒绝。
- 流量监控：勾选【激活】，开启流量监控功能。

- 流量统计：勾选【激活】，开启流量统计功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 警示功能：设定进出资料封包之最高流量（KBytes/Sec）警示值。
- 频宽管理：设定频宽管理功能是否在此项管制条例有效执行的功能。

步驟3. 点选屏幕下方【确定】按钮，变更指定的至外部网络管制条例，或点选【取消】取消变更。



若要变更或新增下拉选单的选项，需至各选项的原始设定单元重新设定。

- 来源网络→【地址表】之【内部网络】；
- 目的网络→【地址表】之【外部网络】；
- 服务表内的服务名称→【服务表】之【基本服务】、【自订服务】或【服务群组】。

## 移除内部至外部管制条例

- 步驟**1.** 在【内部至外部】窗口中，找到欲变更设定的网络区域名称，对映至右方【设定】栏，点选【删除】。
- 步驟**2.** 在【移除管制条例】确定对话框中，点选【确定】按钮移除设定，或点选【取消】取消移除。（如图 7-4）



图 7-4 移除内部网络至外部网络管制条例

## 外部至内部管制条例功能设定

在设定外部至内部管制条例时，必须在【虚拟服务器】中，先设定好各项参数。虚拟服务器设定请参考第八章。

来源网络地址是在外部网络区，目的网络地址是在内部网络区。系统管理员在此功能中，订定外部网络至内部网络间所有封包的管制、服务项目的管制规则。

步骤1. 在左方的功能选项中，点选【管制条例】功能，再点选【外部至内部】次功能选项。（如图7-5）









图 7-5 外部网络至内部网络管制条例功能设定

步骤2. 管制条例表格说明（由外部网络至内部网络）：

- 编号：所设定之管制条例编号，此处编号由 1 开始。
- 来源网络地址：已于【地址表】之【外部网络】功能中所指定的外部网络地址，或所有外部网络地址。
- 目的网络地址：已于【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】功能中所指定的 IP 对映网络地址，或虚拟服务器网络地址。






- 服务名称：虚拟服务器（或 IP 对映）提供的服务项目。
- 管制作：指定外部网络 1/2、虚拟服务器（或 IP 对映）进出频宽管理器资料封包的准许与拒绝动作。
- 监控功能：指定外部网络 1/2、虚拟服务器（或 IP 对映）进出频宽管理器资料封包的各种监控功能。第一栏为流量监控功能，第二栏为流量统计功能，第三栏为排程表功能，第四栏为流量警示功能，第五栏为频宽管理功能。当该栏出现图标即表示该项监控功能已激活，反之，若未有任何图标，则监控功能未开启。（图标说明如下方表格。）
- 频宽管理：设定频宽管理功能是否在此项管制条例有效执行的功能。
- 变更：变更至内部网络中各项管制条例设定值。点选【修改】，可修改各项相关参数值；点选【删除】，可删除该项设定。
- 移动：该项管制条例之编号排列次序。由下拉选单中点选编号，可移动该项管制条例次序。

#### 管制条例图标说明：

图 示	名 称	说 明
	准许	准许指定的所有外部到内部网络资料封包进出。
	拒绝	拒绝指定的所有外部到内部网络资料封包进出。
	监控	流量、事件监控功能已开启。
	统计	流量统计功能已开启。
	排程	已激活排程表所制订时间范围内自动执行功能。
	警示	流量、事件警示功能已开启。
	频宽	频宽管理功能已开启。



**备注:**

1. 检视系统之流量、事件监控纪录，点选屏幕左方【监控功能】选项，系统使用与操作方式，请翻阅第十章。
2. 检视系统之警示记录，点选屏幕左方【警示记录】选项，系统使用与操作方式，请翻阅第十一章。
3. 检视系统之流量统计纪录，点选屏幕左方【流量统计】选项，使用与操作方式，请翻阅第十二章。
4. 频宽管理器自动执行时间范围之排程，修改排程时间，点选屏幕左方【排程表】选项，使用与操作方式，请翻阅第五章。
5. 频宽管理器自动执行频宽管理，修改频宽管理，点选屏幕左方【频宽表】选项，使用与操作方式，请翻阅第六章。

## 外部至内部

### 新增外部至内部管制条例

步驟1. 在【外部至内部】窗口中，点选【新增管制条例】功能按钮。

步驟2. 在出现的【新增管制条例】窗口中，键入下列相关参数（如图7-6）

頻寬管理器		外部至内部	
系統管理	新增管制條例	來源網路位址	Outside_Any
介面位址		目的網路位址	Virtual Server 1 (61.59.229.249)
位址表		服務名稱	eDonkey
服務表		管制動作	允許
排程表		流量監控	<input checked="" type="checkbox"/> 開啓
頻寬表		流量統計	<input checked="" type="checkbox"/> 開啓
管制條例		自動排程	None
內部至外部		最高流量警示值	0.0 KBytes/Sec
外部至内部		頻寬管理	None
內容管制			
虛擬伺服器			
監控記錄			
警告記錄			
流量統計			
系統狀態			

图 7-6 新增外部网络至内部网络管制条例

- 来源网络地址：由下拉选单中点选外部网络名称。  
此部分下拉选单所显示的外部网络名称为：已在【地址表】之【外部网络】所设定的外部网络地址。若要新增需至【地址表】之【外部网络】功能窗口中设定，此处无法新增。
- 目的网络地址：由下拉选单中点选内部网络名称。  
此部分下拉选单所显示的内部网络名称为：已在【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】，所设定的 IP 对映网络地址，或虚拟服务器网络地址。若要新增选单内的选项需至【虚拟服务器】功能窗口中设定（新增方法请详见第七章虚拟服务器），此处无法新增。

- 服务名称：由下拉选单中点选服务项目。  
此部分下拉选单所显示的服务项目为：系统管理员已在【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】，所定义之该 IP 对映，或该虚拟服务器的服务项目。若要新增或修改选单内的服务项目选项，需至【虚拟服务器】工作窗口中设定（新增方法请详见第七章虚拟服务器），此处无法修改。
- 管制动作：由下拉选单中点选指定的外部网络 1/2、虚拟服务器（或 IP 对映）资料封包进出的准许或拒绝。可选择【准许】；或【拒绝】。
- 流量监控：勾选【激活】，开启流量监控功能。
- 流量统计：勾选【激活】，开启流量统计功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围内自动有效执行的功能。
- 流量警示：设定进出资料封包之最高流量（KBytes/Sec）警示值。
- 频宽管理：设定频宽管理功能是否在此项管制条例有效执行的功能。

步骤3. 点选【确定】执行新增群组；或点选【取消】取消新增。



若要变更本单元【外部至内部】表格内管制条例次序，可于表格右方【次序】栏，下拉选单中点选编号，即可移动该项管制条例。

## 变更外部至内部管制条例

步驟1. 在【外部至内部】窗口中，找到欲变更设定的网络区域名称，对映至右方【设定】栏，点选【变更】。

步驟2. 在出现的【变更管制条例】窗口中，键入各项欲变更之参数值 (如图 7-7)

變更管制條例	
來源網路位址	Outside_Any
目的網路位址	Virtual Server 1 (61.59.229.249)
服務名稱	eDonkey
管制動作	拒絕
流量監控	<input checked="" type="checkbox"/> 開啓
流量統計	<input checked="" type="checkbox"/> 開啓
自動排程	True
最高流量警示值	0.1 KBytes/Sec
頻寬管理	512

图 7-7 变更外部网络至内部网络管制条例

- 来源网络：由下拉选单中点选已在【地址表】之【外部网络】所设定的外部网络地址名称。
- 目的网络：由下拉选单中点选已在【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】，所设定的 IP 对映网络地址，或虚拟服务器网络地址名称。
- 服务名称：由下拉选单中点选已在【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】，所定义之该 IP 对映，或该虚拟服务器的服务项目。
- 管制动作：由下拉选单中点选指定的外部网络、虚拟服务器（或 IP 对映）资料封包进出的准许或拒绝。

- 流量监控：勾选【激活】，开启流量监控功能。
- 流量统计：勾选【激活】，开启流量统计功能。
- 自动排程：在下拉选单中，点选已于【排程表】设定之排程表名称，可开启此项管制条例在特定时间范围自动有效执行的功能。
- 流量警示：设定进出资料封包之最高流量（KBytes/Sec）警示值。
- 频宽管理：设定频宽管理功能是否在此项管制条例有效执行的功能。

步驟3. 点选【确定】执行变更管制条例；或点选【取消】取消变更。



若要变更或新增下拉选单的选项，需至各选项的原始设定单元重新设定。

- 来源网络→【地址表】之【外部网络】；
- 目的网络→【地址表】之【内部网络】；
- 服务项目→【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】提供的服务项目。

## 移除外部至内部管制条例

- 步驟1. 在【外部至内部】窗口中，找到欲变更设定的网络区域名称，对映至右方【设定】栏，点选【移除】。
- 步驟2. 在【移除管制条例】确定对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。（如图 7-8）



图 7-8 移除外部网络至内部网络管制条例

# 内容管制

内容管制分为「网站管制」与「Script 管制」两种。

(一) **【网站管制】**: 系统管理员可使用完整网域名称、关键词、万用字符（“~”及“\*”）针对特定网站作「开放」或「限制」进入的制订。

(二) **【Script 管制】**: 管制 Popup、ActiveX、Java、Cookie「开放」或「限制」进入。



## 如何运用内容管制

系统管理员可使用完整网域名称、关键词、万用字符（“~”及“\*”）针对特定网站作「开放」或「限制」进入的制订。

## 网站管制

### 网站管制功能设定

设定管制的网站，系统管理员可使用完整网域名称、关键词、万用字符（“~”及“\*”）针对特定网站作「开放」或「限制」进入的制订。

步驟1. 于左方功能选项，先点选【系统组态】，接着点选下方的【网站管制】，进入【网站管制】工作窗口。（如图8-1）



图 8-1 进入网站管制功能设定

步驟2. 网站管制工作窗口名词定义：

- 网站名称：受到频宽管理器管制进入或仅开放进入的网域名称。
- 排程表：可利用排程表来管制何时禁止或开放。
- 变更：变更网站管制中各项设定值。点选【修改】，可修改网站管制各项参数；点选【删除】，可删除该项设定。



### 步驟3. 网站管制使用方法：

符号说明：“~”表示开放；“\*”表示万用字符。

限制无法进入特定网站：在新增网站管制功能的网站名称中，键入欲禁止网站的「完整网域名称」、或「关键词」。如：www.yahoo.com 或 yahoo。

仅开放特定网站可进入：

1. 先将欲开放网站一一加入网站管制中，新增时，必须于「完整网域名称」、或「关键词」前加入表示开放进入的符号“~”。（如：~www.yahoo.com 或~yahoo）。
2. 在所有欲开放的网站设定完成后，于最后一条欲开放的网站管制后，新增一条全部禁止的指令，亦即在网站名称中，仅键入“\*”。*注意！*此全部禁止的指令必须永远放置于最后。（如下图）
3. 若欲新增开放网站，必须先全部禁止指令移除，再键入新网域名称，完成后，再重新加入全部禁止指令。

網站管制		
網站名稱	排程表	變更
~www.yahoo.com	None	修改 刪除
~www.kimo.com	None	修改 刪除
~www.nine.net	None	修改 刪除
*	None	修改 刪除

开放 →

↑ 万用字符

新增

## 新增网站管制

- 步驟1. 點選下方【新增】网站管制功能按钮。
- 步驟2. 在新窗口网站名称空栏中，键入欲管制进入的网址或关键词。（如图8-2）
- 步驟3. 在排程表下拉选单中，點選欲指定的排程表。
- 步驟4. 點選【确定】新增网站管制，或【取消】取消新增。



图 8-2 新增网站管制

## 变更网站管制

步驟1. 在【网站管制】的表格中，找到欲变更设定的网站名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在【修改网站管制】窗口中，键入新网站的网址，或点选新排程表。（如图8-3）

步驟3. 点选屏幕下方【确定】按钮，变更设定，或点选【取消】取消变更。



图 8-3 变更网站管制

## 移除网站管制

- 步驟1. 在【网站管制】的表格中，找到欲删除设定的网站名称，对应至右方【变更】栏，点选【删除】。
- 步驟2. 在【确定删除】网站管制对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。（如图 8-4）



图 8-4 移除网站管制

## 一般管制

### 一般管制功能设定

管制 Popup、ActiveX、Java、Cookie「开放」或「限制」进入。

步驟1. 【一般管制】各项侦测功能说明 (如图8-5)



图 8-5 设定频宽管理器一般管制功能

- Popup 管制：可阻挡自动弹跳出的窗口。
- ActiveX 管制：可阻挡 ActiveX 封包。
- Java 管制：可阻挡 Java 封包。
- Cookie 管制：可阻挡 Cookie 封包。

勾选各项侦测功能后，点选屏幕右下方【确定】按钮。



完成此部分设定后，当系统侦测到管制现象时，频宽管理器将会自动阻挡。

# 虚拟伺服器

频宽管理器将企业内部网络与网际网络( Internet ) 分隔成内部网络与外部网络, 因IP地址已不够分配, 企业内的内部网络为了有足够的IP地址分配给每一台计算机, 大都是将计算机设定成私有IP地址 ( Private IP Address ), 透过频宽管理器的NAT ( Network Address Translation ) 功能, 转换成真实IP地址( Real IP Address ), 如果对外提供服务的服务器是置于内部网络时, 它的私有IP地址将无法让外部的使用者直接联机使用。

对于此类问题, 可使用本频宽管理器的虚拟服务器功能得以解决, 所谓虚拟服务器是将频宽管理器外部接口子网络的一个真实IP地址设成虚拟服务器IP地址, 藉由频宽管理器IP转换的功能, 将外部使用者寻求服务的联机, 由虚拟服务器IP地址转换成内部网络实际提供服务服务器的私有IP地址。

虚拟服务器还拥有一项特色, 一对多的对映功能, 即一个外部接口的虚拟服务器 IP 地址可对映到多部提供相同服务的内部网络服务器的私有 IP 地址, 因虚拟服务器提供负载平衡(Load Balance)功能, 可将寻求服务的联机, 依权值比重分配给内部网络的服务器群组, 如此可减少服务器的负载, 降低当机的风险, 提高服务器的工作效率。

于本章节, 将针对【IP 对映】、【虚拟服务器 1/2/3/4】作详细的介绍与使用说明:

**【IP 对映】**: 因为内部网络是透过 NAT (Network Address Translation) 机制转换的私有 IP 地址, 如果服务器放于内部网络时, 它的 IP 地址是属于私有 IP (Private IP) 地址; 外部网络的使用者无法直接连上其私有 IP 地址, 必须先连接上外部接口子网络真实 IP (Real IP) 地址, 再由真实 IP 地址对映到内部网络私有 IP 地址, 对映的方式有「IP 对映」与「虚拟服务器」两项。「IP 对映」是一一对映, 即一个外部接口真实 IP 地址的所有服务, 对映到一个内部网络私有 IP 地址。

【虚拟服务器 1/2/3/4】：虚拟服务器是一对多对映，即一个外部接口真实 IP 地址，对映到 1~4 个内部网络私有 IP 地址，并提供【服务表】中基本服务之项目。



### 如何运用虚拟服务器

虚拟服务器和IP对映是因NAT转换机制而产生IP地址对映方式，他们是运用于【管制条例】中【至内部网络】的管制条例，虚拟服务器和IP对映两者功能相当类似，都是以真实IP地址对映到私有IP地址（和NAT转换方式相反）实际的服务器是放在私有IP地址上，但是它们之间仍有些差异性存在：

- 虚拟服务器可以对映到内部多台服务器，IP对映只能对映到一台内部服务器，并且虚拟服务器有负载平衡（Load Balance）功能，将服务的联机对映到不同的服务器主机。
- 虚拟服务器址能对映内部实际服务器某一种服务项目，而IP对映可对映到实际服务器所有服务。

无论是 IP 对映或是虚拟服务器，都是运用将外部接口虚拟服务器的 IP 地址转换成内部网络实际提供服务的服务器的私有 IP 地址的功能，使得外部网络的使用者可藉由与虚拟服务器的 IP 地址寻求服务联机而顺利的使用内部网络的服务器。

## IP 对映

### IP 对映功能设定

【IP 对映】：即一个外部接口真实 IP 地址的所有服务，对映到一个内部网络私有 IP 地址。

步驟1. 在左方的功能选项中，点选【虚拟服务器】功能，再点选【IP 对映】次功能选项。（如图 9-1）



图 9-1 IP 对映功能设定

步驟2. IP 对映表格说明：

- 外部网络地址：外部网络 IP 地址。
- 对映到虚拟网络地址：该外部网络对映至服务器内之虚拟网络所指定的 IP 地址。
- 变更：变更 IP 对映各项设定值。点选【修改】，可修改 IP 对映各项参数；点选【删除】，可删除该项设定。



## 新增 IP 对映

- 步驟**1.** 在 IP 对映窗口中，点选【新增】功能按钮。
- 步驟**2.** 在出现的新增 IP 对映窗口中，键入下列相关参数 (如图 9-2)
- 外部网络地址：可键入外部网络地址。
  - Assist：可直接了解目前外部网络 1/2 的 IP 地址。
  - 对映到虚拟网络地址：键入该外部网络对映至虚拟网络的指定 IP 地址。
- 步驟**3.** 点选屏幕下方【确定】按钮，新增指定的 IP 对映，或点选【取消】取消新增。

新增對映IP	
外部網路位址	61.59.237.131 <span>輔助選取</span>
對映到虛擬網路位址	192.168.1.2
<span>確定</span> <span>取消</span>	

图 9-2 新增 IP 对映

## 变更 IP 对映

- 步驟1. 在【IP 对映】窗口中，找到欲变更设定的 IP 对映，对映至右方【变更】栏，点选【修改】。
- 步驟2. 在出现的【修改 IP 对映】窗口中，键入欲变更的参数值（如图 9-3）
- 步驟3. 点选屏幕下方【确定】按钮，变更指定的 IP 对映设定，或点选【取消】取消设定。



图 9-3 变更 IP 对映



若在【外部至内部网络】管制条例中的目的地址，已设定某 IP 对映，则无法对该条 IP 对映作变更之动作。

## 移除 IP 对映

- 步驟1. 在【IP 对映】窗口中，找到欲变更设定的 IP 对映列，对映至右方【变更】栏，点选【删除】。
- 步驟2. 在【移除 IP 对映】确定对话框中，点选【确定】按钮，移除设定，或点选【取消】取消移除。（如图 9-4）



图 9-4 移除 IP 对映

## 虚拟服务器

### 虚拟服务器 1/2/3/4 功能设定

虚拟服务器是一对多对映，即一个外部接口真实 IP 地址，对映到 1~4 个内部网络私有 IP 地址，并可以对映到内部多台服务器，并且虚拟服务器有负载平衡（Load Balance）功能，将服务的联机对映到不同的服务器主机。

**步骤1.** 在左方的功能选项中，点选【虚拟服务器】功能，再点选【虚拟服务器 1/2/3/4】次功能选项。（如图 9-5）



图 9-5 虚拟服务器功能设定

**步骤2.** 虚拟服务器窗口内名词定义说明：

- 虚拟服务器 IP：此虚拟服务器所设定的外部网络 IP 地址。若尚未设定，可点选【选择】功能按钮，即可新增新虚拟服务器地址，若欲变更，则直接点选该【虚拟服务器 IP 地址】后，键入新 IP 地址。
- 服务名称：此虚拟服务器所提供的服务项目名称。
- 埠号：此虚拟服务器所提供的服务项目所代表之 TCP 端口号码或

UDP 端口号码。

- 服务器 IP 地址：此虚拟服务器所对映的虚拟网络 IP 地址。
- 变更：变更虚拟服务器之各项服务设定值。点选【修改】，可修改 IP 对映各项参数；点选【删除】，可删除该项设定。



本虚拟服务器功能提供四个外部接口真实 IP 地址，亦即最多可设定四个虚拟服务器（由次功能选项之虚拟服务器 1/2/3/4 中设定）。系统管理员可点选虚拟服务器 1/2/3/4 工作窗口中，【虚拟服务器 IP 地址】新增或变更虚拟服务器之 IP 地址；新增或变更该虚拟服务器服务设定，则点选下方【新增服务】功能按钮。

## 新增虚拟服务器

- 步驟1. 在【虚拟服务器 1（或 2、3、4）】窗口中，点选【虚拟服务器 IP】功能按钮。
- 步驟2. 在【新增虚拟服务器 IP】窗口，由【虚拟服务器 IP】键入可使用外部网络 IP 地址。*(如图 9-6)*
- 步驟3. 点选【确定】执行新增虚拟服务器；或点选【取消】取消新增。



9-6 新增虚拟服务器

## 变更虚拟服务器 IP 地址

- 步驟1. 在【虚拟服务器 1（或 2、3、4）】窗口中，点选【虚拟服务器 IP】功能按钮。
- 步驟2. 在【变更虚拟服务器】窗口，由【虚拟服务器 IP】所使用外部网络 IP 地址中，变更 IP 地址。*(如图 9-7)*
- 步驟3. 点选【确定】执行变更虚拟服务器 IP 地址；或点选【取消】取消变更。

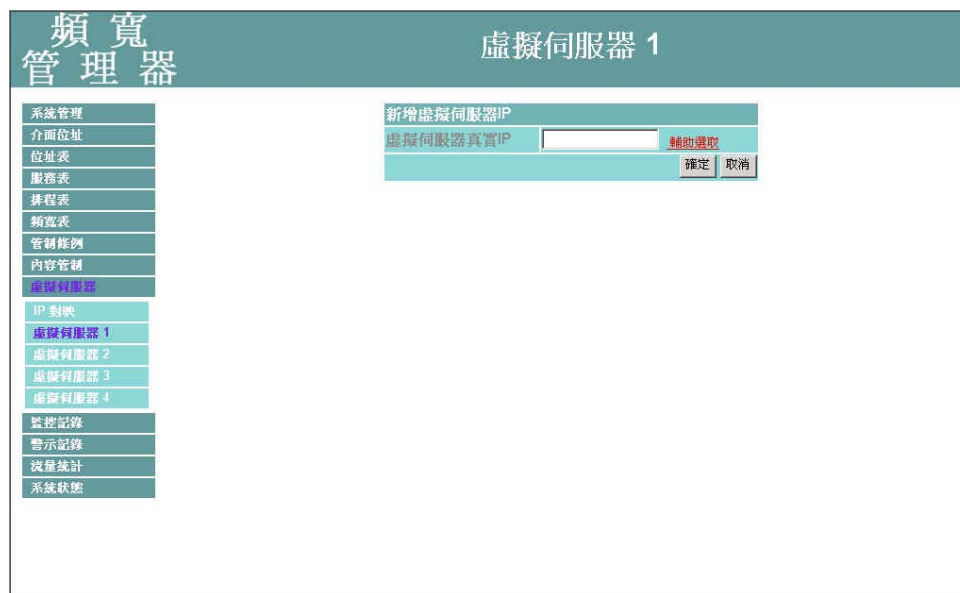


图 9-7 变更虚拟服务器 IP 地址

## 移除虚拟服务器 IP 地址

- 步驟1. 在【虚拟服务器 1（或 2、3、4）】窗口中，点选【虚拟服务器 IP】功能按钮。
- 步驟2. 在【变更虚拟服务器】窗口，由【虚拟服务器 IP】，清除 IP 地址。（如图 9-8）
- 步驟3. 点选【确定】执行移除虚拟服务器 IP 地址；或点选【取消】取消变更。



图 9-8 移除虚拟服务器 IP 地址



## 虚拟服务器服务设定

步驟1. 在左方的功能选项中，点选【虚拟服务器】功能，再点选【虚拟服务器 1（或 2、3、4）】次功能选项。（如图 9-5）

步驟2. 在【虚拟服务器 1（或 2、3、4）】窗口中，点选虚拟服务器表格下方【新增】功能按钮。

步驟3. 在【虚拟服务器组态】设定对话框中（如图 9-9）

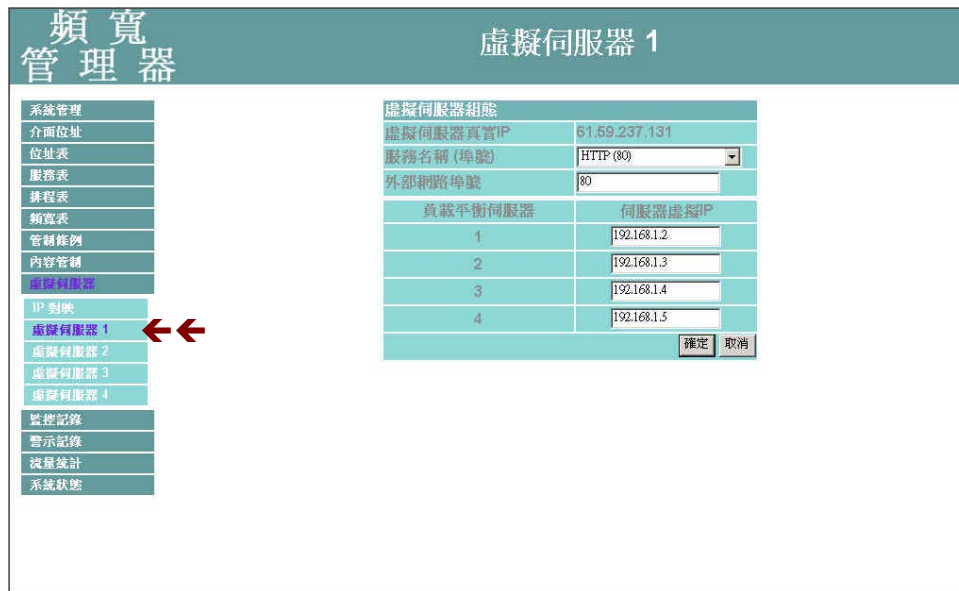


图 9-9 新增虚拟服务器服务

- 虚拟服务器 IP：显示此虚拟服务器所设定的外部网络 IP 地址。
- 服务名称埠号：此虚拟服务器所提供的服务项目的代码。
- 服务名称：此虚拟服务器所提供的服务项目。在此下拉选单内所列的服务项目名称，皆为【服务表】内基本服务所定义。
- 编号：服务器编号。
- 内部网络 IP：此虚拟服务器所对映的内部服务器 IP 地址。最多可设定 4 台计算机的 IP 地址，可达到负载均衡的功能。

## 新增虚拟服务器服务设定

步驟1. 在【虚拟服务器 1（或 2、3、4）】窗口中，点选虚拟服务器表格下方【新增服务】功能按钮。

步驟2. 在【虚拟服务器组态】对话框中，键入下列参数（如图 9-10）



图 9-10 新增虚拟服务器服务

- 虚拟服务器 IP：键入此虚拟服务器所设定的外部网络 IP 地址。
- 服务名称埠号：无须填写，点选下方服务项目时，系统会直接显示该服务项目代码。
- 服务名称：点选下拉选单内所列服务项目名称，此部分窗体内容皆为【服务表】之【基本服务】所定义之服务项目。
- 内部网络 IP：此虚拟服务器所对映的内部服务器 IP 地址。最多可设定 4 台计算机的 IP 地址，可达到负载均衡的功能。

步驟3. 点选【确定】执行新增虚拟服务器服务；或点选【取消】取消新增。

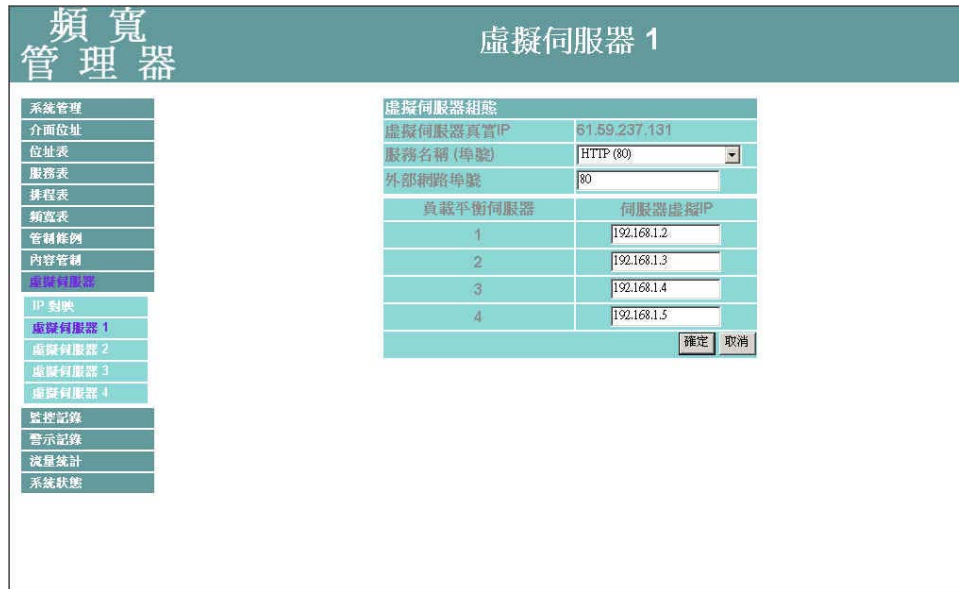


系统主管理员可依需求，点选【虚拟服务器】工作窗口中的【新增服务】控制按钮，增加虚拟服务器的服务项目，并在设定【管制条例】前，完成所有虚拟服务器必须提供的服务项目。否则，于管制条例的服务名称中将不会显示，而无法选择。

## 变更虚拟服务器服务设定

步驟1. 在【虚拟服务器 1（或 2、3、4）】窗口中，由显示该虚拟服务器服务项目的表格中，找到欲变更设定的服务名称，对映至右方【变更】栏，点选【修改】。

步驟2. 在【变更虚拟服务器】窗口，键入欲变更的参数值（如图9-11）



The screenshot shows the 'Virtual Server 1' configuration window. On the left is a navigation menu with options like 'System Management', 'Interface', 'Services', and 'Virtual Servers'. The main area is titled 'Virtual Server Group' and contains a table for service settings. The table has columns for 'Load Balancing Virtual Server' and 'Virtual Server IP'. The 'Service Name' is set to 'HTTP (80)' and the 'External Network IP' is '80'. Below the table are 'Confirm' and 'Cancel' buttons.

虛擬伺服器組態	
虛擬伺服器真實IP	61.59.237.131
服務名稱 (埠號)	HTTP (80)
外部網路埠號	80
負載平衡伺服器	伺服器虛擬IP
1	192.168.1.2
2	192.168.1.3
3	192.168.1.4
4	192.168.1.5

图 9-11 变更虚拟服务器服务设定

- 外部网络：键入此虚拟服务器所设定的外部网络 IP 地址。
- 服务埠：无须填写，点选下方服务项目时，系统会直接显示该服务项目代码。
- 服务名称：点选下拉选单内所列服务项目名称，此部分窗体内容皆为【服务表】之【基本服务】所定义之服务项目。
- 内部网络 IP：输入此虚拟服务器所对映的内部网络 IP 地址。最多可设定四组 IP 地址。

步驟3. 点选【确定】执行变更虚拟服务器服务；或点选【取消】取消变更。



若在【管制条例】中的目的网络，已设定某条虚拟服务器，则无法对该条虚拟服务器作变更动作。须先移除【管制条例】中该项设定，才可执行变更设定。

## 移除虚拟服务器服务设定

- 步驟1. 在【虚拟服务器 1（或 2、3、4）】窗口中，由虚拟服务器服务项目的表格中，找到欲变更设定的服务名称，对映至右方【变更】栏，点选【删除】。
- 步驟2. 在【删除虚拟服务器】窗口，点选【确定】执行删除虚拟服务器 IP 地址；或点选【取消】取消删除。（如图 9-12）

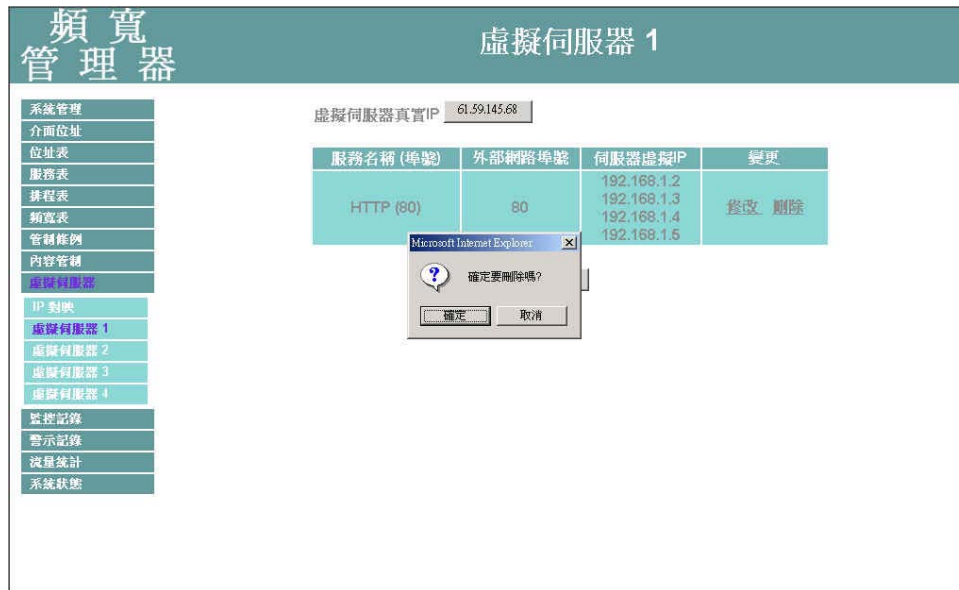


图 9-12 移除虚拟服务器服务设定



若在【管制条例】中的目的网络，已设定某条虚拟服务器，则无法对该条虚拟服务器作变更之动作。须先移除【管制条例】中该项设定，才可执行变更设定。

# 监控记录

监控记录为所有符合【管制条例】的联机记录，分为流量监控与事件监控两种，流量监控的参数是在制定管制条例时同时设定，流量监控详细记录每条管制条例资料封包联机内容，包含此封包的联机起始时间、封包来源地址、目的地址、服务项目及处置方式。事件监控则记录频宽管理器系统组态参数值(System Configurations)更改内容，包含更改者、更改时间、修改的参数，从什么 IP 地址登入频宽管理器...等。

本频宽管理器提供之「流量监控」与「事件监控」功能，为针对系统管理员所指定的「来源地址」与「目的地址」进行「服务项目」及「处置方式」的记录，让系统管理员掌握频宽管理器系统状况。同时，本频宽管理器亦提供系统管理员将各种记录下载备份。

(一) 【流量监控】系统管理员可在流量监控记录里，查询目前进出频宽管理器各个联机状态，包括：联机起始时间、来源地址、目的地址与处置方式等。并每隔一段时间，将流量监控记录储存备份，再删除线上记录，让线上维持最新记录。

(二) 【事件监控】当频宽管理器侦测到系统发生某些事件时，系统管理员可经由此事件监控功能，了解事件发生的时间详细说明，并将其下载备份。

(三) 【联机纪录】：系统管理员可以利用此功能,了解目前对联机状态作纪录。

(四) 【监控报告】：系统管理员可利用此功能，设定系统自动发出 E-mail 提醒管理员流量监控与事件监控的记录，也可利用远程记录实时接收频宽管理器的监控报告。



## 如何运用监控记录

系统管理员可利用监控记录，监控网络的使用情形，以作为网络管理的依据。

## 流量监控

### 流量监控功能

系统管理员可在流量监控记录里，查询目前进出频宽管理器各个联机状态，包括：联机起始时间、来源地址、目的地址与处置方式等。并每隔一段时间，将流量监控记录储存备份，再删除线上记录，让线上维持最新记录。

時間	來源位址	目的位址	協定 & 埠號	處置方式
May 1 03:22:01	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:21:53	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:20:54	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:20:12	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:20:09	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:19:44	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:19:24	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:18:55	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:18:19	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:16:51	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:16:50	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:13:59	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:13:16	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:11:37	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:11:31	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT
May 1 03:11:22	210.59.145.158	192.168.1.2	TCP : 18712	DROP
May 1 03:11:16	210.59.145.64	192.168.1.2	TCP : 3383	DROP
May 1 03:11:16	210.59.145.60	192.168.1.2	TCP : 16327	DROP
May 1 03:11:12	66.35.229.173	192.168.1.2	TCP : 3368	DROP
May 1 03:10:50	192.168.1.3	192.168.1.1	TCP : 80	ACCEPT

图 10-1 流量监控功能

流量监控窗口名词名称定义：

- 下拉选单：点选下拉选单所显示的联机时间，以检视于该联机时间之流量状态。点选【上一页】，检视其它联机时间之流量状态。点选【下一页】，回到原流量监控画面。
- 时间：此监控记录发生的联机起始时间（月/日/时/分/秒）。
- 来源地址：来源端使用者的 IP 地址与协议端口号码。
- 目的地址：目的端的 IP 地址与协议端口号码。
- 协议与埠号：服务项目名称与服务端口。
- 处置方式：ACCEPT 表示允许通过，DROP 表示禁止通过。



## 下载流量监控记录

步驟1. 在【流量监控】窗口中，點選屏幕下方【下载监控记录】功能按钮。

步驟2. 在【档案下载】对话框，将该流量监控记录储存至指定的硬盘目录位置 (如图10-2)



图 10-2 下载流量监控记录

## 清除流量监控记录

步驟1. 在【流量监控】窗口中，点选屏幕下方【清除记录】功能按钮。

步驟2. 在【清除记录】确认窗口中，点选【确定】执行清除记录；或点选【取消】取消清除。(如图10-3)



图 10-3 清除流量监控记录

## 事件监控

### 事件监控功能

当频宽管理器侦测到系统发生某些事件时，系统管理员可经由此事件监控功能，了解事件发生的时间详细说明，并将其下载备份。



图 10-4 事件监控功能

事件监控窗口名词名称定义：

- 时间：此联机发生的起始时间。
- 事件：此联机发生时间的事件说明。

## 下载事件监控记录

步驟1. 在【事件监控】窗口中，点选屏幕下方【下载监控记录】功能按钮。

步驟2. 在【档案下载】对话框，将该事件监控记录储存至指定的硬盘目录位置（如图10-5）



图 10-5 下载事件监控记录

## 清除事件监控记录

- 步驟1. 在【事件监控】窗口中，点选屏幕下方【清除记录】功能按钮。
- 步驟2. 在【清除记录】确认窗口中，点选【确定】执行清除记录；或点选【取消】取消清除。(如图10-6)



图 10-6 清除事件监控记录

## 联机纪录

### 联机纪录功能

系统管理员可以利用此功能,了解目前对外部联机的状态作成纪录。

The screenshot shows the '頻寬管理器' (Bandwidth Manager) interface. The main title is '連線紀錄' (Connection Log). The interface includes a sidebar with navigation options, a main content area with a log table, and control buttons at the bottom.

System Management (系統管理) | Interface Location (介面位址) | Address List (位址表) | Service List (服務表) | Queue List (排程表) | Bandwidth List (頻寬表) | Policy List (管制條例) | Content Control (內容管制) | Server List (虛擬伺服器) | **連線紀錄** (Connection Log) | Traffic Monitoring (流量監控) | Event Monitoring (事件監控) | Monitoring Report (監控報告) | Warning Log (警告記錄) | Traffic Statistics (流量統計) | System Status (系統狀態)

Time (時間) | Connection Log (連線紀錄)

時間	連線紀錄
May 1 03:19:54	pppd 2.4.1 started by root, uid 0
May 1 03:19:54	Couldn't allocate PPP unit -1073449922 as it is already in use
May 1 03:19:54	Using interface ppp0
May 1 03:19:54	PPPoE : Couldn't increase MTU to 1500
May 1 03:19:54	Couldn't increase MRU to 1500
May 1 03:19:54	local IP address 10.64.64.64
May 1 03:19:54	remote IP address 10.107.177.249
May 1 03:19:54	linkname : interface : ppp0
May 1 03:19:55	Starting link
May 1 03:19:55	Sending PADI

Clear Log (清除記錄) | Download Monitoring Log (下載監控記錄)

图 10-7 联机纪录功能

联机纪录窗口名词名称定义：

- 时间：此联机发生的起始时间。
- 联机纪录：此联机发生时间的事件说明。

## 下载联机记录

步驟1. 在【联机记录】窗口中，点选屏幕下方【下载联机记录】功能按钮。

步驟2. 在【档案下载】对话框，将该联机记录储存至指定的硬盘目录位置  
(如图10-8)



图 10-8 下载联机记录

## 清除联机记录

- 步驟1. 在【联机纪录】窗口中，点选屏幕下方【清除记录】功能按钮。
- 步驟2. 在【清除记录】确认窗口中，点选【确定】执行清除记录；或点选【取消】取消清除。(如图10-9)



图 10-9 清除联机记录



## 监控报告

### 监控报告功能

系统管理员可利用此功能，设定系统自动发出 E-mail 提醒管理员流量监控与事件监控的记录，也可利用远程记录实时接收频宽管理器的监控报告。

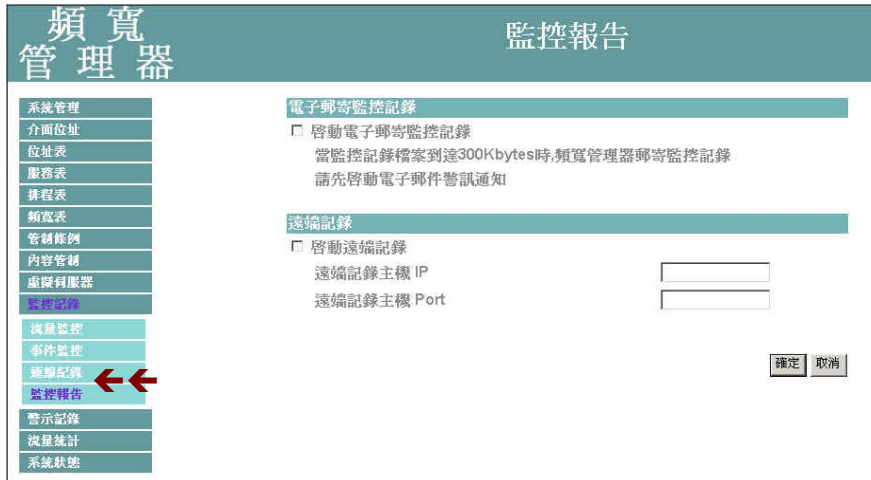


图 10-10 监控报告

#### 步驟1. 【监控报告】窗口名词名称定义：

- 电子邮箱监控记录：当监控记录档案到达 **300Kbytes** 时，频宽管理器将会以电子邮件方式发出流量监控与事件监控记录通知系统管理员。  
※请注意：激活此功能必须先于系统管理的系统设定填入 **E-mail**。
- 远程记录：设定此功能，系统会将流量监控与事件监控记录同步传送到此设定的 **IP** 地址的主机计算机。（该主机必须为提供 **Syslog** 功能之伺服主机）



欲重新起始联机监控记录，在【联机记录】工作窗口中。点选右方【重新设定】功能按钮，联机监控功能即由设定时实时激活。

## 激活电子邮件与远程监控记录

**步驟1.** 开启电子邮箱监控记录功能：请先于选单【系统管理】的【系统设定】中的【E-mail 设定】，勾选【开启电子邮件警讯通知】并键入欲接收监控记录之电子邮件地址，点选【确定】后再于【监控记录】的【监控报告】勾选【激活电子邮箱监控记录】，最后点选屏幕右下方【确定】按钮。（如图 10-11）

**步驟2.** 激活远程记录：勾选【激活远程记录】，并于下方【远程记录主机 IP】空栏中，键入提供接收记录监控的主机 IP 地址与 Port number 后，点选屏幕右下方【确定】按钮。（如图 10-11）

頻寬管理器

監控報告

系統管理  
介面位址  
位址表  
服務表  
排程表  
頻寬表  
管制條例  
內容管制  
虛擬伺服器  
監控記錄  
流量監控  
事件監控  
連線記錄  
監控報告  
警示記錄  
流量統計  
系統狀態

電子郵件監控記錄

啟動電子郵件監控記錄  
當監控記錄檔案到達300Kbytes時,頻寬管理器將寄監控記錄  
請先啟動電子郵件警訊通知

遠端記錄

啟動遠端記錄

遠端記錄主機 IP

遠端記錄主機 Port

確定 取消

图 10-11 激活电子邮件监控记录

## 取消电子邮件与远程监控记录

- 步驟1. 取消电子邮寄监控记录：取消勾选【激活电子邮寄监控记录】功能，并点选屏幕右下方【确定】按钮。（如图10-12）
- 步驟2. 取消远程记录：取消勾选【激活远程记录】功能，并点选屏幕右下方【确定】按钮。（如图10-12）

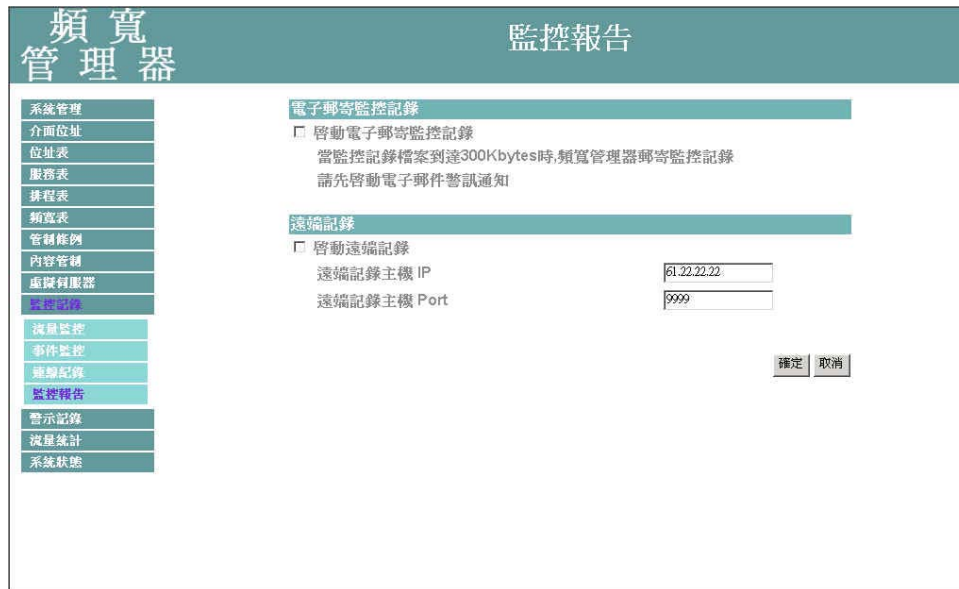


图 10-12 取消电子邮件监控记录

# 警示记录

警示记录分为「流量警示」与「事件警示」两种。

(一) **【流量警示】**: 在制定管制条例时须先设定流量警示值，系统每隔一段时间会检查经过管制条例的资料量是否超过警示值，如果超过警示值，系统会将其记录在流量警示档案。

(二) **【事件警示】**: 当频宽管理器侦测出网络正受到骇客恶意攻击时，系统会将攻击资料写入事件警示档，并发出 E-mail 通知管理员采取警急措施。



## 如何运用警示记录

系统管理员可利用「警示记录」功能，查询进出频宽管理器「来源地址」、「目的地址」、「网络服务」以及网络繁忙状况。每隔一段时间，系统主管理员可将「流量警示记录」与「事件警示记录」储存备份，再删除线上记录，让线上维持最新网络状态记录。

## 流量警示

### 流量警示功能

在制定管制条例时须先设定流量警示值，系统每隔一段时间会检查经过管制条例的资料量是否超过警示值，如果超过警示值，系统会将其记录在流量警示档案。

頻寬管理器

流量警示

時間	來源位址	目的位址	服務名稱	網路流量
May 1 05:00-05:15	Inside_Any	Outside_Any	ANY	1.576K/Sec
May 1 04:45-05:00	Inside_Any	Outside_Any	ANY	0.225K/Sec
May 1 04:30-04:45	Inside_Any	Outside_Any	ANY	3.659K/Sec
May 1 03:30-03:45	Inside_Any	Outside_Any	ANY	0.179K/Sec
May 1 03:15-03:30	Inside_Any	Outside_Any	ANY	1.401K/Sec
May 1 03:00-03:15	Inside_Any	Outside_Any	ANY	0.619K/Sec

清除記錄

下載監控記錄

系統管理  
介面位址  
位址表  
服務表  
排程表  
類表  
管制條例  
內容管制  
虛探伺服器  
監控記錄  
警示記錄  
流量警示  
事件警示  
流量統計  
系統狀態

图 11-1 流量警示功能

流量警示窗口，表格内数值显现目前系统联机的状态。

- 时间：连结起始至结束的时间（起始时间 月/日/时/秒 至 结束 时/秒）。
- 来源地址：来源端网络地址。
- 目的地址：目的端网络地址。
- 服务名称：服务项目名称。
- 网络流量：网络流量（Kbytes/Sec）。

## 下载流量警示记录

步驟1. 在【流量警示】窗口中，點選屏幕下方【下载监控记录】功能按钮。

步驟2. 在【档案下载】对话框，将该流量警示记录储存至指定的硬盘目录位置（如图 11-2）



图 11-2 下载流量警示记录

## 清除流量警示记录

- 步驟1. 在【流量警示】窗口中，点选屏幕下方【清除记录】功能按钮。
- 步驟2. 在【清除记录】确认窗口中，点选【确定】执行清除记录；或点选【取消】取消清除。(如图 11-3)



图 11-3 清除流量警示记录

## 事件警示功能

当频宽管理器侦测出网络正受到骇客恶意攻击时，系统会将攻击资料写入事件警示档，并发出 E-mail 通知管理员采取警急措施

時間	事件
Feb 13 14:41:57	Possible ICMP FLOOD from 172.19.1.183 (00:cc:00:00:00:08) against 172.19.1.106, recieved 2 packets
Feb 13 14:41:43	Possible ICMP FLOOD from 172.19.1.183 (00:cc:00:00:00:08) against 172.19.1.106, recieved 2 packets

图 11-4 事件警示记录功能

在【事件警示】窗口中，表格内数值显现目前系统联机状态

- 下拉选单：可點選下拉选单所显示的事件警示发生时间，以检视于该联机时间警示说明。点选【上一页】，检视其它联机时间之事件警示。点选【下一页】，回到原事件警示画面。
- 时间：事件发生的联机时间（月/日/时/秒）。
- 事件：事件说明。



## 下载事件警示记录

- 步驟1. 在【事件警示】窗口中，點選屏幕下方【下载记录】功能按钮。
- 步驟2. 在【档案下载】对话框，将该事件警示记录储存至指定的硬盘目录位置（如图 11-5）



图 11-5 下载事件警示记录

## 清除事件警示记录

- 步驟1. 在【事件警示】窗口中，点选屏幕下方【清除记录】功能按钮。
- 步驟2. 在【清除记录】确认窗口中，点选【确定】执行清除记录；或点选【取消】取消清除。(如图 11-6)



图 11-6 清除事件警示记录

# 统计报告

统计报告可细分为内部到外部统计报告及  
外部到内部统计报告两种

[内部至外部统计报告]



将所有从所有通过频宽管理器 的内部网络和外部网络及各种通讯服务下载 / 上传 流量所做的统计

**来源 IP:** 通过频宽管理器内部网络使用者 IP 地址。

**目的 IP:** 通过频宽管理器的外部网络服务器 IP 地址。

**Service:** 内部网络使用者通过频宽管理器到外部网络服务器所有通讯服务名称。

## 「外部至内部统计报告」



将外部网络使用者通过频宽管理器的至内部网络服务器及各种通讯服务 下载 / 上传 流量所做的统计

**来源 IP:** 通过频宽管理器外部网络使用者 IP 地址。

**目的 IP:** 通过频宽管理器内部网络服务器 IP 地址。

**Service:** 外部网络使用者通过频宽管理器到内部网络服务器所有通讯服务名称

系统管理员可运用统计报告功能，查询频宽管理器的**内部网络** IP 使用者或**外部网络** IP 使用者，并对进出频宽管理器的所有使用者的 IP 进行「**下载流量/上传流量**」「**起始时间 / 结束时间 / 持续时间**」及 [Service] 统计资料，提供系统管理员监控网络上每个 IP 流量及图表分析。

## 内部至外部

### 内部至外部统计报告

步骤1. 在左方的功能选项中，点选【统计报告】功能，再点选【内部至外部】次功能选项。(如图 12-1)

頻寬管理器

内部至外部

Top: 1-5

清除記錄時間: Wed May 1 00:07:24 2002

編號	來源IP	下載流量	上傳流量	開始時間	結束時間	持續時間
1	192.168.1.6	0.0 B 0.0%	97.7 KB 11.2%	05/01 00:38:16	05/01 00:40:01	00:01:45
2	192.168.1.5	0.0 B 0.0%	323.9 KB 37.2%	05/01 00:33:53	05/01 00:38:00	00:04:07
3	192.168.1.4	0.0 B 0.0%	135.0 KB 15.5%	05/01 00:31:48	05/01 00:33:36	00:01:48
4	192.168.1.3	0.0 B 0.0%	124.3 KB 14.3%	05/01 00:28:28	05/01 00:31:25	00:02:57
5	192.168.1.2	0.0 B 0.0%	189.6 KB 21.8%	05/01 00:08:23	05/01 00:28:18	00:19:55
總流量		0.0 Bytes	870.4 KBytes	Reporting Time: Wed May 1 00:40:03 2002		

清除記錄

图 12-1 内部至外部统计报告

## 内部至外部 来源 IP 统计报告

来源 IP: 内部网络通过频宽管理器的使用者 IP 地址, 传送/接收 封包时的下载流量 / 上传流量 / 开始时间 / 结束时间 / 持续时间 等产生的统计资料。

步骤1. 来源 IP 窗口内名词定义说明: (如图 12-2)

- TOP: 选择想要检视的第几笔资料, 每十笔为一页。
- 下拉式选单中选择  
来源 IP: 内部网络通过频宽管理器的使用者 IP 地址
- 下载流量: 每一个外部网络服务器通过频宽管理器到内部网络使用者流量数值及下载总流量的百分比。
- 上传流量: 每一个内部网络使用者通过频宽管理器到外部网络服务器流量数值及上传总流量的百分比。
- 开始时间: 内部网络的每一个使用者通过频宽管理器, 第一个封包开始纪录时间。
- 结束时间: 内部网络的每一个使用者通过频宽管理器, 最后一个封包结束纪录时间。
- 持续时间: 内部网络的每一个使用者通过频宽管理器, 第一个封包及最后一个封包所经历的时间。
- 总流量: 累计内部网络的每一个使用者通过频宽管理器下载/上传总流量及百分比 最后产生统计报告时间。
- 清除纪录: 为清除所有纪录, 重新开始计算报告。



图 12-2 内部至外部来源 IP 统计报告

## 内部至外部 目的 IP 统计报告

**目的 IP:** 外部网络服务器通过频宽管理器所使用的 IP 地址 传送/接收 封包时的 下传流量 / 上载流量 / 开始时间 / 结束时间 / 持续时间 等产生的统计资料。

**步骤1.** 来源 IP 窗口内名词定义说明: (如图 12-3)

- **TOP:** 选择想要检视的第几笔资料, 每十笔为一页。
- 下拉式选单中选择  
目的 IP: 外部网络服务器通过频宽管理器所使用的 IP 地址
- **下载流量:** 每一个外部网络服务器通过频宽管理器到内部网络使用者流量数值及下载总流量的百分比。
- **上传流量:** 每一个内部网络使用者通过频宽管理器到外部网络服务器流量数值及上传总流量的百分比。
- **开始时间:** 通过频宽管理器的每一个外部网络服务器, 第一个封包开始纪录时间。
- **结束时间:** 通过频宽管理器的每一个外部网络服务器, 最后一个封包结束纪录时间。
- **持续时间:** 通过频宽管理器的每一个外部网络服务器, 第一个封包及最后一个封包所经历的时间。
- **累计** 通过频宽管理器的每一个外部网络服务器 下载/上传 总流量及百分比 最后产生统计报告时间。
- **清除纪录:** 清除所有纪录, 重新开始计算报告。



# 頻寬 管理器

## 內部至外部

系統管理

介面位址

位址表

服務表

排程表

頻寬表

管理雜例

內容管制

重轉伺服器

監控記錄

警告記錄

統計報告

內部至外部

外部至內部

流量統計

系統狀態

Top: [11-20]

清除記錄時間: Wed May 1 00:07:24 2002

編號	目的IP	下載流量	上傳流量	開始時間	結束時間	持續時間
11	66.160.2.76	10.9 KB 1.2%	0.0 B 0.0%	05/01 00:12:28	05/01 00:13:19	00:00:51
12	203.204.59.76	10.4 KB 1.2%	0.0 B 0.0%	05/01 00:32:21	05/01 00:33:08	00:00:47
13	168.95.1.1	8.2 KB 0.9%	0.0 B 0.0%	05/01 00:08:23	05/01 01:18:46	01:10:22
14	209.197.247.183	7.6 KB 0.8%	0.0 B 0.0%	05/01 00:32:19	05/01 00:32:53	00:00:34
15	207.46.106.94	6.3 KB 0.7%	0.0 B 0.0%	05/01 00:32:13	05/01 01:20:00	00:47:47
16	211.20.188.140	4.4 KB 0.5%	0.0 B 0.0%	05/01 00:28:18	05/01 01:18:03	00:49:46
17	165.21.82.165	4.1 KB 0.5%	0.0 B 0.0%	05/01 00:12:32	05/01 01:19:39	01:07:07
18	209.171.43.28	3.8 KB 0.4%	0.0 B 0.0%	05/01 00:32:19	05/01 00:38:41	00:06:22
19	65.54.230.240	3.8 KB 0.4%	0.0 B 0.0%	05/01 00:32:18	05/01 00:39:39	00:07:21
20	211.22.93.142	3.5 KB 0.4%	0.0 B 0.0%	05/01 00:29:23	05/01 01:17:29	00:48:06
總流量		897.6 KBytes	0.0 Bytes	Reporting time Wed May 1 01:22:57 2002		

清除記錄


图 12-3 内部至外部目的 IP 统计报告

## 内部至外部 Service 统计报告

**Service:** 内部网络使用者通过频宽管理器外部网络服务器所有通讯服务名称  
下载流量 / 上传流量 / 开始时间 / 结束时间 / 持续时间 等产生的统计资料及图表。

**步骤1.** 来源 IP 窗口内名词定义说明：*(如图 12-4)*

- TOP: 选择想要检视的第几笔资料，每十笔为一页。

- : 依照所选择的 TOP 编号 绘出 下载/上传 统计报告的长条图及饼图 *(如图 12-5)*

- 下拉式选单中选择

**Service:** 内部网络使用者通过频宽管理器到外部网络服务器通讯服务名称的统计报告

- 下载流量: 内部网络使用者通过频宽管理器到外部网络服务器通讯服务统计数值及下载总流量的百分比。

- 上传流量: 内部网络使用者通过频宽管理器到外部网络服务器通讯服务的统计数值及上传总流量的百分比。

- 开始时间: 通过频宽管理器的外部网络服务器通讯服务，第一个封包开始纪录时间。

- 结束时间: 通过频宽管理器的外部网络服务器通讯服务，最后一个封包结束纪录时间。

- 持续时间: 通过频宽管理器的外部网络服务器通讯服务，第一个封包及最后一个封包所经历的时间。

- 总流量: 累计外部网络每一个通讯服务 下载/上传 总流量及百分比最后产生统计报告时间。

- 清除纪录: 清除所有纪录，重新开始计算报告。



图 12-4 内部至外部 Service 统计报告



图 12-5 内部至外部 Service 上传/下载 分析统计报告的饼图及长条图



按



返回统计表格

## 外部至内部

### 外部至内部统计报告

步驟1. 在左方的功能选项中，点选【统计报告】功能，再点选【外部至内部】次功能选项。(如图 12-6)

頻寬管理器 外部至內部

Top: 1-10 清除記錄時間: Wed May 1 00:07:24 2002

編號	來源IP	下載流量	上傳流量	開始時間	結束時間	持續時間		
1	210.85.174.43	1008.9 KB	23.1%	0.0 B	0.0%	05/01 01:47:28	05/01 01:58:44	00:11:16
2	211.74.30.209	790.0 B	0.0%	0.0 B	0.0%	05/01 01:49:51	05/01 01:51:22	00:01:31
3	140.115.10.150	608.0 B	0.0%	0.0 B	0.0%	05/01 01:46:26	05/01 02:00:55	00:14:29
4	218.164.218.250	661.0 B	0.0%	0.0 B	0.0%	05/01 01:54:30	05/01 01:55:27	00:00:57
5	193.111.198.137	662.0 B	0.0%	0.0 B	0.0%	05/01 02:02:13	05/01 02:02:21	00:00:08
6	140.112.121.97	837.0 B	0.0%	0.0 B	0.0%	05/01 01:47:33	05/01 01:48:18	00:00:45
7	218.32.148.13	57.8 KB	1.3%	0.0 B	0.0%	05/01 01:50:44	05/01 01:56:34	00:05:50
8	203.73.7.188	723.0 B	0.0%	0.0 B	0.0%	05/01 01:51:45	05/01 01:53:34	00:01:49
9	61.231.77.49	1.2 KB	0.0%	0.0 B	0.0%	05/01 01:54:18	05/01 02:04:24	00:10:06
10	61.220.219.223	891.0 B	0.0%	0.0 B	0.0%	05/01 01:51:41	05/01 01:52:29	00:00:48
總流量		4.3 MBytes	0.0 Bytes	Reporting time: Wed May 1 02:05:05 2002				

清除記錄

图 12-6 外部至内部统计报告

## 外部至内部 来源 IP 统计报告

**来源 IP:** 外部网络使用者通过频宽管理器所使用 IP 地址 传送/接收 封包时的 下载流量 / 上传流量 / 开始时间 / 结束时间 / 持续时间 等产生的统计资料。

### 步骤1. 来源 IP 窗口内名词定义说明: (如图 12-7)

- **TOP:** 选择想要检视的第几笔资料, 每十笔为一页。
- 下拉式选单中选择  
来源 IP: 外部网络使用者通过频宽管理器所使用 IP 地址
- **下载流量:** 每一个外部网络使用者通过频宽管理器到内部网络服务器流量数值及下载总流量的百分比。
- **上传流量:** 每一个内部网络服务器通过频宽管理器的外部网络使用者流量数值及上传总流量的百分比。
- **开始时间:** 每一个外部网络使用者通过频宽管理器到内部网络服务器, 第一个封包开始纪录时间。
- **结束时间:** 每一个外部网络使用者通过频宽管理器到内部网络服务器, 最后一个封包结束纪录时间。
- **持续时间:** 每一个外部网络使用者通过频宽管理器到内部网络服务器, 第一个封包及最后一个封包所经历的时间。
- **总流量:** 累计每一个外部网络使用者到内部网络服务器 下载/上传总流量及百分比 最后产生统计报告时间。
- **清除纪录:** 清除所有纪录, 重新开始计算报告。

# 頻寬管理器

## 外部至內部

Top: [1-10] 清除記錄時間: Wed May 1 00:07:24 2002

編號	來源IP	下載流量	上傳流量	開始時間	結束時間	持續時間
1	210.85.174.43	1008.9 KB 23.1%	0.0 B 0.0%	05/01 01:47:28	05/01 01:58:44	00:11:16
2	211.74.30.209	790.0 B 0.0%	0.0 B 0.0%	05/01 01:49:51	05/01 01:51:22	00:01:31
3	140.115.10.150	608.0 B 0.0%	0.0 B 0.0%	05/01 01:46:26	05/01 02:00:55	00:14:29
4	218.164.218.250	681.0 B 0.0%	0.0 B 0.0%	05/01 01:54:30	05/01 01:55:27	00:00:57
5	193.111.198.137	682.0 B 0.0%	0.0 B 0.0%	05/01 02:02:13	05/01 02:02:21	00:00:08
6	140.112.121.97	837.0 B 0.0%	0.0 B 0.0%	05/01 01:47:33	05/01 01:48:18	00:00:45
7	218.32.148.13	57.8 KB 1.3%	0.0 B 0.0%	05/01 01:50:44	05/01 01:56:34	00:05:50
8	203.73.7.188	723.0 B 0.0%	0.0 B 0.0%	05/01 01:51:46	05/01 01:53:34	00:01:49
9	61.231.77.49	1.2 KB 0.0%	0.0 B 0.0%	05/01 01:54:18	05/01 02:04:24	00:10:06
10	61.220.219.223	891.0 B 0.0%	0.0 B 0.0%	05/01 01:51:41	05/01 01:52:29	00:00:48
<b>總流量</b>		<b>4.3 MBytes</b>	<b>0.0 Bytes</b>	Reporting time Wed May 1 02:05:05 2002		

[清除記錄](#)

图 12-7 外部至内部来源 IP 统计报告

## 外部至内部 目的 IP 统计报告

**目的 IP:** 内部网络服务器通过频宽管理器所使用的 IP 地址 传送/接收 封包时的 下载流量 / 上传流量 / 开始时间 / 结束时间 / 持续时间 等产生的统计资料。

### 步骤1. 来源 IP 窗口内名词定义说明: (如图 12-8)

- **TOP:** 选择想要检视的第几笔资料, 每十笔为一页。
- 下拉式选单中选择  
目的 IP: 内部网络服务器通过频宽管理器所使用的 IP 地址
- **下载流量:** 外部网络使用者通过频宽管理器到每一个内部网络服务器流量数值及下载总流量的百分比。
- **上传流量:** 每一个内部网络服务器通过频宽管理器到外部网络使用者流量数值及上传总流量的百分比。
- **开始时间:** 通过频宽管理器内部网络每一个服务器, 第一个封包开始纪录时间。
- **结束时间:** 通过频宽管理器内部网络每一个服务器, 最后一个封包结束纪录时间。
- **持续时间:** 每一个通过频宽管理器内部网络服务器, 第一个封包及最后一个封包所经历的时间。
- **总流量:** 累计每一个内部网络服务器到外部网络使用者 下载/上传总流量及百分比 最后产生统计报告时间。
- **清除纪录:** 清除所有纪录, 重新开始计算报告。



图 12-8 外部至内部 目的 IP 统计报告




## 外部至内部 Service 统计报告

**Service:** 外部网络使用者通过频宽管理器到内部网络服务器通讯服务名称  
下载流量 / 上传流量 / 开始时间 / 结束时间 / 持续时间 等产生的统计资料及图表。

步骤1. 来源 IP 窗口内名词定义说明: (如图 12-9)

■ TOP: 选择想要检视的第几笔资料, 每十笔为一页。

■ : 依照所选择的 TOP 编号 绘出 下载/上传 统计报告的长条图及饼图 (如图 12-10)

■ 下拉式选单中选择

**Service:** 外部使用者通过频宽管理器到内部网络服务器通讯服务名称的统计报告

■ 下载流量: 外部网络使用者通过频宽管理器到内部网络服务器通讯服务统计数值及下载总流量的百分比。

■ 上传流量: 内部网络服务器通过频宽管理器到外部网络使用者通讯服务统计数值及上传总流量的百分比。

■ 开始时间: 每一个通过频宽管理器内部网络服务器通讯服务, 第一个封包开始纪录时间。

■ 结束时间: 每一个通过频宽管理器内部网络服务器通讯服务, 最后一个封包结束纪录时间。

■ 持续时间: 每一个通过频宽管理器内部网络服务器通讯服务, 第一个封包及最后一个封包所经历的时间。

■ 总流量: 累计每一个内部网络服务器通讯服务的 总流量及百分比最后产生统计报告时间。

■ 清除纪录: 清除所有纪录, 重新开始计算报告。



图 12-9 外部至内部 Service 统计报告

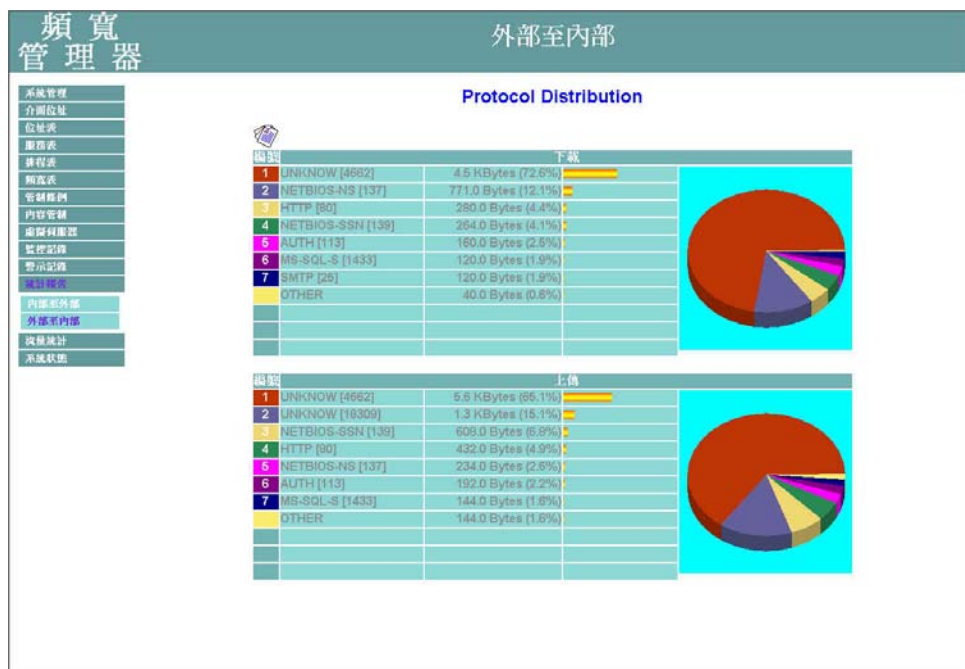


图 12-10 外部至内部 Service 上传/下载 分析统计报告的饼图及长条

图



按



返回统计表格

# 流量统计

「外部网络流量统计」即为所有符合【外部网络】的上传/下载封包及上传/下载流量记录的统计资料。

「管制条例流量统计」即为所有符合【管制条例】的封包记录的统计资料。

系统管理员可运用流量统计功能，查询频宽管理器针对【管制条例】内之「来源网络」、「目的网络」、「网络服务」与管制动作等各联机进出频宽管理器的「封包」、「传输量」流量统计，以提供系统管理员监控网络系统流量状况，查看网络繁忙状况。



## 如何运用流量统计

系统管理员需先至【管制条例】中，设定欲统计流量的网络地址，以经由「流量统计」功能得知目前网络的使用状况，作为网络管理的依据。

## 外部网络流量

### 外部网络流量统计功能

即为所有符合【外部网络】的 下载/上传 封包及 下载/上传 流量记录的统计资料。



图 13-1 外部网络流量统计功能

显现目前系统外部流量统计图。

- 时间：检视分别以分、时、日为时间单位的流量统计。
- 外部网络下传流量图
- 外部网络上传流量图
- 外部网络下传封包数图
- 外部网络上传封包数图



若欲使用【流量统计】，系统管理员须先至【管制条例】功能设定中，在指定的网络地址，激活【流量统计】功能。

## 检视外部网络流量统计

步驟1. 在【流量统计】窗口中，找到欲检视的网络区域名称，对应至右方【检视】栏：点选【分】，可检视以每分钟（min）为单位的流量统计图表；点选【时】，可检视以每小时(hour)为单位的流量统计图表；点选【日】，可检视以日（day）为单位的流量统计图表。

步驟2. 流量统计图表（如图 13-2）

- 纵坐标：网络流量（Kbytes/Sec）。
- 横坐标：时间（时/分/日）。

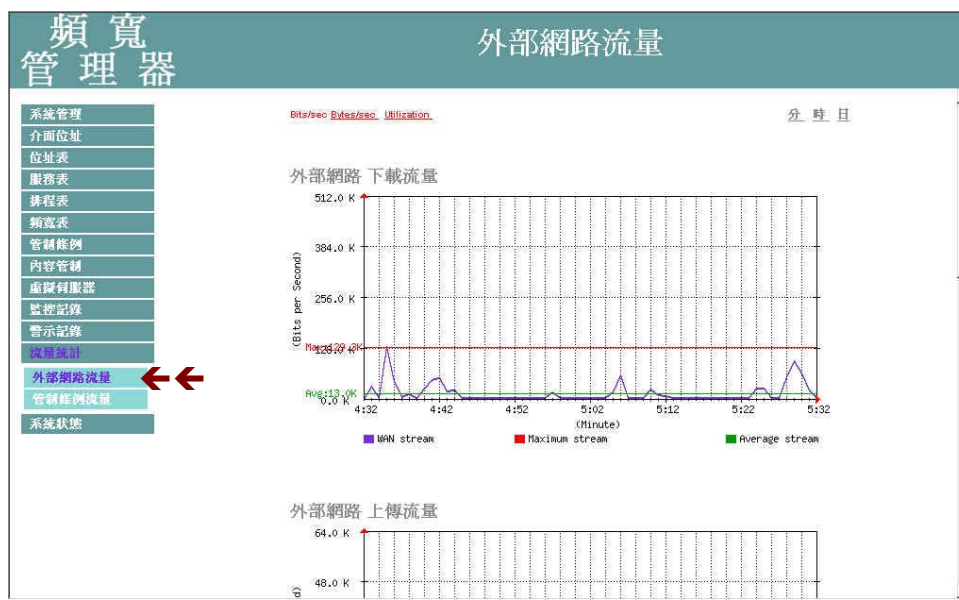


图 13-2 检视外部网络流量统计

## 管制条例流量

### 管制条例流量功能

本功能即为符合【管制条例】内设定的封包记录所产生该管制条例的统计资料



來源位址	目的位址	服務名稱	管制動作	時間
Inside_Any	Outside_Any	ANY	PERMIT	5 時 日

图 13-3 管制条例流量功能

流量统计窗口，表格内数值显现目前系统联机流量。

- 来源/目的 地址：来源/目的 端网络地址。
- 服务名称：服务项目名称。
- 管制动作：来源端网络地址、目的端网络地址进出频宽管理器资料封包的准许与拒绝动作。
- 时间：检视分别以分、时、日为时间单位的流量统计。



若欲使用【管制条例流量】，系统管理员须先至【管制条例】功能设定中，在指定的网络地址，激活【流量统计】功能。

## 检视管制条例流量

步驟1. 在【管制条例流量】窗口中，找到欲检视的网络区域名称，对应至右方【检视】栏：点选【分】，可检视以每分钟（min）为单位的流量统计图表；点选【时】，可检视以每小时(hour)为单位的流量统计图表；点选【日】，可检视以日（day）为单位的流量统计图表。

步驟2. 流量统计图表（如图 13-4）

- 纵坐标：网络流量（Kbytes/Sec）。
- 横坐标：时间（时/分/日）。

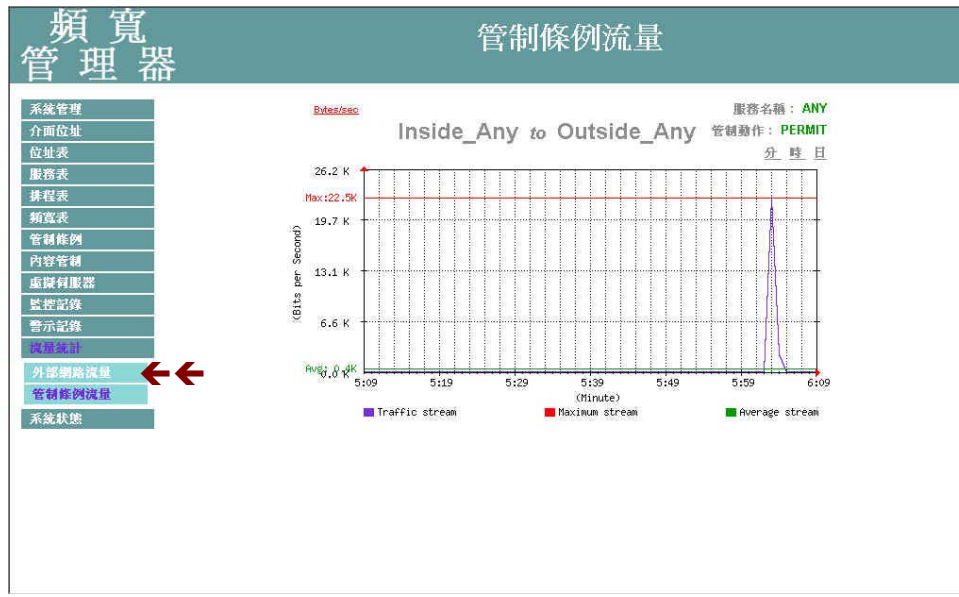


图 13-4 检视管制条例流量

# 系统状态

使用者可随时由系统状态中，得知目前网络联机，如局域网络与外部网络的 IP 地址、子网掩码、预设网关、DNS 服务器联机 IP 地址等各项信息。

(一) **【接口地址】**：目前网络服务器所设的接口地址信息。

(二) **【ARP 表】**：将网卡的 MAC 地址转译为 IP 地址。

(三) **【DHCP 用户表】**：记录 DHCP 用户 IP 地址与 MAC 地址及其租约时间等信息。



## 接口状态

### 接口状态功能

目前频宽管理器所设定的 内部网络/外部网络 接口地址信息。

	內部網路介面位址	外部網路介面位址
系統模式	NAT	PPPoE 設定
PPPoE 連線狀態	---	連線
PPPoE 連線時間	---	2:51:13
MAC位址	44:44:44:44:44:47	44:44:44:44:44:48
IP位址	192.168.1.1	61.59.145.60
子網路掩碼	255.255.255.0	255.255.255.255
預設網橋	---	61.59.145.1
DNS伺服器1	---	139.175.55.244
DNS伺服器2	---	139.175.252.16
接收封包數, 錯誤封包數	14202, 0	42954, 0
傳送封包數, 錯誤封包數	15124, 0	11968, 0
Ping	開啟	開啟
WebUI	開啟	開啟

图 14-1 接口状态功能

内部网络接口地址 (Internal Interface)

【接口状态】窗口内，显现目前系统联机之接口地址。

- 系统开机历时：频宽管理器开机历时时间。
- 系统模式：显示所使用的为 **NAT 模式** 或 **Transparent 模式**
- MAC 地址：网络卡识别号码。
- IP 地址/子网掩码：内部网络 IP 地址/内部网络子网掩码。
- 接收封包数, 错误封包数：显示接收封包数,显示接收错误封包数。
- 传送封包数, 错误封包数：显示传送封包数,显示传送错误封包数。
- Ping, WebUI,:

显示 Ping 到频宽管理器外部网络接口地址功能使用状态。

显示 WebUI 外部网络接口地址联机至频宽管理器功能使用状态。

外部网络接口地址 (ADSL 拨接/固接 专线使用者或缆线调制解调器使用者)

- 系统模式：显示你的外部网络联机模式。
- 联机状态：显示你的外部网络联机状态。
- 联机时间：显示你的外部网络联机时间。
- MAC 地址：网络卡识别号码。
- IP 地址/子网掩码：外部网络 IP 地址/外部网络子网掩码。
- 预设网关：显示外部通讯闸的地址。
- 接收封包数, 错误封包数：显示接收封包数,显示接收错误封包数。
- 传送封包数, 错误封包数：显示传送封包数,显示传送错误封包数。
- DNS 服务器 1：显示目前所使用的 DNS 服务器 1。
- DNS 服务器 2：显示目前所使用的 DNS 服务器 2。
- Ping, WebUI,：  
显示 Ping 到频宽管理器外部网络接口地址功能使用状态,  
显示 WebUI 外部网络接口地址联机至频宽管理器功能使用状态,

## ARP 表

显示网卡的 MAC 地址转译为 IP 地址的对照表。

IP 位址	MAC 位址	介面位址
192.168.1.3	00:50:BF:16:EA:CE	內部網路

图 14-3 ARP 表

【ARP 表】工作窗口内表格名词定义：

- IP 地址：内部网络 IP 地址。
- MAC 地址：网络卡识别号码。
- 接口地址：内部网络 IP 地址所属之接口地址。

## DHCP 用户表

记录 DHCP 用户 IP 地址与 MAC 地址及其租约时间等信息。

系統管理	IP 位址	MAC 位址	租用時間	
			起始	結束
介面位址	192.168.1.3	00:50:bf:16:ea:ce	2002/5/1 6:23:46	2002/5/2 6:23:46
位址表				
服務表				
排程表				
頻寬表				
管制權例				
內容管制				
虛擬伺服器				
監控記錄				
警告記錄				
流量統計				
系統狀態				
介面狀態				
ARP 表				
DHCP 用戶表				

图 14-4 DHCP 用户表

【DHCP 用户表】工作窗口内表格名词定义：

- IP 地址：动态 IP 地址。
- MAC 地址：连接动态 IP 地址的 MAC 地址。
- 租用时间：动态地址租用的(起始时间 / 结束时间)  
(年/月/日/时/分/秒)。

# 操作范例

## 内部至外部管制条例

以【管制条例】的制定流程为范例，让内部网络的所有 IP 地址都可以联机到网际网络。

- 步驟1. 在左方的功能选项中，点选【管制条例】功能，再点选【内部至外部】次功能选项。
- 步驟2. 在【内部至外部】窗口中，点选【新增】功能按钮。
- 步驟3. 在出现的【新增管制条例】窗口中，键入相关参数 (如图 ex1-1)
- 步驟4. 点选屏幕下方【确定】按钮，新增指定的内部网络。

頻寬管理器		內部至外部	
系統管理	新增管制條例	來源網路位址	Inside_Any
介面位址		目的網路位址	Outside_Any
位址表		服務名稱	ANY
服務表		管制動作	允許
排程表		流量監控	<input type="checkbox"/> 開啓
頻寬表		流量統計	<input type="checkbox"/> 開啓
管制條例		自動排程	None
內部至外部		最高流量警示值	0.0 KBytes/Sec
外線至內部		頻寬管理	None
內容管制			確定 取消
虛擬伺服器			
監控記錄			
警示記錄			
流量統計			
系統狀態			

图 ex1-1 新增内部至外部管制条例

## 管制条例与地址表应用

本范例让公司内部的 IP 地址只能连到 kimo 的网站的操作说明，制定流程为【地址表】至【管制条例】。

步驟1. 在左方的功能选项中，点选【地址表】功能，再点选【外部网络】次功能选项。

步驟2. 点选【新增】外部网络地址功能按钮。

步驟3. 在新窗口中，键入新外部网络各项参数值。（如图 ex2-1）

步驟4. 点选屏幕下方【确定】按钮，新增指定外部网络。

新增位址	
名稱	007
IP	202.1.237.23
子網路遮罩	255.255.255.255
<input type="button" value="確定"/> <input type="button" value="取消"/>	

图 ex2-1 新增外部网络地址

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】窗口中，點選【新增】功能按鈕。

步驟7. 在出現的【新增管制條例】窗口中，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。

頻寬管理器		內部至外部	
系統管理	新增管制條例	來源網路位址	Inside_Any
介面位址		目的網路位址	007
位址表		服務名稱	ANY
服務表		管制動作	允許
排程表		流量監控	<input type="checkbox"/> 開啓
頻寬表		流量統計	<input type="checkbox"/> 開啓
管制條例		自動排程	None
內部至外部		最高流量警示值	0.0 KBytes/Sec
外部至內部		頻寬管理	None
內容管制			
虛擬伺服器			
監控記錄			
警告記錄			
流量統計			
系統狀態			

圖 ex2-2 新增內部至外部管制條例

## 虚拟服务器设定

本范例将以使用【IP对映】来制定【外部至内部】网络，达到将服务器架在公司内部(Internal区)，现在要使外界的使用者，透过IP对应来使用服务器的功能。其制定流程为由【虚拟服务器】至【管制条例】。

- 步驟1. 在左方的功能选项中，点选【虚拟服务器】功能，再点选【IP对映】次功能选项。
- 步驟2. 在IP对映窗口中，点选【新增】功能按钮。
- 步驟3. 在出现的新增IP对映窗口中，键入相关参数 (如图 ex3-1)
- 步驟4. 点选屏幕下方【确定】按钮，新增指定的IP对映。



图 ex3-1 新增 IP 对映



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】窗口中，點選【新增】功能按鈕。



图 ex3-3 管制条例的外部至内部窗口

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



图 ex3-4 新增管制条例

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



图 ex3-5 开放所有服务项目

## 架设服务器于内部网络

本范例将公司的服务器放在【内部网络】，开放给内部和外部所有 I P 地址使用，来制定【管制条例】。其制定流程为由【虚拟服务器】至【管制条例】。

- 步驟1. 在左方的功能选项中，点选【虚拟服务器】功能，再点选【虚拟服务器 1】次功能选项。进入【虚拟服务器 1】工作窗口。(如图ex4-1)
- 步驟2. 点选屏幕上方的【选择】控制按钮。

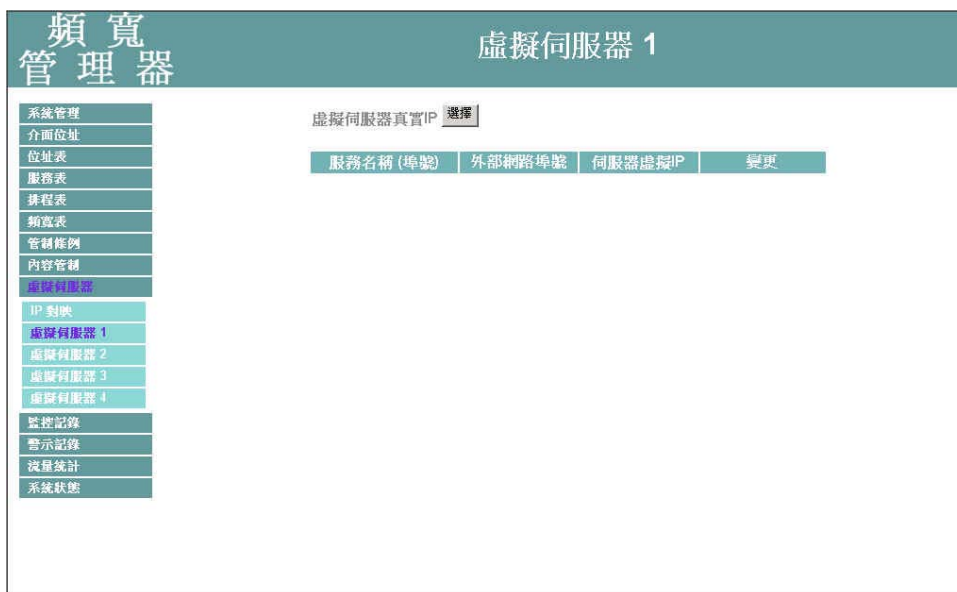


图 ex4-1 进入虚拟服务器窗口

步驟3. 在【新增虚拟服务器 IP】窗口中，选择虚拟服务器 IP 地址后，点选下方【确定】按钮。(如图 ex4-2)



图 ex4-2 新增虚拟服务器

步驟4. 新增虚拟服务器 IP 后，再接着点选屏幕下方的【新增】控制按钮。(如图 ex4-3)

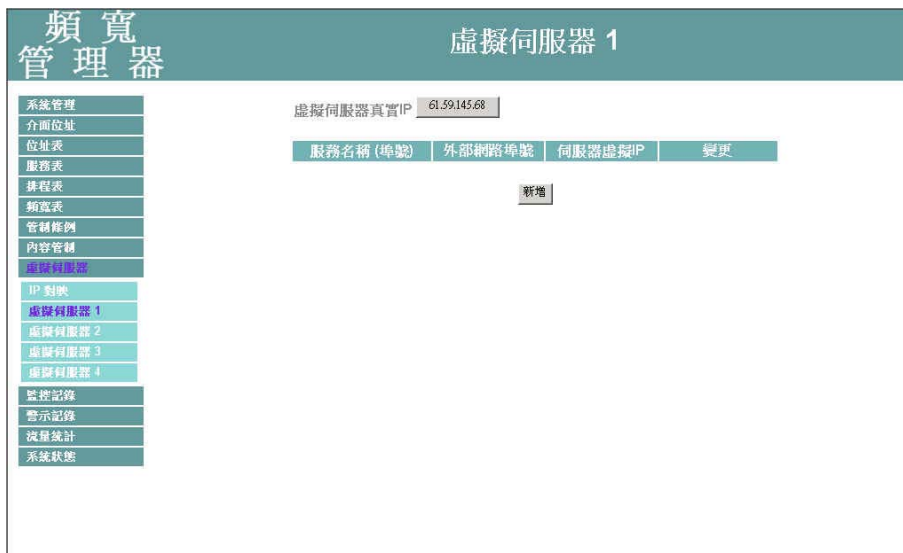


图 ex4-3 新增虚拟服务器服务设定

步驟5. 依照服务器所提供的服务项目，设定好各项参数后，按【确定】。  
(如图 ex4-4)

頻寬管理器 虛擬伺服器 1

系統管理  
介面位址  
位址表  
服務表  
排程表  
頻寬表  
管制條例  
內容管制  
虛擬伺服器  
IP 對映  
虛擬伺服器 1  
虛擬伺服器 2  
虛擬伺服器 3  
虛擬伺服器 4  
監聽記錄  
警示記錄  
流量統計  
系統狀態

虛擬伺服器組態

虛擬伺服器真實IP 61.59.145.68  
服務名稱 (埠號) ANY (0-65535)  
外部網路埠號 0-65535

負載平衡伺服器	伺服器虛擬IP
1	
2	
3	
4	

確定 取消

图 ex4-4 设定虚拟服务器

步驟6. 出现下列画面，即表示【虚拟服务器 1】部分设定完成。(如图 ex4-5)

頻寬管理器 虛擬伺服器 1

系統管理  
介面位址  
位址表  
服務表  
排程表  
頻寬表  
管制條例  
內容管制  
虛擬伺服器  
IP 對映  
虛擬伺服器 1  
虛擬伺服器 2  
虛擬伺服器 3  
虛擬伺服器 4  
監聽記錄  
警示記錄  
流量統計  
系統狀態

虛擬伺服器真實IP 61.59.145.68

服務名稱 (埠號)	外部網路埠號	伺服器虛擬IP	變更
FTP (21)	21	192.168.1.2	修改 刪除

新增

图 ex4-5 完成虚拟服务器设定

步驟7. 再到【管制條例】里的【外部至內部】工作窗口。(如圖 ex4-7)

步驟8. 點選屏幕下方的【新增】控制按鈕。



圖 ex4-7 進入管制條例之外部至內部窗口

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

## 设定频宽表于内部网络

本范例将以使用【频宽表】来制定【内部至外部】网络，达到最佳设定使用上传/下载频宽。其制定流程为由【频宽表】至【管制条例】。

- 步驟1. 在左方的功能选项中，点选【频宽表】功能。
- 步驟2. 在频宽表窗口中，点选【新增】功能按钮。
- 步驟3. 在出现的新增频宽表窗口中，键入相关参数 (如图 ex5-1)
- 步驟4. 点选屏幕下方【确定】按钮，新增频宽表。

頻寬管理器		頻寬表	
系統管理	新增頻寬表	名稱	384
介面位址	下載頻寬	保證頻寬	200 kbps
位址表		最大頻寬	300 kbps
服務表	上傳頻寬	保證頻寬	60 kbps
排程表		最大頻寬	100 kbps
頻寬表	優先權		中
管制條例			確定 取消
內容管制			
虛擬伺服器			
監控記錄			
警告記錄			
流量統計			
系統狀態			

图 ex5-1 新增频宽表



步驟5. 出現以下畫面，表示完成頻寬表的設定。(如圖 ex5-2)

頻寬管理器		頻寬表			
名稱	下載頻寬	上傳頻寬	優先權	變更	
384	G Bandwidth = 200 Kbps M Bandwidth = 300 Kbps	G Bandwidth = 80 Kbps M Bandwidth = 64 Kbps	Middle	修改 刪除	

新增

圖 ex5-2 新增頻寬表

步驟6. 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 ex5-3)

步驟7. 在【內部至外部】窗口中，點選【新增】功能按鈕。

頻寬管理器		內部至外部			
<p>編製來源網路目的網路服務名稱管制動作監控功能變更移動</p> <p>新增</p>					

圖 ex5-3 管制條例的內部至外部窗口

步驟8. 在出現的【新增管制條例】窗口中，鍵入相關參數後，點選【確定】執行新增。（*如圖 ex5-4*）

圖 ex5-4 新增管制條例

步驟9. 開放所有的服務項目（A N Y），設定頻寬表及完成。（*如圖 ex5-5*）

圖 ex5-5 完成頻寬表所有服務項目

## 设定频宽表于外部网络

本范例将公司的服务器放在【内部网络】，开放给内部和外部所有 I P 地址使用，以使用【频宽表】来制定【管制条例】达到最佳设定使用上传/下载频宽。其制定流程为由【频宽表】【虚拟服务器】至【管制条例】。

步驟1. 在左方的功能选项中，点选【频宽表】功能。

步驟2. 在频宽表窗口中，点选【新增】功能按钮。

步驟3. 在出现的新增频宽表窗口中，键入相关参数 (如图 ex6-1)

步驟4. 点选屏幕下方【确定】按钮，新增频宽表。

The screenshot shows the '頻寬管理器' (Bandwidth Manager) interface. On the left is a navigation menu with options: 系統管理, 介面位址, 位址表, 服務表, 排程表, 頻寬表 (highlighted), 管制條例, 內容管制, 虛擬伺服器, 監控記錄, 警告記錄, 流量統計, 系統狀態. The main area is titled '頻寬表' and contains a '新增頻寬表' (Add Bandwidth Table) form. The form has the following fields:

新增頻寬表			
名稱	<input type="text" value="384"/>		
下載頻寬	保證頻寬	<input type="text" value="200"/>	kbps
	最大頻寬	<input type="text" value="300"/>	kbps
上傳頻寬	保證頻寬	<input type="text" value="60"/>	kbps
	最大頻寬	<input type="text" value="100"/>	kbps
優先權	<input type="text" value="中"/>		
			<input type="button" value="確定"/> <input type="button" value="取消"/>

图 ex6-1 新增频宽表

步驟5. 出現以下畫面，表示完成頻寬表的設定。(如圖 ex6-2)

The screenshot shows the '頻寬管理器' (Bandwidth Manager) interface. On the left is a navigation menu with options like '系統管理', '介面位址', '位址表', '服務表', '排程表', '頻寬表', '管制條例', '內容管制', '虛擬伺服器', '監控記錄', '警告記錄', '流量統計', and '系統狀態'. The main area is titled '頻寬表' and contains a table with the following data:

名稱	下載頻寬	上傳頻寬	優先權	變更
384	G Bandwidth = 200 Kbps M Bandwidth = 300 Kbps	G Bandwidth = 80 Kbps M Bandwidth = 64 Kbps	Middle	修改 刪除

Below the table is a '新增' (Add) button.

圖 ex6-2 新增頻寬表

步驟6. 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】工作窗口。(如圖 ex6-3)

步驟7. 點選螢幕上方的【選擇】控制按鈕。

The screenshot shows the '頻寬管理器' (Bandwidth Manager) interface for '虛擬伺服器 1' (Virtual Server 1). The left navigation menu is the same as in the previous screenshot, but '虛擬伺服器' is highlighted. The main area is titled '虛擬伺服器 1' and contains a '選擇' (Select) button for '虛擬伺服器真實IP'. Below this is a table with the following columns:

服務名稱 (埠號)	外部網路埠號	伺服器虛擬IP	變更
-----------	--------	---------	----

图 ex6-3 进入虚拟服务器窗口

步驟8. 在【新增虚拟服务器 IP】窗口中，选择虚拟服务器 IP 地址后，点选下方【确定】按钮。(如图 ex6-4)



图 ex6-4 新增虚拟服务器

步驟9. 新增虚拟服务器 IP 后，再接着点选屏幕下方的【新增】控制按钮。(如图 ex6-5)

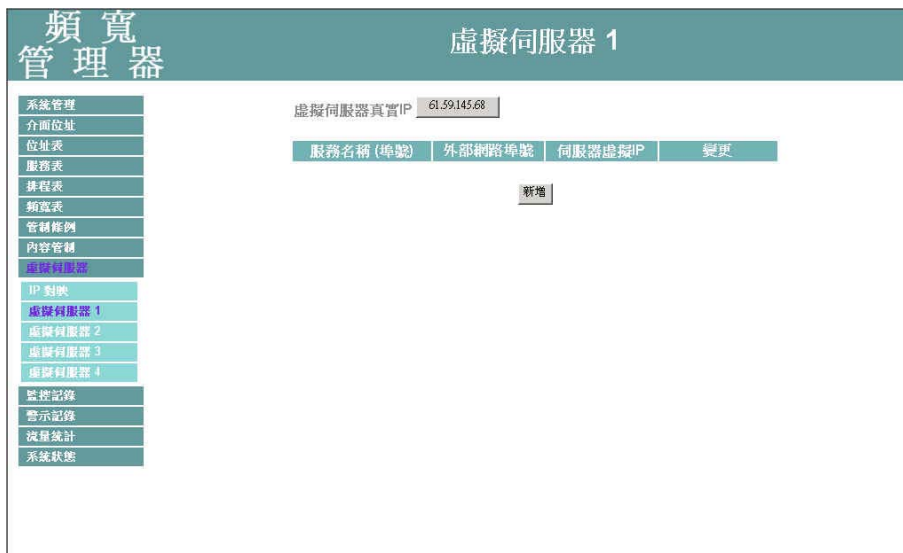


图 ex6-5 新增虚拟服务器服务设定

步驟**10**. 依照服务器所提供的服务项目，设定好各项参数后，按【确定】。  
(如图 ex6-6)

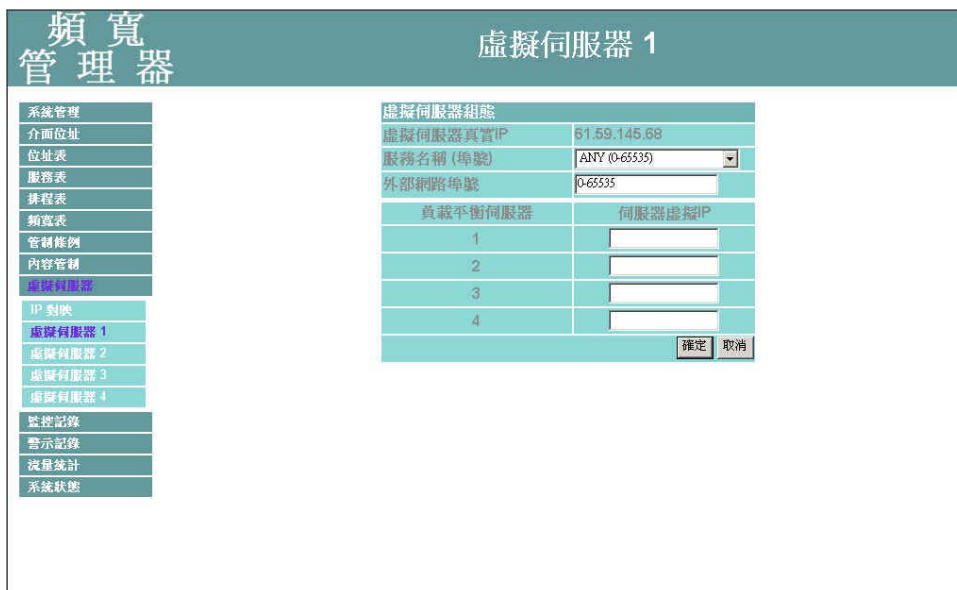


图 ex6-6 设定虚拟服务器

步驟**11**. 出现下列画面，即表示【虚拟服务器 1】部分设定完成。(如图 ex6-7)



图 ex6-7 完成虚拟服务器设定

步驟12. 再到【管制條例】里的【外部至內部】工作窗口。(如图 ex6-8)

步驟13. 点选屏幕下方的【新增】控制按钮。



图 ex6-8 进入管制条例之外部至内部窗口

步驟14. 在【新增管制条例】设定各项参数，完成后按【确定】。(如图 ex6-9)



图 ex6-9 新增频宽表管制条例