Bandwidth Management

使 用 手 册

目　　录

频宽管理器硬件安装

一、 频宽管理器硬件外部接口说明：

图 H-1 频宽管理器接口、指示灯说明

- **Power LED** : 电源显示
- **Status LED**：当 LED 灯为开始闪烁时，表示系统正在开机状态，约一分钟后系统开机程序结束，当 LED 停止闪烁，表示系统已开机成功。
- **RESET**：将频宽管理器回复到原厂默认值。
- **WAN**：外部网络接口，与外部路由器连结。
- **LAN**：内部网络接口，与内部计算机连结。

二、 Transparent Mode 频宽管理器连接图：

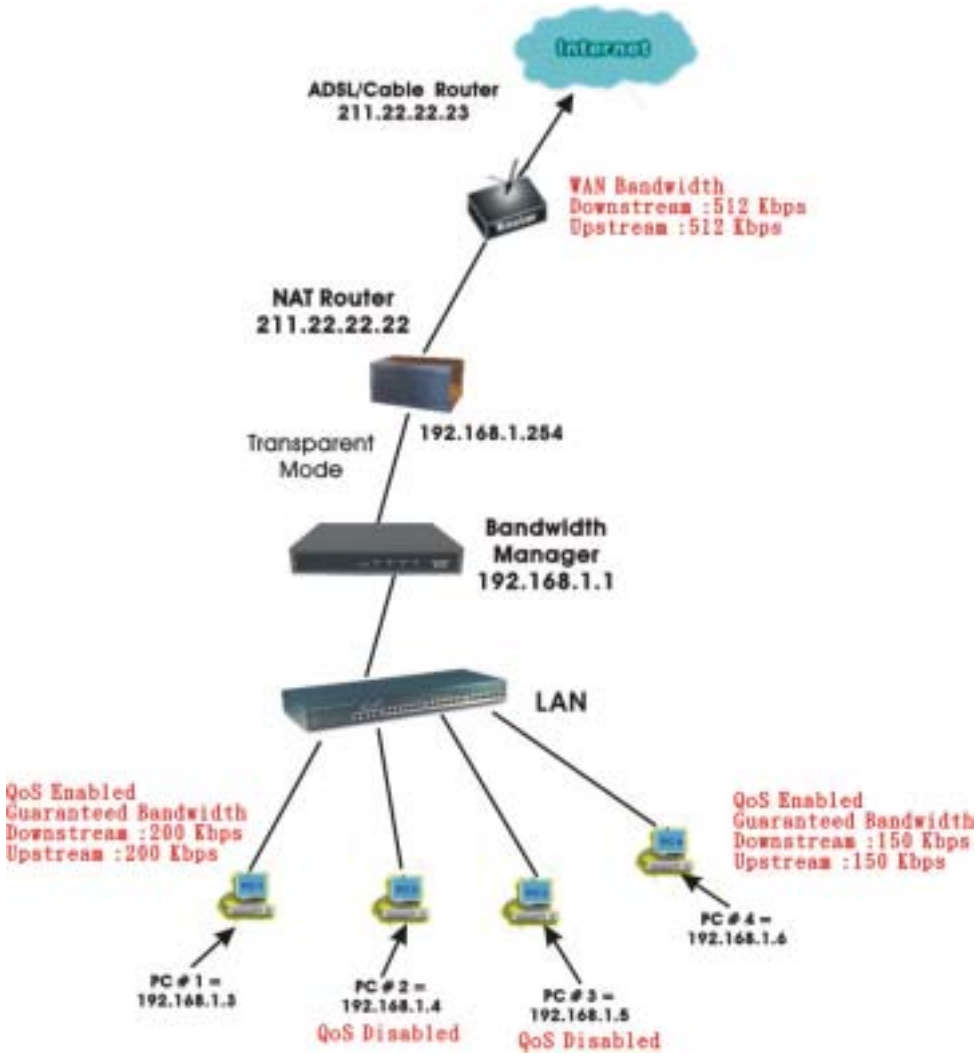


图 H-2 Transparent Mode 频宽管理器连接图

■ **频宽管理器 ：**

内部端口【LAN Port】= **192.168.1.1**

外部端口【WAN Port】= **192.168.1.1**

三、 NAT Mode 频宽管理器连接图：

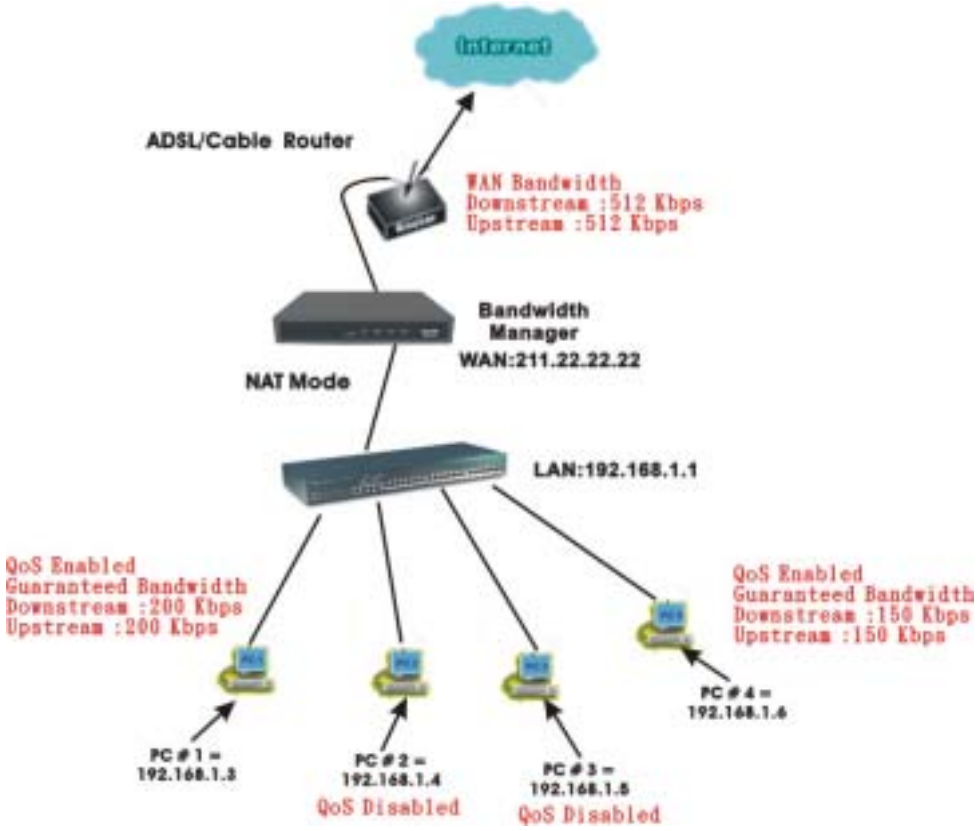


图 H-3 NAT Mode 频宽管理器连接图

■ **频宽管理器 ：**

内部端口【LAN Port】= **192.168.1.1**

外部端口【WAN Port】= **211.22.22.22**

频宽管理器软件安装

步驟1. 首先将系统管理员的计算机和频宽管理器内部适配卡接到同一个 HUB 或 Switch，再使用浏览器（IE 或 Netscape）连结至频宽管理器。频宽管理器 Internal port 的 IP 地址内定值为 http://192.168.1.1，所以远程计算机的 IP 地址必须是 192.168.1.2 至 192.168.1.254 其中之一，子网掩码为 255.255.255.0。

步驟2. 设定新环境的 内部网络接口地址（配合公司的环境），外部网络接口地址 (由 ISP 网络公司分配)。如果新设定的 内部网络接口地址 不属于 192.168.1.0 网络，例如新 内部网络接口地址 为 172.16.0.1，管理员必须更改计算机端的 IP 地址为：172.16.0.2，或其它相同子网络的 IP 地址，此时管理员的计算机或许须重新开机，新的 IP 地址才能生效。

步驟3. 当管理员的计算机和频宽管理器的内部网络接口地址 属于 192.168.1.0 网段的网络，开启浏览器（IE 或 Netscape）连结至 http://192.168.1.1 。连上频宽管理器的 WebUI，即可开始使用浏览器设定频宽管理器的参数。

下列表格为标准虚拟 IP 地址范围，不可使用外部真实 IP 地址。

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

步驟4. 浏览器会询问使用者名称及密码，输入管理员名称与密码。*（如图S-1）*

- 使用者名称：admin
- 密码：admin
- 点选【确定】

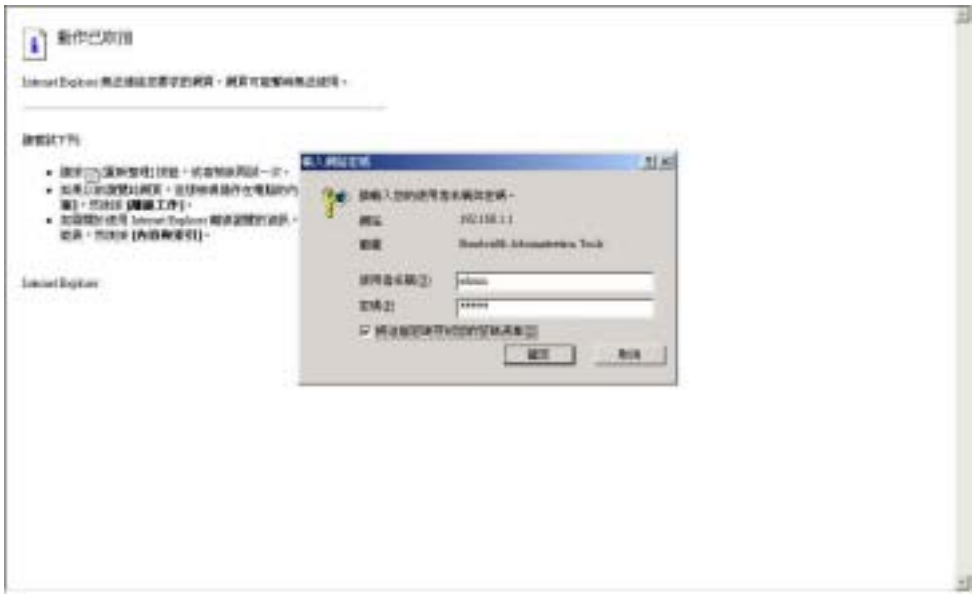


图 S-1　键入使用者名称与密码

Transparent Mode 设定安装

步骤1. 进入频宽管理器软件系统主画面后，在左方的功能选项中，点选【接口地址】功能选项。 *(如图 S-2)*

- 点选 Transparent 模式
- 键入所设定的 IP 地址，NetMask，预设网关及 DNS 服务器等相关讯息

系统接口地址	IP Address	192.168.1.1
	NetMask	255.255.255.0
	Default Gateway	192.168.1.254
	DNS Server 1	168.95.1.1

图 S-2 键入 Transparent Mode 相关 IP 地址

步驟2. 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3. 点选屏幕下方的【新增管制条例】功能按钮。 *（如图 S-3）*

步驟4. 在出现的【新增管制条例】窗口中，键入下列相关参数：

- 来源网络：选择【Inside Any】
- 目的网络：选择【Outside Any】
- 网络名称：选择【ANY】
- 管制动作：选择【允许】

图 S-3 至管制条例功能设定来源网络与目的网络

步驟5. 看到*图S-4* 画面即表示安装成功。最后将企业内部所有计算机的 IP 地址须设定与频宽管理器的内部网络接口同一个网域，而预设网关则要设定为 192.168.1.254，或将内部的计算机设为自动取得 IP，企业内部网络可马上连结至网际网络存取资料，如欲使用频宽管理器的管制功能，请在【地址表】和【管制条例】功能项增加相关设定值。

图 S-4　安装设定成功画面

NAT Mode 设定安装

步骤1. 进入频宽管理器软件系统主画面后，在左方的功能选项中，点选【接口地址】功能选项。 *（如图S-5）*

- 内部网络接口地址：
  IP 地址：192.168.1.1
  子网掩码：255.255.255.0
- 外部网络接口地址：
  IP 地址：211.22.22.22
  子网掩码：255.255.255.0
  预设网关：211.22.22.254
  DNS 服务器 1：168.95.1.1

图 S-5 键入内部网络 IP 地址与子网掩码

如果新的内部网络接口地址不是 192.168.1.1，点选【OK】后，在浏览器网址字段输入新的内部网络接口地址，再重新连结频宽管理器。

步驟2. 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3. 点选屏幕下方的【新增管制条例】功能按钮。 *（如图 S-6）*

步驟4. 在出现的【新增管制条例】窗口中，键入下列相关参数：

- 来源网络：选择【Inside Any】
- 目的网络：选择【Outside Any】
- 网络名称：选择【ANY】
- 管制动作：选择【允许】

图 S-6　至管制条例功能设定来源网络与目的网络

步驟5. 看到*图S-7*画面即表示安装成功。最后将企业内部所有计算机的 IP 地址须设定为频宽管理器内部网络接口的同一个网域与预设网关设定为频宽管理器内部网络接口，或将内部的计算机设为自动取得 IP，企业内部网络可马上连结至网际网络存取资料，如欲使用频宽管理器的管制功能，请在【地址表】和【管制条例】功能项增加相关设定值。

图 S-7　安装设定成功画面

第一章

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理员设定。系统主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【到频宽管理器封包】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】：本软件提供繁体中文、简体中文与英文三种语言版本，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 Subnet】：内部网络可支持多个区段的网络地址。

【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。

【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。

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

【DNS 代理服务器】：系统管理员可利用此 DNS 代理服务器功能，指定公司内部服务器的网域名称对应到内部计算机或服务器的 IP 地址。

【DDNS】：可让浮动 IP 使用者做实时更新 DNS 与 IP 对映的功能。

【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。

频宽管理器之【管理员】功能设定

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

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（可读/写）与次管理员（只读）。
- 变更：管理员之组态设定。点选表格下方【修改】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。
- 系统主管理员：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。

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。

步驟2. 在【新增管理员】窗口中，键入以下资料：*(如图1-2)*

- 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 1-2 新增次管理员

变更主/次管理员密码

步骤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】。

步骤2. 在【修改管理员密码】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1-3)*

步骤3. 点选【确认】修改密码，或点选【取消】取消变更设定。

图 1-3 变更管理员密码

删除次管理员

步骤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】。

步骤2. 屏幕上会立即产生【删除管理员】的确认对话框。*（如图1-4）*

步骤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

步驟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)*

图 1-5 【系统管理】功能之【系统设定】工作窗口

汇出频宽管理器组态设定档

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【汇出系统组态文件至客户端】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 选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。

步驟1. 在【系统设定】窗口中，点选【频宽管理器组态】下【从客户端汇入系统组态文件】右方的【浏览】功能按钮。

步驟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)*

步驟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【恢复至出厂设定值】。

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【恢复至出厂设定值】

设定实时警讯通知

步驟1. 勾选【**E-Mail 设定**】下之【开启电子邮件警讯通知】。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。）

步驟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。

步驟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。

步驟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。

步驟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。

步驟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

步驟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

设定 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端口号。

步驟1. **设定 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端口号。*(如图1-10)*

图 1-10 设定 Web 管理

认证管理

提供系统管理员在设定内部使用者到外部网络使用认证管理时所设定的认证时所需输入的端口号及认证时间。(需先行设定认证表)

认证管理工作窗口名词定义：*(如图1-11)*

认证端口号：当内部使用者到外部网络时,闲置超过设定的时间,产生离线,当需要重新对外部网络进行联机时,需要重新输入认证的帐号跟密码所使用的端口号。

允许联机闲置：当内部使用者到外部网络,设定联机闲置的时间,超过设定的时间,即刻产生离线作用。

图 1-11 认证管理

设定 MTU

提供系统管理员在任何时候改变频宽管理器的进出封包长度。

步驟1. **MTU 设定**。输入需要改变的封包长度。*(如图1-12)*

图 1-12 设定 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

步驟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1-13）*

图 1-13 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. 频宽管理器将被重新激活：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1-14)*

图 1-14 重新激活频宽管理器

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。*(如图 1-15)*

勾选【开启与外部时间服务器同步】。

步驟1. 可点选下拉式选单设定与 GMT 相差时间(以小时为单位)。

步驟2. 可输入外部时间服务器网络地址。

步驟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 1-15 系统时间设定

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*（如图1-16）*

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． 点选【确定】更换软件的语言版本，或点选【取消】取消设定。

图 1-16 频宽管理器软件语言版本设定

管理地址功能设定

可让系统管理者设定仅允许的 内 / 外 部网络地址，来进行频宽管理器的管理设定。*（如图1-17）*

图 1-17 管理地址

新增管理地址

步驟1. 点选下方【新增】功能按钮。

步驟2. 在新增管理地址窗口中，键入内部或外部 IP 地址。 *（如图1-18）*

- IP 地址：键入 内 / 外 部网络之 IP 地址。
- 子网掩码：键入 内 / 外 部网络的子网掩码。
- 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. 点选【确定】新增管理地址，或【取消】取消新增。

图 1-18 新增管理地址

变更管理地址

步驟1. 在【管理地址】的表格中，找到欲变更设定的 IP 地址，对应至右方【变更】栏，点选【修改】。

步驟2. 在【修改管理地址】窗口中，键入新的 IP 地址。 *（如图 1-19）*

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 1-19 变更管理地址

移除管理地址

步驟1. 在【管理地址】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 1-20）*

图 1-20 移除管理地址

NAT 模式

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 192.168.1.1/24(Internal) ←→ 168.85.88.253(External)
2.客服部网段 192.168.2.1/24(Internal) ←→ 168.85.88.252(External)
3.业务部网段 192.168.3.1/24(Internal) ←→ 168.85.88.251(External)
4.采购部网段 192.168.4.1/24(Internal) ←→ 168.85.88.250(External)
5.会计室网段 192.168.5.1/24(Internal) ←→ 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 Subnet，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 Subnet 的 NAT 模式功能。

步驟1. 于左方功能选项，先点选【系统管理】，接着点选下方的【Multiple Subnet】，进入【Multiple Subnet】工作窗口。*(如图 1-21)。*

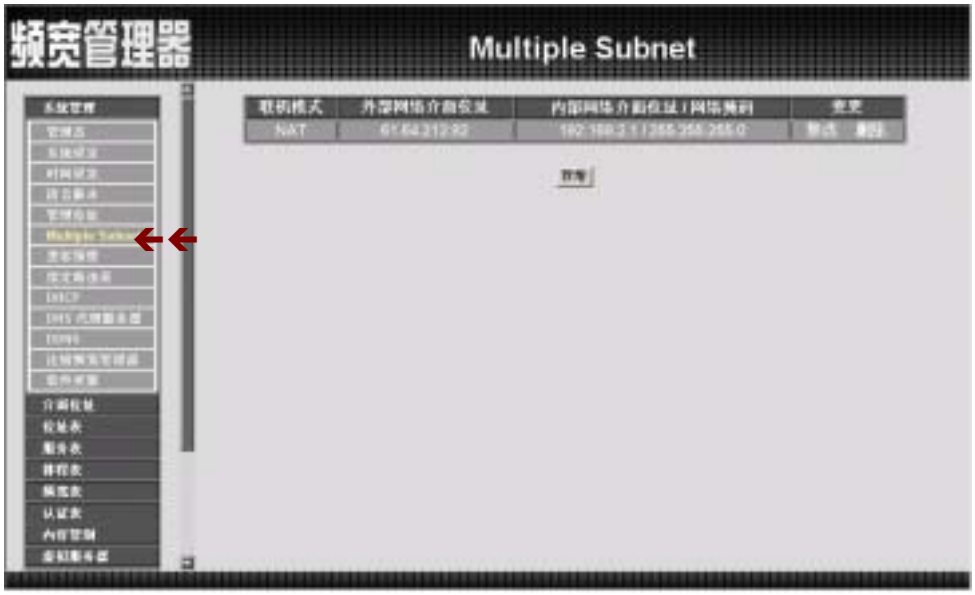


图 1-21 进入 Multiple Subnet NAT 模式功能设定

步驟2. Multiple Subnet 工作窗口名词定义：

- 联机模式：显示目前是使用 NAT 模式或是 Routing 模式。
- 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 Multiple Subnet 中各项设定值。点选【修改】，可修改 Multiple Subnet 各项参数；点选【删除】，可删除该项设定。

新增 Multiple Subnet NAT 模式

步驟1. 点选下方【新增】Multiple Subnet 功能按钮。

步驟2. 在新增 Multiple Subnet 窗口中，键入 IP 地址。 *(如图 1-22)。*

- 联机模式：选择联机模式 NAT 模式。
- 外部网络接口地址：选择外部网络之 IP 地址。
- 内部网络接口地址：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. 点选【确定】新增 Multiple Subnet，或【取消】取消新增。

图 1-22 新增 Multiple Subnet NAT 模式

变更 Multiple Subnet NAT 模式

步驟1. 在【Multiple Subnet】的表格中，找到欲变更设定的 IP 地址，对应至右方【变更】栏，点选【修改】。

步驟2. 在【修改 Multiple Subnet】窗口中，键入新的 IP 地址。 *（如图1-23）。*

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。

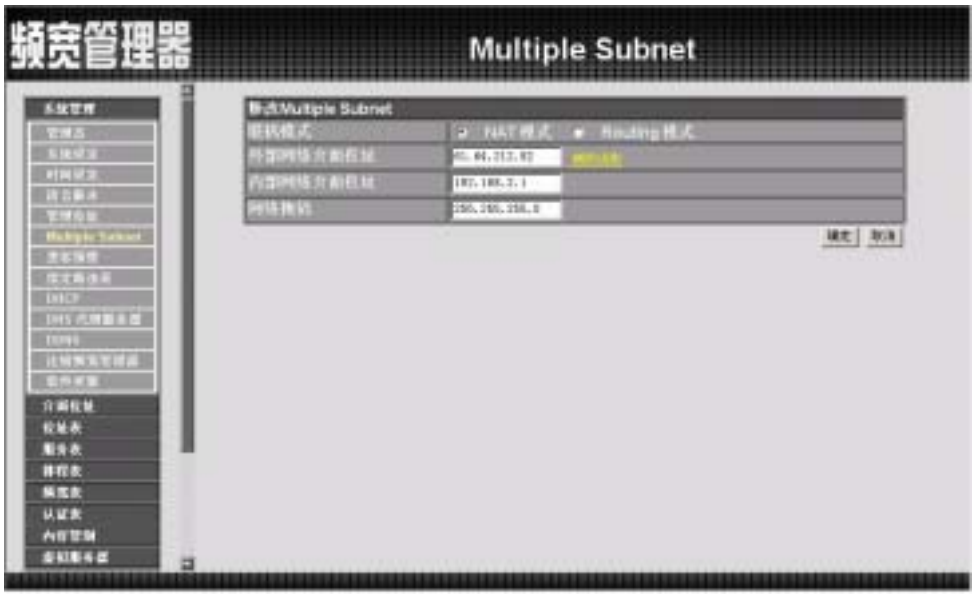


图 1-23 变更 Multiple Subnet NAT 模式

移除 Multiple Subnet NAT 模式

步驟1. 在【Multiple Subnet】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】。

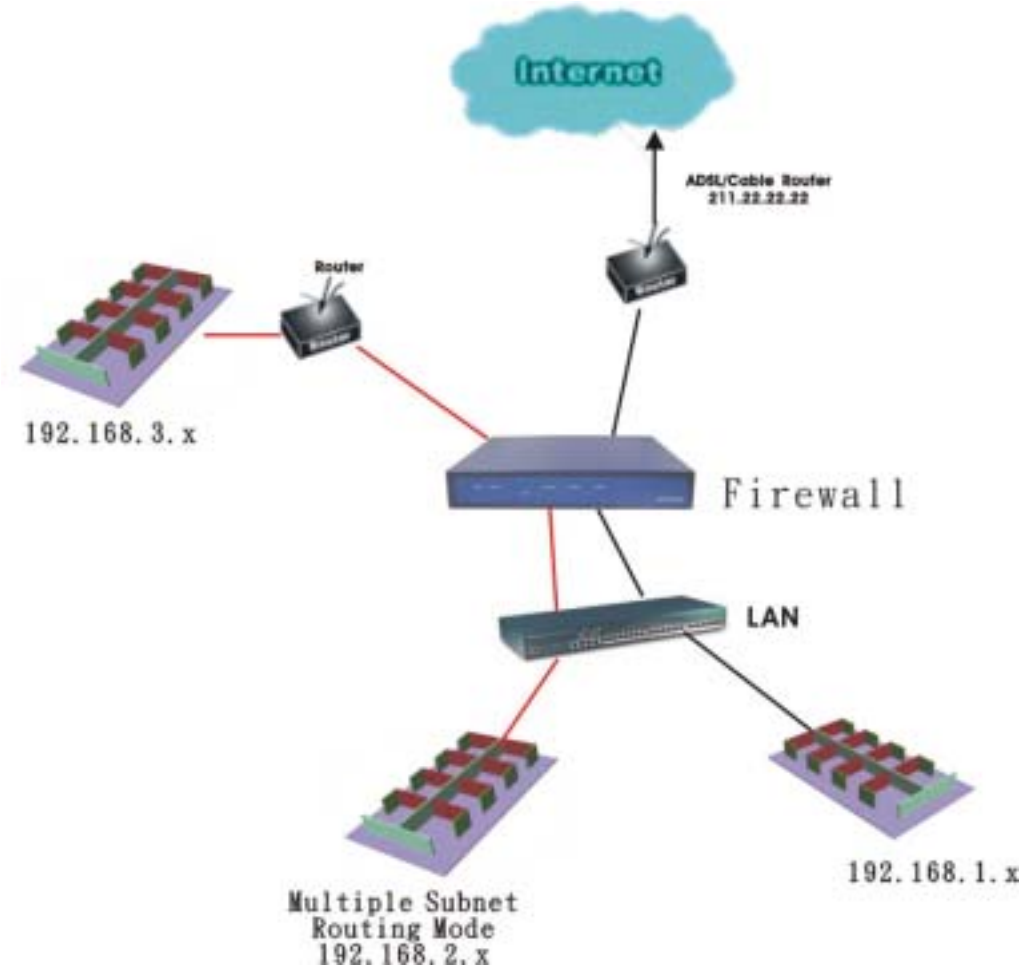
步驟2. 在【确定删除】对话框中，点选【确定】按钮，移除设定，或 点选【取消】取消移除。 *（如图 1-24）。*

图 1-24 移除 Multiple Subnet NAT 模式

Routing 模式

可让公司网络在设定 Multiple Subnet Routing 模式时,连接不同网段地址,并经由不同的网段地址来建立联机沟通。

例如：公司的申请专线拥有多个 IP 地址 192.168.2.0/24，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，和不同的 IP 区段进行联机,设定 Multiple Subnet Routing 可方便整合各部门信息,。



设定方式如下：

步驟1. 于左方功能选项，先点选【系统组态】，接着点选下方的【Multiple Subnet】，进入【Multiple Subnet】工作窗口。*(如图 1-25)。*

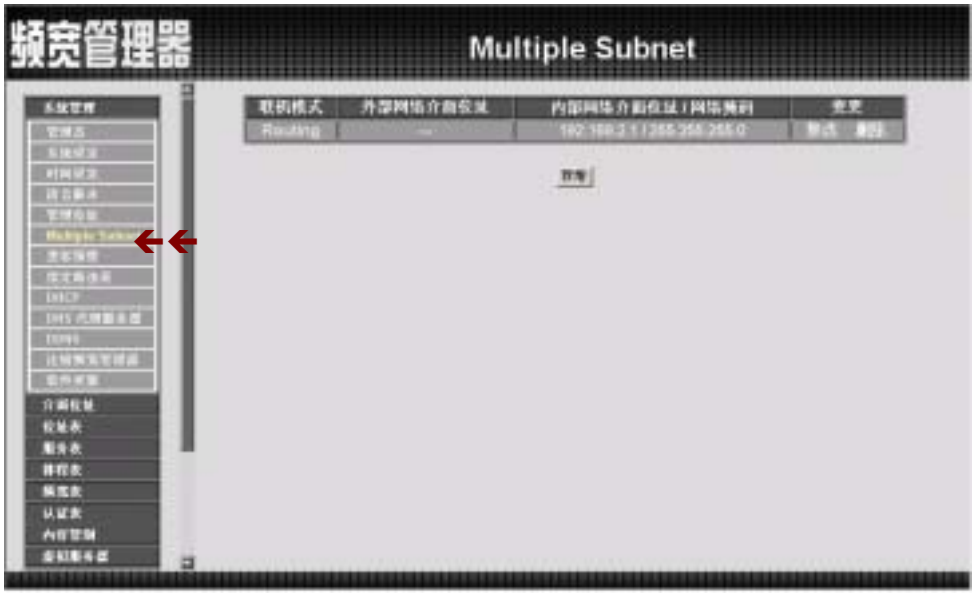


图 1-25 进入 Multiple Subnet Routing 模式功能设定

步驟2. Multiple Subnet 工作窗口名词定义：

- 联机模式：显示目前是使用 NAT 模式或是 Routing 模式。
- 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 Multiple Subnet 中各项设定值。点选【修改】，可修改 Multiple Subnet 各项参数；点选【删除】，可删除该项设定。

新增 Multiple Subnet Routing 模式

步驟1. 点选下方【新增】Multiple Subnet 功能按钮。

步驟2. 在新增 Multiple Subnet 窗口中，键入 IP 地址。 *(如图 1-26)。*

- 联机模式：选择联机模式 Routing 模式。
- 外部网络接口地址：选择外部网络之 IP 地址。
- 内部网络接口地址：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. 点选【确定】新增 Multiple Subnet，或【取消】取消新增。

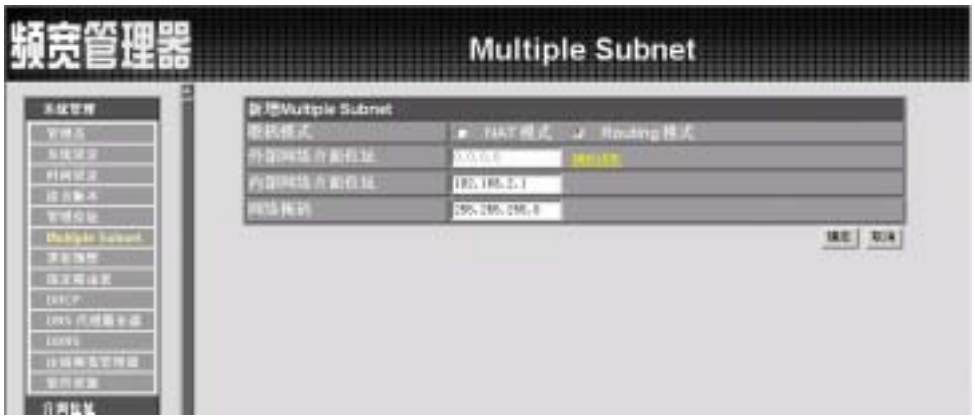


图 1-26 新增 Multiple Subnet Routing 模式

步驟4. 新增外部至内部管制条例， 在【外部至内部】窗口中，点选【新增】管制条例功能按钮。新增外部至内部管制条例 (如下图)

变更 Multiple Subnet Routing 模式

步驟1. 在【Multiple Subnet】的表格中，找到欲变更设定的 IP 地址，对应至右方【变更】栏，点选【修改】。

步驟2. 在【修改 Multiple Subnet】窗口中，键入新的 IP 地址。 *（如图1-27）。*

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。

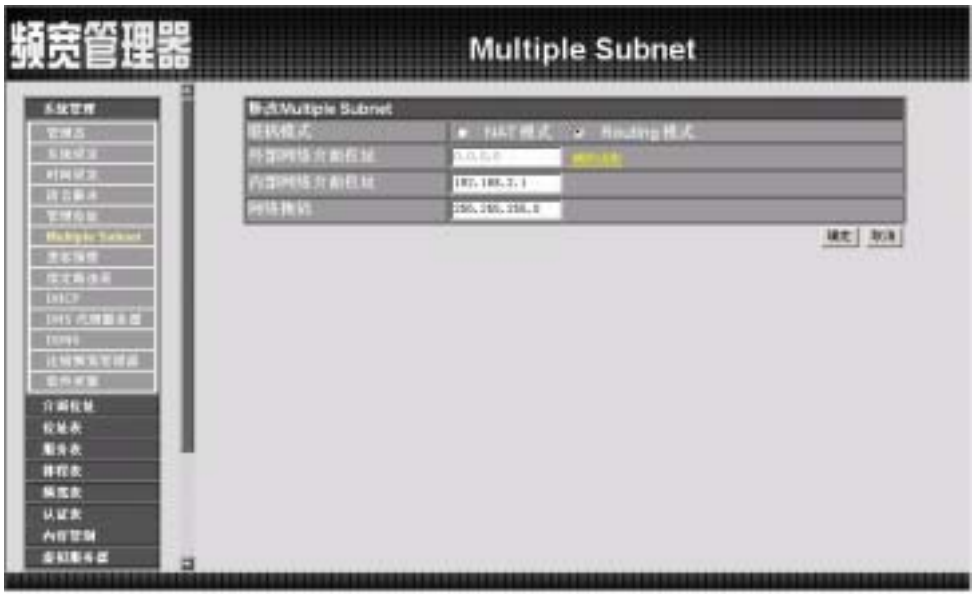


图 1-27 变更 Multiple Subnet Routing 模式

移除 Multiple Subnet Routing 模式

步驟1. 在【Multiple Subnet】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 1-28）。*

图 1-28 移除 Multiple Subnet Routing 模式

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。

步驟1. 【骇客预警】各项侦测功能说明 *（如图1-29）*

图 1-29 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瞄侦测服务器开放的端口号（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。如果攻击者送出制订的封包，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地址，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地址与目的地址相同，来源端口号与目的端口号相同，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。

步驟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】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。*（如图 1-30）*

图 1-30 【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，为内部网络或外部网络。
- 目的地址：连结目的网域之 IP 地址。
- 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地址、子网掩码、网关地址等资料。*（如图1-31）*

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. 点选【确定】新增所指定的网络网关，或点选【取消】取消设定。

图 1-31 新增指定路由网关

变更指定路由表中的网络网关设定

步骤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】。

步骤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。

步骤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1-32）*

图 1-32 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】。*（如图1-33）*

步驟2. 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 1-33 删除指定路由表中的网关设定

DHCP 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】。

步驟1. 于左方功能选项，先点选【系统管理】，接着点选下方的【DHCP】，进入【DHCP】工作窗口。*(如图1-34)*

图 1-34 DHCP 设定

步驟2. DHCP 设定信息：

- 子网络 ：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 DHCP 功能

步驟1. 勾选【激活 DHCP 服务器】。并键入下列信息 *(如图 1-35)*

激活 DHCP 服务器：可选择是否激活 DHCP 服务器。

- 网域名称：键入内部私有网域名称。

自动取得 DNS：选择是否自动取得 DNS 服务器。

- 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）
- 租用时间：为动态 IP 的设定租用时间。

步驟2. 点选【确定】执行 DHCP 支持功能，或【取消】取消激活 DHCP 功能。

图 1-35 激活 DHCP 功能

DNS 代理服务器功能设定

当使用者自行架设服务器，且已申请合法网域名称，为使内部网络计算机可使用该网域名称来连接此服务器，必须先于此功能中将网域名称对映至该服务器在频宽管理器后的虚拟 IP 地址。且内部网络计算机必须将其 DNS 服务器设定值定义为在频宽管理器【系统管理】接口地址中的「内部网络接口ＩＰ地址」。

步驟1. 于左方功能选项，先点选【系统管理】，接着点选下方的【DNS 代理服务器】，进入【DNS 代理服务器】工作窗口。*（如图 1-36）*

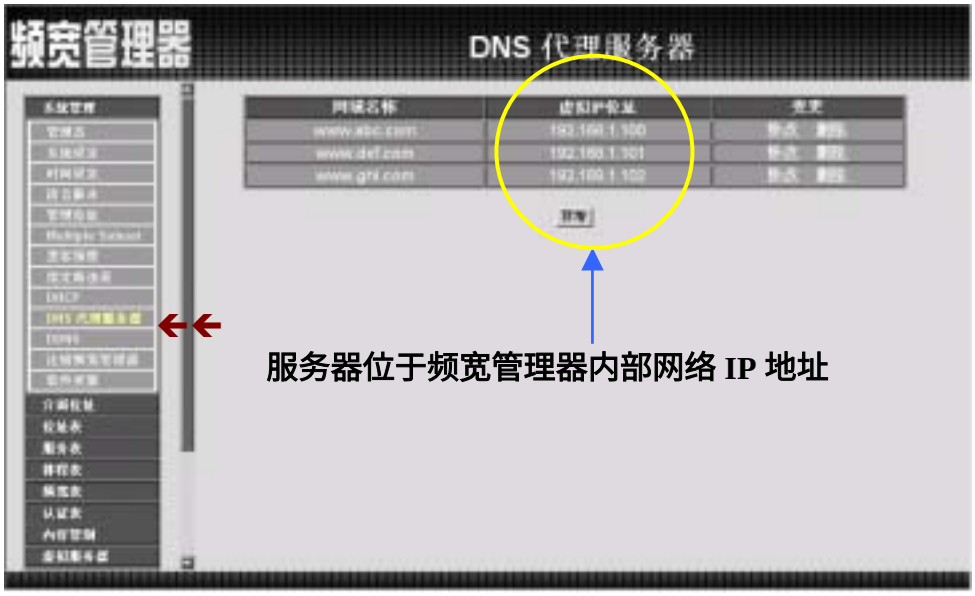


图 1-36 DNS 代理服务器功能

DNS 代理服务器设定信息：

- 网域名称：内部内计算机的网域名称地址。
- 虚拟 IP 地址：该网域名称所对映之内部虚拟 IP 地址。
- 变更：变更 DNS 代理服务器中各项设定值。点选【修改】，可修改 DNS 代理服务器各项参数；点选【删除】，可删除该项设定。

要使用频宽管理器的 DNS 服务器功能，使用者 PC 端的第一个（主）DNS 服务器一定要指向频宽管理器的 IP，也就是计算机端所设定的预设网关（Gateway）。

新增 DNS 代理服务器

步驟1. 点选下方【新增】DNS 代理服务器功能按钮。

步驟2. 在【新增 DNS 代理服务器】窗口中，键入相关参数。 *(如图 1-37)*

- 网域名称：键入网域名称。
- 虚拟 IP 地址 ： 键入该网域名称所对映之虚拟 IP 地址。

步驟3. 点选【确定】新增 DNS 代理服务器，或【取消】取消新增。

图 1-37 新增 DNS 代理服务器

变更 DNS 代理服务器

步骤1. 在【DNS 代理服务器】的表格中，找到欲变更设定的网域名称，对应至右方【变更】栏，点选【修改】。

步骤2. 在【修改 DNS 代理服务器】窗口中，键入各项欲变更参数。*（如图 1-38）*

步骤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 1-38 变更 DNS 代理服务器

删除 DNS 代理服务器

步驟1. 在【DNS 代理服务器】的表格中，找到欲删除设定的网域名称，对应至右方【变更】栏，点选【删除】。

步驟2. 在【确定删除】DNS 代理服务器对话框中，点选【确定】按钮，删除设定，或 点选【取消】取消删除。 *(如图1-39)*

图 1-39 删除 DNS 代理服务器

DDNS 功能设定

设定 DDNS，可让使用浮动 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【DDNS】，进入【DDNS】工作窗口。*(如图 1-40)*

图 1-40 DDNS 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；联机时间逾时，更新失败；更新成功；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. DDNS 使用方法：

频宽管理器里提供十一家的服务厂商，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【DDNS】，进入【DDNS】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 1-41）*

图 1-41 DDNS 功能设定

新增 DDNS

步驟1. 点选下方【新增】动态 DNS 功能按钮。

步驟2. 在新增动态 DNS 窗口空栏中，键入相关信息。 *（如图 1-42）*

- 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，注册办法请自行参阅网站说明。
- 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：申请时所注册的名称及网域。

步驟3. 点选【确定】新增动态 DNS，或【取消】取消新增。

图 1-42 新增 DDNS

变更 DDNS

步驟1. 在【DDNS】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 1-43）*

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。

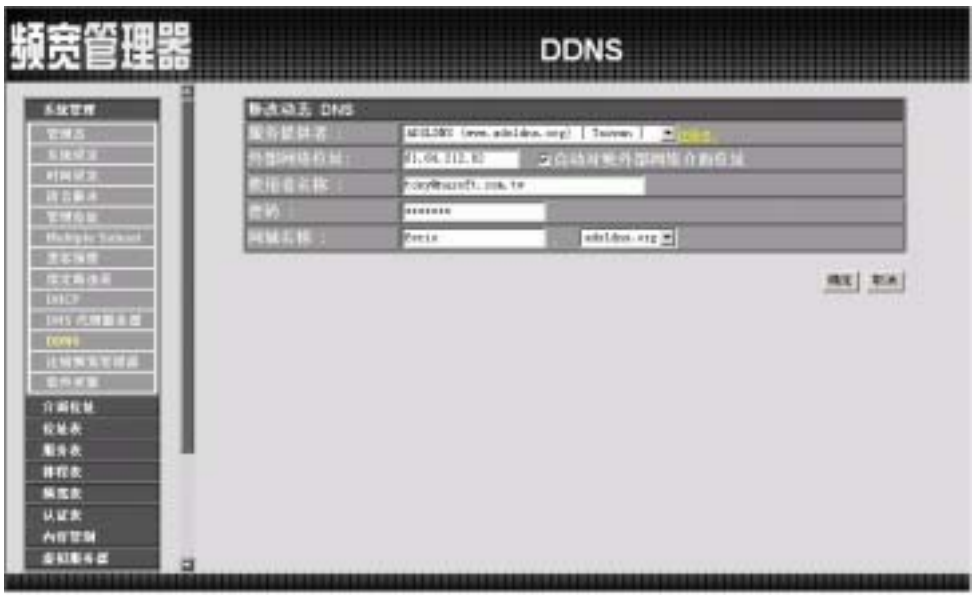


图 1-43 变更 DDNS

移除 DDNS

步驟1. 在【DDNS】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 1-44）*

图 1-44 移除 DDNS

注销频宽管理器设定

为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。

步驟1. 于左方功能选项，先点选【系统管理】，接着点选下方的【注销频宽管理器】功能。*(如图1-45)。*

步驟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 1-45 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 PC 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1-46）*

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 1-46 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。

第二章

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和外部网络的 IP 地址、子网掩码、网关地址等接口地址。

键入内部网络之各项接口地址设定

NAT 模式

内部网络接口地址（Internal Interface）

- Transparent 模式：内部网络的 IP 地址均使用真实 IP。
- NAT 模式：内部网络的 IP 地址均使用 NAT 转址。
- IP 地址: 键入内部网络之 IP 地址。
- 子网掩码: 键入内部网络之子网掩码。
- Ping：勾选此项，激活频宽管理器允许内部网络所有接口地址 Ping。
- WebU1：勾选此项，则可藉由内部网络接口地址联机至频宽管理器设定画面。 *（如图 2-1）*

图 2-1 内部网络接口地址设定

ADSL 拨接使用者之接口地址设定

外部网络接口地址 PPPoE（External Interface）

勾选外部网络接口地址下方【PPPoE 设定(ADSL 拨接使用者)】。 *(如图2-2)。*

步驟1. 键入外部网络之各项接口地址设定：

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 30Mbps)
- 自动联机：勾选此项，当有封包到外部网络时，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。您可自行设定网络闲置时间，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。
- WebU1：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2. 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

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

步驟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 30Mbps)
- 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。

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)

步驟1. 勾选外部网络接口地址下方【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 30Mbps)
- 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。

图 2-4 指定 IP 地址(固接式或 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。

第三章

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)或目的地址(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。

地址表之【内部网络】功能

步骤1. 在左方的功能选项中，点选【地址表】功能，再点选【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

步骤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。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。

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

步骤1. 点选【新增】功能按钮。

步骤2. 在新窗口中，键入内部网络之网络地址名称、IP 地址、子网掩码、MAC 地址等各项参数值。 *（如图 3-2）*

步骤3. 勾选【从 DHCP 服务器取得固定 IP 地址】，可使此 MAC 地址每次皆取得同一 IP 地址。

步骤4. 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。

图 3-2 新增内部网络地址

若欲使用【从 DHCP 服务器取得固定 IP 地址】功能，必须先键入 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. 在出现的新增地址群组窗口中 *（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

步骤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】。

步骤2. 在出现的变更地址群组窗口中 *（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。

步骤3. 点选【确定】执行变更群组；或点选【取消】取消变更。

图 3-7 变更内部网络群组设定

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

外部网络功能设定

步骤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

步骤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 地址与子网掩码。
- 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

步骤1. 点选【新增】外部网络地址功能按钮。

步骤2. 在新视地址窗中，键入外部网络各项参数值。 *（如图3-10）*

步骤3. 点选屏幕下方【确定】按钮，新增外部网络地址，或点选【取消】取消设定。

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。

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

外部网络群组功能设定

步骤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）*

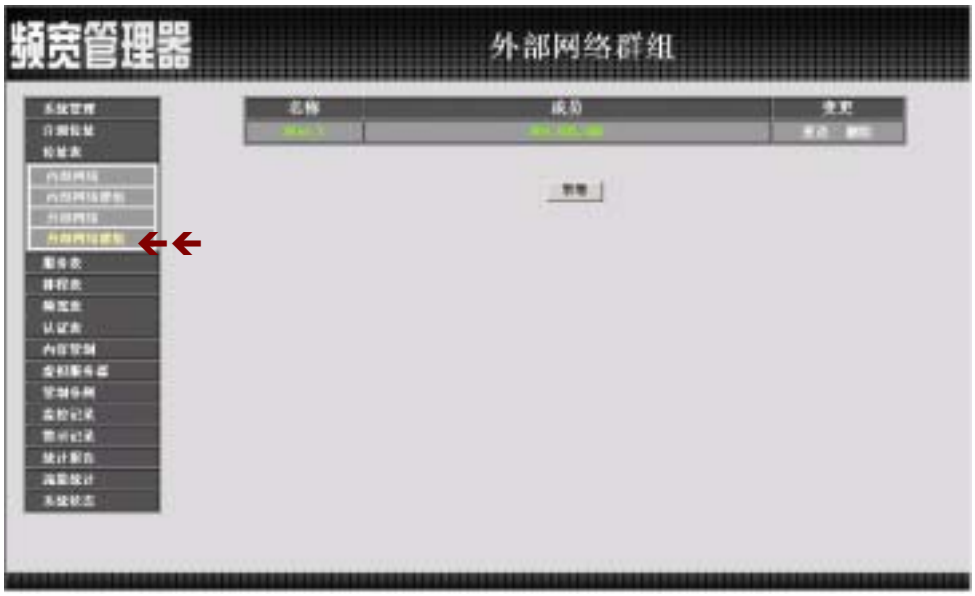


图 3-13 外部网络群组功能设定

步骤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，点选【新增】外部网络群组功能按钮。

步驟2. 在出现的新增地址群组窗口中 *(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，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。

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. 在出现的变更地址群组窗口中 *（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

第四章

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 ： 基本服务表和制订服务表，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制订服务表设定适当 TCP 端口和 UDP 端口号码。在制订服务时，客户端端口(Client Port)设定的区间预设为 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 10x5=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。

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

制订服务功能设定

步驟1. 在左方的功能选项中，点选【服务表】功能，再点选【自定服务】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端口范围。
  在客户端两个空格内输入的 port 号如为不同端口号，则是开启端口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 号如为相同端口号，则是开启端口号为同一个 port 号

- 服务器端：自定服务项目中之服务器端的出入端口范围。
  在服务器端两个空格内输入的 port 号如为不同端口号，则是开启端口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 号如为相同端口号，则是开启端口号为同一个 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. 在出现的新增自订服务窗口中 *（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端口范围。
  在客户端两个空格内输入的 port 号如为不同端口号，则是开启端口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 号如为相同端口号，则是开启端口号为同一个 port 号
- 服务器端：输入新服务之服务器端的出入端口范围。
  在服务器端两个空格内输入的 port 号如为不同端口号，则是开启端口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 号如为相同端口号，则是开启端口号为同一个 port 号

步驟3.　点选【确定】执行新增服务；或点选【取消】取消新增。

图 4-3 新增自订服务

变更制订服务

步驟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】。

步驟2. 在出现的变更制订群组窗口中 *（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端口范围。
  在客户端两个空格内输入的 port 号如为不同端口号，则是开启端口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 号如为相同端口号，则是开启端口号为同一个 port 号
- 服务器端：输入新服务之服务器端的出入端口范围。
  在服务器端两个空格内输入的 port 号如为不同端口号，则是开启端口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 号如为相同端口号，则是开启端口号为同一个 port 号

步驟3. 点选【确定】执行变更服务；或点选【取消】取消变更。

图 4-4 变更自订服务

移除制订服务

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. 在出现的变更服务群组窗口中 *（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

第五章

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】功能中，选择特定时间内开放资料封包的出入，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】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】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】中，移除该项设定，才可执行变更。。

新增排程表

步驟1. 点选【新增】功能按钮。

步驟2. 在出现的【新增排程】窗口中 *(如图 5-2)*

- 排程名称：输入新排程名称。
- 时段：在每周特定日期的表格内，于【起始时间】与【结束时间】的下拉选单中，点选有效执行的时间范围。

步驟3. 点选【确定】执行新增排程表；或点选【取消】取消新增。

图 5-2 新增排程表

制定排程表时，【起始时间】字段，必须小于【结束时间】字段，否则无法进行新增或修改的设定。

变更排程表

步驟1. 在【排程表】窗口中，找到欲变更设定的排程表名称，对应至右方【变更】栏，点选【修改】。

步驟2. 在出现的变更排程窗口中，键入新排程表名称，并设定排程表时间范围 *（如图5-3）*

步驟3. 点选【确定】执行变更；或点选【取消】取消变更。

图 5-3 变更排程表

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

第六章

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：变更频宽表中各项设定值。点选【修改】，可修改频宽表各项参数信息；点选【删除】，可删除该项设定。

新增频宽表功能

步驟1. 点选屏幕下方【新增】按钮，新增指定的频宽表。

步驟2. **新增频宽表**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. 点选屏幕右方【确定】按钮，新增指定的频宽表，或按【取消】钮取消新增频宽表。 *（如图 6-2）*

图 6-2 新增频宽表功能设定

修改频宽表功能

步骤1. 点选屏幕右方【变更】栏下的【修改】按钮，变更指定的频宽表。

步骤2. **修改频宽表**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。

步骤3. 点选屏幕右方【确定】按钮，变更指定的频宽表，或按【取消】钮取消变更频宽表。 *（如图 6-3）*

图 6-3 修改频宽表功能设定

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【变更】栏，点选【删除】。

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

第七章

认　证　表

频宽管理器经由认证表的设定，管理人员可设定控管内部网络使用者对外部网络的上网时闲置时间过长。当内部网络使用者需重新到外部网络联机时，所需要输入的认证帐号跟密码。

管理人员可依据内部网络使用者，来做设定认证帐号及密码,来确认内部使用者的权限。

认证使用者功能设定

步驟1． 在左方的功能选项中，点选【认证表】功能选项。*(如图7-1)*

图 7-1 认证表功能设定

步驟2． 认证表格说明

- 使用者名称：所设定认证表之使用者帐号。
- 变更：变更认证表中各项设定值。点选【修改】，可修改认证表各项参数信息；点选【删除】，可删除该项设定。

新增认证使用者功能

步驟1. 点选屏幕下方【新增使用者】按钮，新增指定的认证表。

步驟2. 新增使用者表格说明

- **使用者名称**：所设定认证表之使用者帐号。
- **密码**：建立认证时所需要的密码。
- **确认密码**：键入与上列密码栏一致的字符串。

步驟3. 点选屏幕右下方【确定】按钮，新增指定的认证表，或点选【取消】取消新增。 *(如图7-2)*

图 7-2 新增认证表使用者功能

此功能欲进行开启时须在【系统设定】表格中设定进行认证管理使用的认证端口号(预设:82)及当网络闲置允许联机闲置时间设定(预设:30 分钟)。*(如图7-3)*

图 7-3 认证管理设定画面

将【内部至外部】表格内管制条例，设定【勾选】认证，将认证功能开启。*(如图7-4)*

图 7-4 管制调例认证功能设定画面

当联机闲置时间超过频宽管理器所设定的时间,内部网络使用者重新进行联机时,频宽管理器会进行使用者登入画面，进行认证。完成认证即可进行重新联机。
（如图7-5）

认证使用者登入表格说明：

- 使用者名称：使用者进行认证时的帐号
- 密码：输入进行认证的密码

图 7-5 认证使用者登入画面

修改认证使用者功能

步驟1. 点选屏幕右方【变更】栏之【修改】按钮，变更指定的认证表。

步驟2. **认证使用者**表格说明

- **使用者名称**：所设定认证表之使用者帐号。
- **密码**：显示原认证时的密码。
- **新密码**：输入新修改的密码。
- **确认密码**：键入与上列新密码栏一致的字符串。

步驟3. 点选屏幕右方【确定】按钮，变更指定的认证表，或点选【取消】取消变更。 *（如图7-6）*

图 7-6 修改认证使用者功能

删除认证使用者功能设定

步驟1. 在【认证表】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【删除】。

步驟2. 在【删除认证使用者】确定对话框中，点选【确定】按钮，删除设定，或点选【取消】取消删除。 *(如图7-7)*

图 7-7 删除认证使用者功能设定

第八章

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【内容管制】，接着点选下方的【网站管制】次功能选项，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。
- 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，必须先将全部禁止指令移除，再键入新网域名称，完成后，再重新加入全部禁止指令。

新增网站管制

步驟1. 点选下方【新增】网站管制功能按钮。

步驟2. 在新增网站管制窗口的网站名称空栏中，键入欲管制进入的网址或关键词。 *（如图 8-2）*

步驟3. 点选【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。 *（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

一般管制功能设定

于左方功能选项，先点选【内容管制】，接着点选下方的【一般管制】，进入【一般管制】工作窗口。

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档。

第九章

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 地址可对映到四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」是一对一对映，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即由与虚拟服务器的 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. 在出现的新增对映 IP 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。
- 辅助选取：可直接了解目前外部网络的 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。

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【修改对映 IP】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 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 1/2/3/4】次功能选项。 *（如图9-5）*

图 9-5 虚拟服务器功能设定

步驟2. 虚拟服务器窗口内名词定义说明：

- 虚拟服务器真实 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。
- 端口号 :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。

- 服务器虚拟 IP：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，【虚拟服务器真实 IP】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 IP 地址

步骤1. 在【虚拟服务器 1（或 2、3、4）】窗口中，点选【虚拟服务器真实 IP】右方的【选择】功能按钮。

步骤2. 在【新增虚拟服务器 IP】窗口，于【虚拟服务器真实 IP】右方的字段中键入可使用外部网络 IP 地址。*（如图 9-6）*

步骤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 新增虚拟服务器真实 IP

变更虚拟服务器 IP 地址

步骤1. 在【虚拟服务器 1（或 2、3、4）】窗口中，点选【虚拟服务器真实 IP】右方的【虚拟服务器 IP 地址】功能按钮。

步骤2. 在【新增虚拟服务器 IP】窗口，于【虚拟服务器真实 IP】右方的字段中键入可使用外部网络 IP 地址， 来变更 IP 地址。*(如图 9-7)*

步骤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 变更虚拟服务器真实 IP 地址

移除虚拟服务器 IP 地址

步骤1. 在【虚拟服务器 1（或 2、3、4）】窗口中，点选【虚拟服务器真实 IP】右方的【虚拟服务器 IP 地址】功能按钮。

步骤2. 在【新增虚拟服务器 IP】窗口，于【虚拟服务器真实 IP】右方的字段中，清除 IP 地址。*（如图9-8）*

步骤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 移除虚拟服务器真实 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。

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

- 虚拟服务器真实 IP：显示此虚拟服务器所设定的外部网络 IP 地址。
- 服务名称(端口号)：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。
- 外部网络端口号：此虚拟服务器所提供的服务项目的代码。
- 负载平衡服务器：服务器编号。
- 服务器虚拟 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，可达到负载平衡的功能。

新增虚拟服务器服务设定

步骤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。

步骤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

- 虚拟服务器真实 IP：显示此虚拟服务器所设定的外部网络 IP 地址。
- 服务名称(端口号)：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。
- 外部网络端口号：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。
- 服务器虚拟 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，可达到负载平衡的功能。

步骤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

步骤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】。

步骤2. 在【变更虚拟服务器】窗口，键入欲变更的参数值 *（如图 9-11）*

图 9-11 变更虚拟服务器服务设定

- 虚拟服务器真实 IP：显示此虚拟服务器所设定的外部网络 IP 地址。
- 服务名称(端口号)：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。
- 外部网络端口号：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。
- 服务器虚拟 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，可达到负载平衡的功能。

步骤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。

第十章

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网络地址、目的网络地址、服务名称、管制动作、流量监控、流量统计、认证、内容管制、自动排程、最高流量警示值及频宽管理等。系统管理员可以由这些参数，管理、设定不同出入端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两项，以便利系统主管理员，针对不同资料封包的来源 IP、来源端口、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，制订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，制订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：源网络地址、目的网络地址、服务名称、管制动作、流量监控、流量统计、认证、内容管制、自动排程、最高流量警示值及频宽管理。其中，来源网络地址和目的网络地址之 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端口号(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，制订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10-1）*

图 10-1 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，第三栏为认证表功能，第四栏为内容管制功能，第五栏为排程表功能，第六栏为流量警示功能，第七栏为频宽管理功能。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。
	流量监控	流量监控功能已开启。
	流量统计	流量统计功能已开启。
	认证	认证功能已开启。
	内容管制	内容管制功能已开启。
	自动排程	已激活排程表所制订时间范围内自动执行功能。
	最高流量警示	最高流量警示功能已开启。
	频宽管理	频宽管理功能已开启。

备注：

1. 检视系统之流量监控纪录  ，点选屏幕左方【监控功能】选项，系统使用与操作方式，请翻阅第十一章。
2. 检视系统之流量警示记录  ，点选屏幕左方【警示记录】选项，系统使用与操作方式，请翻阅第十二章。
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，请翻阅第十四章。
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。
6. 频宽管理器自动执行认证管理  ，修改认证管理，点选屏幕左方【认证表】选项，使用与操作方式，请翻阅第七章。
7. 频宽管理器自动执行内容管制管理  ，修改内容管制管理，点选屏幕左方【内容管制】选项，使用与操作方式，请翻阅第八章。

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10-2）*

图 10-2 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【外部网路】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【开启】，开启流量监控记录功能。
- 流量统计：勾选【开启】，开启流量统计功能。
- 认证：勾选【开启】，开启认证功能。
- 内容管制：勾选【开启】，开启内容管制功能。
- 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：点选已于【频宽表】设定之排程表名称，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. 点选屏幕右下方【确定】按钮，新增指定的内部至外部网络管制条例，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10-3）*

图 10-3 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【开启】，开启流量监控功能。
- 流量统计：勾选【开启】，开启流量统计功能。

- 认证：勾选【开启】，开启认证功能。
- 内容管制：勾选【开启】，开启内容管制功能。
- 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。
- 最高流量警示值功能：设定进出资料封包之最高流量（KBytes/Sec）警示值。
- 频宽管理：点选已于【频宽表】设定之排程表名称，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，变更指定的内部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 10-4）*

图 10-4 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

注 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九章。

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，制订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。

步驟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10-5）*

图 10-5 外部网络至内部网络管制条例功能设定

步驟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。
- 管制动作：指定外部网络、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、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。）
- 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。
	流量监控	流量监控功能已开启。
	流量统计	流量统计功能已开启。
	自动排程	已激活排程表所制订时间范围内自动执行功能。
	最高流量警	最高流量警示功能已开启。
	频宽管理	频宽管理功能已开启。

备注：

1. 检视系统之流量监控纪录  ，点选屏幕左方【监控功能】选项，系统使用与操作方式，请翻阅第十一章。
2. 检视系统之流量警示记录  ，点选屏幕左方【警示记录】选项，系统使用与操作方式，请翻阅第十二章。
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，请翻阅第十四章。
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。

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10-6）*

图 10-6 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（新增方法请详见第九章虚拟服务器），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（新增方法请详见第九章虚拟服务器），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 、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【开启】，开启流量监控功能。
- 流量统计：勾选【开启】，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。
- 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。
- 频宽管理：点选已于【频宽表】设定之排程表名称，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】执行新增指定的外部至内部网络管制条例；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 10-7）*

图 10-7 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【开启】，开启流量监控功能。
- 流量统计：勾选【开启】，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。
- 频宽管理：点选已于【频宽表】设定之排程表名称，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】执行变更指定的外部至内部网络管制条例；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【外部网络】；*
- *目的网络→【虚拟服务器】之【IP 对映】或【虚拟服务器 1/2/3/4】设定的对映 IP；*
- *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10-8）*

图 10-8 移除外部网络至内部网络管制条例

第十一章

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）【监控备份】：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。

流量监控功能

于左方功能选项，先点选【监控记录】，接着点选下方的【流量监控】，进入【流量监控】工作窗口。*(如图 11-1)*

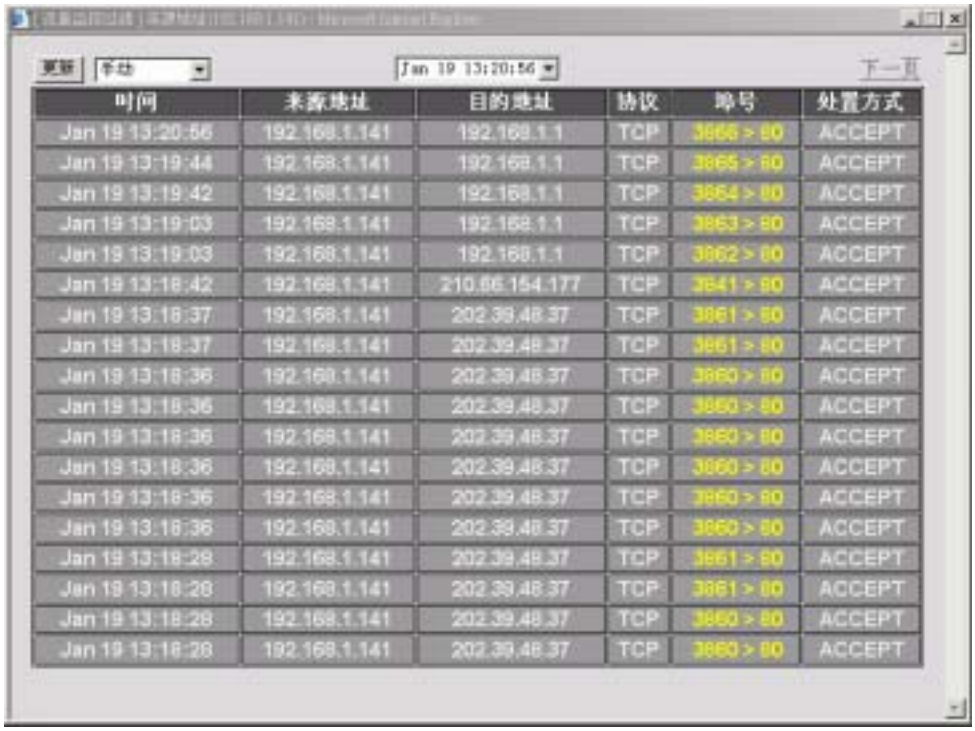
系统管理员可在流量监控记录里，查询目前进出频宽管理器各个联机状态，包括：联机起始时间、来源地址、目的地址与处置方式等。并每隔一段时间，将流量监控记录储存备份，再删除线上记录，让线上维持最新记录。

图 11-1 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【下一页】，检视其它联机时间之流量状态。点选【上一页】，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。
- 目的地址：目的端的 IP 地址。
- 协议与端口号：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。

点选来源地址时，频宽管理器会依来源地址过滤,并整理所有相关的流量监控资料,供 MIS 人员进行参考。*(如下图)*

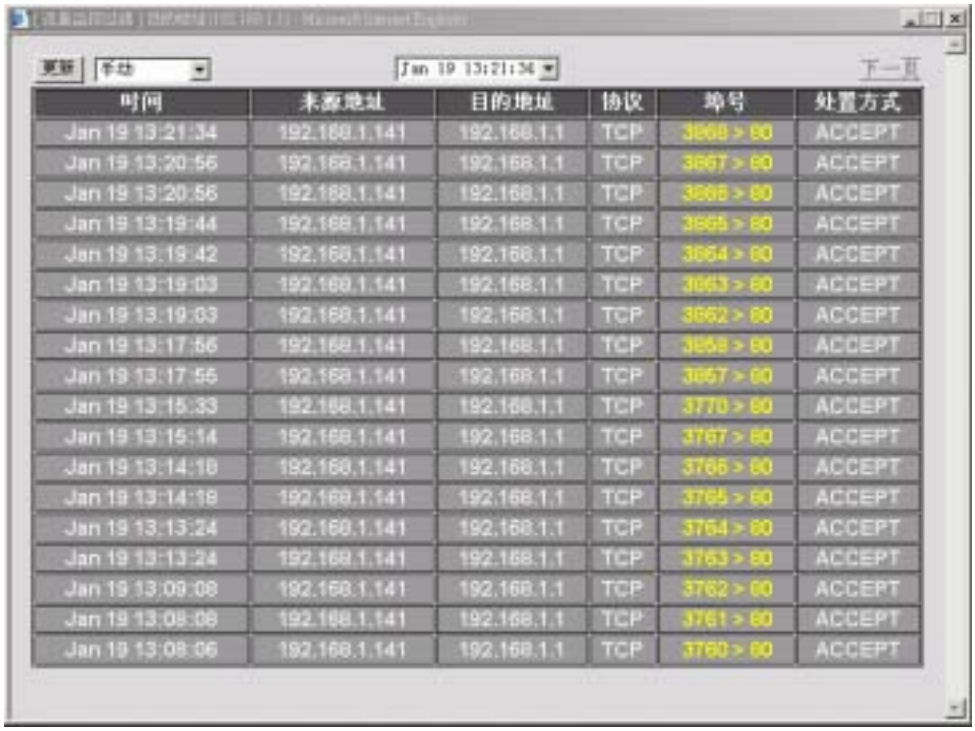


流量监控过滤窗名词名称定义：

- 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。
- 目的地址：目的端的 IP 地址。
- 协议与端口号：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。

点选目的地址时，频宽管理器会依目的地址过滤,并整理所有相关的流量监控资料,供 MIS 人员进行参考。*(如下图)*



流量监控过滤窗名词名称定义：

- 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。
- 目的地址：目的端的 IP 地址。
- 协议与端口号：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

步骤1. 在【流量监控】窗口中，点选屏幕下方【下载监控记录】功能按钮。

步骤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 11-2）*

图 11-2 下载流量监控记录

清除流量监控记录

步骤1. 在【流量监控】窗口中，点选屏幕下方【清除记录】功能按钮。

步骤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 清除流量监控记录

事件监控功能

于左方功能选项，先点选【监控记录】，接着点选下方的【事件监控】，进入【事件监控】工作窗口。*(如图 11-4)*

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 11-4 事件监控功能

事件监控窗口名词名称定义：

- 时间：此事件发生的起始时间。
- 事件：此事件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11-5）*

图 11-5 下载事件监控记录

清除事件监控记录

步骤1. 在【事件监控】窗口中，点选屏幕下方【清除记录】功能按钮。

步骤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 清除事件监控记录

联机纪录功能

于左方功能选项，先点选【监控记录】，接着点选下方的【联机记录】，进入【联机记录】工作窗口。*(如图 11-7)*

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。

图 11-7 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【联机纪录】窗口中，点选屏幕下方【下载监控纪录】功能按钮。

步驟2. 在【档案下载】对话框，将该联机纪录储存至指定的硬盘目录位置 *（如图 11-8）*

图 11-8 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 11-9）*

图 11-9 清除联机记录

监控备份功能

于左方功能选项，先点选【监控记录】，接着点选下方的【监控备份】，进入【监控备份】工作窗口。*(如图 11-10)*

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 11-10 监控备份

步驟1. 【监控报告】窗口名词名称定义：

- 电子邮寄监控记录：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至此设定的 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。点选左下方【清除记录】功能按钮，联机监控功能即由设定时实时激活。

激活电子邮寄与远程监控记录

步驟1. 开启电子邮寄监控记录功能：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【监控备份】勾选【激活电子邮寄监控记录】，最后点选屏幕右下方【确定】按钮。*(如图 11-11)*

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】和【远程记录主机 Port】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 11-11)*

图 11-11 激活电子邮寄和远程监控记录

取消电子邮寄与远程监控记录

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，点选屏幕右下方【确定】按钮。*（如图11-12）*

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11-12）*

图 11-12 取消电子邮寄和远程监控记录

第十二章

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。

流量警示功能

于左方功能选项，先点选【警示记录】，接着点选下方的【流量警示】，进入【流量警示】工作窗口。*(如图 12-1)*

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。

图 12-1 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

步骤1. 在【流量警示】窗口中，点选屏幕下方【下载监控记录】功能按钮。

步骤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12-2）*

图 12-2 下载流量警示记录

清除流量警示记录

步骤1. 在【流量警示】窗口中，点选屏幕下方【清除记录】功能按钮。

步骤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12-3)*

图 12-3 清除流量警示记录

事件警示功能

于左方功能选项，先点选【警示记录】，接着点选下方的【事件警示】，进入【事件警示】工作窗口。*(如图 12-4)*

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

图 12-4 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：可点选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【下一页】，检视其它联机时间之事件警示。点选【上一页】，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

步骤1. 在【事件警示】窗口中，点选屏幕下方【下载监控记录】功能按钮。

步骤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 12-5）*

图 12-5 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12-6）*

图 12-6 清除事件警示记录

第十三章

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]

将内部网络使用者通过频宽管理器的至外部网络服务器及 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，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13-1）*

图 13-1 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。

步驟1. 来源 IP 窗口内名词定义说明：*(如图 13-2)*

- 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 13-2　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。

步驟1. 来源 IP 窗口内名词定义说明：***(如图 13-3)***

- 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。
- 总流量：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。

图 13-3　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。

步驟1. 来源 IP 窗口内名词定义说明：*（如图 13-4）*

- 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 13-5）*
- 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 13-4　内部至外部 Service 统计报告

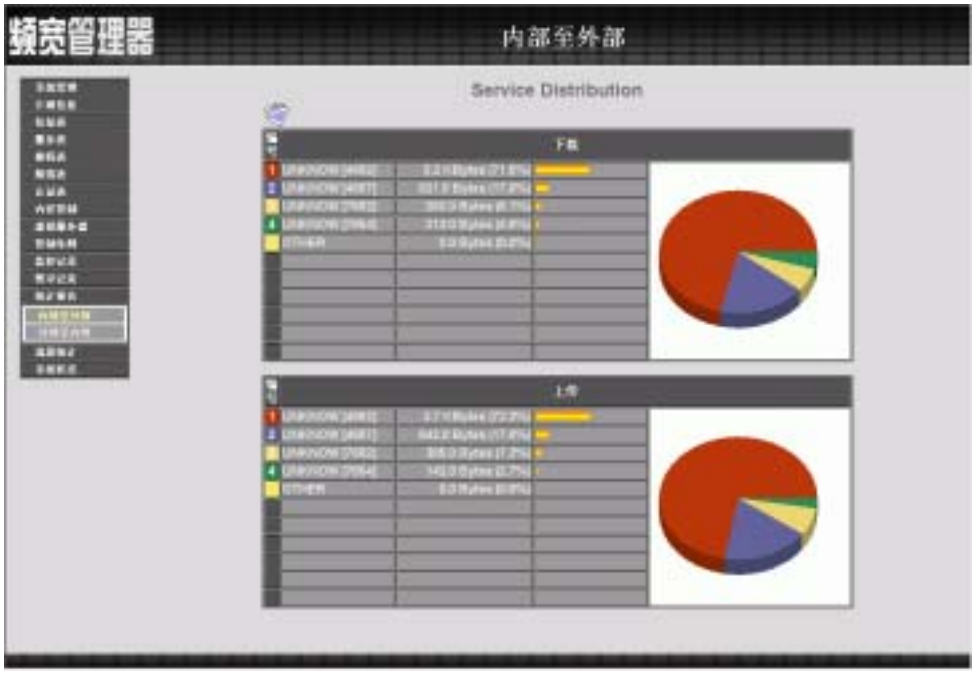


图 13-5 内部至外部 Service 上传/下载 分析统计报告的饼图及长条图

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13-6）*

图 13-6 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。

步驟1. 来源 IP 窗口内名词定义说明：*（如图 13-7）*

- 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。

图 13-7　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。

步驟1. 来源 IP 窗口内名词定义说明：*（如图 13-8）*

- 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 13-8　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。

步驟1. 来源 IP 窗口内名词定义说明：*（如图13-9）*

- 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13-10）*
- 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 13-9　外部至内部 Service 统计报告

图 13-10　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

第十四章

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。

外部网络流量统计功能

于左方功能选项，先点选【流量统计】，接着点选下方的【外部网络流量】，进入【外部网络流量】工作窗口。*(如图 14-1)*
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。

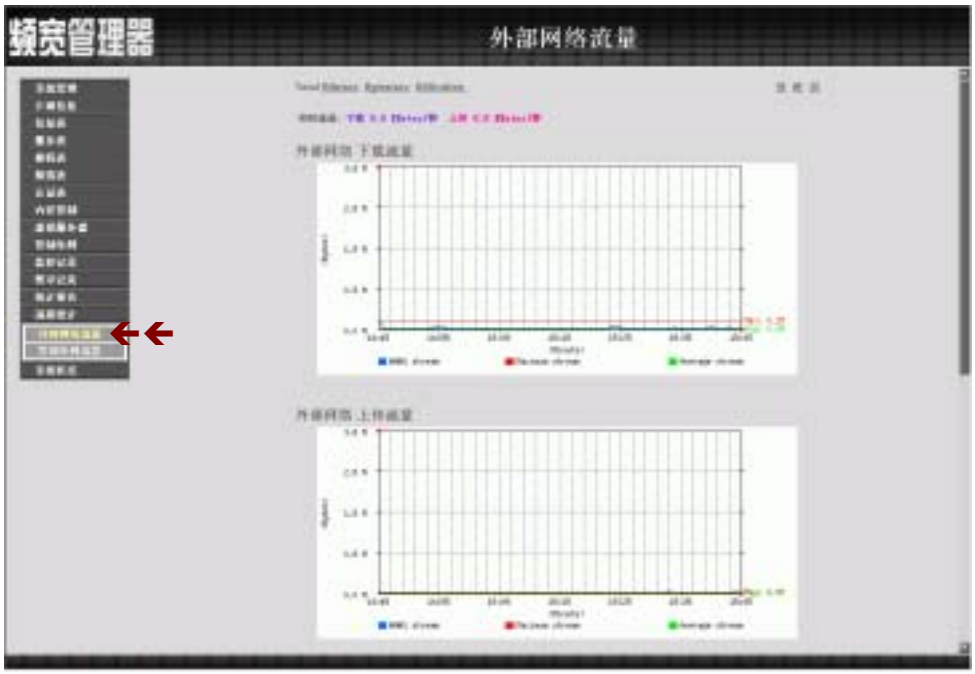


图 14-1 外部网络流量统计功能

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。
- 实时流量：显示 实时 下载 / 上传 流量(KByte/s)
- 外部网络下载流量图
- 外部网络上传流量图
- 外部网络下载封包数图
- 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【外部流量统计】窗口中，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14-2）*

- 实时流量：显示 实时 下载 / 上传 流量(KByte/s)
- 纵坐标：网络流量（Kbytes/Sec）。
- 横坐标：时间（时/分/日）。

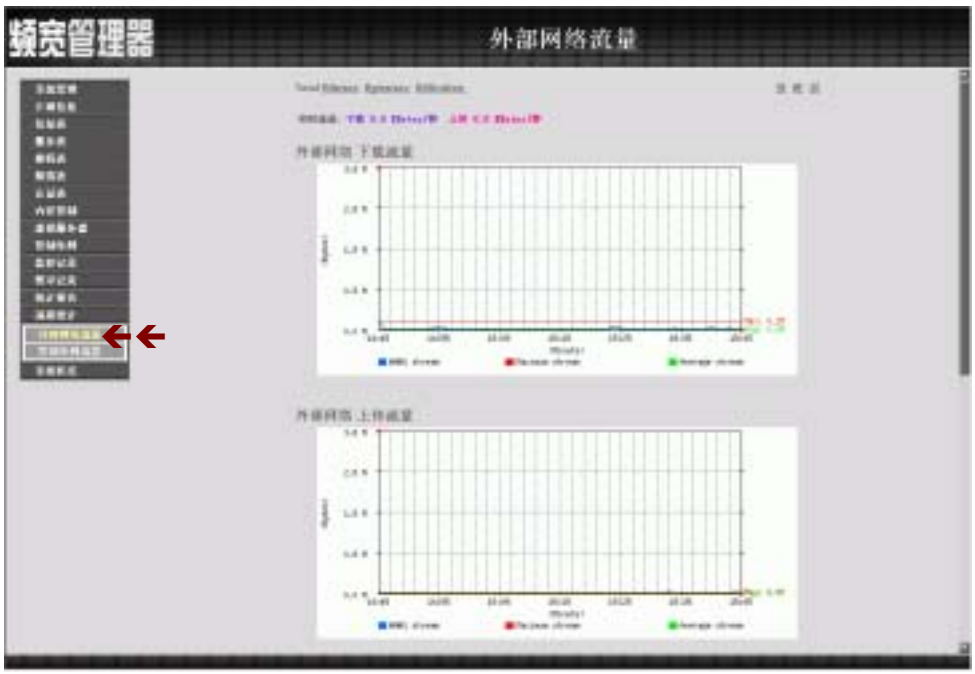


图 14-2 检视外部网络流量统计

管制条例流量功能

于左方功能选项，先点选【流量统计】，接着点选下方的【管制条例流量】，进入【管制条例流量】】工作窗口。*（如图 14-3）*

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

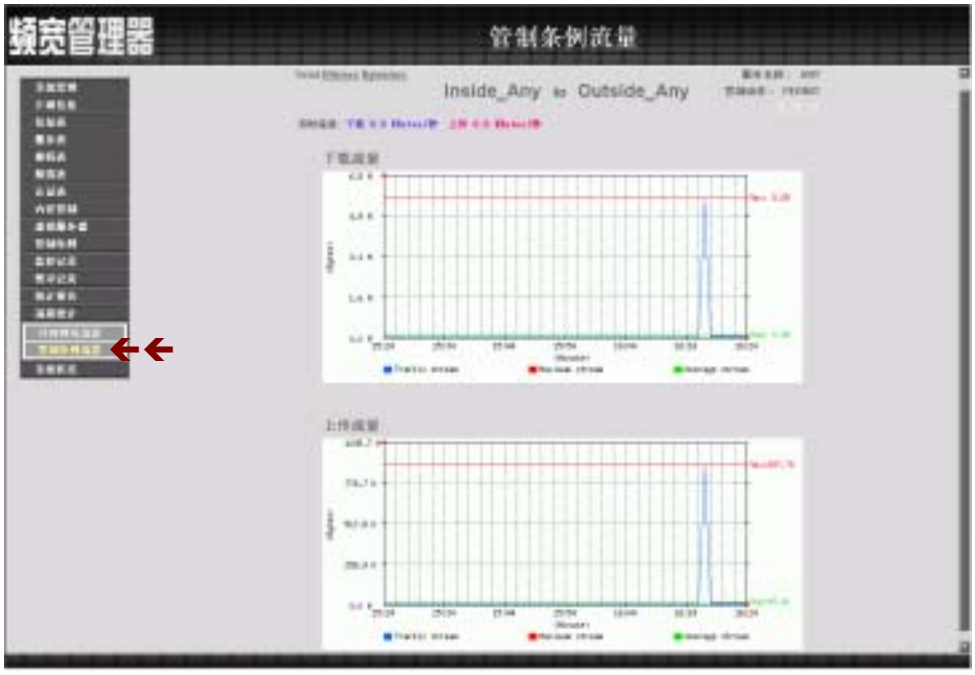


图 14-3 管制条例流量功能

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14-4）*

- 实时流量：显示 实时 下载 / 上传 流量(KByte/s)
- 纵坐标：网络流量（Kbytes/Sec）。
- 横坐标：时间（时/分/日）。

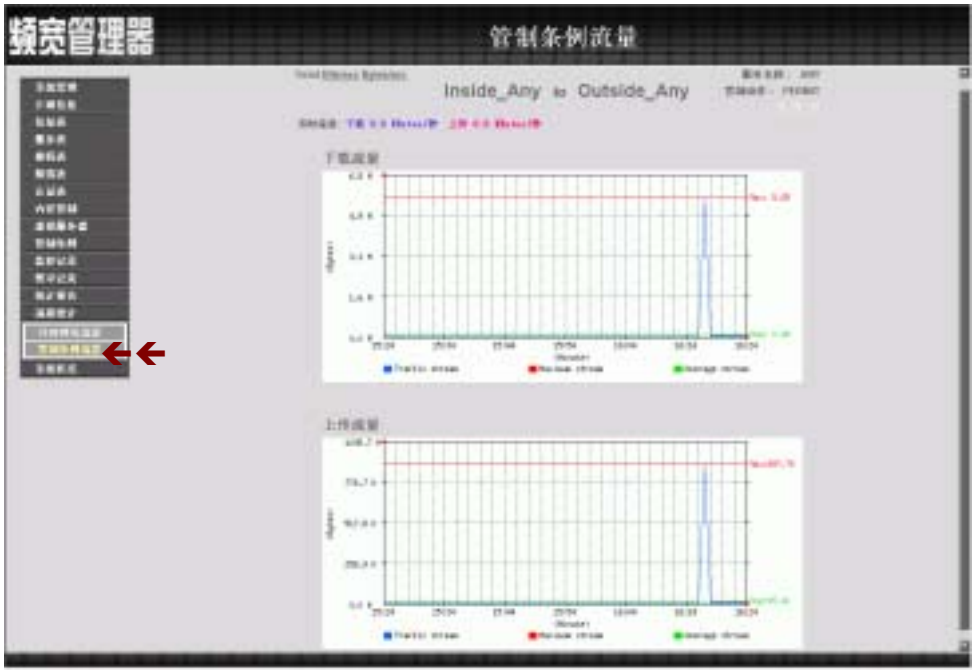


图 14-4 检视管制条例流量

第十五章

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。

接口状态功能

于左方功能选项，先点选【系统状态】，接着点选下方的【接口状态】，进入【接口状态】工作窗口。*(如图15-1)*

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。

图 15-1 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

于左方功能选项，先点选【系统状态】，接着点选下方的【ARP 表】，进入【ARP 表】工作窗口。*（如图 15-2）*

显示网卡的 MAC 地址转译为 IP 地址的对照表。

图 15-2 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

于左方功能选项，先点选【系统状态】，接着点选下方的【DHCP 用户表】，进入【DHCP 用户表】工作窗口。*（如图 15-3）*

记录 DHCP 用户 IP 地址与 MAC 地址及其租约时间等信息。

图 15-3　DHCP 用户表

【DHCP 用户表】工作窗口内表格名词定义：

- IP 地址：DHCP。
- MAC 地址：连接 DHCP 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

操作范例 1

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。

图 ex1-1 新增内部至外部管制条例

本范例让公司内部的 IP 地址只能连到 IP 地址为 61.11.11.11 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。

图 ex2-1 新增外部网络地址

步驟5. 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6. 在【内部至外部】窗口中，点选【新增】功能按钮。

步驟7. 在出现的【新增管制条例】窗口中，键入相关参数*（如图 ex2-2）*。

步驟8. 点选屏幕下方【确定】按钮，新增指定的内部网络。

图 ex2-2　新增内部至外部管制条例

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． 出现以下画面，表示完成 IP 对映的设定。*（如图 ex3-2）*

图 ex3-2 新增 IP 对映

步驟6． 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 ex3-3）*

步驟7． 在【外部至内部】窗口中，点选【新增】功能按钮。

图 ex3-3 管制条例的外部至内部窗口

步驟8. 在出现的【新增管制条例】窗口中，键入相关参数后，点选【确定】执行新增群组。 *（如图 ex3-4）*

图 ex3-4 新增管制条例

步驟9. 开放所有的服务项目（ＡＮＹ），设定及完成。*（如图 ex3-5）*

图 ex3-5 开放所有服务项目

操作范例 4

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ＩＰ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【新增虛拟服务器 IP】窗口中，选择虛拟服务器 IP 地址后，点选下方【确定】按钮。*（如图 ex4-2）*

图 ex4-2　新增虛拟服务器

步驟4． 新增虛拟服务器 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　新增虛拟服务器服务设定

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）*

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）*

图 ex4-5　完成虚拟服务器设定

步驟7． 再到【管制条例】里的【外部至内部】工作窗口。*(如图 ex4-7)*

步驟8． 点选屏幕下方的【新增】控制按钮。

图 ex4-7　进入管制条例之外部至内部窗口

步驟9． 在【新增管制条例】设定各项参数，完成后按【确定】。*(如图 ex4-8)*

图 ex4-8　新增管制条例

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。

图 ex5-1 新增频宽表

步骤5． 出现以下画面，表示完成**频宽表**的设定。*（如图 ex5-2）*

图 ex5-2 新增频宽表

步骤6． 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 ex5-3）*

步骤7． 在【内部至外部】窗口中，点选【新增】功能按钮。

图 ex5-3 管制条例的内部至外部窗口

步驟8. 在出现的【新增管制条例】窗口中，键入相关参数后，点选【确定】执行新增。 *（如图 ex5-4）*

图 ex5-4　新增管制条例

步驟9. 开放所有的服务项目（ＡＮＹ），设定频宽表及完成。*（如图 ex5-5）*

图 ex5-5　完成频宽表所有服务项目

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ＩＰ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。

图 ex6-1 新增频宽表

步驟5． 出现以下画面，表示完成**频宽表**的设定。*（如图 ex6-2）*

图 ex6-2 新增频宽表

步驟6． 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 ex6-3）*

步驟7． 点选屏幕上方的【选择】控制按钮。

图 ex6-3 进入虚拟服务器窗口

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

图 ex6-4　新增虛拟服务器

步驟9. 新增虛拟服务器 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　新增虛拟服务器服务设定

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【管制条例】里的【外部至内部】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