2 WAN Load Balancer

使用手册

目录

Document Version: 1.0

1:介绍

感谢您选购我们的产品，这一台 2 WAN 的负载均衡防火墙不仅提供 2 WAN Port 的选择,也为您的局域网络（LAN）用户提供了一个安全的方式连接 Internet。

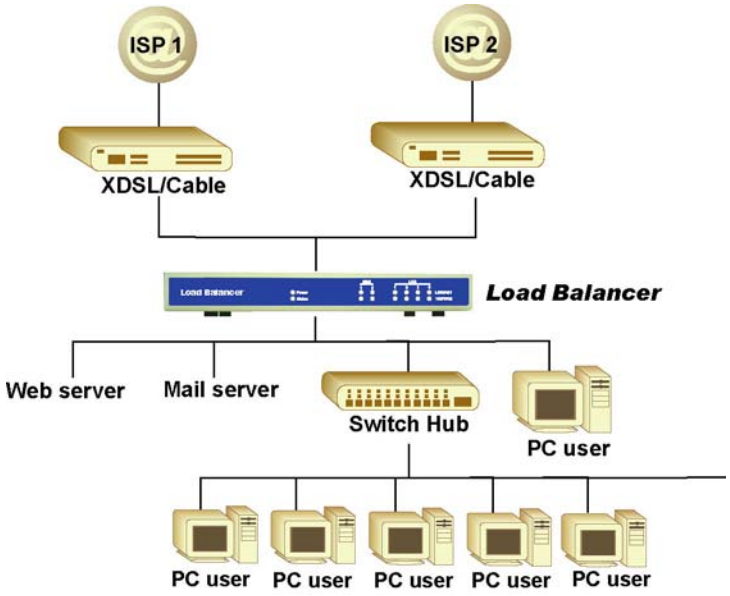


图 1-1: 2 WAN 負載平衡器

Internet 功能

- ***共享安全的Internet宽带连接***
  所有的 LAN 用户能通过这台设备安全的访问 Internet。
- ***高效能的支持多条宽带连接***
  允许同时连接 2 条宽带，并可以经由负载均衡及线路备援的功能达到数据的分流让您的带宽发挥充分的功能。
- ***支持多种不同的宽带连接方式***
  支持各类型的 DSL， 电缆调制解调器，FTTB+LAN 的连接方法，包括： 固定的 IP， 动态 IP，PPPoE 和 PPTP…等。
- ***Inbound/Outbound流量负载均衡及线路质量侦测***
  网络设备管理员可以透过流量负载均衡功能有效的管理进/出的流量，并经由智能的线路质量侦测来确保网络的畅通。
- ***PPPoE 联机管理***
  如果需要的情况下您可以选择将联机对应到您的PC上。
- ***支持多组IP地址***
  如果您的ISP 分配您多个IP 地址， 您能“映像” IP 地址对选择的个人计算机或是服务器。
- ***特殊应用***
  这个特点允许您使用一些非标准应用；例如，透过不同的外部端口对应到不同的内部端口。
- ***虚拟服务器***
  这个功能允许 Internet 用户访问内网的服务器，如 Web、FTP 或 E-Mail 服务器。

- ***IP对应***

  IP 对应可以让您将 IP 指定到内网的某一台 PC 或是服务器上，如果您的 ISP 提供多个 IP 的话您可以设定多台 PC 或是服务器对应到多个不同的 IP 上。
- ***访问过滤***

  网络管理员可以通过这个功能来管理内部人员的权限，并可以分组管理配置不同的权限。
- ***锁定特定的网站***

  网络管理员可以锁定特定的网站来防止内部人员进行访问。
- ***最大联线数控制***

  这个功能的特性是如果新的联线数超出了网络管理员所设定的极限的话新的联线将会被阻挡，用以管理网络质量。
- ***系统过滤例外***

  这个功能确保每个经由未被确认的端口传输的封包将会被阻挡掉，以防止黑客对端口的扫描，但是在一些的情况下也许会导致有一些服务器的问题或外网的用户要求某些封包的响应来核实他们通信的可及性。

其它功能

- ***4-Port 网络交换机***

  4 port 的 10/100BaseT 交换机，可以依照您的内部网络使用或是进行扩充。
- ***提供DHCP服务器功能***

  开启 DHCP 的功能可以提供动态 IP 分配给内网的 PC 或是其它设备使用。
- ***支持多重网段***

  支持多重网段使用静态路由表。
- ***简易的设置***

  经由浏览器可以轻易的配置好所有的设置。
- ***远程管理***

  您可以透过 LAN 或是 Internet 来设置您的 2 WAN Load Balancer。
- ***使用密码来保护您的设置***

  使用密码来防止未经批准的用户修改您的数据及设置。
- ***使用HTTP方式升级及备份***

  使用浏览器即可从 LAN 或是 Internet 升级 2 WAN Load Balancer 的韧体或是将您的配置下载到您的 PC 中。
- ***Email 警报***

  可设定 Email 警报当设备有问题发生的时候会发出 Email 去通知网络管理员。
- ***Syslog/系统日志***

  这是一个非常有用的功能，他可以将系统的日志显示在网页上也可以将讯息发布到一台独立的服务器上。
- ***QoS 设定***

  经由频宽管理的功能可以让一些特定的应用(如 VOIP、视讯会议…等)确保可以获得足够的带宽。
- ***UPnP***

  支持 UPNP 功能，让您具备 UPNP 的其它设备可以轻松的完成设置，并协调的一起工作。

物理状态

前面板

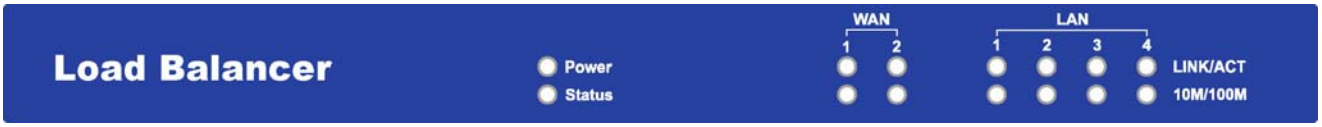


图 1-2: 正面面板

面板 LED 所代表的意义如下:

LAN	
LINK/ACT	ON – Physical connection or data in/out. OFF – No physical connection.
10M/100M	ON – The corresponding LAN port is using 100BaseT. OFF – 10BaseT connection on the corresponding LAN port or no connection.
WAN	
LINK/ACT	ON – Physical connection to the Broadband modem on WAN port 1/2 established. OFF – No physical connection on WAN port 1/2.
10M/100M	ON – Physical connection using 100BaseT on WAN port 1/2 established. OFF – 10BaseT connection or no connection on WAN port 1/2.
System	
Power	OFF – No power. ON – Normal Operation
Status	OFF – Normal operation. ON – Firmware not loaded or Hardware error. Blinking – Data in/out

以太网口和 Reset 按键的用途

以太网口(RJ45)	WAN ports: 可设置 2 个 WAN Port LAN ports:可直连接 PC 或是接上另外的网络交换机.
Reset 按键	按下一秒以内再放开机器会重新启动,持续按下三秒以上会将设备恢复初始值.

面板上的灯号所代表的意义将依照下表被显示:

LED Action	Condition
WAN1 LINK/ACT & 10M/100M LEDs flash alternatively.	Firmware Download in progress.
WAN1 LINK/ACT & 10M/100M LEDs flash concurrently.	MAC address not assigned.
WAN1 LINK/ACT & 10M/100M LEDs solid On	SDRAM error
WAN2 LINK/ACT & 10M/100M LEDs solid On	Timer/Interrupt error
LAN1 LINK/ACT & 10M/100M LEDs solid On	LAN/WAN error

出厂设置

当 2 WAN Load Balancer 完成启动之后所有的设置将按照以下的出厂值运作:

- *IP地址为http://192.168.1.1 子网掩码为 255.255.255.0*
- *DHCP 服务器处于开启状态*
- *用户名称为: admin*
- 密码为清空(无密码)

TFTP 下载

这个功能只在您需要恢复出厂值或是需要作软体升级时才使用，如果您需要的话请依照以下的步骤：

1. 将 2 WAN Load Balancer 电源打开。
2. 您可以使用 Windows 内建的或是一个 TFTP 的客户端程序来升级您的软体,他看起来将会类似于以下的例子：

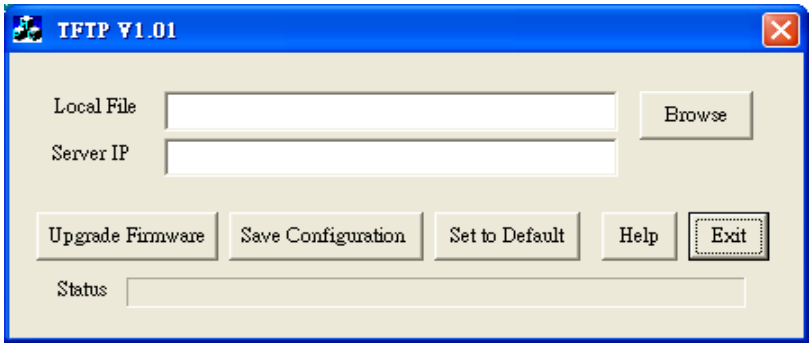


图 1-4: Windows TFTP utility

- 输入在您的 PC 中软体的位置或是点击"浏览"按钮寻找文件。
- 输入 2 WAN Load Balancer 的 IP 地址。
- 点击“升级软体”发送升级软体到设备中。

3. 当升级动作结束后设备将会重启并恢复到出厂值。

注意:

TFTP 所提供的功能还有以下三种：

- 保存当前的设置到您的 PC 中。
- 将之前的设置导入设备中。
- 将设备恢复出厂值。

2: 基本设置

概述

2 WAN Load Balancer 的基本设置请参照以下的步骤：

1. 将您的 PC 或是 LAN 上的网络交换机连接上 2 WAN Load Balancer 的 LAN Port 并将他设置为符合您的 LAN 的设置
2. 将宽带的线路或是 DSL/Cable Modem 连接上 2 WAN Load Balancer 的 WAN Port
3. 配置您的设备，让它可以连接上 Internet
4. 配置您的 PC 让它们可以连接上 Internet

需求

- 准备好一个(最多八个)宽带线路或是 DSL/Cable Modem 以及由 ISP 所提供相对应的账号
- 网络线，使用标准具备 RJ45 接头的 10/100BaseT 的网络线
- TCP/IP 网络协议必须安装在每一台 PC 上

步骤

1: 将 2 WAN Load Balancer 安装到您的 LAN 中

1. 使用标准的网络线将您的 PC 连接到任何一个 LAN Port 上.
2. 将电源线接上插座
3. 将您的 PC 电源开启，如果您的 PC 已经启动，请先将您的 PC 的 IP 地址设为自动获得 IP 并重启 PC，让您的 PC 的 IP 由 2 WAN Load Balancer 分配
4. 打开您的浏览器
5. 输入 http://192.168.1.1
6. 您会看到以下的对话窗：

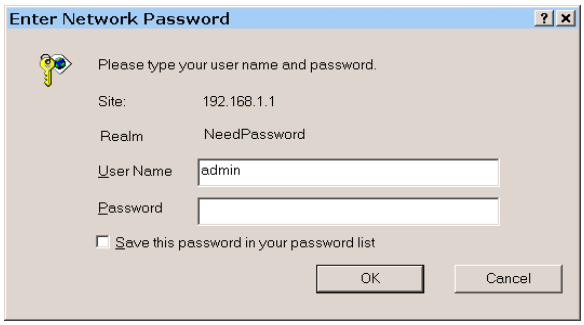


图 2-1: 密码输入对话框

7. 输入用户名称(admin)及密码(空白)
   - 用户名称都将会是 admin.
   - 为了安全因素,请设置一个密码
8. 当您登录以后您可以在管理的页面中设置您的账号密码

图 2-2: 管理员

9. 从菜单选择网络设定-内部网络您会看到以下的画面：

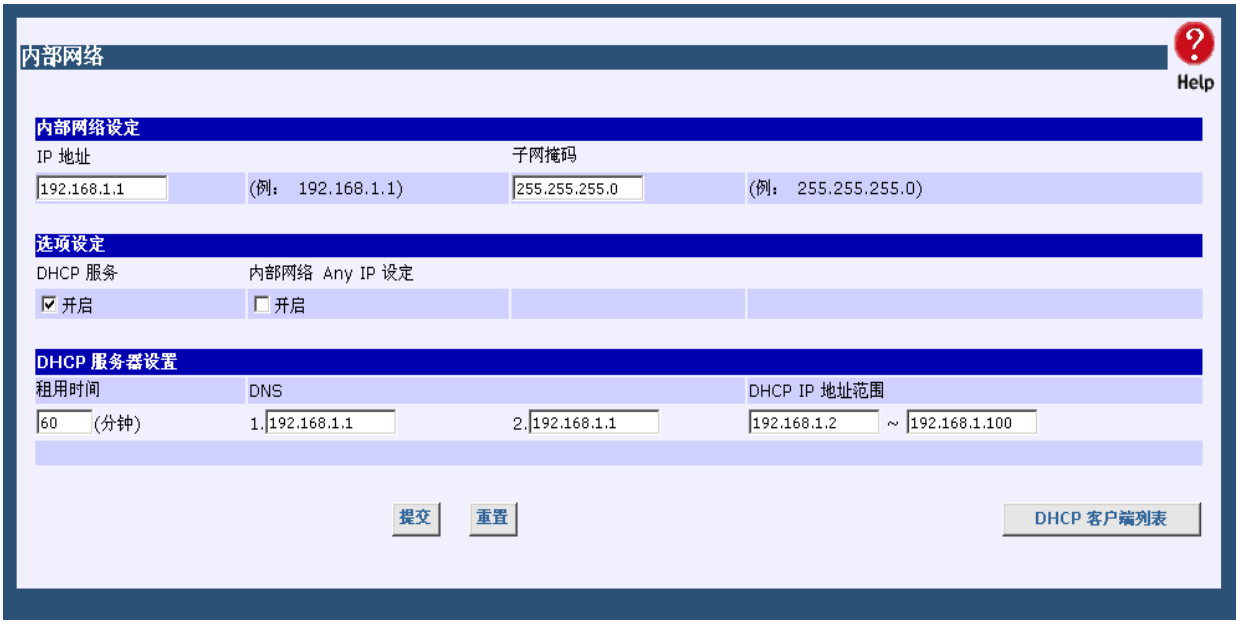


图 2-3: 内部网络

10. 如果您的 LAN 中已经有一台 DHCP 服务器而且您希望继续使用它的话请按照以下配置:
    - 首先在 2 WAN Load Balancer 中的 DHCP 必须是关闭的
    - 您的 DHCP 服务器必须将 2 WAN Load Balancer 设置为："预设网关"
    - 您的 DHCP 服务器必须提供正确的 DNS 给 LAN 中所有的 PC

11. 确定这些设置符合您 LAN 的需求：
    - 检查以下的设置,大多数的情况下默认值是合适的.

设定 – LAN & DHCP

LAN IP 设置	• **IP 地址** – 您可以设置一个 IP 地址给您的设备，出厂值是 http://192.168.1.1 您可以参照您的 LAN 的设置去调整为符合您的需要的 IP 地址 • **子网掩码** –出厂值是 255.255.255.0(class C)，您可以按照您的需求去设置符合您的需求，大多数中小型网络的情况下使用默认值是合适的设置
选用设置	• **DHCP 服务器设置** – 如果您启用了 DHCP 服务器的话(出厂值为开启)，2 WAN Load Balancer 会分配 IP 给 LAN 中的每一台 TCP/IP 设置为自动取得 IP 的 PC • **LAN Any IP** – 这个功能在出厂值是关闭的，如果您将此功能开启的话只要您的 LAN 中的 PC 是设置为固定 IP 的话，无论他是否在同一个网段中这些 PC 都可以通过 NAT 来使用 Internet
DHCP 设置	• **租用时间** – 您可以设定一个时间给 DHCP 服务器来设定分配出去的 IP 的租用时间 • **DNS Server –** 可以设定 DNS 的 IP 地址接由 DHCP 服务器分配给 LAN 中的 PC • **分配的 IP 范围** – 设置 DHCP 服务器分配的 IP 范围段.
DHCP 客户端列表	这个选项显示哪些 IP 是由 DHCP 服务器分配的，并显示以下的讯息： • **空余数量** – 这里显示的是还有多少剩余的 IP 可以经由 DHCP 服务器去分配 • **名称** – 显示的是 DHCP 客户端的 PC 名称 • **MAC 地址** – 显示的是 DHCP 客户端的 PC 的物理地址. • **IP 地址** – DHCP 所分配给这台 PC 的 IP 地址 • **类型** – 显示此 IP 是动态还是静态的 • **状态** – 显示此 IP 的状态 • **剩余时间** – 显示分配的时间

12. 保存您的设置，然后进入步骤 2，安装 2 WAN Load Balancer 在的 LAN 中

步骤 2，安装 2 WAN Load Balancer 在的 LAN 中

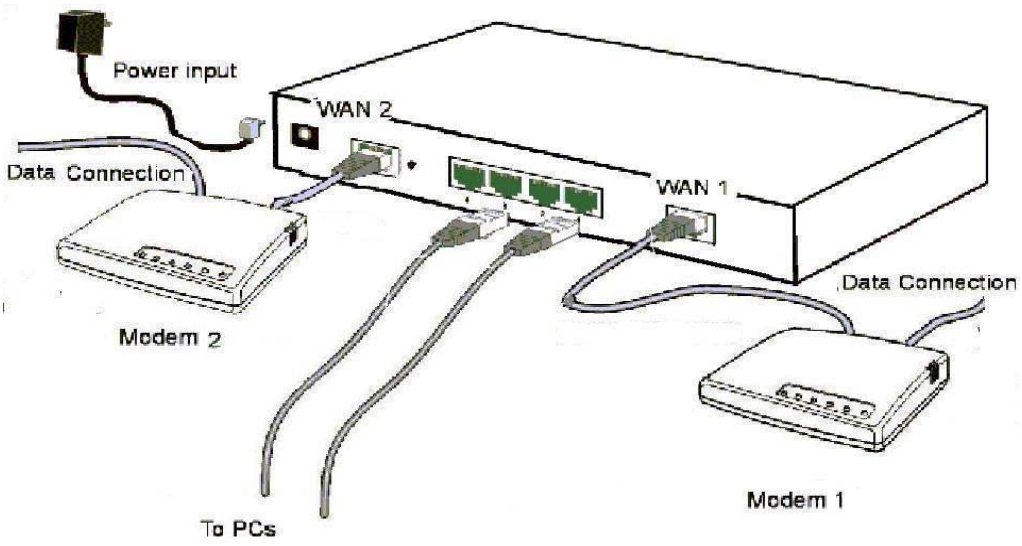


图 2-4: 安装图

1. 确认每一台调制解调器的电源是关闭的并将 ISP 所提供的数据线连接到调制解调器上
2. 将调制解调器连接到 2 WAN Load Balancer
   - 如果您只有一台调制解调器的话请将它接到 WAN1
   - 请使用调制解调器配发的网络线进行连接，如果没有的话请使用标准的网络线
   - 请使用标准的网络线连接您的个人计算机到 2 WAN Load Balancer
   - 如果您需要将 2 WAN Load Balancer 接到其它的网络交换机以进行扩充的话，请使用一条标准的网络线连接到任何一个 2 WAN Load Balancer 上的 LAN 接口，另一端连接到您要使用的网络交换机
3. 打开电源
   - 请将调制解调器的电源打开
   - 请将 2 WAN Load Balancer 接上电源并打开电源
4. 检查面板上的灯号
   - 首先确认”Power”灯号是亮的
   - 然后连接调制解调器的端口对应的 ***Link/ACT*** *灯号必须是亮的*
   - 将所有个人计算机连接到 2 WAN Load Balancer 的 LAN 端口,对应的灯号应该亮起.

3. 设置相关的 Internet 联机

从菜单中选择外部网络，您将会看见一个画面像以下的例子：

- 通过选定 WAN 接口的下拉菜单逐个配置各 WAN Port.
- 在下列的情况下请参照章节三:端口进阶设置,来设置其它必须的配置.
   - 使用多个 WAN Port.
   - 单一 WAN Port 有多个真实 IP.
   - 使用多个 PPPoE 联机.
   - PPTP 连接方式.

图 2-5: 外部网络

设置- 外部网络

连接方式	• **网络接口** – 一个下拉式菜单让您选择各个 WAN Port. • **联机模式 – 开启** – 如果您将宽带线路连接到这个端口的话请点选此处. **关闭** – 如果您没有使用这个端口的话请关闭它.
连接类型	请检查 ISP 所提供给您的数据和选择适当的选项. • **固定 IP** – 如果您的 ISP 提供给您的是固定或是静态 IP 的话请选择此处并将正确的数据填入. • **动态 IP** – 如果您的 ISP 提供的是动态 IP 的话请点选此处. • **PPPoE** – 如果您的 ISP 是使用这个方式联机的话请点选此处。(通常您的 ISP 会提供一个 PPPoE 的软件，但是在您使用此设备的时候请不要使用这个软件) 如果您点选此处，您必须要填入 PPPoE 相关的拨号设置 **注意:** 如果您选择 PPTP 的方式的话,您可能需要填入 ISP 所提供的相关讯息
地址讯息	这是提供给静态 IP 的用户使用.输入由 ISP 所提供的地址讯息(IP 地址、子网掩码、网关)，如果您的 ISP 提供多个 IP 给您的话，您可以在 Multi-DMZ 的画面设定所有其它的 IP
PPPoE / PPTP 拨号	如果您的 ISP 是使用 ***PPPoE*** 或 ***PPTP*** 请选择此处 • 请输入由 ISP 所提供的用户名称及密码 • 如果您的ISP 是使用PPTP 的方式连接请点选 ***PPTP 联机***的选项并输入PPTP 的 IP 地址 • **PPPoE 服务器名称** (选用) – 如果您的 ISP 需要的话请输入此名称 **注意:** 有另外的 PPPoE/PPTP 选项在“端口选项”的画面中，如果您要使用多个 PPPoE 连现在其它的端口的话请在进阶 PPPoE 里面设置

DNS	如果使用的是一个固定的 IP 的话您必须输入至少一个 DNS 的 IP 地址，如果使用动态 IP、PPPoE 或 PPTP 的话， DNS 的资料可空白
选项	• **服务器名称** – 如果您的 ISP 提供服务器名称给您的话请在此输入，如果没有的话请保持空白 • **域名** – 如果您的 ISP 提供一个域名请填入它,否则请保持空白 • **MAC 地址** – 有些 ISP 会纪录您的 MAC 地址，如果是的话请输入相应的 MAC 地址；否则请将此处空白

2 WAN Load Balancer 的基本设置现在已经完成,有关于个人计算机在您的 LAN 必须的配置请参照以下的细节

4: 设置局域网中的个人计算机

概述

以下的设置需要对所有的个人计算机作配置：

- TCP/IP 网络协议设置
- 因特网接入配置

TCP/IP 设置

假设您使用 2 WAN Load Balancer 的默认值及使用预设的 Windows 95/98/ME/2000/XP TCP/IP 设置，您不需要做任何的设置即可使用。您只需开启(或是重启)您的个人计算机。

- 在默认值的情况下，2 WAN Load Balancer 会作为 DHCP 服务器，自动提供一个适当的 IP 地址(以及其它相关的讯息)给所有的个人计算机
- 对于所有非服务器版本的 Windows 操作系统，默认值的 TCP/IP 设置将会是作为 DHCP 的客户端。在 Windows 操作系统里面，这个设置会自动取得 IP 地址
- 请开启(或重启)您的个人计算机并且他会自动从 2 WAN Load Balancer 获取一个 IP 地址

如果您的 LAN 是使用固定 IP 地址的话，或是您需要检查你的 TCP/IP 设置，请参见附录 B – Windows TCP/IP 设定

因特网接入

请参照以下做法去设置您的个人计算机连接互联网：

Windows 9x/2000

1. 选择”开始”→”控制面板”→”网络联机”
2. 选择”联机”然后点击”设定”按钮.
3. 选择”我要手动设置我的互联网联机”或是”我想要通过一个局域网络(LAN)”然后点选下一步.
4. 选择”通过一个局域网络(LAN)”然后点击下一步.
5. 确认所有局域网络的选项都没有选上.
6. 当提示”您想要现在设定互联网邮件账户”时选择”不要”.
7. 按下*结束*关闭互联网连接的向导.
   设定现在完成。

Windows XP

1. 选择”开始”→控制面板→网络连接.
2. 选择”建立一个新的连接.
3. 在建立新连接向导中按下”下一步”.
4. 选择”连接到互联网”然后按”下一步”.
5. 选择”手动设置我的连接”然后按下一步.
6. 选择”保持宽带连接”然后按下一步.
7. 按下”结束”关闭新连接向导.
   设定现在完成。

3: 进阶设定

概述

- ***端口选择*** 包含可能被设置在任何一个 WAN port 的选择，在大多数的情况下，默认值是合适的选择
- ***负载均衡*** 是在您使用 2 WAN Port 时，他可以允许您分配不同的 WAN Port 流量
- ***进阶的 PPPoE*** 设定是如果您需要在同一个 WAN Port 上运行多个联机时使用，并可以对 PPPoE 联机进行连接或是断开，如果不需要使用的话，这个设定可以忽略
- ***进阶的 PPTP*** 设定是必须的，当然是在您需要使用 PPTP 联机的情况下

高级设定

图 3-1: 高级设定

设定 – 端口选择

界面	• **WAN Port** – 从下拉菜单选择一个您要设置的 WAN Port 进行设置. • **MTU** – 一般的情况下这不需要被改变,但如果您的 ISP 通知您使用特殊的 MTU 值的话,您可以进入并改变他.默认值是 1500.
检查联机的质量	• **方式** – 有三个方法可以检查 WAN Port 的联机质量并确定 WAN Port 联机与否.您可以选择多项去配合您的使用. • *如果您选择关闭的话此功能将不会去检查联机的质量.*默认值是开启的. • **间隔时间** – 检查联机质量的间隔时间默认值是 60 秒.
透明桥接选项	• **桥接模式** – 如果设为开启,这个 WAN Port 将不能使用 NAT 及负载均衡的功能,并且 WAN/LAN 的 IP 必须是同一个网段. • **NetBIOS Broadcast** –如果您打开了 NetBIOS 广播,这将允许您通过网上邻居存取文件.
透明桥接选项 (所有端口)	• **流量管理 – 严格绑定:** 限定桥接的封包流量(如透明至WAN1)只能经由限定的WAN口通过. **模糊绑定:** 这作为透明桥接模式故障转移机制的方式.当线路故障的时候流量可以从主要的出口(如WAN1)可以转移到任一个出口(如WAN2 或是其它). **负载均衡:** 这作为透明桥接模式负载均衡的方式.流量可以从主要的出口(如WAN1)平均分配到其它出口(如WAN2 或是其它). • **ARP 表** – ARP 表是用来使用在确定主机的位置（WAN 或 LAN）,并且它的大小是可以调整的. **查看表格** 查看在每一个 WAN Port 上的桥接模式是否开启. **清除表格**清除失效的 ARP 列表.

负载均衡

这个功能只在使用多个 WAN Port 的时候才能启用.

图 3-2: 负载均衡

此功能在当使用两个 WAN 以上时候用以确定各个 WAN Port 的流量比例.

设定 – 负载均衡

负载均衡设定	• **开启** – 选择开启并检查其它的相关设置以达到有效的功能.
	• **平衡类型** – 您可以选择平衡类型.
	  • Bytes Tx + Rx – 依据 Bytes 测量流量
	  • Packets Tx + Rx – 依据封包测量流量
	  • Sessions established – 依据联机数测量流量
	  • IP Address – 依据 IP 地址测量流量
	• **负荷分配** – 在各个 WAN Port 输入流量的百分比,如果一个 WANPort 的带宽比另一个 WAN Port 的带宽更大的话,您应该将他的百分比设定的更高.
	点击"提交" 按钮保存您的变动。

NAT 统计	这个部份显示各个 WAN Port 当前的资料信息,您可以使用这里的讯息帮您优化您的设置.
接口统计	这个部份显示累计的统计数据. 使用”重新统计”按钮去重新计算.
按钮功用	• **刷新** –更新数据讯息. • **重置记录** – 在界面统计部份重新计算.

进阶的 PPPoE

进阶的 PPPoE 设定是为了在同一个 WAN Port 上使用多个 PPPoE 联机.也可以设定针对 PPPoE 联机设定自动联机或是断线.

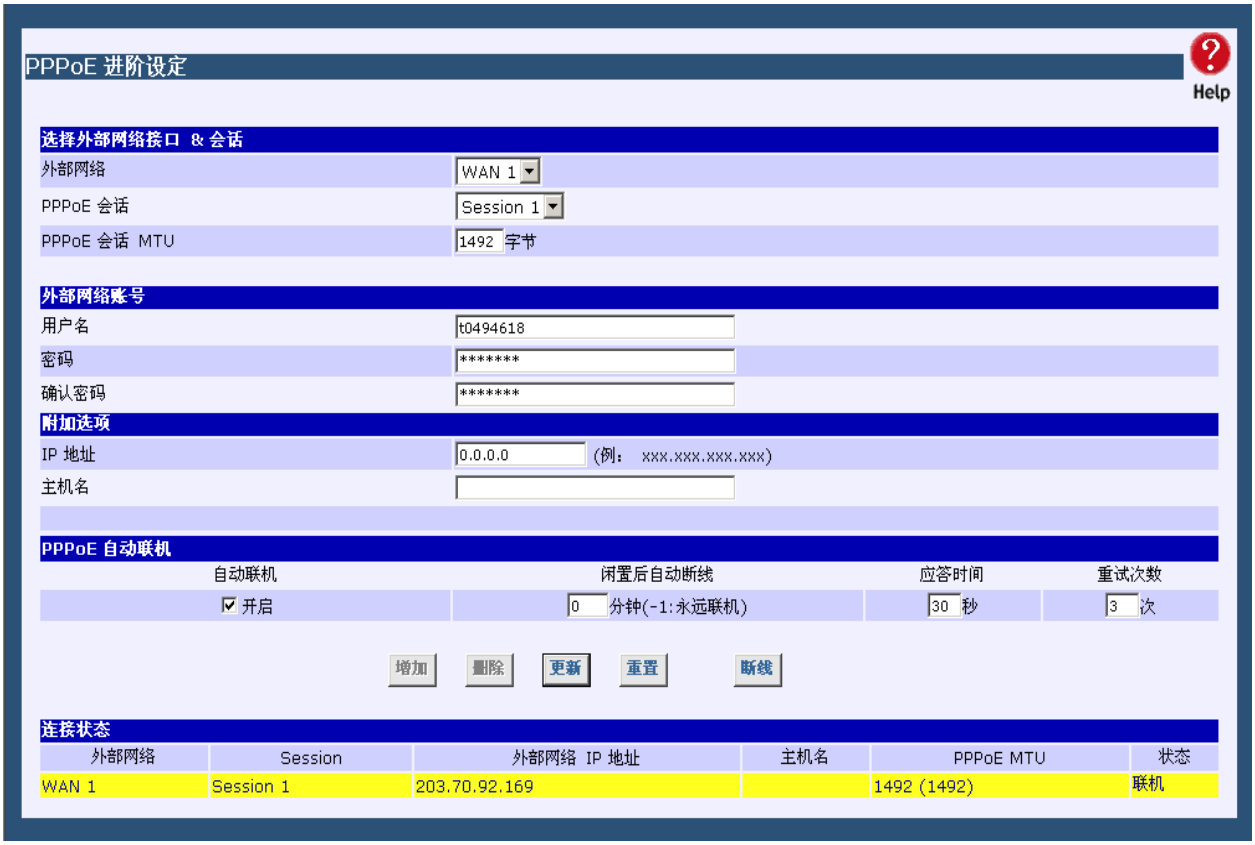


图 3-3: PPPoE 进阶设定

设定 – PPPoE 进阶设定

选择外部网络接口 & 会话	**外部网络** – 选择使用 PPPoE 联机的 WAN Port. **PPPoE 会话** – ISP 通常会提供多个不固定的真实 IP 给用户,每个 WAN Port 最多可以设置八个 PPPoE 联机,每个联机可以设置一个真实的 IP. **PPPoE 会话 MTU** – 最大传输 PPPoE 封包单位,一般来说不需要更改他的数值,除非您的 ISP 提供给您另外的数据,默认值是 1492bytes.
WAN IP 账号	• **用户名** – 输入您的 ISP 所提供的 PPPoE 用户名称. • **密码** – 输入您的 ISP 所提供的 PPPoE 密码. • **确认密码** – 再次输入密码.
附加选项	• **IP 地址** – 如果您有一个固定的 IP 地址,请在这里设置,否则,请在这里保持 0.0.0.0 即可. • **主机名** –如果您的 ISP 需要的话,这里提供给您设置一个服务器名称.

PPPoE 自动联机	• **自动联机** (connect-on-demand) – 如果设置打开的话,每当有流量尝试经由 WAN Port 出去的话将会自动发起联机.如果设置关闭的话,您将必须以手动方式发起联机. • **闲置后自动断线** – 您可以设置一个时间,在没有流量的情况下将会自动断线.(-1:保持联机). • **应答时间** – 您可以在这里输入发送到 PPPoE 服务器的请求的频率.这个响应请求是确定联机是否存在,通常不需要改变设定值. • **重试次数** – 如果对第一个请求没有响应,响应请求将被尝试的次数,通常不需要改变设定值.
联机状态	这里显示每个联机的状态.

进阶的 PPTP

只有在使用 PPTP 的方式联机的时候才需要设置.

图 3-4: PPTP 进阶设定

设定 – PPTP 进阶设定

外部网络	选择需要设置的 WAN Port,被选择的 WAN Port 数据将会被显示在 WAN IP 账号部份. **PPTP MTU** – PPTP 最大的传输单位.缺省值是 1460 PPTP MTU.
外部网络账号	• **用户名** – 这个 PPTP 用户名称(登入名称)将由您的 ISP 提供. • **密码** – 这个密码由您的 ISP 提供,让您搭配您的用户名称使用来登入 PPTP 服务器时使用. • **确认密码** – 再次输入密码确认. • **服务 IP 地址** – 输入由 ISP 提供的 PPTP 服务器 IP 地址. • **固定 IP 地址** – 如果您有固定 IP 地址的话请输入,否则这里应该保持 0.0.0.0
PPTP 自动联机	• **自动联机** (connect-on-demand) – 如果设置打开的话,每当有流量尝试经由 WAN Port 出去的话将会自动发起联机.如果设置关闭的话,您将必须以手动方式发起联机. • **闲置后自动断线** – 您可以设置一个时间,在没有流量的情况下将会自动断线.(-1:保持联机). • **应答时间** – 您可以在这里输入发送到 PPTP 服务器的请求的频率.这个响应请求是确定联机是否存在,通常不需要改变设定值. • **重试次数** – 如果对第一个请求没有响应,响应请求将被尝试的次数,通常不需要改变设定值.
连接状态	这里显示每个联机的状态.

4、高级设置

概述

具有如下特点：

- 系统管理 – 主机与群组
- 系统管理 – 路由表
- 虚拟服务器 – 虚拟服务器
- 系统管理 – 特殊应用
- 系统管理 – 动态域名
- 虚拟服务器 – Multi DMZ
- 系统管理 – UPnP 设定
- 虚拟服务器 – NAT 设定
- 系统管理 – 进阶功能

这一章包括了所有这些特点的细节及具体配置。

主机与群组

这一属性应用于下列环境：

- 你拥有 Multi-Session PPPoE（多联机以太网点对点协议），并且希望把每个联机绑定到局域网的特定的一台计算机上。
- 你希望使用过滤访问功能。这需要运用主机与群组对每台 PC 进行辨别（包括 IP 与 MAC 信息）
- 你希望阻塞不同的 PC 访问不同的 URL（统一资源定位符）。这需要运用主机与群组对每台 PC 进行辨别。
- 你希望把局域网上的一个特定的 IP 分配给一台特定的计算机。这使得这台 PC 在得到固定 IP 的好处时可以使用动态主机配置协议(DHCP,在 windows 操作系统中,这一设置对应于“自动获取 IP”)。这台 PC 的 IP 地址不会再改变，使得它可以提供给其它用户以及其它应用。

图 4-1:主机与群组

主机与群组的设置

主机网络身份	这个部分辨认每台主机（PC） • **主机名** – 输入一个适合的名称。通常情况下，你应该使用主机自己定义的主机名（计算机名） • **MAC 地址**– 也称网络适配器地址。输入这台主机的 MAC 地址。 • **选择群组** – 选择你希望这台主机包括的组。 • **在 DHCP 中保留** – 选择激活(Enable)为一台特定的计算机保留一个固定的 IP. 这使得这台 PC 可以使用 DHCP（在 windows 操作系统中这一设置对应于“自动获取 IP”）时，同时保持固定的 IP 地址。 • **保留 IP 地址**–如果上面提到的 DHCP 的设置处于激活状态(Enable)., 选择希望保留的 IP 地址。否则，忽略这个设置。

主机网络绑定	• **绑定外部网络接口 / Session–** 如果希望把这台 PC 绑定到一个特定的 PPPoE（以太网点对点协议）联机，则激活选项。这样，这台 PC 所有的传输都将通过被选的 PPPoE 端口及对应的联机来完成。 • **绑定方式** – 假设你的 PC 绑定到了广域网 1 的端口上，并且你选择了“严格绑定”。那么如果广域网 1 的端口断开，你的信息包无法通过其它的广域网端口，即使其它这些广域网仍处于良好状态。如果你选择“宽松绑定”，那么如果 WAN1 的端口断开了,你的信息包自动从其它良好的广域网发出。 • **选择外部网络接口** – 若绑定方法中的设置处于激活（Enable），则选择所希望的端口或联机，否则，忽略这些设置。 **注意**: Multiple PPPoE sessions（多联机以太网点对点协议） 在进阶 PPPoE 视屏中定义.
按钮	• **增加** – 根据屏幕上列出的数据可以加入数据库的新入口。 • **删除** – 点击删除选择的入口. • **更新** – 完成修改后，使用这个按钮更新所选的入口。 • **重置–** 通过从载入路由中的数据取消你所做的所有修改
主机&群组列表	这个表显示了当前的绑定。

路由表

这一部分只有当你的局域网有其它的路由器或网关时才会涉及到。

- 如果你的局域网没有路由器或者网关，你可以完全忽略静态路由表页面。
- 如果你的局域网有其它的路由器或者网关，你必须配置如下所示的静态路由表信息，以及其它的路由器。

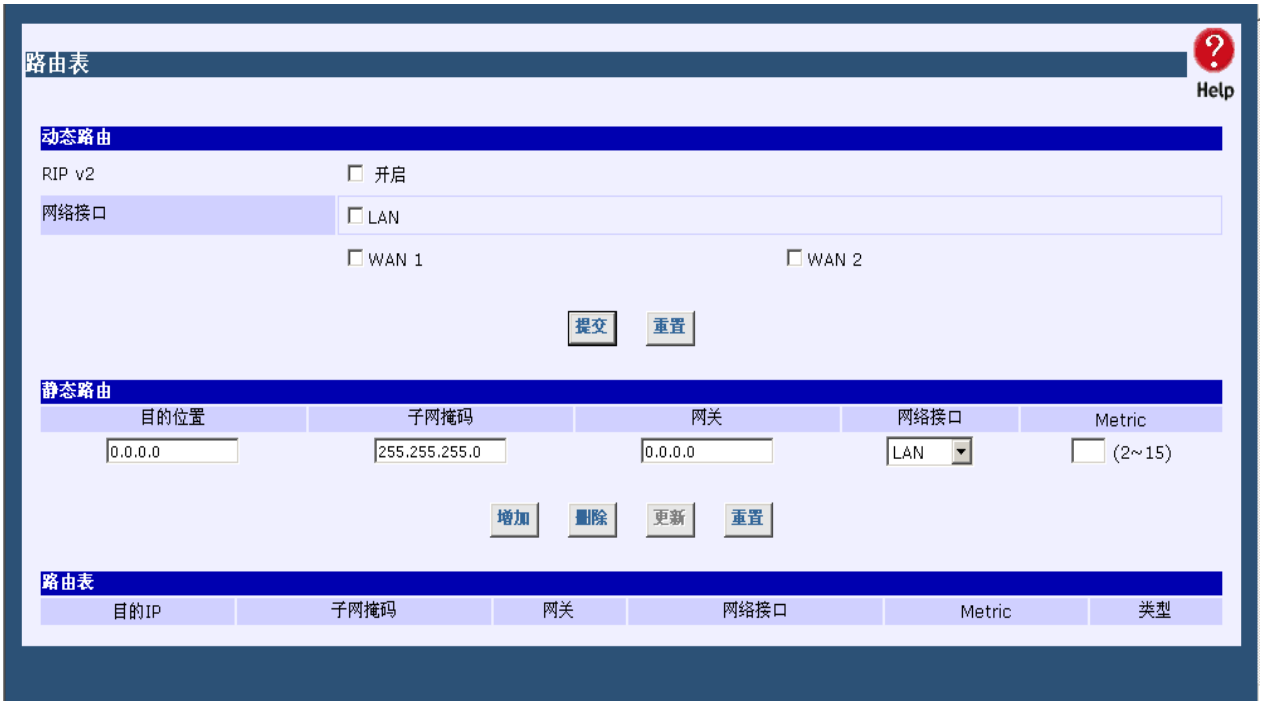


图 4-2: 路由表

注意:

如果路由表（routing list）中有一个或多个入口（下标从 0 开始），这些是系统入口，你不能修改或者删除这些入口。

路由设置

动态路由	• **RIP v2（路由信息协议 2）** – 它起着控制开关的作用.如果激活，所选择的广域网或者局域网将运行 RIPv1/v2，否则 RIP 功能不可用。 • **网络接口** –如果局域网或者其它广域网被激活，则局域网或者相应的广域网可以执行 RIP 功能。

静态路由	• **目的位置** – 远程局域网联机的网络地址。对于标准的“C”类网络，网络地址是 IP 地址的前三个域，第四个域被置为 0。 • **子网掩码** – 远程局域网联机的网络掩码。对于标准的“C”类网络，默认的掩码是 255.255.255.0 • **网关**– 网关或者路由的 IP，通过访问这个网关或者路由的 IP，其它路由最终才能到达目标 IP 地址。 • **网络接口** – 选择正确的接口，通常选“LAN”。“WAN”接口只有在 NAT（网络地址映像）无效时才可选。 • **Metric** – 到达远程局域网联机所经过的路由数目。最短的路径将被采用。
路由表	这个显示了用户当前设置的路由列表

配置局域网上其它的路由

所有非局域网内的设备的信息传输都必须前递给 2 WAN Load Balancer 以便可以前递给互联网。这个通过把其它路由器配置为 *Default Route（默认路由）* or *Default Gateway（默认网关）*来完成，如下所示：

静态路由举例

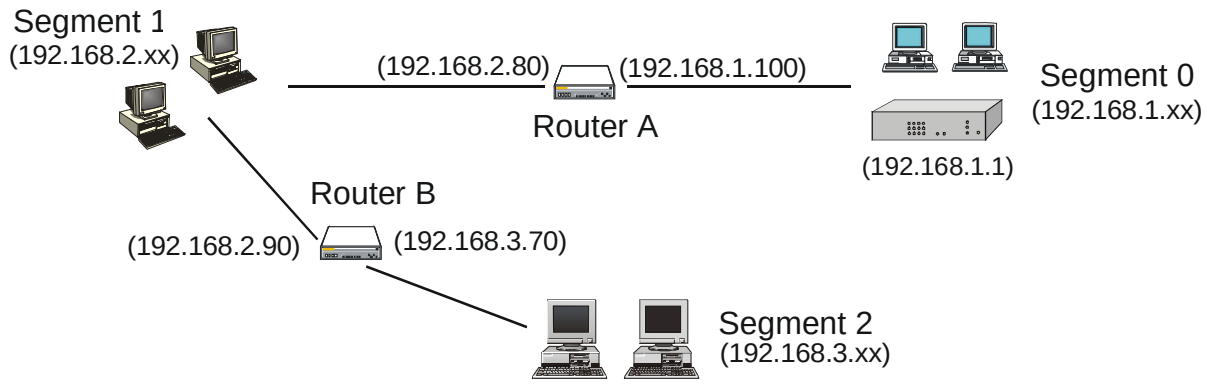


图 4-3: 静态路由举例

对于 2 WAN Load Balancer 网关的路由表

对于上图所示的局域网，有两个路由和三个局域网网段，2 WAN Load Balancer 需要两个入口，如下：

入口 1 (联机 1)	
目标 IP 地址	192.168.2.0
子网掩码	255.255.255.0
网关 IP 地址	192.168.1.100
接口	LAN
计量标准	2
入口 2 (联机 2)	
目标 IP 地址	192.168.3.0
子网掩码	255.255.255.0 (Standard Class C)
网关 IP 地址	192.168.1.100
接口	LAN
计量标准	3

路由器 A 的默认路由

目标 IP 地址	0.0.0.0
子网掩码	0.0.0.0
网关 IP 地址	192.168.1.1
计量标准	2

路由器 B 的默认路由

目标 IP 地址	0.0.0.0
子网掩码	0.0.0.0
网关 IP 地址	192.168.2.80
接口	LAN
计量标准	3

虚拟服务器

这个特性允许你让互联网上的用户访问局域网上的服务器。通常，因特网上的用户不能够访问你局域网上的服务器，因为：

- 你服务器的 IP 只在局域网上有效，在互联网上是无效的。
- 试图访问局域网上设备的操作都被 2 WAN Load Balancer 的防火墙挡住了。

虚拟服务器的特性解决了这些问题并且允许互联网上的用户连接到你的服务器上，如下所示：

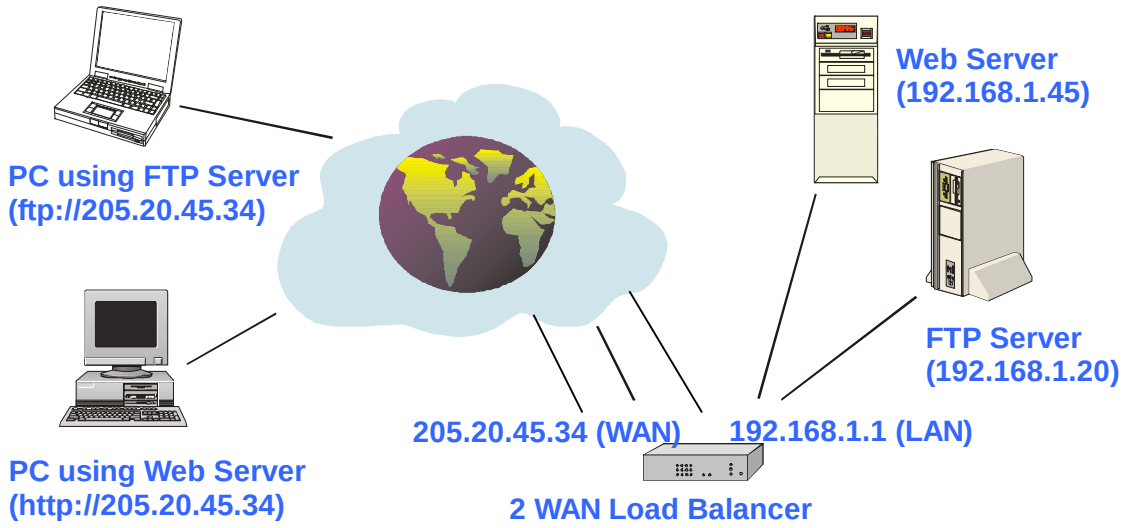


图 4-4: 虚拟服务器

需要注意的是，在这个例子中，两个互联网用户要连接在同一个 IP 地址上，但使用了不同的协议。

连接到虚拟服务器

一旦配置，任何互联网上的用户都可以连接到你的虚拟服务器上。他们必须使用 2 WAN Load Balancer 的互联网 IP 地址（ISP 所分配的 IP 地址）。

例：

```
http://205.20.45.34

ftp://205.20.45.34
```

- 对于互联网用户，所有局域网上的虚拟服务器.使用同一个 IP。这个 IP 地址是由 ISP 分配的。
- 这个地址应该是静态的，而不是动态，以便于互联网上的用户连接到你的服务器上。然而，你可以使用动态域名（动态域名特性，稍后这章会做解释），这样其它用户可以通过使用 URL 连接到你的虚拟服务器上，而不是使用 IP 地址。例如：

http://my_domain_name.dyndns.org
ftp://my_domain_name.dyndns.org

以下视屏允许你定义你自己的服务器类型。

图 4-5: 虚拟服务器

虚拟服务器设置

虚拟服务器配置	• **开启** – 根据需要激活或者关闭每个虚拟服务器 • **服务器名称** – 输入一个合适的服务器名。（默认地，12 个常用的虚拟服务器被列在客户虚拟服务器列表上） • **协议类型** – 选择这台服务器使用的网络协议(TCP/UDP) 。 • **IP 地址（内部网络）**，输入局域网的服务器 IP 地址。每一个服务器需要有一个固定的 IP 地址，或者有一个保留的 IP 地址。(这章前面的 ***Host IP*** 部分有关于保留 IP 地址的详细介绍)每一个服务器必须运行相应的服务器软件。 **（外部网络）**– 这个选择允许这台服务器绑定到任何广域网端口（WAN1 or WAN2），甚至同时绑定到所有的广域网端口上。 • **局域网端口范围** – 输入这台服务器向外传输时的端口范围。如果只需要一个端口，把它输入在两个域中。

	• **广域网端口范围**--输入这台服务器对内传输时的端口范围。如果只需要一个端口，把它输入在两个域中。 • **允许的远程 IP 范围**–它只允许某个范围内的远程 IP 地址访问虚拟服务器。默认的条目是 0.0.0.0 ~ 0.0.0.0,表示所有远程的 IP 都可以访问它。
按钮	• **增加** – 新建一个虚拟服务器条目。 • **删除** – 删除选中的条目。 • **更新** – 保存你对当前条目所做的修改。 • **重置** – 取消你自上次保存后所做的修改
虚拟服务器列表	这个列表描述定义了的所有客户虚拟服务器配置的细节信息。你可以通过点击选择对配置数据进行修改。

特殊应用

如果你通过非标准的连接或者端口使用互联网应用，你可能会发现它们不能正常工作，因为它们被 2 WAN Load Balancer 的防火墙阻塞住了。在这种情况下，你可以定义把这些应用定义为“特殊应用”以使得它们能正常工作。

需要注意的是，屏幕上的标语"流出" and "流入"指的是客户（PC）角度的传输。

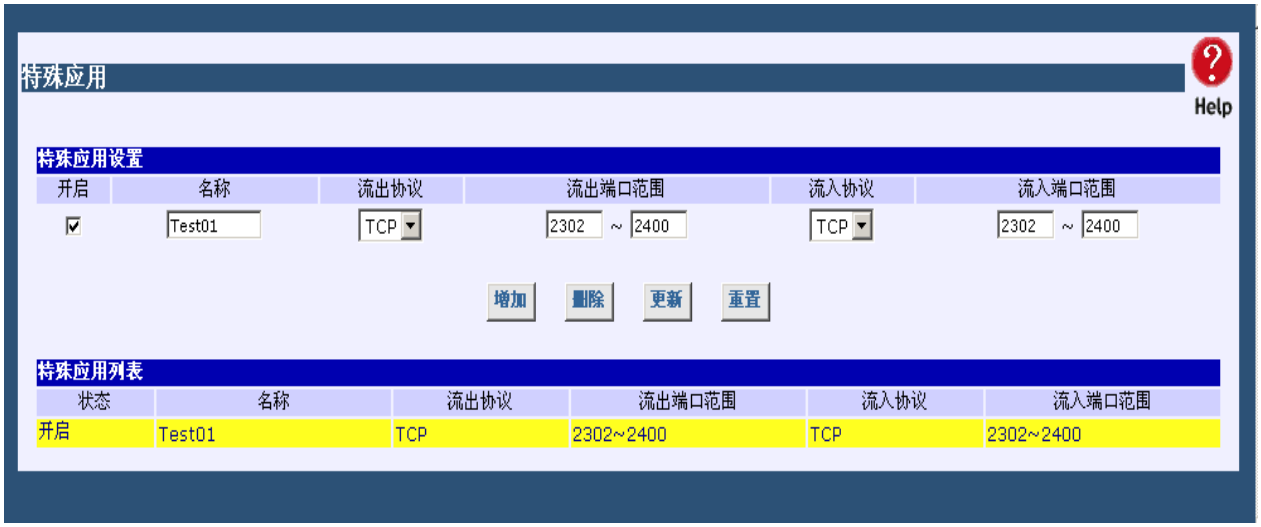


图 4-6: 特殊应用

特殊应用设置

特殊应用配置	• **开启** – 激活或者关闭特殊应用 • **名称** – 输入名字以描述特殊应用 • **流出协议** – 选择在向远程服务器或 PC 发送数据时使用的协议 • **流出端口范围** – 输入你发送数据的应用服务器所使用的端口范围。如果应用使用同一个端口，把它输入到两个域中。 • **流入协议** – 选择从远程服务器或 PC 接收数据时使用的协议 • **流入端口范围** – 输入你接收数据的应用服务器所使用的端口范围。如果应用使用同一个端口，把它输入到两个域中。
按钮	• **增加** – 添加一个特殊应用条目。 • **删除** – 删除所选条目. • **更新** – 保存你对当前条目的修改。 • **重置** – 取消你自上次保存后所做的修改。
特殊应用列表	显示最近定义的所有特殊应用的细节。你可以通过点击选择修改它的配置信息。

在你的 PC 上使用特殊应用

- 一旦特殊应用被正确的配置，你就可以正常的在你的 PC 上使用这些应用了。值得注意的是，任何时候每个特殊应用只能供一台 PC 使用。
- 同时，在一台 PC 使用完一个特殊应用后，需要一个"Time-out"（退出） 时间，之后另一个 PC 才能使用这个特殊应用。
- 如果一个应用仍然不能正常地工作，可以尝试使用“DMZ”（DMZ）特性。

动态域名解析

- 动态域名服务器适合与虚拟主机配合使用。它允许互联网用户使用 URL 连接你的虚拟主机，而不是使用 IP 地址。这也解决了动态 IP 地址产生的问题。通过一个动态 IP 地址，你的 IP 地址可以在每次连接 ISP 的时候发生改变，你必须为动态域名解析服务注册，2 WAN Load Balancer 支持四种类型的服务提供商：
- User Defined DDNS Server，(其它网站也可能提供相同服务，但不保证一定能有效)
- DynDNS ，http://www.dyndns.org
- TZO ，http://www.tzo.com
- 3322 ， http://www.3322.org

使用动态域名特征

1. 从你喜欢的服务提供商处注册服务。
2. 通过服务提供商提供的流程获得一个动态域名（服务器名）。
3. 配置动态域名服务视屏，如下所示：
4. 之后 2 WAN Load Balancer 会自动根据动态域名服务提供商更新你的 I P 地址。
5. 通过互联网，用户现在可以使用你的域名访问你的虚拟服务器了。

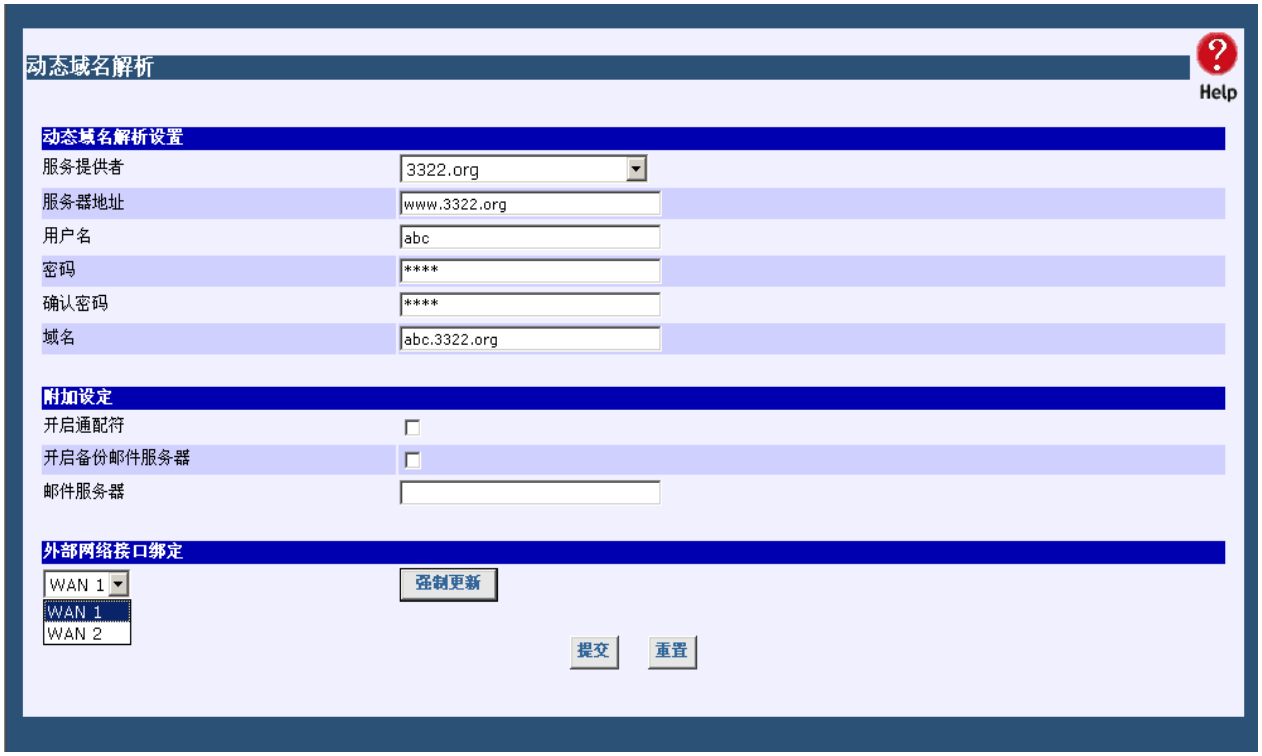


图 4-7: 动态域名解析

动态域名设置

动态域名服务	这个下拉菜单可以激活 / 关闭动态域名服务特性和选择需要的服务提供商 • **Disable** – 关闭动态域名服务。 • **TZO** – 选择这个使用TZO 服务(www.tzo.com)。你必须配置TZO部分的视屏 • **DynDNS** – 选择这个使用标准服务(通过www.dyndns.org或其它的提供商)。你必须配置标准客户视屏。 • **3322** – 这个可以在中国得到. 它类似于 “DynDNS” • **用户定义的 DDNS 服务** – 这个是用户定义的 DNS 服务提供商. 如果提供商不是 TZO, dyndns.org 或者 3322.
附加设置	如果使用标准客户，可以得到如下选项： • **Enable Wildcard（使用通配符）** –如果选中，发送给子域（在你的域名之下）的传输也将提前发给你。 • **Enable backup MX（使用邮件交换备份）** –如果选中，你必须输入邮件交换器。 • **Mail Exchanger（邮件交换器）** –如果之上的设置选中，输入邮件交换器的地址
广域网端口绑定	• 选择动态域名服务使用的广域网端口。 • “强制更新”按钮将立即在动态域名服务上更新你的记录。

Multi DMZ

这个特性允许每个广域网端口 IP 地址连接到你局域网的一个计算机上。所有这台计算机发送的数据都会与这个广域网端口的 IP 连接在一起。所有这个 IP 发送的数据也会前递给这台计算机。这样，在“DMZ PC”和其它互联网用户或服务器之间可以进行自由的双向通讯。

注:

"DMZ PC"在防火墙之外，导致它对于黑客的攻击或其它入侵很脆弱。基于这个原因，你应该只在需要的时候再激活 DMZ 特性。

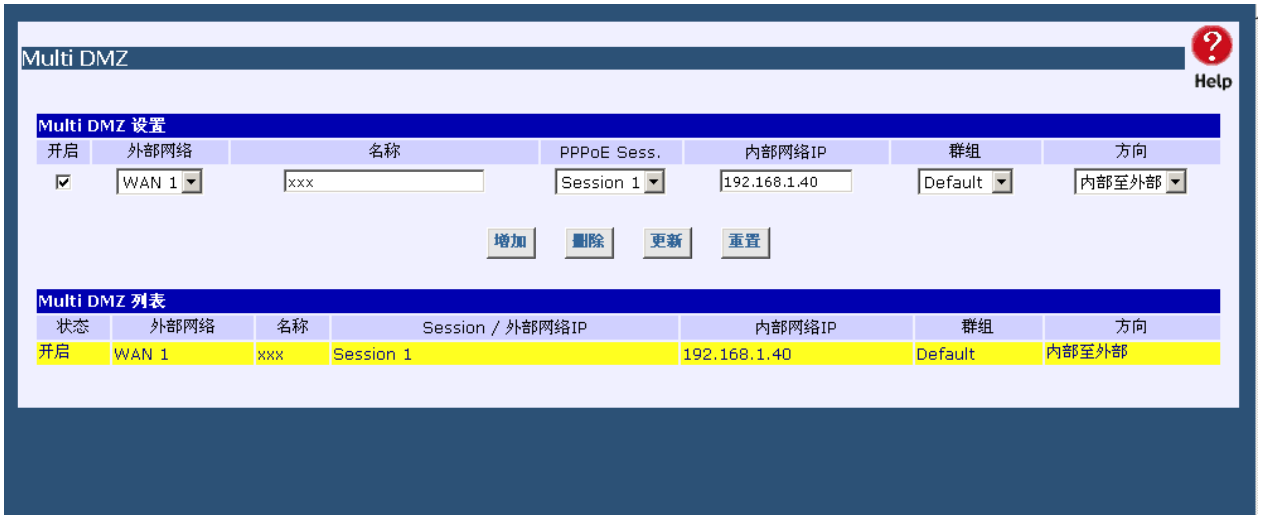


图 4-8: Multi DMZ

Multi DMZ 设置

Multi DMZ 编辑	• **开启** – 根据需要激活或关闭 DMZ • **外部网络** – 把期望的广域网端口绑定在特定的局域网服务器上。（最大有 8 个广域网端口可以使用）。它的连接类型可以根据广域网连接类型改变。 • **名称** – 输入一个可以让你记住这个设置的名字。这个名字可以随便选择并且不会有任何影响。 • **内部网络 IP** – 输入 PC 的 IP 地址，将其连接到广域网端口的 IP 地址。这个 IP 地址需要固定或者保留。（*参考服务器 IP* 关于保留 IP 地址的内容） • **群组** – 你可以通过定义组（在服务器 IP 页面中）授权哪些用户可以使用 DMZ。 • **方向** – 对于 DMZ，你可以允许仅限制内部，仅限制外部，或者限制内部和外部的传输。
Multi DMZ 列表	多组 DMZ 列表列出了当前定义的所有 DMZ 配置数据的详细信息。你可以通过点击选择修改相应的配置信息。

UPnP 设定

通过 UPnP（通用即插即用）功能，你可以轻松的安装和配置整个网络，使网络能自动监测和控制相应的设备和服务。

图 4-9: UPnP 设定

UPnp 安装设置

UPnP 选项	如果设置了*开启 UPnP*，这个设备将在本地网络上注册。你将在 Windows XP 的“网上邻居”处发现一个图标。每次当你用端口映射添加一个新的设备时，新的设备将出现在映射列表中。
UPnP 端口映射列表	如果 UPnP 被置为开启，这个表将展现已定义的所有客户虚拟服务器的详细配置信息。

NAT 设定

NAT (网络地址转换) 技术允许一个广域网（互联网）IP 地址同时被多个局域网用户使用。

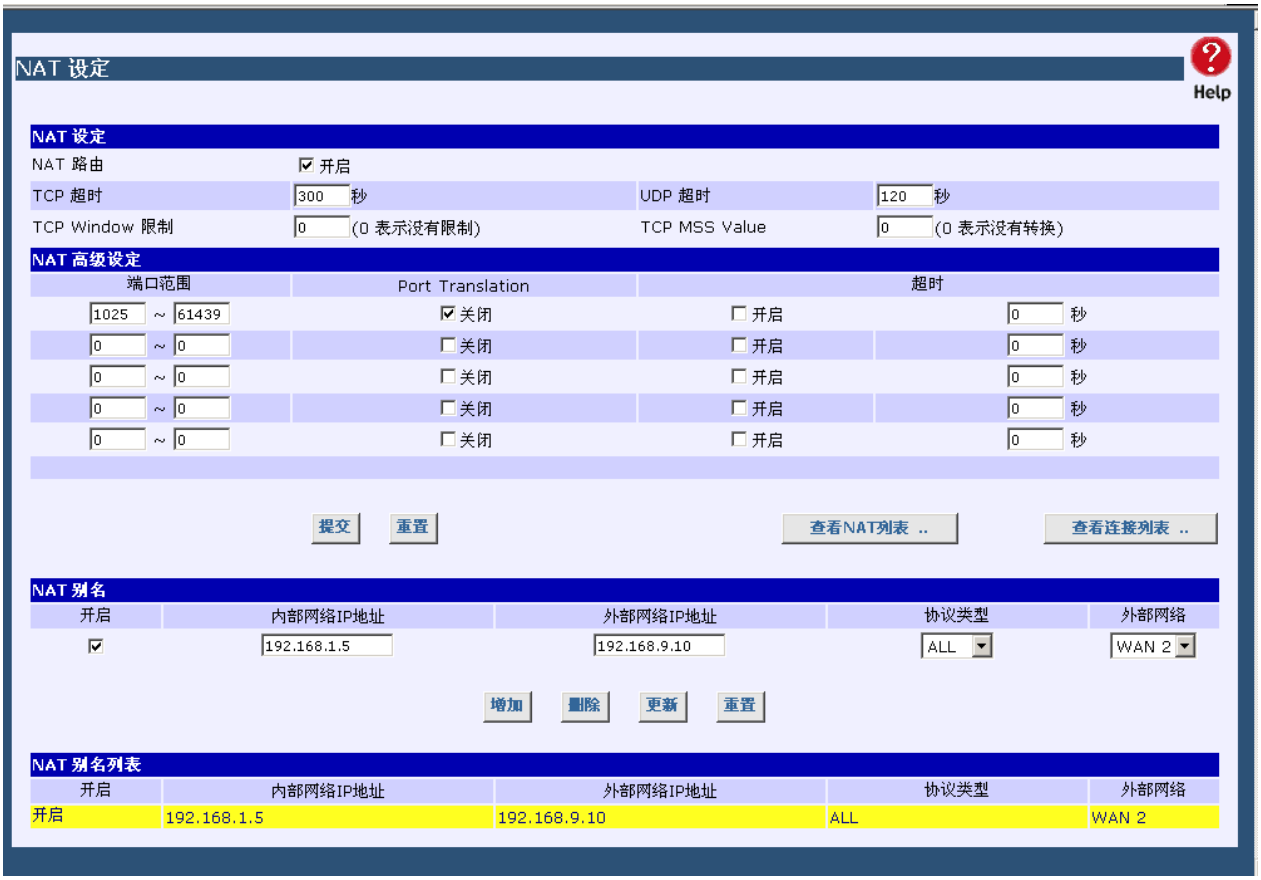


图 4-10: NAT 设定

NAT 设定

NAT 设定	• **NAT 路由**-通过修改状态栏可以激活或者关闭 NAT。如果你关闭了 NAT，那它将像一个桥或静态路由一样工作。它的大多数特性都无法获得。 • **TCP 超时** – 输入每个广域网端口期望的中止时间。默认值是 300 秒。 • **UDP 超时** - 输入每个广域网端口期望的中止时间。默认值是 120 秒。 • **TCP Windows 限制** – 输入输入每个广域网端口期望的窗口数。默认值是 0。 • **TCP MSS Value** – 输入每个广域网端口 MSS（最大联机）的值。
NAT 高级设定	如果一些信息包的端口不能转换成特殊的应用，你必须设置状态为“激活”并输入端口范围的值。另外，如果它的端口不能在规定的时间内转换，你必须设置状态为“激活”并输入中止时间的值。
NAT 别名	对于每一个别名条目，广域网 IP 表现为一个本地局域网 IP 服务器的别名，这些服务器通过特定的广域网端口和特定的协议访问互联网。

NAT 别名列表	NAT 别名类标表示了最近定义的所有 NAT 别名配置信息。你可以通过点击选中对它进行修改。
查看 NAT 列表	列出所有的 NAT 配置细节信息。
查看连接列表	这个表现了所有 NAT 条目的当前细节，包括接口，协议，状态，目标 IP，广域网 IP，本地 IP，闲置时间和接收/发送数据包信息。

进阶设定

- **外部网络安全设定** – 这些设置决定了 2 WAN Load Balancer 是否应当响应广域网端口发出的 ICMP（ping）请求
- **协议&端口绑定** – 这允许你通过选择你想要的协议类型绑定任何广域网端口。

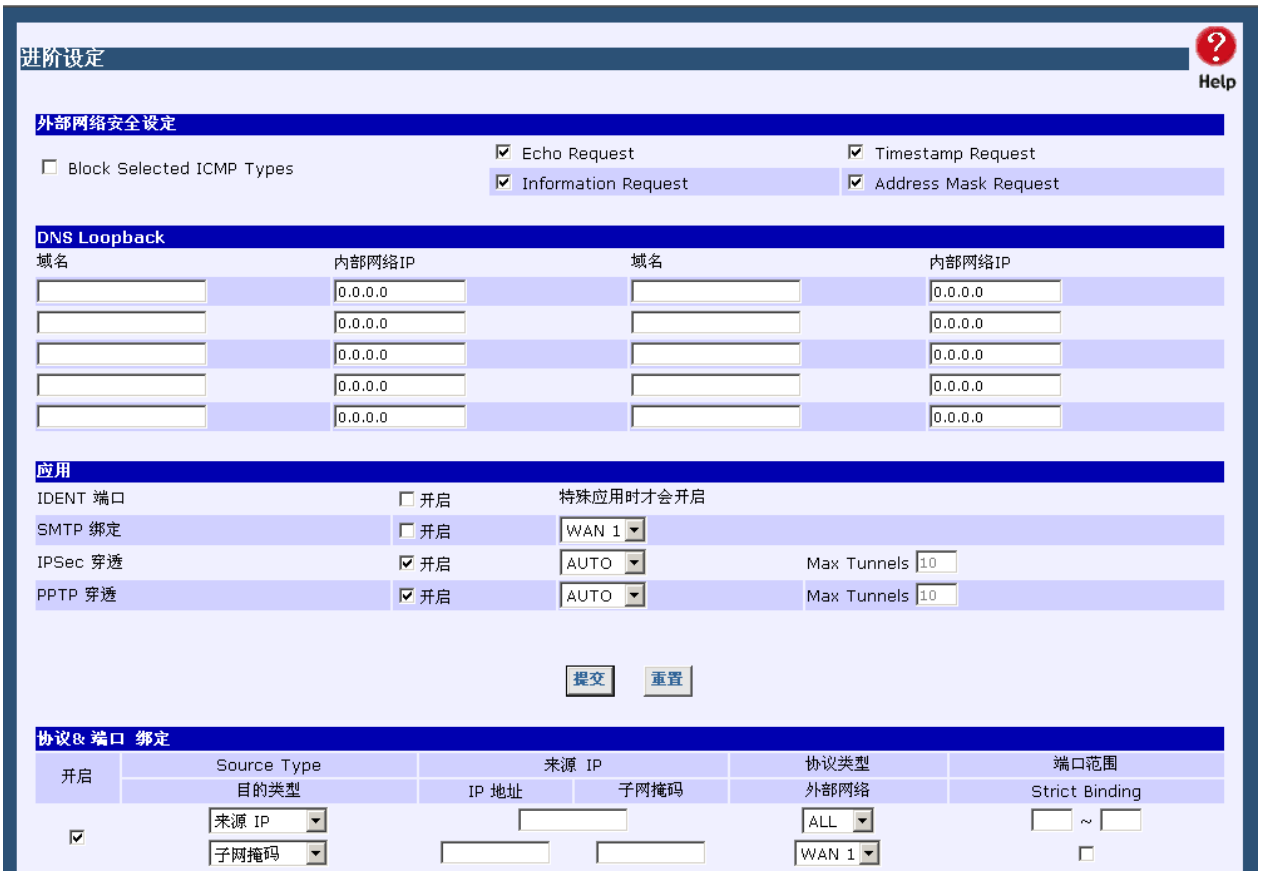


图 4-11：进阶设定

进阶特性设置

外部网络安全设定	• **IDENT 端口** – 端口 113 关系到互联网的验证/授权服务。当你电脑的一个客户程序连接到远程服务器以获得像 POP，IMAP，SMTP 这样的服务时，远端的服务器将发送一个身份验证的请求，这个请求通过 113 端口来监听。这意味着黑客可以通过 113 端口探测你的个人信息。这个选项的默认值为关闭。 • **Block Selected ICMP Types** – 这个设置决定是否这个设备应该来自广域网端口的 ICMP 请求。如果选择了某个类型，相应的信息包将被阻塞。否则，信息包可以接受。 • **IPSec 穿透** – 允许 IPSec 通过 • **PPTP 穿透** – 允许 PPTP 通过
DNS Loopback	这项在你的局域网有多台服务器，并且它们的域名已经在 DNS 上注册的时候使用。为了避免 DNS 循环问题，请输入下列信息： • **域名** – 输入你为本地服务器定义的域名。 • **内部网络 IP** – 输入你本地服务器的私有地址。.

接口绑定	**SMTP (简单邮件传输协议)绑定** 除非在每个端口上使用不同的 ISP 的邮件帐户，你可以忽略这些设置。 一些 ISP 配置它们的 E-mail 服务器使得他们不会接受来自不是他们分配的 IP 的邮件。如果你使用不同 ISP 的帐户，通过错误的广域网端口发送邮件可能导致邮件不被接受。这种情况下，你可以使用下列设置来更正。 • **开启** - 如果激活，你在下面定义的广域网端口将被用于所有发出的 SMTP 传输。否则，广域网端口将不被使用。 • **网络接口** – 选择限制需要的广域网端口。
协议&端口绑定	**协议和端口绑定** 如果你希望确保特殊的传输通过一个特定的广域网端口发出，则使用协议和端口绑定。 • 开启 - 激活或关闭每个需要的条目。 • **来源 IP** - 信息包发送的源 IP 地址。 • **目标 IP** – 信息包发送的目标 IP 地址。 • **子网掩码 –** 通过一个子网掩码（非 255.255.255.255），你可以按你的目标建立一个子网。 • **协议类型** – 选择你希望配置的协议类型。 • **端口范围** - 输入你希望配置的传输的起止端口范围。如果只有一个端口被使用，两个域中都要输入这个端口值。 • **外部网络** -选择你希望传输使用的广域网端口。
协议&端口 绑定列表	这个表展示了最近定义的所有协议和端口配置数据的详细信息。你可以通过点击选择修改它们。

5: 防火墙设定

概述

- ***内容管制*** – 通过 IP 地址，URL 或者关键字封锁一个特定的网站
- ***存取过滤*** – 封锁所有的互联网访问，一个已知的端口或用户根据组访问定义的端口
- ***最大会话数设定*** – 当设备检测到在取样时间内有新的联机超过了联机的最大值，可以限制用户访问互联网。比如，病毒，syn flood （冲击波）等。
- 系统过滤例外 - 这个特性允许配置一个未识别的端口，这些信息包将被处理，使一些程序可以更流畅的运行。这也可以应用于未来的一些应用，通过这种机制它们可以运行的更好。

内容管制

这个特性允许你封锁对不期望的网站的访问。你可以通过 URL，IP 地址，或关键字进行封锁。你还可以对不同的组进行不同的封锁。

- 在操作中，检索每一个 URL，检查它是否匹配或包括这里输入的 URL 或关键词，然后，通过 DNS 检查，决定请求站点的 IP 地址，查看它是否满足视屏上的 IP 地址条目。
- 注意一个单独的 IP 地址可能对应多个网站（共享 IP）。在视屏中输入一个 IP 地址有可能封锁这个 IP 地址上的所有网站。

图 5-1: 内容管制

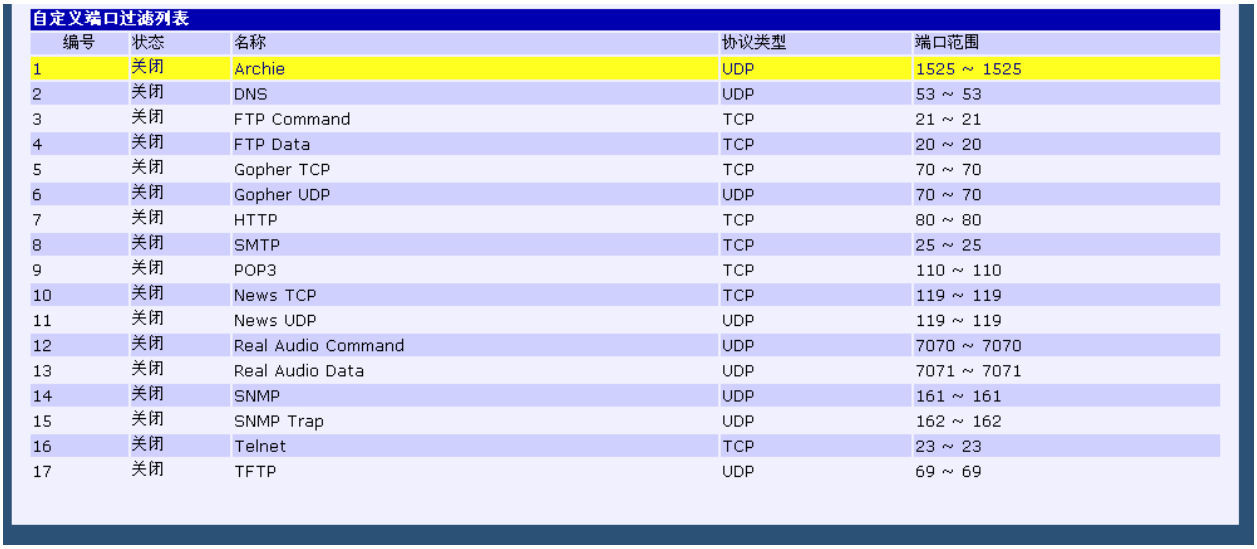
内容管制设置

群组	允许你对不同的计算机组设置不同的封锁规则。 • 所有的 PC 用户如果不移动到特定群组中，都将被放在缺省的组中。 • 如果你希望对每个用户使用相同的约束，选择缺省的组。在这种情况下，不需要将用户加入特定群组。 • 如果你希望对不同的组做不同的约束，选择相应的组，点击“选择”按钮。屏幕将更新选择的组的数据。 • **内容管制类型**– 阻挡 Internet 存取：如果你选择了黑表，它将封锁列表上的 URL 访问项。允许 Internet 存取：如果你选择白表，它只允许列表上的 URL 访问项可以不受管制。 • **设置类型** – 提交黑表或白表的按钮。
存取项目	• **状态（开启/关闭）**– 根据需要激活或关闭每个设置。 • **URL/IP 地址/关键字** – 输入想要封锁的 URL，IP 或关键字。
Internet 存取列表	这个列表将列出所有你建立的封锁规则。你可以通过点击选中相应的行进行修改。

存取过滤

网络管理员可以使用访问过滤器获得互联网访问的控制权以及局域网用户可用的应用。

- 可以使用五个用户组，每个组允许拥有不同的访问权限。
- 所有的 PC 用户都被放在缺省的组里，除非通过主机与群组分配到其它的组里。



自定义端口过滤列表

编号	状态	名称	协议类型	端口范围
1	关闭	Archie	UDP	1525 ~ 1525
2	关闭	DNS	UDP	53 ~ 53
3	关闭	FTP Command	TCP	21 ~ 21
4	关闭	FTP Data	TCP	20 ~ 20
5	关闭	Gopher TCP	TCP	70 ~ 70
6	关闭	Gopher UDP	UDP	70 ~ 70
7	关闭	HTTP	TCP	80 ~ 80
8	关闭	SMTP	TCP	25 ~ 25
9	关闭	POP3	TCP	110 ~ 110
10	关闭	News TCP	TCP	119 ~ 119
11	关闭	News UDP	UDP	119 ~ 119
12	关闭	Real Audio Command	UDP	7070 ~ 7070
13	关闭	Real Audio Data	UDP	7071 ~ 7071
14	关闭	SNMP	UDP	161 ~ 161
15	关闭	SNMP Trap	UDP	162 ~ 162
16	关闭	Telnet	TCP	23 ~ 23
17	关闭	TFTP	UDP	69 ~ 69

图 5-2: 存取过滤

存取过滤设置

群组	允许你为不同的计算机组设置不同的访问权限 • 如果你想要把相同的约束应用到所有用户，为组选择缺省。在这种情况下，不需要进入主机与群组页面。 • 如果你希望对不同的组应用不同的约束，选择相应的组。页面将更新所选的组的数据。
过滤设定	为这个组选择所需的选项: • **不过滤** – 没有阻塞，互联网访问不受约束。 • **阻挡所有** – 所有访问都被封锁，无法访问互联网。 • **阻挡所选项** – 选择的项被封锁。你可以通过复选框封锁已知的服务，或定义自己的过滤器。
ICMP 过滤	如果你激活了 ICMP 过滤器，意味着它将封锁用户定义的本地到远端的 ICMP 信息包类型。
自定义端口过滤	这个部分是可选的。它允许你根据需要定义你自己的过滤器。 • **过滤名称** – 为过滤器输入一个名字。 • **协议类型** – 选择你希望封锁的协议类型。 • **端口范围** – 输入你希望封锁的端口范围。如果只有一个端口需要封锁，在两个域里输入同一个端口。
自定义端口过滤列表	这个列表表现了最近定义的所有用户自定义过滤配置的详细信息。你可以通过点击选中进行修改。

最大会话数

这个新的特性允许当新联机的数目超过你在取样时间域里设置的最大值时， 放弃广域网和局域网的新联机。

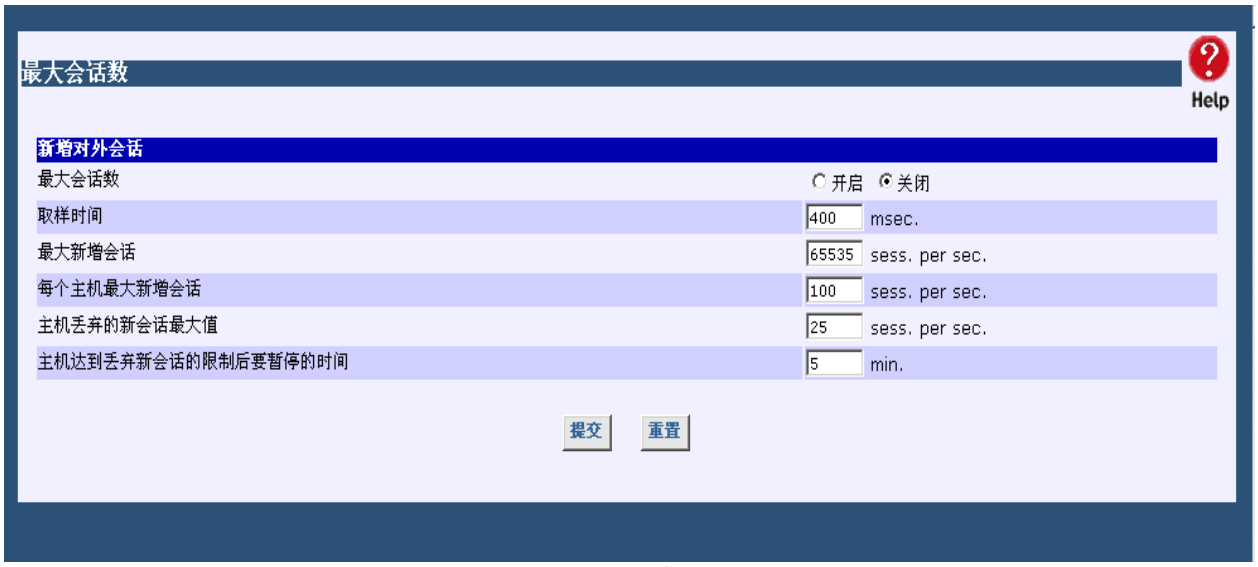


图 5-3:最大会话数

最大会话数 设置

取样时间	新联机之间的时间间隔。只有最近发生的新联机会根据输入的取样时间进行统计。（缺省值是 400 毫秒）
最大新增会话	系统中取样时间可以接受的新联机的最大值。任何新输入的联机将在超时后被抛弃（默认值：65535 联机/秒）
每个主机最大新增会话	取样时间内可接受的最大新联机的值。任何超时的新联机都将被服务器抛弃。（缺省值：100 联机/秒）
主机丢弃的新会话最大值	如果放弃的新联机的数目超过了取样时间内的最大值，任何处于暂停的新联机都将被放弃。（缺省值：25 联机/秒）
主机达到丢弃新会话的限制后要暂停的时间	在暂停时间联机内，当放弃得新联机超过定义得最大值时，系统不再服务暂停服务器的新联机。（缺省值 5 分钟）

系统过滤例外

系统过滤例外 – 它将拒绝任何从未验证的端口发出的信息包，以封锁黑客的扫描端口程序。然而，它也在一些情况下产生问题，在服务器（如，SMTP 服务器的端口 113）或者广域网客户端需要发送一个相应信息包以确认他们交互的活动时。

图 5-4: 系统过滤例外

系统过滤例外设置

系统过滤例外规则	• **开启** – 如果复选框被选中，它将允许系统过滤例外。 • **网络接口** – 你可以选择局域网，任何广域网端口或者所有的产生信息包的接口。 • **协议类型** – 包类型（在以上的接口中选择）将直接在这台设备上进行处理。 • **来源端口范围** – 输入你希望配置的外部端口的起止范围。如果只使用一个端口，在两个域中输入同一个端口。 • **目的端口范围** –输入你希望配置的设备端口的起止范围。如果只使用一个端口，在两个域中输入同一个端口。
系统过滤例外规则列表	这个表显示了你建立的系统过滤例外规则的详细信息。你可以通过点击选中修改数据

6:频宽管理

概述

2 WAN Load Balancer 通过加入一个频宽管理应用程序来提供高质量的网络支持服务。
由于它根据用户定义的策略对发出的信息包进行分类，实时应用需要更好的响应和执行。

QoS 基本设定

下面的网页指导你如何设置激活 QoS

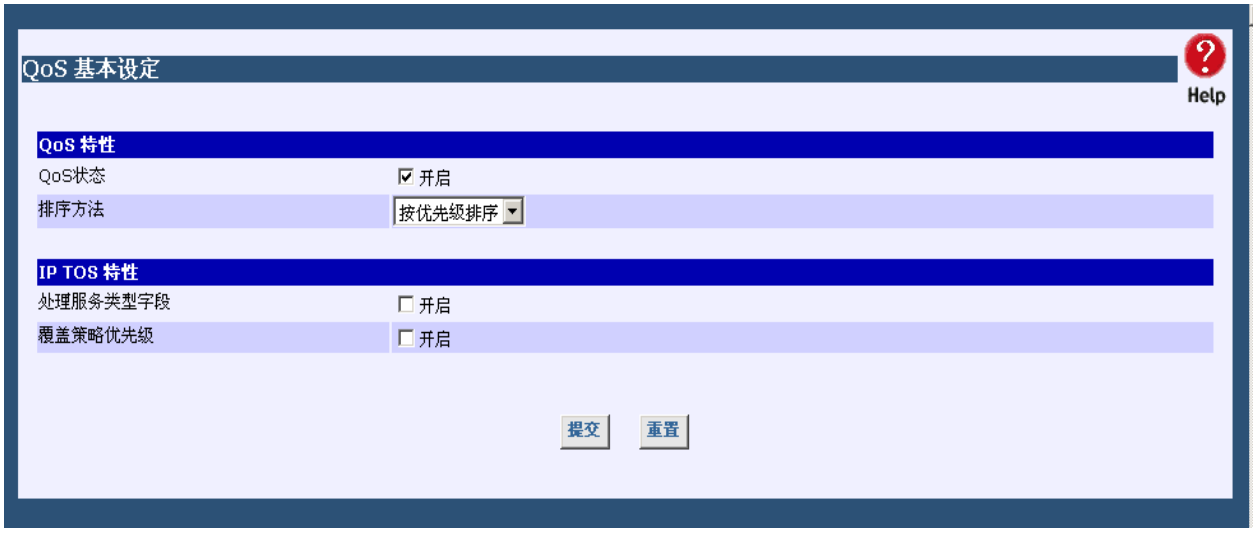


图 7-1: QoS 基本设定

Qos 基本设定

QoS 特性	• **QoS 状态** – 如果设置为激活，它将执行 QoS 功能。 • **排队方法** – 关于信息包队列的选择管理策略。引入“队列优先级”-需要广泛执行的第一个排队变化。
IP TOS (Type Of Service) 特性	• **处理服务类型字段** – 在 IP 封包头里有一个 8 Bits 的栏位,这个栏位有包含一些值是用来 handle network.如果你选择 “Enable” 它就会启动这个服务 • **覆盖策略优先级** – 如果选择 “YES” TOS 的优先权会把 QoS policy configuration 覆写过去

QoS 规则设定

当你使用 QoS 时，你必须定义一些策略，激活所选的信息包，以获得更高的通过优先级。

.

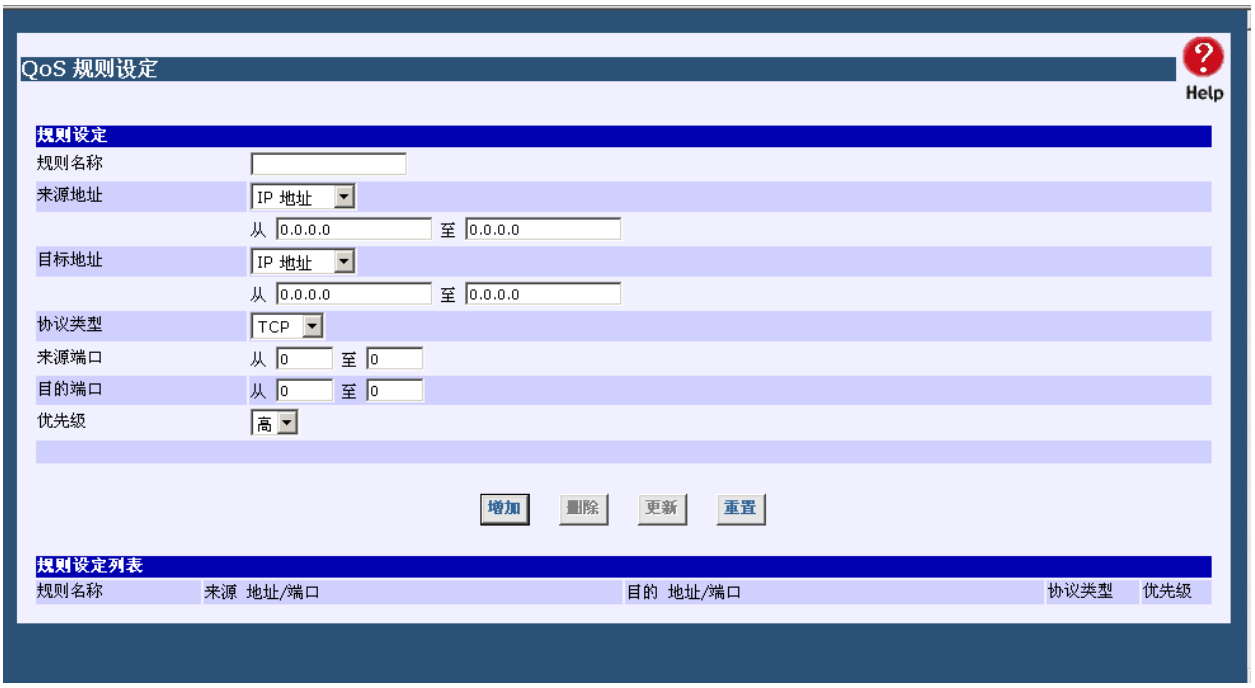


图 7-2: QoS 规则设定

QoS 策略设置

策略优先级	这个部分识别每个策略 • **规则名称** – 输入一个适合的名称。通常，你应该为网络传输使用“策略名”。 • **来源地址** – 定义信息包的源地址。它有两种类型，IP 地址和 MAC 地址。如果你选择 IP 地址，你可以定义 IP 地址范围；如果你选择 MAC 地址，你可以定义四个 MAC 地址。 • **目标地址** – 定义信息包的目标地址。（解释与“Source Address”类同） • **协议类型** – 这个域定义传输信息包的类型，如，ICMP，TCP 或者 AH。 • **来源端口** – 定义信息包源的端口。 • **目标端口** – 定义信息包目标的端口。 • **优先权** – 2 WAN Load Balancer 支援 高,中,低 的封包优先权
规则设定列表	这个列表显示了你设置的所有策略优先级配置的详细信息。你可以通过点击选中某个行进行修改。

7: 管理

概述

提供以下的进阶功能

- 系统管理 – 管理员
- 防火墙设定 – 邮件警讯
- 系统管理 – 简单网络管理协议
- 日志 – 系统日志
- 系统管理 – 软件更新

这个章节包含这些特点的配置和用途.

管理员

远程管理 – 提供您经由 Internet 来对设备进行管理,您可以限定在一个指定的 IP 或是 IP 范围进入.
管理者密码 – 您可以设定一个密码来管理进入设备的使用者.

图 7-1: 管理员

设定 – 管理员

远程管理设定	• **远程升级** – 如果激活此功能,您可以经由 Internet 来进行韧体的升级,如果选择关闭,韧体的升级必须经由一台在 LAN 中的 PC 执行. • **远程管理** –如果激活此功能,您可以经由 Internet 来进行设置,如果选择关闭,设置必须经由一台在 LAN 中的 PC 执行. • **端口** – 您可以设定存取的端口.默认值是 8080. • **允许远程 IP 范围** – 可以设定限定远程的某个 IP 进入设备. 1. 保留空白的话将允许所有的 PC 进入. 2. 这些地址必须是真实 IP,不能为 LAN 中的虚拟 IP. 3. 设定一个特定的 IP.
管理员密码	您可以设定一个设备密码,默认值是"没有密码".
OnMS（可选）	中央管理系统：可以作为中央管理系统的被管理端 **开启** – 激活被管理端模块 **IP 地址** – 中央管理系统服务器端ＩＰ地址

邮件警讯

这个特点是在设备发现有异常现象的时候将会发送电子邮件到网络管理员的信箱.

图 7-2: 邮件警讯

设定 –邮件警讯

全局设定: 通知依据	• **连线失败** – 如果激活此功能,如果有任何 WAN Port 联机中断,他将发送电子邮件通知管理员. • **Ping 攻击**–这个特点是有用防止 ICMP 攻击 WAN 或 LAN 。如果有过量的 ping 包(ICMP)会发送电子邮件到管理员的邮箱.
邮件警讯设置	• **邮件 SMTP 服务器地址** – 当需要时 EMAIL 将经由这个服务器发送. • **用户名** – 对发信者设定一个名称. • **密码** – 对发信者设定一个密码. • **传送者地址** – 发信人收信的地址. • **电子邮件位置** – 警报信件将会被送达此地址,通常这是管理者的地址.
邮件警讯设置列表	这里列出您输入的所有 EMAIL 警报的名单,您并且可以修改它的内容.

SNMP

这是当您有使用 SNMP (Simple Network Management Protocol) 的软件时设定.如果您有 SNMP 软件您可以使用标准的 MIB II 文件与此设备搭配使用.

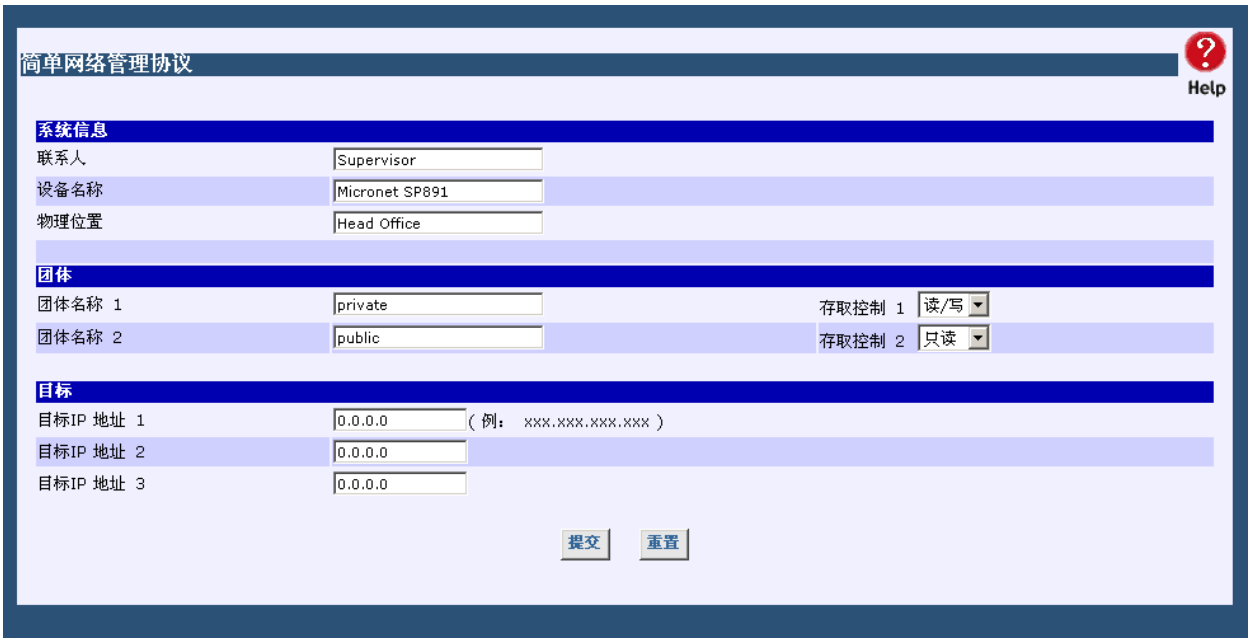


图 7-3: SNMP

设定 – SNMP

系统信息	• **联系人** – 设定负责此设备的管理员名称. • **设备名称** – 设定此设备名称. • **物理位置** – 设定设备的地址.
团体	• **团体名称** – 您需要设定一个密码在这台设备及管理的计算机中.当需要监控的时候管理员必须使用相同的名称. • **存取控制** – 可以设置管理的权限,您可以设置为读写/只读/禁止.
目标	输入接收端的 IP 地址(安装了 SNMP 软件的计算机).

系统日志

这里可以发送实时的系统信息到您的网页或是计算机.

Syslog 设定 – 您可以选择最多三台接收端.

信息监看 – M 您可以监看 100 条实时的系统信息.当机器重新启动或是关机的时候将会被清除.

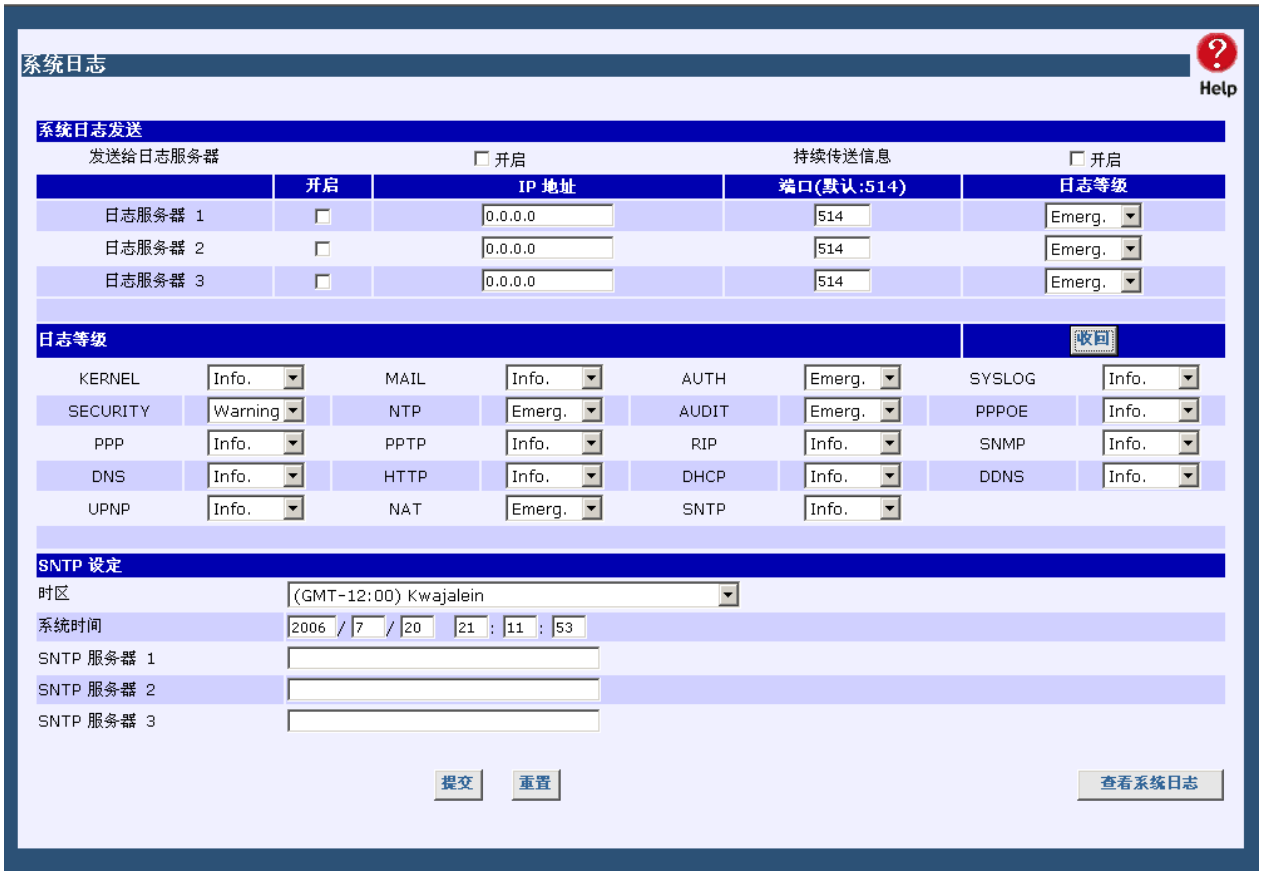


图 7-4: 系统日志

设定 – 系统日志

系统日志发送	• **发送给日志服务器** – 如果您希望系统信息被发送出去,请激活此项.
	• **持续传送信息** – 如果激活此项选择,您将保留发送的信息,否则被发送的信息将会被删除.
	• **日志服务器** – 最多可以设置三台服务器.
	  • **IP 地址**: 设定 Syslog 服务器的 IP 地址.
	  • **端口**: 如果 Syslog 服务器没有使用默认的端口,您可以自行设置 Syslog 服务器的端口.
	  • **日志等级**: Syslog 分为 8 个等级(从紧急到侦测错误),更低的等级会有更多的信息产生.

日志等级	• 按下 “Expand” 按钮,选择合适的等级和服务器.
SNTP (Simple Network Time Protocol) 设定	SNTP 是经由互联网上的时间服务器去同步您的设备.您选择适合的服务器地址去同步您的设备

从远程使用 Web 的方式设定

通过互联网上远程的计算机去设定 2 WAN Load Balancer:

1. 首先确定您的计算机及 2 WAN Load Balancer 已经连接上互联网.
2. 打开您的浏览器.
3. 输入 HTTP://2 WAN Load Balancer 的 IP 地址及端口,如 HTTP://123.123.123.123:8080

   - 这个例子假设, WAN IP 地址是 123.123.123.123 并且端口是 8080 .
   - 如果您有使用动态域名的话,您也可以使用动态域名来进行连接.
     HTTP://my_domain_name.dyndns.org:8080

管理密码

输入您所希望的密码, 再输入一次确认密码.

当您连接到 2 WAN Load Balancer 时,设备会提醒您输入您当时设定的密码,如下图:

图 7-5: 登陆密码

软件更新

软件更新允许您升级软件或备份系统设置.

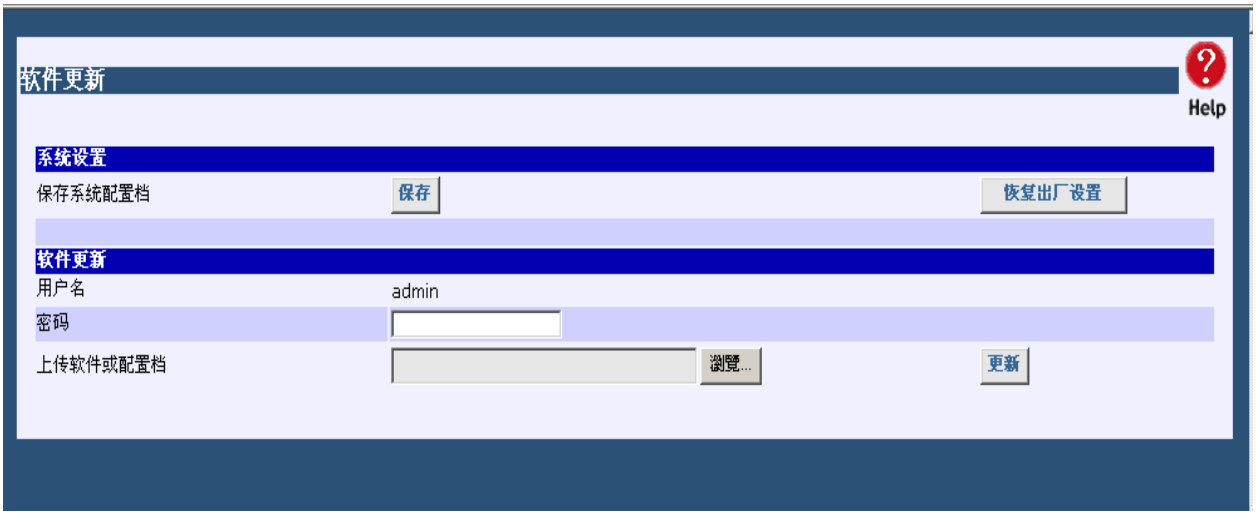


图 7-6: 软件更新

- 您能备份您的系统设置,并保存在其它地方在以后使用.
- 按下恢复出厂值的按钮可以恢复设备到默认值.

8: 网络讯息

系统状态

使用系统状态观看这个屏幕。

图 8-1:系统状态

数据 – 系统状态

WAN 界面	• **连接类型** – 如 DHCP, 固定 IP, PPPoE or PPTP. • **状态** – 联机或是断线 • **强制更新** – 如果您是使用 DHCP 客户端的时候执行更新您的 IP 时使用. • **联机/断线** – 当使用拨号类型的 PPPoE 或是 PPTP 时使用. • **IP 地址** – 2 WAN Load Balancer 的 WAN IP. • **子网掩码** – IP 地址配合的子网掩码. • DNS – 当前的 DNS 地址. • **网关** –2 WAN Load Balancer 的网关地址. • **MAC 地址** – 2 WAN Load Balancer 的 WAN Port MAC 地址.

LAN 界面	• **IP 地址** – 2 WAN Load Balancer 的 LAN Port IP 地址. • **子网掩码** – IP 地址配合的子网掩码. • **MAC 地址** –2 WAN Load Balancer 的 LAN Port MAC 地址. • **DHCP 服务器** – DHCP 服务器的使用状态,您可以开启会是关闭.
系统统计	• **硬件 ID** – 制造商对这台设备所设定的 ID. • **韧体版本** – 此设备当前的韧体版本. • **NAT** – NAT 的状态是开启或是关闭. • **负载均衡** – 负载均衡的状态是开启或是关闭. • **虚拟服务器** – 虚拟服务器的状态是开启或是关闭. • **特殊应用** – 特殊应用的状态是开启或是关闭. • **Multi DMZ** – 查看状态是开启或是关闭. • **阻挡 URL** –查看状态是开启或是关闭.
设备监看	• **系统开启时间** – 查看系统开机时间. • **CPU 使用率** – 当前的 CPU 使用率. • **内存 使用率** – 当前的内存使用率. • **封包队列** –当前的封包队列百分比。
按钮	• **刷新** – 更新数据. • **重启** – 重新启动 2 WAN Load Balancer. • **恢复出厂值** – 删除所有的设置恢复到出厂值.

恢复出厂值

当点击"恢复出厂值" 按钮将出现 以下屏幕:

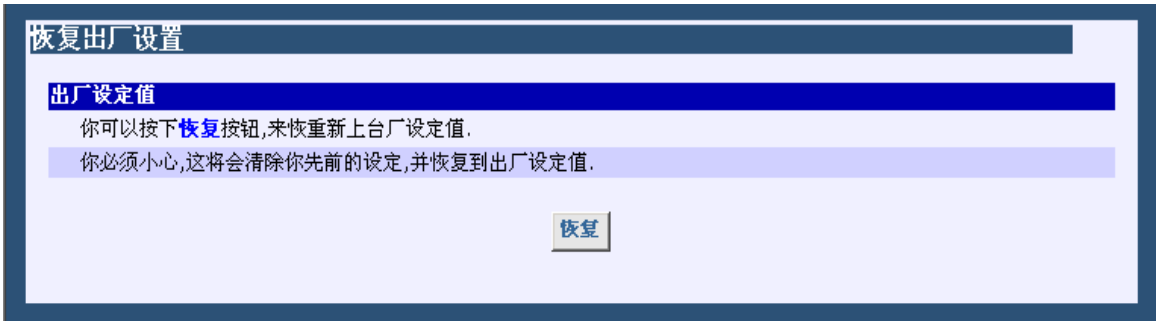


图 8-2: 恢复出厂设置

如果您点击此按钮意味着:

- 所有的设置将会被删除.
- 所有的设置会**恢复**到出厂值.
- DCHP 服务器作用将启用。

外部网络状态

您可以在 WAN 状态查看 WAN 的使用.

图 8-3: 外部网络状态

数据 – WAN 状态

NAT 统计	这个部分显示数据为各个 WAN Port. • **状态** – 显示联机或是断线. • **默认的负载分配** – 各个 WAN Port 默认的流量负载. • **当前的负载分配** –各个 WAN Port 当前的流量负载. • **当前的负载** – 当前的联机数,字节,封包在各个 WAN Port. • **当前的带宽** – 显示每一个 WAN 的上传及下载带宽. • **刷新** – 更新所有的讯息. • **重置记录** – 重新统计数据. • **检查 NAT 列表** – 显示 NAT 的状态.
接口统计	这个部分显示渐增统计。

Appendix A
Specifications

Model	2 WAN Load Balancer
Dimensions	245mm (W) x 137mm (D) x 30mm (H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	6 Ethernet: 4 * 10/100BaseT (RJ45) auto-Switching Hub ports for LAN devices 2 * 10/100BaseT (RJ45) for WAN
LEDs	8 LAN 4 WAN 1 Status 1 Power
External Power Adapter	5 V 1.5A DC

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

CE Marking Warning

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.