# VigorPro 200B
# 双 WAN 口网吧专用型路由器
# 用户手册

*目录*

# 1 介绍

VigorPro200B 是新一代基于 Intel 计算技术的网络路由器设备。针对商务和网吧网络的更高阶网络应用需求，VigorPro200B 配备了 Intel **IXP** 第二代网络处理器，同时辅以 DrayTek 成熟的 DrayOS™ 作为产品内核，提供了强大的防火墙和更高的网络吞吐性能。VigorPro200B 可以支持高达 **50000** 条的并发 NAT 会话，同时支持 **100Mbps 的网络线速转发**。

由于配备了双 WAN 口，VigorPro200B 可以提供**负载均衡**，按需带宽使用以及线路备援等功能。基于规则设定的 QoS 控制，**网页内容过滤以及便利的 IM/P2P 软件屏蔽**进一步提升了网络效率。此外，针对大陆网络情况，特别推出了**“电信网通路由自动选择”**的功能，让同时使用电信、网通线路的用户轻松实现网络速度的最优化。

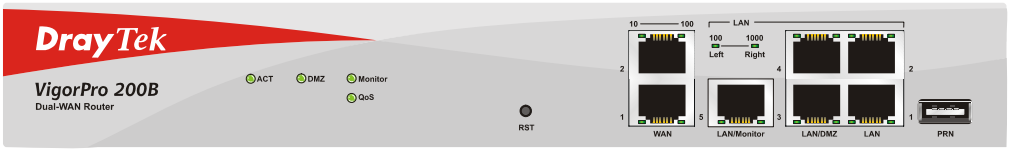
针对迅雷等软件带来的带宽滥用等问题，Pro200B 推出了带宽管理功能，通过**限制带宽，限制会话**等方式，对网络应用加以限制，从而保障了大多数用户的正常网络应用畅通。

业内绝无仅有的千兆以太网交换机配备，可以轻松实现局域网内的千兆交换，为网内视频点播服务留出足够的拓展空间。

该路由器支持 Web，telnet 以及 SNMP 等各种管理方式，方便客户的管理配置需求。快速开始向导可以让用户在很短的时间内就启用路由器。另外，Syslog 可以帮助客户方便的进行故障诊断。

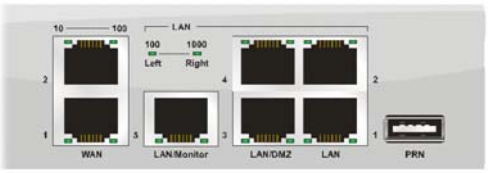
## 1.1 LED 指示灯和接口

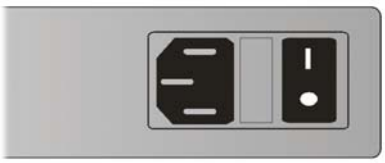
### 1.1.1 VigorPro200B LED 说明




| LED | | 状态 | 说明 |
|---|---|---|---|
| ACT (活动) | | 闪动 | 路由器已开机并正常运行 |
| | | 亮 | 路由器已开机 |
| DMZ | | 亮 | DMZ 主机已经指定 |
| Monitor | | 亮 | LAN 流量检测已激活 |
| QoS | | 亮 | QoS 功能已经启用 |
| *接口 LED* | | | |
| WAN | 10<br>(左 LED) | 亮 | 端口以 10M 速度连接 |
| | | 灭 | 端口未连接 |
| | | 闪动 | 数据正在传输 |
| | 100<br>(右 LED) | 亮 | 端口以 100M 速度连接 |
| | | 灭 | 端口未连接 |
| | | 闪动 | 数据正在传输 |
| LAN/Monitor<br>LAN/DMZ<br>LAN | 100<br>(左 LED) | 亮 | 端口以 100M 速度连接 |
| | | 灭 | 端口未连接 |
| | | 闪动 | 数据正在传输 |
| | 1000<br>(右 LED) | 亮 | 端口以 1000M 速度连接 |
| | | 灭 | 端口未连接 |
| | | 闪动 | 数据正在传输 |

### 1.1.2 VigorPro200B 接口说明



| 接口 | 说明 |
|---|---|
| Factory Reset | 恢复默认设定<br>使用方法：开启路由器（ACT LED 闪动）。用圆珠笔按下这个小孔里的按钮，保持 5 秒左右的按下状态。当发现 ACT LED 快速闪动的时候，松开按钮。路由器随后将重启并恢复出厂设置。 |
| WAN | 连接接到 Internet 的接口 |
| LAN/Monitor | 连接到本地网络的接口 |
| LAN /DMZ | 连接到本地网络/DMZ 的接口 |
| LAN | 连接到本地网络的接口 |
| PRN | USB 打印机接口 |

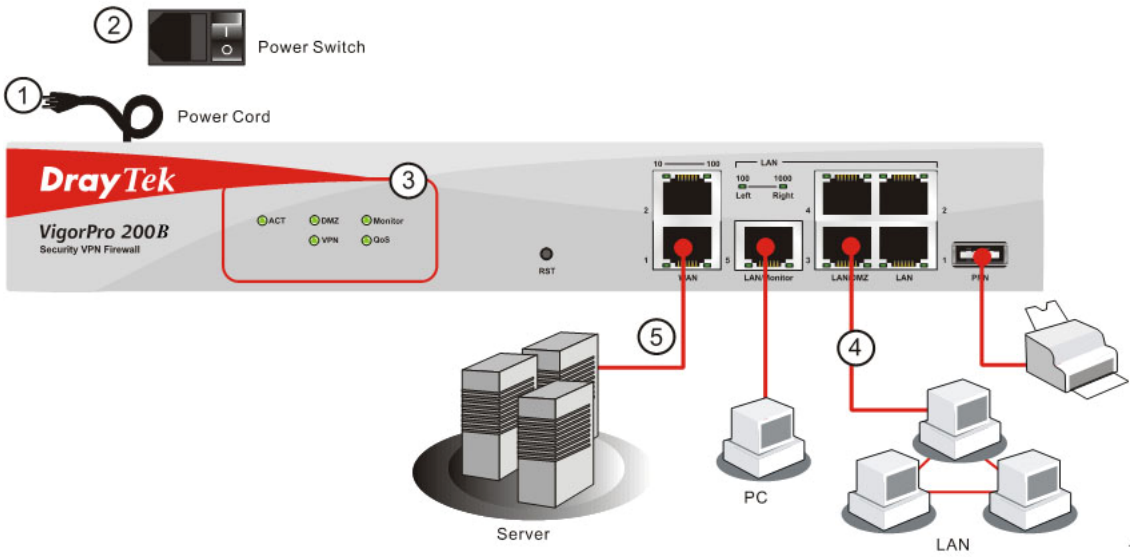
| | |
|---|---|
| ON/OFF | 电源开关 |
| PWR | 电源线接口 |

## 1.2 硬件安装

开始设置路由器之前，要确保设备连接无误。

1. 将电源线连接到路由器背后的插孔。
2. 按下电源开关开启路由器
3. 系统开始启动，当完成自检后，**ACT** LED 将会开始闪动。
4. 用网线连接 PC 到路由器的 LAN 网口，**LAN** LED 相应的 100M/1000M 将变亮。
5. 将任一 WAN 口联入 ISP 提供的线路（modem/路由器/服务器等）。WAN 口相应的速度指示灯会变亮。

（关于 LED 状态的详细信息，请参照 1.1）



# 2 配置基本设定

要使路由器安全并有效地工作，首先要进行密码的修改和一些基本的设置。

本章介绍如何修改管理员密码以及如何修改基本设置以联入 Internet。请注意，只有管理员才能够修改路由器设定。

## 2.1 修改密码

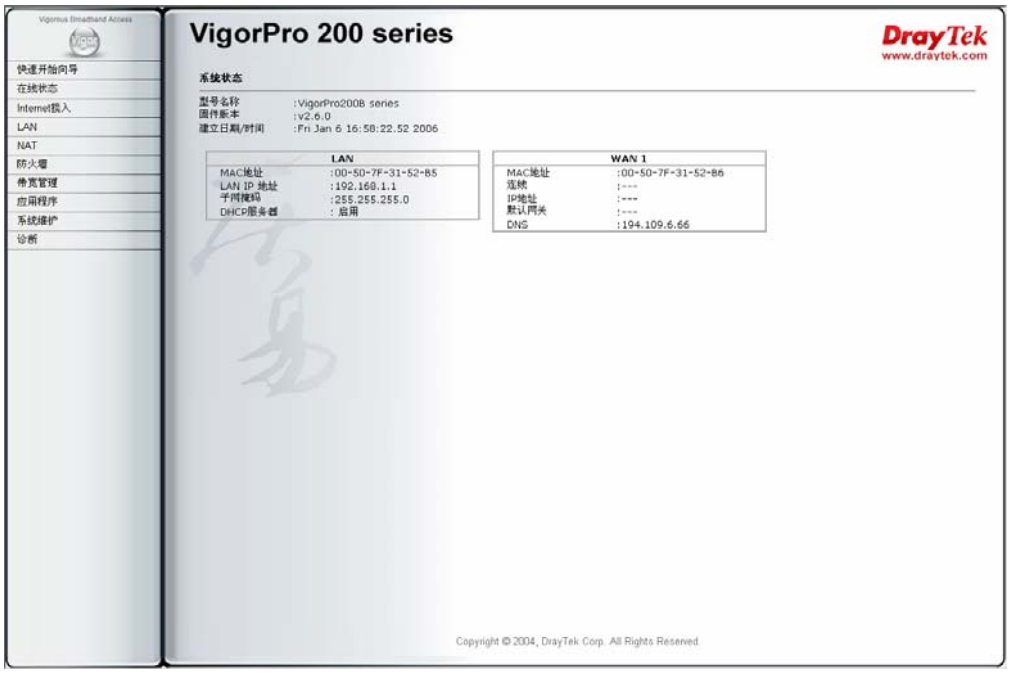
要修改设备密码，首先要以默认密码登录到路由器管理界面。

1. 确保电脑已经正确连接到路由器。

> 注意：可以让计算机自动获取 IP 地址，也可以手动指定电脑的 IP 到路由器 IP 地址 192.168.1.1 的相同网段的其它地址。

2. 打开浏览器，输入http://192.168.1.1到地址栏并回车。会有一个弹出窗口询问用户名和密码，直接点**确定**即可进入路由器设定界面（路由器默认无用户名、密码）


3. 浏览器显示**路由器配置主页面**。



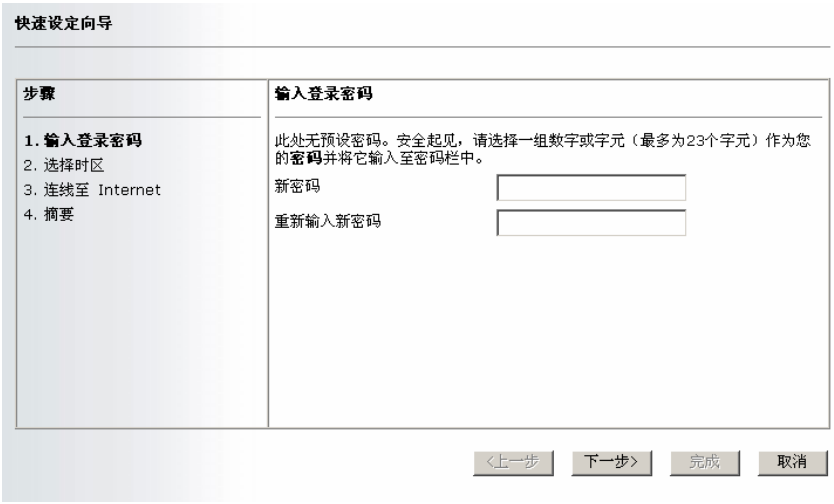

4. 点**系统维护**并选择**系统管理员密码。**


5. 输入新密码并重复输入确认，最后点**确定。**

6. 此时，密码已经完成变更。会再次显示如下窗口，要求输入新密码重新登录到路由器管理界面。

## 2.2 快速开始向导

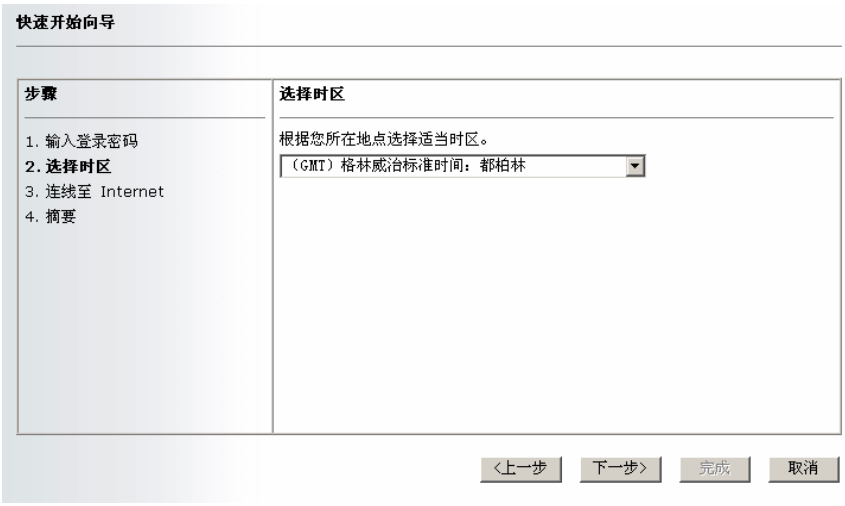
使用快速开始向导可以用最快捷的方式完成路由器部署，快速开始向导的第一个页面就是修改登录密码，输入密码，然后点击**下一步。**



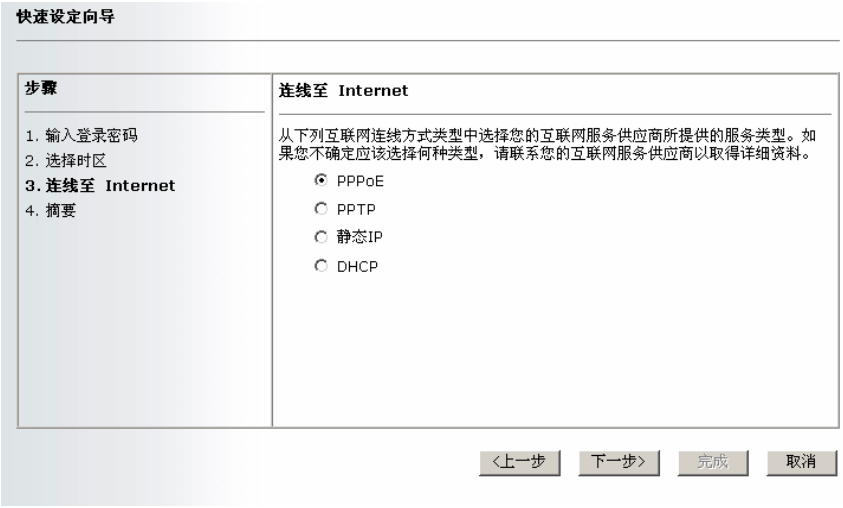

**新密码** 输入一个合法的新密码。

**重新输入新密码** 重复输入一次新密码。

点击**下一步**，将要求选择所在的时区。选择正确的时区即可。

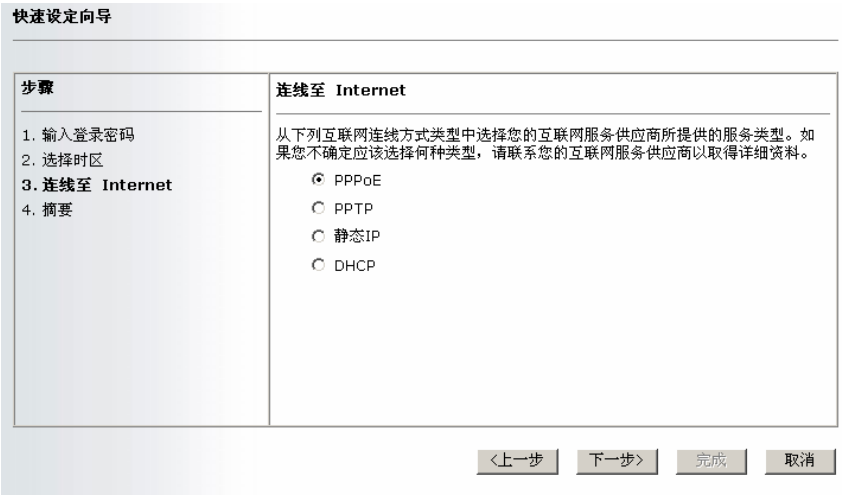



点击**下一步**继续。将进入路由器的协议设定。




## 2.2.1 选择协议

在**快速开始向导**中，可以选择 PPPoE，PPTP，**静态** IP 或 DHCP 作为网络连接的协议。

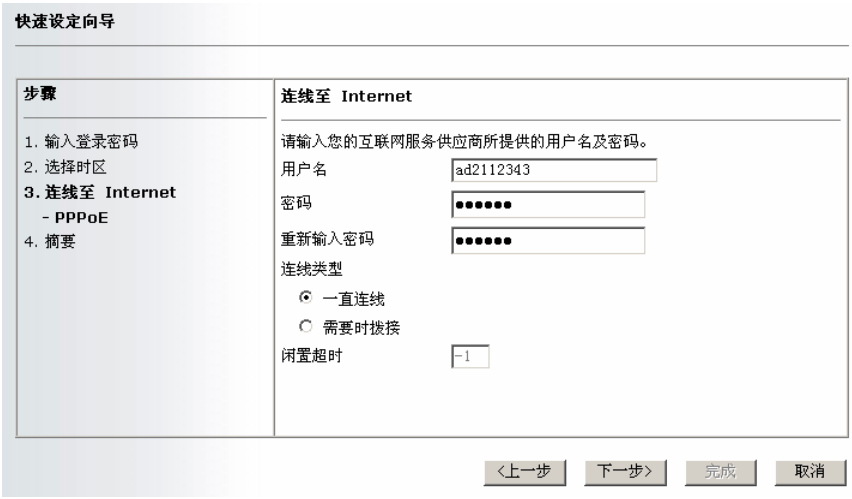



根据自己使用的线路类型，选择相应的协议，然后点击**下一步**继续。

## 2.2.2 PPPoE

PPPoE 代表 Point-to-Point Protocol over Ethernet（**基于以太网的点对点协议**）。 这种连线方式一般是 ADSL 用户的联网方式。所有的本地用户可以通过共享一条 PPPoE 线路来上网。ISP 将提供用户名，密码以及认证方式等必要的拨入信息。

如果 ISP 提供 **PPPoE** 的连接方式，在此页面请选择 **PPPoE** 并继续。将显示如下页面：




**用户名** 输入 ISP 提供的用户名。

**密码** 输入 ISP 提供的密码。

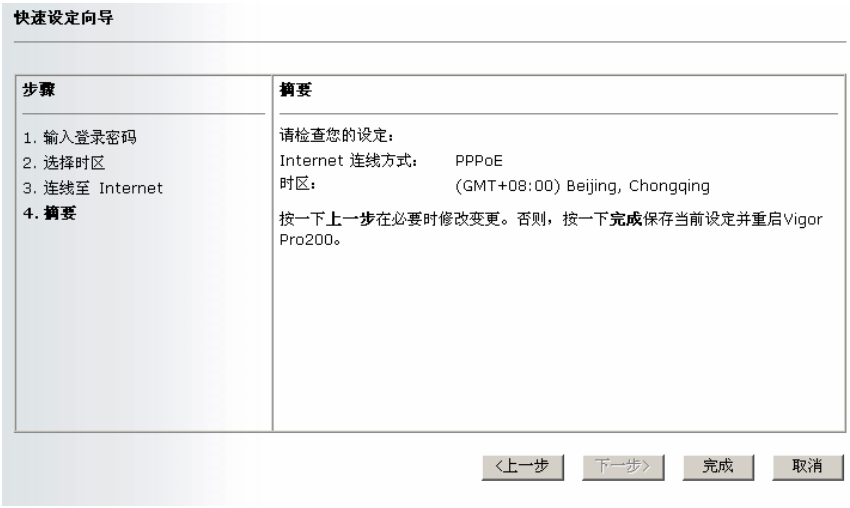
**重新输入密码** 重新输入密码。

**一直在线** 选中表示路由器一直连接到 Internet。

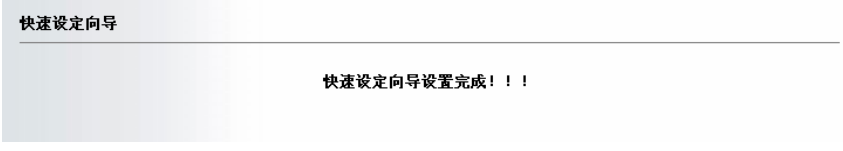
**需要时拨接** 选中表示当有网络访问请求时才会拨号。

**闲置超时** 单位为秒的数值，当网络无流量达指定时间后，断开网络连接。

点**下一步**查看该连接的总结信息。

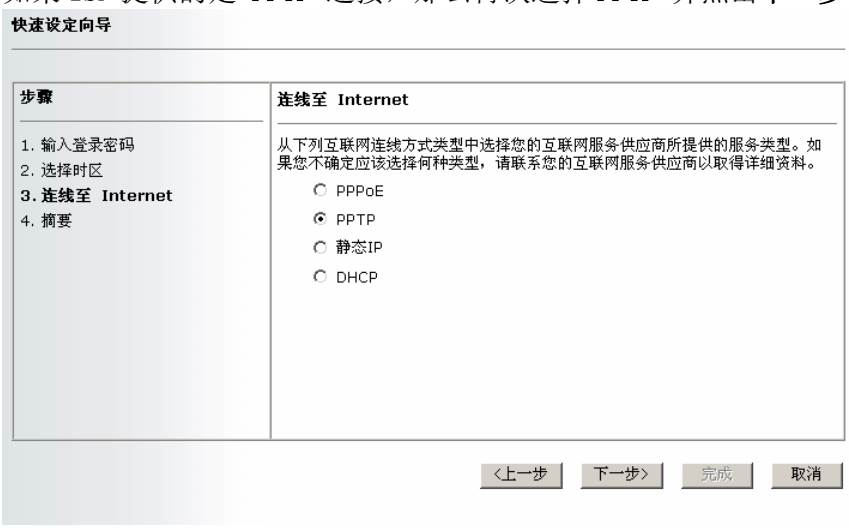



点击**完成**。完成设定的页面将会显示如下。

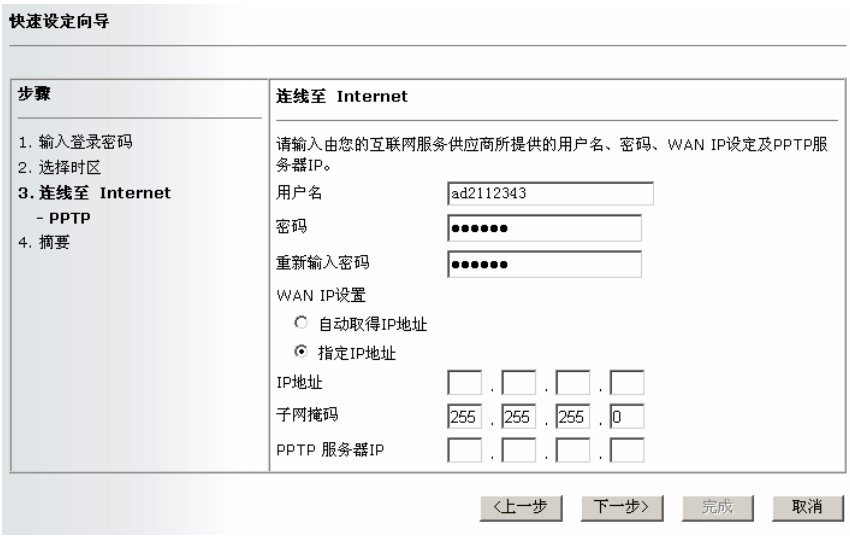


## 2.2.3 PPTP

如果 ISP 提供的是 **PPTP** 连接，那么再次选择 **PPTP** 并点击**下一步**。




会显示下列页面。输入 ISP 提供的全部相关信息到该页面。



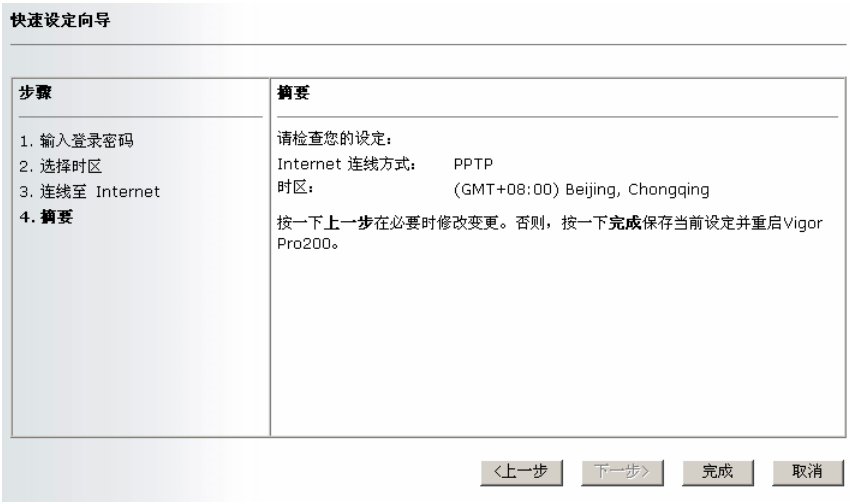

**密码** 输入 ISP 提供的密码。

**重新输入密码** 重新输入密码。

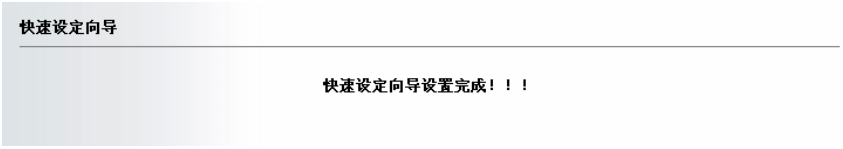
**自动取得 IP 地址** 选中表示自动从 ISP 获得 IP 地址，无需自行输入 IP 地址。

**指定 IP 地址** 输入从 ISP 得到的以下信息
**IP 地址** - 输入 IP 地址
**子网掩码** - 输入子网掩码。
**PPTP 服务器 IP** - 输入 PPTP 服务器 IP 地址

完成此页设定并点击**下一步**，可以看到如下页面。

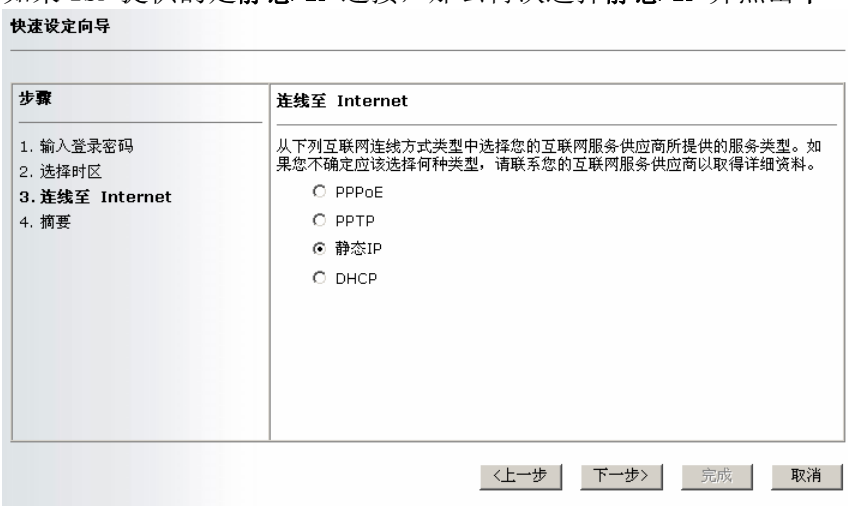



点击**完成**。完成设定的页面将会显示如下。

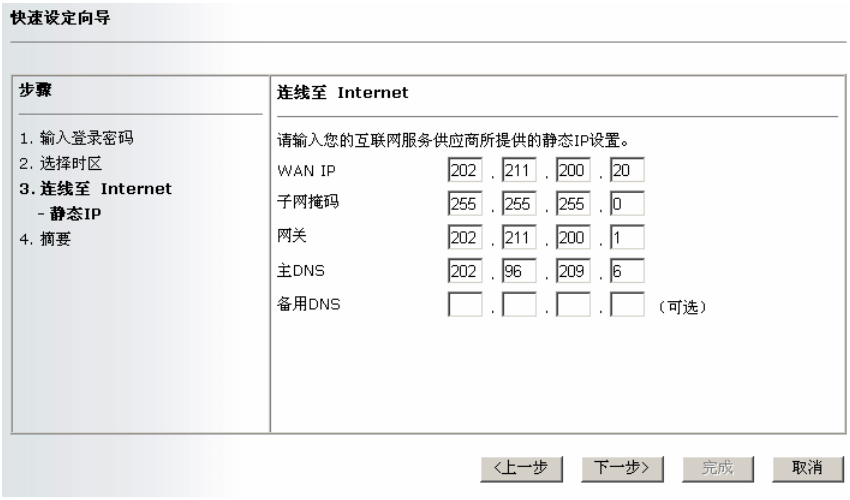


## 2.2.4 静态 IP

如果 ISP 提供的是**静态 IP** 连接，那么再次选择**静态 IP** 并点击**下一步**。




会显示下列页面。

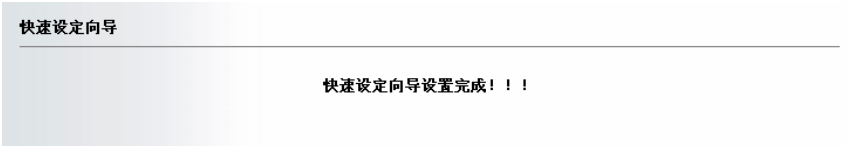



输入 ISP 提供的全部相关信息到该页面。

| | |
|---|---|
| **WAN IP** | 输入 WAN IP。 |
| **子网掩码** | 输入子网掩码。 |
| **网关** | 输入网关 IP 地址。 |
| **主 DNS** | 输入主 DNS 地址。 |
| **备用 DNS** | 输入备用 DNS IP 地址（可选）。 |

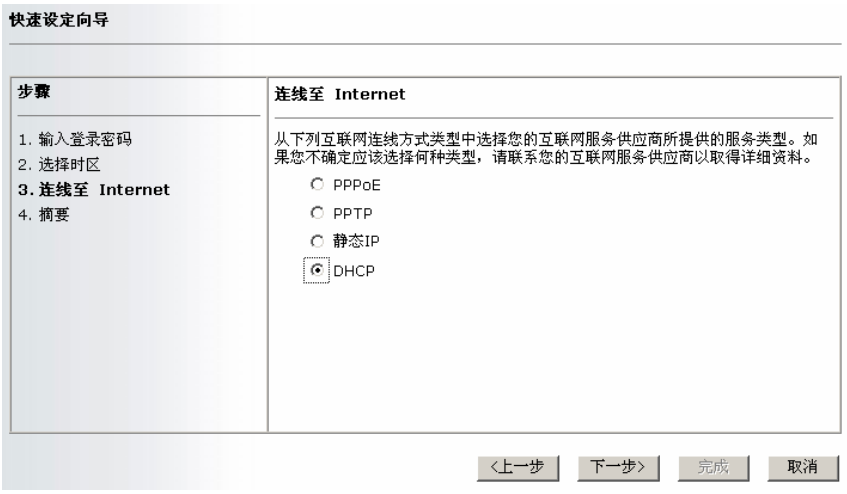
完成此页设定并点击**下一步**，可以看到如下页面。


点击**完成**。完成设定的页面将会显示如下。




## 2.2.5 DHCP

如果 ISP 提供的是 DHCP 连接，那么再次选择 DHCP 并点击**下一步**。



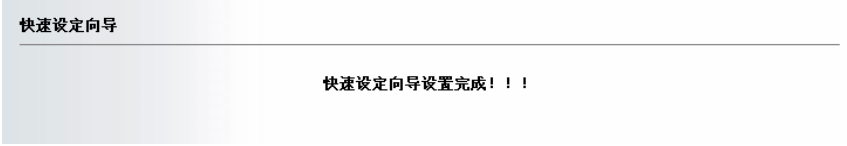

填入必要的信息到以下页面。


**主机名称** 输入主机名，该选项有部分 ISP 要求填写，没有特殊要求的话，可以保留为空。

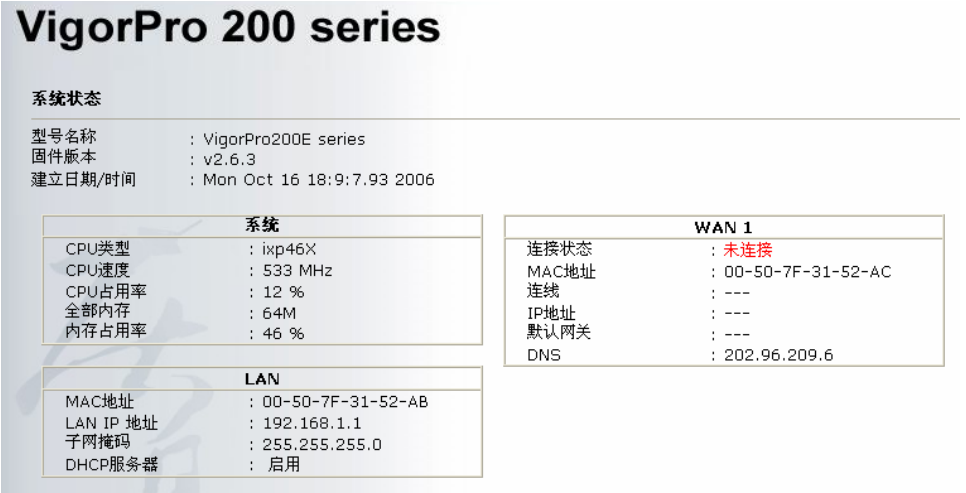
**MAC** 默认显示的 MAC 地址是路由器的出厂 MAC 地址，如果点击**复制 MAC 地址**按钮，则可以将当前使用的 PC 的 MAC 地址复制到地址框中，对于某些锁定 MAC 地址的应用，请使用该按钮。

完成此页设定并点击**下一步**，可以看到如下页面。


点击**完成**。完成设定的页面将会显示如下。



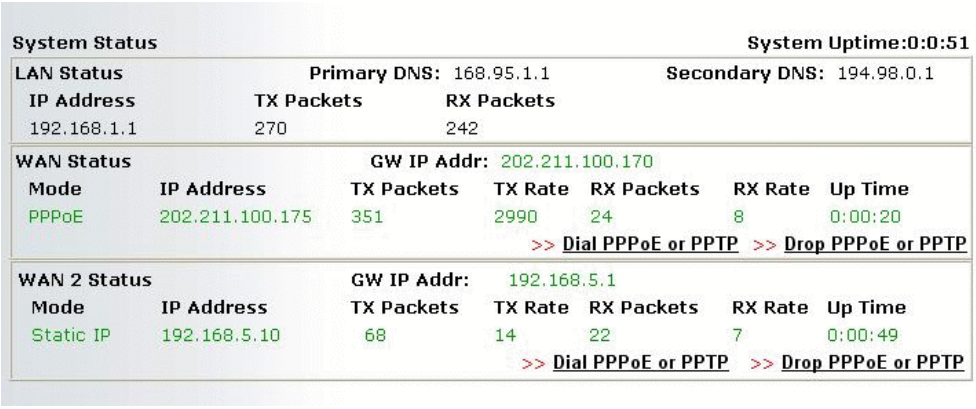

系统状态页面将会显示，如下图。



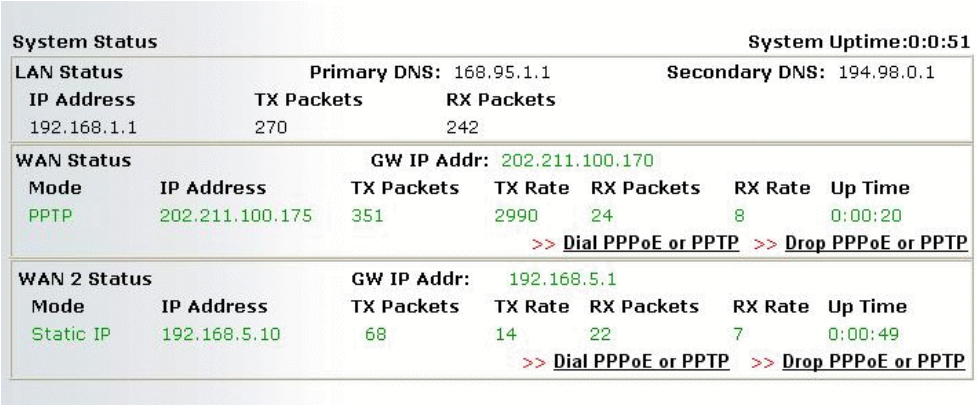

## 2.3 在线状态

在线状态页面显示系统状态，WAN 状态，ADSL 信息以及其它路由器相关信息。如果选择 PPPoE 或者 PPTP 作为 WAN 连接协议，那么页面会显示**拨** PPPoE **或** PPTP 以及**断开** PPPoE **或** PPTP 的按钮。

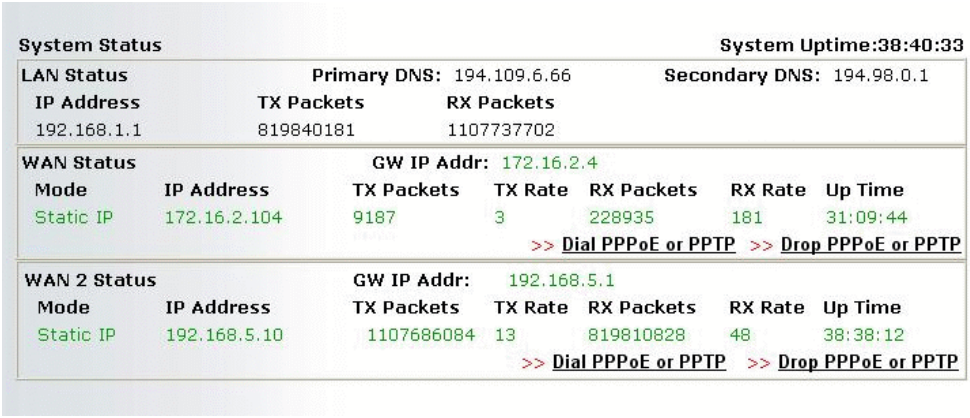
*PPPoE 系统状态 (WAN 1)*




*PPTP 系统状态 (WAN 1)*



*固定 IP 系统状态 (WAN 1)*




*LAN 状态部分:*

**主 DNS** 显示主 DNS 地址

**备用 DNS** 显示备用 DNS 地址

**IP 地址** 显示 LAN 的 IP 地址

**上行封包** 显示 LAN 接口发出的封包数

**下行封包** 显示 LAN 接口接收的封包数

*WAN 状态和 WAN2 状态部分*

**网关 IP 地址:** 显示默认网关的 IP 地址

**IP 地址** 显示 WAN 接口的 IP 地址

**上行速率** 显示 WAN 接口发出封包的速度。

**下行速率** 显示 WAN 接口接收封包的速度。

**在线时间** 显示系统连线总时间

## 2.4 保存设定

每次当点击**确定**保存设定后，web 页下方将显示下列信息，表示系统已经接受了设定的更改。


**已就绪** 表示系统已经可以接受输入

**设定已保存** 表示设定已经保存

# 3 高级 WEB 设定

当完成路由器的基本设定之后，连接好路由器，路由器就可以访问 Internet 了。如果需要做更多的设定，可以参照本章。第四章将介绍一些应用的举例。

## 3.1 Internet 接入

### 3.1.1 IP 网络基础

IP 代表 Internet 协议。IP 网络里面的所有设备，包括路由器，打印服务器以及主机，都需要 IP 地址来标记它在网络中的位置。为了避免地址冲突，IP 地址公开注册到网络信息中心（NIC）。互联网上每台设备的 IP 地址必须是唯一的，不过对于路由器维护的内部网络而言，可以使用一些保留的永远不被注册到 NIC 的地址，这些地址被称为私网地址，列表如下：

从 10.0.0.0 到 10.255.255.255
从 172.16.0.0 到 172.31.255.255
从 192.168.0.0 到 192.168.255.255

#### 什么是公网地址和私网地址

路由器管理着内部局域网络，所有的内部 PC 都有一个**私网 IP 地址**，路由器使用私网 IP 192.168.1.1 与局域网络交换数据。同时，路由器还通过 WAN 接口的**公网 IP** 和 Internet 上的其它设备进行数据交换，当数据通过时，路由器进行网络地址转换（NAT），实现私网地址和公网地址之间的数据交换，所有的数据都会发到正确的 PC 上去。因此，所有的主机都可以共享一个 Internet 连接。

#### 从 ISP 获取公网 IP 地址

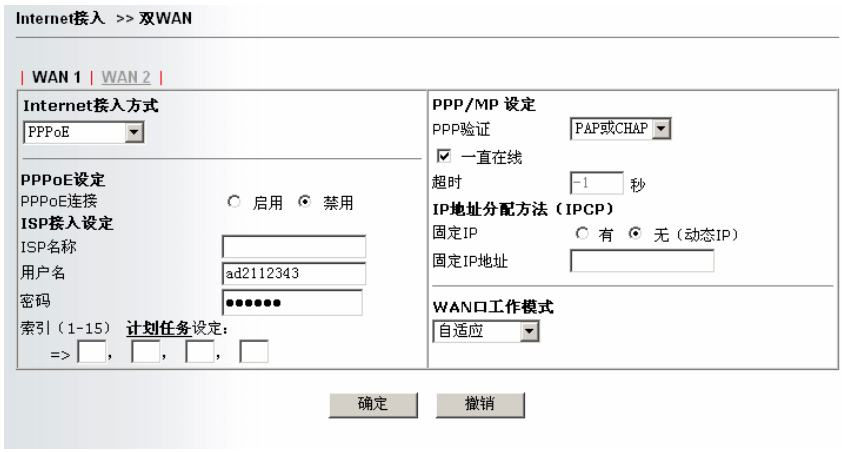
路由器通过以下几种协议从 ISP 获取公网 IP 地址：
**Point to Point Protocol over Ethernet (PPPoE)，PPTP，静态 IP 以及 DHCP (动态 IP)**。

在使用 ADSL 时，通常使用 PPPoE 进行网络连接，身份认证，计费等。当路由器连接到 ISP 时，会通过 **PAP，CHAP** 等进行身份认证，ISP 会将 IP 地址，DNS 服务器地址等相关信息返回给路由器。

### 3.1.2 PPPoE

要选择 PPPoE 作为接入协议，首先打开 **Internet 接入**中的**双 WAN** 设置页面，选择 PPPoE 作为接入方式。


将显示如下页面




**PPPoE 设定**

选中 **PPPoE 设定**的**启用**。如果选择**禁用**，那么该页所有的设定将不生效。

**ISP 接入设定**

输入 ISP 提供的用户名，密码以及验证方式。
**ISP 名称** - 输入 ISP 提供的名称（部分 ISP 需要）
**用户名** - 输入 ISP 提供的用户名信息
**密码** - 输入 ISP 提供的密码信息

**索引（1-15）计划任务设定**

可以键入四个计划任务项。所有的计划任务可以在**应用程序－计划任务**页面进行定义。在这里就填入计划任务的相应编号就可以了

**PPP/MP 设定**

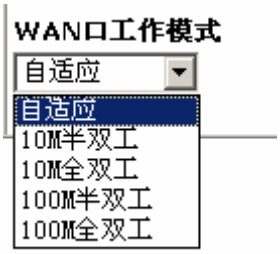
**PPP 验证** - 选择**仅 PAP** 或 **PAP 或 CHAP**
如果要一直连接到 Internet，请选中**一直在线**
**一直在线** - 选择此复选框保持网络一直连线。
**超时** - 超时值代表当无数据流量达此秒数，就断开 Internet 连接。

**IP 地址分配方法**

通常 ISP 在每次接入时动态分配 IP 地址。也有些 ISP 会提供静态 IP 地址，这种情况下，可以将指定的 IP 填写到固定 IP 栏。
**固定 IP** - 选中**有**并将 IP 地址输入文本框。

**WAN 口工作模式**

该项决定了不同网络设备之间协同工作的速度。如果当连接出现问题时，可以在这里手动选择正确的连接类型。默认设定是**自适应。**

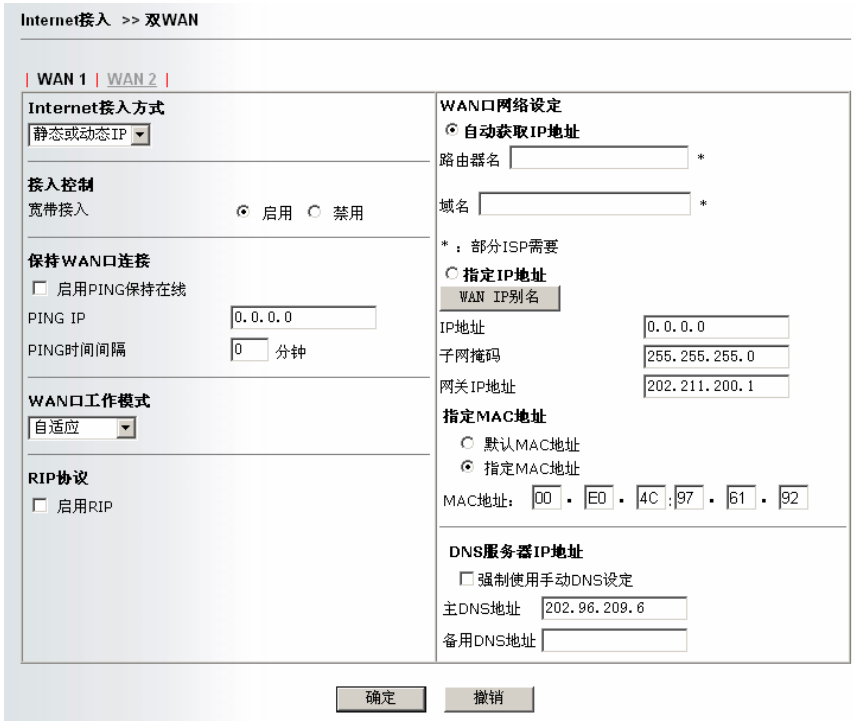



完成设定之后，点击**确定**激活设置。

### 3.1.3 静态 IP 或 DHCP（动态 IP）

选择**静态 IP 或 DHCP** 作为 Internet 接入协议，首先打开**双 WAN** 页面，然后在 **Internet 接入方式**下拉菜单中选择**静态或动态 IP**。


将显示如下页面。




**接入控制** 选择**启用**则启用该模式作为 **Internet 接入方式**。如果选择**禁用**，则所有该页的修改均为无效。

**保持 WAN 口连接** 选中**启用 PING 保持在线**则激活此功能。

PING IP － 指定任意已接入网络的公网 IP 地址。路由器每隔指定的时间间隔就会 ping 该 IP 地址，保持 WAN 口一直在线。

**PING 时间间隔** - 决定路由器 ping 的时间间隔。

**WAN 口工作模式**

决定 WAN 接口的工作速度，默认为**自适应**，如果默认情况下速度不正常，则可以尝试手动选择。


**RIP 协议**

RIP 是路由信息协议的缩写，路由器通过该协议交换路由表信息。选中**启用 RIP** 激活此功能。

**WAN 口网络设定**

该组设定是关于联网 IP 动态获取或手动指定的设置。

**自动获取 IP 地址** - 选中则自动从 ISP 获取 IP 地址。
**路由器名** - 输入 ISP 提供的路由器名称。
**域名** - 输入分配的域名。
**指定 IP 地址** - 选中则手动设置 IP 地址。
**WAN IP 别名** - 如果有多个公网地址，可以设定到 IP 别名中，最多可以设置 8 个公网 IP 在别名中。如果选中**加入 NAT IP 池**，则别名 IP 也会作为上行封包的 NAT 公网地址使用，这样的选择过程为随机选择。如果玩游戏，登录论坛出现掉线情况，请不要勾选该选项。


**IP 地址** - 输入 IP 地址。
**子网掩码** - 输入子网掩码。
**网关 IP 地址** - 输入网关 IP 地址。

**指定 MAC 地址**

输入路由器的 MAC 地址。可以使用**默认 MAC 地址**或者可以自己输入 MAC 地址。

**指定 MAC 地址** – 选中则可以指定一个新的 MAC 地址。
**MAC 地址** – 手动输入路由器的 MAC 地址

**DNS 服务器 IP 地址**

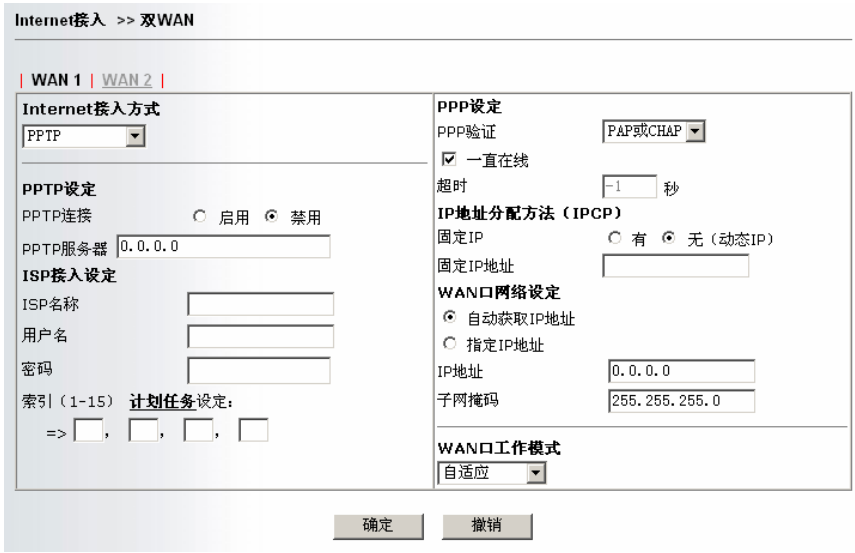
**强制使用手动 DNS 设定** – 选中此处可以强制使用自己输入的 DNS 地址。对于 ADSL 用户来说，会从 ISP 处拨号获取 DNS 地址，如果使用了强制 DNS 设定，则从 ISP 处获取的 DNS 将被忽略。
**主 DNS 地址** – 在此处输入 ISP 给出的 DNS 地址，如果不输入，则使用默认的 194.109.6.66 作为 DNS 地址
**备用 DNS 地址** –在此处输入 ISP 给出的第二 DNS 地址，如果不输入，则使用默认的 194.98.0.1 作为 DNS 地址。

完成所有设定后，点击**确定**保存设定。

## 3.1.4 PPTP

选择 PPTP 作为 Internet 接入协议，首先打开**双 WAN** 页面，然后在 **Internet 接入方式**下拉菜单中选择 **PPTP**。


将显示如下页面




**PPTP 设定**

**PPTP 连接** – 选中**启用**激活 PPTP 作为 **Internet 接入方式**。如果选中**禁用**，此功能将关闭，该页的设置均为无效。
**PPTP Server** – 输入 ISP 给出的 PPTP 服务器地址。

**ISP 接入设定**

输入 ISP 提供的用户名，密码以及验证方式。
**ISP 名称** – 输入 ISP 提供的名称（部分 ISP 需要）
**用户名** – 输入 ISP 提供的用户名信息
**密码** – 输入 ISP 提供的密码信息

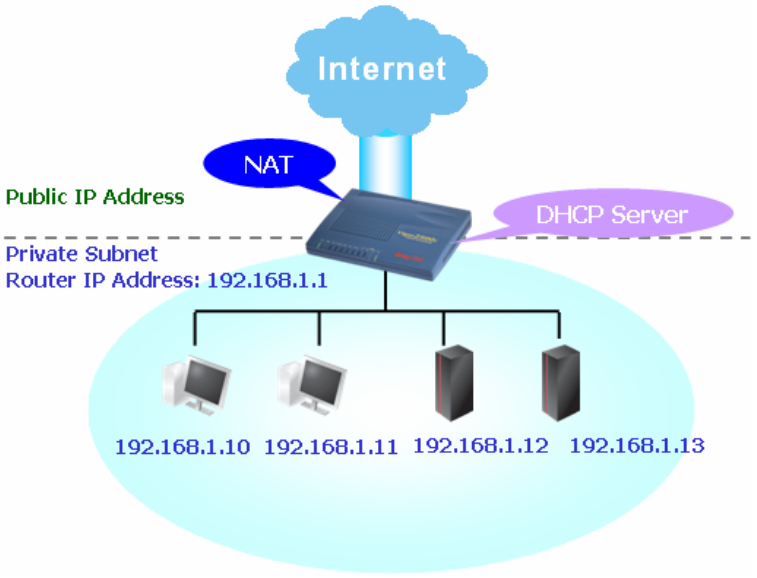
| | |
|---|---|
| **索引（1-15）计划任务设定** | 可以键入四个计划任务项。所有的计划任务可以在**应用程序－计划任务**页面进行定义。在这里就填入计划任务的相应编号就可以了 |
| **PPP 设定** | **PPP 验证** - 选择**仅 PAP** 或 **PAP 或 CHAP**<br>如果要一直连接到 Internet，请选中**一直在线**<br>**一直在线** - 选择此复选框保持网络一直连线。<br>**超时** - 超时值表示当无数据流量达此秒数，就断开 Internet 连接。 |
| **IP 地址分配方法** | 通常 ISP 在每次接入时动态分配 IP 地址。也有些 ISP 会提供静态 IP 地址，这种情况下，可以将指定的 IP 填写到固定 IP 栏。<br>**固定 IP** - 选中**有**并将 IP 地址输入文本框。 |
| **WAN 口网络设定** | 该组设定是关于联网 IP 动态获取或手动指定的设置。<br>**自动获取 IP 地址** - 选中则自动从 ISP 获取 IP 地址。<br>**指定 IP 地址** - 选中则手动设置 IP 地址。<br>**IP 地址** - 输入 ISP 给的 IP 地址<br>**子网掩码** - 输入子网掩码。 |
| **WAN 口工作模式** | 决定 WAN 接口的工作速度，默认为**自适应**，如果默认情况下速度不正常，则可以尝试手动选择。 |


## 3.2 LAN

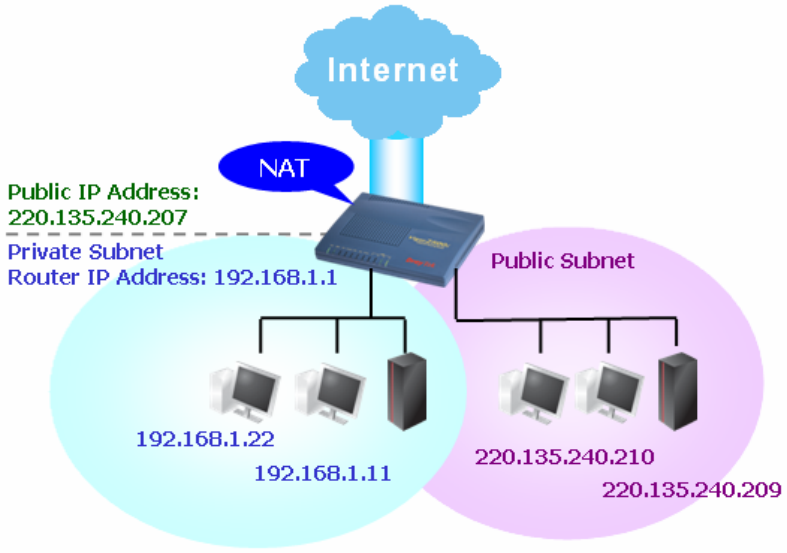
LAN 这里指的是被路由器管理的内部子网。网络结构的设计与 ISP 提供的公网 IP 有关。

### 3.2.1 局域网基础

NAT 是 Vigor 路由器的基本功能。它创建并维护一个私有内部网络。根据前述，Vigor 路由器可以使用公网 IP 和 Internet 主机交流,同时可以使用私网地址和内网主机交流。NAT 的作用是将上行封包的私网地址翻译成公网地址发出，数据下行时又进行反向的翻译,将数据发送到正确的主机,从而实现了多个私网地址的主机分享同一个公网 IP 地址。Vigor 路由器还具有内置的 DHCP 服务器给主机分配私网 IP 地址。
可参照下图进行一个简单的了解。




在某些特殊情况下，ISP 可能会多分配一个子网的公网地址，例如 220.135.240.0/24。这意味着内网可以有一个公网子网（第二子网）。作为第二子网的一部分，Vigor 路由器将为所有的内部公网主机做 IP 路由，使他们可以和 Internet 上的主机进行数据交换。因此，路由器是作为公网主机的网关而存在的。




## 什么是路由信息协议(RIP)

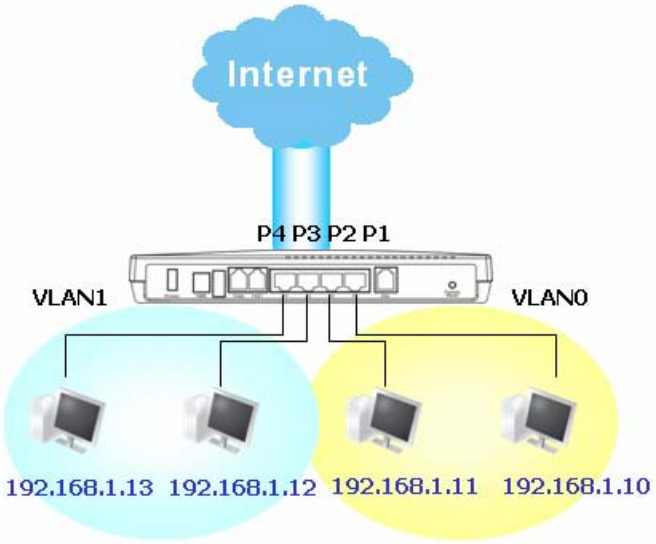
Vigor 路由器可以与临近的路由器进行路由信息的交换以实现 IP 路由。这一特性使得用户对 IP 地址等信息的改变可以自动互相通知。

## 什么是静态路由

当局域网内有多个子网时，更有效率，更快的方法是配置**静态路由**，使用静态路由器，可以在没有 RIP 的情况下，让路由器知道发到特定子网的数据应该通过哪个地址转发。

### 什么是虚拟局域网（VLAN）

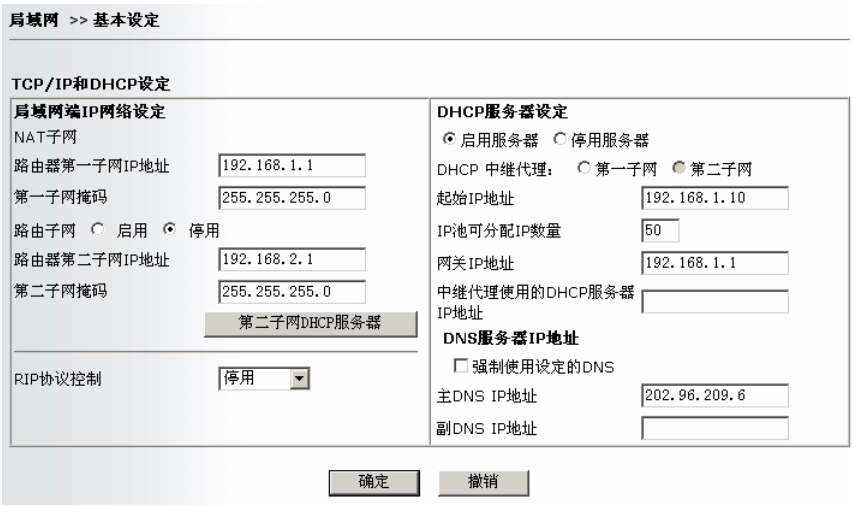
有很多 PC 的情况下，可以通过 VLAN 将路由器的四个端口分别设置成 VLAN，这样，尽管都在一个局域网中，隶属不同 VLAN 组的 PC 之间无法互相交流。这样可以降低局域网内部的广播包数量，有效避免广播风暴。




## 3.2.2 基本设定

此页提供了局域网的基本设定。

点击 LAN 打开局域网设定并选择**基本设定**。




**路由器第一子网 IP** 输入路由器的私网 IP 地址（默认为 192.168.1.1）。

**第一子网掩码** 输入子网掩码，来决定网络的大小。（默认：255.255.255.0/ 24）

**路由子网** 选择**启用**以使用此功能，默认设定是**停用**。

**第二子网 IP 地址** 输入第二子网 IP 地址，该地址作为内部公网主机的网关。（默认： 192.168.2.1/ 24）

**第二子网掩码** 输入子网掩码，来决定网络的大小。（默认： 255.255.255.0/ 24）

**第二子网 DHCP 服务器** 可以配置路由器为第二子网主机动态分配 IP 地址。


**开始 IP 地址：**输入第二子网可以 DHCP 分配的 IP 地址的起始地址。例如路由器地址为 220.135.240.1，那么开始 IP 地址就应该是 220.135.240.2 或更大值，必须小于所在子网的最大 IP 值。

**IP 池 IP 数：**输入地址池中的 IP 数，最大值为 10。该值表示第二子网 DHCP 服务器可以分配的 IP 数。

**MAC 地址：** 输入要分配公网地址的主机的 MAC 地址，然后点击**添加**，这样指定 MAC 地址的 PC 在 DHCP 获取 IP 时，就会获得正确的公网地址，而不是像通常情况那样获得第一子网的私网地址。

**RIP 协议控制**

**停用：**停用 RIP 协议。这将停止在路由器间进行路由信息的交换（默认）


**第一子网** – 选择路由器与临近路由器交换第一子网的路由信息。

**第二子网** – 选择路由器与临近路由器交换第二子网的路由信息。

**DHCP 服务器设定**

DHCP 代表动态主机配置协议。路由器默认情况下开启了 DHCP 服务器功能，为接入的 PC 自动分配 IP 等相关的网络设定。

如果想要使用其它的 DHCP 服务器，可以使用中级代理功能来转发 DHCP 信息到 DHCP 服务器。

**启用服务器** – 让路由器为每个主机分配 IP 地址

**禁用服务器** – 手动分配 IP 地址给网内主机

**中继代理** – **（第一子网/第二子网）**指定 DHCP 服务器所在的子网以便中继代理转发 DHCP 请求。

**起始 IP 地址** – 输入 IP 池可以分发的 IP 地址的第一个地址。

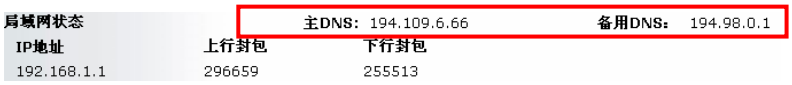
**IP 地址池 IP 数** – 输入 DHCP 服务器最多可以分配的 IP 数。
**网关 IP 地址** – 输入局域网网关地址，DHCP 服务器分配 IP 时，会将此网关 IP 分配给客户机。
**中继代理使用的 DHCP 服务器 IP 地址** – 设定需要使用的外接 DHCP 服务器的 IP 地址。

**DNS 服务器设定**

DNS 服务器域名解析服务器，用来将大家熟知的域名解析成 Internet 传输所需的 IP 地址。

**强制使用设定的 DNS** –
**主 DNS IP 地址** – 在此处设定 ISP 给的 DNS 服务器地址，如果不设定，路由器将使用默认 DNS 地址：194.109.6.66。
**副 DNS IP 地址** – 在此处填一个副 DNS 服务器地址，ISP 通常会提供不止一个 IP 地址，可以分别作为主 DNS 和副 DNS 使用。如果不填写，将使用：194.98.0.1 作为副 DNS 地址

默认 DNS 服务器 IP 地址可以在在线状态页面看到。



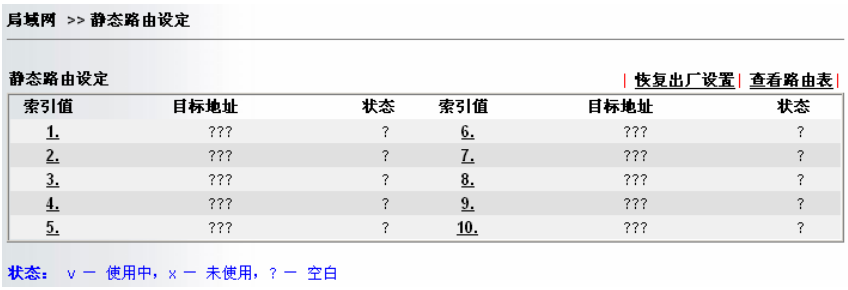

如果主 DNS 和副 DNS 都没有填，路由器将会在 DHCP 分配 IP 的时候将自己的 IP 地址作为 DNS 地址分配给主机，同时充当 DNS 代理的角色，并维护 DNS 缓存。

如果客户机发起的 DNS 请求在缓存里面已经有记录，那么路由器会立即解析，如果没有记录，则转发到到 DNS 服务器，将返回 DNS 回应发送到发起请求的客户机。

第四章会具体介绍两种常见的局域网环境设定。关于配置，可以在第四章获得详细的信息。

## 3.2.3 静态路由

在 LAN 菜单下选择**静态路由**。



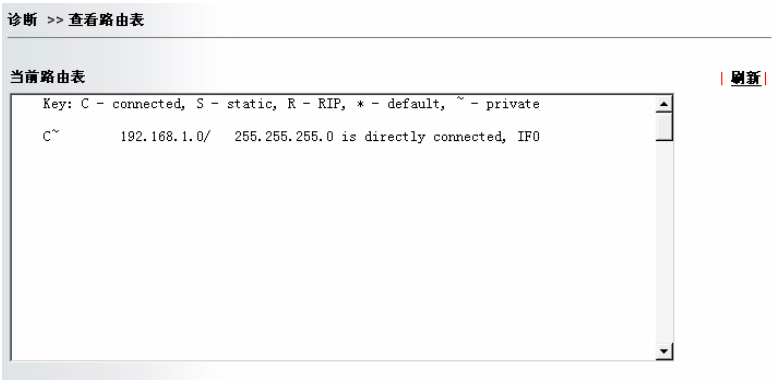

**索引值** 点击任一索引值可以进入相应的静态路由设置页面。

**目标地址** 显示静态路由的目标地址。

**状态** 显示静态路由是否启用

**恢复出厂设置** 将所有静态路由恢复到出厂设置。

**查看路由表** 显示路由表供参考

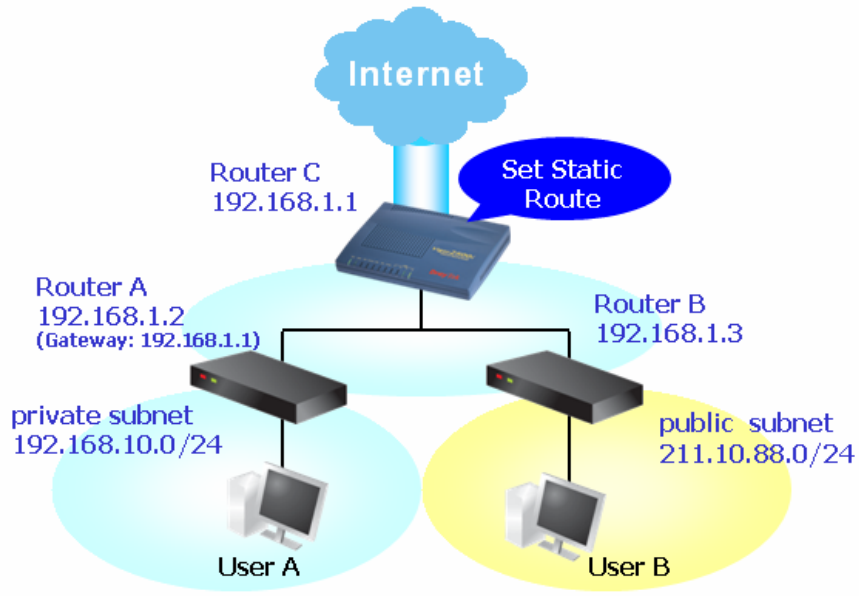



### 添加静态路由到私网或公网

下面为一个静态路由的举例，A 和 B 是不同子网中的设备，可以相互通讯。

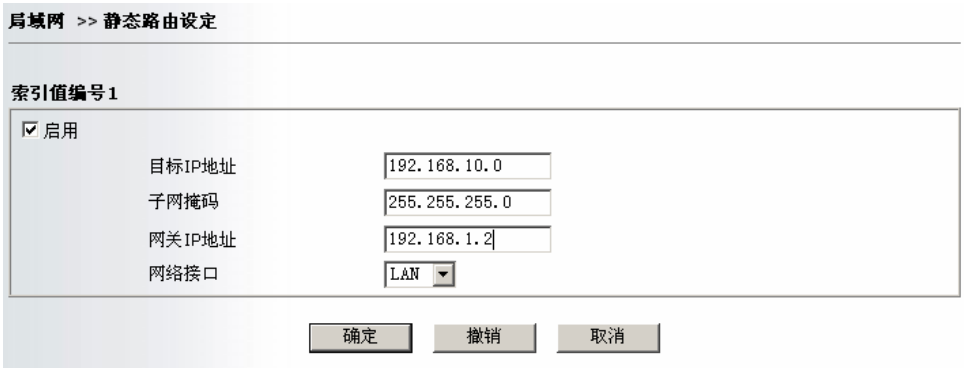
- 使用主路由器访问 Internet
- 在内部路由器 A（192.168.1.2）上创建了一个私网 192.168.10.0。
- 在内部路由器 B（192.168.1.3）上创建了一个公网 211.100.88.0。
- 路由器 A 的默认网关为主路由器德 IP 192.168.1.1。

设置静态路由前，用户 A 不能和用户 B 进行通信，因为 A 只会将数据包发到默认网关路由器 A。



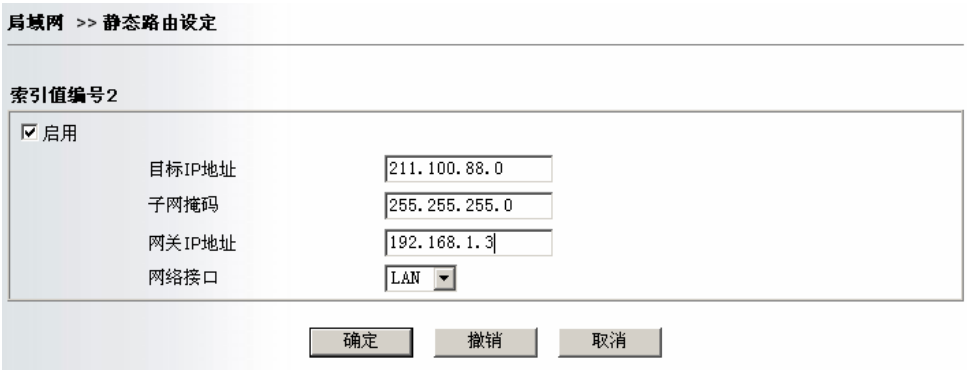

1. 在 LAN 的**基本设定**中，选择第一子网作为 RIP **协议控制**，然后点击“确定”。

2. 点击 LAN – **静态路由**然后点击**索引值** 1。添加下图所示的静态路由。该路由表示所有发到 192.168.10.0 的数据包都发向 192.168.1.2。点击**确定**。

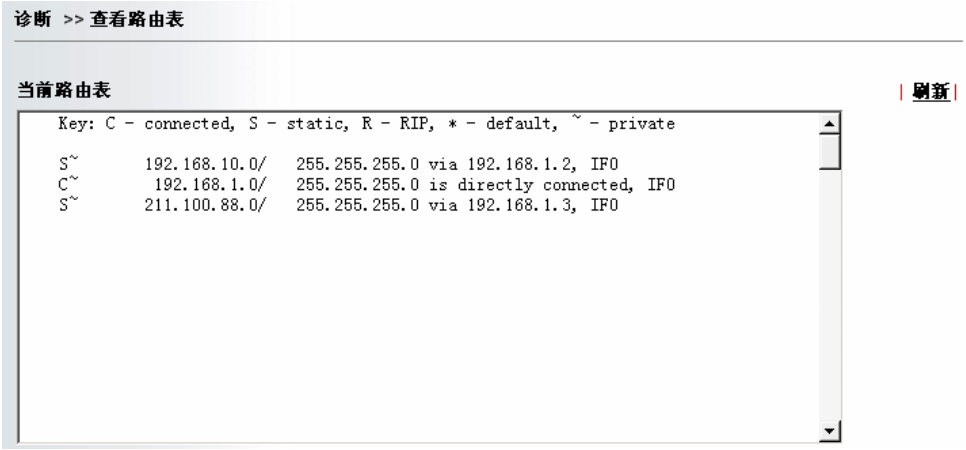



**撤销**允许撤销对当前页面的更改。

3. 返回到**静态路由设定**页面。点击另外一个索引值，添加另一条路由。该路由表示所有发到 211.100.88.0 网段的数据包都发送到 192.168.1.3。

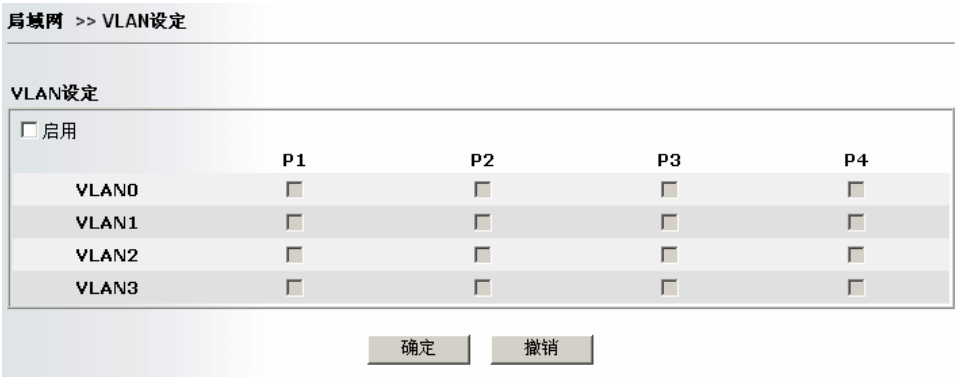



4. 访问**诊断**并选择**路由表**以查看当前路由表。



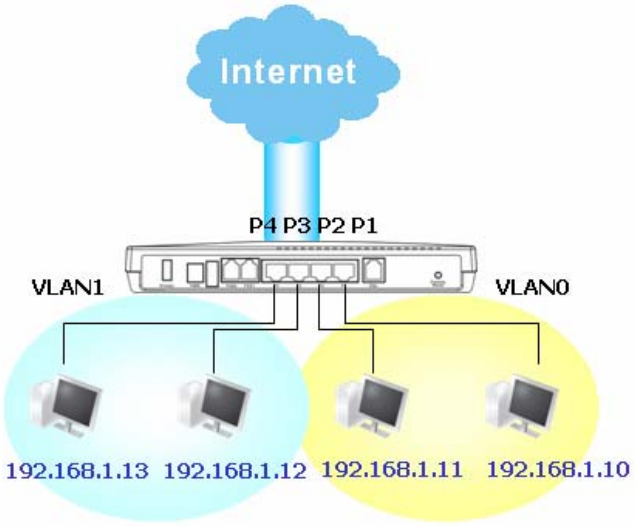

## 3.2.4 VLAN

虚拟局域网通过对物理端口分组来管理主机。在 **LAN** 菜单下点击 **VLAN**。会显示如下页面。点击**启用**则使用 VLAN 功能。

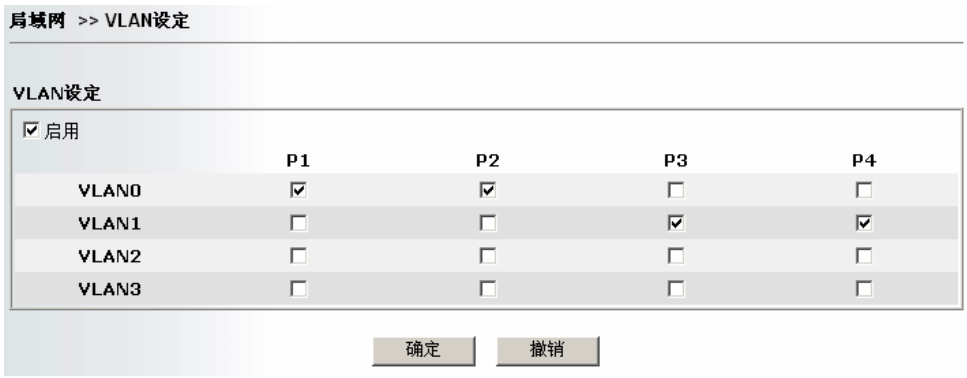



要添加或移除 VLAN，可以参考下面的例子。

1. 假设 VLAN 0 包含了连接到 P1 和 P2 的主机，VLAN1 包含连接到 P3 和 P4 的主机。




2. 启用 VLAN 功能后，可以做如下设置。




3. 要移除 VLAN，取消对相应复选框的选中，然后点**确定**保存即可。

## 3.3 NAT（网络地址转换）

通过 NAT(网络地址转换)技术，我们可以将一个或多个私网 IP 地址映像到一个公网 IP 地址。简单来说，NAT 是将一个网络中使用的 IP 地址转换为其它网络中的 IP 地址，一个代表外，一个代表内。当一个信息包从外部网络进入内部网络时，NAT 会将包中的目标地址信息转化为内网的 IP,代替其原来的值。

使用 NAT 技术一方面可以节省网络资源，防止公网 IP 地址枯竭，另一方面又可以增加内部网络的安全性，使其免遭外部网络的侵袭。在绝大多数情况下，Vigor 路由器是作为 NAT 路由器来使用的。当 NAT 后的主机访问外部网络时，从外部网络将无法看到这台主机的内网 IP 地址，通过路由器的 NAT 技术，外网只能看到由 ISP 提供的公网 IP 地址。通过这一方法，所有的内部主机都可以共享一个公网 IP 地址来同时访问 Internet。

NAT 的好处包括:

- **合理利用公网 IP 地址,节约公网 IP 的使用量**

  通过 NAT, 路由器后局域网内的多个私网 IP 地址可以共享一个公网 IP 上网.

- **通过 NAT 保护路由器后局域网的网络安全**

  目前有很多针对 IP 地址的攻击, 但是这些攻击对 NAT 后的私网 IP 不会生效.

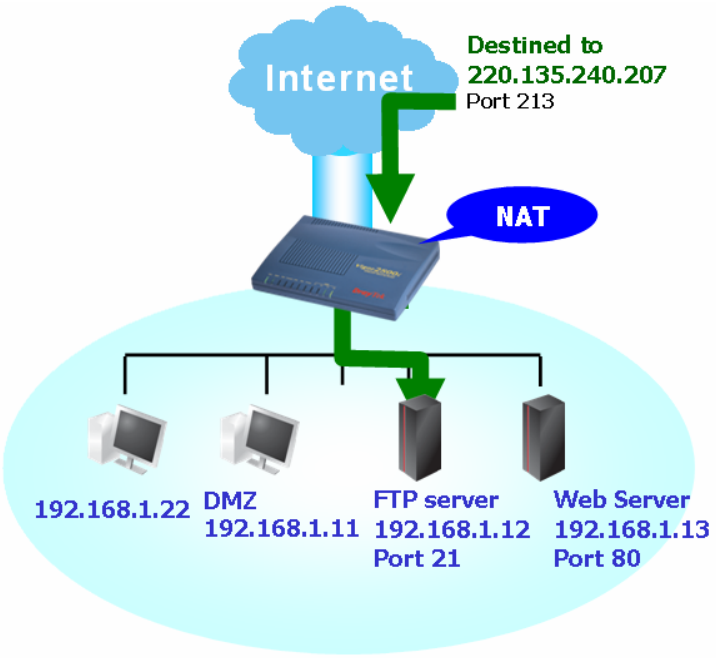
---

关于私网 IP 的定义,请参见 RFC-1918.
我们一般将 192.168.1.0/24 作为路由器后局域网的网段 IP.
NAT 功能是通过端口映射来实现的.

---

### 3.3.1 设定虚拟服务器

设定虚拟服务器功能通常用于为局域网内的服务器,如web服务器或者FTP服务器等设定端口映射.根据设定,发送到路由器外部特定端口的包会被映射到路由器内部服务器的特定端口.由于服务器位于路由器后的局域网,这样很好的保障了其网络安全.




要使用此项功能,请单击 NAT 并选择 **设定虚拟服务器**


**服务名称:** 输入该网络服务的名称。

**协议:** 选择一个传输层协议(TCP 或 UDP)。

**外部端口:** 指定端口复位向的外部端口。

**私有 IP:** 指定提供服务的内部主机的私有 IP。

**私网端口:** 指定端口复位向的私网端口。

**启用:** 启用您所定义的该项端口映射。

**撤销:** 清除所有设定

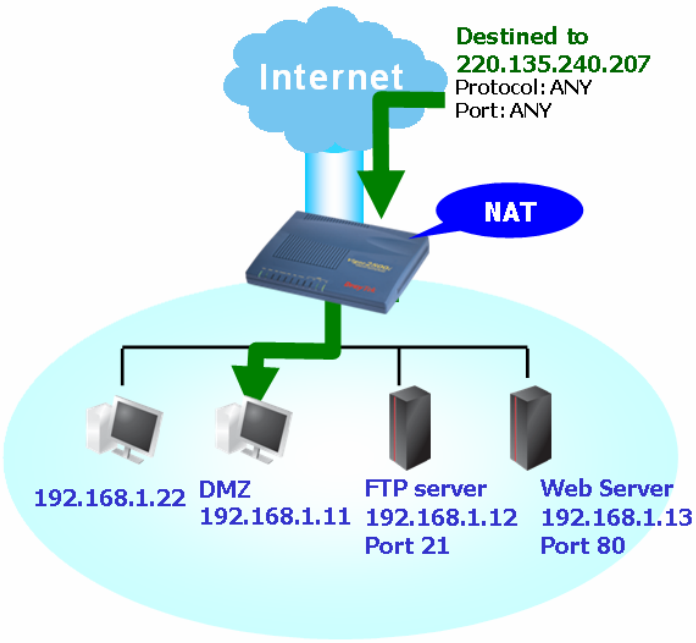
请注意,路由器有自己的内置服务(服务器),比如 Telnet, HTTP and FTP 等等. 由于这些服务使用的端口可能会和局域网内的服务器使用的端口冲突,如果遇到这种情况,必须更改内置服务的使用端口.

举例来说, 如果您要在局域网建立一台 WEB 服务器使用 TCP 80 端口,则您必须把路由器的 HTTP 通讯端口由 80 改为其它值.

具体操作请点击 **系统管理>>管理**

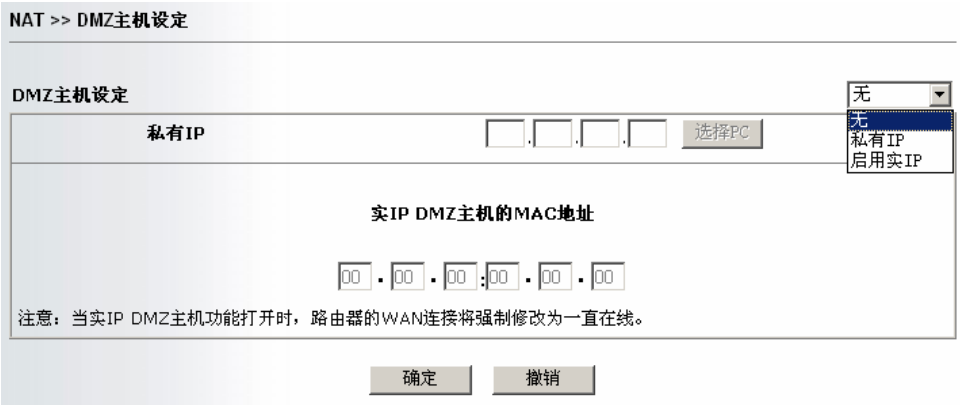
## 3.3.2 DMZ 主机设定

DMZ主机设定功能允许将一台预先设定好的内部主机完全暴露于公网之下，DMZ主机设定适用于一些特定的功能比如视频会议或网络游戏。




我们建议您设定附加的 IP 过滤规则来保护开启 DMZ 功能的主机.

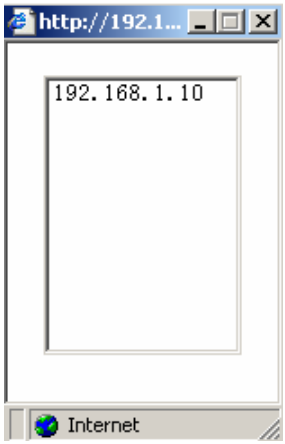
单击 **DMZ 主机设定**，显示如下页面：



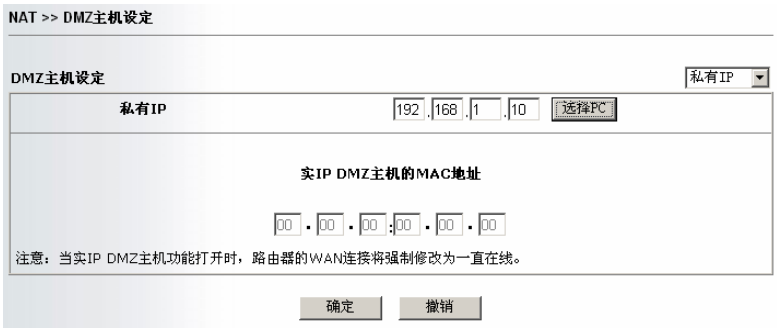

**DMZ 主机设定**　有三种类型的 DMZ 主机设定：**无，私有 IP** 和**启用实 IP**。如果选择**私有 IP**，可以使用**选择 PC** 来指定一台 PC 作为 DMZ 主机。如果选择**启用实 IP**，则可以输入实 IP DMZ 主机的 MAC 地址。

**私有 IP:**　输入一个私网 IP 地址作为 DMZ 主机

**选择 PC:**　单击此按钮将会有一个窗口跳出，其中包含了您的内部私网的所有开启主机的 IP 地址，选择其中之一作为 DMZ 主机：




选择完毕后，单击**确定**完成设定。如果要开启 DMZ 的主机没有打开，也可以通过手动输入的形式完成设定




**实 IP DMZ 主机的 MAC 地址**

如果您选择了**启用实 IP**,您可以输入实 IP DMZ 主机的 MAC 地址.


## 3.3.3 开放端口设定

**开放端口设定**允许您为一些特殊的应用服务打开一段范围内的端口.

单击 **NAT>>开放端口**


**索引:** 显示了个相关条目的号码，您需要单击索引号才能进行编辑。

**注解:** 显示指定的网络服务的名称。

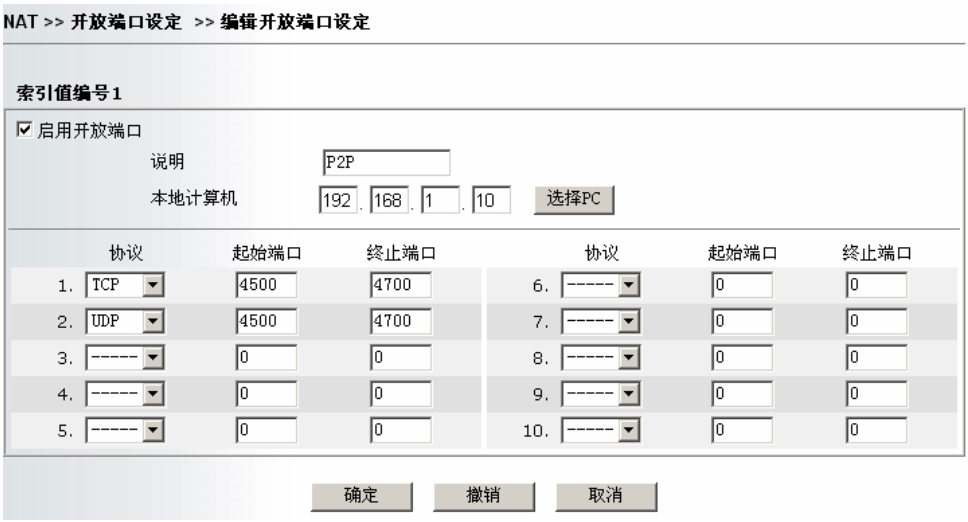
**本地 IP 地址:** 显示提供服务的内部主机的私网 IP 地址。

**状态:** 显示当前条目的状态。用 x 表示未启用，v 表示已启用。.

| | |
|---|---|
| **恢复出厂设置** | 开放端口设定的值回复到出厂设定的值.. |

## 添加/编辑开放端口设定

单击要编辑的索引号,会跳出如下窗口:




**启用开放端口:** 单击来开启此项条目。

**说明:** 输入所定义的网络服务的名称。

**本地计算机:** 输入内网主机的私网 IP。

**选择 PC:** 单击此按钮将会有一个窗口跳出，其中包含了您的内部私网的所有主机的 IP 地址，选择其中之一作为.启用开放端口的主机。

**协议:** 选择一个传输层的协议，此处可选 TCP, UDP, 或者 NONE。

**起始端口:** 为本地的主机所提供的开放端口功能指定一个开始端口。

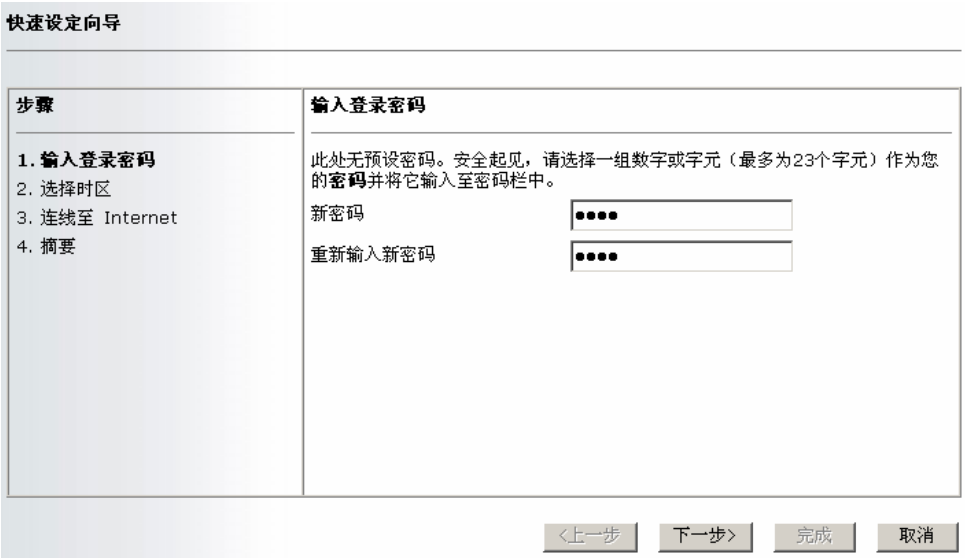
**终止端口:** 为本地的主机所提供的开放端口功能指定一个终止端口。


## 3.4 防火墙

### 3.4.1 防火墙设定基础

当宽带用户在享受网络多媒体服务、交互式应用程序或远程学习时，安全一直是他们最关心的问题。Vigor 路由器的防火墙功能可以帮助您的本地网络防范来自外界的非法攻击。它也可以用于限制本地用户访问 Internet。此外，它还可以用于过滤掉某些能够触发路由器向外界建立连接的数据包，而在有些时候，这种连接是用户并不需要的。

最基本的安全观念就是在安装路由器的时候设置用户名和密码，使得只有网络管理员才能访问路由器的配置页面，杜绝其它未经授权的非法访问。




如果您忘了在安装路由器的时候设置密码，您还可以去**系统管理**选项里设置您的密码。

## 防火墙工具

VigorPro 200B 路由器有以下防火墙防护工具：

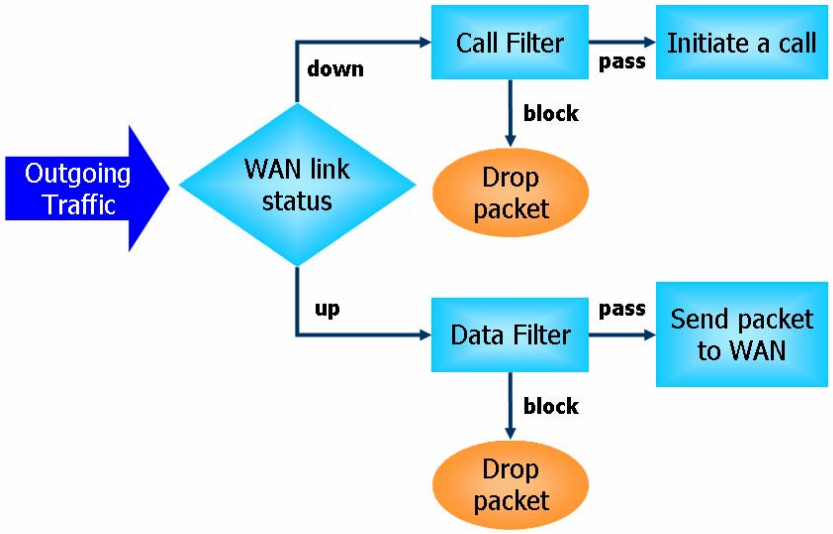
- 可供用户自由配置的 IP 过滤规则(Call Filter/ Data Filter).
- 状态包检测(SPI)：它能够追踪数据包并能拒绝一切未经许可的主动连接数据。
- 可供用户自由选择的攻击防御功能(DoS)，以及分布式攻击防御功能(DDoS)。
- URL 内容过滤器
- 即时通讯软件过滤
- P2P 软件过滤
- Web 内容过滤
- 绑定 IP 到 MAC

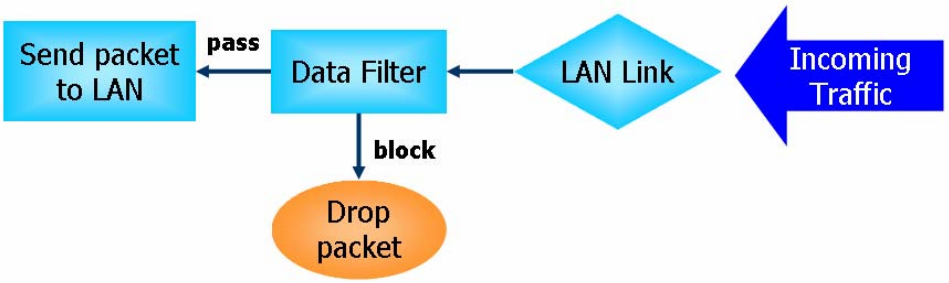
## IP 过滤概述

根据是否存在 Internet 连接或者 WAN 口状态是连接还是未连接，可以将 IP 过滤分为两种：一种是**呼叫过滤器**，另一种是**数据过滤器**。

- **呼叫过滤器**：当路由器没有连接 Internet 时，**呼叫过滤器**用于检查所有外出的数据流。它将根据用户设定好的过滤规则检查数据包。如果是规则允许的，数据就被允许通过。然后路由器就会“**发起一个呼叫**”以建立 Internet 连接，并将此数据包发送到 Internet。
- **数据过滤器**：当路由器已经连接了 Internet 时，**数据过滤器**就用于检查进出的数据。它将根据用户设定好的过滤规则检查数据包。如果是规则允许的，数据就被允许通过。

下面的流程图用于解释路由器如何处理进出的数据包。






## 状态包检测(SPI)

状态检测是一种工作在网络层的防火墙功能。和传统的状态包过滤不同，它是基于包头信息检测的。状态检测增进了状态机制以追踪穿越防火墙每个连接，并确认它们是有效的。Vigor 路由器的状态检测机制不仅检测头信息，而且监视连接状态。

## 即时消息(IM) 软件和点到点软件阻挡

当各种即时聊天软件的不断涌现并逐渐流行起来的时候，通讯就变得不那么容易了。然而，当一些行业以此做为联系客户的一种利器时，另一些行业则因为要减少他们的雇员在上班时间滥用这些工具而影响正常工作或者不知名的安全漏洞，而对此持保留态度。因此，Vigor 路由器中提供该功能，可以让管理员通过简单的选择来实现对即时消息软件的阻挡和通过。

同样，通过 P2P 软件阻挡，可以避免 BT，电驴等软件大量使用给企业网络带来的低效。

## 攻击防御功能 (DoS)

**DoS 防御**功能可以帮助您侦测并防御 DoS 攻击。这些攻击通常分为两种，即 flooding-type 攻击和 vulnerability 攻击。前者是一种企图耗尽您的系统资源的攻击方式，后者则是攻击通讯协议或作业系统的弱点从而使整个系统瘫痪。

**DoS 防御**功能能使 Vigor 路由器对照攻击特征资料库检查每个流入的封包。任何可能使主机瘫痪的封包会被封锁，此时如果您已设置了 Syslog 服务器，一个系统记录会被作为警告马上被发送出去。

Vigor 路由器也会监视流量的变化，任何违反设定好的规则的不正常的流量，例如临界值，都会被当作攻击，并且 Vigor 路由器会实时的启用它的防御体系来减轻攻击。

下面显示的是 DoS 攻击防御功能所能够侦测出的攻击类型：

1. SYN flood 攻击
2. UDP flood 攻击
3. ICMP flood 攻击
4. TCP Flags 扫描
5. 路由追踪
6. IP 选项
7. 不明封包通讯协定
8. Land 攻击
9. Smurf 攻击
10. SYN flood 攻击
11. ICMP 分片攻击
12. Tear Drop 攻击
13. Fraggle 攻击
14. Ping of Death 攻击
15. TCP/UDP 端口扫描

### URL 内容过滤

为了提供一个合适的网络空间给用户，Vigor 路由器配备了**URL 内容过滤**功能，它不仅可以用于限制非法访问不当网站，也可以用于禁止那些隐藏了恶意代码的网站。

当用户输入或点击一个已经存在于 URL 内容过滤里的链接时，URL 关键字阻塞工具将会拒绝 HTTP 请求，该网页也会被限制访问。您可以把**URL 内容过滤**想象成一个训练有素的便利店员不会将成为杂志卖给十几岁的孩子一样。同样，在办公室里，**URL 内容过滤**也能够提供一个和工作有关的环境，以提高雇员的工作效率。怎么样才能使 URL 内容过滤在过滤领域比传统的防火墙工作的好呢？因为它检查URL字符串或是HTTP数据的一些TCP 数据的附载，而传统防火墙则只是基于 TCP/IP 包头来检查数据包。

另一方面，Vigor 路由器可以阻止用户意外的下载来自网页里的恶意代码。恶意代码包含在可执行文件里这是十分常见的，比如 ActiveX，Java 程序，压缩文件以及其它可执行文件。当您从网站上下载这些类型的文件时，这将会对您的系统带来威胁。例如，ActiveX 控件常常被用于提供交互式的网页特性。如果恶意代码隐藏在里面的话，它将占据用户的系统。

### Web 内容过滤

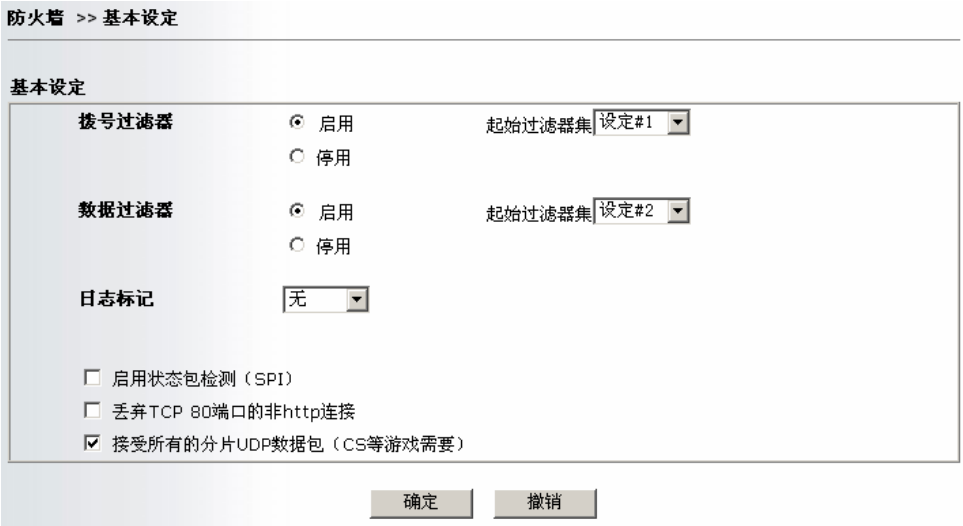
Internet 上的网络资源包罗万象，对于父母来说，一定不希望孩子接触到很多色情的内容；而对于企业主来说，也不会希望员工在上班时间访问游戏站点，新闻站点，而影响正常的工作。通过 Vigor 和网站分类服务提供商合作推出的 Web 内容过滤功能，您可以轻松实现上述的目标。

当您开启了 Vigor 路由器上的 Web 内容过滤服务,并且设置了您想要限制的网站的分类，每一个 URL 地址请求将会依照由 SurfControl 提供的服务器数据库的记录来检查。这个数据库里包含了超过 70 种语言以及 200 个国家，超过 10 亿个网页，并将其分成 40 种容易理解的类别。这个数据库每天都会由 Internet 研究员的全球小组更新。这个服务器将查寻 URL 并返回一个类型给您的路由器。您的 Vigor 路由器然后将会根据您选择的类别以决定是否允许访问这个网站。请注意，这个部分将不会引入任何的延迟在您要访问的网站里，因为每一个多种负载平衡数据库服务器可以处理数百万的分类请求。

## 3.4.2 基本设定

基本设定允许您调整 IP 过滤的设置以及其它常用选项。在这里，您可以开启或关闭**拨号过滤**或**数据过滤**。在一些环境下，您的过滤规则可以连接到一系列方式下工作。所以在这里，您可以只指派**起始过滤器集**。同样，您可以设置**日志标记**设置，**启用状态包检测**，**丢弃 TCP 80 端口的非 http 连接**，以及**接受所有的分片 UDP 数据包**。

点击**防火墙**，并点击**基本设置**可以打开基本设置页面。




**拨号过滤器** 单击**启用**来激活拨号过滤器，并指定起始过滤器组别。

**数据过滤器** 单击**启用**来激活数据过滤器，并指定起始过滤器组别。

**日志标记** 为了及时发现并维修故障，您需要在这里指定过滤日志。
**无** -停用记录功能。
**阻挡** -记录所有被封锁的封包。
**通过** -记录所有通行的封包。
**不匹配** -记录所有不匹配的封包。
注意：当您输入“log -f”指令后，过滤器的记录会显示在 Telnet 终端机上。

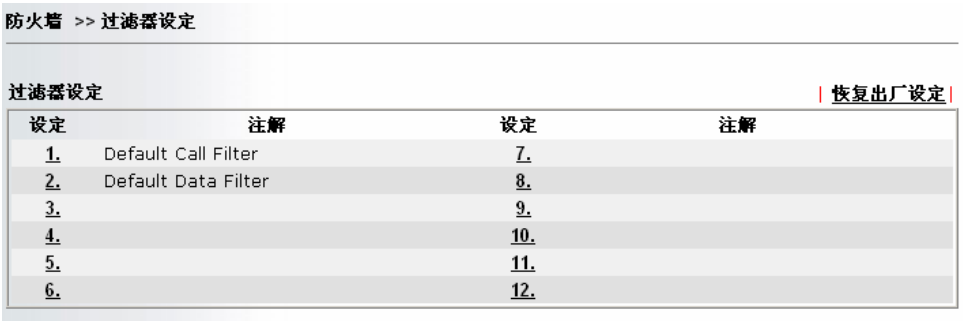
**启用状态包检测** 在此选择框里打勾以启用此功能。

**丢弃 TCP 80 端口的非 http 连接** 在此选择框里打勾以启用此功能。

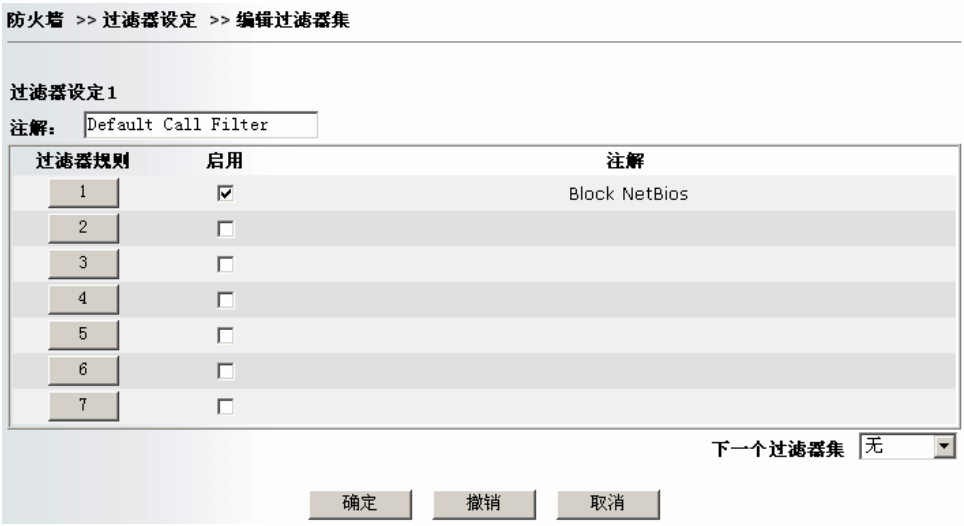
**接受所有的分片 UDP 数据包 Packets** 有些在线游戏（例如：CS）使用长度很长的 UDP 封包传送资料，这些封包需要被切割。如果您没有启用“接收流入的 UDP 封包片段”Vigor 路由器会拒绝这种封包，以避免受到黑客的攻击。如果您启用了此功能，就可以进行这类在线游戏。如果您比较在乎网络的安全性，建议您停用此功能。

## 3.4.3 过滤器设定

点击**防火墙**，并点击**过滤器设定**以打开设置页面。




想要编辑或增加一个过滤，请点击设定的数字以编辑单个设定，接着会出现下面的页面。每个过滤设定包含了最多 7 条规则。点击规则号按钮来编辑每一条规则。检查是否已**启用**来启用这条规则。




**过滤器规则** 点选 1~7 的数字按钮编辑过滤器规则。点击任一按钮将打开编辑过滤规则页面。关于详细的信息，请参照下面的页面。

**启用** 启用或停用过滤器规则。

**注解** 输入过滤器注解描述，最多输入 23 个字符。

**下一个过滤器组别** 在执行完当前过滤设置之后，设置连接到下一个过滤器设定继续执行。注意，请不要设置成循环的顺序！

为了编辑**过滤器规则**，点击**过滤规则**索引按钮进入过滤规则设置页面。


**注解** 输入过滤器组别注解描述，最多输入 14 字符。

**启用此规则** 在此选择框里打勾以启用此功能。

**通过或封锁** 设定当数据包符合条件时所要采取的行动
**立刻封锁** – 当封锁包符合条件时立刻丢弃
**立刻通过** – 当封锁包符合条件时立刻放行
**若无其他规则符合则封锁** – 当封锁包只符合此规则，不符合其它规则时被丢弃。
**若无其他规则符合则通过**– 当封锁包只符合此规则，不符合其它规则时会放行。

**链接到其它过滤器设定** 如果封包符合此规则，则跳过余下的规则而直接用所选规则作为下一条规则。

**记录日志** 在此打勾启动记录功能。当您输入“log -f”指令后，过滤器的记录会显示在 Telnet 终端机上。

**方向** 设定封包流向（上行或下行），它仅用于数据过滤器。对于呼叫过滤器，此项设定是没有用处的，因为呼叫过滤器仅用于外出的数据流。

**通讯协议** 设定通讯规则适用的通讯协议 (TCP, UDP, TCP/UDP, ICMP, IGMP)

**IP 地址** 设定一组适用此过滤规则的来源和目标 IP 地址。如果在 IP 地址前面加上“!”符号则表示此过滤规则不适用于此 IP 地址。要想将此规则用于所有的 IP 地址，输入 **any** 或留为空白。

**子网掩码** 为所设置的 IP 地址选择**子网掩码**以控制过滤规则所应用的范围。

**运算符，起始端口和终止端口** 运算符的设定和通讯的端口有关。如果起始端口为空，则起始端口和终止端口的栏位将被忽略，过滤规则将适用于所有端口。
**(=)** –如果终止端口不填，过滤规则将只适用于起始端口所填的端口；若有填入数值，则过滤规则适用于从起始端口起到终止端口结束的所有端口。
**(!=)** –如果终止端口不填，过滤规则将只不适用于起始端口所填的端口;若有填入数值，则过滤规则不适用于从起始端口起到

终止端口结束的所有端口。其它的端口都适用。
(>) –过滤规则适用于所有端口大于等于起始端口的端口。
(<) –过滤规则适用于所有端口小于等于起始端口的端口。

**记录状态**

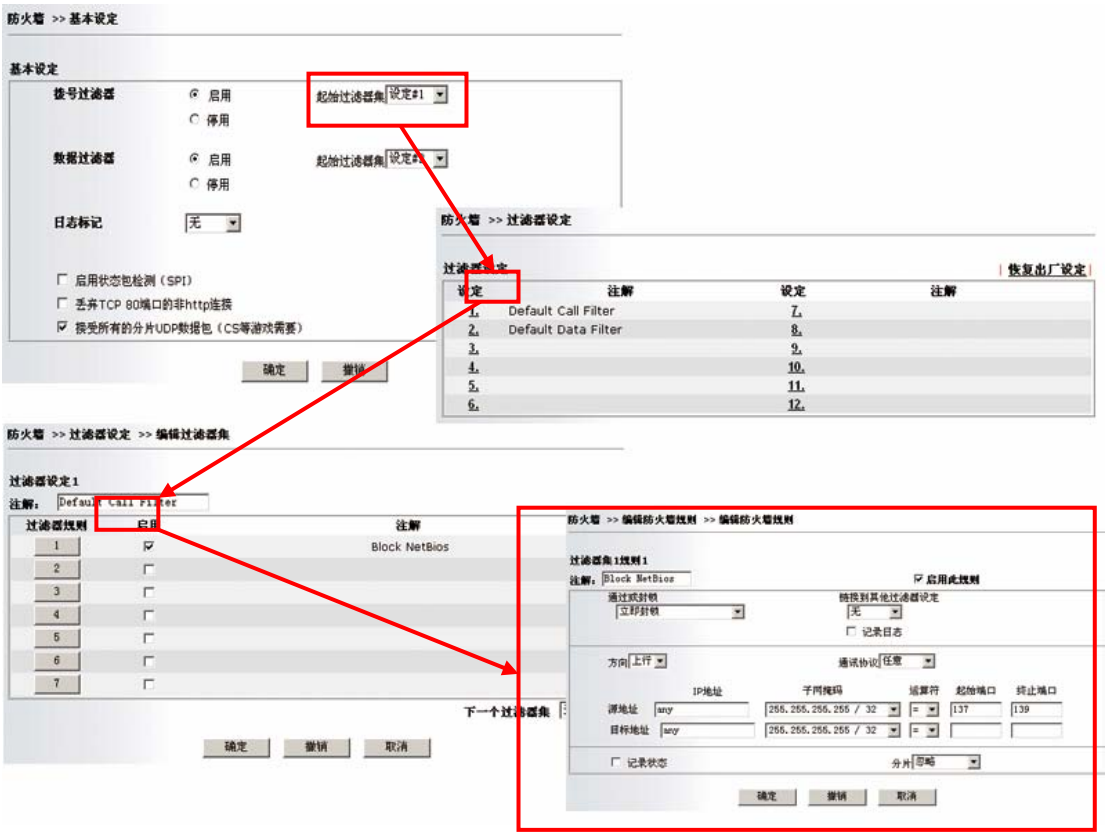
这个功能应该和目标地址，通讯协议，IP 地址，子网掩码，运算符起始端口和终止端口一起用。它只用于数据过滤器。
记录状态和现在的状态包检测具有相同的性质。它追踪数据包并接受以适当性质显示它的状态是协议所定义的合法的数据包。它将拒绝未经请求的流入封包。您在通讯协定选项里必须选择 TCP，UDP，TCP/UDP 或 ICMP。

**分片**

指定处理数据包时对分片数据的处理。它只用于**数据包过滤**。
**忽略** –过滤规则适用于所有的封包切割形式。
**完整无分片** –过滤规则适用于没有被切割的封包。
**片段** – 过滤规则适用于被切割的封包。
**太短** – 过滤规则适用于太短的封包。

## 范例

在设置之前，所有的数据流将会被分别成为两种 IP 过滤器的一种：呼叫过滤器或数据过滤器。您可以预先设置 12 个呼叫过滤器和数据过滤器在**过滤器设置**里，并且可以将它们连接到一系列其它的过滤规则里。每一条过滤集由 7 个过滤规则组成，也可以进一步定义。之后，在**基本设定**里，您可以指定一个过滤集给呼叫过滤器，一个过滤集给数据过滤器。



## 3.4.4 即时通讯软件（IM）屏蔽设定

即时通讯软件屏蔽意味着即时消息屏蔽。点击防火墙并点击即时通讯软件屏蔽可以打开设置页面。您可以看到一个常用即时通讯软件的列表（如，**MSN，Yahoo，QQ，ICQ/AQL**）软件。勾选**启用即时通讯软件（IM）软件过滤**，并选择您想要屏蔽的软件。如果想要在一段时间里屏蔽所选的即时通讯软件，只要输入在**应用**下的**计划任务**里预先设置好的时间设定的值即可。

## 3.4.5 P2P 过滤设定

点击防火墙并点击 P2P 过滤设定就可以打开设置页面。您可以看到一个常用的点到点软件的列表，选择您想要屏蔽的软件即可。如果想要在一段时间里屏蔽所选的点到点软件，只要输入在**应用**下的**计划任务**里预先设置好的时间设定的值即可。


**动作** 对每个协议都有效。
**允许** – 允许客户端通过指定的协议访问应用程序。
**禁止** – 禁止客户端通过指定的协议访问应用程序。
**禁止上传** – 允许客户端通过指定的协议访问应用程序进行下载。而禁止上传。

**索引（1~15）计划任务设定** 您可以为您的规则输入 4 个计划任务。所有的计划任务都可以被提前在**应用**的**计划任务**的页面里设置。

## 3.4.6 拒绝服务（DoS）攻击防御功能设定

作为 IP 过滤器/防火墙的子功能，总共有 15 种防御功能。**DoS 攻击防御**功能在路由器的默认设定中是停用的。点击**防火墙**并点击**拒绝服务（DoS）攻击防御功能设定**就可以打开设置页面。


**启用拒绝服务（DoS）攻击防御功能** 勾选以启用 DoS 攻击防御功能。

**启用 SYN flood 攻击防御** 如果从互联网来的 TCP SYN 数据包超过用户设置的临界值，Vigor 路由器将会在用户设置的超时时间内随机丢弃 TCP SYN 数据包。主要的目标是保护 Vigor 路由器不受企图耗尽路由器资源的 TCP SYN 数据包的威胁。

**启用 UDP flood 攻击防御功能** 勾选以启用 UDP flood 攻击防御功能。一旦从因特网来的 UDP 封包超过使用者设定的临界值，Vigor 路由器将会在使用者设定的逾时时间内丢弃所有随后的 UDP 封包。预设的临界值和逾时数值分别被预设为 300 封包/秒和 10 秒。

**启用 ICMP flood 攻击防御功能** 勾选以启用 ICMP flood 攻击防御功能。如同 UDP flood 攻击防御功能，一旦从因特网来的 ICMP 响应请求封包超过使用者设定的临界值(预设为 300 封包/秒)，Vigor 路由器将会在使用者定义的逾时时间(预设为 10 秒)内丢弃所有随后的 UDP 封包。

**启用通讯端口扫描侦测功能** 通讯端口扫描攻击是指传送很多不同通讯端口的封包，企图扫描有哪些通讯端口正在被使用，得知有哪些可用的服务。为了侦测通讯端口扫描行为，请勾选以启用 Vigor 路由器内的防御通讯端口扫描侦测功能。如果通讯端口扫描速率超过使用者设定的临界值，Vigor 路由器将会发现并且发出警告讯息。预设中，Vigor 路由器将临界值设定为 300 封包/秒。

| | |
|---|---|
| **封锁 IP 选项** | 勾选以启用封锁 IP Options。Vigor 路由器将会忽略任何在数据文件头中有 IP Options 字段的封包。IP Options 让主机可以传送一些重要讯息，例如 Security,Compartmentation, TCC (closed user group)参数，一连串的网址，路由信息等。别人可能会加以分析，而搞清楚您的内部网络。 |
| **封锁 Land 攻击** | 勾选以启用 Vigor 路由器防御 Land 攻击。Land 攻击结合了 SYN 攻击技术和 IP 伪造。Land 攻击方式是攻击者传送伪造的 SYN 封包，封包内含相同的来源和目的地址(和受害者地址相同)以及相同的通讯端口。 |
| **封锁 Smurf 攻击** | 勾选以启用封锁 Smurf 攻击功能。Vigor 路由器会拒绝任何指向广播地址的 ICMP 响应请求。 |
| **封锁路由追踪** | 勾选以启用此功能。Vigor 路由器将不会传送任何路由追踪封包 |
| **封锁 SYN 分片攻击** | 勾选以启用封锁 SYN Fragment 封包功能。任何具有 SYN Flag 以及 More Fragment 位设为 1 的封包会被丢弃。 |
| **封锁 Fraggle 攻击** | 勾选以启用封锁 Fraggle 攻击功能。任何从因特网收到的广播 UDP 封包都会被封锁。注意启用 Dos/DDos 攻击防御功能可能会封锁一些合法的封包。例如，当您启用封锁 Fraggle 攻击功能，所有从因特网上广播的 UDP 封包都会被封锁。所以从因特网上来的 RIP 封包也会被丢弃。 |
| **封锁 TCP Flags 扫描** | 勾选以启用封锁 TCP Flags 扫描功能。任何具有不正常 Flag 设定的 TCP 封包会被丢弃。这些扫描的活动包含 no flag scan，FIN without ACK scan，SYN FIN scan，Xmas scan，以及 full Xmas scan。 |
| **封锁 Tear Drop 攻击** | 勾选以启用封锁 Tear Drop 攻击功能。这种攻击是指攻击，者传送部份重迭的封包到目标主机，当那些主机要重组封包时就会当机。Vigor 路由器会封锁这些封包。 |
| **封锁 Ping of Death 攻击** | 勾选以启用封锁 Ping of Death 攻击功能。许多机器在收到超过最大长度的 ICMP 封包可能会当机。为了避免这种攻击，路由器必须能丢弃任何长度超过 1024 八字节的切割封包。 |
| **封锁 ICMP 分片攻击** | 勾选以启用封锁 ICMP Fragment 封包功能。任何 More Fragment 位设为 1 的 ICMP 封包会被丢弃。 |
| **封锁不明封包通讯协定** | 勾选以启用封锁不明通讯协议封包功能。每个 IP 封包在档头都会有一个通讯协议字段，用来指出在上层使用哪种通讯协议。然而，超过 100 的通讯协议代号目前仍然保留没有被定义，所以路由器要能侦测并拒绝这种封包。 |

在启用了您所需要的设置之后，请按**确定**键保存设置。如果您想清除这里的所有设置，请点击**撤销**键。

## 3.4.7 URL 内容过滤

Vigor 路由器的 URL 内容过滤工具会基于用户自定义关键字列表，对每一个外出的 HTTP 请求都检查其 URL 字符串。不管此 URL 字符串和所设关键字是完全匹配还是部分匹配，Vigor 路由器都将会阻挡相关 HTTP 连接。

例如，您添加了一个关键字里加了一个“sex”,Vigor路由器将会限制访问诸如“www.sex.com”的此类网站或网页。同样，Vigor路由器也将会丢弃所有已含有恶意代码的请求。

点击**防火墙**并点击 **URL 内容过滤**可以打开设置页面。


**启用 URL 访问控制** 勾选此选择框以启用此功能。

**黑名单（屏蔽下列匹配关键词）** 点选此选择框以限制访问已出现在关键字列表里的相应的网页。

**白名单（允许下列匹配关键词）** 点选此选择框以允许访问已出现在关键字列表里的相应的网页。

**关键字** Vigor 路由器提供 8 个关键字列表给用户自定义关键字，而每个关键字列表又可以同时输入多个关键字。关键字可以是名词，名词的一部分，或者是完整的 URL 字符串。在同一个关键字列表里的多个关键字可以以空格，逗号或分号分隔。另外，每个关键字列表里最多可以 32 个字符。在指定好关键字之后，Vigor 路由器会拒绝一切和所设置的关键字相匹配的网页链接请求。

| | |
|---|---|
| **防止使用 IP 地址对网站进行访问** | 勾选此选择框以拒绝任何使用IP地址访问网页，比如 http://202.6.3.2。这样做的目的是防止有些人以此来躲避URL内容过滤的控制。<br><br>您必须清除您所使用的浏览器的缓存以便 URL 内容过滤工具在过滤网页时可以准确无误的运行。 |
| **启用限制网络功能** | 勾选此选择框以启用此功能。<br><br>**Java** - 勾选此选择框以启用阻挡从 Internet 上下载 Java 文件。<br><br>**ActiveX** - 勾选此选择框以启用阻挡从 Internet 上下载 ActiveX 文件。<br>**压缩文件** - 勾选此选择框以启用阻挡从 Internet 上下载压缩文件。Vigor 路由器能够阻挡的压缩文件包括以下几种：<br>**zip, rar, .arj, .ace, .cab, .sit**<br>**可执行文件** -勾选此选择框以启用阻挡从 Internet 上下载可执行文件。Vigor 路由器能够阻挡的可执行文件包括以下几种：<br>**.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg**<br>**Cookie** - 勾选此选择框以阻止您的主机向外发送您的 cookie 信息，以保护用户的隐私。<br>**代理** - 勾选此选择框以拒绝一切代理，以有效的控制带宽的使用。这是一个很好的保护机制以阻挡从网页上下载多媒体文件。Vigor 路由器能够阻挡的多媒体文件包括以下几种：<br>**.mov .mp3 .rm .ra .au .wmv**<br>**.wav .asf .mpg .mpeg .avi .ram** |
| **允许例外子网** | 用户可以指定 4 个例外的 IP 地址或子网以便他们可以不受 URL 内容过滤的限制，而能自由的访问 Internet。请点击**启用**以使您的设置生效。 |
| **索引(1-15)计划任务设定** | 您可以在这里输入 4 个计划任务值以使得 URL 内容功能在您规定的时间里生效。而使用的计划任务都可以在应用的计划任务里预先进行设定。 |

在启用了您所需要的设置之后，请按**确定**键保存设置。如果您想清除这里的所有设置，请点击**撤销**键。

## 3.4.8 Web 内容过滤

该功能是通过第三方网站分类服务，根据网站分类进行网络接入的限制，例如屏蔽新闻分类，则所有网内客户机就无法访问 tom 新闻，新浪新闻等这样的新闻类网站。由于是和专业的服务提供商合作，网站分类做的相当细致详尽，因此，对于企业用户来说，通过分类来禁止员工上不允许访问的网站是非常有用的功能。

需要说明的是，由于分类服务由第三方服务商提供，因此，要长期使用此功能需要向服务商支付一定的费用。不过，Vigor 路由器支持该功能一个月的免费试用，可以先试用再决定是否要向服务商购买。

点击**防火墙**并点击 **Web 内容过滤**就可以打开设置页面，可以看到，网站分类涉及到方方面面，用户可以做到非常细化的设定。


要使用该功能，必须首先到第三方服务商的网站进行注册。

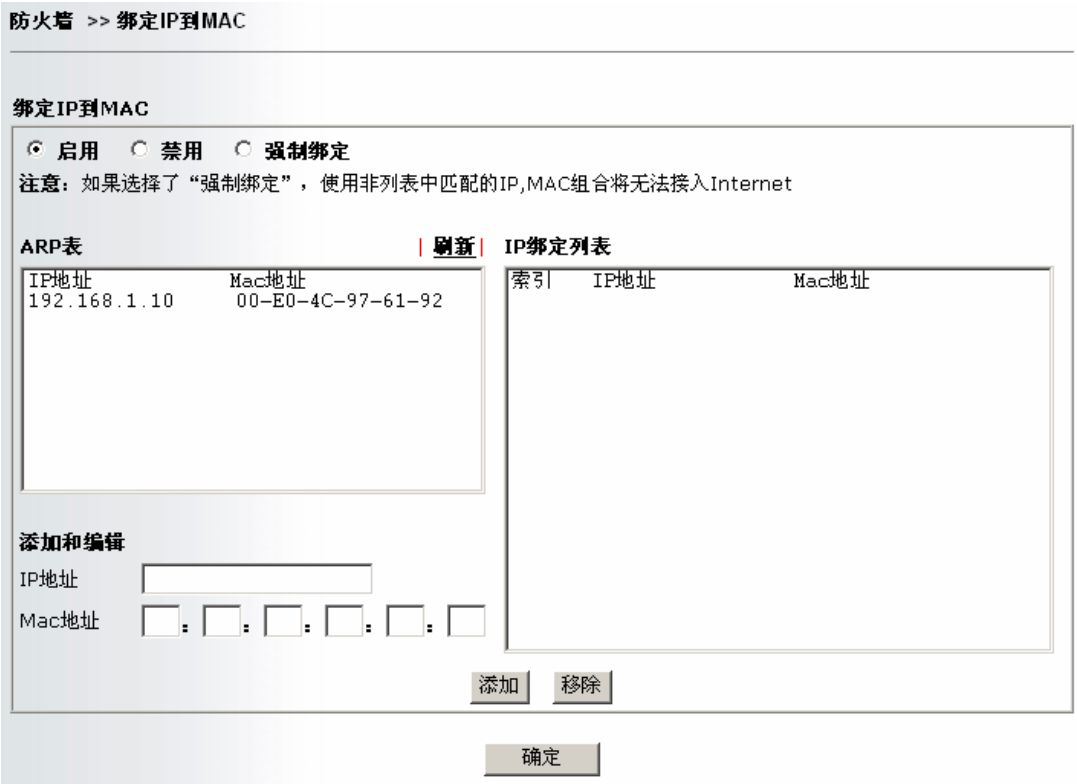
关于该功能的设置使用过程，请参阅第四章 **Web 内容过滤**的用户指南。

## 3.4.9 绑定 IP 到 MAC

该功能用来将局域网内的 IP 地址和 MAC 地址进行绑定，以便对网络加强管控。当启用该功能后，如果修改 IP 或 MAC 地址，将无法上网。

对于此功能，VigorPro200B 最多支持 300 组的绑定设定。

点击**防火墙菜单**，并点击**绑定 IP 到 MAC** 打开配置页面。




| | |
|---|---|
| **启用** | 功能处于启用设置状态，不过不会禁止非绑定 IP 上网，除非选择**强制绑定** |
| **禁用** | 禁用此功能，所有该页面设置将无效 |
| **强制绑定** | 强制执行绑定，所有和列表中不匹配的 IP/MAC 对将无法上网 |
| **ARP 表** | 路由器的 ARP 表，会将现在开机的所有的 IP,MAC 信息显示出来，可以使用鼠标点击选择后，点击**添加**将选中的 IP/MAC 加入列表。使用 SHIFT/CTRL 键可以进行批量选择。 |
| **刷新** | 刷新 ARP 列表，当有新 PC 加入网络时，可以点刷新获得最新的 ARP 表信息 |
| **IP 绑定列表** | 显示已经加入绑定列表的 IP，MAC 信息 |
| **添加** | 将 ARP 表中选中的项或**添加和编辑**中输入的项添加到 **IP 绑定列表**。 |
| **移除** | 选中 **IP 绑定列表**中的项，然后点**移除**可以删除指定的项 |

可以使用手工输入的方式来输入 IP，MAC 地址的绑定。

对于大量的添加时，手动输入的效率就很低，因此可以使用批量添加的功能，在所有电脑都联网的情况下，ARP 表会记录所有 IP 的 ARP 信息，在列表中全选，然后点击“**添加**”就可以一次性添加所有的 IP MAC 信息。

**注意：在选择强制绑定之前，请至少先绑定一台 PC 的 IP MAC 信息，否则，任一 PC 都会无法上网，并无法进入路由器配置页面。**

## 3.5 带宽管理

### 3.5.1 WAN 口路由选择

对于中国用户，尤其是网吧用户来说，往往会申请多条线路进行负载均衡。但是通常情况下，负载均衡是根据流量均衡，不会智能的根据数据流向均衡，如果电信的服务器用网通访问，这样速度就会很慢。如果玩网游时电信服务器走电信线路，网通服务器走网通线路，游戏和上网速度将大大提升。

针对这一需求，VigorPro200B 系列路由器设计了 WAN 口路由选择功能。用户只需要简单的做一下选择，就可以做到电信走电信，网通走网通。

对于一些没有列入我们数据库的 IP 地址，可能会出现无法正确转向的情况，客户可以通过**手动配置 WAN 口选择**来实现正确的转发。例如 ISP 提供的在线点播站点，就可以通过策略路由强制走正确的线路。

在**带宽管理**菜单，选择 **WAN 口路由选择**，将显示如下页面


启用电信网通路由选择，只需要选择**启用**，同时指定电信、网通所在的 WAN 口即可，启用此功能后，路由器会根据自带的 IP 数据库对电信网通流量进行选择，实现**电信走电信，网通走网通**。

对于非电信/网通的流量，默认情况下是自动在两个 WAN 口做负载平衡的，如果要指定其他流量使用的 WAN 口，可以在**其他流量**下拉列表中选择相应的 WAN 口。

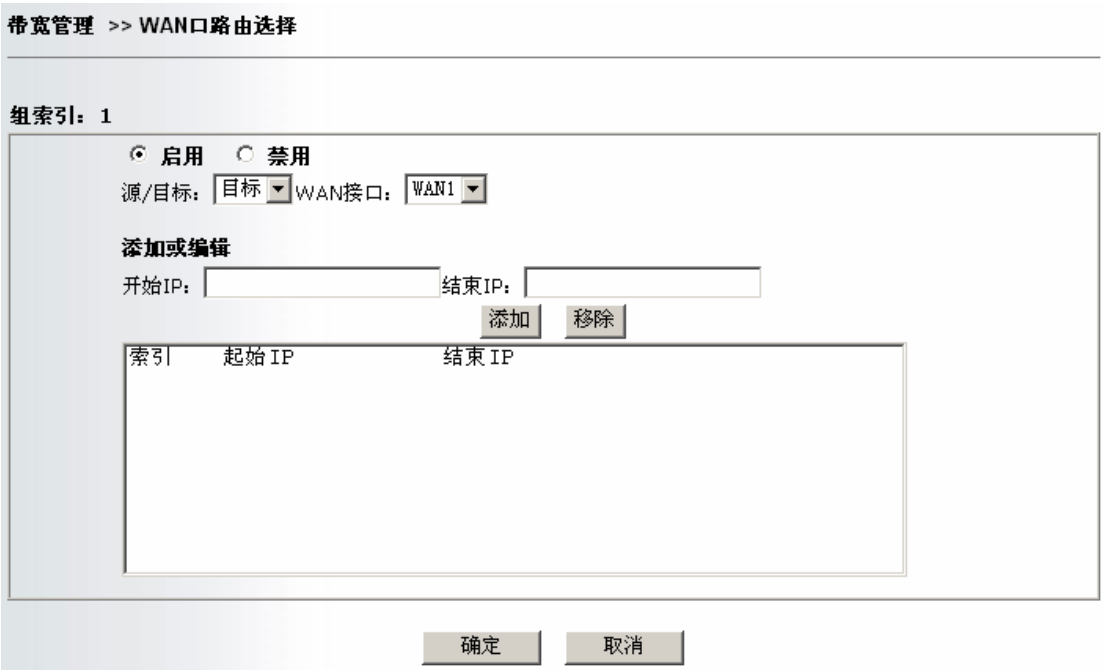
**手动配置 WAN 口选择**

通过启用该功能，可以自行设计网络流向，根据源/目标地址，来确定走哪个 WAN 口，这样网络管理员就可以根据需要来规划网络。

**启用**　　功能处于启用设置状态。设置的组 IP 范围设置生效

| | |
|---|---|
| **禁用** | 禁用此功能，所有该页面设置将无效 |
| **自动** | 根据会话使用情况自动选择 WAN 口（默认设定） |
| **源/目标** | 选择组设定所作用的范围，如果选择源则代表该组设定是针对内网 IP 范围作用;选择目标则说明该组设定对目标 Internet IP 作用。 |
| **WAN 接口** | 指定该组设定的 IP 范围从哪个 WAN 口出去 |
| **编辑** | 编辑该组的 IP 列表 |
| **删除** | 清除全部 IP 列表 |

点击任一组的编号或**编辑**，即可进入组 IP 列表设置页面，如下图：




| | |
|---|---|
| **启用** | 启用该组设置。 |
| **禁用** | 禁用该组设置。 |
| **源/目标** | 选择组设定所作用的范围，如果选择源则代表该组设定是针对内网 IP 范围作用;选择目标则说明该组设定对目标 Internet IP 作用。 |
| **WAN 接口** | 指定该组设定的 IP 范围从哪个 WAN 口出去 |
| **开始 IP** | 输入起始 IP 地址 |
| **结束 IP** | 输入结束 IP 地址 |

应用示例请参见第四章。

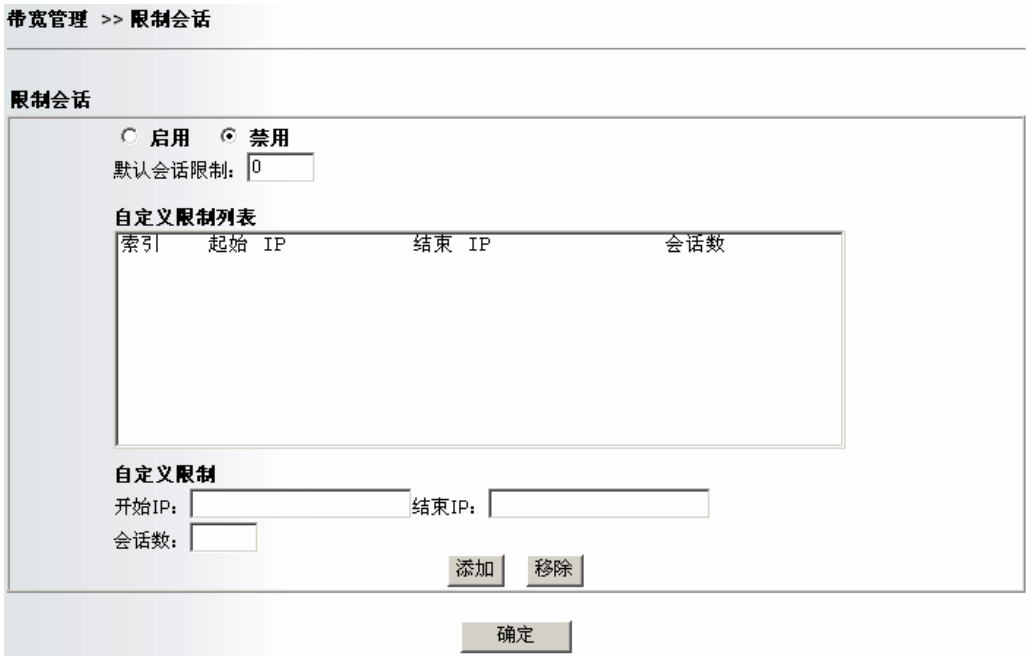
## 3.5.2 会话控制

会话（Session）是指一个主机通过 NAT 向外部 Internet 发起的连接，例如，一台 PC 通过自己私网 IP 的 1234 端口向某个网站发起访问（80 端口），这样就会在 NAT 里有一个记录，成为一条会话。

企业网络管理员往往为网内有人使用 P2P 感到头疼不已,会话控制就是通过对 PC 使用的会话数进行限制来实现对 P2P/蠕虫的控制。

P2P 有一个特点就是要发起大量的会话，占用系统资源和网络带宽。而网络中如果有 PC 中了蠕虫病毒，也会有类似的行为，影响整个网络。在 VigorPro200 中，如果设置了会话控制，每台 PC 的会话将被严格控制，如果超出会话，就无法上网，此时不明就里的用户就会告诉网管，然后网管就可以查一下是哪种情况导致不能上网。

在**带宽管理**菜单，选择**会话控制**，将显示如下页面




启用**会话控制**功能，只需要在该页面选中**启用**并设置一个默认会话限制即可。

| | |
|---|---|
| **启用** | 启用会话控制功能 |
| **禁用** | 禁用会话控制功能 |
| **默认会话限制** | 网内每台 PC 默认可以使用的会话数。 |
| **自定义限制列表** | 该列表中的 IP 地址可以使用指定的会话数，不受默认会话限制的约束。 |
| **开始 IP** | 自定义的起始的 IP 地址 |
| **结束 IP** | 自定义的结束的 IP 地址 |
| **会话数** | 自定义 IP 可使用会话数 |

| | |
|---|---|
| **添加** | 将设定的例外会话限制添加到列表 |
| **移除** | 移除列表中已经存在的设定 |

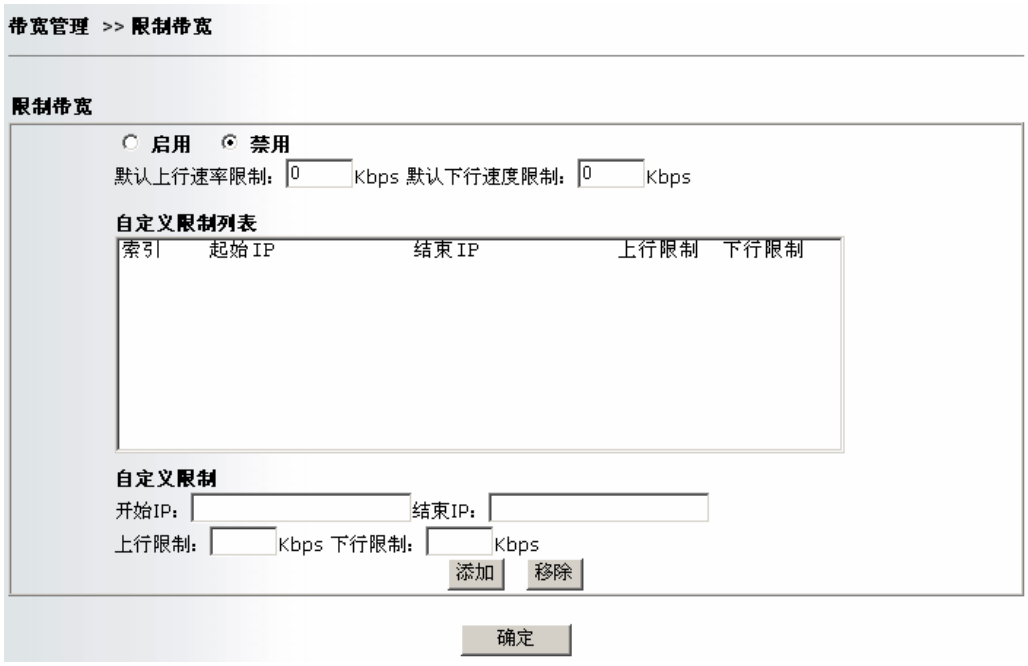
应用示例请参见第四章。

### 3.5.3 带宽使用限制

Flashget，迅雷，BT，电驴等程序的使用频率越来越高，经常会导致一台 PC 占据大量的带宽，而其它多数 PC 却无法保障最基本的上网带宽，从而影响大多数人的网络使用，对于网管来说，对每台机器的带宽进行管控就变得格外重要。

**带宽使用限制**功能，可以对每台 PC 使用的带宽进行控制，使每台 PC 使用的带宽都处于限制范围之内，这样既保障了日常的使用，也不会让少数 PC 大量滥用带宽。该功能不仅可以设置默认带宽，同时还可以为一些指定的 PC 设定例外带宽，这样就保障了部分 PC 可以大量使用带宽，保障了各种应用的灵活性。

在**带宽管理**菜单，选择**带宽使用限制**，将显示如下页面




启用**带宽使用限制**功能，只需要在该页面选中**启用**并设置默认上行下行速度限制即可。

| | |
|---|---|
| **启用** | 启用带宽使用限制功能 |
| **禁用** | 禁用带宽使用限制功能 |
| **默认上行限制** | 网内每台 PC 默认上行的限制速度 |
| **默认下行限制** | 网内每台 PC 默认下行的限制速度 |

| | |
|---|---|
| **自定义限制列表** | 该列表中的 IP 地址可以使用指定的带宽，不受默认带宽的限制。 |
| **开始 IP** | 自定义的起始的 IP 地址 |
| **结束 IP** | 自定义的结束的 IP 地址 |
| **上行限制** | 自定义的上行速度限制 |
| **下行限制** | 自定义的下行速度限制 |
| **添加** | 将设定的例外速度限制添加到列表 |
| **移除** | 移除列表中已经存在的设定 |

应用示例请参见第四章。

### 3.5.4 服务质量（QoS）

Vigor 路由器中提供的服务质量保障技术可以让网络管理员实时监控，分析以及分配各种网络流量或者为重要的数据流量设定优先带宽。

这样一来，实时性更强的应用不会受到网页访问或其它非重要网络访问流量的冲击。如果没有 QoS 的保障，就无法为用户或服务优先安排带宽资源以支持一些实时性较强的服务，例如 VoIP（IP 电话）或在线游戏等等，这些服务的质量就会受到影响（例如声音断断续续）。因此，我们相信服务质量区分将是互联网架构中最为重要的问题。在 Vigor 路由器中，我们同样提供了对 DSCP（区分服务代码）的支持。

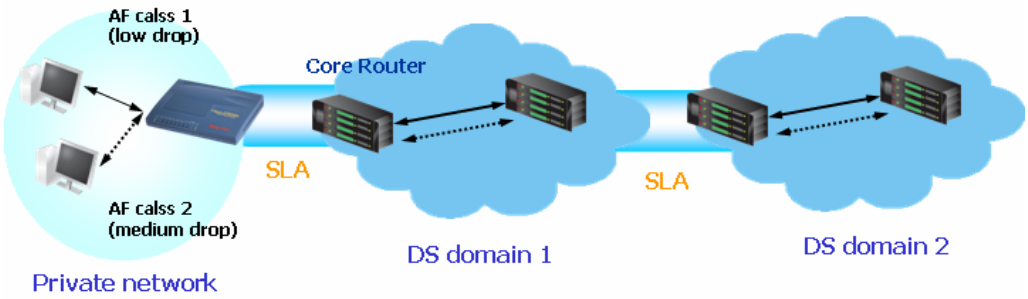
为了给 QoS 一个更为直观的解释，那么，让我们从两个方面来解释 QoS：

- 分类：对应用进行区分，对高优先级的应用进行标记，保障其最及时被发送。
- 安排：根据服务级别的分级来安排数据包通过的顺序，保障最高优先级的最先被发送。

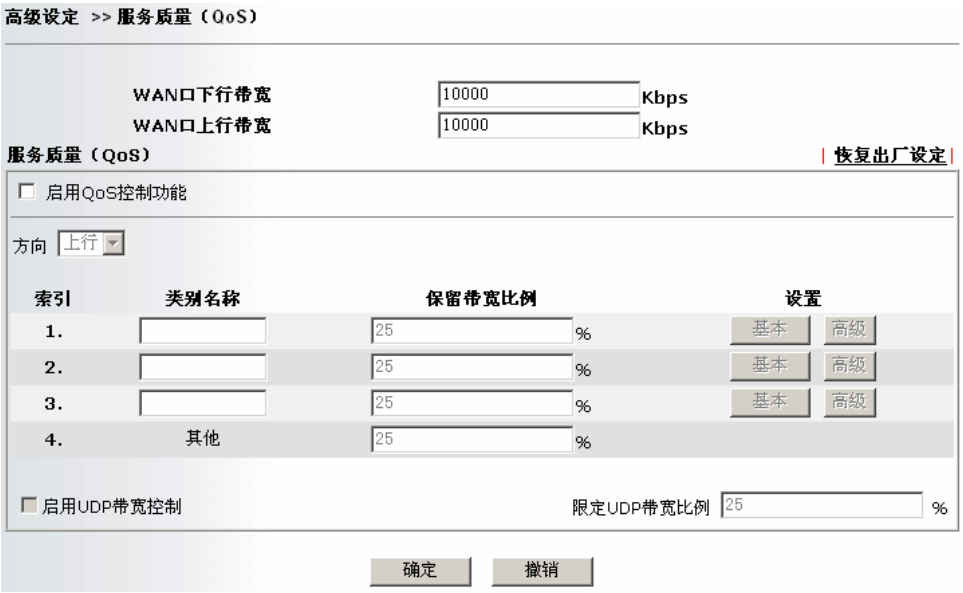
Vigor 路由器中最基本的 QoS 实现是根据 IP 头中的服务类型来对服务进行分类和安排。例如，为了在其它网络流量较多的时候，保障 HTTPS 连接的速度不被影响，可以在 QoS 中对 HTTPS 服务进行设置，这样，HTTPS 的带宽将被保障。

在大规模的 QoS 网络应用中，应用 DSCP（区分服务代码）和 IP 优先级来对网络流量分类和安排。DSCP 可以建立 64 级的优先级并且向下兼容 IP 优先级。在一个 QoS 被应用的网络/区分服务的架构中，一个区分服务的域需要和其它区分服务域的拥有者签订一个服务许可协议（SLA）以定义和其它域之间发送数据的服务级别。这被称作单次跳跃行为（PHB），PHB 的定义包含了迅速发送（EF），确保发送（AF）和尽可能发送（BE）。AF 定义了四种发送级别，在每一级别中，分别定义了三种丢弃优先级别。

Vigor 路由器在作为 DS 域的边界路由器时，要检查通过的流量中 IP 头的 DSCP 值，来安排相应的分类，通过。主干网的核心路由器在执行转发操作之前应该做同样的工作以确保服务级别在整个 QoS 网络中以同一标准被执行。




在**应用程序**菜单，点击**服务质量（QoS）**，打开如下页面。




**WAN 口下行带宽** 设置连接的宽带线路的下行带宽，例如，连接的 ADSL 线路支持 1M 的下行和 256K 的上行带宽，可以在此处设置 1000 在此框中。默认值是 10000kbps。

**WAN 口上行带宽** 设置连接的宽带线路的上行带宽，例如，连接的 ADSL 线路支持 1M 的下行和 256K 的上行带宽，可以在此处设置 256 在此框中。默认值是 10000kbps。

**启用 QoS 控制功能** 出厂设置中，默认是启用 QoS 控制功能的。

**方向** 定义 QoS 控制的目标流量。
**下行-** 仅应用于下行流量
**上行-** 仅应用于上行流量
**双向-** 对下行和上行流量都起作用。

**索引** QoS 控制的索引，一共 4 组 QoS 设定。

**类别名称** 定义类别名称

**保留带宽比率** 对指定的组保留相应的上行带宽和下行带宽

**设置** 有两种类型的设置。请参照下一节。

**启用 UDP 带宽控制** 选中此项则根据设置的带宽比率限制 UDP 流量。因为无节制的 UDP 流量（例如在线点播）会耗尽带宽，影响 TCP 应

用。

**限定 UDP 带宽比例**　　指定 UDP 使用的带宽比例

对于类别名称来说，只有三种类别是可修改的，而最后一个类别是保留作为“其它”流量的带宽的。这里的“其它”是指不属于前面三类已经定义过的类别之外的流量。类别名称最多可以为12 个字符。默认情况下，前三个类别的名称为空，用户可自行修改。

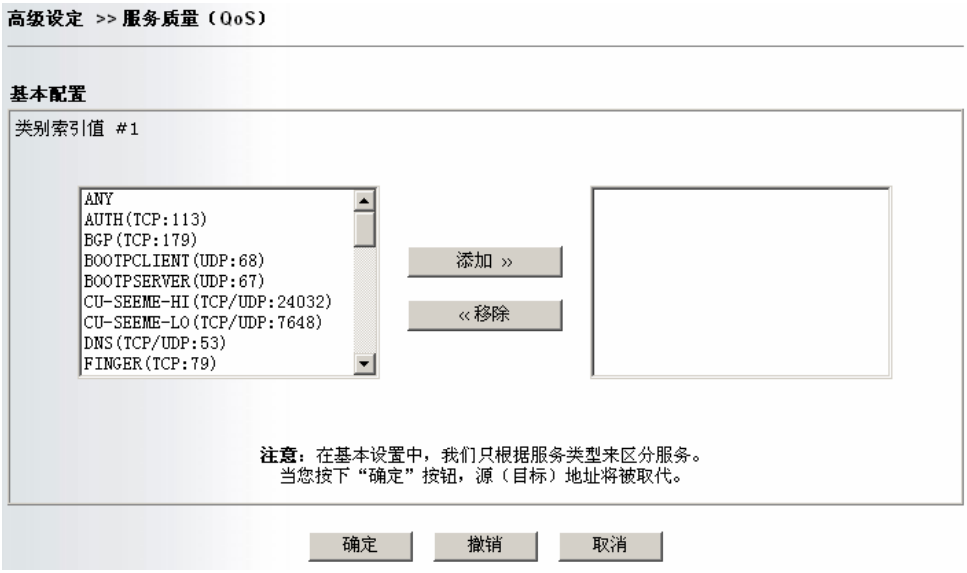
预留带宽比例：用户可以针对每个类别来填写保留带宽比率。默认情况下，这些预留带宽处都为空。保留带宽值可以填写1 到97 的数字，当所有的保留带宽填写完毕后，路由器会将剩余的带宽比例分配给“其它”类别使用。

请注意，如果保留带宽比率的总数超过了100％，路由器将会检测到此错误并且弹出警告消息“所有类别的总保留带宽比率不能超过100％ ”。

## QoS 基本配置

**基本配置**是快速为常用服务设定服务端口的方法，例如，要保障 https 服务，则无需进行复杂的设定，只需要选中 HTTPS 服务并添加即可完成设置。

点击**基本**按钮打开相应 QoS 组的索引值。



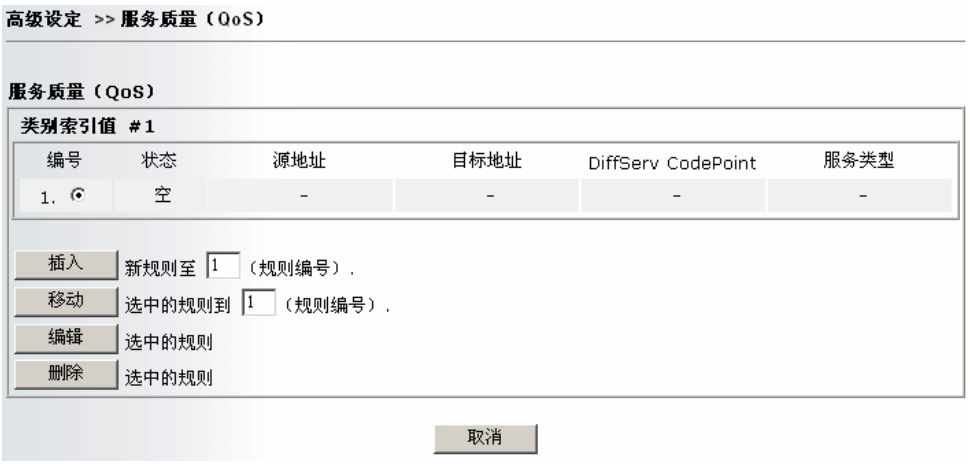

选择左边框中的服务点击**添加>>**将其添加到右边框中，右边框即为选中的所有 QoS 保障服务。要移除选中的 QoS 保障服务，只需要在右边框中选中，并点击**移除**即可。

## QoS 高级设定

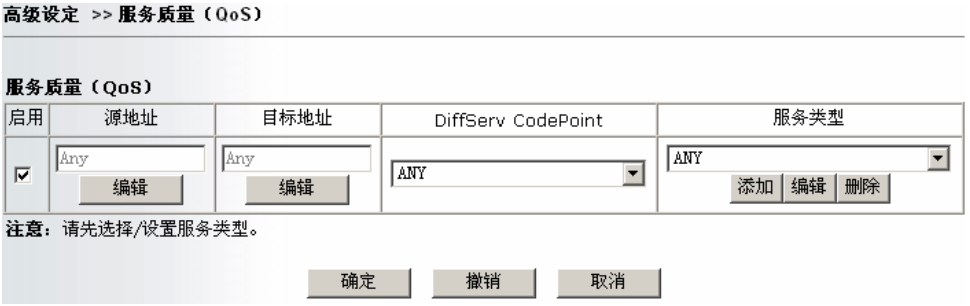
**高级设定**提供了更大的灵活性来保障非常见端口服务以及自定义的带宽应用。

例如，您可以为 192.168.1.10-192.168.1.20 的 PC 使用 12345 端口做 QoS，这样的设定在基本设定中是不可想象的，但是有了高级设定，这就成为了可行的设置。

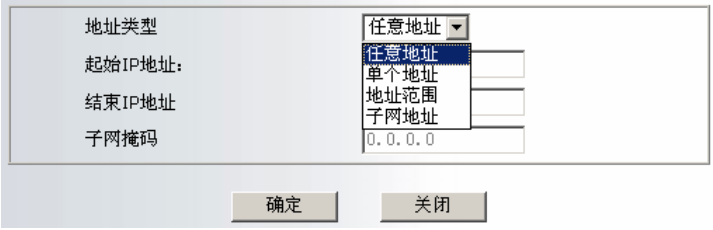
点击**高级**按钮打开相应 QoS 组的高级设定，在如下页面中，可以插入、移动、编辑或删除选中的规则。




点击**添加**打开以下页面添加规则。

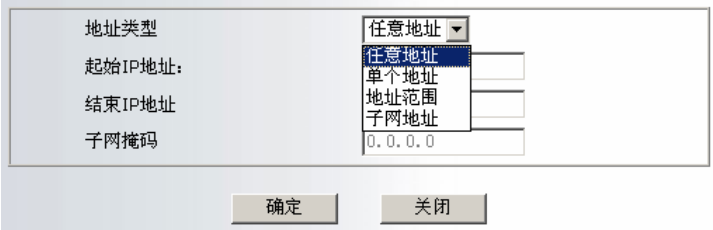



**源地址**　　允许编辑源地址信息




**地址类型** – 决定源地址的地址类型。
**单个地址** – 输入单个 IP 地址到起始 IP 地址栏，其它输入框不可用。
**地址范围** – 输入起始 IP 地址和结束 IP 地址，定义一个地址范围，作为 QoS 的应用对象范围。
**子网地址** – 用子网掩码方式来定义地址范围。

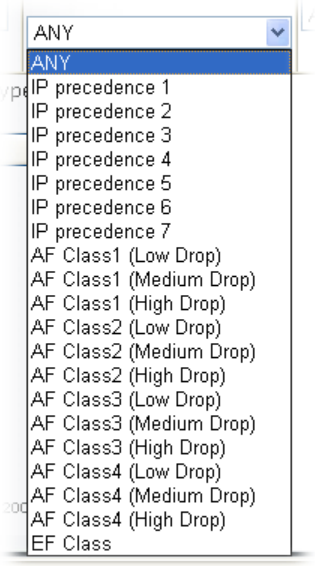
**目标地址**　　允许编辑目标地址信息。




**地址类型** – 决定源地址的地址类型。
**单个地址** – 输入单个 IP 地址到起始 IP 地址栏，其它输入框不可用。
**地址范围** – 输入起始 IP 地址和结束 IP 地址，定义一个地址范围，作为 QoS 的应用对象范围。
**子网地址** – 用子网掩码方式来定义地址范围。

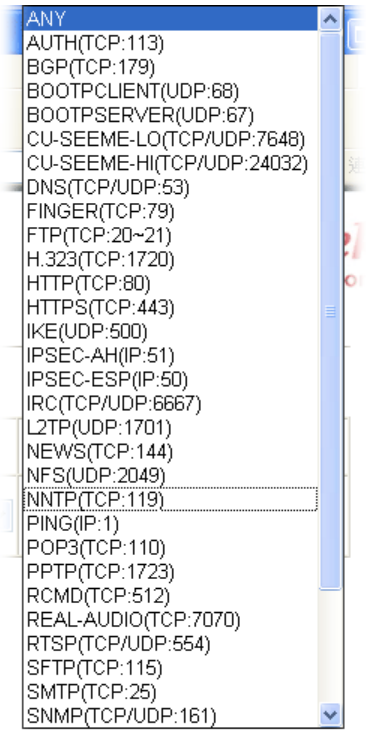
**区分服务编码**

所有的数据包会被系统 QoS 控制功能根据它们的分级类型进行分级处理。

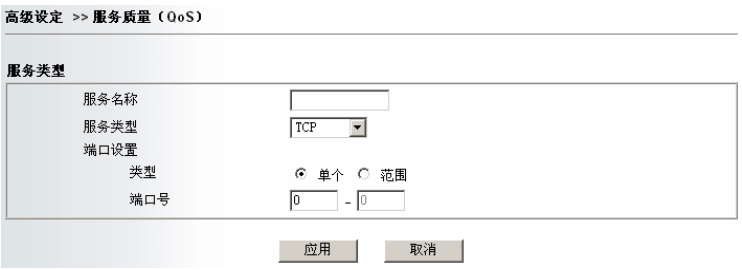



**服务类型**

决定了 QoS 控制处理的服务类型，出厂预设了常用的服务类型，通过选择可以快速设置，对于自定义服务类型，可以自行编辑后加入列表。




通过点击**添加**按钮可以添加新的服务类型，设置页面如下：




**服务名称** – 为要添加的服务输入一个方便辨认的名称。
**服务类型** – 选择类型（TCP，UDP 或 TCP/UDP）
**端口设置类型** – 选单个或一个范围的端口。
**端口号** – 输入起始端口和结束端口（当选择**范围**时）
可以随时根据需要添加新的服务。同时，也可以对自己添加的服务进行**编辑/删除**。

# 3.6 应用程序

## 3.6.1 动态 DNS

通常 ISP 会分配给您一个动态 IP，这意味着每次连接 Internet，您都会获取不同的 IP 地址。动态 DNS 功能可以将域名绑定到您的动态 IP，每次当路由器连接到 Internet，它都会自动更新自己的动态 IP 与域名的绑定。当您使用 Web Server，FTP Server 或其它 Server 时，该功能使客户端的连接更加方便。

在您使用该功能之前，您需要在DDNS服务的提供商那里进行注册，以获取您的动态域名。路由器支持您使用 3 个动态域名，而且路由器支持目前流行的大部分动态域名服务提供商，比如www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic- nameserver.com**以及中国用户常用的**www.ddns.com.cn**和花生壳** www.oray.net 。您可以访问他们的主页进行注册。

**启用该功能并添加一个动态 DNS 帐号。**

1. 首先请确认您已经完成了 DDNS 服务的注册。我们以 hostname.dydns.org 为例，用户名和密码均为 test。

2. 在动态 DNS 设定页面，勾选 **启用动态 DNS 设定**。


3. 选择索引 1 并为路由器添加一个新的 DDNS 帐号。
勾选启用动态 DNS 帐号，选择正确的服务提供商，填写正确的域名，登录名称，以及密码。


**服务提供商** 选择 DDNS 服务的提供商。

**服务类型** **选择服务类型。**(Dynamic, Custom, Static) 分别代表动态，定制，静态

**域名** 填写您注册的动态域名。

**登录名称** 填写登录名称。

**密码** 填写登录密码。

**接口** 选择应用该动态域名服务的 WAN 口连接。

**通配符** 不是所有的 DDNS 服务提供商均提供该服务，具体信息请查询提供商的主页。

**备份 MX** 不是所有的 DDNS 服务提供商均提供该服务，具体信息请查询提供商的主页。

**邮件扩展** 不是所有的 DDNS 服务提供商均提供该服务，具体信息请查询提供商的主页。

4. 点击**确定**按钮完成设置。您可以看到完成设置后的页面。

**禁用此功能并清除所有帐号。**

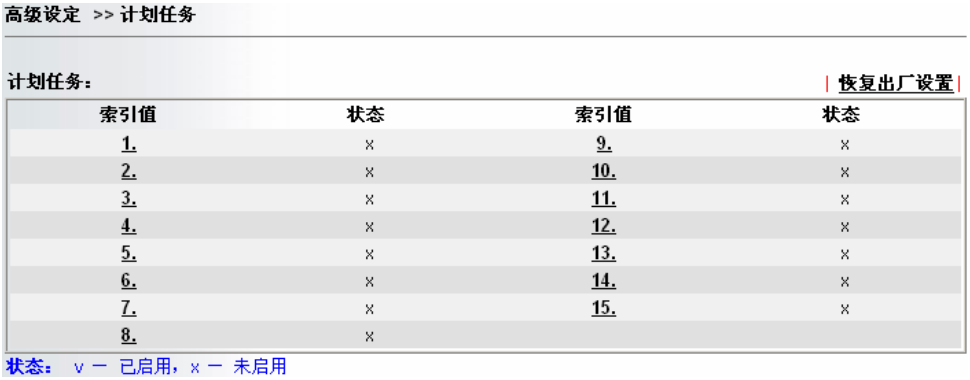
在 DDNS 设置菜单，取消**启用动态 DNS 设定**来禁用此功能。点击**恢复出厂设置**来清除所有帐号。

## 3.6.2 计划任务

Vigor 路由器有一个内置的时钟系统，并可以随时通过手动/自动的方式与 NTP 服务器同步。这样，您不仅可以让路由器在指定的时间内连接 Internet，而且可以控制连接 Internet 的时间长度，比如只有在工作时间才允许路由器连接 Internet。

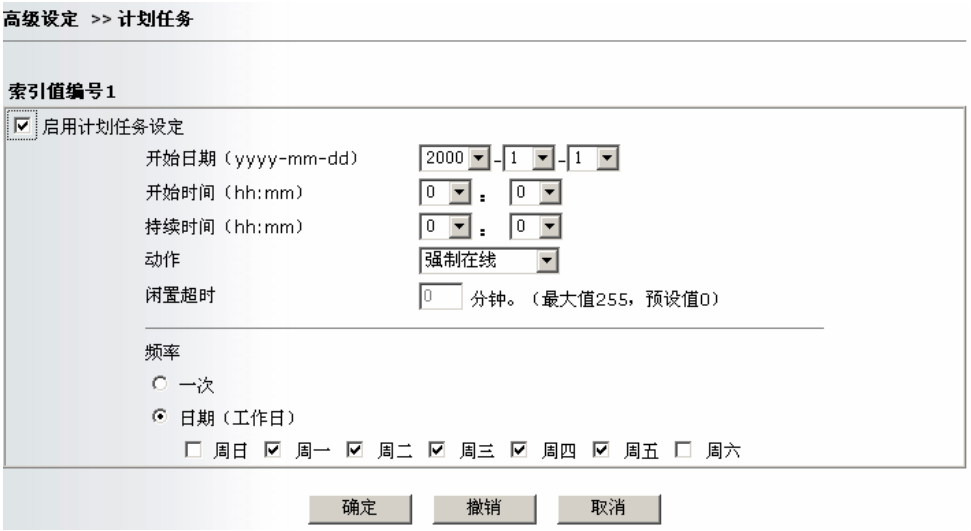
在使用计划任务之前，您必须在**系统维护>> 时间和日期**菜单对时间进行设置。点击**获取时间**按钮来使路由器和您 PC 的时间同步。该时钟会在路由器断电或者重置时恢复出厂值。另外，您可以设置路由器使得路由器的时间与 NTP 服务器同步，此功能只有在路由器连接到 Internet 上时才生效。

在**应用程序**菜单点击**计划任务**打开设置菜单。




您可以设置多达 15 条时间表，然后将他们应用到 Internet 接入等应用。

您可以选择任何一个索引来进行设定，比如说索引 1，进入设置页面，如下图：




**启用计划任务设定**　　启用该时间表。

**开始日期（yyyy-mm-dd）**　　设置启用该时间表的日期。.

**开始时间（hh:mm）**　　设置启用该时间表的具体开始时间。

| | |
|---|---|
| **持续时间 (hh:mm)** | 设置该时间表生效的持续时间。 |
| **动作** | 设置**计划任务**在指定时间段内执行的操作。<br>**强制在线** – **强制建立连接。**<br>**强制离线** – **强制断开连接。**<br>**启用按需拨接** – 设置连接为按需拨接模式，并且在**闲置超时**项中设定闲置超时时间。<br>**禁用按需拨接** – 如果有网络数据流量则保持连接，没有连接时，超过闲置超时时间则断掉连接，并强制路由器处于断线状态。 |
| **闲置超时** | 网络无流量时的连线维持时间，超过此时间则断开网络连接。 |
| **频率** | 指定该计划任务应用的时间。<br>**一次** – 该计划任务仅使用一次。<br>**日期** – 指定一周哪些天执行该计划。 |

**范例：**

架设您想控制路由器的 PPPoE 连接，使得它在在一周内，从早上 9 点到下午 6 点处于一直在线（强制在线）的状态，其它时间断开 Internet 连接（强制离线）。

**办公时间:**

**(强制在线)**

**周一 – 周日　　9:00 am　　到　　6:00 pm**

1. 确定 PPPoE 连接和**时间设定**工作正常。
2. 设置路由器，使得 PPPoE 一周内从早上 9:00 到晚上 6 点一直处于连线状态。
3. 设置路由器，使得每天从晚上 6 点到第二天早上 9 点强制断线。
4. 将这两个时间表应用到PPPoE网络连接。

## 3.6.3 UPnP

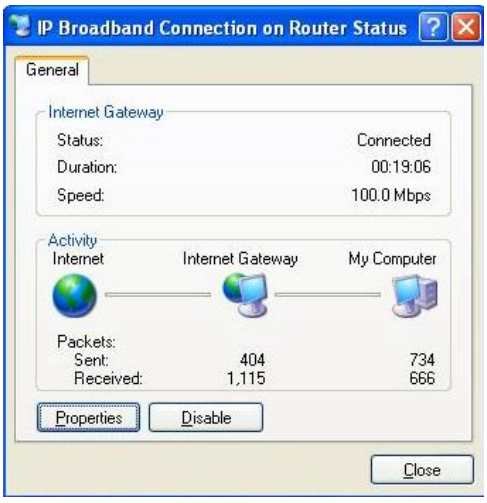
UPnP（通用即插即用协议）可以方便的支持网络连接设备的安装和配置，它已经被广泛的应用于拥有 Windows 即插即用系统的 PC 外围设备。为了解决 NAT 穿透问题，出现了许多技术。比如端口映射和应用级网关等。这些是“透明穿透”，即应用程序不用更改，而在路由层面上动手脚。这类方案虽有这些好处，却有缺点，即需要大量的人工配置才能完成这项工作。为了减少用户的工作量，让配置自动进行，新的解决方案 UPnP 出现了。UPnP 是让网络上任意 2 个设备能够发现对方，并进行通讯的一项技术。通过这项技术，一个希望能跨越 NAT 的应用程序或者设备，能够主动去找到一个同样支持 UPnP 协议的 NAT 路由器，并与之协商，在其帮助下将相应端口映射到自己，从而使外网能够访问到自己。这样的协商工作是程序和设备自行完成的，完全无需用户的参与配置。因而无论该用户使用什么牌子的路由器，什么上网方式，也无论内网中 IP 地址是自动分配还是手动填写，一切都将在幕后自动完成。只有一切配置妥当，程序才能开始运行。

目前，支持 UPnP 的应用有微软的 MSN Messenger 和 Emule 下载软件等。通过 UPnP，MSN messenger 可以进行通畅的语音视频聊天，Emule 也可以获得高 ID 从而高速下载。

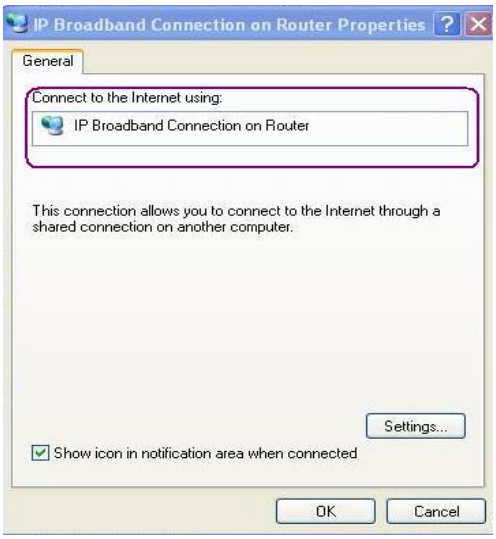

**启用 UPNP 服务**

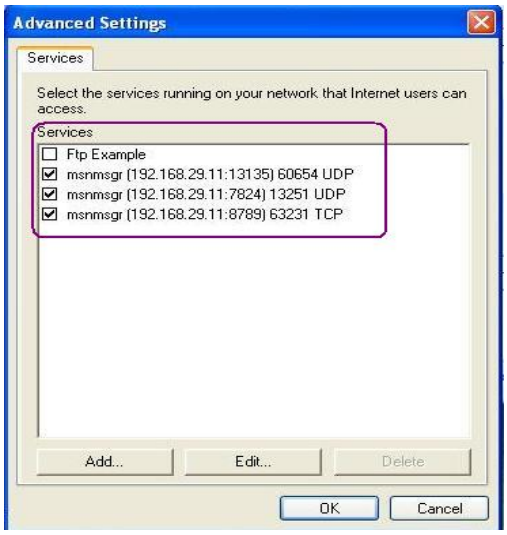
参照上图，您可以选择启用**连线控制服务**或者**连线状态服务**

您可以在路由器的 Web 配置主界面里点击**应用程序->UPnP** 服务设置进入 **UPnP** 设定。选择启用 **UPNP** 服务，这样以来您就打开了连接控制服务或连接状态服务。在 Windows XP 的网络连接里点击“ **路由器**上的 **IP Broadband Connection**”，如下图所示。您能够查看连接状态和控制状态。


路由器的 UPnP 工具可以使那些 UPnP 发现程序（譬如 MSN Messenger）侦测到他们在 NAT 路由器后面，获得外部的 IP 地址，并在路由器上配置端口映像。之后，从外网发往路由器相应端口的数据包会被转发到对应的 UPnP 客户端的应用程序。




UPnP 关于防火墙和 UPNP 的提示：

**PC 上有防火墙软件时 UNnP 可能会失效**

打开 PC 上的防火墙可能导致 UPNP 功能不能正常使用，因为防火墙会关闭某些连接端口

**安全提示**

启用 UPNP 功能会增加 PC 受到的网络威胁，在打开该功能之前，您必需考虑到以下风险：

- 请确定您已经打好最新的补丁来完善您的系统。
- 非法用户可以控制路由器的某些功能，比如添加或者删除端口映射。

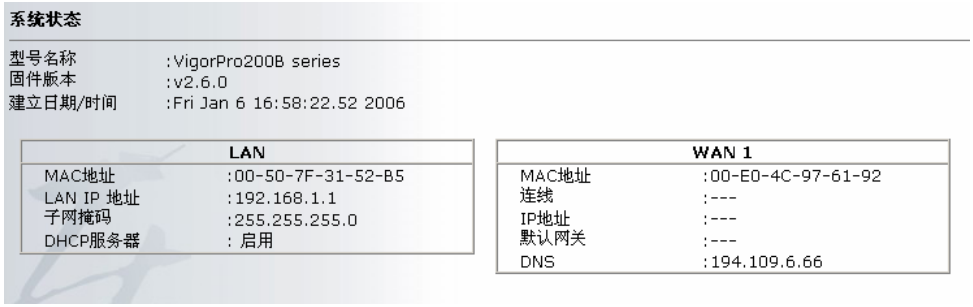
UPnP 为支持 UPnP 的程序动态添加端口映像，当这些程序非正常关闭时，这些映射可能不会被清除。

## 3.7 系统管理

系统管理提供了一些基本和必要的设定，包括：系统状态，管理员密码设定，备份设定，系统日志(Syslog)，时间设定，重启系统，固件升级。

### 3.7.1 系统状态

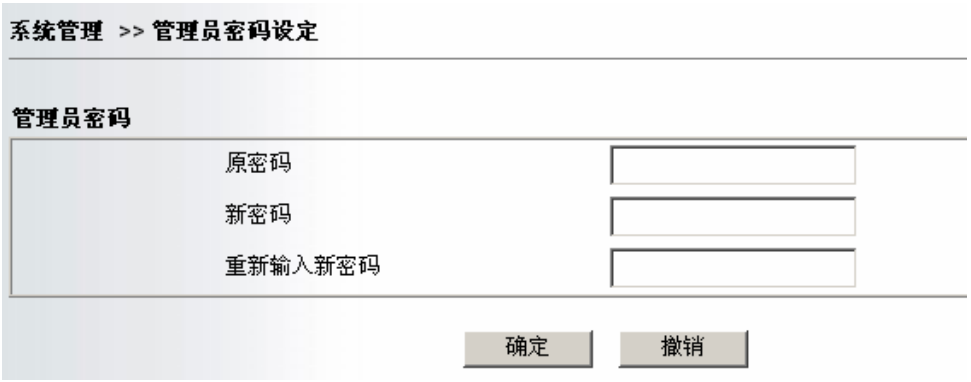
**系统状态**页面提供了 Vigor 路由器的基本网络设定的信息，包括 LAN 和 WAN 接口的信息。同时，您可以在这里查到当前运行的固件的版本或其它相关信息。



| | |
|---|---|
| **型号名称** | 显示路由器的型号名称。 |
| **固件版本** | 显示路由器的固件版本。 |
| **建立日期/时间** | 显示当前固件产生的日期和时间。 |
| *LAN 部分* | |
| **MAC 地址** | 显示 LAN 接口的 MAC 地址。 |
| **LAN IP 地址** | 显示 LAN 接口的 IP 地址。 |
| **子网掩码** | 显示 LAN 接口 IP 地址的子网掩码。 |
| **DHCP 服务器** | 显示 LAN 接口的 DHCP 服务器的当前状态。 |
| *WAN 部分* | |
| **MAC 地址** | 显示 WAN 接口的 MAC 地址。 |
| **连线** | 显示 WAN 连线的模式。 |
| **IP 地址** | 显示 WAN 接口的 IP 地址。 |
| **默认网关** | 显示默认网关的 IP 地址。 |
| **DNS** | 显示主 DNS 的 IP 地址。 |

## 3.7.2 管理员密码设定

在这里您可以更改管理员密码。




| | |
|---|---|
| **原密码** | 输入当前的管理员密码。默认密码为空。 |
| **新密码** | 在该栏输入新的密码。 |
| **重新输入新密码** | 再输入一遍新的密码。 |

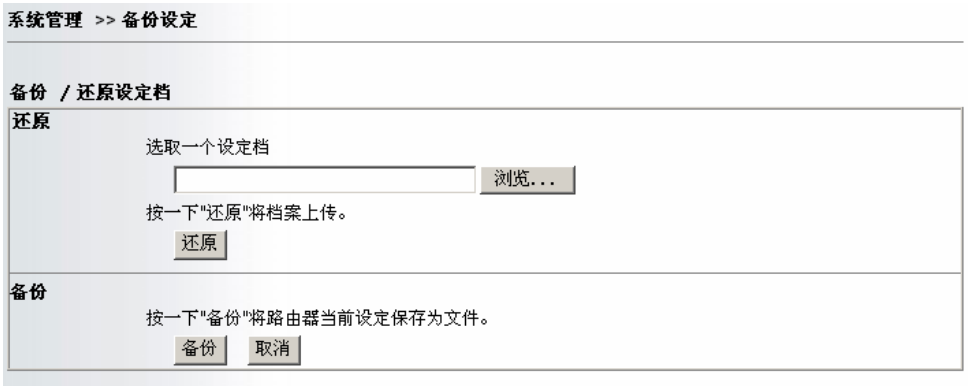
点击确定后，将弹出登录窗口。请使用新的密码重新进入路由器的 web 配置界面。

## 3.7.3 备份设定

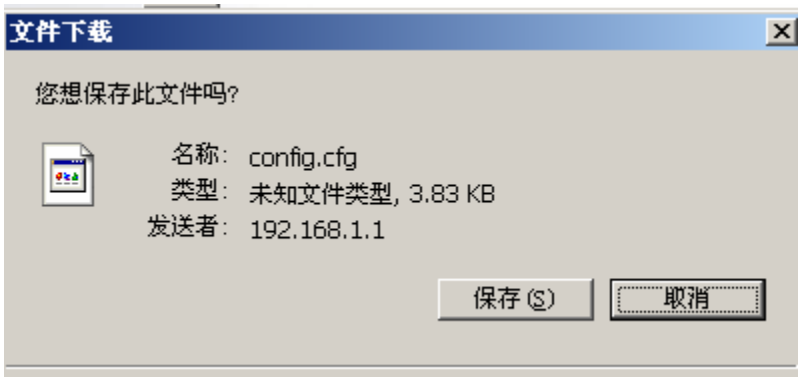
### 备份设定档

请按照以下步骤来备份路由器的设定档。

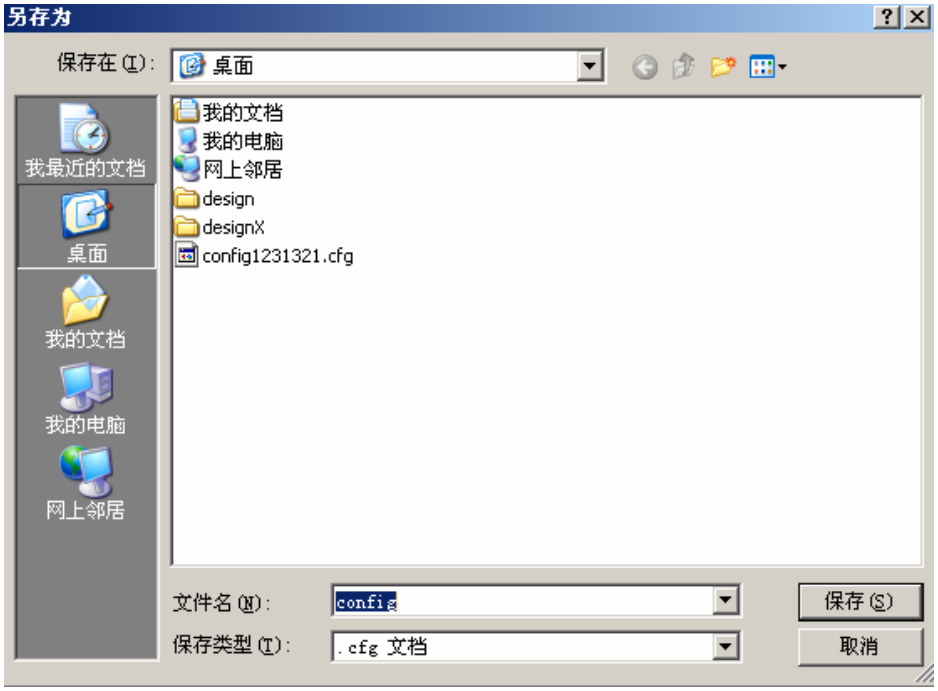
1. 进入**系统管理** >> **备份设定**页面。将显示如下窗口。




2. 点击**备份**按钮，将弹出以下对话框。点击**保存**按钮将打开另一个对话框，可将设定档保存为一个文件。




3. 在另存为对话框里，默认的文件名是 **config.cfg**。您可以给它另取一个名字。

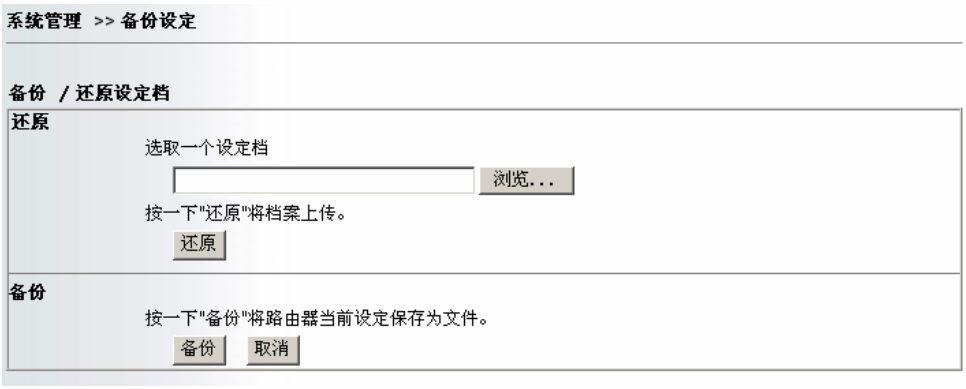



4. 点击**保存**按钮，设定档将自动下载到您的机器上并保存为一个叫 config.cfg 的文件。

以上例子采用 **Windows** 平台示范。**Mac** 或 **Linux** 平台将显示不同的窗口，但是备份功能都是可用的。

### 还原设定档

1. 进入**系统管理** >> **备份设定**页面。将显示如下窗口。

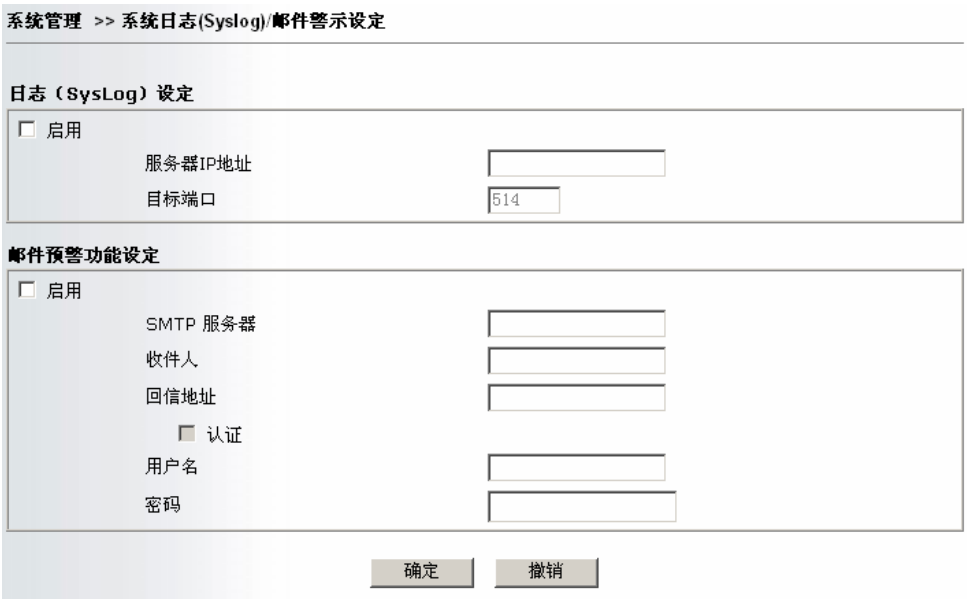



2. 点击**浏览**按钮，选择正确的设定档文件。

3. 点击还原按钮，等待几秒钟。出现如下图片即表明还原操作成功。

## 3.7.4 系统日志(Syslog)/邮件警示

系统日志功能用来监控路由器。通过运行系统日志后台程序来捕捉路由器的所有活动，您以监视路由器的工作状况。这个后台程序可以运行在一台本地主机上或 Internet 上的一台远程主机上。另外，Vigor 路由器还提供了邮件警示工具，可以将系统日志打包以电子邮件的形式发送给需要接收这些信息的人。



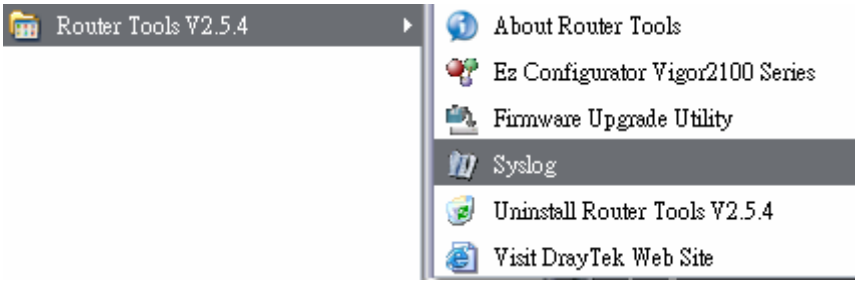

| | |
|---|---|
| **启用** | 勾选**启用**框启动 Syslog 服务。 |
| **服务器 IP 地址** | 指定用于接收 Syslog 信息的主机的 IP 地址。 |
| **目标端口** | 指定 Syslog 服务器监听的 UDP 端口。默认端口为 514。 |
| **SMTP 服务器** | 指定发送邮件的 SMTP 服务器的 IP 地址。 |
| **收件人** | 指定接收者的电子邮件地址，用于接收系统日志信息。 |
| **回信地址** | 指定另一个电子邮件地址，在收件人的邮箱出现问题时，用于接收返回的信息。 |

**认证** 如果用该 SMTP 服务器发送邮件需要认证，请勾选认证框。
**用户名** - 输入用于认证的用户名。
**密码** - 输入用于认证的密码。

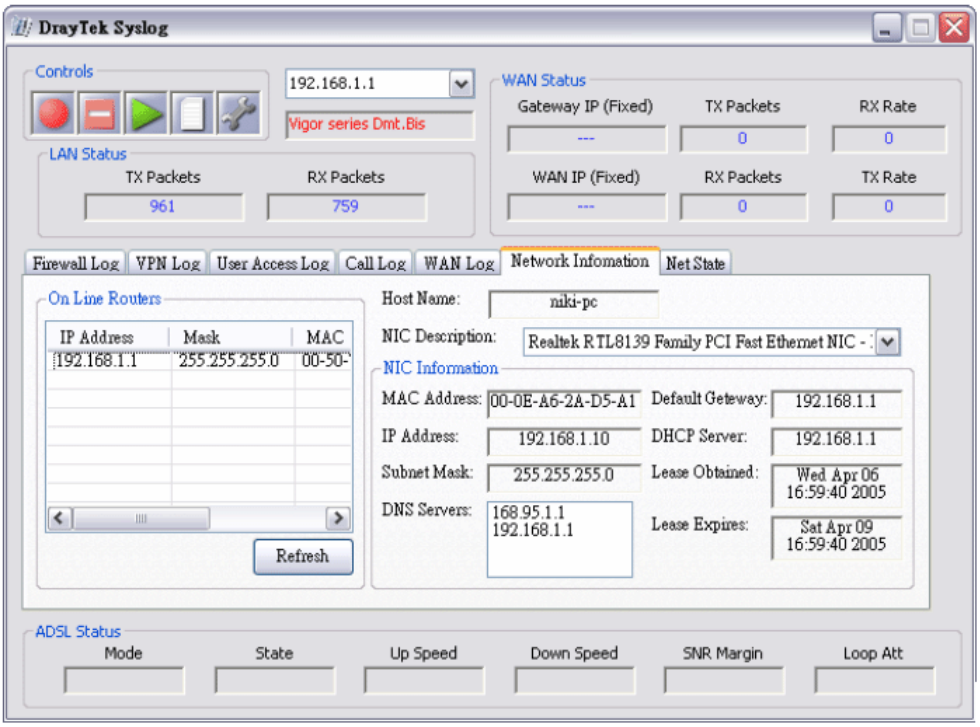
点击**确定**保存设定。

要查看系统日志，请按照以下步骤：

1. 在服务器 IP 地址栏里输入用于监控的 PC 的 IP 地址。
2. 在提供的光盘里找到 **Utility** 文件夹，安装里面的 Router Tools。安装好后，在程序菜单里点击 **Router Tools>>Syslog** 。

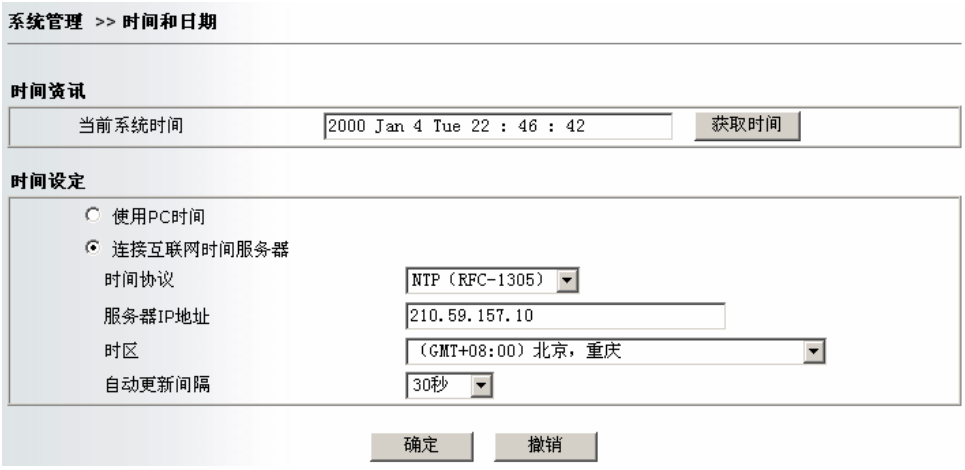



3. 打开 Syslog 工具后，选择您想要监控的路由器的 IP 地址。如果接收不到系统日志，请确保在 IP 地址栏里（图中的 192.168.1.1）选择了正确的网卡（连接路由器的网卡）。




## 3.7.5 时间和日期

在这个页面您可以设定路由器的系统时间。路由器有两种设定时间的方法:其一是使用基于 HTTP 协议的本地电脑时间;另一种方法是基于网络时间协议通过时间服务器来获取时间。如果您想使用任何基于时间的功能（比如说，拨号计划任务设定、URL 内容过滤器等）那么系统的时间必须设置正确。




**当前系统时间** 点击**获取时间**来获得当前的时间和日期。

**使用 PC 时间** 选择该选项将从当前管理员的 PC 上获取系统时间。

**使用互联网时间服务器** 选择该选项将使用指定的协议从 Internet 上的一台时间服务器获取系统时间。

**时间协议** 选择一个时间协议。

**服务器 IP 地址** 输入时间服务器的 IP 地址。

**时区** 选择路由器所在地区的时区。

**自动更新间隔** 选择从时间服务器更新时间的间隔。

点击**确定**保存设定。

## 3.7.6 管理设定

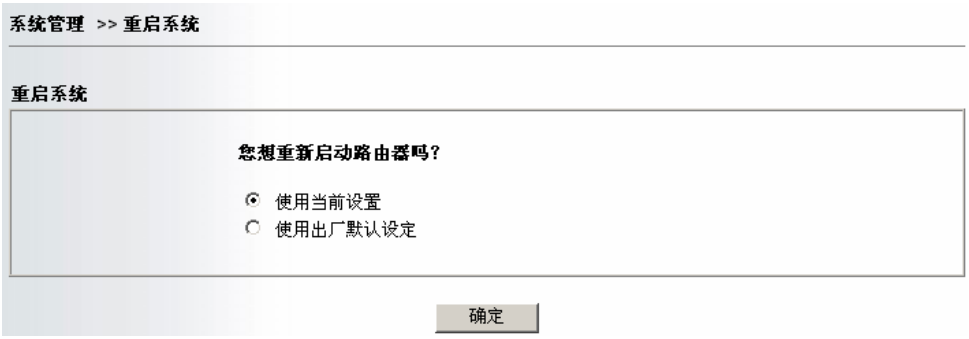
它提供了一些基本的管理条目，包括接入列表，端口设定，SNMP 设定等等。

| | |
|---|---|
| **启用远端固件升级** | 勾选该功能可允许从 Internet 通过 FTP 远程升级固件。 |
| **允许从 Internet 进行管理** | 勾选该功能可允许系统管理员从 Internet 上远程登录路由器。此功能默认是关闭的。 |
| **禁止来自 Internet 的 Ping** | 勾选该功能可以防止别人利用 ping 命令来探测您是否在线。此功能默认是打开的。 |
| **接入列表** | 您可以指定哪些特定的主机或网段可以从 Internet 远程访问您的路由器。最多可以设置三条记录。<br>**列表 IP** – 设定哪些 IP 地址的主机可以访问路由器。<br>**子网掩码** –设定在哪些子网中的主机可以访问路由器 |
| **默认端口** | 路由器出厂时预先设好的通讯端口。 |
| **用户自定义通讯端口** | 为路由器内建的管理服务器设置用户自定义的端口。 |
| **启用 SNMP 代理程序** | 勾选此框可以开启路由器内建的 SNMP 代理程序。 |
| Get Community | 为 SNMP GET 命令的管理 community 指定一个字符串。默认是 **public.** |
| Set Community | 为 SNMP SET 命令的管理 communtiy 指定一个字符串。默认是 **private.** |
| **管理员主机 IP** | 指定 SNMP 管理主机的 IP 地址。 |
| Trap Community | 为 SNMP TRAP 的管理 communtiy 指定一个字符串。默认是 **public.** |
| **通知主机 IP** | 指定一个 IP 地址用于接收 TRAP 通告。 |
| **Trap 超时** | 默认设定是 10 秒。 |

点击**确定**保存设定，点击**撤销**放弃当前更改。

## 3.7.7 重启系统

在这个页面里您可以重新启动您的路由器。在主设置面里点击**重启系统**就会打开如下页面：




有两种重启方式：**使用当前设置**重启和**使用出厂默认设定**重启。如果您想要路由器重启后保存当前设置，就选择第一项并点击**确定**重启。如果您想要路由器重启后恢复到出厂时的默认设置，就选择第二项重启。注：路由器重启需要 5 秒。

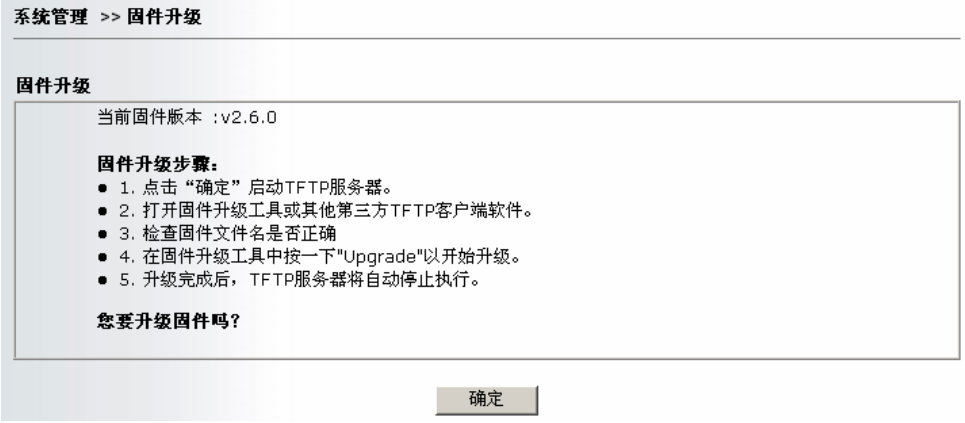
## 3.7.8 固件升级

在升级您的路由器的固件之前，您需要安装一个路由器工具-- Router Tools。固件升级工具(**Firmware Upgrade Utility**)就包含在这个工具包里。下面我们将为您举例说明如何升级您路由器的固件。

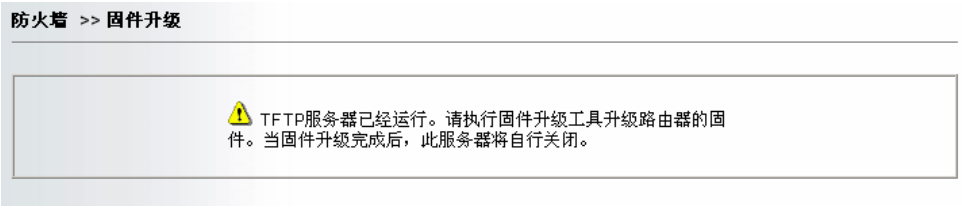
注：这个例子是运行在 Windows 操作系统之上的。

1. 从 DrayTek 网站或 FTP 站点下载最新的固件文件。DrayTek 的网址是 www.draytek.com，（或者在您当地的 DrayTek 代理商的站点也可以下载）。FTP 的地址是 ftp.draytek.com。

2. 点击 开始 > 程序 > Router Tools > Firmware Upgrade Utility 打开固件升级工具。




进入**系统管理 >> 固件升级** 页面，点击确定按钮。将出现以下界面。



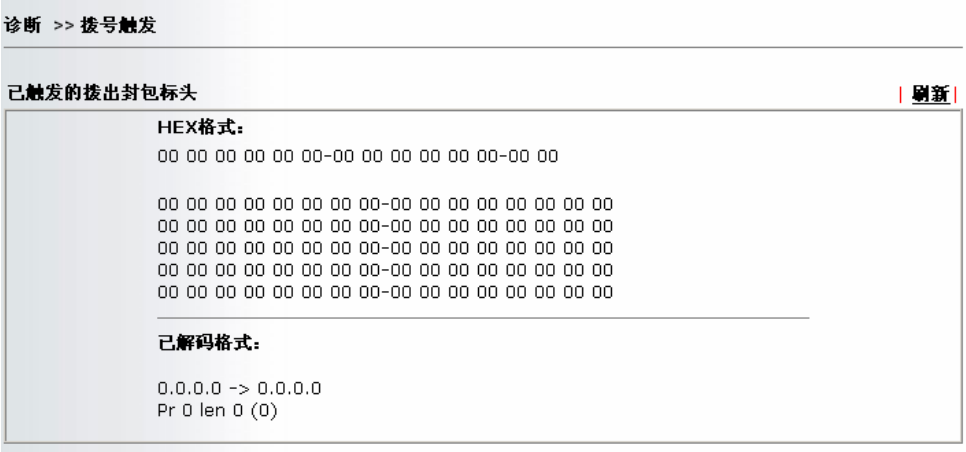

关于升级的具体步骤，请参考第四章。

## 3.8 诊断

使用诊断工具可以观察或诊断您的路由器的运行状态。点击**系统管理>诊断**，就会出现如下所示的画面，接下来我们将对每个工具如何设定做详细的介绍。

### 3.8.1 拨号触发

点击**诊断 >> 拨号触发** 打开如下页面。



**刷新**　　点此按钮刷新页面

## 3.8.2 查看路由表

点击**查看路由表**可以查看路由器的路由表。

这张路由表提供了当前路由器的 IP 路由信息。在这张表的左边是一个关键字，根据关键字的不同，含义也有所不同，如下如示：

C ---直接连接的网络

S ---静态路由

R ---RIP 路由

* ---默认路由

~ ---私网路由域的路由

右侧显示的是端口标识，如下所示：

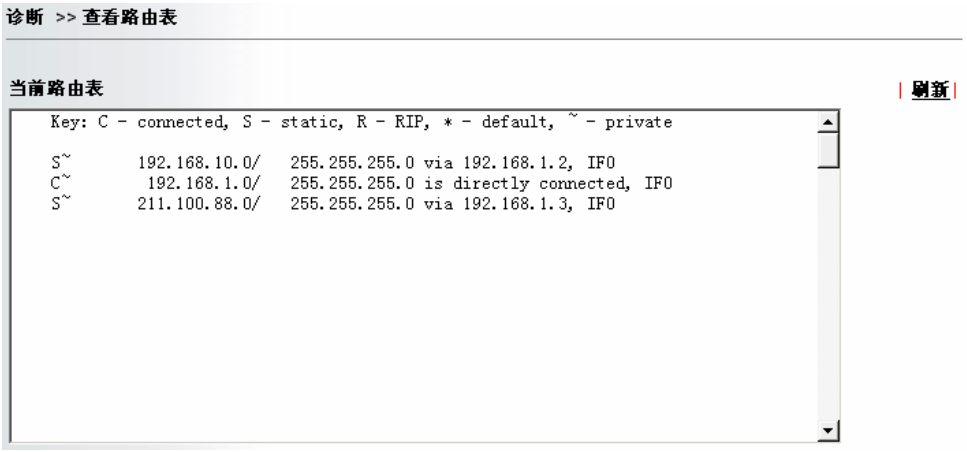
IF0 --- 本地 LAN 口

IF1 --- ISDN B1 通道

IF2 --- ISDN B2 通道

IF3 --- 本地 WAN 口

IFx（x＝4,5,6…..）---VPN 通道。




**刷新**　　点此按钮刷新页面。

## 3.8.3 查看 ARP 缓存表

点击**查看 ARP 缓存表**就可以看到保存在路由器中的 ARP（地址解析协议）缓存里的信息。这张表显示了以太网硬件地址（即 MAC 地址）和 IP 地址之间的映像。

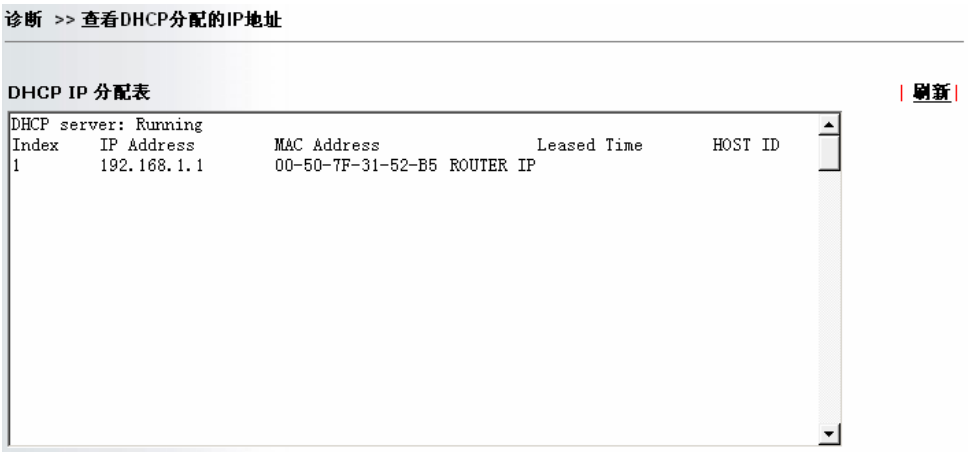

**刷新** 点此按钮刷新页面。

**清除** 点此按钮清除所有记录。

## 3.8.4 查看 DHCP 分配的 IP 地址

使用查看 DHCP 分配的 IP 地址工具可以查看 IP 地址分配情况。这个信息对诊断网络问题，如 IP 地址冲突问题很有帮助。

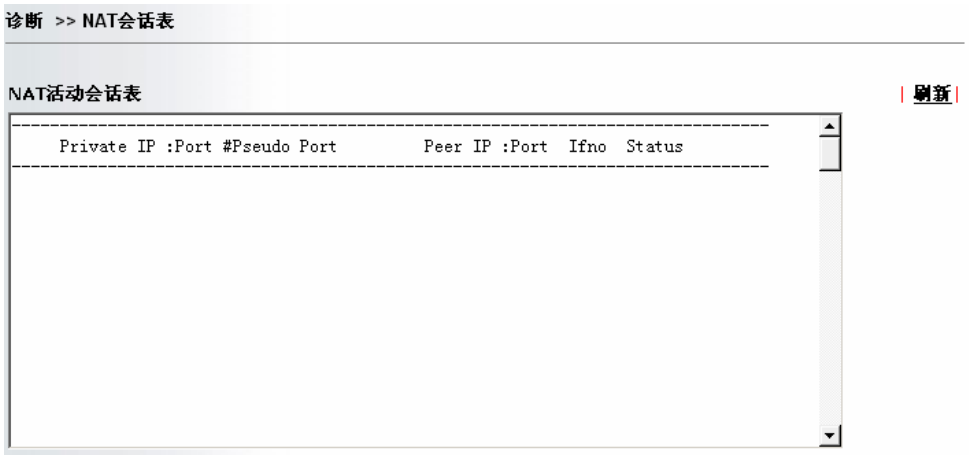
点击**诊断 >> DHCP 表** 打开如下页面。




**刷新** 点此按钮刷新页面。

## 3.8.5 NAT 会话表

当路由器通过 NAT 上网时，点击查看当前 NAT 线程表就可以看到当前出去的线程。




**刷新** 点此按钮刷新页面。

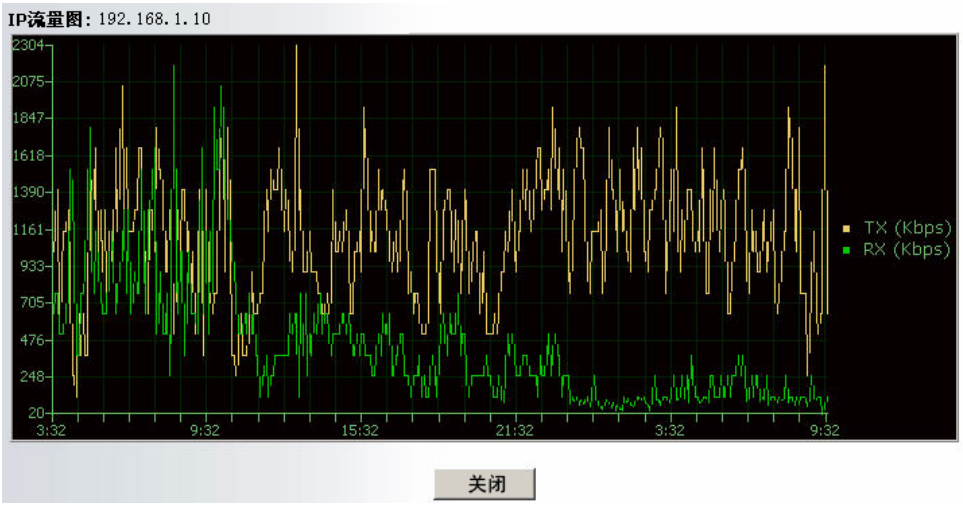
## 3.8.6 流量监控

启用流量监控时，可以及时监控每个 IP 当前的上行/下行流量，以及使用 NAT 会话的情况。该数据可以对管理员设置带宽管理/会话管理提供参考。如果发现有 PC 使用了异常大小的带宽，管理员就可以及时进行调整。

管理员也可以通过点击“封锁”，停止该 IP 接入网络 5 分钟。


**启用流量监控** 选中此选项即可启用流量监控。当带宽和会话管理都处于打开状态时，流量监控会自动启用。

点击列表中的 IP 地址，可以弹出该地址 30 小时内的流量图。如下图：

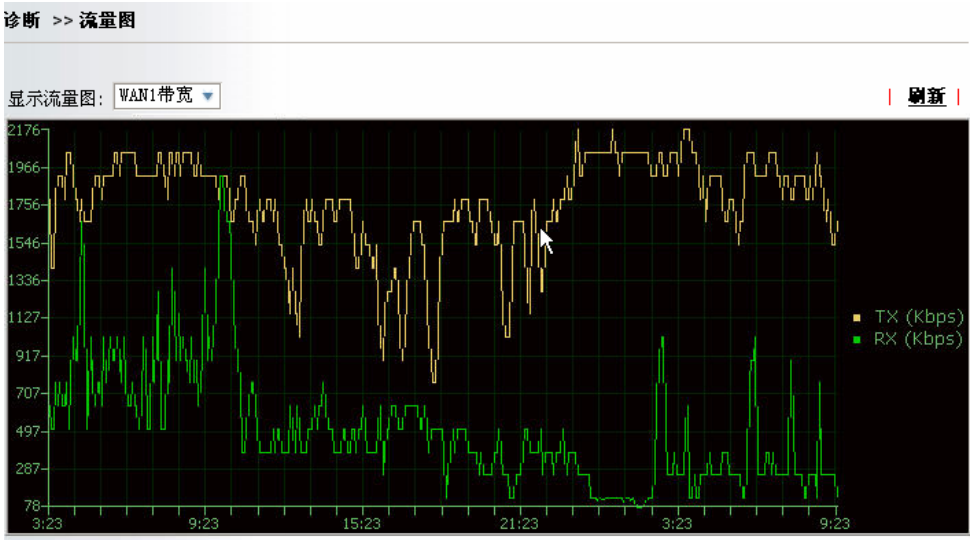



当启用带宽/会话管理时，每个 IP 的 TX/RX/会话都会显示两个值，一个是当前值，一个是限制值，如下图所示：


诊断 >> 流量监控
启用流量监控
排序方式: IP
刷新间隔秒数: 5
页: 1
刷新
索引 IP地址 上行速率（Kbps） 下行速率（Kbps） 会话 动作
1 192.168.1.10 5 / 200 69 / 800 2 / 100 封锁
注意:
1. 点击“封锁”可以停止指定PC上网5分钟。
2. 被屏蔽上网的IP显示为红色，会话数会显示该IP被屏蔽的剩余时间。

## 3.8.7 流量图

流量图可以用来观察 WAN1，WAN2 以及路由器会话的使用情况，路由器记录 30 小时内的数据，并进行统计绘图。通过下拉框，可选择 WAN1，WAN2 以及会话，来查看 30 小时内路由器带宽和会话的使用情况。

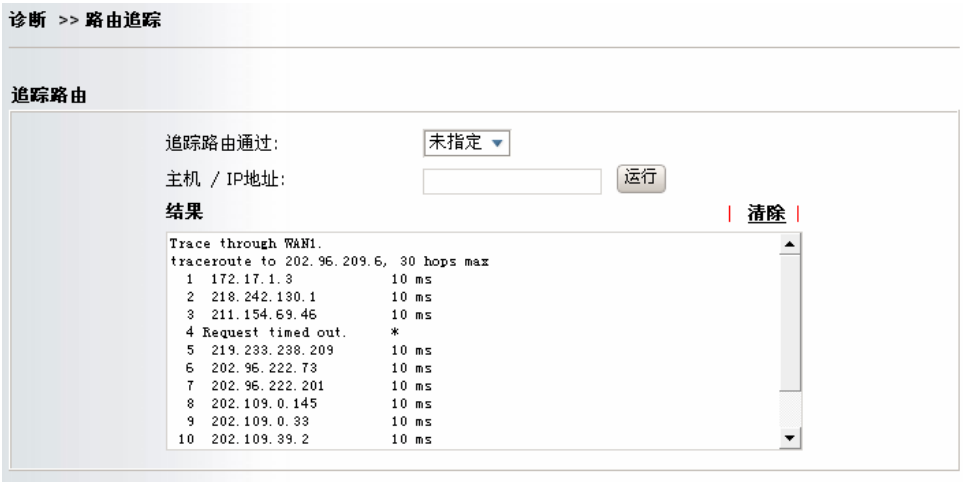


## 3.8.8 PING 诊断

PING 诊断用 PING 来检测网络的连通情况。

## 3.8.9 路由追踪（Tracert）

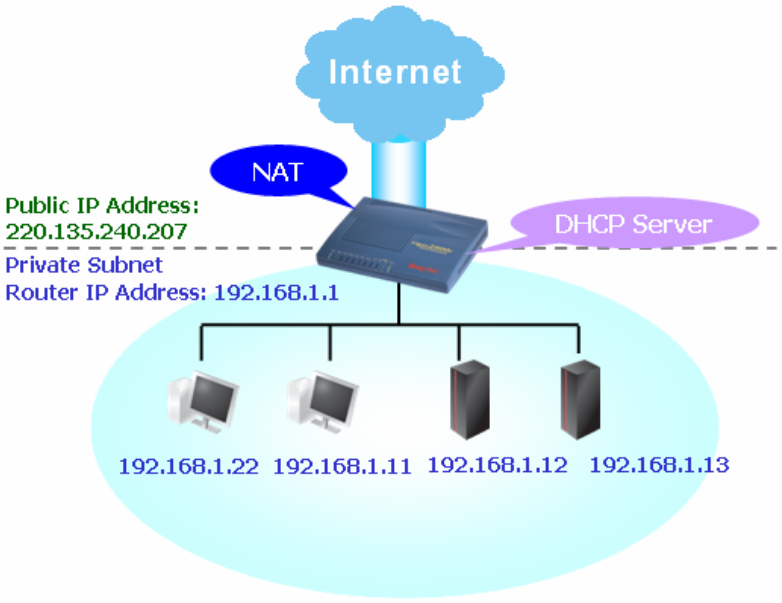
路由追踪和 PC 上的 tracert 命令功能类似，通过追踪本地到一个目标 IP 所经过的全部路由来检查路由情况，协助分析问题。



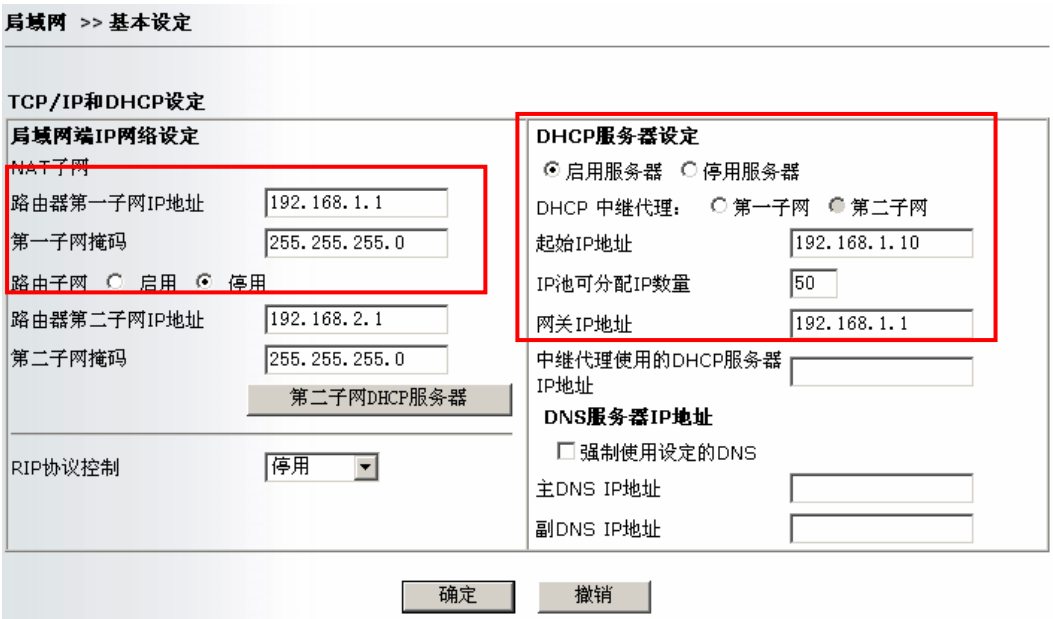
# 4 应用与范例

## 4.1 局域网架设 - 基于 NAT 功能

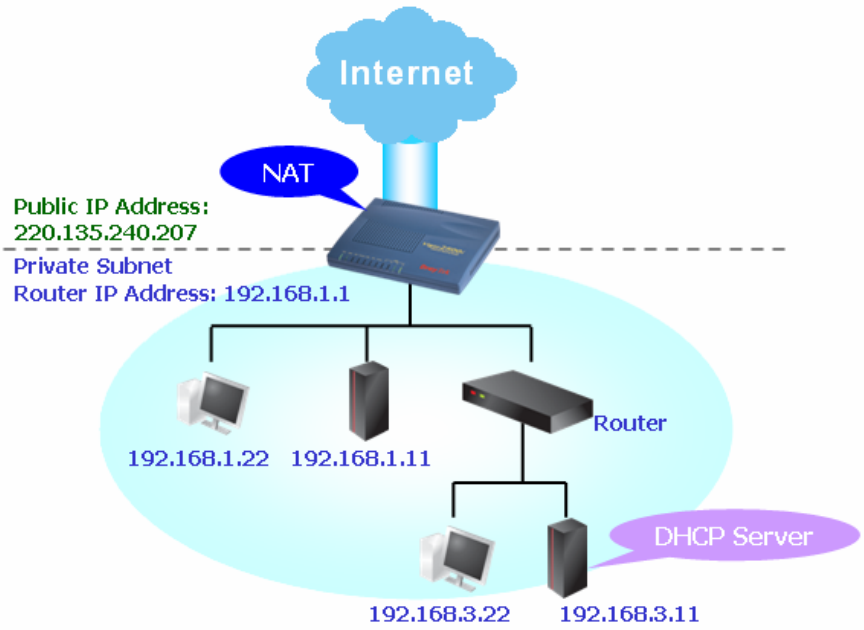
下面给出一个包含具体设置和部署的范例。Vigor 路由器的默认 IP 地址/子网掩码是 192.168.1.1/255.255.255.0。内置的 DHCP 服务器默认开启，因此它会给每一个本地的被 NAT 服务的主机都分配一个从 192.168.1.10 开始的同网段 IP（192.168.1.*）。



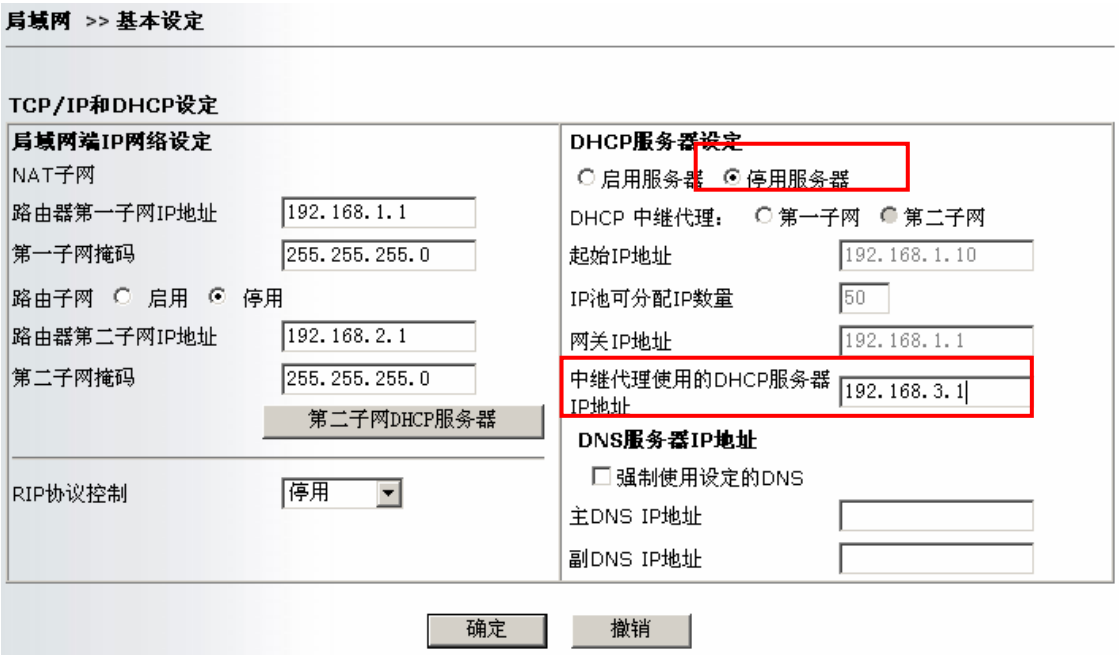

您只需对下面红框中的内容进行配置即可。



若网络内有其它的 DHCP 服务器，并且您不希望使用 Vigor 路由器内置的 DHCP 服务器，那您需要参照下面的网络部署。




然后按照下面红框中的内容进行设置，以满足需要。



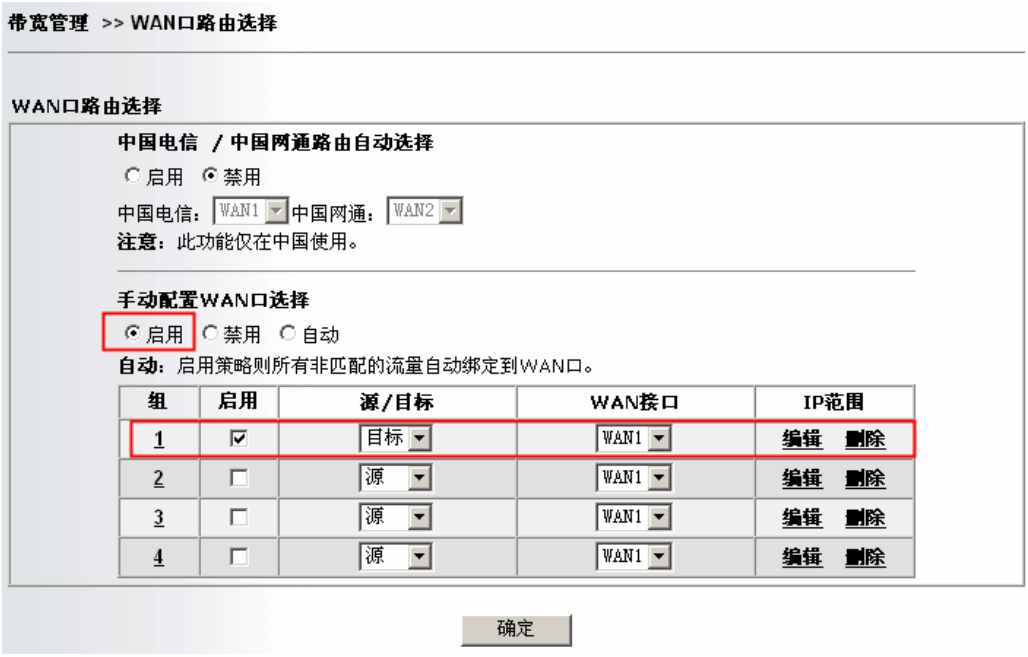

## 4.2 流量规划 － 手动配置 WAN 口选择

对于一些特殊的需要，用户需要对指定的 LAN PC 或者指定的目标地址使用特定的 WAN 口，对于这种应用，可以通过 WAN 口选择的手动配置来实现。

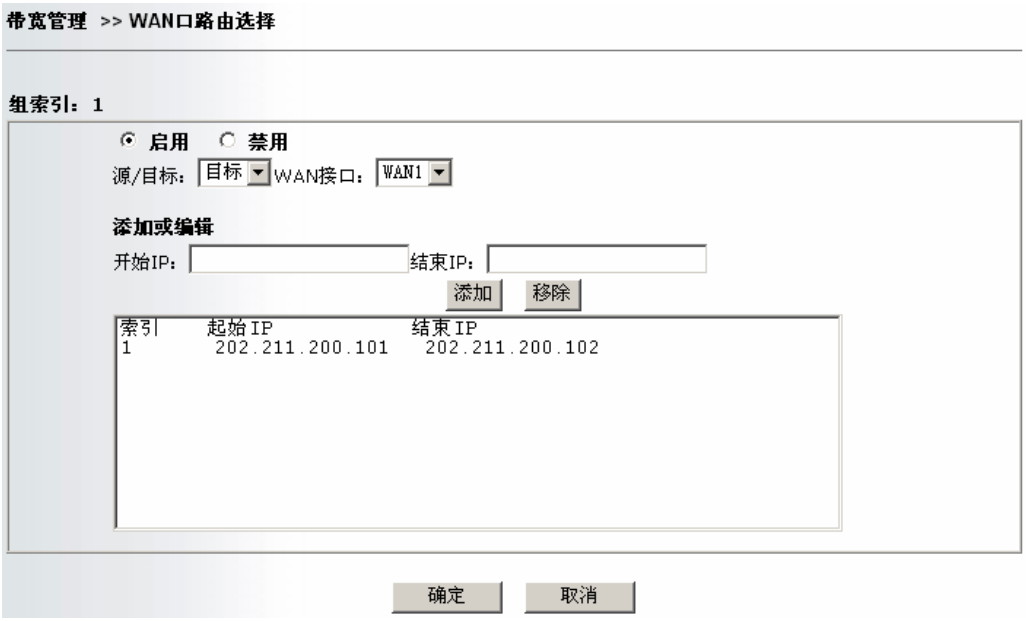
**例 1**：网吧申请了电信，网通各一条线路，电信网通各有一个 VOD 在线视频点播服务器，规定电信 VOD 服务器只能由电信线路访问，网通 VOD 只能由网通线路访问。如果这两个服务器的地址都不在我们默认数据库内的话，流量就会随机走 WAN1/WAN2，这样一来，就有可能会出现使用电信线路访问网通 VOD 的情况，自然结果就是无法访问。

通过手动配置规则可以避免这种情况。

首先，将规则定义为**启用**，同时选择**目标**地址作为组规则的作用对象，WAN 接口选择一个 WAN 口。

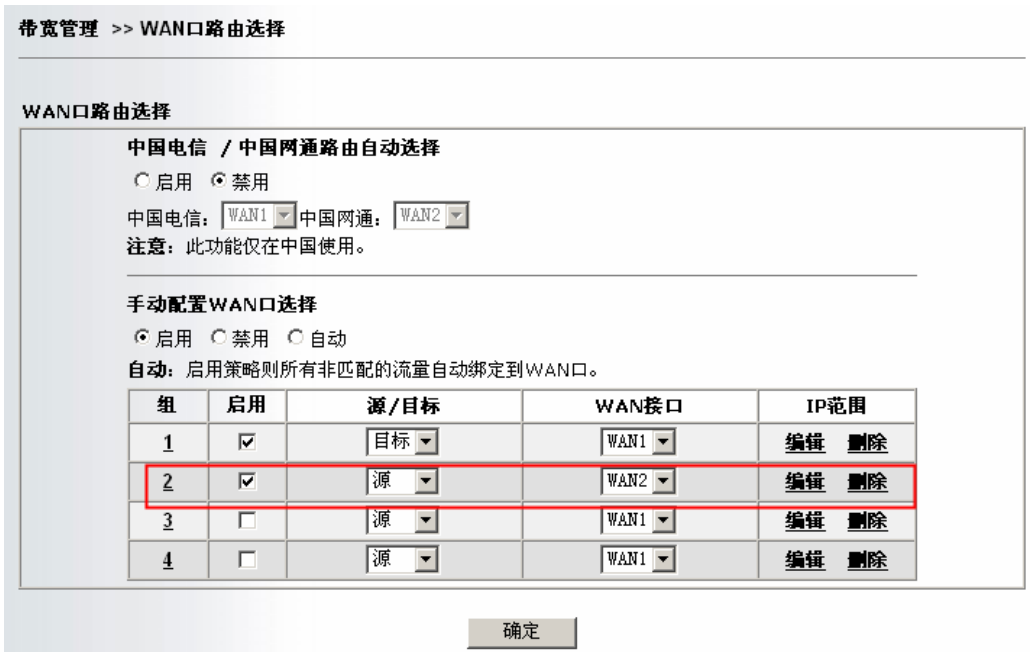


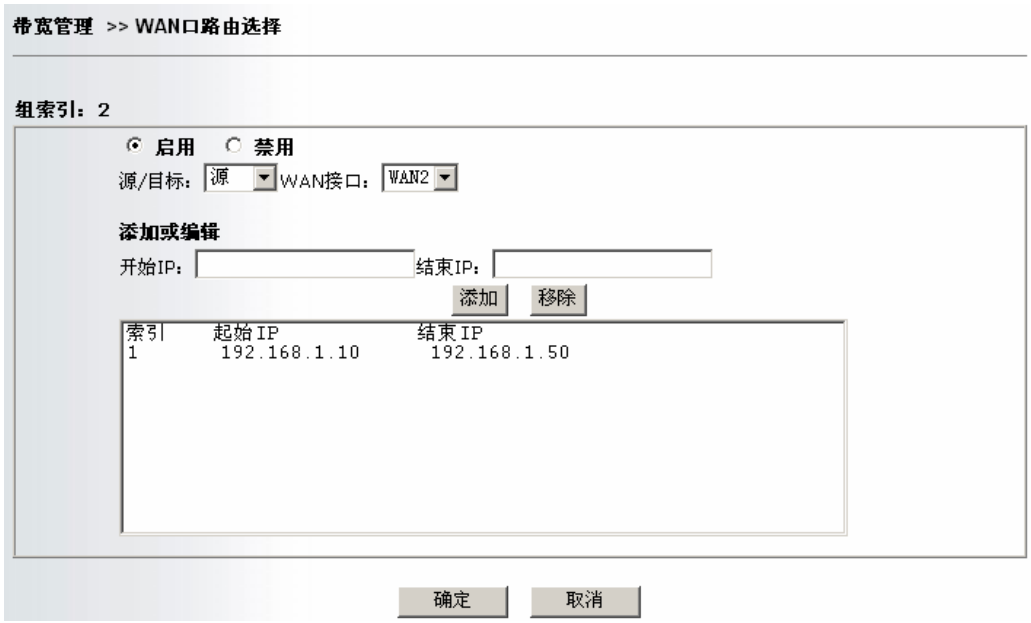

点击**编辑**，进入组规则编辑窗口，进行如下设置，并点击**确定**，则所有发往 202.211.200.101-102 的数据都从 WAN1 出去。




**例 2**：公司内部网络规划，希望销售部门上网 PC（192.168.1.10-192.168.1.50）从 WAN2 出去，也可以利用配置路由策略组的功能来实现。

进行如下图的配置即可：



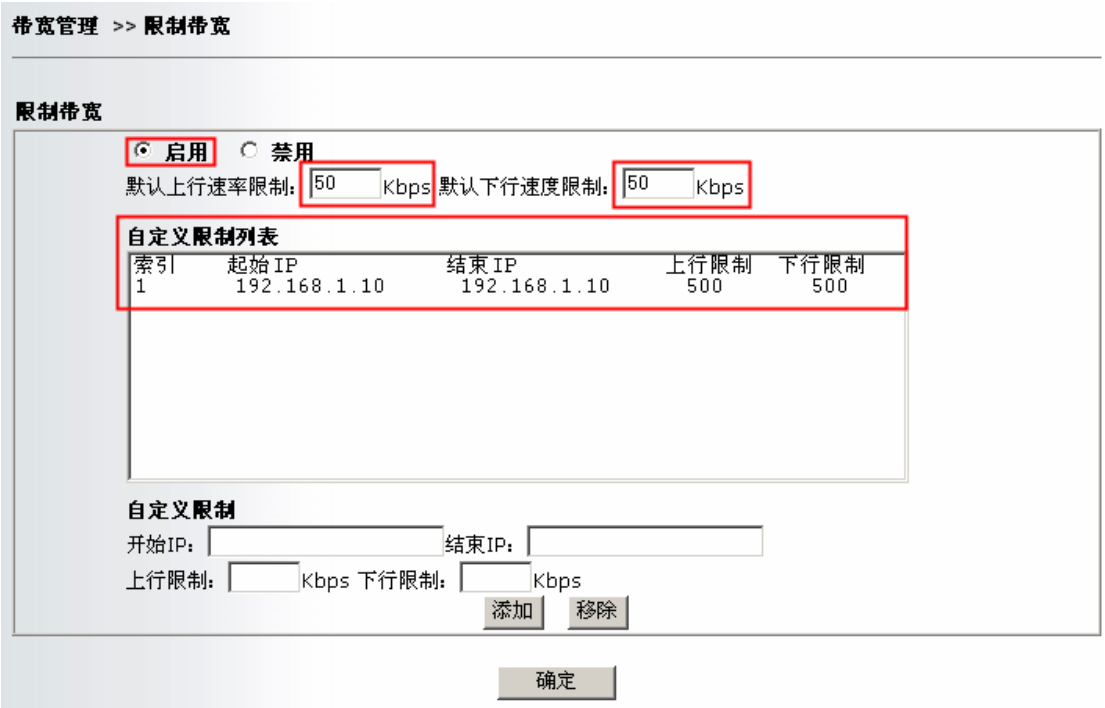




## 4.3 带宽管理——配置规划网内客户机带宽

限制带宽功能可以帮助管理员规划网内客户机带宽。

例如，管理员希望网内所有 PC 默认都只能各使用 50Kbps 的上下行带宽，避免部分员工使用高速下载工具占用绝大多数的网络资源。而对于内部特定的向外开放的 WEB 服务器由于有很多外部用户要访问，50Kbps 的带宽显然是不够用的，所以需要支持更多的带宽。因此可以使用默认限制和例外限制相结合的方式，单独设定 WEB 服务器使用 500Kbps 的上下行带宽。

配置如下图的设置（假设 web 服务器的私网 IP 是 192.168.1.10）即可达成目标。

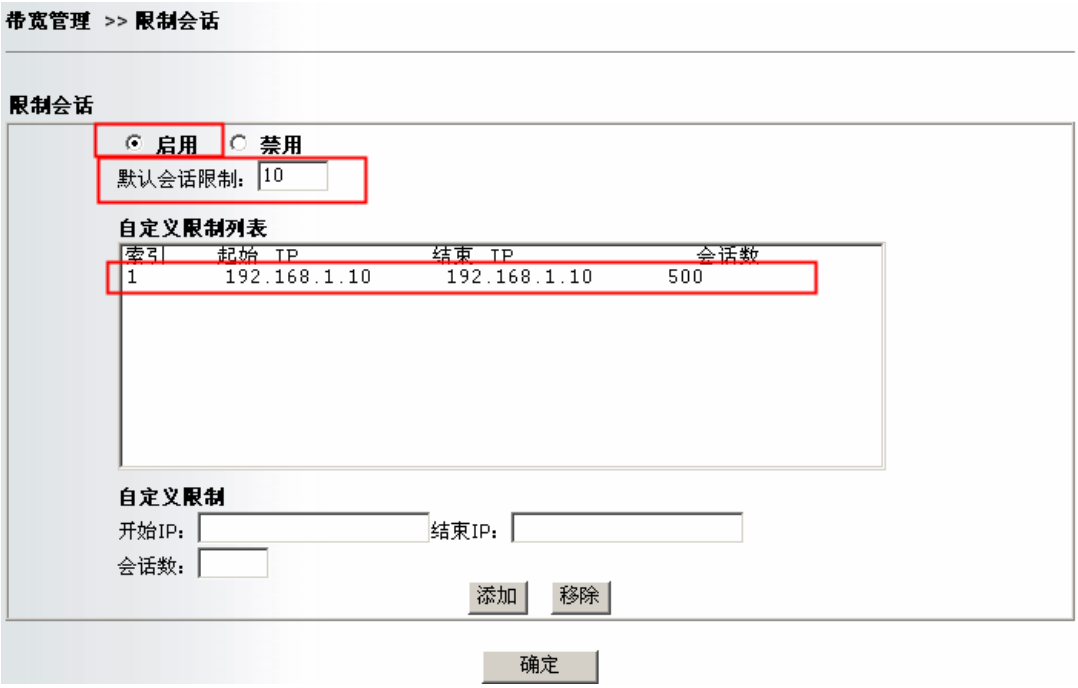



经过如上设置，192.168.1.10 可以使用 500Kbps 的带宽，而其它机器只能支持 50K 带宽。

## 4.4 会话管理－－配置规划网内客户机会话使用

P2P 的使用，病毒的泛滥都会占用大量的会话，会话限制功能可以对每台 PC 使用的会话数进行限制，从而避免会话的滥用造成系统资源的浪费，影响其他正常应用的会话。

例如，管理员希望网内所有 PC 默认都只能各使用 10 个会话，对于 WEB 服务器由于有很多外部用户要访问，所以需要支持更多的会话，因此可以单独设定 WEB 服务器使用 500 条会话，可以做如下设置（假设 web 服务器的私网 IP 是 192.168.1.10）




以上设置就可以达成管理员管理会话的目标。

## 4.5 Web 内容过滤－－分类屏蔽网站

根据网站分类来屏蔽不希望访问的网站是一个很好的做法，对于企业来说，有些不必要的网络访问会造成工作的低效，对于父母来说，不让儿童访问色情网站也是非常重要的功能。

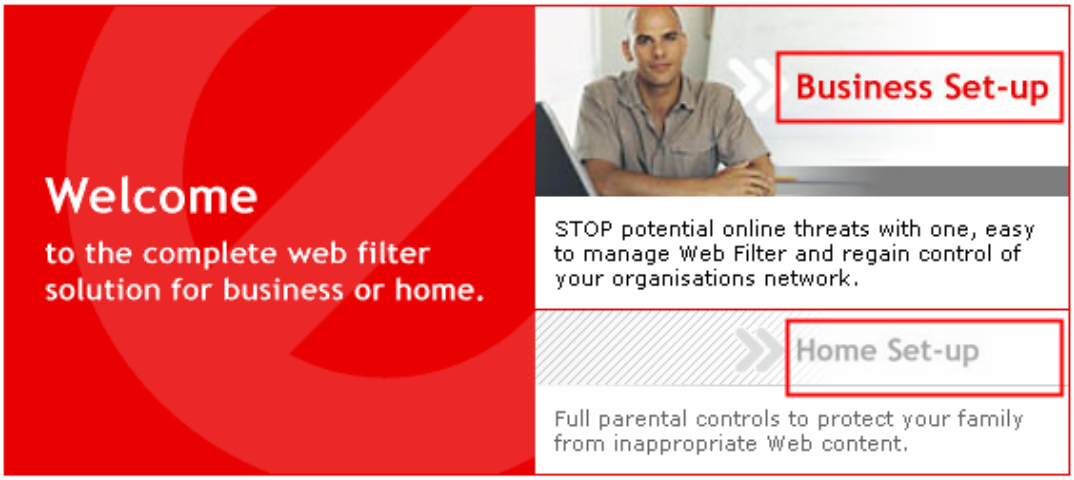
但是，直接封 80 端口的方法在大多数情况下是不可行的，因为一般来说，很少有人希望直接屏蔽掉全部网站的访问。直接封目标网站的 IP 也同样不可行，以新闻网站为例，大的新闻站往往有多个 IP 地址，而互联网上新闻站点也非常多，如果全部设置 IP 规则来屏蔽，肯定是不可能的。而如果使用了此功能，只需要封锁新闻网站这个分类，那么成千上万的新闻网站就都不能访问了，有效的解决了很多网络管理人员面对的难题。

**范例：**

公司网络系统，希望上班时间员工不能访问新闻网站，游戏网站。根据要求，首先要启用此功能，步骤如下：

1. 在**防火墙**菜单点击 **WEB 内容过滤**，打开配置页面，并点击**激活免费使用和购买申请。**


2.会有一个新窗口弹出，访问到第三方 SurfControl 服务的网站，根据需要点击 Business Set-up（商务应用）或 Home Set-up（家庭应用）

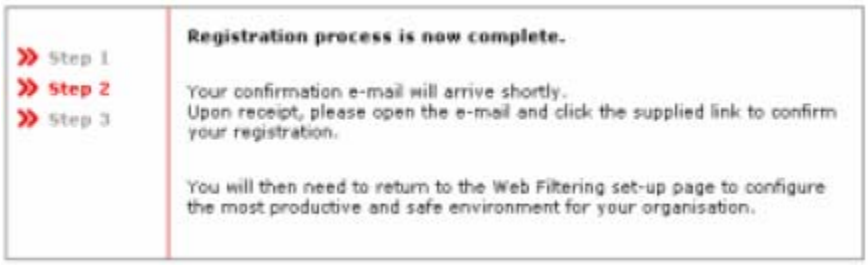



3. 填写如图所示的信息

| | |
|---|---|
| Frist Name： | 名 |
| Last Name： | 姓 |
| E-mail address： | 电子邮件地址 |
| Confirm E-mail address： | 重复确认邮件地址 |

选中 I have read and accepted the Term & Conditions below（**我已经阅读并接受下列条款**），点击 Activate Free Trial(**激活免费试用**)进入下一页面。


4. 注册步骤完成，出现如下页面，服务商的确认邮件会发送到前一步填写的邮箱中。

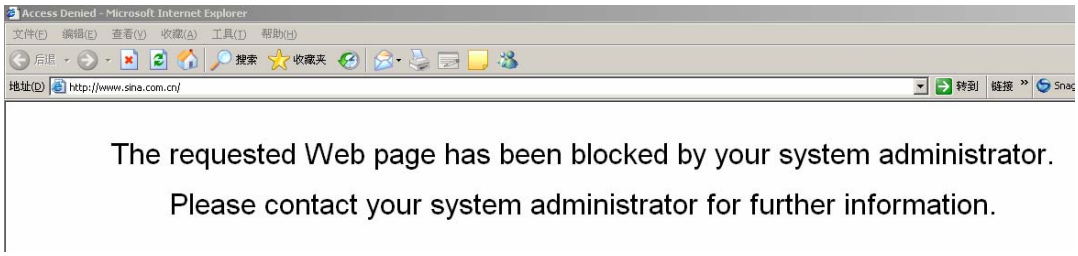



5. 接收服务商发来的确认邮件后，点击邮件中的链接，即可完成为期 30 天的试用注册。


6. 进入路由器 Web 内容过滤页面，选择一个离您最近的 CPA 服务器。


7. 选中**启用 WEB 内容过滤**，然后勾选**新闻**、**游戏**，屏蔽这两类网站的访问，并点击**确定**按钮确认设置。


8. 打开浏览器，试图访问一个新闻站点，回得到如下页面，提示要访问的网页被管理员屏蔽。



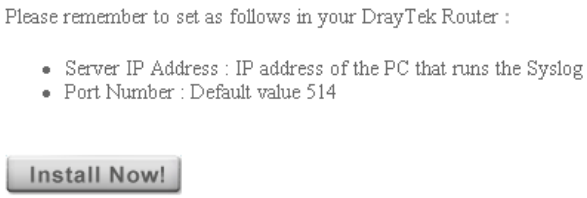

**注：**

该功能支持计划任务功能，可以通过计划任务来实现分时段屏蔽/开启。

## 4.6 升级路由器固件

在升级路由器前您需要先安装路由器工具。升级工具 **Firmware Upgrade Utility** 就在工具内。

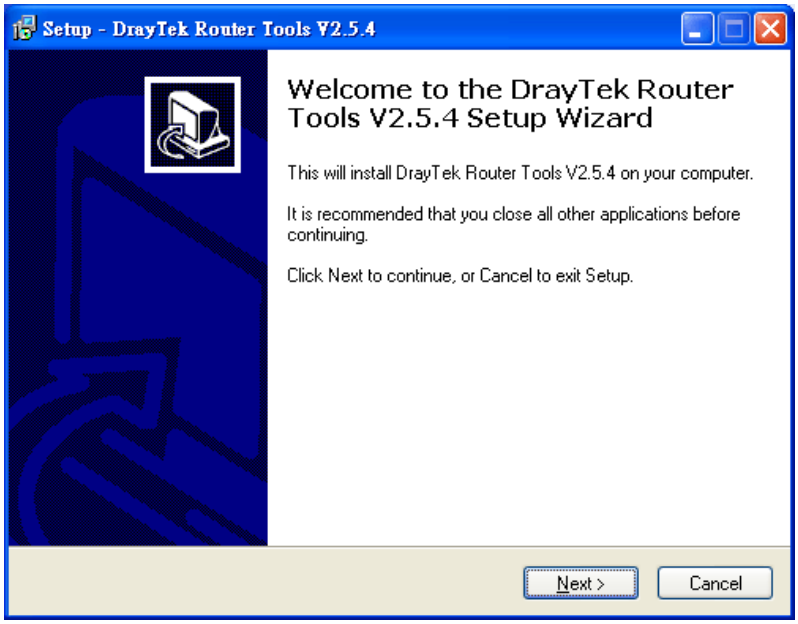
1. 请将附赠的 CD 盘插入您的 CD 光驱。
2. 从页面上找到 **Utility** 菜单并点击它。
3. 在 Utility 的页面上，点击**现在安装**（在 Syslog 描述的下方）




4. 您需要将 **RTSxxx.exe** 文件复制到您的电脑上。请记住存放此文件的路径.
5. 到www.draytek.com.cn 找到路由器的最新固件。
6. 进入**技术支持>> 相关下载**，找到相关型号的路由器后，点击进入，然后下载固件。另外，您还可以获取 Vigor 的路由器工具
7. 选择与您电脑的操作系统相匹配的路由器工具，以及路由器的固件文件，然后下载。

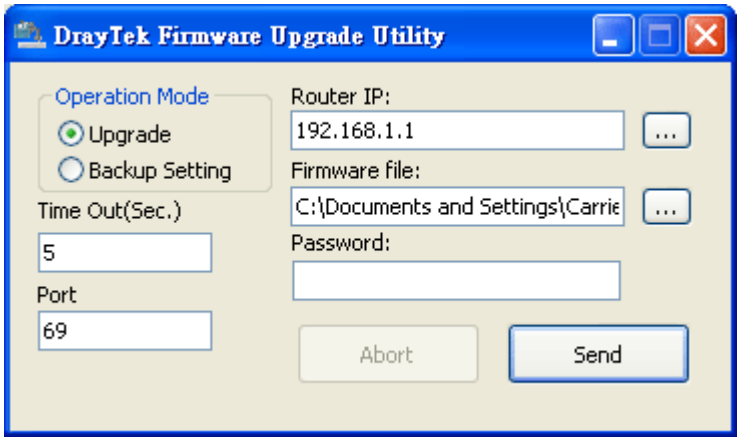
| 产品名称 | 更新日期 | |
|---|---|---|
| Vigor 2100V/VG | 2005/05/11 | 相关下载 |
| Vigor 2104/P/B | 2005/07/22 | 相关下载 |
| Vigor 2200E+ | 2005/02/01 | 相关下载 |
| Vigor 2200V/VG | 2005/05/11 | 相关下载 |
| Vigor 2300 | 2004/07/05 | 相关下载 |
| Vigor 2500/We | 2005/06/08 | 相关下载 |
| Vigor 2500V/Vi | 2005/06/30 | 相关下载 |
| Vigor 2510V/Vi | 2005/06/30 | 相关下载 |
| Vigor 2600+/G | 2005/03/11 | 相关下载 |
| Vigor 2600/W | 2005/07/05 | 相关下载 |
| Vigor 2600Ge | 2004/12/30 | 相关下载 |
| Vigor 2600V/VG | 2005/01/14 | 相关下载 |
| Vigor 2900/G/Gi/i | 2005/03/21 | 相关下载 |
| Vigor 2900V | 2005/06/17 | 相关下载 |
| Vigor 3300/V | 2005/08/17 | 相关下载 |
| Vigor 3300B+ | 2005/08/17 | 相关下载 |

8. 双击路由器工具图表，将会出现安装指导。
9. 按照提示页面上的指导进行安装。最后点击**结束**以完成安装。
10. 在 Windows 操作系统里，到**开始**菜单，打开**程序**，然后选择 **Router Tools XXX >> Firmware Upgrade Utility**。


11. 输入您路由器 IP，通常是 192.168.1.1。

12. 点击固件输入框右侧的按键。找到您在电脑上存放固件的位置。您将发现有两个文件，分别有不同的后缀名.all（升级后会保留旧的设置）和.rst（升级后会擦除旧的设置）。您可以选择任意一个文件升级。




13. 点击 Send，升级将如下进行。

14. 耐心等待一段时间，直到升级完成。

# 5 故障排查

这个章节将会指导您如何解决在完成安装和设置路由器后依然无法上网的问题。请按照以下方法一步一步地进行检查。

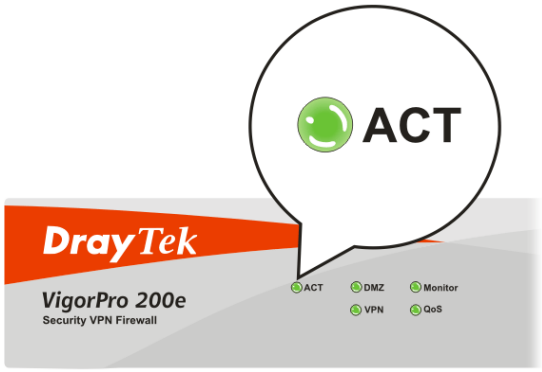
- 检查路由器硬件是否正常。
- 检查您电脑的网络连接是否正常。
- 试试看能否从电脑 ping 到路由器。
- 检查 ISP 的设置是否正常。
- 必要的话将路由器恢复至默认出厂设置。

若以上步骤都无法解决您的问题，您需要联系代理商获取进一步的帮助了。

## 5.1 检查路由器硬件是否正常

按照以下步骤确认硬件状态

1. 检查电源线以及网络连接。详细信息请参考“**2.1 硬件安装**”。
2. 开启路由器，确认 ACT 指示灯每秒闪烁一次，以及相关的 LAN 指示灯是否亮着。




3. 若没有，意味着路由器的硬件有问题。那么请回到“2.1 硬件安装”，再重新执行一次硬件安装，然后再试试。

## 5.2 检查网络连接是否正常

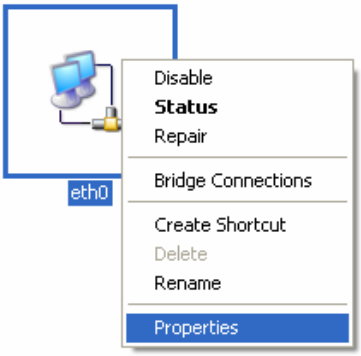
有些时候无法上网是由错误的网络连接设置造成的。若在尝试过上面的方法，连接依然失败，请按以下步骤确认网络连接是否正常。

## 对于 Windows 系统

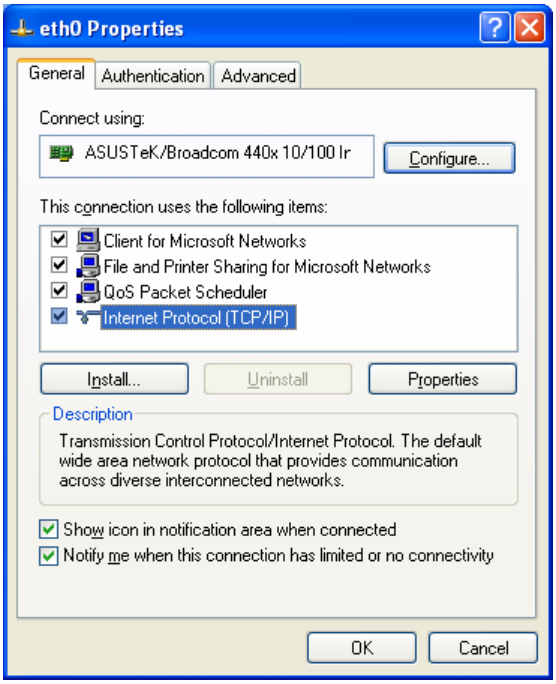
我们以Windows XP系统为基础进行举例，对于其它操作系统，请到 www.draytek.com.cn 上参考相关支持文件。

1. 到**控制面板**中，双击**网络连接**。

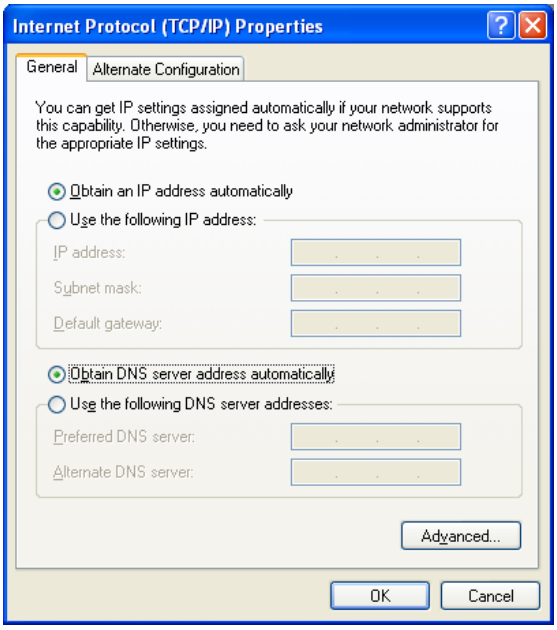

2. 右键点击**本地连接**图标，然后点击**属性**。




3. 选择 Internet 协议（TCP/IP），然后点击**属性**。

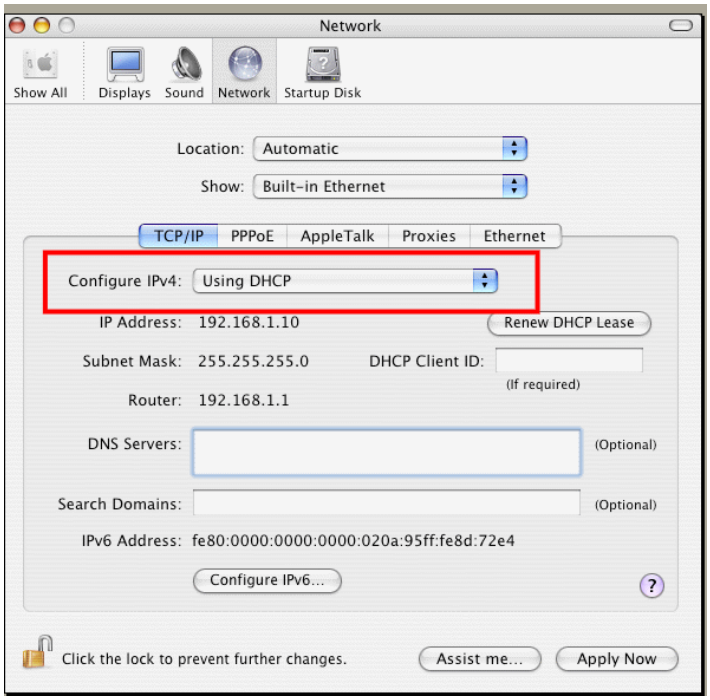


4. 选择**自动获得 IP 地址**以及**自动获得 DNS 服务器地址**。




## 对于 Mac 系统

1. 双击桌面上当前使用的 Mac 系统。
2. 打开**应用**，然后进入**网络**。
3. 在**网络**页面上，从**设置 IPv4** 的下拉菜单中选择**使用 DHCP**。



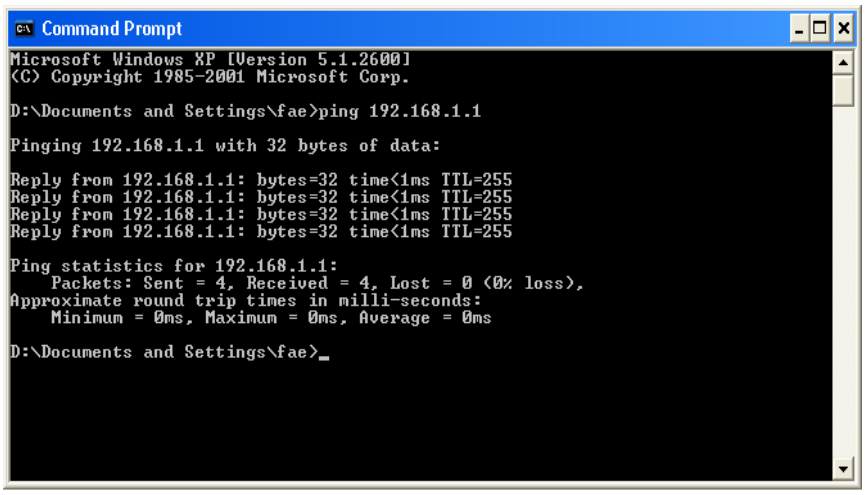
## 5.3 从电脑上 ping 路由器

路由器的默认 IP 地址是 192.168.1.1。您可以使用“ping”命令检查到路由器的连接状态。最重要的是要看电脑是否可以收到从 192.168.1.1 发回来的回应。若没有，请检查您电脑的 IP 地址是多少。我们建议您将网络连接设置为**自动获得 IP 地址**。（请参考 4.2 章节）

请按照以下步骤 ping 路由器。

### 对于 Windows 系统

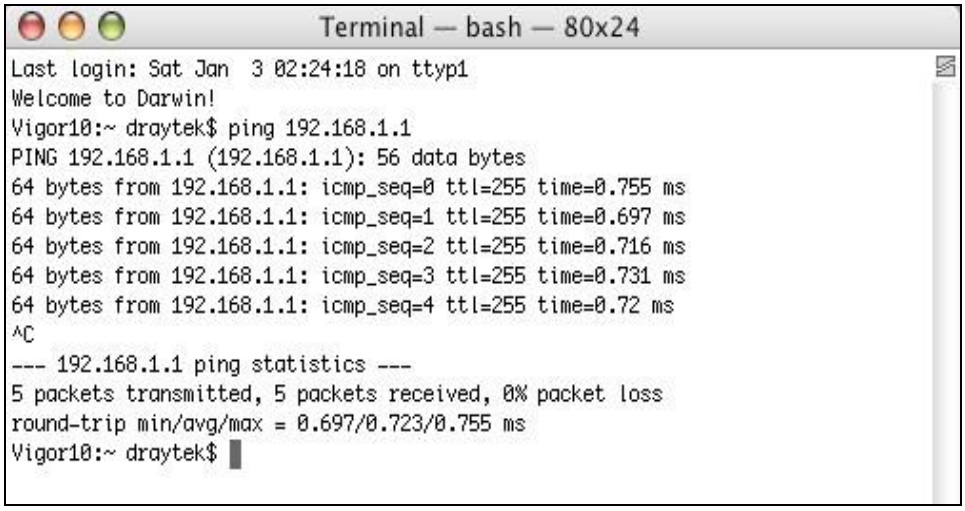
1. 打开命令行提示窗口（从**开始 > 运行**）。
2. 输入 command（Windows 95/98/ME）或是 cmd（Windows NT/2000/XP）。DOS 界面的命令行对话框将会出现。




3. 输入 ping 192.168.1.1 然后按回车。若是连接没有问题，将会有“Reply from 192.168.1.1:bytes=32 time<1ms TTL=25”的回应消息出现。
4. 若是回应消息没有出现，请检查您电脑的 IP 设置是否正确。

### 对于 Mac 系统（终端）

1. 双击桌面当前使用的 Mac 系统。
2. 打开**应用**文件夹，进入**工具**。
3. 双击**终端**，终端窗口将会弹出。
4. 输入 ping 192.168.1.1，然后按回车。若是连接没有问题，会返回“**64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**”回应消息。

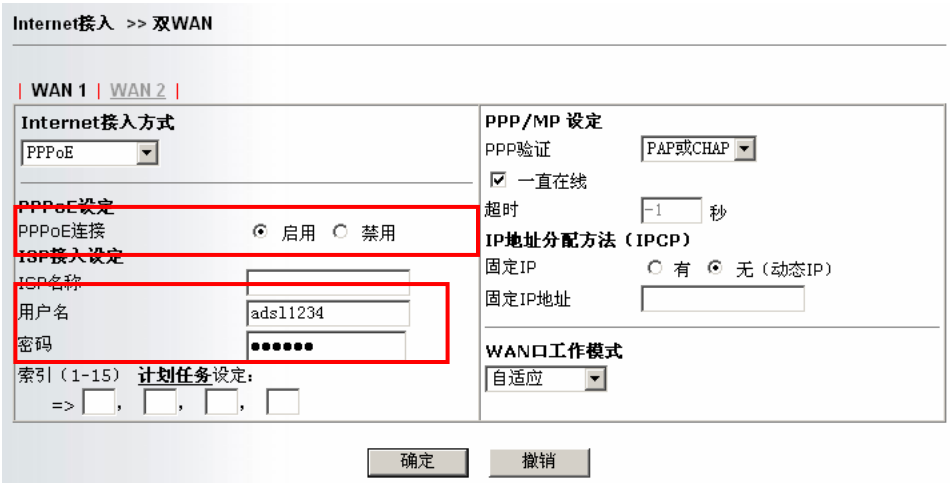

Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

## 5.4 检查 ISP 设置是否正常

点击 Internet 接入，然后检查 ISP 设置是否正确。

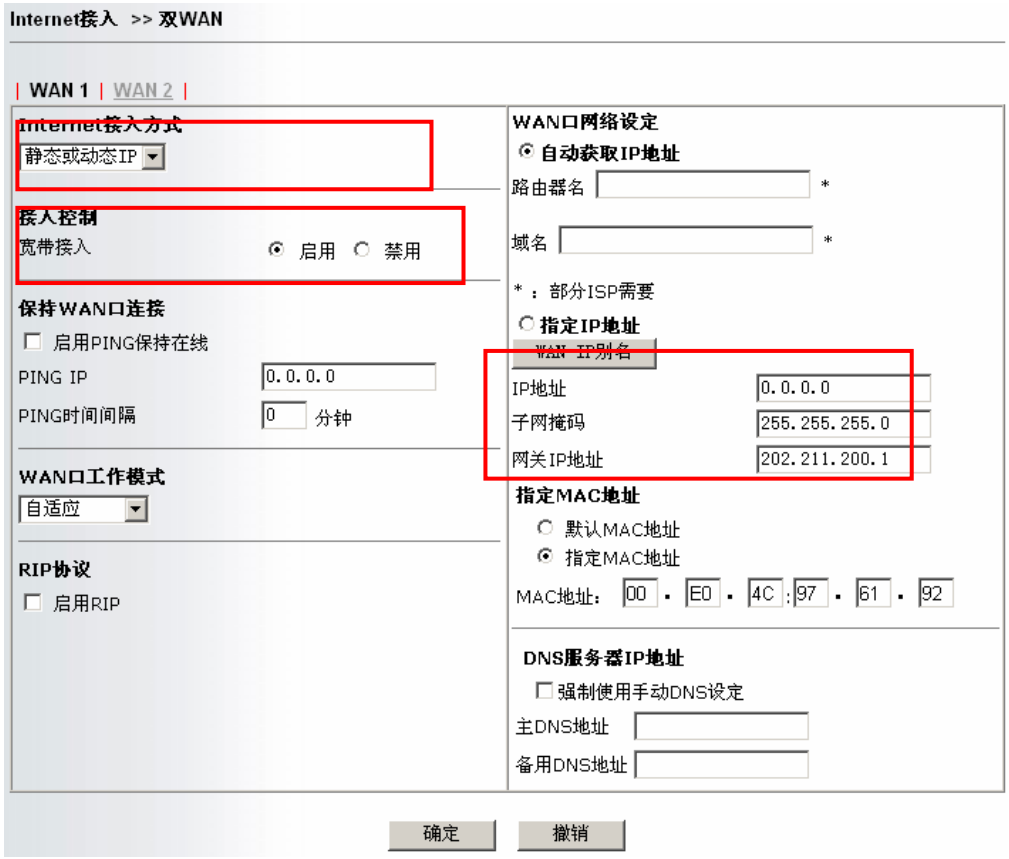

### 对于 PPPoE 用户

1. 检查是否选择了**启用**。
2. 检查您是否正确地输入了 ISP 提供给您的**用户名**和**密码**。



## 对于静态或动态 IP 用户

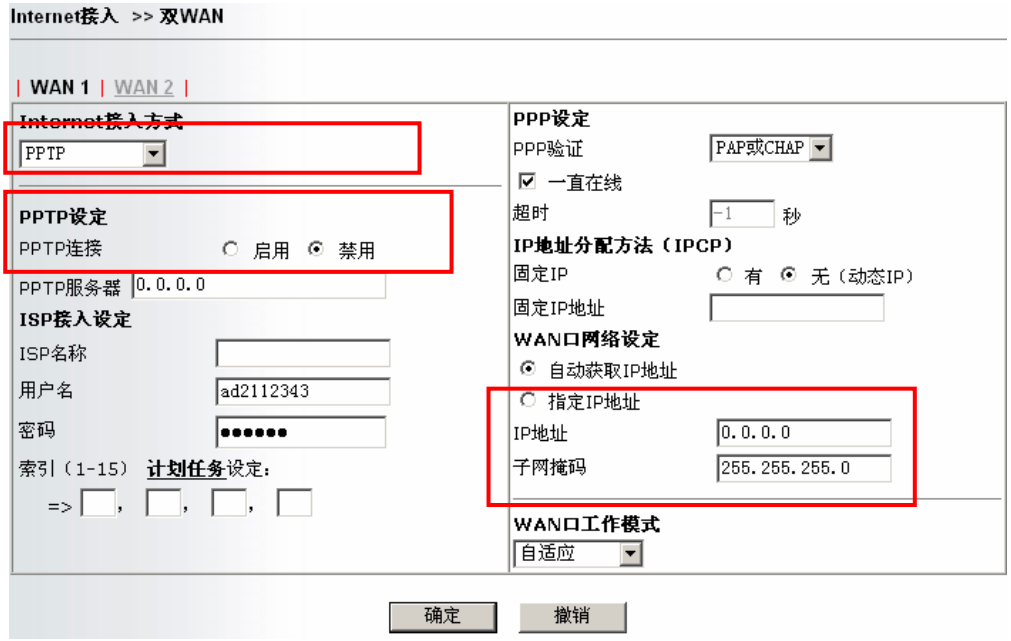
1. 检查是否选择了启用。




2. 若您选择了指定 IP 地址，请确认是否正确输入了 IP 地址，子网掩码以及网关 IP 地址（一定要与您的 ISP 确认相关设置）。

## 对于 PPTP 用户

1. 检查是否选择了 PPTP 的启用。并请检查 PPTP 服务器的 IP 地址。



2. 若您选择了指定 IP 地址，请确认是否正确输入了 IP 地址和子网掩码（一定要与您的 ISP 确认相关设置）。

## 5.5 将路由器恢复至默认出厂设置

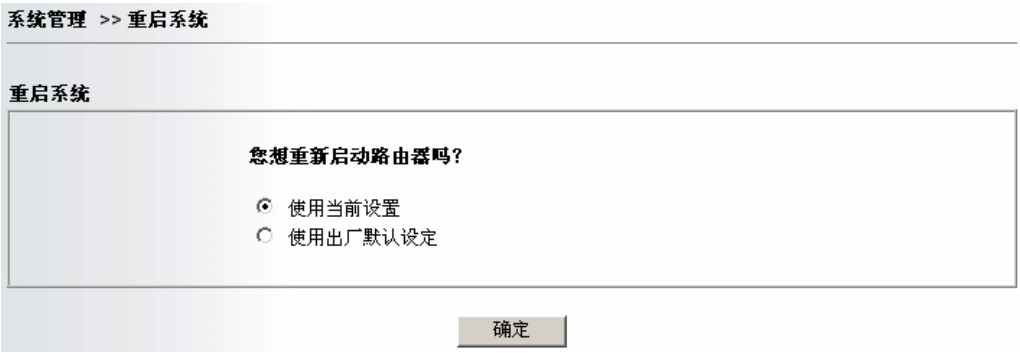
有些时候，恢复路由器至默认出厂设置可以解决错误设置导致的连接失败。请尝试软件或硬件重设路由器。

**注意:**在按下使用出厂默认设定后，您将失去您所有的旧设定。请确认您在确定前记下了重要的设定。重启后的密码为空。

### 软件重置

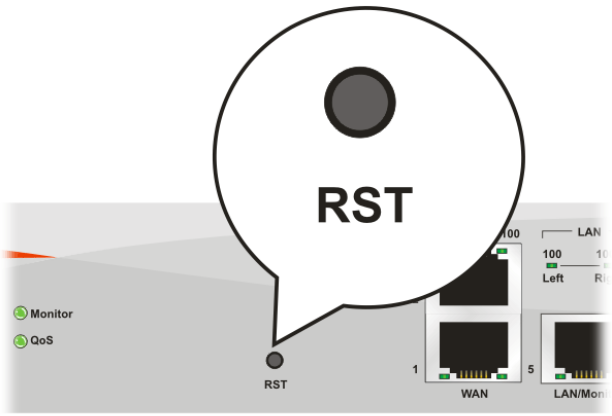
您可以在路由器的 Web 界面直接重置。

到 Web 界面上的**系统管理>>重启系统**，点击**重启系统**，然后会到下图界面。选择**使用出厂默认设定**，并点击确定。几秒钟后，路由器就会恢复至出厂默认设定。




### 硬件重置

当路由器电源开启的时候（ACT 指示灯正在闪烁），按下 RST 键，并保持 5 秒钟。当您看到 ACT 指示等开始快速闪烁时，再放开 RST 键。然后路由器就会恢复到出厂默认设定了。




恢复至默认出厂设定后，您就可以按需求重新配置路由器了。

## 5.6 联系您的代理商

若在大量尝试后，网络仍然无法正常工作，请联系您的代理商以获得进一步的帮助。或者，您还可以发送电子邮件到support@draytek.com