# 版权声明



本手册中的所有图片和产品规格参数仅供参考，随着软件或硬件的升级会略有差异，如有变更，恕不另行通知，如需了解更多产品信息，请浏览我们公司的网站：

http://www.ip-com.com.cn

# 目　　录

# 1 第一章 产品概述

## 1.1 产品简介

T3 是一款专门为出租屋业主设计的管理型路由器。支持双线路接入，可以叠加双 ISP 线路的带宽; 支持 WEB 认证和 PPPOE 服务器用户管理，有效限制非法用户接入; 具有超强的 NAT 转发能力，具备“上网行为管理”功能，以及产品的超强稳定性，使得网络管理员可以轻松的管理网络的运行。

## 1.2 主要特性

- 支持 WEB 认证、PPPOE 服务器，用户管理，用户可搭建小型 ISP 网络
- 提供 2 个 10/100M 自适应以太网接口(WAN)，连接外部网络
- 提供 3 个 10/100M 自适应以太网局域网接口(LAN)
- 符合 IEEE 802.3、IEEE 802.3u 等标准
- 高达 360MHz 的 CPU 处理能力，超强 NAT 转发性能，允许更多用户接入
- 支持多线接入，自动实现带宽叠加，智能负载均衡、按比例负载均衡
- 支持 WAN 口访问控制，允许指定地址的主机对路由器进行远程管理
- 内建 DHCP 服务器，可进行静态地址分配
- 内建防火墙，可精确控制上网时间
- 支持客户端过滤、MAC 过滤、URL 过滤
- 支持弹性带宽，最大化的利用带宽资源
- 支持 IP-MAC 地址绑定功能，有效防止 ARP 攻击 、ARP 欺骗和非授权用户接入
- 支持攻击防御，保证网络安全稳定

- 支持虚拟服务器、DMZ 主机
- 支持 UPnP、DDNS(动态域名解析) 和静态路由等功能
- 提供系统日志和流量统计功能
- 支持配置文件备份与恢复

## 1.3 产品规格

| | | |
|---|---|---|
| 支持的标准和协议 | | IEEE 802.3、IEEE 802.3u、IEEE 802.3x、TCP/IP、UDP/IP、DHCP、ARP、NAT、PPPoE、SNTP、HTTP、DNS、ICMP、GRE |
| 网络介质 | | 10Base-T：3 类或 3 类以上 UTP<br>100Base-TX：5 类 UTP |
| 端口和 LED 指示灯 | WAN 口 | 2 个“WAN”指示灯和 2 个“100M”指示灯 |
| | LAN 口 | 3 个“LAN”指示灯和 3 个“100M”指示灯 |
| | 其它 | Power（电源指示灯）、SYS（系统状态指示灯） |
| 外形尺寸（L x W x H） | | 290mm×180mm×44mm |
| 使用环境 | | 工作温度：0℃到 45℃；<br>存储温度：-40℃到 70℃；<br>工作湿度：10%到 95% RH 无凝结；<br>存储湿度：5%到 90% RH 无凝结； |
| 电源及功耗 | | 输入：AC 220V 50Hz<br>功耗：最大 6W |

## 1.4 物品清单

小心打开包装盒，检查包装盒里是否有以下配件：

- ✓ T3 计费管理型由器*一台
- ✓ 电源线*一条
- ✓ 用户手册*一本
- ✓ 保修卡*一张
- ✓ L 型支架*2 个
- ✓ 螺丝*6 颗
- ✓ 脚垫*4 个

如果发现有所损坏或有任何配件短缺的情形，请及时与当地经销商联系。

# 2 第二章 硬件描述

## 2.1 面板布置

**前面板**


1） Reset ：复位按钮。按住此按钮 3 秒钟后，您设定的资料将被删除，路由器将恢复出厂设置，并自动重启。

2） 指示灯：

| 指示灯 | 描 述 | 功 能 |
|---|---|---|
| POWER | 电源指示灯 | 供电正常，指示灯常亮 |
| SYS | 系统状态指示灯 | 闪烁表示系统正常<br>常亮或不亮表示系统异常 |
| WAN/LAN | 广域网和局域网状态指示灯 | 常亮表示相应端口已正常连接<br>闪烁表示相应端口正在进行数据传输 |
| 100M | 广域网和局域网速度指示灯 | 常亮表示协商速率为 100M<br>熄灭表示协商速率为 10M |

3) WAN：2 个广域网端口（RJ-45）。连接 xDSL Modem/Cable Modem 或以太网。

4) 局域网端口：3 个 LAN 端口（RJ-45）。连接至计算机的以太网网卡，也可级联至集线器和交换机。

**后面板**


## 2.2 系统需求

- 网络适配器
- Internet Explorer 5.0或更高版本
- 宽带Internet服务(接入方式为通过xDSL/Cable Modem/以太网接入)

## 2.3 安装环境要求

- 请不要将路由器放在不稳定的箱子或桌子上，万一跌落，会对路由器造成严重损害。
- 路由器要在正确的电压下才能正常工作，请确认工作电压同路由器所标示的电压相符。为减少受电击的危险，建议接地。在路由器工作时不要打开外壳，即使在不通电的情况下，也不要随意打开路由器机壳。
- 确认路由器的入风口及通风口处留有空间，以利于路由器的散热。

## 2.4 硬件安装步骤

在安装路由器前，请确认您已经能够在单台计算机上通过宽带服务成功上网，如果您单台计算机上网有问题，请先和您的网络供应商联系解决问题。当您成功地利用单台计算机上网后，请遵循以下步骤安装路由器。

- 建立局域网连接

  将路由器 LAN 口和局域网中的 Hub 或交换机连接。您也可以将路由器 LAN 口直接和您的计算机网卡连接。
- 建立广域网连接

将 xDSL 或以太网接入五类线和路由器 WAN 口相连。

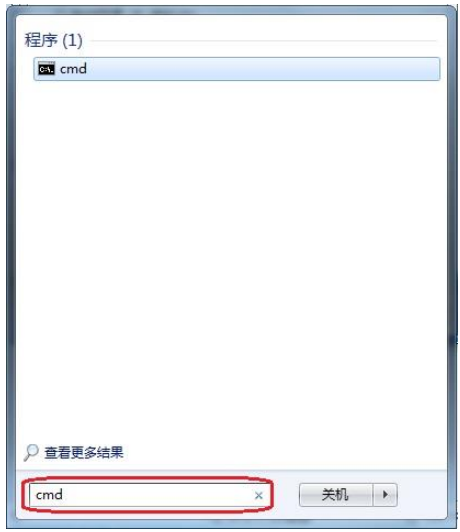
- 连接电源将电源连接好，路由器将自行启动。

# 3 第三章 快速安装

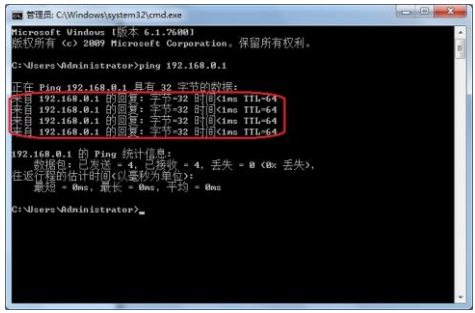
路由器默认 IP 地址是：192.168.0.1，可根据您的需要进行改变，本说明书将使用默认值进行说明。

将您的计算机连接到路由器的 LAN 口，并按照附录一中的步骤配置好 TCP/IP 参数后，您可以使用 Ping 命令检查您的计算机和路由器之间是否连通：

- 选择“开始”，在"搜索程序和文件"对话框中输入“cmd”然后回车。



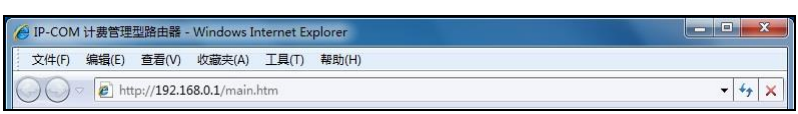

- 输入“ping 192.168.0.1”并回车，如能得到图示的回应，则表明您的计算机与路由器连接正常。否则请检查路由器是否通电，计算机到路由器的网线是否连接好，同时确认 TCP/IP 参数设置是否正确。




## 3.1 快速安装

本产品提供基于浏览器的配置界面、这种配置方式同样适合任何 MS Windows、Macintosh 或 UNIX 平台。

打开 WEB 浏览器，在地址栏中键入“http://192.168.0.1”，并回车；




连接建立后，您会看到登录界面。您需要以系统管理员的身份登录，输入用户名和密码（用户名和密码出厂设置均为“admin”），为方便下次快速进入路由器管理页面，请选择“记住我的凭据”。


⚠**注意：**

为了路由器的安全，请正确登录后修改系统默认的用户名和密码！

如果您输入的用户名和密码正确，浏览器将进入管理员模式的画面，并出现一个快速设置向导，


点击“下一步”，进入上网方式选择画面。


本路由器支持最常见的三种上网方式，默认接入方式为动态 IP 接入：

- 静态 IP：以太网宽带接入方式 ISP（网络服务商）提供的固定 IP 地址。
- 动态 IP：宽带网络或者有线通通过 DHCP 服务为用户分配 IP 地址。
- ADSL 虚拟拨号（PPPoE）：采用 PPPoE 虚拟拨号来进行 Internet 连接。

**注意：**

1. 广域网接口有 2 个端口可供选择，配置的时候要先选择需配置的 WAN 口，然后根据自己实际情况对 WAN 口分别进行配置。
2. 带宽的单位为 KByte/s（千字节/秒）。假设运营商提供的线路为 2M ADSL，上传速度为 512Kbps，下载速度为 2Mbps。单位换算如下：

   上行带宽 512Kbps = 64KByte/s

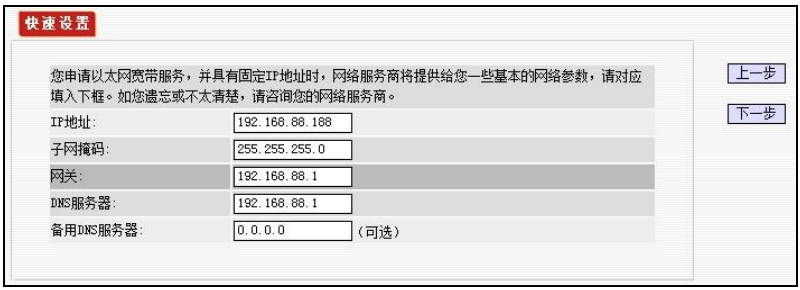
   下行带宽 2Mbps = 2048Kbps = 256KByte/s。

根据自身情况选择需要接入的 WAN 口并选择正确的接入方式，然后填写合适的上下行带宽，最后单击“下一步”填写上网所需的基本网络参数。

### 3.1.1 静态 IP

如果您的上网方式为“静态 IP”，输入 ISP（网络服务商）提供给您的固定 IP 地址，子

网掩码，网关地址以及主 DNS、备用 DNS 地址，点击“下一步”保存即可。




- IP 地址：本路由器对广域网的 IP 地址，即 ISP（网络服务商）提供给您的 IP 地址，不清楚可以向 ISP（网络服务商）询问。
- 子网掩码：本路由器对广域网的子网掩码，即 ISP（网络服务商）提供给您的子网掩码，不清楚可以向 ISP（网络服务商）询问。
- 网关：填入 ISP（网络服务商）提供给您的网关，不清楚可以向 ISP（网络服务商）询问。
- DNS 服务器：填入 ISP（网络服务商）提供给您的 DNS 服务器，不清楚可以向 ISP（网络服务商）询问。
- 备用 DNS 服务器：可选，如果 ISP（网络服务商）提供两个 DNS 服务器地址，您可以将另一个 DNS 服务器地址填入此处。

**⚠注意：**

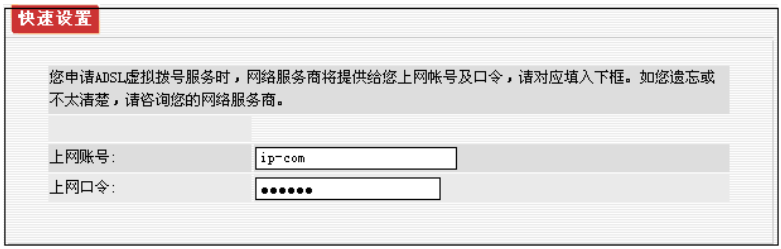
路由器 WAN 口指定的 IP 地址和路由器 LAN 口 IP 地址在同一网段，将会影响路由器的使用，导致路由器无法正常工作。紧急时，请使用面板上的复位键进行复位

### 3.1.2 动态 IP

如果您的上网方式为“动态 IP”，通过此种接入，您可以从 ISP（网络服务商）服务商处动态获取到 IP 地址访问 Internet；不需其它设置，点击“下一步”保存即可。

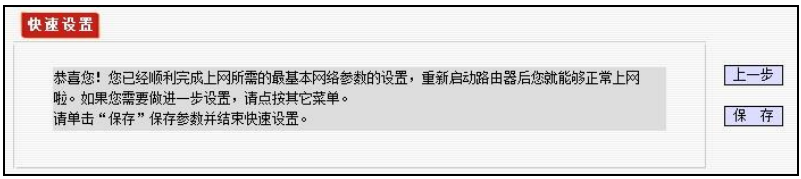
### 3.1.3 PPPoE

如果您的上网方式为“ADSL 虚拟拨号”，只需要在“上网账号”及“上网口令”中输入框中输入 ISP（网络服务商）服务商提供给您的帐号信息。




- 上网帐号：填入 ISP（网络服务商）为您指定的 ADSL 上网用户名，不清楚可以向 ISP（网络服务商）询问。
- 上网口令：填入 ISP（网络服务商）为您指定的 ADSL 上网的密码，不清楚可以向 ISP（网络服务商）询问。

在填写完上网的基本网络参数后，您可来到设置向导的完成画面，点击“保存”完成设置。




当设置完成以后可以到“运行状态”中“WAN 口状态”中查看配置信息。


WAN1状态
WAN2状态
LAN状态
系统信息
连接状态 已连接
连接方式 静态 IP
WAN IP 192.168.88.188
子网掩码 255.255.255.0
网关 192.168.88.1
域名服务器 192.168.88.1
备用域名服务器 0.0.0.0
WAN MAC 地址 50:53:00:01:00:11
WAN口流量 下行:0.00KByte 上行:0.00KByte

# 4 第四章 配置说明

本章介绍路由器各种功能在 Web 界面的配置方法，使用户能够轻松使用和管理路由器。在 Web 管理界面中分以下 10 个菜单栏介绍路由器的各个功能：

- 运行状态
- 快速设置
- 网络
- 用户管理
- 行为管理
- 安全
- 高级
- 监控
- 系统工具
- 退出登录

在使用过程中，如果您对本产品的功能有任何问题，您只需单击页面的“帮助”按钮，下面将详细讲解各个菜单的功能。

## 4.1 运行状态

**WAN 口状态**


此处显示当前 WAN 口的连接状态、连接方式、WAN IP、子网掩码、网关、域名服务器、备用域名服务器、WAN 口 MAC 地址、WAN 流量。

- WAN 口连接状态：显示 WAN 口的连接状态。

  未连接：表示 WAN 口未接网线；

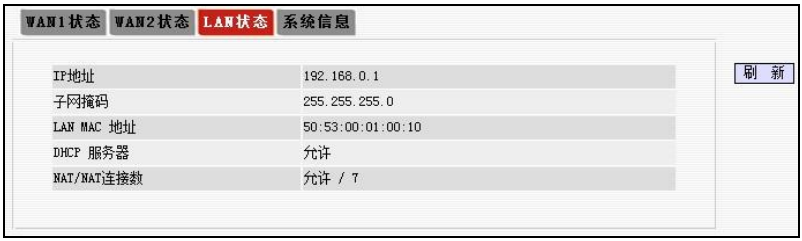
  连接中：表示 WAN 口已接通，正在获取 IP 地址；

  已连接：表示路由器与 ISP（网络服务商）已正常接通；
- 连接方式：表示当前您选的接入方式。
- WAN IP：从 ISP（网络服务商）获取的 IP 地址。
- 子网掩码：从 ISP（网络服务商）获取的子网掩码。
- 网关：从 ISP（网络服务商）获取的网关。
- 域名服务器：从 ISP（网络服务商）获取的主 DNS。
- 备用域名服务器：从 ISP（网络服务商）获取的备用 DNS。
- WAN 口 MAC 地址：显示 WAN 口的 MAC 地址。
- WAN 口流量：表示当前路由器已使用的带宽，单位为 KB/s。
- 连接时间：表示路由器与 ISP（网络服务商）连接的时间（动态 ip 和 PPPoE 接入方式）

**LAN 状态**

此处显示当前路由器的 IP 地址、子网掩码、LAN MAC 地址、DHCP 服务器和 NAT/NAT

连接数。




- IP 地址：显示当前路由器的 IP 地址；
- 子网掩码：显示当前路由器子网掩码；
- LAN MAC 地址：显示路由器 LAN MAC 地址；
- DHCP 服务器：显示 DHCP 服务器开启和关闭状态；
- NAT/NAT 连接数：显示路由器的工作模式/已使用的 NAT 数；

**系统信息**

显示路由器 CPU 使用率、内存使用率、运行时间、系统时间、已连接客户端、系统版本、硬件版本号。

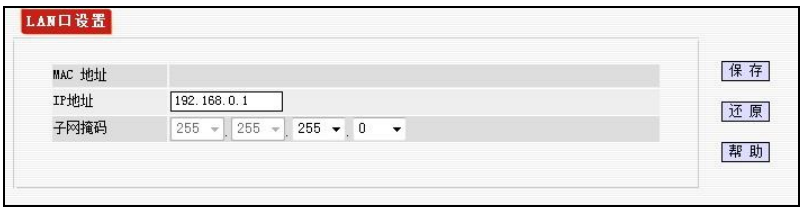

- CPU 使用率：显示当前 CPU 的使用情况；
- 内存使用率：显示当前内存的使用情况；
- 运行时间：显示系统正常启动后的运行时间；
- 系统时间：显示系统更新时间；
- 已连接客户端：显示已连接的计算机数量；
- 系统版本：显示路由器的软件版本；
- 硬件版本号：显示路由器的硬件版本；

CPU 使用率显示图以更加直观的方式显示路由器 CPU 负荷情况。

## 4.2 网络

在“网络”菜单下面，共有“LAN”、“WAN”、“DHCP 服务器”、“DMZ”、“访问控制”、“端口参数设置”六个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。


### 4.2.1 LAN




- MAC 地址：显示路由器 LAN 口的 MAC 地址。
- IP 地址：本路由器对局域网的 IP 地址。出厂值默认为 192.168.0.1，您可以根据需要改变它。
- 子网掩码：该路由器对局域网的子网掩码。

**注意：**

如果您修改了该 IP 地址，您必须用新的 IP 地址才能登录路由器 WEB 界面进行管理，同时局域网中所有计算机的默认网关必须设置为该 IP 地址才能正常上网。

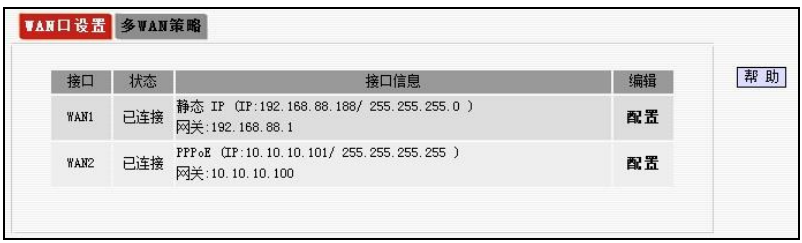
路由器 WAN 口获取或指定的 IP 地址和路由器 LAN 口 IP 地址在同一网段，会导致路由器无法正常工作。紧急时，请使用面板上的复位键进行复位。

### 4.2.2 WAN

在“WAN”菜单下面，有“WAN 口设置”和“多 WAN 策略”两个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

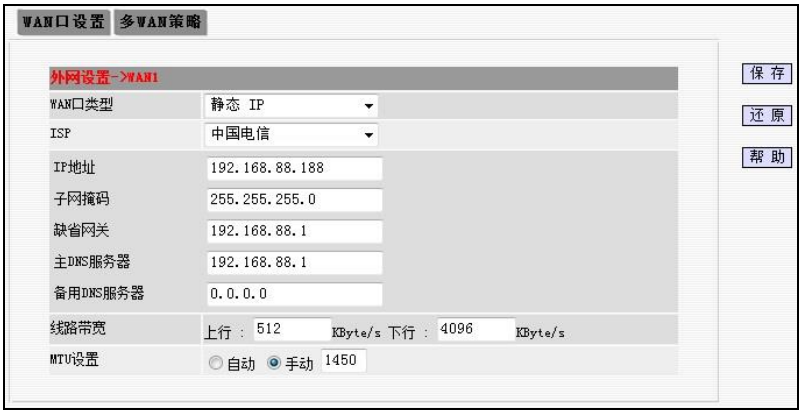
**WAN 口设置**

本界面显示所有 WAN 口的接入状态和接口参数。




选择您要设置的 WAN 口，点击“配置”，即可进入外网设置界面。本界面用于配置 WAN 口的接口参数。每个 WAN 口都支持三种连接方式，静态 IP，动态 IP, PPPOE 拨号。

1）静态 IP：如果您的上网方式为静态 IP，即您拥有网络服务商提供的固定 IP 地址。




- ISP： WAN 口连接线路的 ISP 名称。
- IP 地址：申请的线路的广域网 IP 地址，由网络服务商提供，可以向网络服务商询问获得。
- 子网掩码：当前 IP 所对应的子网掩码，由网络服务商提供，可以向网络服务商询问获得。
- 缺省网关：当前 IP 所对应的网关，由网络服务商提供，可以向网络服务商询问获得。
- 主 DNS 服务器/备用 DNS 服务器：填入网络服务商提供的 DNS 服务器 IP 地址，可以向网络服务商询问获得。
- 线路带宽：申请的 WAN1 口静态线路的带宽，可以向网络服务商询问获得。
- MTU 设置：MTU（最大传输单元），系统默认使用 1450 字节。注意：通常情况下这个参数不用设置，不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

2）动态 IP：如果您的上网方式为动态 IP，即您可以自动从网络服务商获取 IP 地址。

- ISP： WAN 口连接线路的 ISP 名称。
- 线路带宽：申请的 WAN 口动态 IP 线路的带宽，可以向网络服务商询问获得。
- MTU 设置：MTU（最大传输单元），系统默认使用 1450 字节。

**⚠注意：**

通常情况下这个参数不用设置，不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

3） PPPOE 拨号：如果您的上网方式为 PPPOE 拨号，您可以通过 ADSL 虚拟拨号来获取 ip 地址。


- ISP： WAN 口连接线路的 ISP 名称。
- PPPOE 帐号：填入网络服务商提供的 PPPOE 帐号，可以向网络服务商询问获得。
- PPPOE 密码：填入网络服务商提供的 PPPOE 口令，可以向网络服务商询问获得。
- 线路带宽：申请的账号带宽，可以向网络服务商询问。
- MTU 设置：MTU（最大传输单元），系统默认使用 1450 字节。

**⚠注意：**

通常情况下这个参数不用设置，不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

**多 WAN 策略**

在该页面，您可以根据自己需要选择多 WAN 策略，本路由器有两种不同的工作模式，您也可以根据需要自定义 WAN 口策略。


- 智能负载均衡模式（全自动）：系统按流量自动分配负载，自动寻找流量最小的 WAN 口通信，这个方式是最智能的，也是最好的负载模式。负载均衡策略完全不用人工干预，自动分配流量，并能成功实现带宽叠加。

  **注意：**系统默认的工作模式为智能负载均衡。

- 按比例负载均衡：用户根据自己的实际需要，将流量按比例分配到对应 WAN 口，以达到带宽的合理利用。在此工作模式下，您可以根据实际情况定义需要的负载设置。
- 用户自定义策略：用户根据自己的实际需要，针对特定的源地址和目的端口指定特定的 WAN 口。在此工作模式下，您可以根据实际情况定义需要的策略模式。

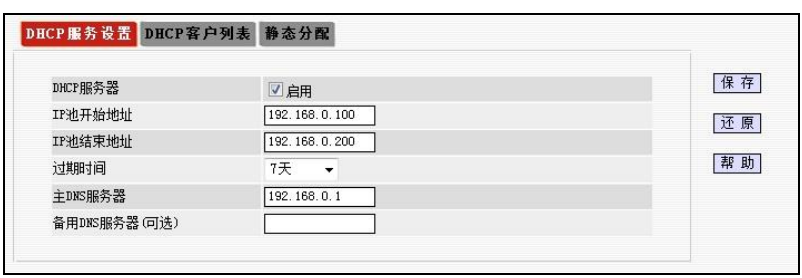
  **注意：**用户在配置自定义策略之前，请在“行为管理”→“组设置”中添加 IP 组。

### 4.2.3 DHCP 服务器

在“DHCP 服务器”菜单下面，有“DHCP 服务设置”、“DHCP 客户列表”和“静态分配”三个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

**DHCP 服务器设置**

TCP/IP 协议设置包括 IP 地址、子网掩码、网关、以及 DNS 服务器等。为您局域网中所有的计算机正确配置 TCP/IP 协议并不是一件容易的事，幸运的是，DHCP 服务器提供了这种功能。如果您使用本路由器的 DHCP 服务器功能的话，您可以让 DHCP 服务器自动替您配置局域网中各计算机的 TCP/IP 协议。




- DHCP 服务器：如果您想使用 DHCP 的自动配置 TCP/IP 参数功能，请勾选该选项。
- IP 池开始地址：DHCP 服务器所自动分配的 IP 的起始地址。
- IP 池结束地址：DHCP 服务器所自动分配的 IP 的结束地址。
- 过期时间：客户端获得 IP 地址的使用时间。
- 主 DNS 服务器：分配的 DNS 服务器地址。
- 备用 DNS 服务器：分配的 DNS 服务器地址（可不填）。

**⚠注意：**

为了使用本路由器的 DHCP 服务器功能，局域网中计算机的 TCP/IP 协议必须设置为“自动获得 IP 地址”。

**DHCP 客户列表**

该客户列表显示了所有通过 DHCP 获得 IP 的主机名、IP 地址、MAC 地址、租约时间。


- 主机名：客户端的主机名。
- IP 地址：客户端申请到的 IP 地址。
- MAC 地址：申请到该 IP 地址的计算机的 MAC 地址。
- 租约时间：主机通过 DHCP 所获得的 IP 的使用时间。

### 4.2.4 静态分配

DHCP 服务器支持静态 IP 地址分配。如果希望内网某台主机每次启动以后都会获取 DHCP 服务器分配的同一 IP 地址，可以使用此功能。

**例如：**内网有台计算机的 MAC 地址是 00:15:58:c0:d4:3f，希望它每次启动以后都会获取 IP 192.168.0.150。首先，填写相应的 IP 地址与 MAC 地址，然后点击“添加”并保存，配置的结果如下图所示：


- IP 地址：预留的 IP 地址。

- MAC 地址：预留 IP 地址的计算机的 MAC 地址。
- 添加：将预留的 IP 地址和 MAC 地址添加到表中。
- 编辑：修改静态分配的 ip 地址和 MAC 地址。
- 更新：对已经编辑好的规则添加到列表中。
- 删除：将已建立的静态分配信息清除。

### 4.2.5 DMZ

在某些特殊情况下，需要让局域网中的一台计算机完全暴露给广域网，以实现双向通信，此时可以把该计算机设置为 DMZ 主机。


设置步骤：首先将需完全映射到外网的主机 IP 地址填入到“WAN 口映射的 DMZ 主机 IP 地址”，然后点击“启用”并保存完成 DMZ 主机的设置。

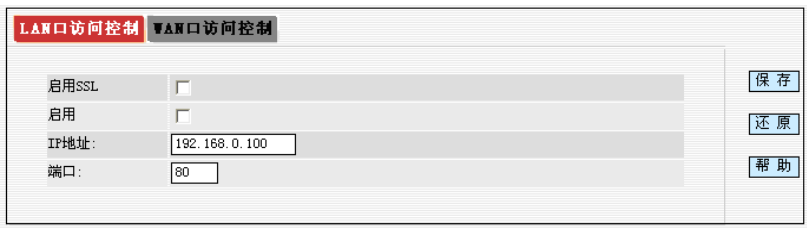
**⚠注意：**

1. 设置 DMZ 之后，与该 IP 相关的防火墙设置将不起作用。
2. 广域网中的主机需要访问 DMZ 主机的时候，访问的 IP 地址是相应的 WAN 口 IP 地址。

### 4.2.6 访问控制

为了保证路由器管理的安全性，您可以指定允许管理路由器的 IP 地址或更改路由器端口号。在“访问控制”菜单下面，有“LAN 口访问控制”和“WAN 口访问控制”两个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能：

**LAN 口访问控制**

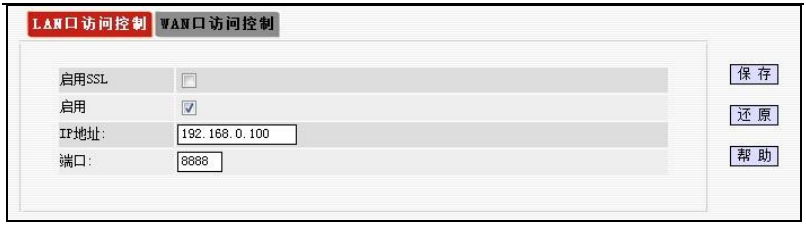



- 启用 SSL：启用 SSL 安全协议，为数据通讯提供安全支持。
- 启用：开启访问路由器 WEB 限制功能。
- IP 地址：输入局域网中计算机的 IP 地址。
- 端口：默认端口为 80，输入您访问路由器 WEB 界面的端口号。

**⚠注意：**

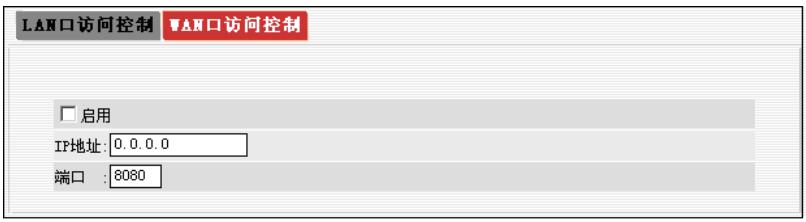
设置指定 IP 地址之后，其它地址的主机将不能登陆路由器 WEB 界面。若启用 SSL，端口会自动跳转为 443，同时路由器的访问方式更改为：https://192.168.0.1，当启用 SSL 后，WAN 口访问控制必须使用 https 访问。

**例如：**路由器的 IP 地址为默认的 192.168.0.1，您仅允许 IP 地址为 192.168.0.100 的客户机，通过端口 8888 访问路由器 WEB 界面，则需要设置如下参数，且路由器的访问地址也更改为：http://192.168.0.1:8888。




**WAN 口访问控制**

通常来讲，只有局域网内的用户才能访问路由器。假如有特殊需要，这个功能可以远程访问控制路由器。



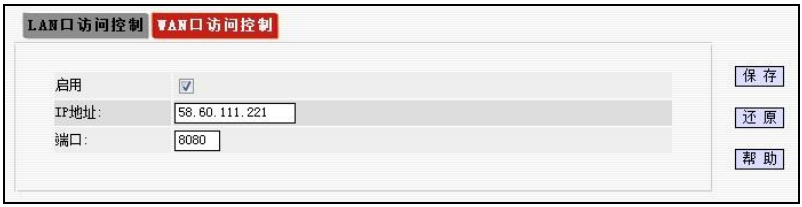

- 启用：开启 WAN 口访问控制路由器功能。
- IP 地址：输入访问控制路由器 WAN 口的 IP 地址。
- 端口：默认端口为 8080，输入您访问路由器 WEB 界面的端口号。

**注意：**

1. 路由器默认的 WAN 口访问控制可以根据需求进行修改，您必须用“IP 地址（此 IP 地址为路由器 WAN 口 IP 地址）端口”的方式( 例如路由器 WAN 口 IP 为 211.23.1.2, 则输入 http://211.23.1.2:8080 ）才能登录路由器执行远程管理。
2. 路由器默认的 WAN 口访问控制 IP 地址为 0.0.0.0，当启用时，广域网中所有计算机都能登录路由器执行远端 WEB 管理，如果您改变了默认的 IP 地址（例如改为 58.60.111.221 ），则广域网中只有具有指定 IP 地址（例如 58.60.111.221 ）的计算机才能登录到路由器管理页面。

**例如：**路由器的 WAN 口的 IP 地址为默认的 58.251.88.90，您仅允许 IP 地址为

58.60.111.221 的客户机，通过端口 8080 访问控制路由器 WEB 界面，则需要设置如下参数，且路由器的访问地址也更改为：http:// 58.251.88.90:8080

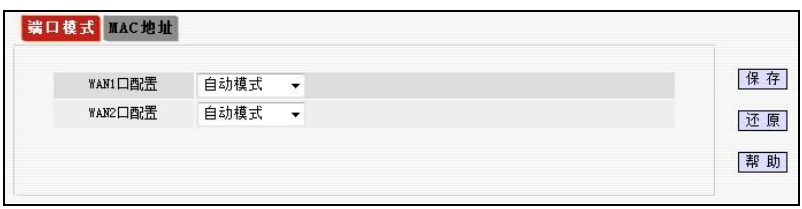



### 4.2.7 端口参数设置

在“端口参数设置”菜单下面，有“端口模式”、“MAC 地址”两个子项，单击某个子项，您即可进行相应的功能设置。

## 端口模式

本页设置各 WAN 口工作模式。



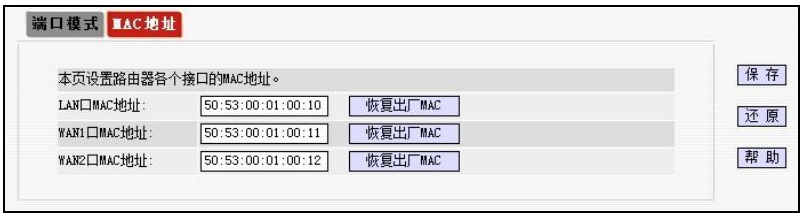

您可以按照需要分别设置 WAN1 和 WAN2 口的端口模式 :自动模式、10M 半/全双工、100M 半/全双工。

**⚠注意：**

WAN 口的工作模式必须与 WAN 口对端端口的工作模式一致，否则可能导致该 WAN 口无法正常收发数据。如果您不清楚 WAN 口对端端口的工作模式，请选择自动模式。

#### 4.2.8 MAC 地址

本页设置路由器各个接口的 MAC 地址。




- LAN 口 MAC 地址：显示路由器的 LAN 口 MAC 地址，可手动输入 MAC 地址。
- WAN2/WAN2 口 MAC 地址：显示路由器的 WAN1/WAN2 口 MAC 地址，可手动输入 MAC 地址。

**⚠注意：**

1. 某些 ISP（网络服务商）会绑定用户计算机的 MAC 地址，请将当前管理者的计算机的 MAC 地址，复制到对应 WAN 口 MAC 地址栏或手动更改 MAC 地址。修改此值后，运行状态中的 WAN 口 MAC 地址将会改变。
2. 修改 WAN 口 MAC 地址后，需重新启动路由器才会生效，如 ISP（网络服务商）没有绑定您的路由器的 MAC 地址，请不要使用此功能，以免出现其它问题。

## 4.3 用户管理

#### 4.3.1 基本设置

**用户上网控制**

当您将“用户上网方式控制”设置为“不需要认证”的时候，网络中的用户可以不用验证身份就能访问 Internet 资源。


当您的网络需要用户进行身份验证后才可以使用的时候，请将“用户上网方式控制”设置为“需要认证”，这时，您可以看到本路由器提供两种客户端上网认证方式：PPPOE 认证和 WEB 认证。


允许上网的方式：

PPPOE 用户直接上网 :当用户需要访问外网时 ,需要使用 PPPOE 拨号方式连接到本路由器。

允许 web 认证上网 :当用户需要访问外网时 ,需要在 WEB 浏览器弹出的对话框中输入正确的用户名和密码。

关闭 WEB 认证页面时：选中此项后，当用户关闭 WEB 认证页面时，用户就不能访问外网了。

用户账号到期提前通知：设置用户账号到期之前的通知时间。

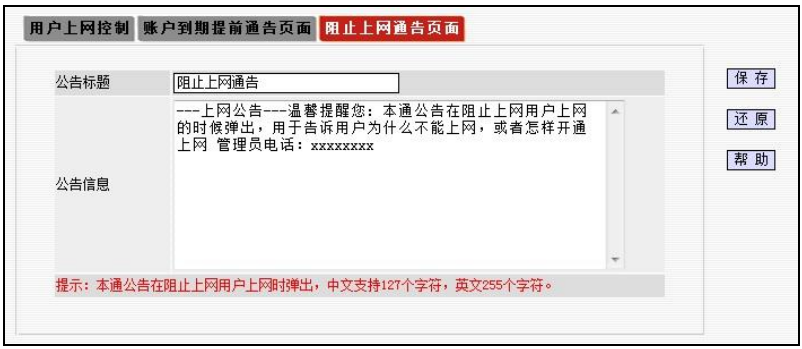
不需要认证的内部主机：设置一些特权 IP 地址，使用这些 IP 地址的客户端不需要进行身份认证就可以访问外网。

**账户到期提前通告页面**

在此页面设置的信息，将用来提示用户的账号即将到期，使用户能及时了解自己的账号使用情况，以便于用户提前续费而不影响使用。

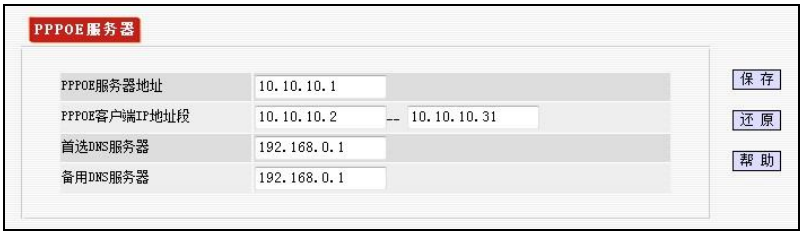

**阻止上网通告页面**

当用户不能访问外网的时候，显示的信息将会是此页面设置的信息。




### 4.3.2 PPPoE 管理

当客户端使用 PPPoE 拨号连接到本路由器时，本路由器的 PPPoE 服务器将会分配一些网络参数给客户端，分配出去的参数在此页面进行设置。




PPPoE 服务器地址：本路由器内置 PPPoE 服务器的 IP 地址。

PPPoE 客户端 IP 地址段：可以分配给客户端用的 IP 地址范围。

首选 DNS 服务器/备用 DNS 服务器：给客户端指定的 DNS 服务器 IP 地址。

### 4.3.3 用户管理

此页面用来添加 PPPoE 服务器/WEB 认证使用的用户账号，只有当客户端使用的账号与此页面中添加的账号相同，并且认证方式一致时，用户才能访问外网。


“查找”按钮，方便您查找已经添加到列表中的账号。

“添加用户”按钮，点击后，进入添加用户账号页面：


用户状态：账号的启用/禁用状态。

登录方式：账号用于哪一种认证方式。

用户名/密码：用于验证用户身份的账号。

MAC 地址：设置客户端 MAC 地址与账号是否绑定。

到期时间：设置账号的使用时间。

IP 地址：设置账号是否绑定一个固定的 IP 地址。

上行流量：此账号最大的上传速率。

下行流量：此账号最大的下载速率。

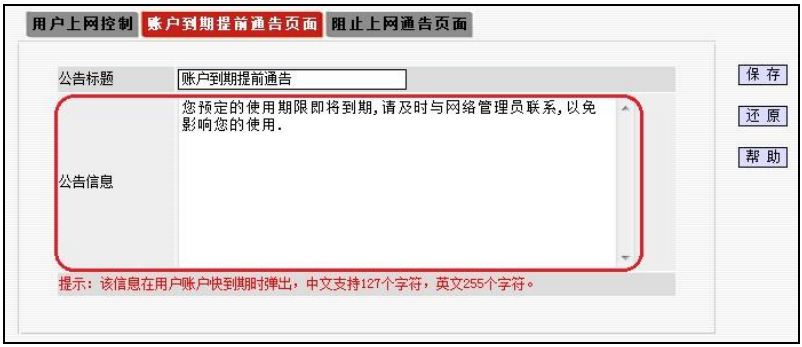
**用户管理设置示例：**

目的：提供一个 PPPoE 账号（Client1/12345678）给用户上网使用，且用户预定的上网带宽为 2M，上网时间为 2 个月，超过预定期限后，提示用户预定的使用期限已到，如需继续使用，请与网络管理员联系。

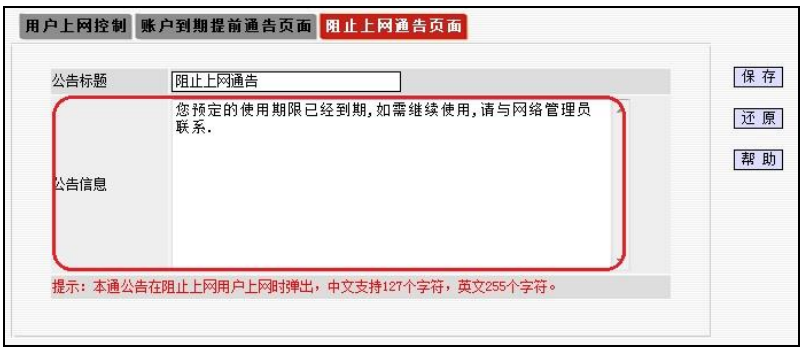
设置步骤：

1. 进行路由器的管理页面后，选择“用户管理” → “基本设置”，并且按下图所示进行设置：


2. 选择“账户到期提前通告页面”选项卡，按下图所示进行设置：




3. 选择“阻止上网通告页面”选项卡，按下图所示进行设置：




4. 选择“用户管理” → “用户管理”，点击“添加用户”按钮，并且按下图所示进行设置：


保存配置后，在“用户管理”页面中显示如下：

## 4.4 行为管理

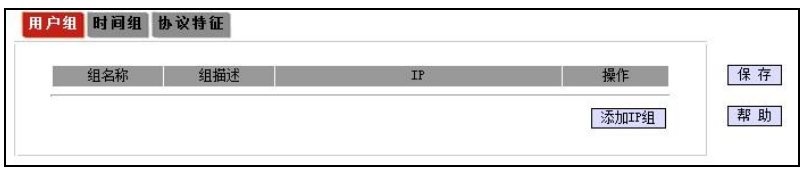
在“行为管理”菜单下面，共有“组设置”、“客户端过滤”、“URL 过滤”和“带宽&连接数设置”四个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。


### 4.4.1 组设置

在“组设置”菜单下面，有“用户组”、“时间组”和“协议特征”三个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

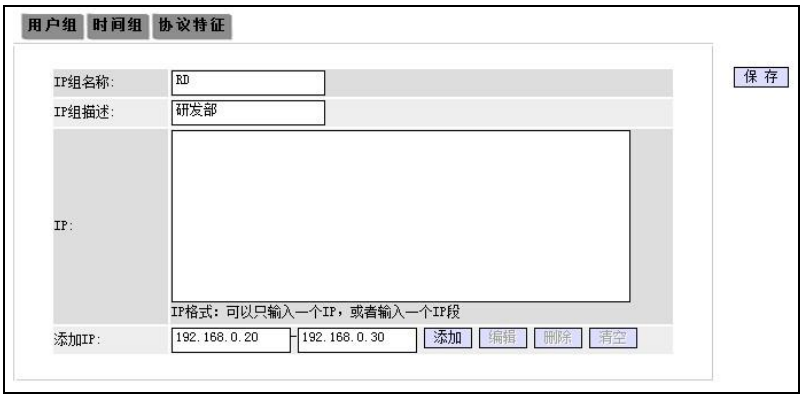
**用户组**

您可以通过添加 IP 组名称、IP 组描述以及合适的 IP 或者 IP 段来设置 IP 组。设置好的 IP 组将与上网行为管理的各个子功能配合使用。




比如公司研发部的 IP 段为：192.168.0.20-192.168.0.30，将研发部配置为一个 IP 组

的方法为，点击“添加 IP 组”。

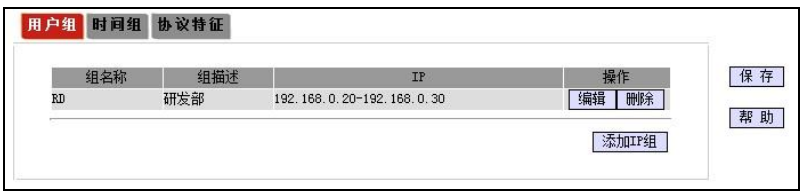



1、 IP 组名称：RD

2、 IP 组描述：添加注释“研发部”。

3、添加 IP：192.168.0.20-192.168.0.30

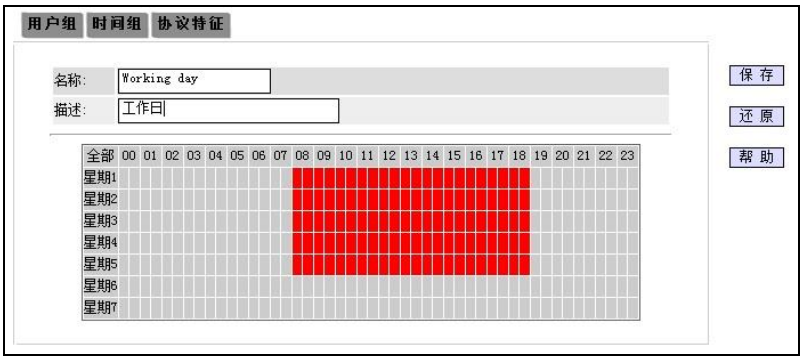
4.点击“添加”并保存后出现如下的界面




**时间组**

您可以通过添加时间组名称、时间组描述以及需要选择合适的时间或者时间段来设置时间组。


比如将工作日星期一到星期五的 8：00-18：00 设置成一个时间组，点击“添加时间组”。




1、名称：Working day

2、描述:工作日

3、时间段：星期一到星期五的 8：00-18:00

4、点击保存会出现如下界面


**协议特征**

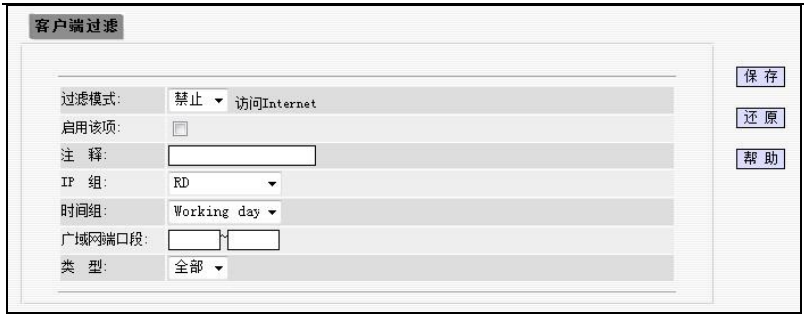
该页面显示可以被过滤的游戏和炒股软件的信息。


| 编号 | 对象名 | 备注 |
|---|---|---|
| 1 | thx | 同花顺 |
| 2 | ql | 钱龙 |
| 3 | dzh | 大智慧 |
| 4 | qqsj | QQ世界 |
| 5 | lzsj | 联众世界 |
| 6 | ppkdc | 跑跑卡丁车 |
| 7 | jwt | 劲舞团 |
| 8 | my | 魔域 |
| 9 | zhx | 诛仙 |
| 10 | zht | 征途 |
| 11 | ppt | 泡泡糖 |
| 12 | wmsj | 完美世界 |

### 4.4.2 客户端过滤

为了方便您对局域网中的计算机进行进一步管理，您可以通过数据包过滤功能来控制局域网中计算机对互联网上某些端口的访问。


点击“添加过滤规则”，会出现如下界面：

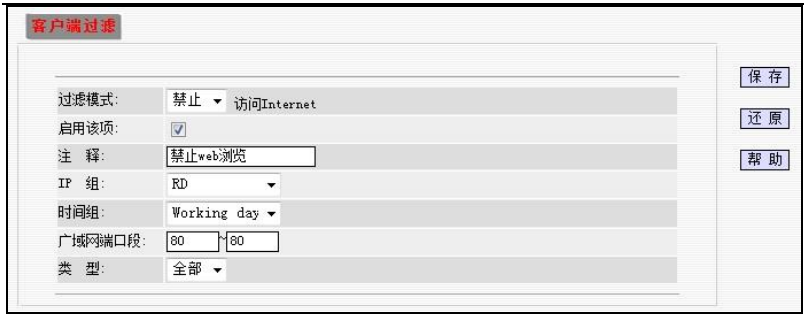



- 过滤模式：更改客户端过滤模式，有“禁止”和“允许”两种选项。

  禁止：禁止符合规则的数据包通过路由器，其它没有被限制的数据包，由设置的默认规则决定。

  允许：允许符合规则的数据包通过路由器，其它没有被限制的数据包，由设置的默认规则决定。
- 启动该项：启动该项过滤。
- 注释：即为此配置文件定义的简单描述。
- IP 组：选择用户组里面添加的 ip 组。
- 时间组：选择用户组里面添加的时间组。
- 广域网端口段：填入端口号，您可以指定一个端口范围，端口范围为 1-65535
- 类型：选择被控制的数据包所使用的协议（“全部”包括 TCP/UDP）；

例如 1：如果您希望局域网中 192.168.0.20-192.168.0.30（ip 组为 RD）的计算机在星期一到星期五的 8:00-18:00(时间组为 Working day)不能浏览 WEB 网站，对局域网中计算机不做其他任何限制，这时您需要设置如下：



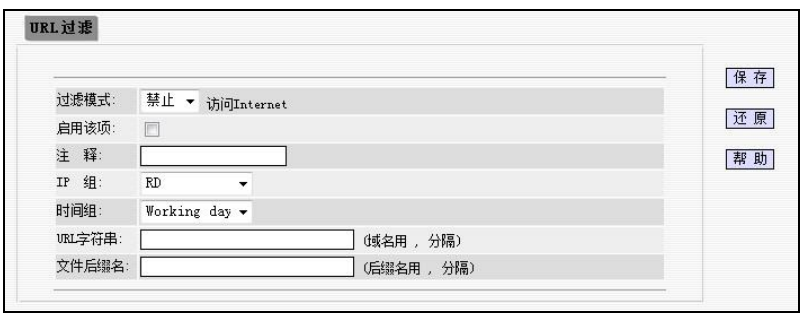

点击保存，出现如下界面


将默认规则设置成“允许”访问 Internet，勾选“启用”客户端过滤功能并保存，即可实现。

### 4.4.3 URL 过滤

为了方便您对局域网中的计算机所能访问的网站进行控制，您可以使用 URL 过滤功能来指定在什么时段不能访问哪些网站。


点击“添加过滤规则”，会出现如下界面：



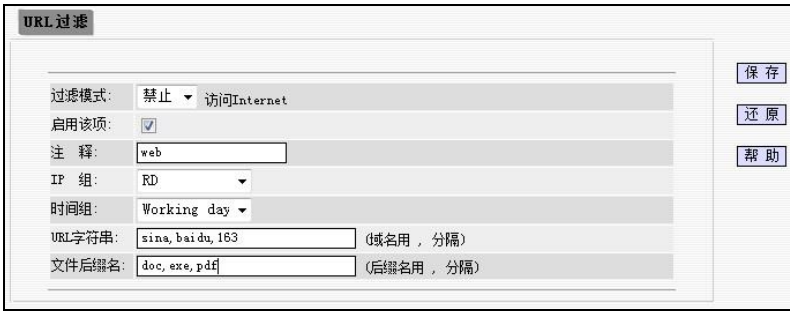

- 过滤模式：更改 URL 过滤的过滤模式，有“禁止”和“允许”两种选项。

  禁止：禁止符合规则的数据包通过路由器，其它没有被限制的数据包，由设置的默认规则决定。

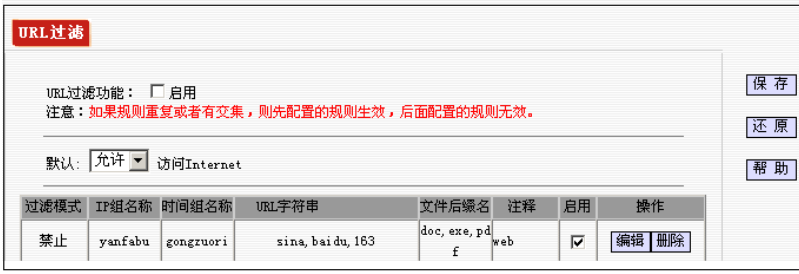
  允许：允许符合规则的数据包通过路由器，其它没有被限制的数据包，由设置的默认规则决定。
- 注释：即为此配置的简单描述。
- IP 组：选择用户组里面添加的 ip 组。
- 时间组：选择用户组里面添加的时间组。
- URL 字符串：填入被过滤的域名。
- 文件后缀名：下载文件的后缀名，如.exe、.pdf。

**例如：**如果您只禁止局域网中 IP 地址为 192.168.0.20~192.168.0.30（IP 组 RD）的计算机在星期一到星期五的 8:00-18:00(时间组 Working day)，不允许浏览包含“sina”，”

baidu”,” 163”字符串的 WEB 网站，，不允许通过 WEB 下载后缀名为.dos,.exe,.pdf 的文件，而可以访问其它网站，且其它计算机可以正常浏览所有的 WEB 网站。您需要设置如下参数：




点击保存，出现如下界面




将默认规则设置成“允许”访问 Internet，勾选“启用”客户端过滤功能并保存，即可实现。

### 4.4.4 宽带&连接数设置

在“宽带&连接数设置”菜单下面，有“带宽设置”和“连接数设置”两个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

**带宽设置**

带宽设置一共有两种模式：智能带宽管理和自定义带宽管理。


- 智能带宽管理：路由器根据当前实时流量，智能分配带宽，保证空闲时带宽的合理利用，线路繁忙时带宽的合理分配。路由器默认为智能带宽管理。
- 自定义带宽管理：您可以根据需要针对 IP 地址手动设置带宽。

自定义带宽管理可以限制内网计算机上网的通信流量 ,支持地址段的配置方式 ,点击“添加带宽限制”，会出现如下界面：


- 启用规则：启用该带宽设置规则。
- IP 地址段：流量控制的主机 IP 地址范围，可以是单个 IP，也可以是一个 IP 段。
- 上行限制：总流量，允许指定 IP 范围内的主机下载的最大总流量。

  p2p 流量，允许指定 IP 范围内的主机下载的最大 p2p 流量。
- 下行限制：总流量，允许指定 IP 范围内的主机下载的最大总流量。

  p2p 流量，允许指定 IP 范围内的主机下载的最大 p2p 流量。

- 上/下行模式：选择此范围内 IP 地址上/下行独享/共享带宽。
- 上/下行策略：选择此范围内 IP 地址上/下行固定/弹性带宽。
- 描述：对该规则的简单描述。

**⚠注意：**

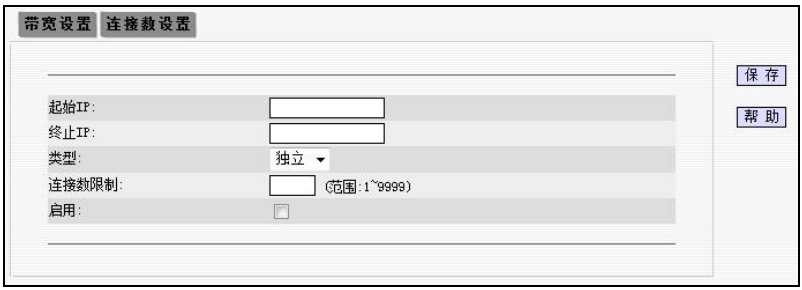
1. 上行限制/下行限制设置时请注意流量单位。

2. 如果您选择“当带宽有剩余时，可使用更多带宽”，路由器会动态弹性管理上/下行的流量，当有剩余带宽可利用时，可以超过您配置的上/下行带宽限制；当无剩余带宽可利用时，可以控制在您配置的上/下行带宽限制范围内。

**连接数设置**

本页设置单机的连接数限制。对指定 IP 地址的计算机连接数进行限制，超过限制的新连接不允许通过路由器，未指定的计算机可以不受限制的建立连接


点击“添加连接数限制”，会出现如下界面：



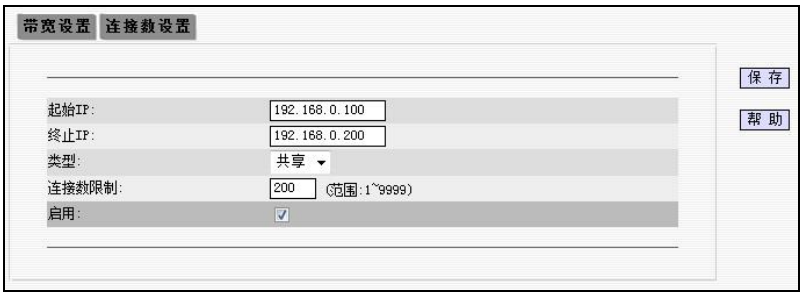

- 起始/终止 IP：输入要控制的 IP 地址段。
- 类型：选择连接数限制的类型。分为二种：独立和共享。

独立：是指对每个用户单独生效，限制每个用户的最大连接数；

共享：是指对组内的整体数据生效，限制整个用户组的连接数总和。

- 连接数限制：允许的最大连接数，设置范围为 1-9999。
- 启用：选择后启用此功能。

**例如：**内网 IP 地址段为 192.168.0.100-192.168.0.200 的计算机总共允许的最大连接为 200，这时您需要做如下图配置：



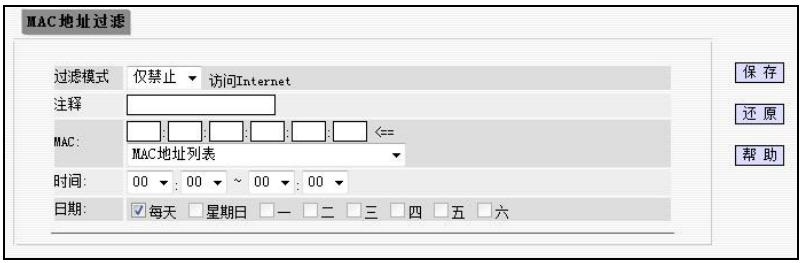
## 4.5 安全

在“安全”菜单下面，共有“MAC 地址过滤”、“ARP 防御”、“攻击防御”和“IP-MAC 地址绑定”四个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。


### 4.5.1 MAC 地址过滤

为了更好的对局域网中的计算机进行管理，您可以通过 MAC 地址过滤功能控制局域网中计算机对 Internet 的访问。


点击“添加过滤规则”，会出现如下界面：

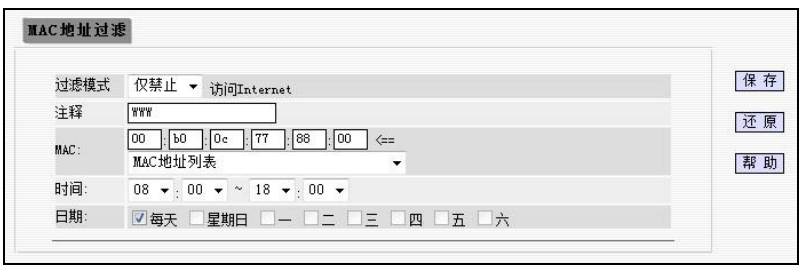


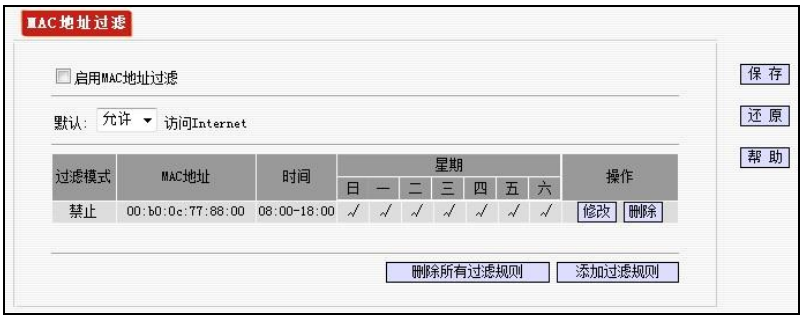

- 过滤模式：更改 MAC 地址过滤的过滤模式。

  仅禁止：只禁止所设置的规则的数据包通过路由器，其它没有被限制的数据包，由设置的默认规则决定。

  仅允许：仅允许所设置的规则的数据包通过路由器，其它没有被限制的数据包，由设置的默认规则决定。
- MAC:输入您要控制的 MAC 地址或直接选择 MAC 地址列表中的 MAC。
- 时间：填入您希望本条规则生效的起始时间和终止时间，如果不设置时间，默认显示为全 0，表示为 24 个小时。
- 日期：根据自身的要求选择相应的日期。

**例如 1：**如果您禁止局域网中 MAC 地址为 00:B0:0C:77:88:00 的计算机在每天 8:00-18:00 时间段内访问 Internet，而其它时段可以正常访问 Internet，，对局域网中其它计算机则不做任何限制，这时您需要设置如下参数：






点击“保存”并将默认设置为“允许”访问 Internet，然后点击“启用 MAC 地址过滤”即可实现。

### 4.5.2 ARP 防御

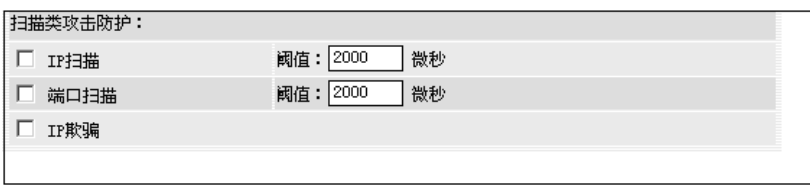
为了防止内网发生 ARP 攻击、欺骗，路由器默认开启了此功能，让您的网络更安全。ARP 广播间隔默认为一秒钟，可设置范围为 1-60 秒钟。

### 4.5.3 攻击防御

在“攻击防御”页面，共有“外网防御”和“内网防御”两个子项，下面将详细讲解各子项的详细功能。

**外网防御**

外网防御里有“扫描类攻击防护”、“DoS 类攻击防护”、“可疑包类防护”、“含有 IP 选项的包防护”和“其它防护”等五类防御。



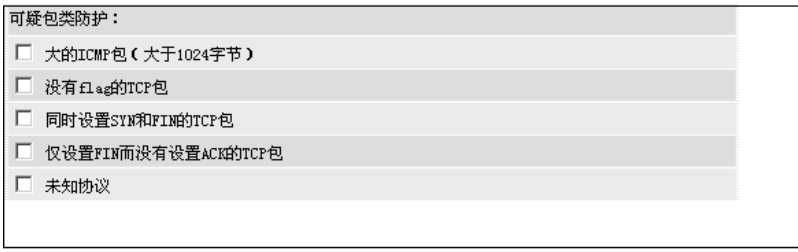

- IP 扫描：这是指在小于规定的时间内，一个源 IP 发送 ICMP 请求包到 10 个不同的目的 IP 地址，则被认为此源地址正在进行 IP 扫描攻击。
- 端口扫描：这是指在小于规定的时间内，一个源 IP 发送 TCP SYN 包到同一目的地址的 10 个不同端口，则被认为此源地址正在进行端口扫描攻击。
- IP 欺骗：选中 IP 欺骗复选框，表明检查来自指定区域的包是否正在进行 IP 欺骗。

**注意：**

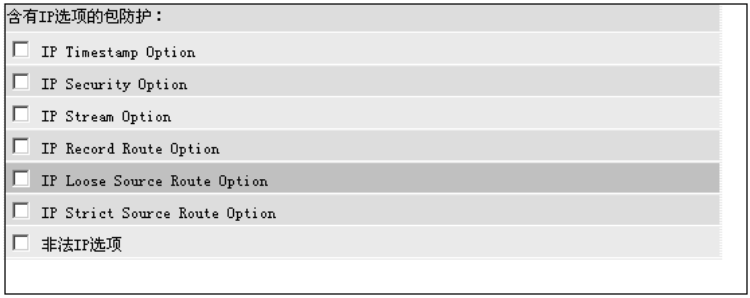
本功能仅在区域为 LAN 时有效，在区域为 WAN 时是无效的。


- ICMP Flood：这是指在一秒钟内，如果一个目的 IP 收到超过规定数量的 ICMP 请求包，则认为此目的 IP 正受到 ICMP Flood 的攻击。

- UDP Flood：这是指在一秒钟内，如果一个目的 IP 的某一端口收到超过规定数量的 UDP 包，则认为此目的 IP 的此端口正受到 UDP Flood 的攻击。
- SYN Flood：这是指在一秒钟内，如果一个目的 IP 的某一端口收到超过规定数量的 TCP SYN 包，则认为此目的 IP 的此端口正受到 SYN Flood 的攻击。
- Land Attack：这是将 SYN Flood 攻击和 IP 欺骗结合在一起的攻击，当攻击者发送含有受害者 IP 地址的欺骗性 SYN 封包 ,将其作为目的和源 IP 地址时 ,就发生了 LAND 攻击。
- WinNuke：WinNuke 是针对网上运行 Windows 的任何计算机的 DoS 攻击。 攻击者将 TCP 片段（通常给设置了紧急[URG]标志的 NetBIOS 端口 139）发送给具有已建连接的主机。 这样就产生 NetBIOS 碎片重叠，从而导致运行 Windows 的机器崩溃。




- 大的 ICMP 包：ICMP 包一般不会大于 1024 字节，大于 1024 字节的 ICMP 包则认为是可疑包。
- 没有 flag 的 TCP 包：正常的 TCP 包包头至少设置有一个标志（flag）。未设置任何控制标志的 TCP 包是一个可疑包。
- 同时设置 SYN 和 FIN 的 TCP 包：在同一 TCP 片段包头中同时设置 SYN 和 FIN 控制标志是异常的 TCP 包。
- 设置 FIN 未设置 ACK 的 TCP 包：设置了 FIN 标志，而未设置 ACK 标志的 TCP 包是异常的 TCP 包。
- 未知协议：IP 包头中协议类型字段的 135 或更大值为保留的，尚未定义。 正是由于这些协议未定义，就无法事先知道某一特定的未知协议是善意的还是恶意的。对这些非标准协议，谨慎的态度是封锁这类未知的元素进入受防护网络。




- IP Timestamp Option：表明是否检查来自指定区域的 IP 包含有 Internet Timestamp 项。

  IP Security Option：表明是否检查来自指定区域的 IP 包含有 Security 项。

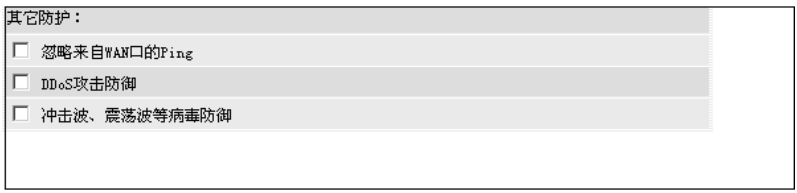
  IP Stream Option：表明是否检查来自指定区域的 IP 包含有 Stream ID 项。

  IP Record Route Option：表明是否检查来自指定区域的 IP 包含有 Record Route 项。

  IP Loose Source Route Option：表明是否检查来自指定区域的 IP 包含有 Loose Source Route 项。

  IP Strict Source Route Option：表明是否检查来自指定区域的 IP 包含有 Strict Source Route 项。

- 非法 IP 选项：表明是否检查来自指定区域的 IP 包的完整性或正确性。




- 忽略来自 WAN 口 Ping :启用此功能后路由器将不再回应来自 WAN 口的 Ping 检测。（默认启用）
- DDOS 攻击防御：启用此功能后路由器将阻止 DDNS 攻击。
- 冲击波、震荡波攻击防御: 启用此功能后路由器将阻止冲击波、震荡波攻击。

**内网防御**

内网防御里有“扫描类攻击防护”、“DoS 类攻击防护”、“可疑包类防护”、“含有 IP 选项的包防护”和“其它防护”等五类防御。


- IP 扫描：这是指在小于规定的时间内，一个源 IP 发送 ICMP 请求包到 10 个不同的目的 IP 地址，则被认为此源地址正在进行 IP 扫描攻击。
- 端口扫描：这是指在小于规定的时间内，一个源 IP 发送 TCP SYN 包到同一目的地址的 10 个不同端口，则被认为此源地址正在进行端口扫描攻击。
- IP 欺骗：选中 IP 欺骗复选框，表明检查来自指定区域的包是否正在进行 IP 欺骗。

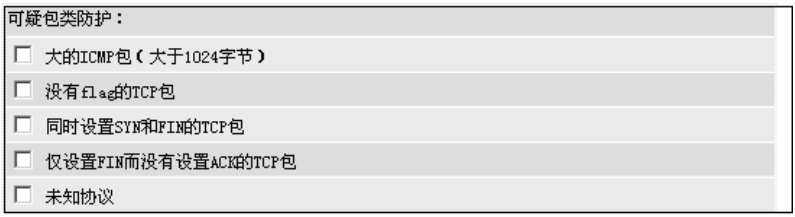
**注意：**

本功能仅在区域为 LAN 时有效，在区域为 WAN 时是无效的。

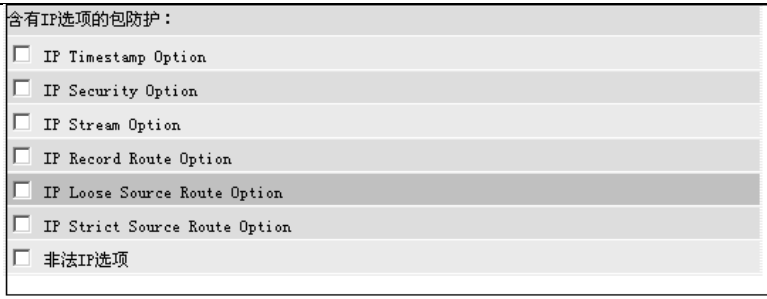

- ICMP Flood：这是指在一秒钟内，如果一个目的 IP 收到超过规定数量的 ICMP 请求包，则认为此目的 IP 正受到 ICMP Flood 的攻击。
- UDP Flood：这是指在一秒钟内，如果一个目的 IP 的某一端口收到超过规定数量的 UDP 包，则认为此目的 IP 的此端口正受到 UDP Flood 的攻击。
- SYN Flood：这是指在一秒钟内，如果一个目的 IP 的某一端口收到超过规定数量的 TCP SYN 包，则认为此目的 IP 的此端口正受到 SYN Flood 的攻击。
- Land Attack：这是将 SYN Flood 攻击和 IP 欺骗结合在一起的攻击，当攻击者发送含有受害者 IP 地址的欺骗性 SYN 封包 ,将其作为目的和源 IP 地址时 ,就发生了 LAND

攻击。

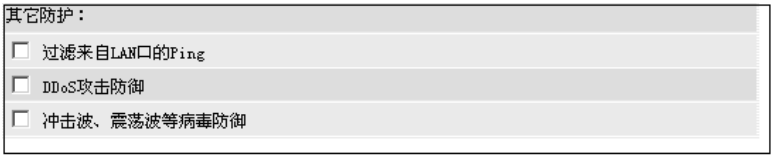
- WinNuke：WinNuke 是针对网上运行 Windows 的任何计算机的 DoS 攻击。 攻击者将 TCP 片段（通常给设置了紧急[URG]标志的 NetBIOS 端口 139）发送给具有已建连接的主机。 这样就产生 NetBIOS 碎片重叠，从而导致运行 Windows 的机器崩溃。




- 大的 ICMP 包：ICMP 包一般不会大于 1024 字节，大于 1024 字节的 ICMP 包则认为是可疑包。
- 没有 flag 的 TCP 包：正常的 TCP 包包头至少设置有一个标志（flag）。未设置任何控制标志的 TCP 包是一个可疑包。
- 同时设置 SYN 和 FIN 的 TCP 包：在同一 TCP 片段包头中同时设置 SYN 和 FIN 控制标志是异常的 TCP 包。
- 设置 FIN 未设置 ACK 的 TCP 包：设置了 FIN 标志，而未设置 ACK 标志的 TCP 包是异常的 TCP 包。
- 未知协议：IP 包头中协议类型字段的 135 或更大值为保留的，尚未定义。 正是由于这些协议未定义，就无法事先知道某一特定的未知协议是善意的还是恶意的。对这些非标准协议，谨慎的态度是封锁这类未知的元素进入受防护网络。




- IP Timestamp Option：表明是否检查来自指定区域的 IP 包含有 Internet Timestamp 项。IP Security Option：表明是否检查来自指定区域的 IP 包含有 Security 项。
- IP Stream Option：表明是否检查来自指定区域的 IP 包含有 Stream ID 项。
- IP Record Route Option：表明是否检查来自指定区域的 IP 包含有 Record Route 项。
- IP Loose Source Route Option：表明是否检查来自指定区域的 IP 包含有 Loose Source Route 项。
- IP Strict Source Route Option：表明是否检查来自指定区域的 IP 包含有 Strict Source Route 项。
- 非法 IP 选项：表明是否检查来自指定区域的 IP 包的完整性或正确性。




- 忽略来自 LAN 口 Ping：启用此功能后路由器将不再回应来自 LAN 口的 Ping 检测。
- DDOS 攻击防御：启用此功能后路由器将阻止 DDNS 攻击。
- 冲击波、震荡波攻击防御: 启用此功能后路由器将阻止冲击波、震荡波攻击。

### 4.5.4 IP-MAC 地址绑定

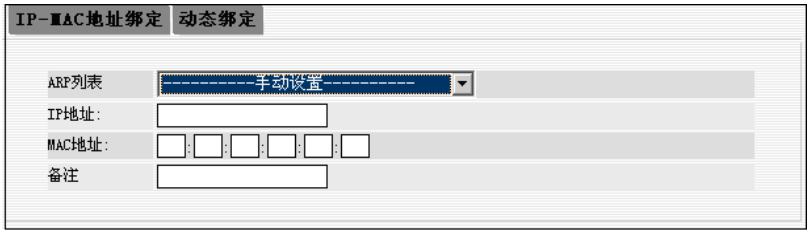
在“IP-MAC 地址绑定”菜单下面，共有“IP-MAC 地址绑定”和“动态绑定”两个子项，下面将详细讲解各子项的详细功能。

**IP-MAC 地址绑定**

本功能用于实现内网计算机的 IP 地址与 MAC 地址之间的绑定。地址绑定一旦配置完成后，指定的 IP 地址就只能被指定的计算机使用，解决了局域网中 IP 地址被随意改动而导致的 IP 地址冲突。

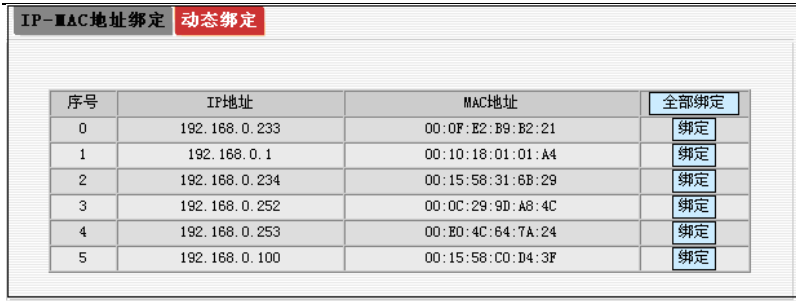

- 启动 IP-MAC 绑定：启动 IP-MAC 绑定功能。

点击“添加绑定”，会出现如下界面：




- ARP 列表：显示 ARP 表中相对应的 IP 和 MAC 地址，如需增加 IP 和 MAC 地址，需在 ARP 列表中选择“手动设置”选项。
- IP 地址：需绑定的 IP 地址。
- MAC 地址：需绑定的 MAC 地址。
- 备注：对该绑定条目的简单描述。

**动态绑定**



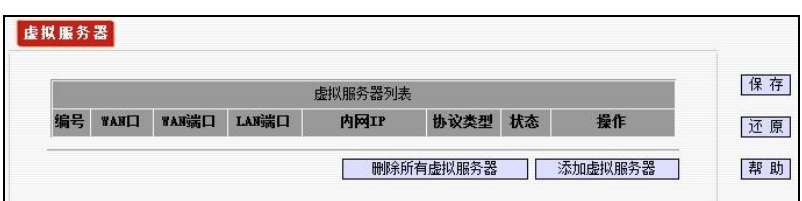

该动态绑定列表显示内网 ip 和对应 mac 地址的接入信息，您可以通过单个绑定或者全部绑定来快速实现 IP-mac 地址绑定。

## 4.6 高级

在“高级”菜单下面，共有“虚拟服务器”、“UPnP”、“DDNS”和“路由表”四个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。


### 4.6.1 虚拟服务器

虚拟服务器设置广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过 IP 地址指定的局域网网络服务器。




点击“虚拟服务器”按钮，添加设置：


- ✧ WAN 口：选择端口映射的 WAN 口。
- ✧ WAN 端口：WAN 服务端口，局域网内部 PC 端口对应映射到外部的端口。

  常用服务：常用服务的选项中列举了一些常用协议的端口，如 DNS（53）、FTP（21）、GOPHER(70)、HTTP(80)、NNTP(1190)、POP3(110)、PPTP(1723)、SMTP(25)、SOCK(1080)、TELNET(23)。

  对于常用服务端口中没有列出的端口，您也可以手动添加。
- ✧ LAN 端口：LAN 服务端口，即局域网内部 PC 的端口；
- ✧ 内网 IP：局域网中作为服务器的计算机的 IP 地址；
- ✧ 协议：包含 TCP、UDP 和全部。当您对使用的协议不确定时，可以选择全部。
- ✧ 启用：只有选中该项后本条目所设置的规则才能生效。

**例如：**您在内部局域网 IP 为 192.168.0.10 的计算机上搭建了一个 WEB 服务器，服务器使用端口为 80，如果需要实现在广域网以 http://x.x.x.x:40 访问到 WEB 服务器（x.x.x.x 为路由器 WAN2 IP 地址），就可以此页面中的“WAN 端口”中输入 40，“LAN 端口”中输入 80，“内网 IP”设置为 192.168.0.10，“协议”选择全部，选择启用，添加到列表保存后，即可生效。


**⚠注意：**

如果设置 WAN 端口为 80 的虚拟服务器，则需要将“网络”菜单中“WAN 口访问控制”的端口设置为 80 以外的值，如默认的 8080，否则会发生冲突，导致虚拟服务器不生效。

### 4.6.2 UPnP

支持最新的 Universal Plug and Play (UPnP 通用即插即用网络协议)，此功能需要 Windows ME/Windows XP 以上的操作系统(注：系统需集成，安装 Directx9.0 或更新版本)或支持 UPnP 的应用软件才能生效。

例如：Windows XP 系统上安装了迅雷等 P2P 软件 ,在上传和下载时可以利用 UPnP 协议。启用 UPnP 功能后，当启用迅雷时就可以看到端口转换信息，端口转换信息由应用程序发出请求时提供。


- ID：表示建立表项的序号。
- 远端主机：接受或发出响应的远端主机的描述。
- 外部端口：端口转换使用的路由器端口号。
- 内部主机：接受或发出响应的内部主机的描述。
- 内部端口：需要进行端口转换的主机端口号。
- 协议：表明是对 TCP 还是 UDP 进行端口转换。
- 描述：映射端口的软件信息

### 4.6.3 DDNS

本页设置动态的 DNS 的各种参数，当连接状态显示成功之后，互联网上的其它主机可以通过以域名的方式对您的路由器或虚拟服务器进行访问了。

本路由器对于每个 WAN 口都提供动态 DNS 配置，其配置方法完全相同，本说明书只对 WAN1 口设置进行说明。


- 开启动态 DNS：选择后启动此功能。
- 服务提供商：选择提供 DDNS 的服务提供商，可选择 3322.org 和 88ip.cn。
- 用户名：在 DDNS 服务器上注册的用户名。
- 密码：在 DDNS 服务器上注册的密码。
- 域名信息：在 DDNS 服务器注册的域名。
- 连接状态：当前和 DDNS 服务器的连接状态。

### 4.6.4 路由表

在“路由表”菜单下面，共有“路由表”和“静态路由设置”两个子项，下面将详细讲解各子项的详细功能。

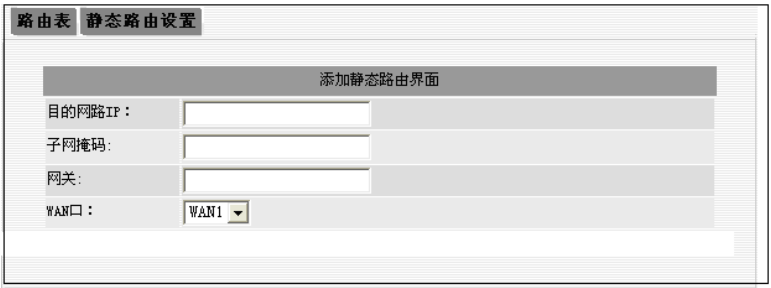
**路由表**

本页显示路由器路由表的内容。


| 目的IP | 子网掩码 | 网关 | metric | 接口 |
|---|---|---|---|---|
| 192.168.1.114 | 255.255.255.255 | 192.168.1.114 | 0 | eth2.2 |
| 239.255.255.250 | 255.255.255.255 | 0.0.0.0 | 0 | br0 |
| 192.168.1.0 | 255.255.255.0 | 0.0.0.0 | 0 | eth2.2 |
| 192.168.0.0 | 255.255.255.0 | 0.0.0.0 | 0 | br0 |
| 0.0.0.0 | 0.0.0.0 | 192.168.1.114 | 0 | eth2.2 |

**静态路由设置**

本页设置路由器的静态路由功能，点击“添加静态路由”，您可以指定静态路由规则。




- 目的网络 IP：目的主机的 IP 地址或目的网络的 IP 地址。
- 子网掩码：目的地址的子网掩码，一般为 255.255.255.0。
- 网关：下一跳路由器入口的 IP 地址。
- WAN 口：指定 WAN 口。

## 4.7 监控

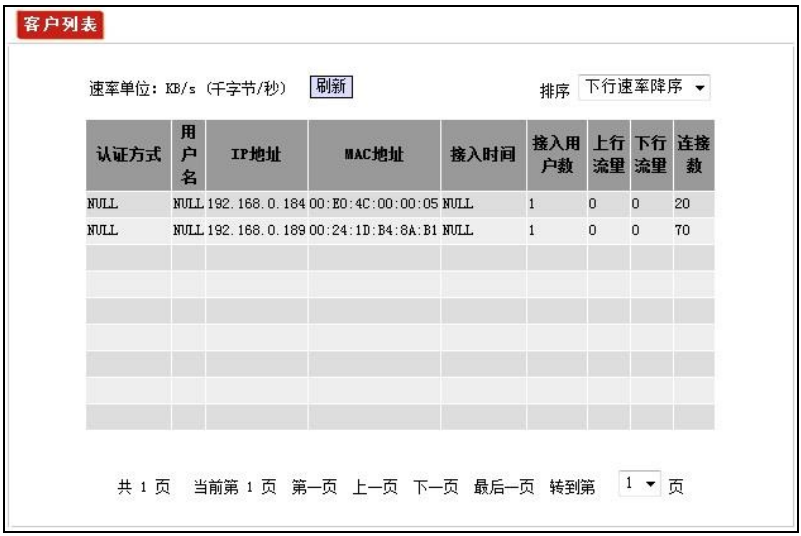
在“监控”菜单下面，共有“QQ 列表”、“客户列表”、“日志查看”” 和“日志设置”四个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。


### 4.7.1 QQ 列表

在此页面中，显示局域网中有哪些客户端已经登录 QQ 软件。

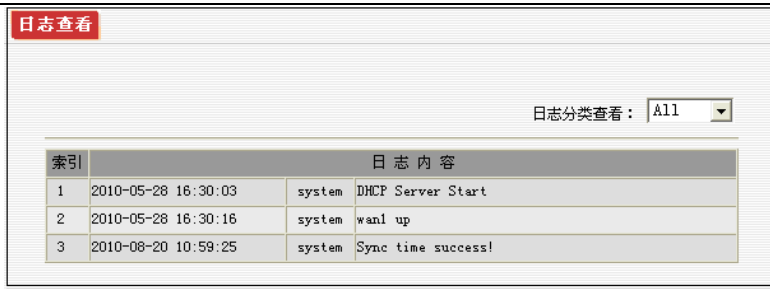
### 4.7.2 客户列表

在此页面中，显示局域网中有哪些客户已经连接到本路由器。



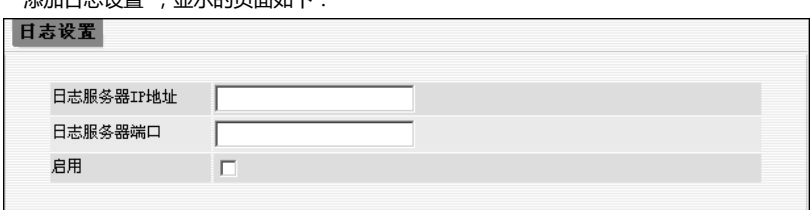

### 4.7.3 日志查看

在系统日志里，您可以查看系统启动出现的各种情况，也可以查看有无网络攻击发生。日志类型包括：All、system、Wan 口。




### 4.7.4 日志设置

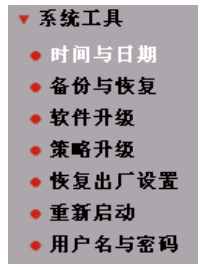
默认的情况下，当系统日志满 2000 条后，旧的记录将会被路由器自动清除。为了更完整的了解路由器的运行状态，日志设置功能可以把路由器的日志信息传给日志服务器，点击“添加日志设置”，显示的页面如下：



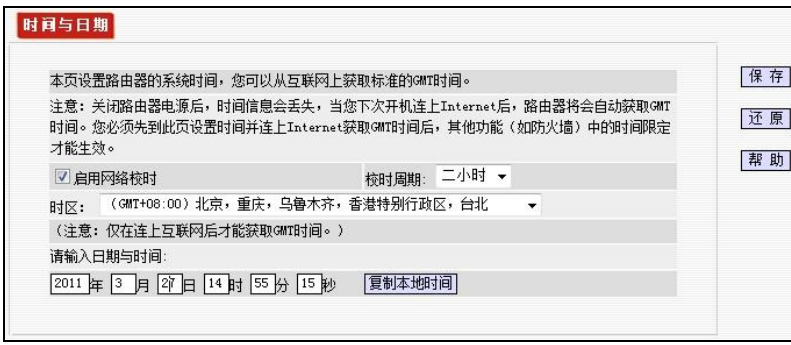

- 日志服务器 IP 地址：搭建日志服务器的 IP 地址。
- 日志服务器端口：日志服务器开启的服务端口。
- 启动：启动日志服务功能。

## 4.8 系统工具

在“系统工具”菜单下面，共有“时间与日期”、“备份与恢复”、“软件升级”、“策略升级”、“恢复出厂设置”、“重新启动”和“用户名和密码”七个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。




### 4.8.1 时间与日期



您可以选择自己设置时区从互联网上获取标准的 GMT 时间。当连上互联网后才能获取 GMT 时间，您也可以手动输入当前的时间。

- 启用网络校时：系统时间从网络上自动获取。
- 校时周期：系统时间从网络校时周期，请根据您的需要进行选择，系统默认校时周期为二个小时。
- 时区：选择您当地的时区。

### 4.8.2 备份与恢复

在这里您可以备份当前或恢复以前的路由器设置。


备份/恢复设置步骤：

- 备份：单击“备份”，便出现导出配置页面，请指定保存配置文件的路径！选择确定可以在指定目录生成一个系统配置的备份文件。
- 恢复：选择正确的上传的系统配置文件后，点击“恢复”按钮，重新启动路由器后将可以恢复到备份的系统配置。

### 4.8.3 软件升级

通过升级本路由器的软件，您将获得更加稳定的路由器版本及增值的路由功能。


软件升级步骤：

- 浏览选择升级文件的路径，单击“升级”进行软件升级。
- 升级完成后，路由器将自动重新启动。

**⚠注意：**

升级过程不能关闭路由器电源，否则将导致路由器损坏而无法使用。升级成功后，路由器将自动重启。升级过程约数分钟，请耐心等候。

### 4.8.4 策略升级

通过升级本路由器的策略文件，您将获得更加稳定的过滤功能。


策略升级步骤：

- 点击“浏览”选择策略文件的路径，单击“升级”进行策略升级。

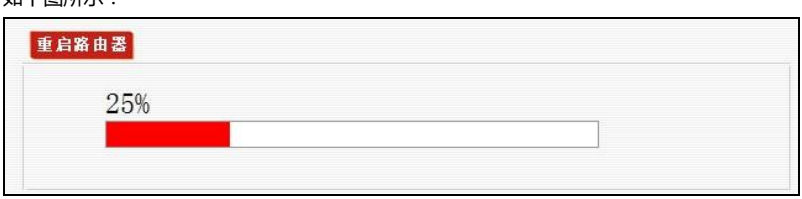
### 4.8.5 恢复出厂设置


单击“恢复出厂设置”按钮，将使路由器的所有设置恢复到出厂时的默认状态。

- 默认的用户名为：admin
- 默认的密码为：admin
- 默认的 IP 地址为：192.168.0.1
- 默认的子网掩码为：255.255.255.0
- 恢复出厂设置后，路由器重新启动才能生效

### 4.8.6 重新启动

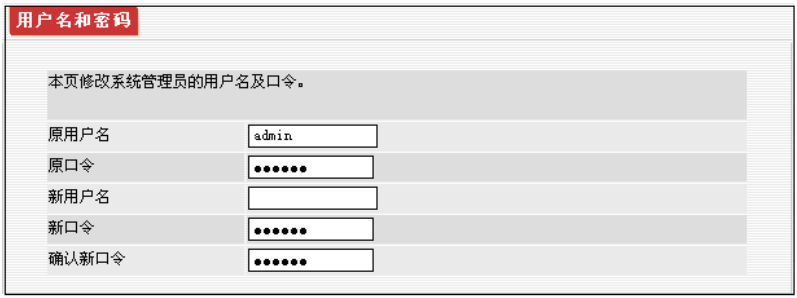
本界面提供的功能是从软件上重启路由器，路由器的重启过程大概需要 40 秒。界面如下图所示：




点击“重启路由器”按钮，将使一些需要重新启动才能生效的设置生效。路由器在重启

前，会自动断掉网络连接。

### 4.8.7 用户名和密码




- 本页修改系统管理员的用户名和口令。
- 请您首先输入新的用户名和原来的登陆口令，然后输入您希望使用的新的口令 ，如果您原来的用户口令输入无误的话，单击“保存”即可成功修改系统的用户名和口令。

**注意：**

出于安全考虑，我们强烈推荐您改变初始系统员用户名和密码。

## 4.9 退出登录

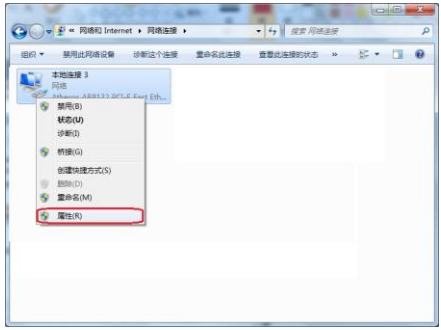
各项设置完成后请点击“退出登录”安全退出路由器的 WEB 管理页面。

# 5 附录一 TCP/IP地址设置方法（以Windows 7为例）

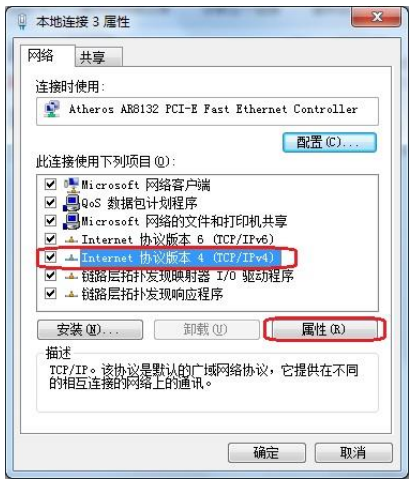
- 在您正在使用的桌面上，用右键单击“网络”，在弹出的菜单中选择“属性”；


- 在随后打开的窗口里，点击“更改适配器设置”；

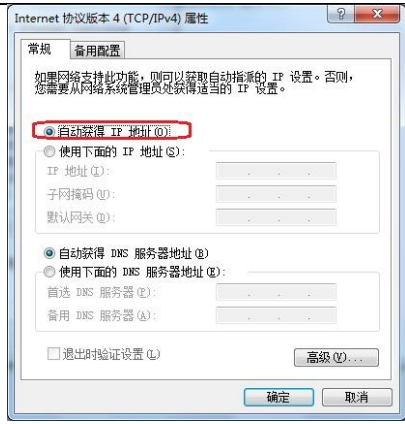

- 用鼠标右键点击“本地连接”，选择“属性”；



- 在弹出的对话框里，先选择“Internet 协议版本 4（TCP/IPv4）”，再用鼠标点击“属性”按钮；



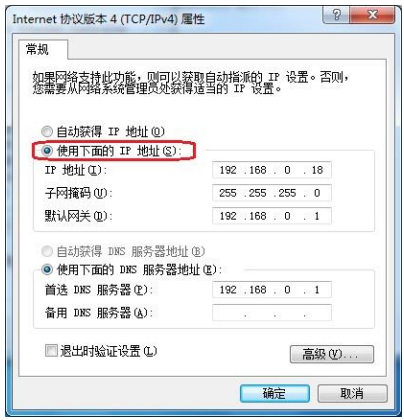

- 在随后打开的窗口里，您可以选择“自动获得 IP 地址（O）”或者是“使用下面的 IP 地址（S）”；
  - ✓ “自动获得 IP 地址（O）”如图：




✓ “使用下面的 IP 地址（S）”

设置您计算机的 IP 地址为 192.168.0.xxx(xxx 为 2~254)，子网掩码：255.255.255.0，网关：192.168.0.1，DNS 服务器：您可以填写您当地的 DNS 服务器地址（可咨询您当地的网络服务提供商）也可以由路由器作为 DNS 代理服务器。

设置完成后点击“确定”提交设置，再在本地连接“属性”中点击“确定”保存设置。




点击“确定”回到“本地连接 属性”对话框。

再点击“确定”退出设置界面。

在这一节中，我们介绍了如何为您的个人计算机配置 TCP/IP 协议。

请您确认已经在您的计算机中成功安装了网卡，如果没有，请参阅网卡的用户手册，正确安装网卡硬件及驱动程序。

# 6 附录二：常用命令介绍

| 常用命令 | 命令说明 |
| --- | --- |
| cmd | 运行此命令可快速进入 Windows 的命令行模式（适用与 Windows2000 以上操作系统） |
| ipconfig | 显示本机 IP 地址，如 ipconfig /all 查看 |
| ping | 这是 TCP / IP 协议中最有用的命令之一，它给另一个系统发送一系列的数据包，该系统本身又发回一个响应，这条实用程序对查找远程主机很有用，它返回的结果表示是否能到达主机，宿主机发送一个返回数据包需要多长时间。 |
| netstat | 能检验 IP 的当前连接状态，在断定您的基本通信正在进行后，就要验证系统上的服务。这个服务包括检查正在收听输入的通信量和 / 或验证您正在创建一个与远程站点的会话，它可以很轻松地做到这一点。 |
| tracert | Tracert 命令用来显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间。命令功能同 Ping 类似，但它所获得的信息要比 Ping 命令详细得多，它把数据包所走的全部路径、节点的 IP 以及花费的时间都显示出来。 |
| net stop | 停止 Windows NT 网络服务，<br>如：net stop dnscache |
| net send | 向网络的其他用户、计算机或通信名发送消息。要接收消息必须运行信使服务。 |