TP-LINK®

VPN 路由器

TL-R400VPN

用户手册

1910040146
Rev: 1.0.0

声明

目录

物品清单

请您小心打开包装盒，里面应有以下配件：

- 一台路由器
- 一根电源线
- 一本安装手册
- 一张保修卡
- 一张光盘
- 其它配件

注意：

如果发现有配件短缺或损坏的情况，请及时和当地经销商联系。

第1章 用户手册简介

在您准备安装使用本产品之前，请先仔细阅读本手册，以全面利用本产品的所有功能。

1.1 约定

本手册中所提到的路由器，如无特别说明，系指TL-R400VPN路由器，下面简称为TL-R400VPN。

本手册采用的图片中都配有相关参数，实际产品的配置界面并没有提供，请根据实际需要设置这些参数。

本手册中网络拓扑图中所采用的产品图片制作为组网时的参考，与产品实物可能有所差别，请以产品实物图为准。

用户在本用户手册中将会看到几种特殊的图形符号（图标），指出标识中的内容很重要，需要引起您的关注，本用户手册中使用的图标说明如下：

注意: 该图标表示这部分内容很重要，提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。

提示: 该图标为提醒您某些问题出现的可能原因。

举例: 该图标举例说明本设备，具体功能设置的步骤。

1.2 用户手册概述

第 1 章：用户手册简介。

第 2 章：产品概述。简述路由器的功能及主要特性。

第 3 章：硬件安装。帮助您进行路由器的硬件安装。

第 4 章：快速安装指南。帮助您配置路由器的基本网络参数。

第 5 章：配置指南。帮助您配置路由器的高级特性。

附录 A：FAQ。

附录 B：TCP/IP 的详细设置。

附录 C：技术参数表格。

第2章 产品概述

2.1 产品简介

TL-R400VPN是深圳市普联技术有限公司专为远程安全互联需求开发的 VPN 路由器产品，提供标准的 IPSec VPN 功能，最多可建立 5 条 VPN 隧道，适合中小型企业分支机构、机关单位、连锁机构等建立远程安全通信，此外该路由器还支持带宽控制、ARP 防护、DoS 攻击防护、访问控制、DDNS、虚拟服务器、中文 WEB 网管等丰富的功能特性，方便组建安全、高速及易管理的网络。

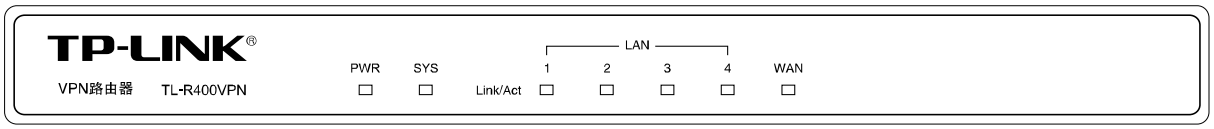
2.2 主要特性

- 支持 TCP/IP，DHCP，ICMP，NAT，PPPoE，SNTP，HTTP，DNS 等协议
- 提供 1 个 WAN 口 4 个 LAN 口，10/100Mbps 自适应，支持端口自动翻转（Auto MDI/MDIX）
- 支持标准的 IPSec VPN 功能，最多可建立 5 条 VPN 隧道
- 支持基于 IP 或基于端口的 QoS 设置，可限制单机带宽
- 支持 VPN Pass-through、UPnP 和 DDNS
- 支持虚拟服务器、特殊应用程序、DMZ 主机和静态路由等功能
- 提供攻击防护，可对网络攻击和病毒攻击进行防范
- 支持 IP 与 MAC 地址绑定，有效防范 ARP 攻击
- 支持 MAC 地址修改和克隆
- 提供系统日志功能，支持配置文件备份与载入
- 支持 Web 和远程管理，全中文配置界面，支持在线升级
- 内置电源，桌面型壳体

第3章 硬件安装

3.1 面板布置

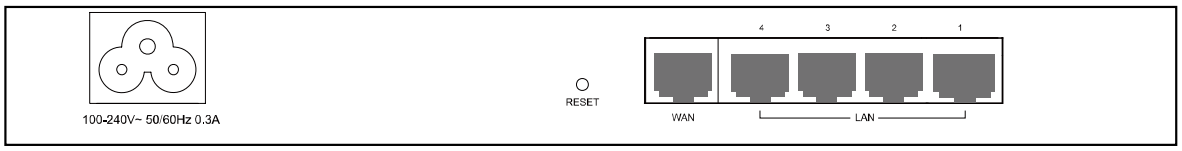
3.1.1 前面板



指示灯：

指示灯	描述	功能
PWR	电源指示灯	常亮表示系统正在运行
SYS	系统指示灯	闪烁表示系统正常
		常亮或常灭表示系统不正常
Link/Act	状态指示灯	常亮表示相应端口已正常连接
		闪烁表示相应端口正在进行数据传输

3.1.2 后面板



- **WAN** 1 个广域网端口(RJ45)。连接 xDSL/Cable Modem 或以太网。
- **LAN** 4 个 RJ45 接口。计算机和集线器/交换机通过这个端口连入局域网。
- **RESET** 复位按钮，可以将设备恢复为出厂设置。复位方式：通电状态下长按 RESET 按钮，待系统指示灯闪烁 5 次后松开按钮，路由器将重启并恢复出厂设置。

注意:

在路由器未完全启动前，不能关闭电源，否则，配置有可能没有恢复到出厂默认值。

- **电源插孔** 这个插孔供您插接电源。电源规格为：100-240V~ 50/60Hz 0.3A。如果使用不匹配的电源，可能会导致路由器损坏。

3.2 系统需求

- 宽带 Internet 服务（接入方式为 xDSL/Cable Modem 或以太网）
- 具有以太网 RJ45 连接器的调制解调器（直接接入以太网时不需要此物件）
- 每台 PC 的以太网连接（网卡和网线）

- TCP/IP 网络软件（Windows 95/ 98/ ME/ NT/ 2000/ XP/ VISTA/ 7 自带）
- Internet Explorer 5.0 或更高版本

3.3 安装环境

安装环境要求：

1. 将路由器水平放置。
2. 尽量将路由器放置在远离发热器件处。
3. 不要将路由器置于太脏或潮湿的地方。
4. 电源插座请安装在设备附近便于触及的位置，以方便操作。

路由器推荐使用环境：

- 温度：0 ºC～40 ºC
- 湿度：5％～90％RH，无凝结

3.4 硬件安装步骤

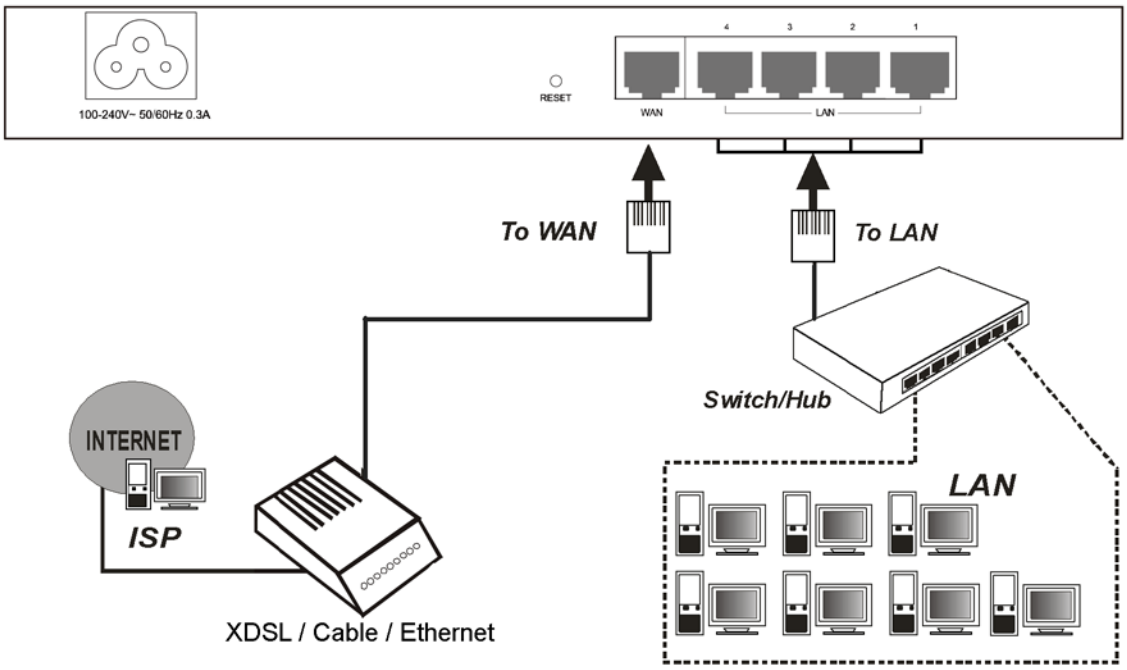
在安装路由器前，请确认是否能通过宽带服务访问网络。如果无法访问，请先和您的网络服务商（ISP）联系解决问题。成功访问网络后，请遵循以下步骤安装您的路由器。安装时拔除电源插头，保持双手干燥。

1) 建立局域网连接

用一根网线连接路由器的 LAN 口和局域网中的集线器或交换机，如下图所示。也可以用一根网线将路由器与计算机网卡直接相连。

2) 建立广域网连接

用网线将路由器 WAN 口与 Internet 相连，如下图所示。



注意:

以上网络拓扑图为您进行网络设置的参照用例，您可以根据实际情况，实际需求配置适合您的网络构架。

3) 连接电源

将电源连接好，路由器将自行启动。

第4章 快速安装指南

如果对路由器进行基本配置，请阅读本章内容；如果进行高级配置，请继续阅读第 5 章内容。

4.1 建立正确的网络设置

路由器默认 IP 地址是 192.168.1.1，默认子网掩码是 255.255.255.0。这些值可以根据实际需要而改变，但本用户手册上将按默认值说明。

首先请将计算机接到路由器的局域网端口，接下来可以使用两种方法为您的计算机设置 IP 地址。

方法一：手动设置 IP 地址。

设置计算机的 TCP/IP 协议。如果已经正确设置完成，请跳过第一步。

设置计算机的 IP 地址为 192.168.1.xxx（xxx 范围是 2 至 254），子网掩码为 255.255.255.0，默认网关为 192.168.1.1。

方法二：利用路由器内置 DHCP 服务器自动设置 IP 地址。

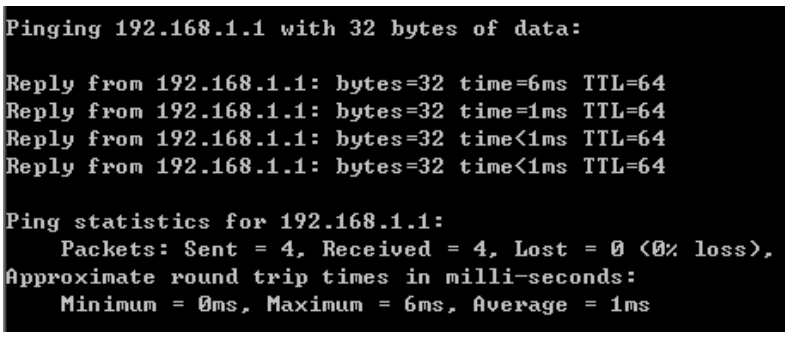
设置计算机的 TCP/IP 协议为“自动获取 IP 地址 ”。

在设置好 TCP/IP 协议后，使用 Ping 命令检查计算机和路由器之间是否连通。下面的例子为一个在 Windows XP 环境中，执行 Ping 命令，操作步骤如下：

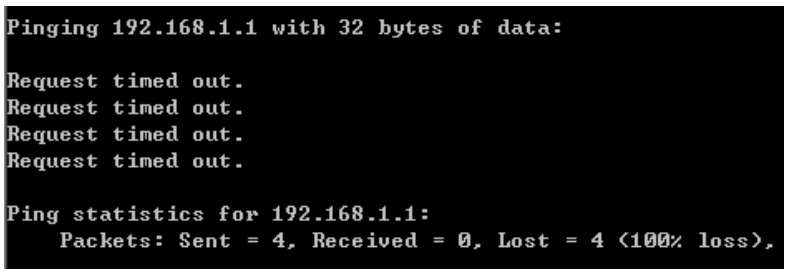
首先请点击桌面的“开始”菜单，再选择“运行”选项，并在随后出现的运行输入框内输入 cmd 命令，然后回车或点击“确认”键即可进入下图所示界面。

最后在该界面中输入命令 Ping 192.168.1.1，其结果显示如下。

如果屏幕显示为：



那么计算机已与路由器成功建立连接。如果屏幕显示为：



这说明设备还未安装好，请按照下列顺序检查：

1） 硬件连接是否正确？

提示：

路由器面板上对应局域网端口的 Link/Act 指示灯和您计算机上的网卡灯必须亮。

2） 您的计算机的 TCP/IP 设置是否正确？

提示：

如果路由器的 IP 地址为 192.168.1.1，那么您的计算机 IP 地址必须为 192.168. 1.xxx（xxx 范围是 2~254）。

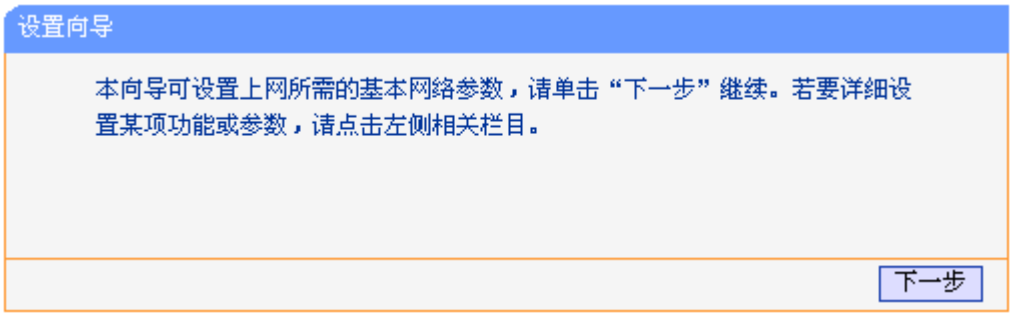
4.2 快速安装指南

本产品提供基于浏览器（Internet Explorer 或 Netscape Communicator）的配置界面，这种配置方案适宜于任何 MS Windows，Macintosh 或 UNIX 平台。

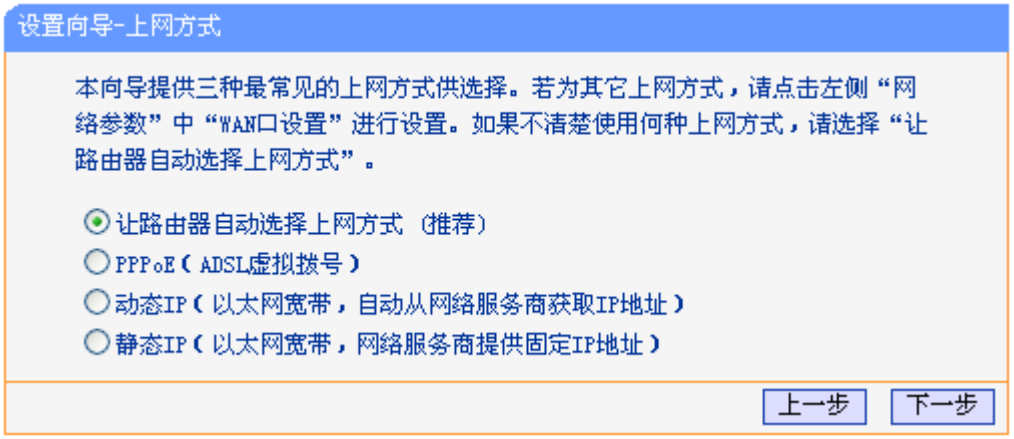
激活浏览器，取消“使用代理服务器”选项或者将路由器的 IP 地址添加到“代理服务器设置”中的“例外”栏中（在 IE 中选择“工具－Internet 选项－连接－局域网设置”，就可以找到这些设置）。接着在浏览器的地址栏里输入路由器的 IP 地址，例如 http://192.168.1.1。

连接建立后将会看到下图所示登录界面。输入用户名和密码（用户名和密码的出厂设置均为“admin”），然后单击确定按钮。

成功登录后会弹出一个设置向导的画面（如果没有自动弹出，可以单击管理员模式画面左边“设置向导”菜单将它激活）。



单击“下一步”，进入上网方式选择画面。



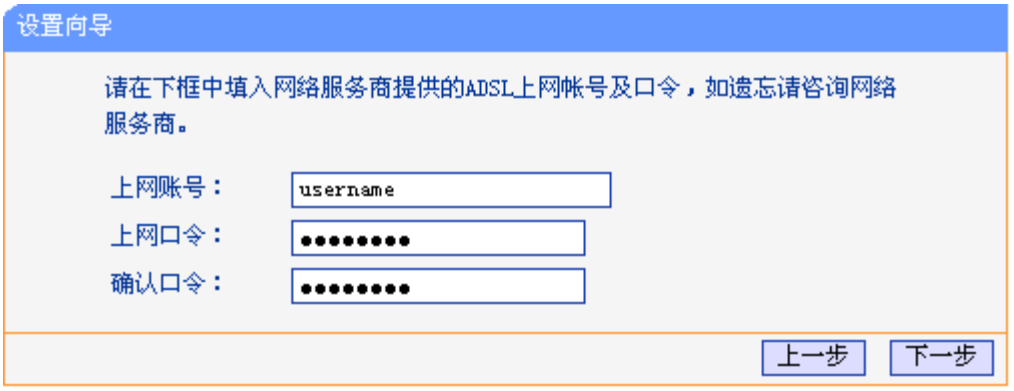
以上画面显示了最常用的三种上网方式，请根据 ISP 提供的上网方式进行选择，然后单击“下一步”填写上网所需的基本网络参数。

◆ **让路由器自动选择上网方式（推荐）**

选择该选项后，路由器会自动判断上网类型，然后跳到相应上网方式的设置页面。为了保证路由器能够准确判断上网类型，请保证路由器已正确连接。

◆ **使用要求用户名和密码的 ADSL 虚拟拨号方式（PPPoE）**

如果上网方式为 PPPoE，即 ADSL 虚拟拨号方式，ISP 会提供上网帐号和口令，在下图所示页面中填写内容：



◆ **从网络服务商获取由 DHCP 自动分配的 IP 地址（动态 IP）**

如果上网方式为动态 IP，则可以自动从网络服务商获取 IP 地址，点击**下一步**完成设置。

◆ **使用网络服务商提供的固定 IP 地址（静态 IP）**

如果上网方式为静态 IP，网络服务商会提供 IP 地址参数，在下图所示页面中输入 ISP 提供的参数，若有不明白的地方请咨询网络服务商。

IP 地址： 本路由器对广域网的 IP 地址，即 ISP 提供的 IP 地址，不清楚可以向 ISP 询问。

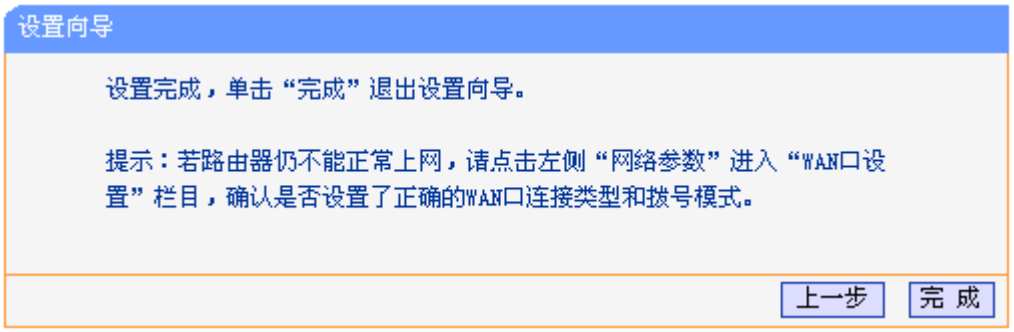
子网掩码： 本路由器对广域网的子网掩码，即 ISP 提供的子网掩码，一般为 255.255.255.0。

网关： 填入 ISP 提供的网关参数，不清楚可以向 ISP 询问。

DNS 服务器： 填入 ISP 提供的 DNS 服务器地址，不清楚可以向 ISP 询问。

备用 DNS 服务器： 可选项，如果 ISP 提供了两个 DNS 服务器地址，可以把另一个 DNS 服务器地址的 IP 地址填于此处。

设置完成后，单击**下一步**，将弹出下图所示的设置向导完成界面，单击**完成**退出设置向导。



第5章 配置指南

5.1 启动和登录

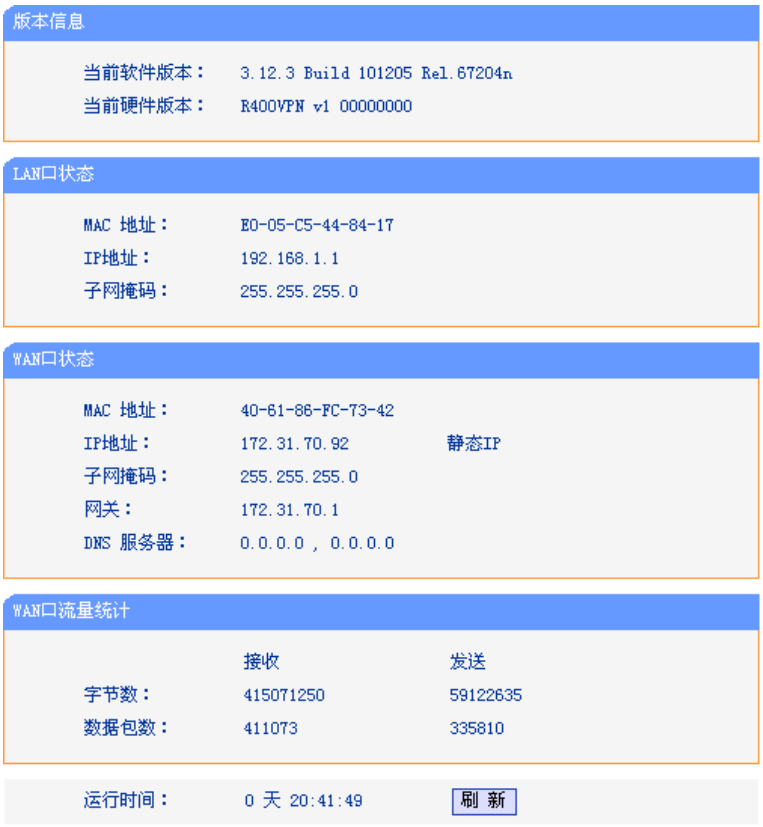
在启动和登录成功以后，浏览器会显示管理员模式下的路由器配置页面。

在左侧菜单栏中，共有“运行状态”、“设置向导”、“网络参数”、“DHCP 服务器”、“VPN”、“转发规则”、“安全策略”、“路由功能”、“QoS”、“IP 与 MAC 绑定”、“动态 DNS”和“系统工具”十二个菜单。单击某个菜单项，即可进行相应的功能设置。

在使用过程中，如果您对本产品的功能有任何疑问，您只需单击该页面的“帮助”按钮，即可获得详细的联机帮助。

下面将详细讲解各个菜单的功能。

5.2 运行状态



本页显示路由器的工作状态。

- **版本信息** 此处显示当前的软、硬件版本。
- **LAN 口状态** 此处显示当前 LAN 口的 MAC 地址、IP 地址和子网掩码。
- **WAN 口状态** 此处显示当前 WAN 口的 MAC 地址、IP 地址、子网掩码、网关和 DNS 服务器。同时 IP 地址右侧将显示用户上网方式（PPPoE/动态 IP/静态 IP）。如果用户的上网方式为 PPPoE（ADSL 拨号上网）的话，当用户已经连接上 Internet 时，此处将会显示用户的上网时间和“断线”按钮，单击此按钮可以进行即时的断线操作，当用户未连接 Internet 时，此处将会显示“连接”按钮，单击此按钮可以进行即时的连接操作。
- **WAN 口流量统计** 此处显示当前 WAN 口接收和发送的数据流量信息。

5.3 设置向导

请参考第 4 章的快速安装指南。

5.4 网络参数

在“网络参数”菜单下面，共有“LAN 口设置”、“WAN 口设置”和“MAC 地址克隆”三个子项。单击其中某个子项，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。

5.4.1 LAN 口设置

选择网络参数下的 LAN 口设置项，将进入 LAN 口的设置界面，如下图示。请按照下面各子项说明设置该 LAN 口的参数。

- **MAC 地址** 设置路由器对局域网的 MAC 地址。
- **IP 地址** 请输入本路由器对局域网的 IP 地址。该 IP 地址出厂默认值为 192.168.1.1，请根据实际需要设置该值。
- **子网掩码** 本路由器对局域网的子网掩码，可以在下拉列表中选择 B 类（255.255.0.0）或者 C 类（255.255.255.0）地址的子网掩码。一般情况下选择 255.255.255.0 即可。

注意:

如果您改变了此处 LAN 口的 IP 地址，则您必须用新的 IP 地址才能登录路由器管理界面，并且局域网中所有计算机的默认网关也必须设置为该 IP 地址，这样才能正常上网。

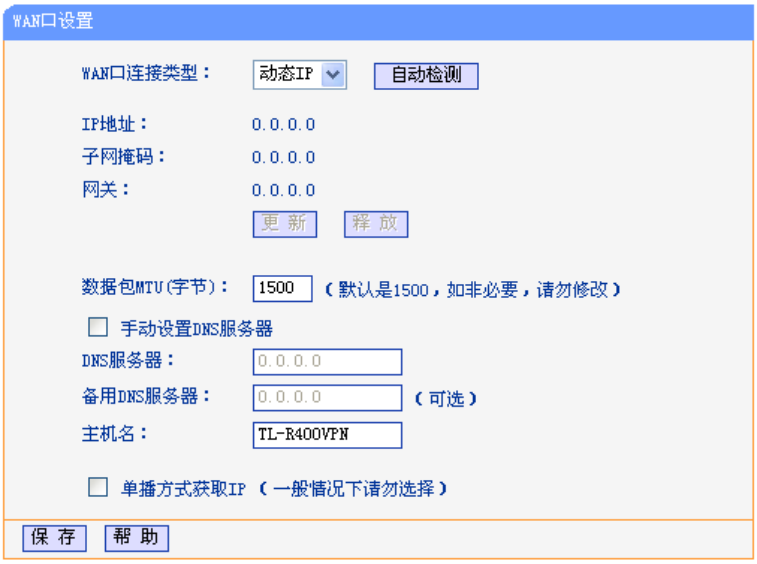
局域网中所有计算机的子网掩码必须与此处子网掩码相同。

5.4.2 WAN 口设置

选择网络参数下的 WAN 口设置项，将进入 WAN 口的设置界面（默认为动态 IP 设置界面），如下图示。首先请选择 WAN 口的连接类型，即上网方式。本路由器默认上网方式为“动态 IP”。

5.4.2.1 动态 IP

如果选择的 WAN 口连接类型是“动态 IP”，即可以从网络服务商（ISP）自动获取 IP 地址，其设置界面如下图示。请按照下面各子项说明，设置相应的参数。



- **WAN 口连接类型** 上图中选择的是“动态 IP”上网方式。本路由器支持三种常用的上网方式：动态 IP、静态 IP、PPPoE 方式，请根据实际情况选择。
- **IP 地址** 显示从 ISP 的 DHCP 服务器动态得到的 IP 地址，它是路由器对广域网的地址。
- **子网掩码** 显示从 ISP 的 DHCP 服务器动态得到的子网掩码。
- **网关** 显示从 ISP 的 DHCP 服务器动态得到的网关。
- **数据包 MTU** 请输入需要限制的数据包的最大长度（MTU），可以输入的范围是 576～1500，默认值为 1500。若非必要，请不要修改该默认值。
- **手动设置 DNS 服务器** 选择该复选框，可以手动设置自己想要的 DNS 服务器地址。
- **DNS 服务器** 显示从 ISP 的 DHCP 服务器动态得到的 DNS 服务器地址，也可以在此处手动设置想要的 DNS 服务器地址。
- **备用 DNS 服务器** 显示从 ISP 的 DHCP 服务器动态得到的备用 DNS 服务器地址，也可以在此手动设置想要的备用 DNS 服务器地址，可以不选。
- **单播方式获取 IP** 如果的 ISP 服务器支持以单播方式获取 IP 地址，请选择该复选框，将以单播的方式从 ISP 获取 IP 地址。

注意：

单播方式获取 IP 是指主机以点对点的单播包向指定的 DHCP 服务器请求分配 IP 地址。大多数网络服务商的 DHCP 服务器支持广播的请求方式，只有少数是支持单播的请求方式。如果您在网络连接正常的情况下无法获取 IP 地址，可以选择单播的方式（一般情况下不要选择此项）。

- **按钮功能** 包括“自动检测”、“更新”和“释放”按钮。
- 自动检测 点击此按钮，路由器能检测动态 IP、静态 IP 和 PPPoE 三种上网方式，检测结果仅供参考，确切的上网方式请咨询 ISP。

- 更新　　单击此按钮，可以从 ISP 的 DHCP 服务器更新 WAN 口的 IP 地址、子网掩码、网关、DNS 服务器等设置。
- 释放　　单击此按钮，本路由器将发送 DHCP 释放操作到 ISP 的 DHCP 服务器，释放 IP 设置。

设置完上面的参数后，点击保存按钮，设置的参数将生效。

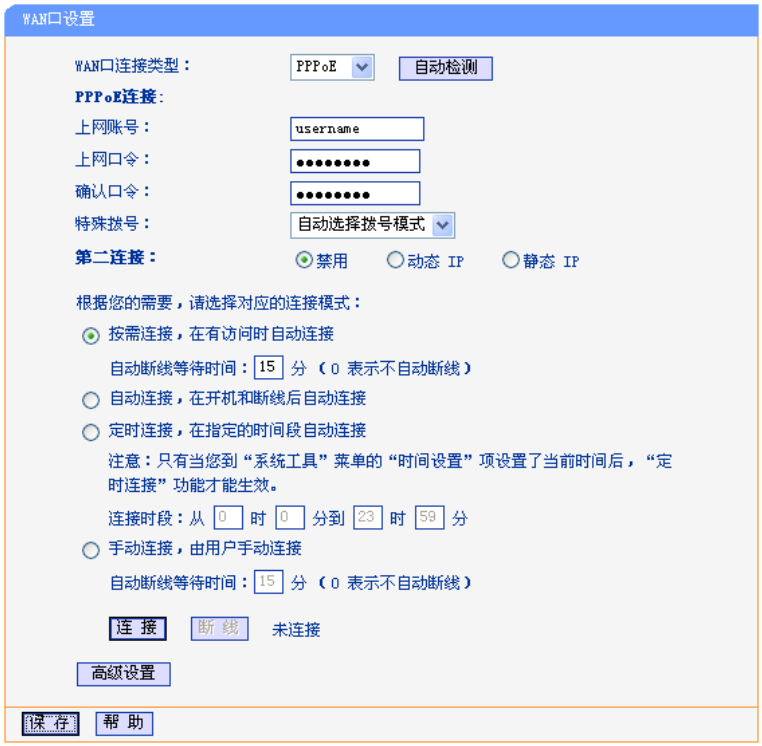
5.4.2.2 静态 IP

如果选择的 WAN 口连接类型是“**静态 IP**”,即 拥有网络服务商（ISP）提供的固定 IP 地址，其设置界面如下图示。请按照下面各子项说明设置相应的参数。

- **IP 地址**　　请输入 ISP 提供的固定 IP 地址，它是路由器对广域网的 IP 地址，不清楚可以向 ISP 询问。
- **子网掩码**　　请输入 ISP 提供的子网掩码，它是路由器对广域网的子网掩码，一般为 255.255.255.0。
- **网关**　　请输入 ISP 提供的网关，不清楚可以向 ISP 询问。
- **数据包 MTU**　　请输入需要限制的数据包的最大长度（MTU），可以输入的范围是 576～1500，默认值为 1500。若非必要，请不要修改该默认值。
- **DNS 服务器**　　请输入 ISP 提供的一个 DNS 服务器地址，不清楚可以向 ISP 询问，也可以不填。
- **备用 DNS 服务器**　　请输入 ISP 提供的另一个 DNS 服务器地址，也可以不填。

5.4.2.3 PPPoE

如果选择的 WAN 口连接类型是“**PPPoE**”，即可以从网络服务商（ISP）自动获取 IP 地址时，其设置界面如下图示。请按照下面各子项说明设置相应的参数。



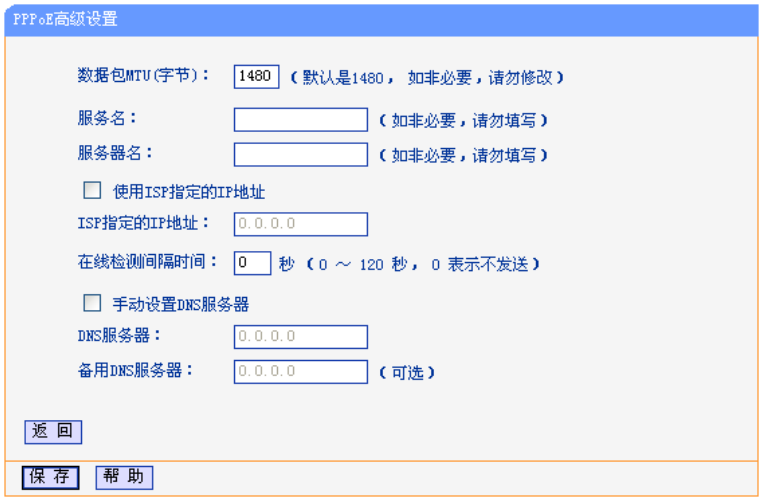
- **拨号模式选择** 此项默认为正常拨号模式，但是由于某些地区运营商局端设备的限制，可能导致正常拨号模式下 PPPoE 无法连接成功，在此情况下您可以依次尝试 6 种特殊拨号模式。
- **上网帐号** 请输入 ISP 指定的 ADSL 上网帐号，不清楚可以向 ISP 询问。
- **上网口令** 请输入 ISP 指定的 ADSL 上网口令，不清楚可以向 ISP 询问。
- **第二连接：** 如果 ISP 还提供了以动态 IP 或静态 IP 的方式连接到局域网的连接，请选择“动态 IP”或“静态 IP”来启动这个连接。
- **按需连接：** 若选择按需连接模式，当有来自局域网的网络访问请求时，系统会自动进行连接。若在设定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。对于采用按使用时间进行交费的用户，选择按需连接可以有效节省上网费用。
- **自动断线等待时间：** 如果自动断线等待时间 T 不等于 0(默认时间为 15 分钟)，则在检测到连续 T 分钟内没有网络访问流量时自动断开网络连接，保护上网资源。此项设置仅对“按需连接”和“手动连接”生效。
- **自动连接：** 在开机后系统自动连接网络。在使用过程中，如果由于外部原因网络被断开，系统就会主动尝试连接，直到成功连接。若网络服务是包月交费形式，推荐选择该项连接方式。
- **定时连接：** 系统在连接时段的开始时刻主动进行网络连接，在终止时刻自动断开网络连接。选择此连接模式，可以有效控制内网用户的上网时间。
- **手动连接：** 开机或断线后，在此处或个人计算机中手动拨号连接。若在指定时间内(自动断线等待时间)没有任何网络请求时，系统会自动断开连接。若网络服务是按时间交费，选择手动连接可有效节省上网费用。
- **连接/断线：** 单击此按钮，可进行即时的连接/断线操作。

注意:

只有当您在“系统工具”的“时间设置”项，设置了当前时间后，“定时连接”功能才能生效。

您可以根据需要选择上面 4 种连接方式中的任意一种，设置完后可以点击保存按钮，使设置生效。

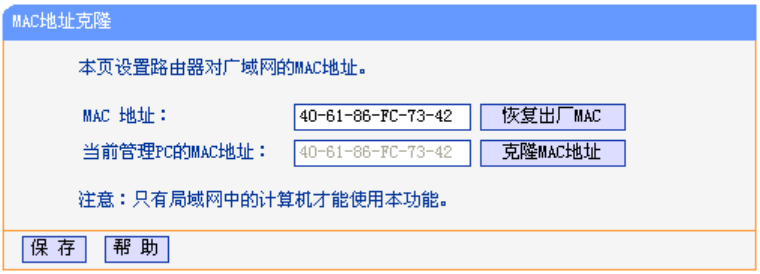
您还可以根据实际需要，进入到“高级设置”界面对相关设置项进行设置、调整。其设置界面如下图示，您可以按照下面各子项说明设置相应的参数。



- **数据包 MTU** 请输入需要限制的数据包的最大长度（MTU），默认值为 1492。若非必要，请不要修改该默认值。
- **服务名** Service Name，若不是 ISP 特别要求，请不要填写。
- **服务器名** AC Name，如果不是 ISP 特别要求，请不要填写。
- **使用 ISP 指定的 IP 地址** 选中复选框，可以设置 ISP 提供的指定 IP 地址。
- **ISP 指定的 IP 地址** 请输入 ISP 提供的指定 IP 地址。
- **在线检测时间间隔** 请根据需要填写所需的在线检测时间间隔。路由器将根据该时间间隔发送检测信号，以检测服务器是否在线。若该值为 0，则表示不发送检测信号。如果在系统日志中经常发现有“接收 PADT,服务端请求断开本次连接”这样的日志信息时，请将该值设为 0。
- **DNS 服务器** 请输入 ISP 提供的一个 DNS 服务器地址，不清楚可以向 ISP 询问，也可以不填。
- **备用 DNS 服务器** 请输入 ISP 提供的另一个 DNS 服务器地址，也可以不填。

5.4.3 MAC 地址克隆

选择网络参数下的 MAC 地址克隆项，将进入下面的设置界面，如下图示。请按照下面各子项说明正确使用该功能。



- **MAC 地址** 显示当前路由器对广域网的 MAC 地址，此值一般不用更改。但某些 ISP 可能要求对 MAC 地址进行绑定，此时 ISP 会提供一个有效的 MAC 地址给用户，您只要根据它所提供的值，输入到“MAC 地址”栏，然后单击“保存”，即可根据 ISP 的要求更改本路由器对广域网的 MAC 地址。
- **恢复出厂 MAC** 若您要恢复本路由器对广域网的出厂默认 MAC 地址，则您可以单击此按钮来恢复。
- **当前管理 PC 的 MAC 地址** 显示当前正在进行管理操作的计算机的 MAC 地址。
- **克隆 MAC 地址** 单击此按钮，您即可把当前管理 PC 的 MAC 地址填入到“MAC 地址”栏内。

注意：

只有局域网中的计算机能使用“克隆 MAC 地址”功能。并且，任意两个 WAN 口的 MAC 地址不可以相同，否则将会导致不可预料的错误。

5.5 DHCP 服务器

DHCP 服务器主要用来自动配置和管理网络内部主机的 TCP/IP 参数。在“DHCP 服务器”菜单下面，有“DHCP 服务”、“客户端列表”和“静态地址分配”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。

5.5.1 DHCP 服务

选择 DHCP 服务器下的 DHCP 服务，将进入下面的设置界面。使用本路由器的 DHCP 服务器功能可以让 DHCP 服务器自动配置局域网中各计算机的 TCP/IP 协议。请按照下面各子项说明正确设置这些参数。

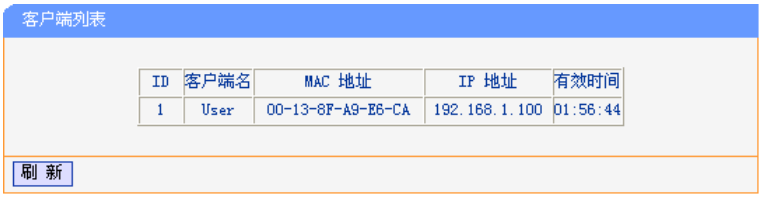
- **DHCP 服务器** 若想使用 DHCP 的自动配置 TCP/IP 参数功能，请选择启用。
- **地址池开始地址** 请输入 DHCP 服务器自动分配 IP 地址的起始地址。
- **地址池结束地址** 请输入 DHCP 服务器自动分配 IP 地址的结束地址。
- **地址租期** 请输入所分配 IP 地址的有效使用时间，超时将重新分配。
- **网关** 请输入路由器 LAN 口的 IP 地址，本路由器缺省是 192.168.1.1。
- **缺省域名** 请输入本地网域名，也可以不填。
- **主 DNS 服务器** 请输入 ISP 提供的 DNS 服务器地址，不清楚可以向 ISP 询问，也可以不填。
- **备用 DNS 服务器** 如果 ISP 提供了两个 DNS 服务器地址，则请输入另一个 DNS 服务器的 IP 地址，也可以不填。

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”。

5.5.2 客户端列表

选择 DHCP 服务器下的客户端列表，将进入下面界面。该客户端列表罗列了所有通过 DHCP 获得 IP 的主机信息，具体如下图示：



- **ID** 条目序号。
- **客户端名** 显示分配到 IP 地址的客户端的计算机名。
- **MAC 地址** 显示分配到 IP 地址的客户端的计算机的 MAC 地址。

- **IP 地址** 显示 DHCP 服务器分配给客户端的计算机的 IP 地址。
- **有效时间** 显示主机通过 DHCP 获得 IP 地址后，该 IP 地址剩余的有效时间。客户端软件会在租期到期前自动续约。

5.5.3 静态地址分配

选择 DHCP 服务器下的静态地址分配，将进入下面的设置界面。为了方便您对局域网中计算机的 IP 地址进行控制，本路由器内置了静态地址分配功能。它可以为指定 MAC 地址的计算机预留静态 IP 地址。之后，若此计算机请求 DHCP 服务器分配 IP 地址时，DHCP 服务器将自动给它分配此预留的 IP 地址。具体设置见下图示：

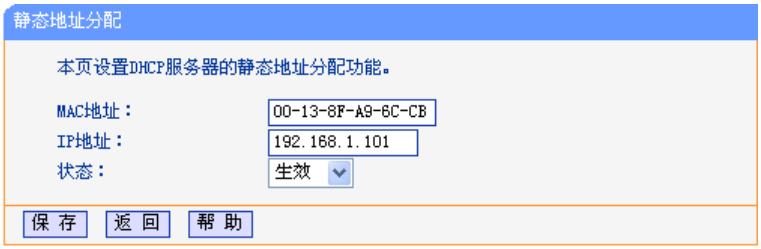
- **静态地址条目表** 显示静态地址条目信息。
- MAC 地址 显示预留了 IP 地址的计算机的 MAC 地址。
- IP 地址 显示预留的 IP 地址
- 状态 显示该条目是否生效。
- 配置 显示对该条目进行的超级链接——编辑或删除。
- **添加新条目** 单击该按钮，可以增加新的静态地址条目，详见后面所述。
- **使所有条目生效** 单机该按钮，可以使所有静态条目生效。
- **使所有条目失效** 单机该按钮，可以使所有静态条目失效。
- **删除所有条目** 单机该按钮，可以删除当前列表中的所有启用或未启用的静态条目。

注意：

此功能需要在重启路由器后才能生效。

5.5.3.1 添加或编辑静态地址

点击上图所示界面中的**添加新条目**或条目右侧的**编辑**按钮，将进入下面的设置界面。该页用来设置静态地址条目。



- **MAC 地址** 请输入预留了 IP 地址的计算机的 MAC 地址。
- **IP 地址** 请输入要预留的 IP 地址。
- **状态** 请选择该条目是否生效。

设置完以上三项后，点击保存按钮，该设置将会在静态地址条目表中显示。

5.6 VPN

在“VPN”菜单下，有“IKE”、“IPsec”和“安全联盟列表”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。

VPN (Virtual Private Network, 虚拟专用网)是一个建立在公用网（通常是因特网）上的专用网络，但因为这个专用网络只是逻辑存在并没有实际物理线路，故称为虚拟专用网。VPN 通过隧道技术在两个站点间建立一条虚拟的专用线路，使用端到端的认证和加密保证数据的安全性。隧道是通过对数据报的封装实现的，因为数据报封装和解封的过程都是在路由器上完成，所以对于用户来说是透明的。本路由器支持的隧道协议为三层隧道协议 IPsec VPN。

5.6.1 IKE

在 IPsec VPN 中，为了保证信息的私密性，通信双方需要使用彼此都知道的信息来对数据进行加密和解密，所以在通信建立之初双方需要协商安全性密钥，这一过程便由 IKE (Internet Key Exchange, 互联网密钥交换)协议完成。

整个 IKE 协商过程被分为两个阶段。第一阶段，通信双方将协商交换验证算法、加密算法等安全提议，并建立一个 ISAKMP SA，用于在第二阶段中安全交换更多信息。第二阶段，使用第一阶段中建立的 ISAKMP SA 为 IPsec 的安全性协议协商参数，创建 IPsec SA，用于对双方的通信数据进行保护。至此，IKE 协商完毕。

IKE 设置界面如下图所示。

5.6.1.1 添加或编辑 IKE 条目

点击上图所示界面中的**添加单个条目**或条目右侧的**编辑**按钮，将进入下面的设置界面。该页用来设置 IKE 安全策略条目。

- **安全策略描述** 为 IKE 安全策略命名。设置好的 IKE 安全策略可以被应用在 IPsec 安全策略中。

- **协商模式** 选择 IKE 的协商模式，通信双方必须使用相同的协商模式。在 IKE 协商的第一阶段定义了两种操作模式：主模式和野蛮模式。主模式中进行交换和认证的报文较多，并提供身份保护，适用于高安全性需求场合；野蛮模式中进行交换和认证的报文较少，不提供身份保护，但是协商速度快。

- **本地/对端 ID 类型** 当协商模式选择“野蛮模式”时，需要设置本地和对端的 ID (Identity, 身份标识)类型，用于进行 ID 的交换与验证，通信双方的设置需保持一致。

- **本地/对端 ID** ID 类型选择“IP 地址”时，无需进行设置；ID 类型选择“NAME”时，可自定义本地/对端的 ID。路由器的“本地 ID”需与通信对端的“对端 ID”保持一致，而“对端 ID”则需与通信对端的“本地 ID”保持一致。

- **验证算法** 选择应用于 IKE 会话的验证算法。路由器支持以下验证算法：

  MD5 (Message Digest Algorithm, 消息摘要算法)：对一段消息产生 128bit 的消息摘要，防止消息被篡改。

  SHA1 (Secure Hash Algorithm, 安全散列算法)：对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。

  AUTO 表示自动适应对端算法。若对端使用本路由器不支持的算法将会协商失败，双方不能建立 VPN 连接。若对端同是 AUTO 模式，则双方会默认使用 SHA1 验证算法。

- **加密算法** 选择应用于 IKE 会话的加密算法。路由器支持以下加密算法：

  DES (Data Encryption Standard, 数据加密标准)：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。

  AES (Advanced Encryption Standard, 高级加密标准)：AES128/192/256 表示使用长度为 128/192/256 bit 的密钥进行加密。

AUTO 表示自动适应对端算法。若对端使用本路由器不支持的算法将会协商失败，双方不能建立 VPN 连接。若对端同是 AUTO 模式，则双方会默认使用 AES256 加密算法。

- **DH 组** Diffie-Hellman 算法的组信息，用于产生加密 IKE 隧道的会话密钥。DH1/2/5 分别对应着 768/1024/1536 bit 的 DH 组。
- **预共享密钥** 当 IKE 协商模式选择“主模式”时，需设置通信双方互相认证的密钥，双方必须使用同一个预共享密钥。
- **生存时间** 设定 IKE 密钥的生存时间。
- **DPD 检测开启** DPD (Dead Peer Detect,对端存活检测)开启后，IKE 一端能够定时主动检测对端的在线状态。
- **DPD 检测时间周期** 当开启 DPD 检测时可设置检测周期。

注意:

使用 IKE 时，请确保 IPsec 连接两端的 IKE 设置一致，否则将无法通信。当本路由器的验证/加密算法设置为 AUTO 时，另一端验证/加密算法则可在本路由器支持的算法中任意选择。

5.6.2 IPsec

IPsec (IP Security, IP 安全性) 是一系列服务和协议的集合，在 IP 网络中保护端对端通信的安全性、防止网络攻击。

为了实现安全通信，通信双方的 IPsec 协议必须协商确定用于编码数据的具体算法、用于理解对方数据格式的安全协议，并通过 IKE 交换解密编码数据所需的密钥。

在 IPsec 中有两个重要的安全性协议 AH (Authentication Header, 鉴别首部)和 ESP (Encapsulating Security Payload, 封装安全性载荷)。AH 协议用于保证数据的完整性，若数据报文在传输过程中被篡改，报文接收方将在完整性验证时丢弃报文；ESP 协议用于数据完整性检查以及数据加密，加密后的报文即使被截取，第三方也难以获取真实信息。

IPsec 设置界面如下图所示。

如需应用 IPsec 功能，请选择“启用”，并点击保存按钮。

5.6.2.1 添加或编辑 IPsec 条目

点击上图所示界面中的**添加单个条目**或条目右侧的**编辑**按钮，将进入下面的设置界面。该页用来设置 IPsec 安全策略条目。

- **安全策略名称** 为 IPsec 安全策略命名。
- **本地子网** 设定本地子网地址，以子网掩码值划分地址范围。
- **对端子网** 设定对方子网地址，以子网掩码值划分地址范围。
- **对端网关** 输入通信对端的路由器相应 WAN 口的 IP 地址或域名。
- **协商方式** 建立 IPsec 安全隧道可以有两种协商方式。IKE 为自动协商，手动模式则需手动设定相关的安全参数。
- **安全协议** 选择 IPsec 连接使用的安全协议。
- **验证算法** 选择 IPsec 连接使用的验证算法。路由器支持以下验证算法：

  MD5 (Message Digest Algorithm, 消息摘要算法)：对一段消息产生 128bit 的消息摘要，防止消息被篡改。

  SHA1 (Secure Hash Algorithm, 安全散列算法)：对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。

  AUTO 表示自动适应对端算法。若对端使用本路由器不支持的算法将会协商失败，双方不能建立 VPN 连接。若对端同是 AUTO 模式，则双方会默认使用 SHA1 验证算法。
- **加密算法** 选择 IPsec 连接使用的加密算法。路由器支持以下加密算法：

  DES (Data Encryption Standard, 数据加密标准)：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。

  AES (Advanced Encryption Standard, 高级加密标准)：AES128/192/256 表示使用长度为 128/192/256 bit 的密钥进行加密。

  AUTO 表示自动适应对端算法。若对端使用本路由器不支持的算法将会协商失败，双方不能建立 VPN 连接。若对端同是 AUTO 模式，则双方会默认使用 AES256 加密算法。

- **入方向的 SPI** “手动模式”时，可以设定 SPI 参数。SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPsec 安全联盟，通信对端的“出 SPI”值必须与此值相同。
- **入方向的验证密钥** “手动模式”时，可以设定入方向的验证密钥。通信对端的“出方向的验证密钥”必须与此值相同。
- **入方向的加密密钥** “手动模式”时，可以设定入方向的加密密钥。通信对端的“出方向的加密密钥”必须与此值相同。
- **出方向的 SPI** “手动模式”时，可以设定 SPI 参数。SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPsec 安全联盟，通信对端的“入 SPI”值必须与此值相同。
- **出方向的验证密钥** “手动模式”时，可以设定出方向的验证密钥。通信对端的“入方向的验证密钥”必须与此值相同。
- **出方向的加密密钥** “手动模式”时，可以设定出方向的加密密钥。通信对端的“入方向的加密密钥”必须与此值相同。
- **IKE 安全策略** 选择“IKE 协商”时，可以指定相应的 IKE 安全策略。如果下拉菜单中没有想选择的条目，请点击右侧链接进行设置。
- **PFS 组** PFS (Perfect Forward Secrecy, 完善的前向安全性) 特性使得 IKE 第二阶段协商生成一个新的密钥材料，该密钥材料与第一阶段协商生成的密钥材料没有任何关联，这样即使 IKE 第一阶段的密钥被破解，第二阶段的密钥仍然安全。如果没有使用 PFS，第二阶段的密钥将根据第一阶段生成的密钥材料来产生，一旦第一阶段的密钥被破解，用于保护通信数据的第二阶段密钥也岌岌可危，这将严重威胁到双方的通信安全。PFS 是通过 DH 算法实现的，通信双方的 PFS 设置需保持一致。
- **生存时间** 设定 IKE 协商方式下 IPsec 会话密钥的生存时间。
- **生效** 设置该条策略是否生效。

5.6.3 安全联盟列表

在此将列出路由器上所有已成功建立的 IPsec 安全联盟相关信息，如下图所示。

序号	联盟名称	SPI	隧道发起端	隧道接收端	安全协议	AH验证算法	ESP验证算法	ESP加密算法
1	IPsec_1	3324	58.11.76.132	58.11.76.101	ESP	--	MD5	3DES
2	IPsec_1	7654	58.11.76.101	58.11.76.132	ESP	--	MD5	3DES

图中显示的是一组 IPsec 安全联盟信息。本例中路由器 WAN 接口的 IP 地址为 58.11.76.101，对端网关地址为 58.11.76.132。IPsec 隧道的安全协议、验证算法和加密算法等相关设置需与对端路由设置相同。

由于安全联盟是单向的，所以当 IPsec 隧道成功建立后，每条隧道会产生一对出方向和入方向的安全联盟。出方向和入方向的 SPI 值是不同的，但与对端的入方向和出方向 SPI 值相同。图中显示的本端隧道出方向 SPI 值为 7654，入方向 SPI 值为 3324。

5.7 转发规则

在“转发规则”菜单下面，有“虚拟服务器”、“特殊应用程序”、“DMZ 主机”和“UPnP 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。

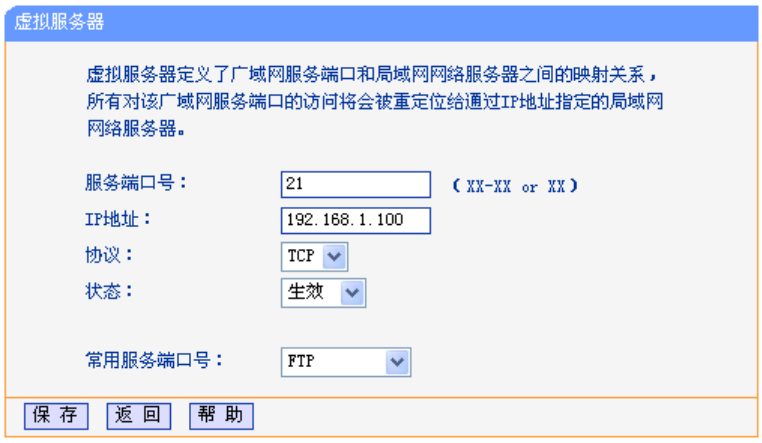
5.7.1 虚拟服务器

选择转发规则下的虚拟服务器，您将进入下面的设置界面。本路由器自身集成了防火墙功能，在路由器默认设置下，广域网中的计算机不能通过本路由器访问局域网中的某些服务器。但是，为了让路由器既保护局域网内部不被侵袭，又方便广域网中合法的用户访问，路由器提供了虚拟服务器功能。虚拟服务器可以定义一个服务端口，外网所有对此端口的服务请求都将被重新定位给路由器指定的局域网中的服务器（通过 IP 地址指定），这样外网的用户便能成功访问局域网中的服务器，而不影响局域网内部的网络安全。具体设置界面如下图示。

- **虚拟服务器条目表** 显示虚拟服务器条目信息。
- 服务端口 显示 WAN 端服务端口，即路由器提供给广域网的服务端口，外网对该端口的访问都将重定位到局域网中指定的服务器。
- IP 地址 显示局域网中指定为服务器的计算机的 IP 地址。外网对该局域网的访问都将重定位到该指定的计算机。
- 协议 显示数据包的协议类型。
- 状态 显示条目的状态。只有生效时，该条目的设置才起作用。
- 编辑 显示对该条目操作的超级链接——编辑或删除。
- **添加新条目** 点击该按钮，可以添加新的虚拟服务器条目。
- **使所有条目生效** 点击该按钮，可以使所有虚拟服务器条目生效。
- **使所有条目失效** 点击该按钮，可以使所有虚拟服务器条目失效。
- **删除所有条目** 点击该按钮，可以删除所有已设的虚拟服务器条目。

5.7.1.1 添加或编辑虚拟服务器

点击上图所示界面中的添加新条目或条目右侧的编辑按钮，将进入下面的设置界面。下面以添加新的虚拟服务器条目为例。



- **服务端口号** 请输入单个端口值或端口段。端口段输入格式为“开始端口-结束端口”，中间用“-”隔开。如上界面所示。
- **常用服务端口号** 请在该项选择服务端口号。在“常用服务端口”中，列出了常用协议的端口，可以直接从其中选择一个，系统会直接将选中的端口填入服务端口号中。对于常用服务端口中没有列出的端口，也可以在服务端口号处手动输入。

设置完成后，请点击保存按钮，然后在局域网服务器上进行相应的设置，这样，广域网中的计算机便可以成功访问局域网中的服务器了。

举例：

如果您的FTP服务器（端口号为21）IP地址为192.168.1.2，Web服务器（端口号为80）地址为192.168.1.3，POP3服务器（端口号为110）IP地址为192.168.1.6，这时您需要指定如下的虚拟服务器映射表：

注意：

如果设置了服务端口为 80 的虚拟服务器，则需要将“系统工具”菜单中的“远端 WEB 管理”项的 WEB 管理端口设置为 80 以外的值，如 8080。否则会发生冲突，从而导致虚拟服务器设置无效。

5.7.2 特殊应用程序

选择转发规则下的特殊应用程序，将进入下面的设置界面。某些程序需要多条连接，如 Internet 网络游戏、视频会议、网络电话等。由于防火墙的存在，这些程序无法在简单的 NAT 路由器下工作。然而，特殊应用程序使得某些这样的应用程序能够在 NAT 路由器下工作。当一个应用程序给触发端口上发起连接时，对应开放端口中的所有端口就会打开，以备后续连接。

- **特殊应用程序条目列表** 显示特殊应用程序条目信息。
- **触发端口** 显示应用程序首先发起连接的端口，即触发端口。

注意：

触发端口是为应用程序申请建立连接时，路由器指定的用于触发应用程序的端口。只有给该端口发起连接时，对应开放端口中的所有端口才可以开放，并为应用程序提供服务，否则开放端口中的所有端口是不会开放的。

- **触发协议** 显示触发端口上使用的协议，选项有 ALL、UDP 和 TCP。
- **开放端口** 显示该特殊应用程序条目采用的开放端口。

注意：

开放端口是为应用程序提供服务的多个端口。当给触发端口上发起连接后，开放端口打开，之后应用程序便可以给这些开放端口上发起后续的连接。

- **开放协议** 显示开放端口采用的协议，选项有 ALL、UDP 和 TCP。
- **状态** 显示该条目状态，只有状态为生效时，本条目所设的规则才能生效。
- **编辑** 显示对该条目的超级链接——编辑或删除。
- **添加新条目** 点击该按钮，可以在列表中添加新的条目，详见下面章节所述。
- **使所有条目生效** 点击该按钮，可以将该列表中的所有条目的状态设为“生效”。
- **使所有条目失效** 点击该按钮，可以将该列表中的所有条目的状态设为“失效”。
- **删除所有条目** 点击该按钮，可以删除当前已设的所有条目。

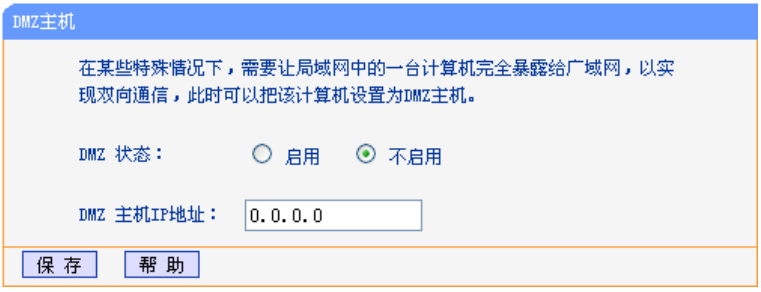
5.7.2.1 添加或编辑特殊应用程序

点击上图所示界面中的添加新条目或条目右侧的编辑按钮，将进入下面的设置界面。

- **触发端口** 请输入应用程序首先发起连接的端口触发号，如上图示。
- **触发协议：** 触发端口上使用的协议，可选项有 TCP、UDP 和 ALL。若对采用的协议不清楚，推荐选择 ALL。
- **开放端口** 请输入为应用程序提供服务的开发端口号，如上图示。可以输入一个或者多个端口或端口段，端口段输入格式为“开始端口-结束端口”，中间用“-”隔开，不同的端口段用“,”隔开。
- **开放协议** 开放端口上使用的协议，可选项有 TCP、UDP 和 ALL。若对采用的协议不清楚，推荐选择 ALL。
- **状态** 设置该条目是否生效。只有状态为生效时，本条目的设置才有效。
- **常用应用程序** 请在该项选择应用程序。在“常用应用程序”中，列出了常用的应用程序，可以直接在其中选中一个，系统会直接将选中的应用程序的触发端口和开发端口号自动填入到对应项中。对于“常用应用程序”中没有列出的端口，也可以在触发端口和开放端口处手动输入。

5.7.3 DMZ 主机

选择转发规则下的 DMZ 主机，将进入下面的设置界面。在某些特殊情况下，我们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。设置界面如下。



- **DMZ 主机 IP 地址** 请您输入局域网中指定为 DMZ 主机的 IP 地址。

举例：

DMZ 主机设置步骤如下：

首先在 DMZ 主机 IP 地址栏内输入欲设为 DMZ 主机的局域网计算机的 IP 地址，然后选中“启用”，最后单击“保存”按钮，即可完成 DMZ 主机的设置。

注意：

设置 DMZ 主机之后，与该 IP 相关的防火墙设置将不起作用。

5.7.4 UPnP 设置

选择转发规则下的 UPnP 设置，将进入下面的设置界面。依靠 UPnP（Universal Plug and Play）协议，局域网中的主机可以请求路由器进行特定的端口转换，使得外部主机能够在需要时访问内部主机上的资源，例如，Windows XP 和 Windows ME 系统上安装的 MSN Messenger，在使用音频和视频通话时就可以利用 UPnP 协议，这样原本受限于 NAT 的功能便可以恢复正常使用。

- **UPnP 设置列表** 显示 UPnP 条目信息。
- 应用描述 显示应用程序通过 UPnP 向路由器请求端口转换时的描述。
- 外部端口 显示端口转换时采用的路由器端口号。
- 协议类型 表明是对 TCP 还是 UDP 进行端口转换。
- 内部端口 显示需要进行端口转换的主机端口号。
- IP 地址 显示需要进行端口转换的主机 IP 地址。
- 状态 显示条目状态。“Enabled”表示应用程序请求并启用了端口转换；"Disabled"表示应用程序请求了端口转换，但并没有启用。

举例：

使用 UPnP 的方法如下：

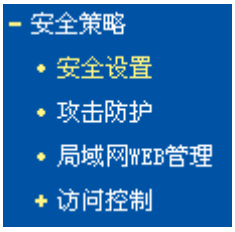
如果您的电脑开启了防火墙功能，请您在 Windows 防火墙界面的例外项中，选则启用 UPnP 框架程序。具体操作方法步骤为：开始→控制面板→安全中心→ Windows 防火墙→例外→选中 UPnP 框架。若例外项中没有 UPnP 项，则点击添加程序，再选中 UPnP 功能即可。

1. 在路由器 UPnP 界面中点击“启用 UPnP”按钮开启 UPnP 功能。
2. 当 MSN Messenger 等程序在运行中使用本功能时，按“刷新”按钮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。

注意:

- 不使用时请单击“关闭 UPnP”按钮，关闭 UPnP 功能。
- 因为现阶段版本的 UPnP 协议的安全性还未得到充分保证，所以在不需要时请关闭 UPnP 功能。
- 只有支持 UPnP 协议的应用程序才能使用本功能，MSN Messenger 还需要操作系统的支持（如 Windows XP/ME）。

5.8 安全策略



在“安全策略”菜单下面，共有“安全设置”、“攻击防护”、“局域网 WEB 管理”和“访问控制”四个子项。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.8.1 安全设置

选择安全策略下的安全设置，将进入下面的设置界面。

- **状态检测防火墙（SPI）：** 开启时，只有内网主动发起的请求才可以建立连接，所有来自外网的主动请求均被防火墙拒绝，从而能够保证内网免受来自外网的恶毒攻击，保护内网的安全。推荐保持默认状态“启用”。
- **虚拟专用网络（VPN）：** VPN 为远程计算机通过广域网进行安全通信提供了方法。如果内网主机需要使用 VPN 协议(如 PPTP、L2TP、IPSec)通过路由器连接到远程 VPN 网络，那么应开启相应的 VPN 穿透功能。

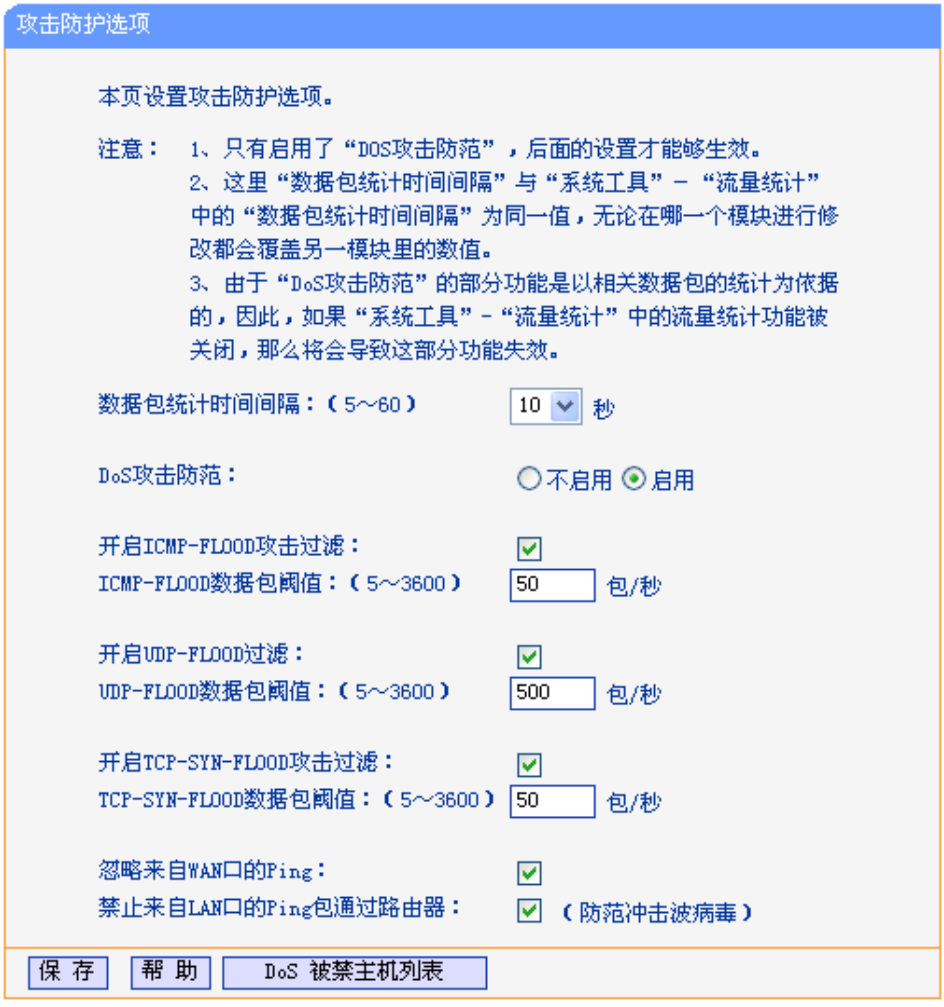
- **应用层网关（ALG）：** ALG 为某些采用“控制/数据”模式的应用层协议（如 FTP、TFTP、H323、RTSP 等）在通过 NAT 网关时作网络地址和端口的转换。推荐保持默认状态“启用”。

5.8.2 攻击防护

选择安全设置下的攻击防护，将进入下面的攻击防护的设置界面。攻击防护是防火墙通过对数据包的检查，以应对一些恶意的攻击。攻击检查和防护分为四类：

DoS 攻击的目的是用极大量的虚拟信息流耗尽目标主机的资源。受害者被迫全力处理虚假信息流，从而影响对正常信息流的处理。如果 DoS 攻击始发自多个源地址，则称为分布式拒绝服务(DDoS)攻击。通常 DoS 与 DDoS 攻击中的源地址都是欺骗性的。开启 DoS 攻击防范后，若某主机向目标主机发送某种数据包的速率大于设定值，那么该主机将被列入“DoS 被禁主机列表”而不能上网，从而很好地防止了 DoS 攻击。

如果在数据包中查到符合指定的攻击模式，则进行相应的防护处理。设置界面如下图所示。



- **数据包统计时间间隔** 设置对数据包进行统计的时间间隔。如果统计得到发往同一目标 IP 地址的某种数据包(例如 UDP FLOOD)达到了指定的阈值，那么系统将认为 UDP-FLOOD 攻击已经发生。如果 UDP-FLOOD 过滤已经开启，那么路由器将会停止接收该类型的数据包，从而达到防范攻击的目的。此处的值和**系统工具→流量统计**中的“数据包统计时间间隔”是一样的，一处的更改将引起另一处作同样的更改。

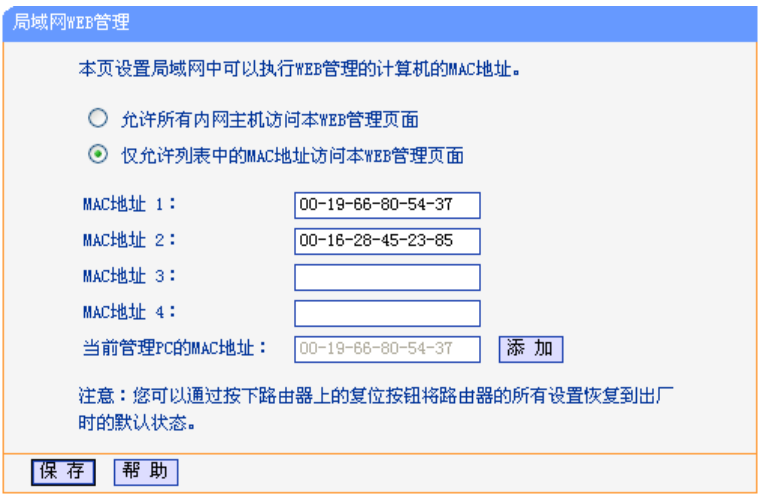
- **DoS 攻击防范** 该项是开启下面各种攻击防范的总开关，只有选择此项后，以下的几种防范措施才能生效。
- **开启 ICMP-FLOOD 攻击过滤** 若需要防范 ICMP-FLOOD 攻击，请选择此项。
- **ICMP-FLOOD 数据包阈值** 当开启 ICMP-FLOOD 功能后，如果在指定时间间隔内发往同一目标 IP 地址的 ICMP 包达到了设定值，防范措施将立即启动。
- **开启 UDP-FLOOD 攻击过滤** 若需要防范 UDP-FLOOD，请选择此项。
- **UDP-FLOOD 数据包阈值** 当开启 UDP-FLOOD 功能后，如果在指定时间间隔内发往同一目标 IP 地址的 UDP 包达到了设定值，防范措施则立即启动。
- **开启 TCP-SYN-FLOOD 攻击过滤** 若需要防范 TCP-SYN-FLOOD，请选择此项。
- **TCP-SYN-FLOOD 数据包阈值** 当开启 TCP-SYN-FLOOD 功能后，如果在指定时间间隔内发往同一目标 IP 地址的 TCP 的 SYN 包达到了设定值，防范措施则立即启动。
- **忽略来自 WAN 口的 Ping** 若开启该功能，广域网的计算机将不能 Ping 通路由器。
- **禁止来自 LAN 口的 Ping 包通过路由器** 若开启该功能，局域网的计算机将不能 Ping 通广域网中的计算机。
- **DoS 被禁主机列表** 点击该按钮，可以查看被禁止的计算机列表，如下图所示。点击**刷新**按钮可以更新列表信息。若希望被禁计算机能够重新上网，可以点击**删除**按钮；若需要释放所有被禁计算机，可以点击**清空**按钮。

注意：

*只有在开启了**系统工具→流量统计**中的流量统计功能后，DoS 攻击防范才能正常生效。*

5.8.3 局域网 WEB 管理

选择安全设置下的局域网 WEB 管理，将进入下面的设置界面。可以在此设置允许访问此 WEB 页面的局域网计算机的 MAC 地址。



如果要允许局域网中的所有计算机访问此 WEB 页面，请保持默认设置“允许所有内网主机访问本 WEB 管理页面”；如果只允许局域网中的部分计算机访问此 WEB 页面，请选择“仅允许列表中的 MAC 地址访问本 WEB 管理页面”，并将所允许的计算机的 MAC 地址添加到列表中。单击**添加**按钮还可以把当前正在访问此 WEB 页面的计算机的 MAC 地址复制到列表中。

注意：

如果选择了“仅允许列表中的 MAC 地址访问本 WEB 管理页面”，而没有把当前管理 PC 的 MAC 地址加入到列表中，那么当点击保存按钮以后，将无法继续通过当前 PC 来管理本路由器。在这种情况下，要重新获得对路由器的控制权，请将路由器恢复到出厂设置（如何恢复请参考 3.2 复位）。

5.8.4 访问控制

5.8.4.1 规则管理

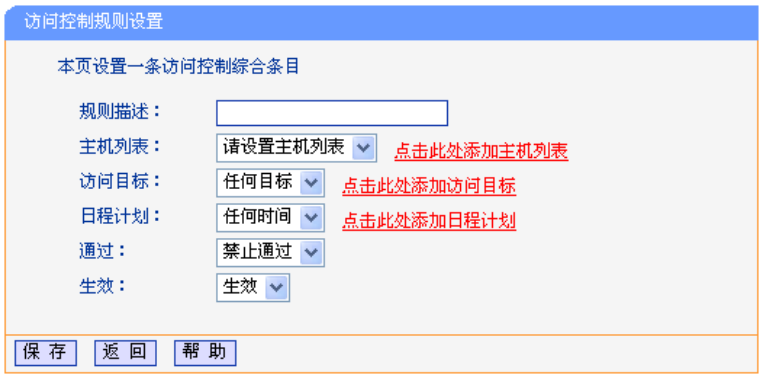
通过规则管理，可以设置和管理局域网内主机上网的规则，允许或禁止“主机列表”中的主机在“日程计划”时间段内访问“访问目标”网站。

- **开启访问控制**　　选中则开启访问控制功能，若不选中则规则无效。
- **缺省过滤规则**　　凡是不符合已设访问控制规则的数据包，允许通过本路由器--选择此项，则凡是和已设置的访问控制规则不符的数据包，均可以通过本路由器。

凡是不符合已设访问控制规则的数据包，禁止通过本路由器--选择此项，则凡是和已设置的访问控制规则不符的数据包，均不能通过本路由器。

- **移动** 通过该按钮来调整各条控制规则的顺序，以达到不同的控制优先级(ID 序号越靠前则优先级越高)。

点击**增加单个条目**按钮，可以在下图界面中设置新的访问控制条目。

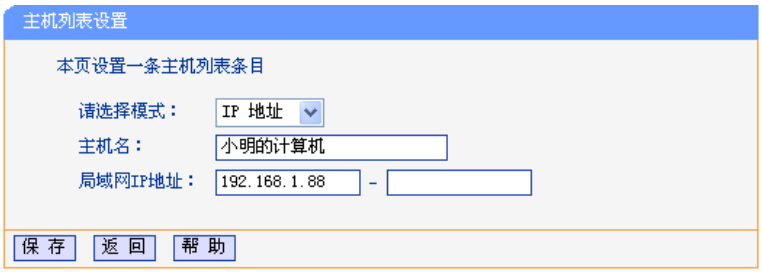


- **规则描述** 对该访问控制条目的简单描述，此描述必须是唯一的，如“周末 8：00-12：00”，用于标识设置的上网规则。
- **主机列表** 此条目为要控制的内网主机。如果已在**访问控制→主机列表**中设置好了要控制的主机的信息，请直接在下拉列表中选择，否则请单击**点击此处添加主机列表**进入主机列表设置对话框进行设置。有关主机列表的设置请参阅本文档**5.8.4.2 主机列表**部分。
- **访问目标** 允许或禁止“主机列表”中的主机访问的网站域名或 IP 地址。如果已在**访问控制→访问目标**中设置好了访问目标信息，请直接在下拉列表中选择，否则请单击**点击此处添加访问目标**进入访问目标设置对话框进行设置。有关访问目标的设置请参阅本文档**5.8.4.3 访问目标**部分。
- **日程计划** 允许或禁止“主机列表”中的主机访问目标网站的时间段。如果已在**访问控制→日程计划**中设置好了时间，请直接在下拉列表中选择，否则请单击**点击此处添加日程计划**进入日程计划设置对话框进行设置。有关日程计划的设置请参阅本文档**5.8.4.4 日程计划**部分。
- **通过** 对符合上述控制规则的情况，允许或禁止上网。
- **生效** 该访问控制条目是否生效。

5.8.4.2 主机列表

主机列表列举了需要遵守访问控制规则的主机信息，包括主机名，主机信息等。在主机列表设置中，可以增加，编辑和删除相应的主机列表。

单击**增加单个条目**按钮，可以在下图界面中设置新的受上网规则控制的主机信息。



- **请选择模式** 选择标识受控主机身份的模式，有 IP 地址和 MAC 地址两个选项。
- **主机名** 给受控主机的一个简单描述，不同主机列表条目中的主机名不能相同。
- **局域网 IP 地址/MAC 地址** 如果选择的模式为 IP 地址，请在此输入一台受控主机的 IP 地址或 IP 地址连续的多台受控主机的首尾 IP 地址。如果选择的模式为 MAC 地址，请在此输入受控主机的 MAC 地址。

单击**删除所有条目**按钮，可以一次性删除列表中的所有条目。删除所有条目后，则原先设置的访问控制规则对相应主机失效。

5.8.4.3 访问目标

访问目标显示了主机上网访问的目标网站或目标 IP 地址，如“www.baidu.com”，“192.168.1.71”等。

单击**增加单个条目**按钮，可以在下图界面中设置新的访问目标的信息。

- **请选择模式** 选择描述访问目标信息的模式，有 IP 地址和网站域名两个选项。
- **目标描述** 给访问目标的一个简单描述，此描述必须是唯一的。
- **目标 IP 地址** 输入一个访问目标的 IP 地址或连续的访问目标 IP 地址段。
- **目标端口** 允许或限制访问的目标 IP 地址的服务端口，可以为一个端口号或连续的端口段。如果不清楚目标端口号，可以在“常用服务端口号”的下拉列表中通过选择服务来自动填入。
- **协议** 访问目标的服务器所使用的协议。如果不清楚采用的协议，推荐选择 ALL。
- **常用服务端口号** 下拉列表中列举了一些常用的服务端口，从中选择需要的服务，则该服务对应的端口号会自动填入上面的“目标端口”输入框中。
- **网站域名** 在域名模式下，可以为列表设置 4 个网站完整域名或域名的关键字，如果在此处填入某一个字符串（例如：yahoo），则含有该字符串的域名（www.yahoo.com、www.yahoo.com.cn）都可以被匹配。

5.8.4.4 日程计划

在“日程计划”中，可以设置上网规则生效的时间。此处的时间包括日期和时间段。日期可以为一个星期的某几天，也可以为每天。时间段可以设为某两个时间点间的时间段，也可以为“全天 24 小时”。

注意：

在设置之前，请确保路由器的时间是正确的，有关路由器的时间设置请参阅本文档**5.13.1 时间设置**部分。

单击**增加单个条目**按钮，可以在下图界面中设置新的日程计划。

- **日程描述** 给日程计划的简单描述，此描述必须是唯一的，例如“周末 8：00-20：00”。
- **星期** 点选“每天”，可以将时间设置为每天，点选“选择星期”，则可将时间设置为每个星期的某几天。
- **时间** 如果要设置为全天，请直接选择“全天—24 小时”，否则请在开始时间、结束时间中输入具体时间，注意时间格式为 HHMM，即前两位为小时，后两位为分钟。

5.9 路由功能

在“路由功能”菜单下面，只有“静态路由表”一个子项。单击该子项，即可进行静态路由功能设置，下面将详细讲解静态路由功能的设置。

5.9.1 静态路由表

选择路由功能下的静态路由表项，将进入下面所示界面。本页设置路由器的静态路由功能，可以通过**添加新条目**按钮来增加新的过滤规则；或者通过“编辑”、“删除”链接来修改或删除旧的过滤规则。

- **静态路由表** 显示静态路由条目表中的信息。
- 目的 IP 地址 显示欲访问的主机的 IP 地址。
- 子网掩码 显示子网掩码，一般为 255.255.255.0。
- 网关 显示数据包被发往的路由器或主机的 IP 地址。

- 状态　　显示本条目的状态，即本条目是否生效。
- 编辑　　显示对本条目操作的超级链接——编辑或删除。
- **添加新条目**　　点击该按钮，可以在路由列表中添加新的条目。
- **使所有条目生效**　　点击该按钮，可以将列表中所有条目的状态设为“生效”。
- **使所有条目失效**　　点击该按钮，可以将列表中所有条目的状态设为“失效”。
- **删除所有条目**　　点击该按钮，可以删除当前列表中已设的所有条目。

当点击“添加新条目”或点击“编辑”链接界面时，将进入下面的设置界面。

5.9.2　系统路由表

选择路由功能下的系统路由表项，将进入下面所示界面。本页将显示所有正在使用的路由表条目，包括手动设置的和系统自动生成的路由条目，每条路由表条目由目的网络地址，子网掩码，网关和接口组成。

当路由条目有新增或修改时，可以单击**刷新**按钮获取最新的系统路由表。

5.10　QoS

在“QoS”菜单下面，共有“控制设置”、“控制规则”两个子项。单击某个子项，即可进行相应的功能设置，下面将详细讲解各子项的功能。

5.10.1　控制设置

选择 QoS 下的控制设置，将进入下面所示界面。本页主要对 QoS 的开启与关闭进行设置。

- **开启 QoS** 请您选择是否开启 QoS 设置，选中该复选框则表示启用该功能。
- **上行总带宽** 请您输入希望路由器通过 WAN 口提供的上传速率，最大值为 100000Kbps。
- **下行总带宽** 请您输入希望路由器通过 WAN 口提供的下载速率，最大值为 100000Kbps。

注意:

只有 QoS 的总开关开启时，后续的“控制规则”才能够生效，反之，则无效。

5.10.2 控制规则

选择 QoS 下的控制规则，将进入下面所示界面。控制规则分为 QoS 规则列表和 QoS 规则配置。

在 QoS 规则列表中，可以查看用户创建的全部规则。每个规则包含的条目有：

- **QoS 规则列表** 显示用户创建的所有规则信息。每个规则包含的条目有
- ID 规则序号。
- 描述 显示描述的信息，包括地址段，传输层的端口段和协议；其格式有：地址段/端口段/协议，端口段/协议，端口段，地址段。
- 上行带宽 显示 WAN 口允许的最大上传速度限制和最小上传速度保证，为 0 时表示采用缺省值。输入范围为 0-100000Kbps。
- 下行带宽 显示 WAN 口允许的最大下载速度限制和最小下载速度保证，为 0 时表示采用缺省值。输入范围为 0-100000 Kbps。
- 启用 显示规则的状态，选中该复选框则表示该规则生效。
- 配置 显示可以对该规则进行的超级链接——编辑或删除。

- **添加新条目** 点击该按钮，可以添加新的 QoS 规则。
- **删除所有条目** 点击该按钮，可以删除列表中的所有规则条目。

点击 QoS 规则列表中的添加新条目或编辑按钮，将进入下面的设置界面。在 QoS 规则配置中，可以创建新的 QoS 规则或修改已存在的规则。具体设置见下图示。

- **启用** 请您选择是否启用该规则。
- **地址段** 请您输入内部主机的地址范围。当全部为空或为 0.0.0.0 时表示该域无效。
- **端口段** 请您输入内部主机访问外部服务器的端口范围。当全部为空或为 0 时表示该域无效。
- **协议** 请您输入传输层采用的协议类型，这里有 ALL(任意匹配)、TCP 和 UDP；该域只有在端口段选中下才有效。
- **上行、下行** 请您参考 QoS 规则列表中所述来设置。

5.11 IP 与 MAC 绑定

在“IP 与 MAC 绑定”的菜单下面，有“静态 ARP 绑定设置”和“ARP 映射表”两个子项。单击某个子项，即可进行相应功能的设置，下面将详细讲解各个子项的功能。

5.11.1 静态 ARP 绑定设置

选择 IP 与 MAC 绑定下的静态 ARP 绑定设置，即可进入该项的设置界面。ARP 绑定是指，指定的 IP 地址的主机在向路由器发送 ARP 请求时，当 MAC 地址与绑定的 MAC 地址相同时，才允许其通过路由器，否则不允许使用该 IP 地址的主机发送的 ARP 请求通过路由器。ARP 绑定功能分为两种：普通绑定和强制绑定。其中普通绑定允许您限制计算机使用 IP 地址，强制绑定允许您限制计算机的上网行为。

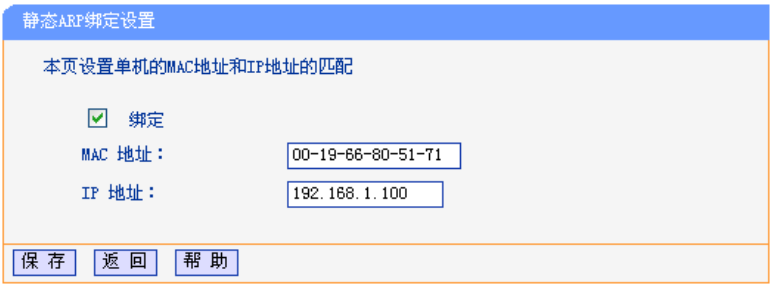
本页显示已经设置的 ARP 静态列表。可以利用按钮“增加单个条目”来增加新的 ARP 静态条目，或者通过按钮“编辑”或“删除”链接来修改或删除旧的 ARP 静态条目。

要使用 ARP 绑定功能，需要先设置以下项目：

- **ARP 绑定** 选择“启用”或“不启用”ARP 绑定功能，点击保存按钮生效。
- **静态 ARP 绑定列表** 显示 IP 与 MAC 地址绑定的条目信息。
- MAC 地址 显示您希望控制的计算机的 MAC 地址。
- IP 地址 显示您希望与指定 MAC 地址绑定的 IP 地址。
- 绑定 显示该条目的状态，选中该复选框则表示绑定条目生效。
- 配置 显示对该绑定条目操作的超级链接——编辑或删除。
- **增加单个条目** 点击该按钮，您可以在静态绑定列表中添加新的条目。
- **删除所有条目** 点击该按钮，您可以删除静态列表中的所有条目。
- **查找指定条目** 点击该按钮，您可以在静态列表中查找指定 IP 地址或 MAC 地址的条目。具体查找方法见后面所述。
- **使所有条目生效** 点击该按钮，您可以使当前静态列表中的所有绑定条目生效。

5.11.1.1 添加或编辑静态 ARP 绑定条目

添加或编辑静态 ARP 绑定条目时，请点击上图所示界面中的**增加单个条目**或**编辑**按钮，可以进入下面的设置界面。



举例：

设置只允许局域网中 MAC 地址为 00-19-66-80-51-71 的计算机使用 IP 地址 192.168.1.100，其他计算机不能使用该 IP 地址。

设置步骤如下：

首先，请设置该节首页中的“ARP 绑定”为“普通绑定”，并保存。

然后请点击“增加单个条目”按钮，并按上图设置添加新的静态绑定条目。最后按下保存即可。

您也可以通过条目上配置中的“编辑”按钮，对已经设置的条目进行编辑，其界面与上图相同。

举例：

设置只允许局域网中 MAC 地址为 00-19-66-80-51-71 且 IP 地址 192.168.1.100，其他计算机不能上网。

设置步骤如下：

首先，请点击“增加单个条目”按钮，并按上图设置添加新的静态绑定条目。最后按下保存即可。

然后，请设置该节首页中的“ARP 绑定”为“强制绑定”，并保存。

注意：

开启强制绑定功能时，必须确保当前登录路由器的管理计算机已经设置了 MAC 和 IP 绑定条目，并且该条目已经绑定。否则启用该功能后，您的计算机将不能继续登录路由器，也不能上网。

5.11.1.2 查找静态 ARP 绑定条目

如果您希望查找特定的 IP 地址或 MAC 地址是否已经设置到静态绑定表中，您可以在首页中点击**下一页**、**上一页**按钮或直接选择指定页进行浏览查找。另外，您也可以点击按钮**查找指定条目**进入到下图界面中进行快速查找。

举例：

例如您要查找 IP 地址为 192.168.1.100 的条目。

查找步骤如下：

首先，请单击按钮“查找指定条目”，然后进入下图设置查找信息，您可以在 IP 地址栏中输入 192.168.1.100 进行查找。

最后，单击按钮“查找”，则可以得到结果。

在上图中，如果您需要对该条目进行进一步的编辑操作，可以点击上图所示界面中的链接——“转至该页”按钮，进入该条目所在的 ARP 静态绑定列表所在页（条目呈黄色高亮），再选择条目旁边的“编辑”按钮，进入编辑界面对它进行编辑。如下图示：

5.11.2 ARP 映射表

选择 IP 与 MAC 绑定下的 ARP 映射表，可以进入 ARP 映射表显示界面。本页显示当前设置的和通过路由器 ARP 的映射列表，并显示是否已经绑定。同时也可以将指定映射条目导入到 ARP 静态列表中进行进一步的编辑操作，或者直接删除该映射条目。

- **ARP 映射表** 显示映射表条目信息。
- MAC 地址 显示网络中计算机的 MAC 地址。
- IP 地址 显示与 MAC 地址匹配的计算机的 IP 地址。
- 状态 显示该条目状态，绑定或未绑定。
- **配置** 显示对该条目的操作的超级链接——导入或删除。
- 导入 点击该按钮，可以将该条目导入到前面的静态 ARP 绑定列表中。
- 删除 点击改按钮，可以将该条目从 ARP 映射表中删除。

注意:

只有静态 ARP 绑定设置界面选择了普通绑定或强制绑定，且条目已经绑定时，ARP 映射表中对应条目的状态才会显示“已绑定”。

ARP 映射表中的条目状态为“已绑定”时，点击其右侧的“删除”，ARP 映射表及静态 ARP 绑定列表中对应的条目状态都将由“绑定”变成“不绑定”。

ARP 映射表中的条目状态为“不绑定”时，其右侧的“删除”不起任何作用。

- **全部绑定** 点击该按钮，可以动态绑定当前列表中所有条目(不保存到静态 ARP 绑定列表中)。
- **全部导入** 点击改按钮，可以把当前 ARP 映射表的所有条目全部导入到静态 ARP 绑定列表中，如果有冲突条目，将忽略冲突条目，添加其他条目；如果静态绑定表已满，则忽略多余的条目。

5.12 动态 DNS

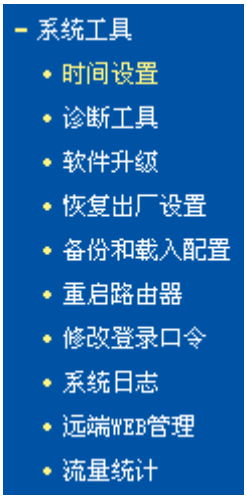
动态 DNS 又名 DDNS，它的主要功能是实现固定域名到动态 IP 地址之间的解析。对于使用动态 IP 地址的用户，在每次上网得到新的 IP 地址后，安装在主机上的动态域名软件就会将该 IP 地址发送到由 DDNS 服务商提供的动态域名解析服务器，并更新域名解析数据库。当 Internet 上的其他用户需要访问这个域名的时候，动态域名解析服务器就会返回正确的 IP 地址。这样，大多数不使用固定 IP 地址的用户，也可以通过动态域名解析服务经济、高效地构建自身的网络系统。本路由器提供花生壳 DDNS 服务，服务提供者是 www.oray.net。

选择动态 DNS 菜单，在界面的“服务提供者”下拉选项中选择“花生壳（www.oray.net）”，将进入下图所示的花生壳 DDNS 设置界面。本页设置“花生壳”的 DDNS 参数，当连接状态显示成功之后，互联网上的其它主机就可以通过域名的方式对您的路由器或虚拟服务器进行访问了。

选择服务提供者“花生壳(www.oray.net)”，可以在下图界面中设置 DDNS。在注册成功后，可以用注册的用户名和密码登录到 DDNS 服务器上。当连接状态显示成功之后，互联网上的其它主机就可以通过域名的方式访问您的路由器或虚拟服务器了。

- **服务商链接** 成功连接外网后，点击该项，可以分别链接到“花生壳动态域名解析服务申请”和“花生壳动态域名解析服务帮助”页面。
- **服务提供者** 请您选择提供 DDNS 的服务器名。
- **用户名** 请您输入在 DDNS 服务器上注册的用户名。
- **密码** 请你输入在 DDNS 服务器上注册的密码。
- **启用 DDNS** 请您选择是否启用该 DDNS 功能。
- **连接状态** 显示当前与 DDNS 服务器的连接状态。
- **服务类型** 显示当前用户的类型。
- **域名信息** 显示当前 DDNS 服务器获得的域名服务列表。

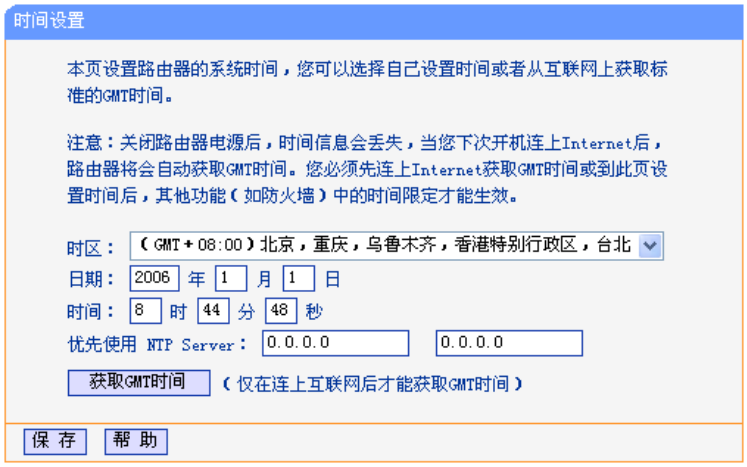
5.13 系统工具



在“系统工具”菜单下面，共有“时间设置”、“诊断工具”、“软件升级”、“恢复出厂设置”、“备份和载入配置”、“重启路由器”、“修改登录口令”、“系统日志”、“远端 WEB 管理”、“流量统计”十个子项。单击其中某个子项，即可对它进行相应的功能设置，下面将详细讲解各子项的功能。

5.13.1 时间设置

选择系统工具下的时间设置，可以进入下面的时间设置界面。本页用来设置路由器的系统时间，您可以选择自己设置时间，也可以选择从互联网上获取标准的 GMT 时间。具体设置页面如下：



- 优先使用 NTP Server　请输入希望采用的 NTP Server 的 IP 地址（可以输入两个）。NTP Server 是网络时间服务器，用于 Internet 网上的计算机时间同步。当路由器获取 GMT 时间时，优先从该时间服务器上获取。

举例：

系统时间设置步骤：

首先请您选择您所在的时区，然后在日期和时间栏内填入相应值，最后单击保存按钮完成系统时间的设置。

如果您已经连上了互联网，则您也可以直接单击获取 GMT 时间按钮，从互联网上获取标准的 GMT 时间。

注意：

关闭路由器电源后，时间信息会丢失，只有当您下次开机连上 Internet 后，路由器才会自动获取 GMT 时间。

您必须先连上 Internet 获取 GMT 时间或在此页手动设置系统时间，路由器其他功能（如防火墙）中的时间限定才能生效。

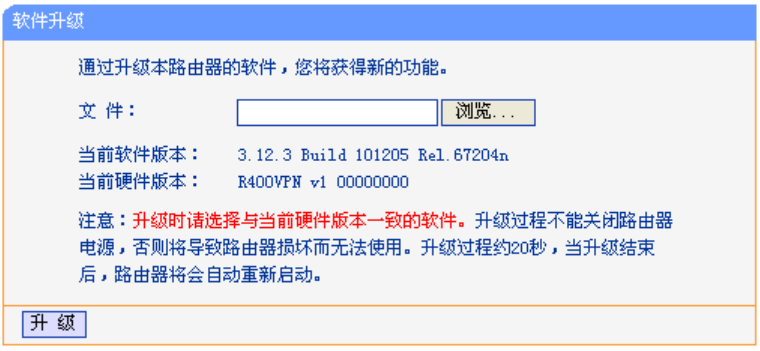
5.13.2 诊断工具

选择系统工具下的诊断工具，可以进入下面的诊断界面。使用 Ping 或者 Tracert 命令，可以诊断路由器的连接状态，页面如下：

- **选择操作** 选择 Ping 或者 Tracert 操作。
- **IP 地址/域名** 目的 IP 地址或者域名。
- **Ping 包数目** Ping 操作发出的 Ping 包数目。
- **Ping 包大小** Ping 操作发出的 Ping 包的大小。
- **Ping 超时设置** Ping 操作的超时时间。
- **Tracert 跳数** 设置 Tracert 的跳数。

5.13.3 软件升级

选择系统工具下的软件升级，可以进入下面的软件升级界面。通过升级本路由器的最新版本软件获得最新的功能。升级页面如下：



举例：

升级步骤：

请先登录本公司的网站(www.tp-link.com.cn)，下载最新版本的软件。

选择系统工具下的软件升级项，在上图界面中的文件栏内填入已下载文件的全路径文件名，或用浏览按钮选择已下载的升级文件。

单击升级按钮进行软件升级。

升级完成后，路由器将自动重启。

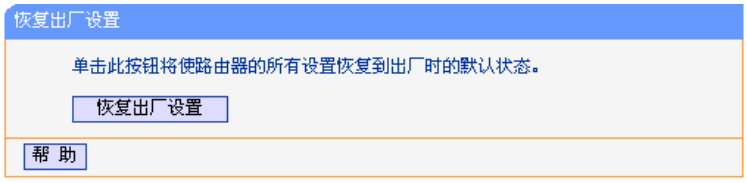
注意:

升级时请选择与当前硬件版本一致的软件。

在升级过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。升级过程需要一段时间，升级完成后，路由器将会自动重启。

5.13.4 恢复出厂设置

选择系统工具下的恢复出厂设置，可以进入下面的操作界面。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。操作页面如下：



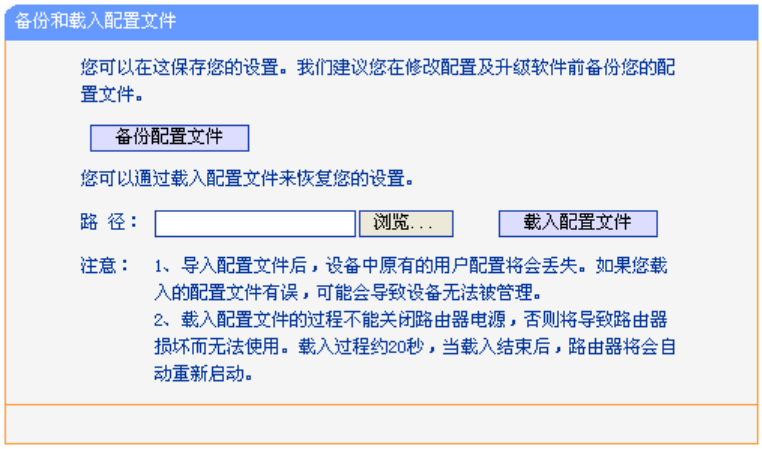
出厂默认情况下的各参数如下：

- **默认的用户名** admin
- **默认的密码** admin
- **默认的 IP 地址** 192.168.1.1
- **默认的子网掩码** 255.255.255.0

恢复出厂设置后，路由器将自动重启。

5.13.5 备份和载入配置

选择系统工具下的备份和载入配置，可以进入下面的操作界面。配置备份功能可以将路由器的设置以文件形式保存到电脑中，以备下次使用；配置载入功能则是将先前保存的或已编辑好的配置重新装入。配置界面如下：



- **备份配置文件** 将配置以文件形式保存。
- **路径** 配置文件的全路径。
- **浏览** 选择配置文件。
- **载入配置文件** 装入先前保存的或已编辑好的配置文件。

举例：

典型用法：

升级软件或在载入新配置文件前备份原配置，以防止升级软件或载入新配置文件时操作有误，丢失配置。

为多台路由器配置相同的设置。先设置一台路由器，保存其配置文件后，再将它载入到其它的路由器中，以节省时间。

注意：

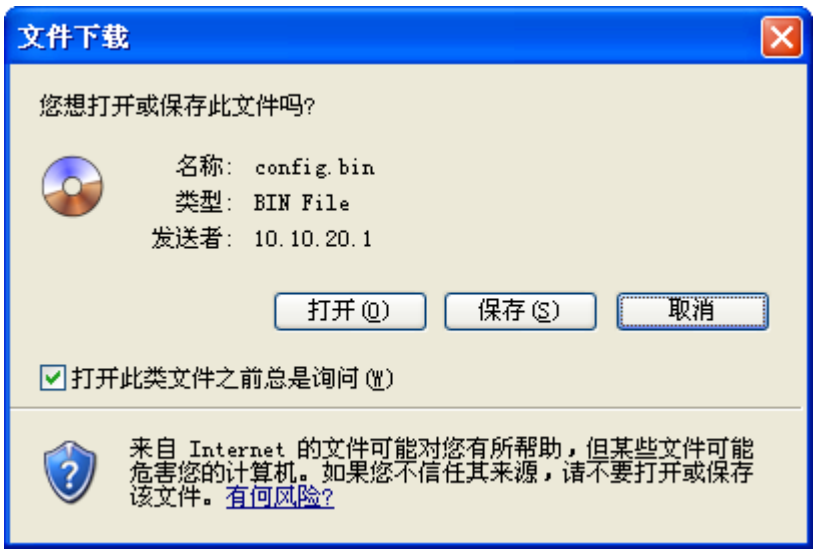
载入配置文件后，设备中原有的用户配置将会丢失，如果您需要保存原有配置，请先进行配置备份。如果您载入的配置文件有误，可能会导致设备无法管理和使用。

载入配置文件的过程中不能关闭路由器电源，否则将导致路由器损坏而无法使用。载入文件的大小及配置命令正确与否会影响载入过程所需要的时间。如果载入结束且没有错误，路由器将会自动重启。如果载入有错，请根据提示信息及生效的配置选择自己是否需要保存配置，然后最好再重启路由器。

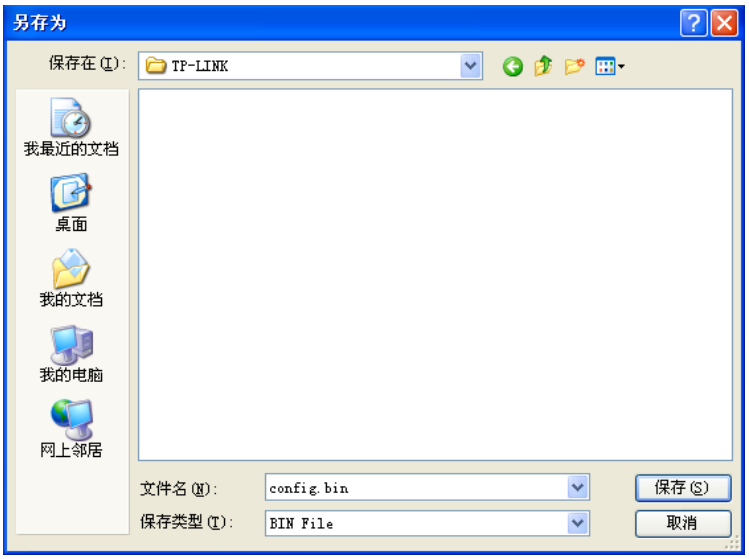
备份配置到：C:\TP-LINK\ config.bin；然后，将其载入到另一台路由器中。

备份配置步骤如下：

选择系统工具下的备份和载入配置项，单击备份配置文件按钮，出现下面操作界面：

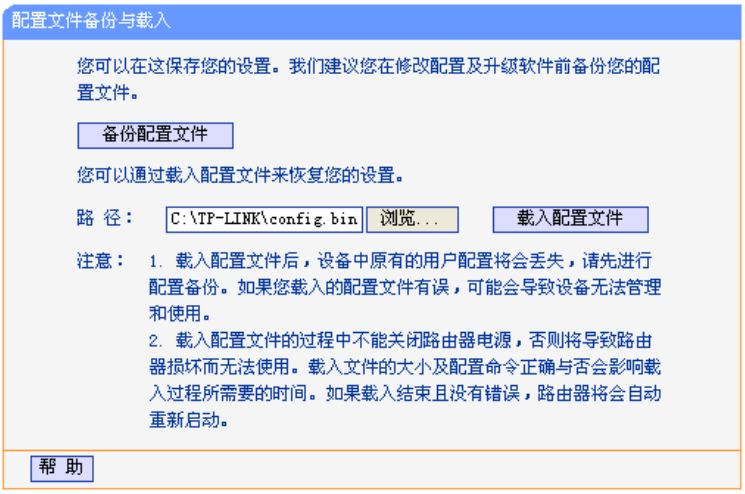


点击保存按钮，将配置文件 config.bin 保存在文件夹 C:\TP-LINK 中。如下图示:



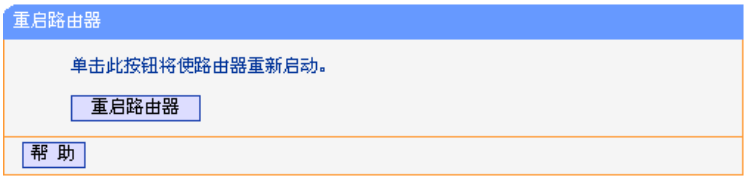
载入配置步骤如下:

更换另一台路由器，选择系统工具下的备份和载入配置项，输入载入文件夹的详细路径（如: C:\TP-LINK\config.bin）或点击浏览按钮选择载入文件夹，然后单击载入配置文件按钮即可完成文件载入。下图为输入文件路径，载入配置文件的示意图。



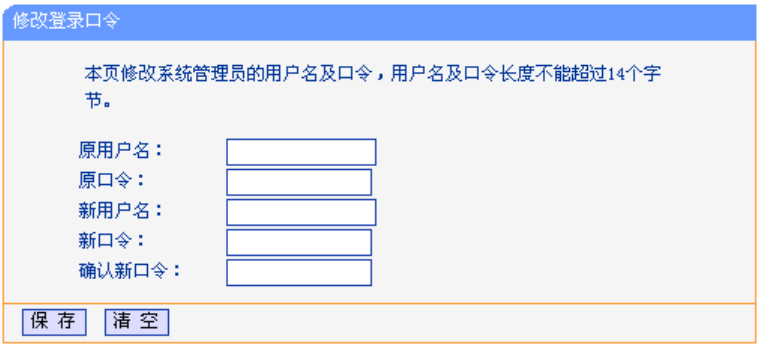
5.13.6 重启路由器

选择系统工具下的重启路由器，可以进入下面的操作界面。单击重启路由器按钮，路由器就会重新启动。操作界面显示如下：



5.13.7 修改登录口令

选择系统工具下的修改登录口令，可以进入下面的操作界面。本页修改系统管理员的用户名及口令。修改界面如下：



举例：

登录口令修改步骤：

首先请您输入原来的用户名和口令，然后输入您希望使用的新用户名和口令。如果您原来的用户名和口令输入无误的话，单击“保存”即可成功修改用户名和口令。

注意：

出于安全考虑，我们强烈推荐您改变初始系统管理员用户名及密码。如果您忘了系统密码，请使用复位按钮恢复到出厂设置。

5.13.8 系统日志

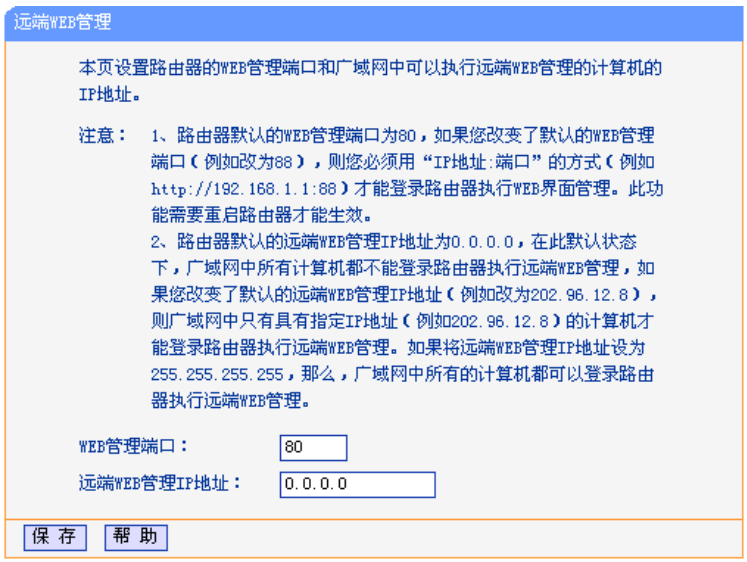
选择系统工具下的系统日志，可以进入下面的显示界面。该部分记录了路由器的系统日志，您可以通过查询日志了解路由器上发生的系统事件。界面显示如下：

点击邮件发送设置按钮，可以将路由器上的日志信息定时发往指定邮箱，设置界面如下图所示。

- **邮件账户设置** 可以设置收发邮箱账户信息。
- 发信邮箱地址 设定后路由器将通过该账户发送日志信息。
- 收信邮箱地址 设定接受路由器日志信息的邮箱账户。
- SMTP 服务器地址 提供 SMTP 服务的服务器地址。
- 启用验证 如果邮箱需要用户名/密码，请勾选此项。
- 用户名 登录邮箱的用户名(不含@后面的字段)。
- 密码 登录邮箱的密码。
- **启用定时发送日志功能** 勾选此项后，路由器将按设置规则发送日志信息。
- 每天发送 设置后路由器将在每天的指定时间发送日志信息。
- 间隔发送 设置后路由器将在指定的间隔期间发送日志信息。

5.13.9 远端 WEB 管理

选择系统工具下的远端 WEB 管理，您可以进入下面的操作界面。本页设置路由器的 WEB 管理端口和广域网中可以执行远端 WEB 管理的计算机的 IP 地址。设置界面如下：



- **WEB 管理端口** 可以执行 WEB 管理的端口号。
- **远端 WEB 管理 IP 地址** 广域网中可以执行远端 WEB 管理的计算机的 IP 地址。

注意:

路由器默认的 WEB 管理端口为 80，如果您改变了默认的 WEB 管理端口(例如改为 88)，则您必须用“IP 地址端口”的方式（例如 http://192.168.1.1:88）才能登录路由器执行 WEB 界面管理。此功能需要重启路由器才生效。

路由器默认的远端 WEB 管理 IP 地址为 0.0.0.0，在此默认状态下，广域网中所有计算机都不能登录路由器执行远端 WEB 管理，如果您改变了默认的远端 WEB 管理 IP 地址（例如改为 202.96.12.8），则广域网中只有具有指定 IP 地址（例如 202.96.12.8）的计算机才能登录路由器执行远端 WEB 管理。

5.13.10 流量统计

选择系统工具下的流量统计，可以进入下面的操作界面。

- **当前流量统计状态** 请您选择是否需要开启流量统计，如无需进行流量统计，可点击关闭流量统计按钮禁用该功能，这样可以提高路由器的数据处理能力。
- **数据包统计时间间隔** 请您选择当前统计流量的时间间隔。它与“安全设置”－“高级安全设置”中的“数据包统计时间间隔”为同一值，无论在哪一个模块进行修改都会覆盖另一模块里的数值。

- **流量统计列表** 显示流量统计的信息。
- IP 地址 显示被统计主机的 IP 地址。
- 带宽 显示被统计主机 10 秒钟内收、发数据的字节数。
- 总流量 显示当前数据的总流量，分别用数据包和字节数来衡量该值。
- 数据包数 路由器总的收、发数据包的个数。
- 字节数 路由器收、发数据的总计字节数。
- 当前流量 显示当前设置的时间间隔内（图中为 10 秒）的数据流量。
- 数据包数 路由器当前 10 秒钟内收、发数据包的个数。
- 字节数 路由器当前 10 秒钟内收、发数据的字节数。
- ICMP Tx 路由器当前 10 秒钟内发送到广域网的 ICMP 包的个数。
- UDP Tx 路由器当前 10 秒钟内发送到广域网的 UDP 包的个数。
- TCP SYN Tx 路由器当前 10 秒钟内发送到广域网的 TCP SYN 包的个数。
- 每页显示 设置每页可以显示的最大条目数（默认值为 5）。
- 上一页、下一页 单击该按钮，可以分别转入界面的上一页或下一页。
- 当前第 页 显示当前的页码。

附录 A　FAQ

一. ADSL 用户如何设置上网？

1） 首先，将 ADSL modem 设置为桥模式（1483 桥模式）。

2） 用网线将路由器的 WAN 口与 ADSL modem 相连，电话线连 ADSL modem 的 Line 口。

3） 进入管理界面，选择菜单“网络参数”下的“WAN 口设置”，在右边主窗口中，“WAN 口连接类型”选择“PPPoE”，输入“上网帐号”及“上网口令”，点击连接按钮即可。

4） 如果是包月上网的用户，可以选择“自动连接”的连接模式；如果是非包月用户，可以选择“按需连接”或者“手动连接”，并且输入自动断线等待时间，防止忘记断线而浪费上网时间。

二. LAN 接入的用户如何设置上网？

1） 进入管理界面，选择菜单“网络参数”下的“WAN 口设置”，在右边主窗口中，“WAN 口连接类型”选择“动态 IP”，点击“保存”按钮即可。

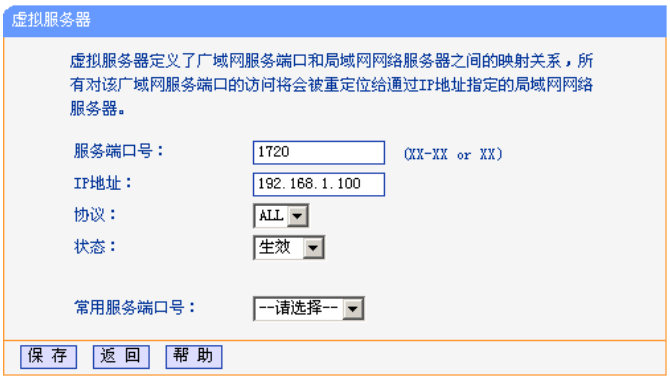
2） 在某些网络服务商绑定了用户计算机网卡 MAC 地址的情况下，需要对路由器进行 MAC 地址克隆操作，将路由器的指定 WAN 口（WAN1、WAN2、WAN3、WAN4）MAC 地址设置为被绑定的网卡 MAC 地址。选择菜单“网络参数”下的“MAC 地址克隆”，在右边主窗口中点击“克隆 MAC 地址”按钮，然后按“保存”按钮，待路由器重启动后生效。

三. 怎样使用 NetMeeting 聊天？

1） 如果是主动发起 NetMeeting 连接，则不需要任何配置，直接在 NetMeeting 界面中输入对方的 IP 地址，即可进行 NetMeeting 呼叫。

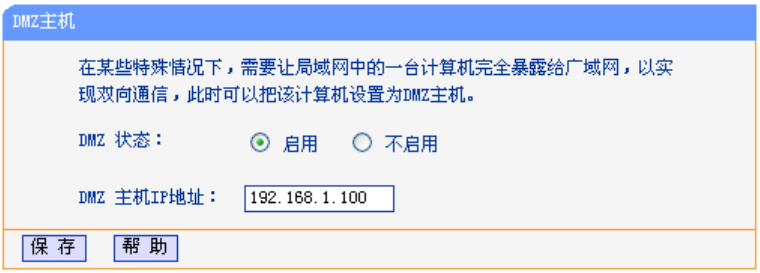
2） 如果希望能接收来自对方的 NetMeeting 呼叫，则需要设置虚拟服务器或 DMZ 主机。

3） 设置虚拟服务器方法：进入管理界面，选择菜单“转发规则”下的“虚拟服务器”，点击“添加新条目”按钮，在“服务端口号”栏填入“1720”（NetMeeting 的连接端口），“IP 地址”栏填入您计算机的 IP 地址（假设您的 IP 地址是 192.168.1.100），再在状态栏选择“生效”，点击“保存”按钮即可。如图：



这样，对方呼叫您时只需输入您路由器 WAN 口的地址即可。

4） 设置 DMZ 主机方法：进入管理界面，选择菜单“转发规则”下的“DMZ 主机”，在“DMZ 主机 IP 地址”栏填入您计算机的 IP 地址（假设您的 IP 地址是 192.168.1.100），再将“启用”选择框选中，点击“保存”按钮即可。如图：

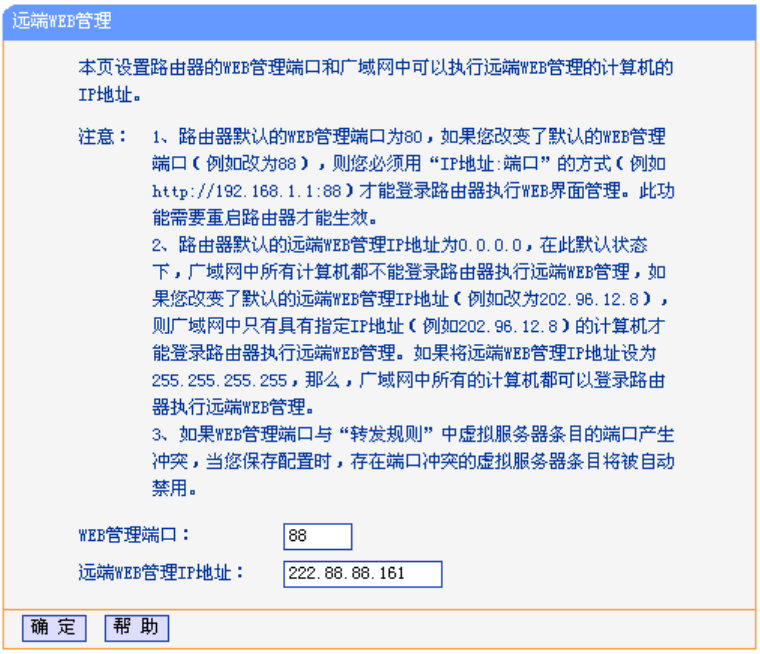


四. 怎样在局域网构建 Web 服务器？

1） 在局域网构建服务器，只需要按问题 3 的第三点设置虚拟服务器即可。

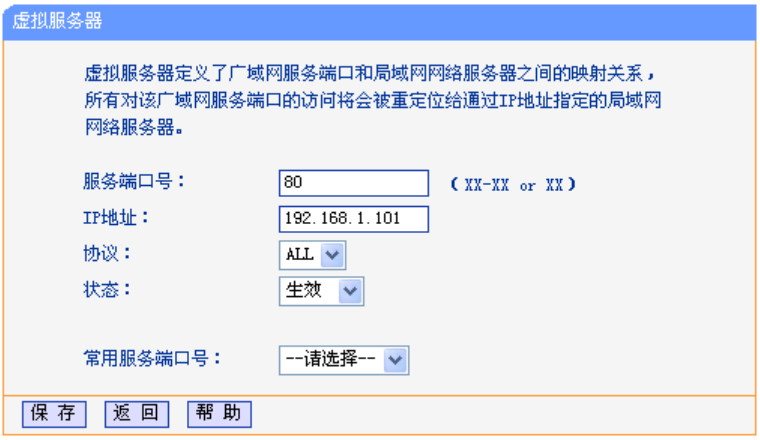
2） 但在构建 Web 服务器时，Web 服务的服务端口与路由器本身 Web 管理界面的缺省端口相同，都是 80，这样就引起冲突。解决办法是修改路由器 Web 管理界面的端口。

3） 进入管理界面，选择菜单“系统工具”下的“远端 Web 管理”，在右边主窗口中，“Web 管理端口”栏输入 80 以外的值，如 88。点击保存并重启路由器。如图：



4） 再次进入管理界面时，需要在浏览器的地址栏输入：http://192.168.1.1:88 才能进入。

5） 进入管理界面，选择菜单“转发规则”下的“虚拟服务器”，点击“添加新条目”按钮，在“服务端口号”栏填入“80”，这是 Web 服务器的连接端口，“IP 地址”栏填入 Web 服务器的 IP 地址（假设您的 Web 服务器的 IP 地址是 192.168.1.101），再在状态栏选择“生效”，点击“保存”按钮即可。如图：

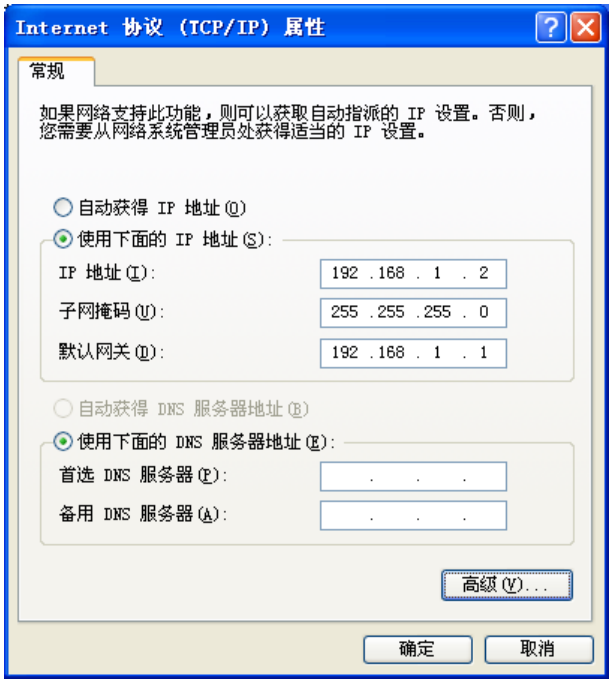

虚拟服务器
虚拟服务器定义了广域网服务端口和局域网网络服务器之间的映射关系，所有对该广域网服务端口的访问将会被重定位给通过IP地址指定的局域网网络服务器。
服务端口号：
80
（XX-XX or XX）
IP地址：
192.168.1.101
协议：
ALL
状态：
生效
常用服务端口号：
--请选择--
保 存
返 回
帮 助

附录 B　TCP/IP 的详细设置

在这一节中将详细介绍 TCP/IP 的配置(本部分内容以 Windows XP 为例)：

1. 打开“开始→控制面板”中的“网络连接”，右键点击“本地连接”图标，单击“属性”选项，出现如下图所示页面：

2. 双击“Internet 协议”（TCP/IP），出现如下图所示页面。如果您希望拥有固定的 IP 地址，请选择**使用下面的 IP 地址**和**使用下面的 DNS 服务器地址**，然后手动设置网络参数，其中 IP 地址为 192.168.1.2－192.168.1.254 范围内的任意值，参数设置可以参照下图设置：



3. 如果您希望自动从路由器获得 IP 地址，请选择自动获得 IP 地址和自动获得 DNS 服务器地址，点击确定后设置将生效。

附录 C　技术参数表格

支持的标准和协议		IEEE 802.3、IEEE 802.3u、IEEE 802.3x、TCP/ IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS
端口	LAN口	4个10/100M自适应RJ45端口（Auto MDI/MDIX）
	WAN口	1个10/100M自适应RJ45端口（Auto MDI/MDIX）
网络介质		10Base-T：3类或3类以上UTP
		100Base-TX：5类UTP
LED指示灯	LAN/WAN口	Link/Act（状态）
	其它	PWR（电源）、SYS（系统状态）
外形尺寸(L x W x H)		209mm x 126mm x 26mm
使用环境		工作温度：0ºC~40ºC
		存储温度：-40ºC~70ºC
		工作湿度：10%~90%RH 不凝结
		存储湿度：5%~90%RH 不凝结
电源输入		100-240V~ 50/60Hz 0.3A

深圳市普联技术有限公司
TP-LINK TECHNOLOGIES CO., LTD.
技术支持热线：400-8863-400
公司地址：深圳市南山区桃源街道平山大园工业区南区2栋1-6楼
技术支持E-mail：smb@tp-link.com.cn
http：//www.tp-link.com.cn