

MERCURY[®]

300M无线路由器

详细配置指南

声明

Copyright © 2014 深圳市美科星通信技术有限公司
版权所有，保留所有权利

未经深圳市美科星通信技术有限公司明确书面许可，任何单位或个人不得擅自仿制、复制、誊抄或转译本书部分或全部内容。不得以任何形式或任何方式（电子、机械、影印、录制或其他可能的方式）进行商品传播或用于任何商业、赢利目的。

MERCURY[®] 为深圳市美科星通信技术有限公司注册商标。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。除非有特殊约定，本手册仅作为使用指导，本手册中的所有陈述、信息等均不构成任何形式的担保。



联系方式

网址: www.mercurycom.com.cn

技术支持热线: 400-8810-500

技术支持 E-mail: fae@mercurycom.com.cn

目 录

第一章 产品概述.....	1
1.1 产品简介.....	1
1.2 主要特性.....	2
第二章 硬件描述.....	3
2.1 面板布置.....	3
2.1.1 前面板.....	3
2.1.2 后面板.....	4
2.2 复位.....	4
2.3 系统需求.....	4
2.4 安装环境.....	5
2.5 硬件安装.....	5
第三章 快速安装指南.....	7
3.1 建立正确的网络设置.....	7
3.2 快速安装指南.....	9
第四章 配置指南.....	14
4.1 启动和登录.....	14
4.2 运行状态.....	14
4.3 设置向导.....	16
4.4 网络参数.....	16
4.4.1 WAN 口设置.....	16
4.4.2 LAN 口设置.....	21
4.4.3 MAC 地址克隆.....	23
4.4.4 WAN 口速率/模式.....	23
4.5 无线设置.....	24
4.5.1 基本设置.....	24
4.5.2 无线安全设置.....	27
4.5.3 无线 MAC 地址过滤.....	29

4.5.4	无线高级设置.....	31
4.5.5	无线主机状态.....	32
4.6	带宽控制.....	32
4.7	DHCP 服务器.....	34
4.7.1	DHCP 服务设置.....	34
4.7.2	静态地址分配.....	35
4.7.3	客户端列表.....	36
4.8	路由功能.....	37
4.8.1	默认路由设置.....	37
4.8.2	静态路由表.....	38
4.9	转发规则.....	39
4.9.1	虚拟服务器.....	39
4.9.2	特殊应用程序.....	41
4.9.3	DMZ主机.....	42
4.9.4	UPnP设置.....	43
4.9.5	应用层网关设置.....	44
4.10	家长控制.....	44
4.11	防火墙.....	46
4.11.1	规则管理.....	46
4.11.2	内网主机.....	49
4.11.3	外网主机.....	50
4.11.4	日程计划.....	52
4.11.5	攻击防护.....	53
4.12	IP 与 MAC 绑定.....	55
4.12.1	静态 ARP 绑定设置.....	55
4.12.2	ARP 映射表.....	56
4.13	动态 DNS	57
4.14	系统管理.....	58
4.14.1	系统日志.....	58
4.14.2	诊断工具.....	59
4.14.3	流量统计.....	59
4.14.4	软件升级.....	60

4.14.5 恢复出厂设置.....	61
4.14.6 备份和载入配置.....	61
4.14.7 重启路由器.....	63
4.14.8 管理控制.....	64
4.14.9 时间设置.....	65
附录A FAQ.....	66
附录B IE浏览器设置.....	70
附录C 规格参数.....	72

第一章 产品概述

1.1 产品简介

水星 MW313R 300M 无线路由器专为满足小型企业、办公室和家庭办公室的无线上网需要而设计，它功能实用、性能优越、易于管理。

水星 MW313R 300M 无线路由器基于 IEEE 802.11n，它能扩展无线网络范围，提供最高达 300Mbps 的稳定传输，同时兼容 IEEE 802.11b 和 IEEE 802.11g 标准。传输速率的自适应性提高了其与其他网络设备进行互操作的能力。大范围的无线覆盖空间为您提供了自由轻松的网络环境。稳定的数据传输以及带宽供给为您的网上冲浪、MP3 下载、网络电话、文件共享、网络游戏等网络服务提供了强大的技术保证，实现无忧上网。

水星 MW313R 300M 无线路由器提供多重安全防护措施，可以有效保护用户的无线上网安全。支持 SSID 广播控制，有效防止 SSID 广播泄密；支持 64/128 位 WEP 无线数据加密，可以保证数据在无线网络传输中的安全。内置的特有防火墙功能，可以有效防止入侵，为用户的无线上网提供更加稳固的安全防护。

水星 MW313R 300M 无线路由器还提供多方面的管理功能，可以对 DHCP、DMZ 主机、虚拟服务器等进行管理；能够组建内部局域网，允许多台计算机共享一条单独宽带线路和 ISP 账号，并提供自动或按时连通和断开网络连接功能，节省用户上网费用。

水星 MW313R 300M 无线路由器采用全中文的配置界面，每步操作都配有详细的帮助说明。特有的快速配置向导更能帮您轻松快速地实现网络连接。为了充分利用该款路由器的各项功能，请仔细阅读该详细配置指南。

提示：

在本手册中，

- 所提到的路由器，如无特别说明，系指水星 300M 无线路由器，下面以 MW313R 为例进行说明。
- 用“→”符号说明在 WEB 界面上的操作引导，其方法是单击菜单、选项、按钮等。
- 路由器配置界面的菜单或按钮名采用“宋体+加粗”字表示，其它选项名或操作项等用“”（引号）表示。
- 图片界面都配有相关参数，这些参数主要是为您正确配置产品参数提供参考。实际产品的配置界面并没有提供，您可以根据实际需要设置这些参数。

1.2 主要特性

- 提供一个 10/100M 以太网(WAN)接口，可接 xDSL Modem/Cable Modem/Ethernet
- 内部集成四口交换机，提供四个 10/100M 以太网(LAN)接口
- 支持最高达 300Mbps 的无线传输速率，具备速率自适应功能，可以自动调整无线传输速率
- 支持 64/128 位 WEP 加密，WPA/WPA2、WPA-PSK/WPA2-PSK 等加密与安全机制，可以保证数据在无线网络传输中的安全
- 支持 11b only、11g only、11n only、11bg mixed 和 11bgn mixed 等多种无线模式
- 支持 SSID 广播控制，有效防止 SSID 广播泄密
- 支持 WDS 功能，扩大无线网络覆盖范围
- 内置网络地址转换(NAT)功能，支持虚拟服务器、特殊应用程序和 DMZ 主机
- 内置 DHCP 服务器，同时可进行静态地址分配
- 支持通用即插即用(UPnP)，符合 UPnP 标准的数据可顺利通过
- 内置防火墙功能，支持域名过滤和 MAC 地址过滤，可以有针对地开放指定计算机的上网权限
- 支持 DoS 攻击防范，具有病毒自动隔离功能
- 支持 IP 与 MAC 绑定功能，可以有效防止网络攻击
- 支持动态 DNS 功能，能够为动态 IP 地址提供域名服务
- 内置静态路由功能，可以根据需要构建特殊网络拓扑
- 支持软件升级，可以免费获得路由器的最新软件
- 可以根据上网动作，自动或按时连通和断开网络连接
- 支持远程和 WEB 管理，全中文配置界面，配备简易安装向导(Wizard)

第二章 硬件描述

2.1 面板布置

2.1.1 前面板

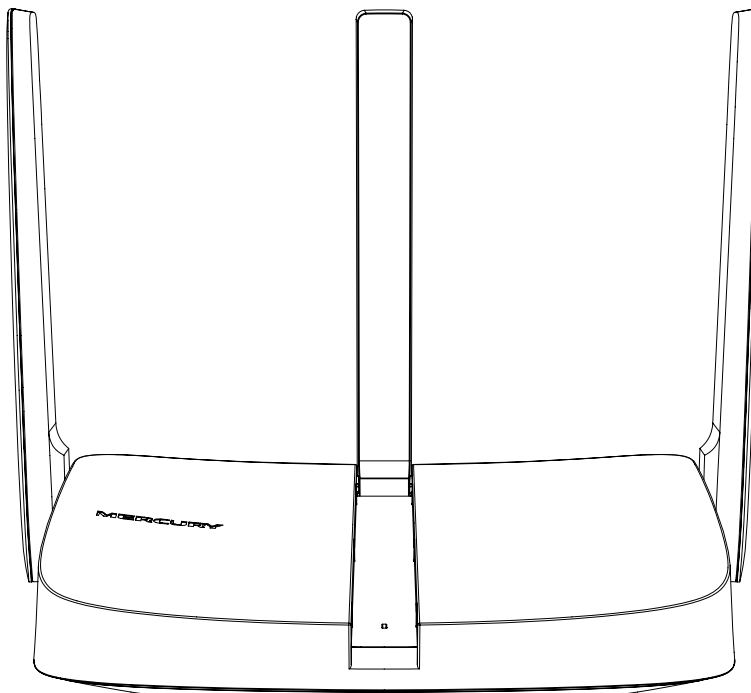


图 1 MW313R 前面板示意图

指示灯:

指示灯	指示状态
常亮	系统正常
慢闪	WAN 口有数据传输
快闪 10 下	有设备接入

2.1.2 后面板

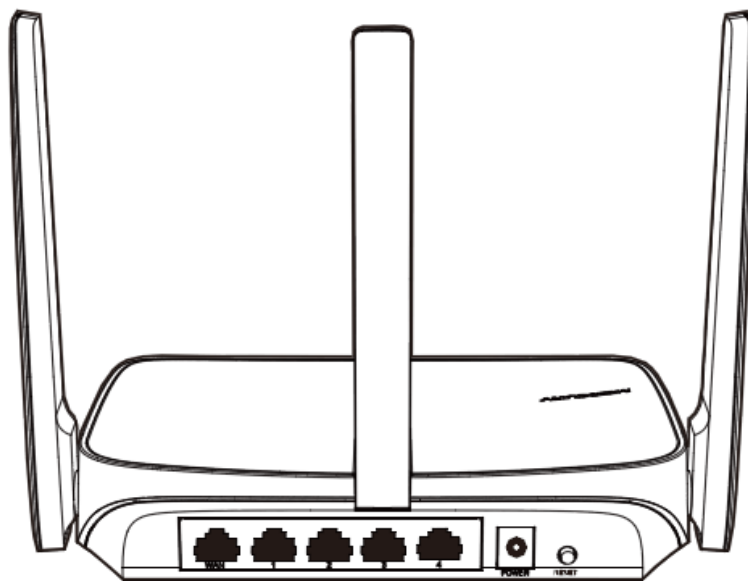


图 2 MW313R 后面板示意图

- 1) **WAN:** 广域网端口插孔(RJ45)。该端口用来连接以太网电缆或 xDSL Modem/Cable Modem。
- 2) **1/2/3/4:** 局域网端口插孔(RJ45)。该端口用来连接局域网中的集线器、交换机或安装了网卡的计算机。
- 3) **POWER:** 电源插孔，用来连接电源，为路由器供电。

☞ 注意:

为保证设备正常工作，请使用该机型配套电源。

- 4) **RESET:** 复位按钮。长按该按钮，用来使设备恢复到出厂默认设置。

2.2 复位

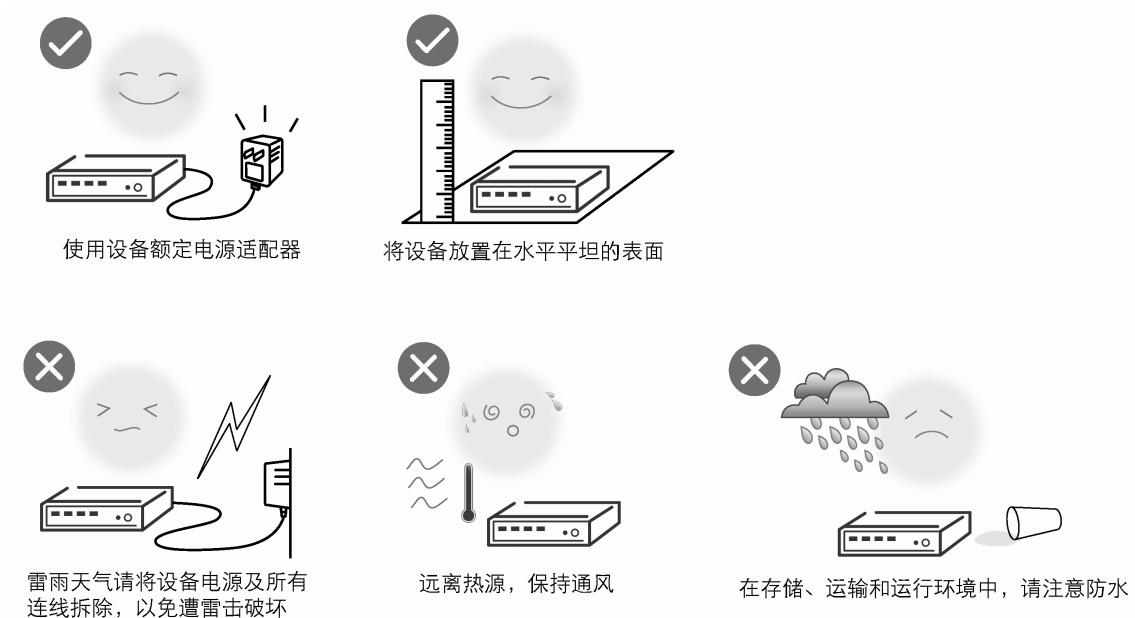
若要将路由器系统设置恢复为出厂默认设置，请按压 **RESET** 按钮 5 秒钟以上，当系统指示灯快速闪烁时放开按钮，路由器将重启，重启完毕后路由器将成功恢复为出厂设置。

2.3 系统需求

- 宽带 Internet 服务(接入方式为以太网电缆接入或通过 xDSL/Cable Modem 接入)
- 具有 RJ45 口的调制解调器(直接使用以太网电缆接入时不需要此设备)
- 每台 PC 的以太网连接设备(无线网卡或有线网卡及网线)
- 支持 TCP/IP 协议的操作系统
- Web 浏览器，如 Microsoft Internet Explorer、Mozilla Firefox、Apple Safari 等

2.4 安装环境

本路由器可放置在办公室或家中任何方便的位置，但是为了保证设备长期正常工作，请注意下列安全事项：



2.5 硬件安装

在安装路由器前，我们希望您已经能够利用您的宽带服务在单台计算机上成功上网。如果您单台计算机上宽带网有问题，请先和您的网络服务商（ISP）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您的路由器。切记安装时拔除电源插头，保持双手干燥。

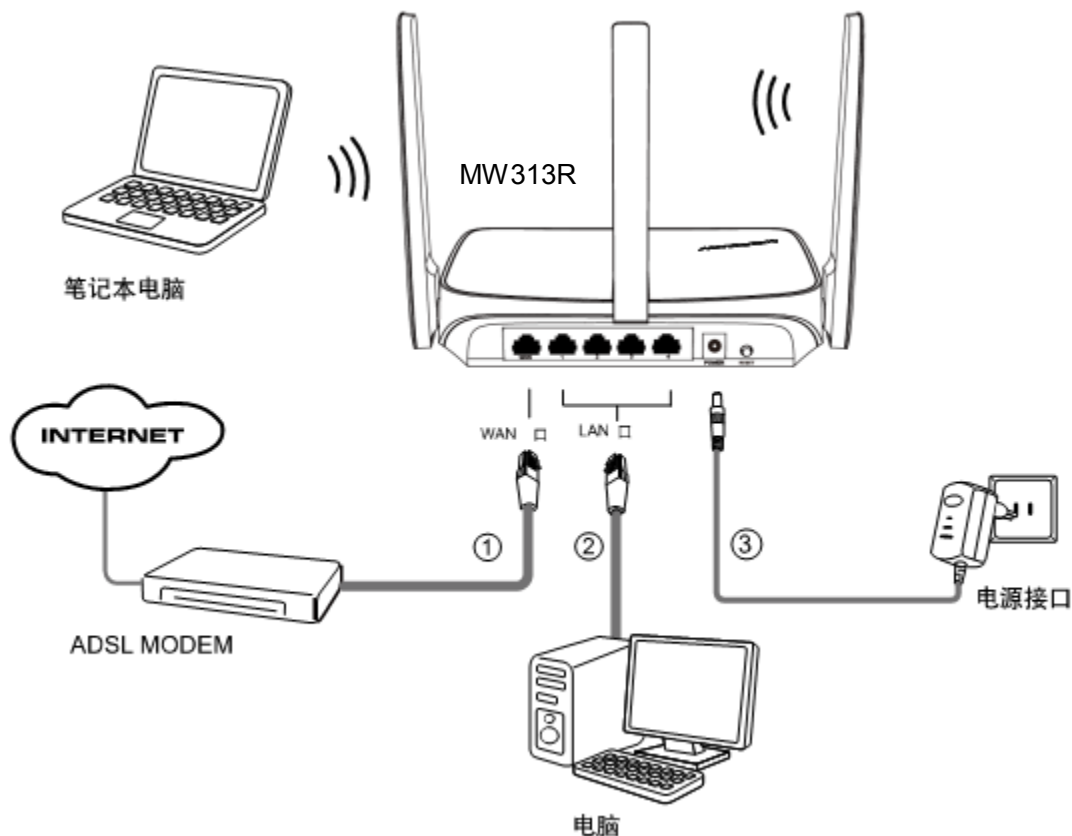


图 3 硬件连接图

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。您也可以一根网线将路由器与您的计算机网卡直接相连。

2. 建立广域网连接

用网线连接路由器和 xDSL/Cable Modem 或以太网。

3. 连接电源

连接好电源，路由器将自行启动。

👉 注意：

无线宽带路由器允许您通过有线或无线方式进行连接，但是第一次配置时，我们推荐您使用有线方式连接。以下设置步骤，均基于有线连接。

第三章 快速安装指南

3.1 建立正确的网络设置

要正确使用路由器，首先请按照 2.5 节的硬件安装方法连接好线路，并打开电源开关。接下来您还必须合理配置网络。下面以 Windows XP 为例，讲述具体配置过程。如果只进行基本配置，您只需阅读本章内容；如果要进行高级配置，请继续阅读第四章内容。

注意：

设备默认 IP 地址是 192.168.1.1，默认子网掩码是 255.255.255.0。这些值可以根据您的实际需要而改变，但本用户手册将按默认值说明。

计算机 IP 地址设置：

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



图 4 TCP/IP 协议属性

2. 双击“Internet 协议”（TCP/IP），接下来推荐您设定计算机为自动获取IP地址方式，如下图所示请选择自动获得IP地址，自动获得DNS服务器地址。

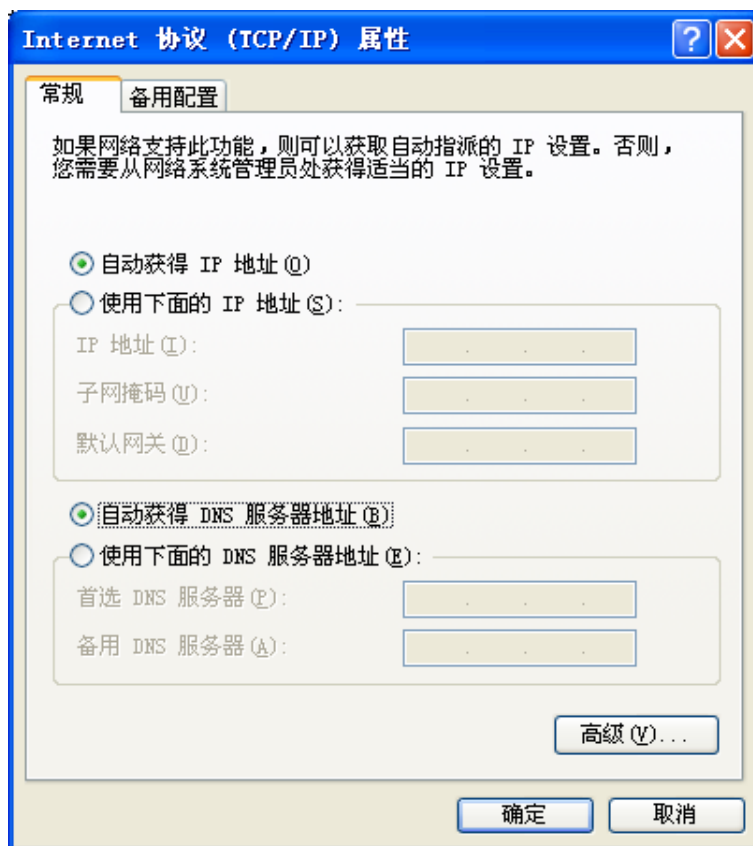


图 5 计算机 IP 设置

注意：

- 1) MW313R内置DHCP服务器并默认为启用，因此推荐您设定计算机为自动获取IP地址方式，即在设备初始状态下，计算机可以利用DHCP服务器自动获取IP地址。
- 2) 如果您需要手动配置IP地址，请在图5中选择使用下面的IP地址和使用下面的DNS服务器地址。并设置您计算机的IP地址为192.168.1.x（x可以是2至254之间的任意整数），子网掩码为255.255.255.0，默认网关为192.168.1.1，DNS服务器地址请向您的网络服务提供商咨询。

在设置好TCP/IP协议后，您可以使用Ping命令检查您的计算机和路由器之间是否联通。执行Ping命令，操作步骤如下：

1. 首先请您单击桌面的“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，然后回车或单击“确认”键即可进入Windows命令行模式。
2. 在该界面中输入命令Ping 192.168.1.1（设备默认的IP地址是192.168.1.1）并按回车键，如果屏幕显示为：

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=6ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms
```

那么恭喜您！您的计算机已与设备成功建立连接。

如果屏幕显示为：

```
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

这说明设备还未安装好，您可以按照下列顺序检查：

1. 硬件连接是否正确？

 提示：

设备面板上对应局域网端口的LAN状态指示灯（1/2/3/4）和您计算机上的网卡灯必须亮。

2. 设备的IP地址是否为默认的值192.168.1.1？

 提示：

如果不确定设备是否为默认的IP地址192.168.1.1，您可以按照2.2节所述的复位方法，将设备恢复为出厂默认设置。

3. 您的计算机的TCP/IP设置是否正确？

 提示：

如果设备的IP地址为192.168.1.1，那么在手动配置计算机IP地址时，必须为192.168.1.x（x可以是2至254之间的任意整数）。

3.2 快速安装指南

本产品提供基于 Web 浏览器（如 Internet Explorer）的配置界面，这种配置方案适宜于任何 MS Windows, Macintosh 或 UNIX 平台。下面以 IE 浏览器为例进行说明（基本设置请参见附录 B IE 浏览器设置）。

开启 IE 浏览器程序，在地址栏中输入“http://192.168.1.1”，回车确认后您将会看到下图所示登录页面，在“设置密码”框中为路由器设置登录密码，在“确认密码”框中再次输入后，单击“确认”按钮。

为保护路由器安全，请务必设置管理员密码



图 6 设置密码

输入上一步设置的登录密码，单击“确认”。

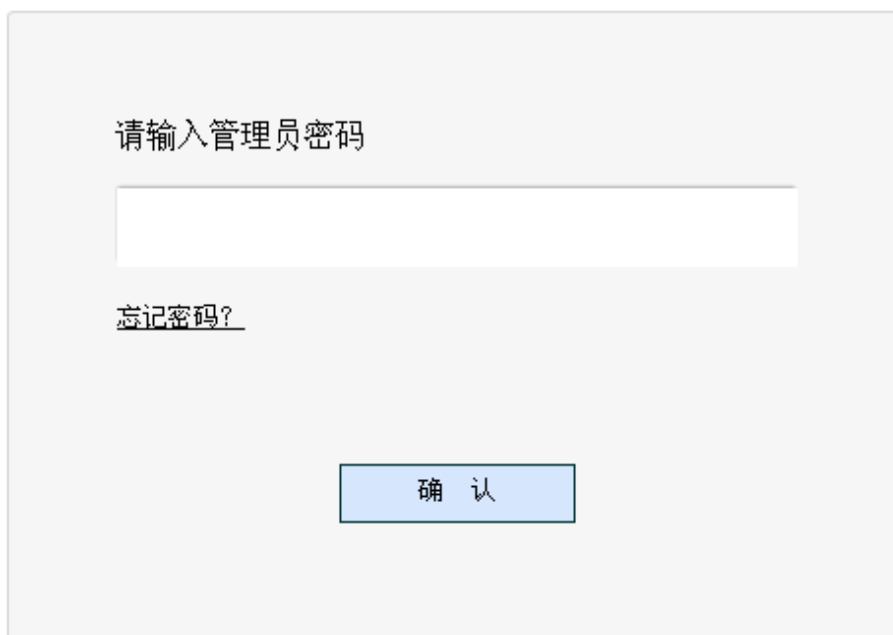


图 7 登录设备

如果名称和密码正确，浏览器将显示管理员模式的画面，并会弹出一个设置向导的画面（如果没有自动弹出的话，可以单击管理员模式画面左边菜单中的“设置向导”将它激活）。



图 8 设置向导

单击“下一步”，进入上网方式选择页面。页面显示了最常用的几种上网方式，您可以根据自身情况进行选择，然后单击“下一步”。

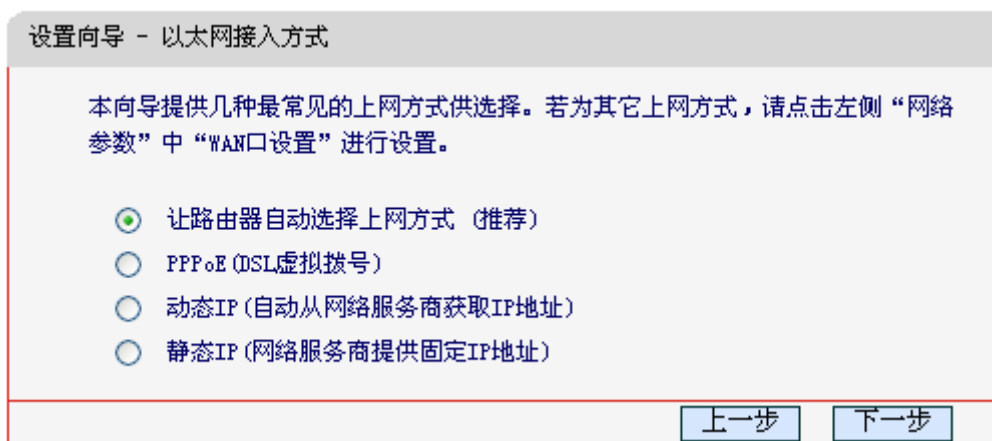


图 9 上网方式选择

以上画面显示了最常用的几种上网方式，请根据 ISP 提供的上网方式进行选择，然后点击下一步填写 ISP 提供的网络参数。

1. PPPoE (DSL 虚拟拨号)

如果您的上网方式为 PPPoE，即 DSL 虚拟拨号方式，则您需要填写以下内容：

图 10 上网方式—PPPoE

- 用户名：填入 ISP 为您指定的 ADSL 上网帐号，不清楚可以向 ISP 询问。
- 密码：填入 ISP 为您指定的 ADSL 上网口令，不清楚可以向 ISP 询问。
- 密码确认：确认之前填入的上网口令，防止错误发生。

2. 动态 IP（自动从网络服务商获取 IP 地址）

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，则您不需要填写任何内容即可直接上网。

3. 静态 IP（网络服务商提供固定 IP 地址）

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，则需要填写以下内容：

图 11 上网方式—静态 IP

- IP 地址：本路由器对广域网的 IP 地址，即 ISP 提供给您的 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 提供给您的子网掩码，一般为 255.255.255.0。
- 默认网关：填入 ISP 提供给您的网关，不清楚可以向 ISP 询问。
- DNS 服务器：填入 ISP 提供给您的 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 提供给您了两个 DNS 服务器地址，则您可以把另一个 DNS 服务器地址的 IP 地址填于此。

设置完成后，单击下一步，您将看到图 12所示的基本无线网络参数设置页面。

设置向导 - 无线

本页设置无线网络的基本参数。

无线功能：

SSID：

信道：

模式：

加密方式：

WPA-PSK/WPA2-PSK

密码：

(最短为8个字符，最长为63个ASCII码字符或64个16进制字符)

无加密

图 12 设置向导—无线

- SSID：设置任意一个字符串来标明您的无线网络。
- WPA-PSK/WPA2-PSK：您路由器无线网络的加密方式，如果选择了该项，请在**密码**中输入您想要设置的密码，密码要求为 **64** 个十六进制字符或 **8-63** 个 ASCII 码字符。
- 无加密：关闭无线安全功能，即您路由器的无线网络不加密。

 **注意：**

以上提到的信道带宽设置仅针对支持 IEEE 802.11n 协议的网络设备，对于不支持 IEEE 802.11n 协议的设备，此设置不生效。

设置完成后，单击**下一步**，在弹出的页面确认已设置的参数，点击“保存”保存配置并生效。在弹出的图 13所示的设置向导完成界面，单击**完成**结束设置向导。

设置向导 - 完成

设置状态：

正在设置系统模式	成功
正在配置WAN口连接	成功
正在配置默认网关和DNS	成功
正在配置无线	成功

设置已生效，请点击“完成”退出设置向导。

提示：若设备仍不能正常上网，请点击左侧“网络参数”进入“WAN口设置”栏目，确认是否设置了正确的WAN口连接类型和拨号模式。

图 13 设置向导—完成

第四章 配置指南

4.1 启动和登录

启动路由器并成功登录路由器管理页面后，浏览器会显示管理员模式的界面，如图 14。

在左侧菜单栏中，共有如下几个菜单：**运行状态**、**设置向导**、**网络参数**、**无线设置**、**带宽控制**、**DHCP 服务器**、**路由功能**、**转发规则**、**家长控制**、**防火墙**、**IP 与 MAC 绑定**、**动态 DNS** 和 **系统管理**。单击某个菜单项，您即可进行相应的功能设置。下面将详细讲解各个菜单的功能。



图 14 启动和登录

4.2 运行状态

选择菜单**运行状态**，您可以查看路由器当前的状态信息，包括版本信息、WAN 口状态、LAN 口状态、WLAN 状态信息，如图 15。

版本信息

当前软件版本： 0.9.0 1.0 v102a.0 Build 140114 Rel.49807n
 当前硬件版本： MW313R v1 00000001
 运行时间： 0 day(s) 00:18:58

WAN口状态

MAC地址： 00:0A:EB:13:09:6A
 IP 地址： 0.0.0.0 PPPoE拨号
 子网掩码： 0.0.0.0
 网关： 0.0.0.0
 DNS服务器： 0.0.0.0 0.0.0.0

LAN口状态

MAC地址： 00:0A:EB:13:09:69
 IP 地址： 192.168.1.1
 子网掩码： 255.255.255.0
 DHCP： 启用

WLAN状态

状态： 已开启
 SSID： MERCURY_130969
 信道： 自动(信道 1)
 频段带宽： 自动
 模式： 11bgn Mixed
 加密方式： WPA-PSK/WPA2-PSK
 MAC地址： 00:0A:EB:13:09:69
 最大传输速率： 300Mbps
 WDS状态： 未开启

图 15 运行状态

- 版本信息：此处显示路由器当前的软硬件版本号。
- WAN口状态：此处显示路由器当前WAN口的MAC地址、IP地址、子网掩码、网关和DNS服务器地址。
- LAN口状态：此处显示路由器当前LAN口的MAC地址、IP地址和子网掩码。
- WLAN状态：此处显示路由器当前的无线设置状态，包括SSID、频段和频段带宽信息。

4.3 设置向导

详见[3.2 快速安装指南](#)。

4.4 网络参数

选择菜单**网络参数**，您可以看到：



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 WAN口设置

选择菜单**网络参数**→**WAN口设置**，您可以在随后出现的界面中配置WAN口的网络参数。

WAN是广域网(Wide Area Network)的缩写。在WAN设置中全部IP信息都是公有IP地址，可以在互联网上访问。该WAN口一共提供3种上网方式：动态IP、静态IP、PPPoE。具体配置时，请首先选择您所需要的WAN口连接类型，即上网方式。如果您不清楚您的上网方式，请咨询您的ISP（网络服务提供商）。本路由器默认上网方式为动态IP。

1. 动态IP

选择**动态IP**，路由器将从ISP（网络服务提供商）自动获取IP地址。当ISP未给您提供任何IP网络参数时，请选择这种连接方式。如图16。

以太网接入设置

本页面进行以太网接入设置。

以太网接入类型：

IP地址：

子网掩码：

网关：

选择系统默认网关：

数据包MTU(字节)： (默认值1500，如非必要，请勿修改)

启用NAT

启用Fullcone NAT

启用SPI防火墙

启用IGMP多播代理

单播方式获取IP (一般情况下请勿选择)

手动设置DNS服务器

主机名：

图 16 WAN 口设置-动态 IP

- 更新：单击**更新**按钮，路由器将从ISP的DHCP服务器动态得到IP地址、子网掩码、网关以及DNS服务器，并在界面中显示出来。
- 释放：单击**释放**按钮，路由器将发送DHCP释放请求给ISP的DHCP服务器，释放IP地址、子网掩码、网关以及DNS服务器设置。
- 选择系统默认网关：从下拉菜单中选择一条连接，该连接对应的网关为本 300M 无线路由器的默认网关。

点击“**高级**”，展开 WAN 口服务设置高级选项。

- 数据包 MTU：MTU 全称为最大数据传输单元，缺省为 1500。请向 ISP 咨询是否需要更改。如非特别需要，一般不要更改。
- 启用 NAT：NAT（网络地址转换）将私网 IP 地址转换为公网 IP 地址，默认开启。如果有其他路由器工作在您所在的网络，请勿启用该功能。
- 启用 Fullcone NAT：NAT 的一种，关闭该功能，则启用默认 NAT。
- 启用 SPI 防火墙：开启时只有内网主动发起的请求才可以建立连接，所有来自外网的请求均被此防火墙拒绝；关闭时内、外网发起的请求均可以建立连接，而这将导致内网中的主机都暴露给外网，存在安全隐患。

- 启用IGMP多播代理：IGMP协议用于管理Internet网络上的组播，某些ISP通过IGMP为用户端设备提供远程配置服务。默认关闭，如不清楚，请向ISP咨询。
- 单播方式获取IP：少数网络服务商的DHCP服务器不支持广播的请求方式，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。（一般情况下不需要选择此项）
- DNS服务器、备用DNS服务器：该处显示从ISP处自动获得的DNS服务器地址。若选择**手动设置DNS服务器**，则您可以在此处手动设置DNS服务器和备用DNS服务器(至少设置一个)，连接时，路由器将优先使用手动设置的DNS服务器。
- 主机名：设置路由器的主机名。ISP的DHCP服务器可以通过主机名识别您的身份。

完成更改后，单击**保存**按钮。

2. 静态 IP

当 ISP 给您提供了所有 WAN IP 信息时，请选择**静态 IP**，并在下图 17 界面中输入 IP 地址、子网掩码、网关和 DNS 地址(一个或多个)。具体设置网络参数时，若不清楚，请咨询 ISP。如图 17。

以太网接入设置

本页面进行以太网接入设置。

以太网接入类型：静态IP 自动检测

IP地址：

子网掩码：

网关： (可选)

DNS服务器： (可选)

备用DNS服务器： (可选)

选择系统默认网关：

数据包MTU(字节)： (默认值1500，如非必要，请勿修改)

启用NAT

启用Fullcone NAT

启用SPI防火墙

启用IGMP多播代理

图 17 WAN 口设置-静态 IP

- IP地址：本路由器对广域网的IP地址。请填入ISP提供的公共IP地址，必须设置。
- 子网掩码：本路由器对广域网的子网掩码。请填入ISP提供的子网掩码。根据不同的网络类型子网掩码不同，一般为255.255.255.0(C类)。
- 网关：请填入ISP提供给你的网关。它是连接的ISP的IP地址。

- **DNS服务器、备用DNS服务器：**ISP一般至少会提供一个DNS(域名服务器)地址，若提供了两个DNS地址则将其中一个填入“备用DNS服务器”栏。

点击“**高级**”，展开WAN口服务设置高级选项。

- **数据包 MTU：**MTU 全称为最大数据传输单元，缺省为 1500。请向 ISP 咨询是否需要更改。如非特别需要，一般不要更改。
- **启用 NAT：**NAT（网络地址转换）将私网 IP 地址转换为公网 IP 地址，默认开启。如果有其他路由器工作在您所在的网络，请勿启用该功能。
- **启用 Fullcone NAT：**NAT 的一种，关闭该功能，则启用默认 NAT。
- **启用 SPI 防火墙：**开启时只有内网主动发起的请求才可以建立连接，所有来自外网的请求均被此防火墙拒绝；关闭时内、外网发起的请求均可以建立连接，而这将导致内网中的主机都暴露给外网，存在安全隐患。
- **启用 IGMP 多播代理：**IGMP 协议用于管理 Internet 网络上的组播，某些 ISP 通过 IGMP 为用户端设备提供远程配置服务。默认关闭，如不清楚，请向 ISP 咨询。

完成更改后，单击**保存**按钮。

3. PPPoE

如果 ISP 给您提供的是 **PPPoE**(以太网上的点到点连接),ISP 会给您提供上网账号和上网口令。具体设置时,若不清楚,请咨询 ISP。如图 18。

以太网接入设置

本页面进行以太网接入设置。

以太网接入类型：

用户名：

密码：

密码确认：

特殊拨号：

根据您的需要，请选择对应的连接模式：

按需连接，在有访问时自动连接
自动断线等待时间： 分钟（0 表示不自动断线）

自动连接，在开机和断线后自动连接

手动连接，由用户手动连接
自动断线等待时间： 分钟（0 表示不自动断线）

选择认证类型：

选择系统默认网关：

图 18 WAN 口设置-PPPoE

- 用户名、密码、密码确认：请正确填入ISP提供的上网账号和口令，必须填写。
- 特殊拨号：由于某些ISP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提供的7种特殊拨号模式。
- 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，可以选择该项连接方式，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，保护您的上网资源。此项设置仅对“按需连接”和“手动连接”生效。
- 自动连接：若选择**自动连接**模式，则在开机后系统自动进行连接。在使用过程中，如果由于外部原因，网络被断开，系统则会每隔一段时间(10秒)尝试连接，直到成功连接为止。若您的网络服务是包月交费形式，可以选择该项连接方式。
- 手动连接：选择该项，开机后需要用户手动才能进行拨号连接，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。若您的网络服务是按使用时间进行交费,可以选择该项连接方式。

- 连接/断开: 单击此按钮,可进行即时的连接/断线操作。

若需要进一步设置,可以单击**高级**按钮,在下图19界面中进行高级设置。

Figure 19 shows the advanced settings for the WAN port in PPPoE mode. The interface includes the following fields and options:

- 服务名:** [Empty text box] (如非必要,请勿修改)
- 服务器名:** [Empty text box] (如非必要,请勿修改)
- 数据包MTU(字节):** [1480] (默认值1480,如非必要,请勿修改)
- 启用Fullcone NAT:**
- 启用SPI防火墙:**
- 启用IGMP多播代理:**
- 使用ISP指定的IP地址:**
- 在线检测间隔时间:** [0] (0~120秒,0表示不发送)
- 手动设置DNS服务器:**

A **保存** (Save) button is located at the bottom left of the settings panel.

图 19 WAN 口设置-PPPoE-高级设置

- 服务名、服务器名: 如果不是ISP特别要求,请不要填写这两项。
- 数据包MTU: 填入网络数据包的MTU值,缺省为1480,如非特别需要,一般不要更改。
- 使用ISP指定IP地址: 该项仅适用于静态PPPoE。如果您的ISP提供上网账号和口令时,亦提供了IP地址,请选中此选择框,并输入PPPoE连接的静态IP地址。
- 在线检测间隔时间: 设置该值后,路由器将根据指定的时间间隔发送检测信号,以检测服务器是否在线。如果该值为0,则表示不发送检测信号。
- DNS服务器、备用DNS服务器: 该处显示从ISP处自动获得的DNS服务器地址。若选择**手动设置DNS服务器**,则您可以在此处手动设置DNS服务器和备用DNS服务器(至少设置一个),连接时,路由器将优先使用手动设置的DNS服务器。

完成更改后,单击**保存**按钮。

4.4.2 LAN口设置

选择菜单**网络参数**→**LAN口设置**,您可以在下图20界面中配置LAN接口的网络参数。如果需要,可以更改LAN接口IP地址以配合实际网络环境的需要。

LAN口设置

本页面进行LAN口服务设置。

注意：当LAN口IP参数（包括IP地址、子网掩码）发生变更时，为确保DHCP server能够正常工作，应保证DHCP server中设置的地址池、静态地址与新的LAN口IP是处于同一网段。

所属分组：	Default	
IP地址：	<input type="text" value="192.168.1.1"/>	
子网掩码：	<input type="text" value="255.255.255.0"/>	
启用第二IP	<input type="checkbox"/>	
DHCP服务器：	<input type="radio"/> 不启用 <input checked="" type="radio"/> 启用 <input type="radio"/> DHCP Relay	
地址池开始地址：	<input type="text" value="192.168.1.100"/>	
地址池结束地址：	<input type="text" value="192.168.1.199"/>	
地址租期：	<input type="text" value="1440"/> 分钟（1~2880分钟，缺省为1440分钟）	
网关：	<input type="text" value="192.168.1.1"/>	（可选）
缺省域名：	<input type="text"/>	（可选）
主DNS服务器：	<input type="text" value="0.0.0.0"/>	（可选）
备用DNS服务器：	<input type="text" value="0.0.0.0"/>	（可选）

图 20 LAN 口设置

- 所属分组：LAN口所属分组的组名。
- IP地址：LAN口所在组对局域网的IP地址。Default组出厂默认值为192.168.1.1，您可以根据需要改变它。
- 子网掩码：LAN口所在组对局域网子网掩码。您可以根据实际的网络状态输入不同的子网掩码。
- 启用第二IP：点击“启用第二IP”，您可以为LAN口所在组设置第二对IP地址和子网掩码。通过第二IP，您也可以登录300M无线路由器的WEB管理界面。

具体DHCP服务器设置，请参见[4.7.1 DHCP服务设置](#)。

完成更改后，单击**保存**按钮以使现有设置生效。

 **注意：**

- 1) 如果改变了本地IP地址，您必须用新的IP地址才能登录路由器的WEB管理界面，并且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。
- 2) 局域网中所有计算机的子网掩码必须与此处子网掩码设置相同。
- 3) 如果您所设置的新的LAN口IP地址与原来的LAN口IP地址不在同一网段的话，路由器的动态IP服务将会自动更改到新LAN口IP所在的网段；但是虚拟服务器（DHCP Server）和DMZ主机功能将失效，因为DHCP设置中的地址池、静态地址，DMZ主机设置中的主机IP地址，与LAN口IP地址必须处于同一网段。如果您希望启用这些功能，请重新对其进行设置。

4.4.3 MAC地址克隆

选择菜单**网络参数**→**MAC地址克隆**，您可以在下图 21 界面中设置路由器对广域网的 MAC 地址。

WAN 连接	MAC地址	操作
当前PC的MAC	90:2B:34:65:39:3E	克隆到 pppoe_eth1_d
pppoe_eth1_d	00:0A:EB:13:09:6A	恢复出厂MAC

保存

图 21 MAC 地址克隆

- **MAC地址**：此项为路由器对广域网的MAC地址，默认的MAC地址为路由器上WAN的物理接口MAC地址。某些ISP可能会要求对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。不建议更改MAC地址，除非ISP有特别要求。
- **当前PC的MAC**：此处显示当前正在管理路由器的计算机的MAC地址。
- **恢复出厂MAC**：单击此按钮，即可恢复MAC地址为出厂时的默认值。
- **克隆**：单击此按钮，可将当前管理PC的MAC地址克隆到“MAC地址”栏内。若您的ISP提供服务时要求进行MAC地址克隆，则应进行该项操作，否则无须克隆MAC地址。

完成更改后，单击**保存**按钮，路由器会自动重启。

☞ 注意：

只有局域网中的计算机才能使用“MAC地址克隆”功能。

4.4.4 WAN口速率/模式

选择菜单**网络参数**→**WAN口速率/模式**，下图 22 界面将显示路由器当前的双工模式，且您可在该界面中配置 WAN 口速率模式。WAN 口速率和双工模式可调能够解决路由器与某些小区宽带的兼容性问题。例如小区宽带线路被强制为 10Mbps，将路由器 WAN 口强制为 10Mbps 即可正常使用。

当前模式： 自动协商

模式设置： 自动协商

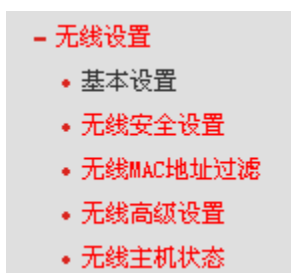
保存

图 22 WAN 口速率和双工模式

- 当前模式：显示路由器当前的WAN口速率模式。
- 模式设置：该选项可配置路由器的WAN口速率模式。可选择自动协商、100Mbps全双工、100Mbps半双工、10Mbps全双工和10Mbps半双工。

4.5 无线设置

选择菜单**无线设置**，您可以看到：



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 基本设置

选择菜单**无线设置**→**基本设置**，您可以在下图 23 界面中设置无线网络的基本参数和安全认证选项。

无线功能是该路由器的一项重要功能，利用该功能，可以组建内部无线网络。组建网络时，内网主机需要一张无线网卡来连接无线网络。**Service Set IDentification (SSID)**和信道是路由器无线功能必须设置的参数，各项的详细设置情况见下面所述。

The image shows the '无线基本设置' (Wireless Basic Settings) configuration page. It includes the following fields and options:

- SSID: MERCURY_130969
- 模式: 11bgn mixed
- 信道: 自动
- 频段带宽: 自动
- 开启无线功能
- 开启SSID广播
- 开启WDS

A '保存' (Save) button is located at the bottom left of the configuration area.

图 23 无线网络基本设置

- SSID：该项标识无线网络的名称。
- 模式：该项用于设置您路由器的无线工作模式，推荐使用11bgn mixed模式。
- 信道：该项用于选择无线网络工作的频率段，可以选择的范围从1到13。如果您选择的是自动，则AP会自动根据周围的环境选择一个最好的信道。
- 频道带宽：设置无线数据传输时所占用的信道宽度，可选项为：20MHZ、40MHZ。

 **注意：**

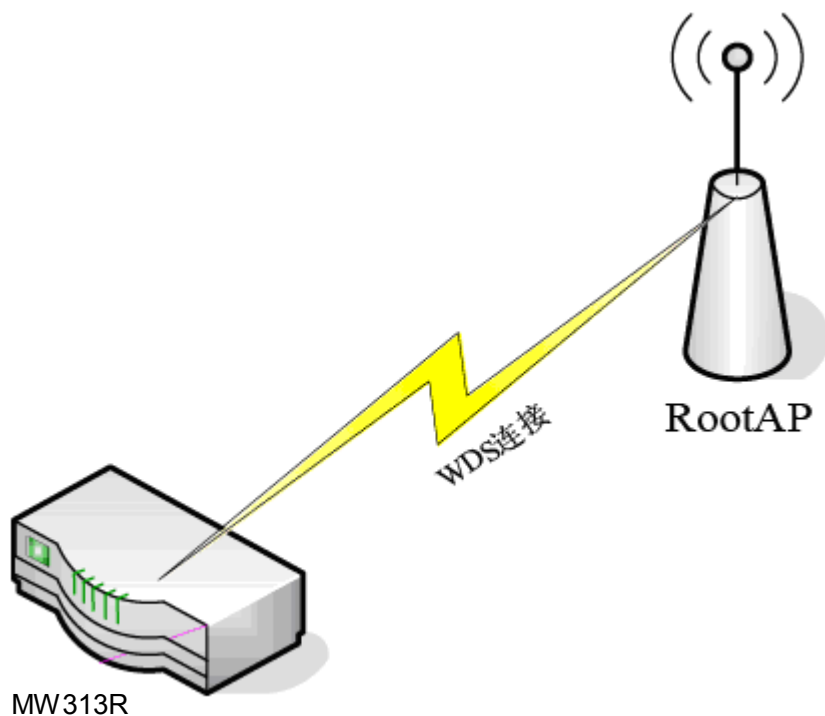
以上提到的频道带宽设置仅针对支持 IEEE 802.11n 协议的网络设备，例如，当本路由器与 11N 系列网卡客户端进行通信时；对于不支持 IEEE 802.11n 协议的设备，此设置不生效。

- 开启无线功能：若要采用路由器的无线功能，必须选择该项，这样，无线网络内的主机才可以接入并访问有线网络。
- 开启SSID广播：该项功能用于将路由器的SSID号向无线网络内的主机广播，这样，主机将可以扫描到SSID号，并可以选择将路由器加入该SSID标识的无线网络。
- 开启WDS：该项功能用于桥接多个无线局域网。如果您开启了这个功能，请将要桥接的AP的信息正确填写到下面的配置页面中。
 - （桥接的）SSID：请填入您要桥接的AP的SSID。
 - （桥接的）BSSID：请填入您要桥接的AP的BSSID。
 - 扫描：单击此按钮扫描您路由器周围的无线局域网。
 - 密钥类型：这个选项需要根据您桥接的AP的加密类型来设定，注意：最好情况下应该保持这个加密方式和您AP设定的加密方式相同。
 - WEP密钥序号：如果密钥类型选择的是WEP加密，请选择您要桥接的AP的WEP密钥的序号。
 - 认证类型：如果密钥类型选择的是WEP加密，请选择您要桥接的AP的认证类型。
 - 密钥：请正确填入您要桥接的AP设置的密钥。

完成更改后，点击**保存**按钮并重启路由器使现在的设置生效。

 **注意：**

WDS连接的拓扑图如下所示，其中RootAP表示MW313R要桥接的AP。



- 1) 基本设置中开启WDS后需要填写的信息：“桥接的SSID”、“桥接的BSSID”、“密钥类型”、“WEP密钥序号”、“认证类型”、“密钥”，这些信息必须和RootAP配置的信息保持一致，否则可能会影响MW313R无线的正常工作。
- 2) 推荐MW313R的无线安全设置使用和RootAP相同的加密方式。
- 3) 如果MW313R和RootAP使用的都是WEP加密且序号相同，则必须保证这两个WEP密钥相同。
- 4) RootAP只需要保证开启AP功能且支持WDS，不需要进行其他配置。至于RootAP是否支持WDS，请咨询RootAP的厂商。
- 5) 推荐使用MW313R管理页面中的扫描功能来获取RootAP的相关信息。

4.5.2 无线安全设置

选择菜单无线设置→无线安全设置，您可以在图 24 界面中设置无线网络安全选项。

无线安全设置

为保障网络安全，强烈推荐开启安全设置，并使用WPA2-PSK AES加密方法。

关闭无线安全选项

WEP

认证类型：

WEP密钥格式：

密钥选择 WEP密钥 密钥类型

密钥1：	<input checked="" type="radio"/>	<input type="text"/>	<input type="text" value="禁用"/>
密钥2：	<input type="radio"/>	<input type="text"/>	<input type="text" value="禁用"/>
密钥3：	<input type="radio"/>	<input type="text"/>	<input type="text" value="禁用"/>
密钥4：	<input type="radio"/>	<input type="text"/>	<input type="text" value="禁用"/>

WPA-PSK/WPA2-PSK

认证类型：

加密算法：

PSK密码：

（最短为8个字符，最长为63个ASCII码字符或64个16进制字符）

组密钥更新周期： （单位为秒，最小值为30，不更新则为0）

图 24 无线网络安全设置

在无线网络安全设置页面，您可以选择开启或者不开启无线安全功能。

- 如果您无需开启无线安全功能，请选中**关闭无线安全选项**以关闭无线安全功能。
- 如果您要开启无线安全功能，则请选择页面中两种安全类型中的一种进行无线安全设置。

本页面提供了两种无线安全类型供您进行选择：WEP 以及 WPA-PSK/WPA2-PSK。不同的安全类型下，安全设置项不同，下面将详细介绍。

1. WEP

WEP 是 Wired Equivalent Privacy 的缩写，它是一种基本的加密方法，其安全性不如另外一种安全类型高。选择 WEP 安全类型，路由器将使用 802.11 基本的 WEP 安全模式。这里需要注意的是因为 802.11N 不支持此加密方式，如果您选择此加密方式，路由器可能会工作在较低的传输速率上。其具体设置项见下图示。

The screenshot shows the WEP configuration page. At the top, there is a 'WEP' status indicator. Below it, the '认证类型' (Authentication Type) is set to '开放系统' (Open System). The 'WEP密钥格式' (WEP Key Format) is set to '十六进制' (Hexadecimal). Under '密钥选择' (Key Selection), '密钥1' (Key 1) is selected with a radio button. To the right, there is a 'WEP密钥' (WEP Key) label and a '密钥类型' (Key Type) label. Below these are four rows for keys. Each row has a radio button for selection, a text input field for the key value, and a dropdown menu for the key type. All key type dropdowns are currently set to '禁用' (Disabled).

图 25 WEP 加密

- 认证类型：该项用来选择系统采用的安全方式，即自动、开放系统、共享密钥。
 - 自动：若选择该项，路由器会根据主机请求自动选择开放系统或共享密钥安全模式。
 - 开放系统：若选择该项，路由器将采用开放系统方式。此时，无线网络内的主机可以在不提供认证密码的前提下，通过认证并关联上无线网络，但是若要进行数据传输，必须提供正确的密码。
 - 共享密钥：若选择该项，路由器将采用共享密钥方式。此时，无线网络内的主机必须提供正确的密码才能通过认证，否则无法关联上无线网络，也无法进行数据传输。
- WEP密钥格式：该项用来选择即将设置的密钥的形式，即16进制、ASCII码。若采用16进制，则密钥字符可以为0~9，A、B、C、D、E、F；若采用ASCII码，则密钥字符可以是键盘上的所有字符。
- 密钥选择：您可以预先储存4条密钥，并根据需要选择当前生效的WEP密钥。
- WEP密钥：请填写您需要设置的密钥值。密钥的长度和有效字符范围受密钥类型的影响。如果没有设置任何密钥，无线数据将不进行加密。
- 密钥类型：可以选择使用64位、128位的WEP密钥，选择“禁用”将不使用该密钥。

注意：

选择64位密钥需输入16进制字符10个，或者ASCII码字符5个；选择128位密钥需输入16进制字符26个，或者ASCII码字符13个。

2. WPA-PSK/WPA2-PSK

WPA-PSK/WPA2-PSK 安全类型是基于共享密钥的WPA模式，安全性很高，设置也比较简单，适合普通家庭用户和小型企业使用。其具体设置详见下图示。

WPA-PSK/WPA2-PSK

认证类型：

加密算法：

PSK密码：

(最短为8个字符, 最长为63个ASCII码字符或64个16进制字符)

组密钥更新周期： (单位为秒, 最小值为30, 不更新则为0)

图 26 WPA-PSK/WPA2-PSK 加密

- 认证类型：该项用来选择系统采用的安全方式，即自动、WPA、WPA2。
 - 自动：若选择该项，路由器会根据主机请求自动选择WPA或WPA2安全模式。
 - WPA：若选择该项，路由器将采用WPA的安全模式。
 - WPA2：若选择该项，路由器将采用WPA2的安全模式。
- 加密算法：该项用来选择对无线数据进行加密的安全算法，选项有自动、TKIP、AES。默认选项为自动，选择该项后，路由器将根据网卡端的加密方式来自动选择TKIP或AES加密方式。
- PSK密码：该项是WPA-PSK/WPA2-PSK的初始设置密钥，由64个十六进制字符或8-63个ASCII码字符组成。
- 组密钥更新周期：该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为30，若该值为0，则表示不进行更新。

👉 注意：

当路由器的无线设置完成后，无线网络内的主机若想连接该路由器，其无线设置必须与此处设置一致，如：SSID号。若该路由器采用了安全设置，则无线网络内的主机必须根据此处的安全设置进行相应设置，如密码设置必须完全一样，否则该主机将不能成功连接该路由器。

4.5.3 无线MAC地址过滤

选择菜单**无线设置**→**无线 MAC 地址过滤**，您可以在下图 27 界面中查看或添加无线网络的 MAC 地址过滤条目。

MAC 地址过滤功能通过 MAC 地址允许或拒绝无线网络中的计算机访问广域网，有效控制无线网络内用户的上网权限。您可以利用按钮**添加新条目**来增加新的过滤规则；或者通过“编辑”、“删除”链接来编辑或删除旧的过滤规则。

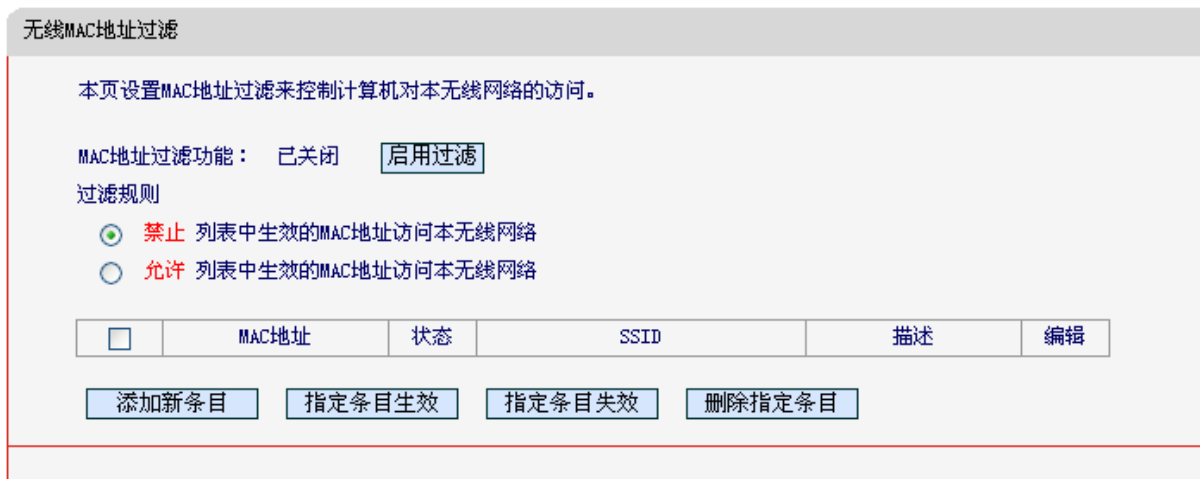


图 27 无线网络 MAC 地址过滤设置

- **MAC地址过滤功能**：请在该处选择是否开启路由器的无线网络MAC地址过滤功能。默认状态为关闭。
- **过滤规则**：请选择MAC地址过滤规则，该规则对下面MAC地址条目列表生效。
- **MAC地址**：该项指需要进行访问限制的无线网络内的主机MAC地址。
- **状态**：该项显示MAC地址过滤条目的状态。“生效”表示该设置条目被启用，“失效”表示该设置条目未被启用。
- **描述**：该项显示对主机的简单描述。
- **添加新条目**：单击该项，您可以在随后的界面中添加新的MAC地址过滤条目。
- **指定条目生效**：单击该按钮，您可以使表中的指定条目生效。
- **指定条目失效**：单击该按钮，您可以使表中的指定条目失效。
- **删除指定条目**：单击该按钮，您可以删除表中指定的条目。

例1：如果您想禁止MAC地址为“00:0A:EB:00:07:BE”和“00:0A:EB:00:07:5F”的主机访问无线网络，其他主机可以访问无线网络，您可以按照以下步骤进行配置：

第一步：在图27中，选择过滤规则为“禁止列表中生效的MAC地址访问本无线网络”，并确认访问控制列表中没有任何生效的条目，如果有，将该条目状态改为“失效”或删除该条目。

第二步：在图27中，单击“添加新条目”按钮，按照下图28界面，设置MAC地址为“00:0A:EB:00:07:BE”，状态为“生效”。设置完成后，单击**保存**按钮。

无线MAC地址过滤

本页设置MAC地址过滤来控制计算机对本无线网络的访问。

MAC地址： 例如：00:1D:0F:11:22:33

描述：

状态：

图 28 添加无线网络 MAC 地址过滤条目

第三步：参照第二步，继续添加过滤条目，设置MAC地址为“00:0A:EB:00:07:5F”，状态为“生效”。设置完成后，单击**保存**按钮。

第四步：在上图27中，单击“启用过滤”按钮，开启无线网络的访问控制功能。

设置完成后生成的MAC地址过滤列表为：

<input type="checkbox"/>	MAC地址	状态	SSID	描述	编辑
<input type="checkbox"/>	00:0A:EB:00:07:BE	生效	1		编辑
<input type="checkbox"/>	00:0A:EB:00:07:5F	生效	2		编辑

☞ 注意：

如果您开启了无线网络的MAC地址过滤功能，并且过滤规则选择了“允许列表中生效的MAC地址访问本无线网络”，而过滤列表中又没有任何生效的条目，那么任何主机都不可以访问本无线网络。

4.5.4 无线高级设置

选择菜单**无线设置**→**无线高级设置**，您可以在下图中设置无线高级设置项。

无线高级设置

注意：当前无线模式包含11n，分片阈值将默认设定为最大值

传输功率：

Beacon时槽： (25-1000)

RTS时槽： (1-2346)

分片阈值： (256-2346)

DTIM阈值： (1-255)

开启 Short GI

开启 Client隔离

开启 WMM

图 29 无线高级设置

- 传输功率：设置无线网络的传输功率，推荐保持默认值“100%”。

- **Beacon时槽**：路由器通过发送Beacon广播进行无线网络连接的同步。Beacon时槽表示路由器发送Beacon广播的频率，即Beacon帧的发包间隔，可以设置为(20~1000)内的值，单位为毫秒（ms），默认值为100。设定值较小有助于路由器被无线网络内的主机快速发现，加快连接速度。设定值较大有助于路由器省电。
- **RTS时槽**：为数据包指定RTS（Request to Send，发送请求）阈值。当数据包长度超过RTS阈值时，路由器就会发送RTS到目的站点来进行协商。接收到RTS帧后，无线站点会回应一个CTS（Clear to Send，清除发送）帧来回应路由器，表示两者之间可以进行无线通信。
- **分片阈值**：为数据包指定分片阈值。当数据包的长度超过分片阈值时，会被自动分成多个数据包。过多的数据包将会造成网络性能降低，所以分片阈值不应设置过低。默认值为2346。
- **DTIM阈值**：指定传输指示消息(DTIM)的间隔，该值在1至255毫秒之间。DTIM是一种倒计时作业，用以告知下一个要接收广播及多播的客户端窗口。当路由器已经为相关联的客户端缓存了广播或者多播信息时，它就会传送夹带有下一个DTIM时槽的DTIM；当客户端听到Beacon讯号时，就会接收该广播和组播信息。默认值为1。
- **开启Short GI**：打开Short GI，选择此项可以使路由器具有较高的数据传输速率，建议选择此选项。
- **开启Client隔离**：选择此项可以隔离关联到AP的各个无线站点。
- **开启WMM**：选择该选项将使路由器可以处理带有优先级信息的数据包，建议选择此选项。

4.5.5 无线主机状态

选择菜单**无线参数**→**无线主机状态**，您可以在下图 30 界面中查看当前连接到无线网络中的所有主机的基本信息。单击**刷新**按钮，您可以更新列表中的条目信息。



图 30 无线网络主机状态

- **MAC地址**：该处显示当前已经连接到无线网络的主机的MAC地址。
- **当前状态**：此项显示当前主机的运行状态。
- **接收数据包数、发送数据包数**：这两项显示当前主机接收和发送的数据包的总数。
- **刷新**：页面每隔5秒钟自动刷新一次，您也可以点击该按钮随时刷新页面。

4.6 带宽控制

选择菜单**带宽控制**，您可以在下图中设置设置项。

带宽控制

带宽控制功能可以实现对局域网计算机上网带宽的控制。在本页面，您可以开启或关闭此功能，并设定宽带线路类型及带宽大小，同时，还可进行带宽控制规则的添加、删除等。只有开启了带宽控制的总开关，“带宽控制规则”才能够生效，反之，则失效。
注意：选择带宽线路类型及填写带宽大小时，请根据实际情况进行选择 and 填写，如不清楚，请咨询您的带宽提供商（如电信、网通等）。

开启带宽控制

宽带线路类型： ADSL线路 其他线路

上行总带宽： Kbps

下行总带宽： Kbps

带宽控制规则

<input type="checkbox"/>	规则描述	优先级	上行带宽 (Kbps)		下行带宽 (Kbps)		状态	编辑
			最小	最大	最小	最大		
<input type="checkbox"/>								

图 31 带宽控制

- 开启带宽控制：请您选择是否开启带宽控制设置，选中该复选框则表示启用该功能。
- 带宽线路类型：请选择您的带宽线路类型。
- 上行总带宽：请输入您当前线路上运营商提供的最大上传速率，最大值为100000Kbps。
- 下行总带宽：请输入您当前线路上运营商提供的最大下载速率，最大值为100000Kbps。

完成更改后，单击**保存**按钮。

当您点击控制规则列表中的**增加新的条目**或**编辑**按钮时，您将进入下图的设置界面。在控制规则配置中，您可以创建新的控制规则或修改已存在的规则。若您想修改上下行带宽，首先需在图31所示界面开启带宽控制，设置上下行总带宽并保存。

带宽控制规则

开启

IP地址段： --

端口段： --

协议： ▾

优先级： ▾

	最小带宽 (Kbps)	最大带宽 (Kbps)
上行：	<input type="text"/>	<input type="text"/>
下行：	<input type="text"/>	<input type="text"/>

图 32 带宽控制规则

- 开启：请选择是否启用该规则。

- IP地址段：请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。
- 优先级：规则的级别，有1~8个级别可供选择，1的级别最高，级别高的规则优先被实现。
- 上行、下行带宽：请参考控制规则列表中所述来设置。

设置完成后，单击**保存**。

注意：

- 1) 优先级不影响规则的最小保障带宽，不论优先级是否相同，规则的最小带宽都能得到保障。
- 2) 剩余带宽是指保障了各规则的最小带宽后，余下的可用带宽。
- 3) 优先级的作用是用来抢占剩余带宽，优先级越高，抢占剩余带宽的能力越强。即：优先级最高的规则，最先对剩余带宽进行抢占，其抢占带宽的大小受限于规则的最大带宽限制。高优先级的规则抢占完后，如果还有剩余带宽，则由次高优先级的规则来抢占，依此类推。对于优先级相同的规则，最小带宽的值越大，能抢到的带宽就越多。

4.7 DHCP服务器

选择菜单 **DHCP 服务器**，您可以看到：



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 DHCP服务设置

选择菜单 **DHCP 服务器**→**DHCP 服务设置**，您将看到 DHCP 设置界面，如图 33。

DHCP指动态主机控制协议(Dynamic Host Control Protocol)。MW313R有一个内置的DHCP服务器，它能够自动分配IP地址给局域网中的计算机。对用户来说，为局域网中的所有计算机配置TCP/IP协议参数并不是一件容易的事，它包括IP地址、子网掩码、网关、以及DNS服务器的设置等。若使用DHCP服务则可以解决这些问题。您可以按照下面各子项说明正确设置这些参数。

DHCP服务设置

本页面进行DHCP服务设置，路由器的DHCP服务器能自动配置局域网中各计算机的TCP/IP协议。

所属分组： Default

IP地址： 192.168.1.1

子网掩码： 255.255.255.0

DHCP服务器： 不启用 启用 DHCP Relay

地址池开始地址：

地址池结束地址：

地址租期： 分钟（1~2880分钟，缺省为1440分钟）

网关： （可选）

缺省域名： （可选）

主DNS服务器： （可选）

备用DNS服务器： （可选）

图 33 DHCP 服务

- 地址池开始地址、地址池结束地址：这两项为DHCP服务器自动分配IP地址时的起始地址和结束地址。设置这两项后，内网主机得到的IP地址将介于这两个地址之间。
- 地址租期：该项指DHCP服务器给客户端主机分配的动态IP地址的有效使用时间。在该段时间内，服务器不会将该IP地址分配给其它主机。
- 网关：此项应填入路由器LAN口的IP地址，缺省是192.168.1.1。
- 缺省域名：此项为可选项，应填入本地网域名(默认为空)。
- 主DNS服务器、备用DNS服务器：这两项为可选项，可以填入ISP提供给您的DNS服务器，不清楚可以向ISP询问。

完成更改后，单击**保存**按钮。

注意：

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

4.7.2 静态地址分配

选择菜单 **DHCP 服务器**→**静态地址分配**，您可以在下图 34 界面中设置静态 IP 地址。

静态地址分配功能可以为指定MAC地址的计算机预留静态IP地址。当该计算机请求DHCP服务器分配IP地址时，DHCP服务器将给它分配表中预留的IP地址。并且一旦采用，该主机的IP地址将不再改变。

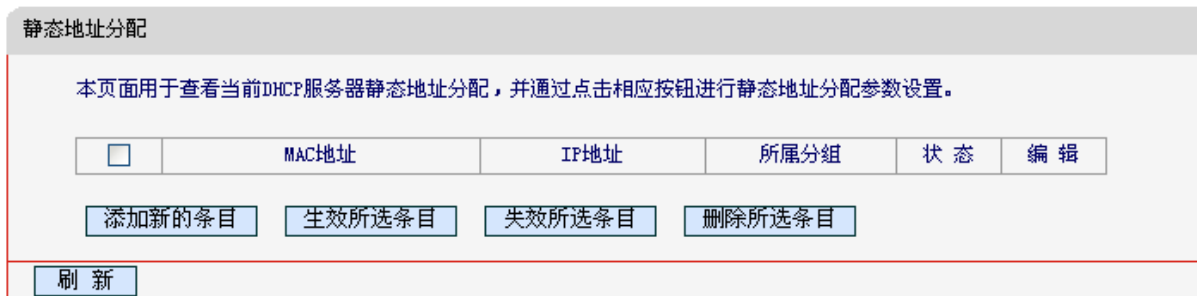


图 34 静态地址分配

- **MAC地址**：该项指定将要预留静态IP地址的计算机的MAC地址。
- **IP地址**：该项指定给内网主机预留的IP地址。
- **状态**：显示该条目状态“生效”或“失效”，只有状态为生效时，本条过滤规则才生效。
- **添加新的条目**：单击该按钮，您可以在随后的界面中添加新的静态地址条目，如图35。
- **生效所选条目**：单击该按钮，您可以使表中的所选条目生效。
- **失效所选条目**：单击该按钮，您可以使表中的所选条目失效。
- **删除所选条目**：单击该按钮，您可以删除表中所选条目。

例1：如果您希望给局域网中MAC地址为00:13:8F:A9:6C:CB的计算机预留IP地址：192.168.1.101。这时您可以按照如下步骤设置：

第一步：在图34界面中单击**添加新的条目**。

第二步：在图35界面中设置MAC地址为“00:13:8F:A9:6C:CB”，IP地址为“192.168.1.101”，状态为“生效”。

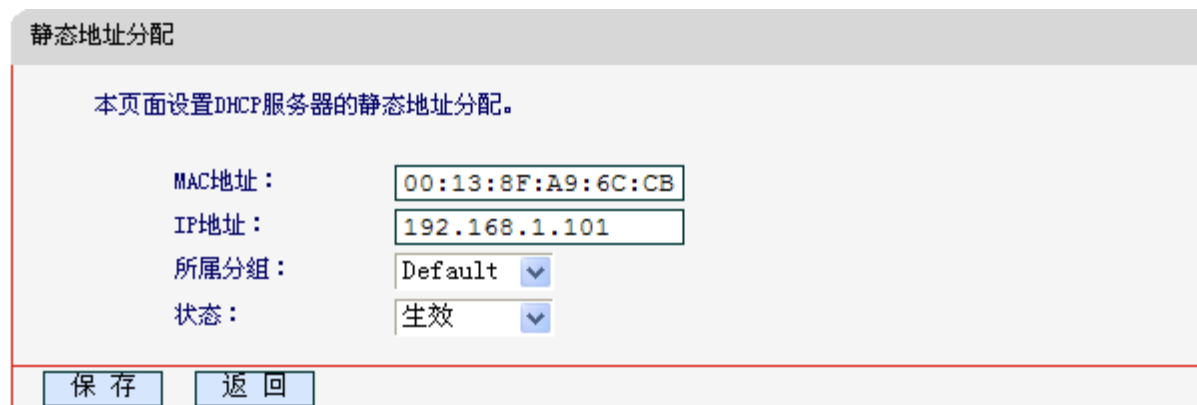


图 35 添加静态地址条目

第三步：单击**保存**按钮。

第四步：重启路由器使设置生效。

4.7.3 客户端列表

选择菜单 **DHCP 服务器**→**客户端列表**，您可以查看所有通过 DHCP 服务器获得 IP 地址的主机的信息，单击**刷新**按钮可以更新表中信息，如图 36。

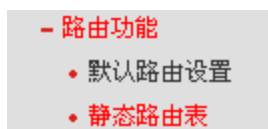
客户端列表				
本页面用于查看当前DHCP服务器的客户端信息。				
ID	客户端名	MAC地址	IP地址	有效时间
1	24705	40:61:86:E5:D2:B2	192.168.1.100	21:11:57
2	test-PC	E0:3F:49:11:36:C0	192.168.1.102	23:55:36
<input type="button" value="刷新"/>				

图 36 客户端列表

- 客户端名：该处显示获得了IP地址的客户端计算机的名称。
- MAC地址：该处显示获得了IP地址的客户端计算机的MAC地址。
- IP地址：该处显示DHCP服务器分配给客户端主机的IP地址。
- 有效时间：该项指客户端主机获得的IP地址离到期的时间，每个IP地址都有一定的租用时间，客户端软件会在租期到期前自动续约。

4.8 路由功能

选择菜单**路由功能**，您可以看到：



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 默认路由设置

选择菜单**路由功能**→**默认路由设置**，您可以在下图 37 的界面中设置默认路由信息。

默认路由是一种特殊的静态路由，指的是当路由表中与 IP 包的目的地之间没有匹配的表项时路由器选择的路由。如果没有默认路由，那么目的地在路由表中没有匹配表项的包将被丢弃。

默认路由设置	
本页面进行默认路由设置，请选择一个WAN接口作为默认路由。	
选择 WAN 接口：	<input type="text" value="pppoe_eth1_d"/>
<input type="button" value="保存"/>	

图 37 默认路由设置

- 选择WAN接口：请从下拉菜单中选择一个WAN接口作为默认路由。

设置完成后，单击**保存**按钮。

4.8.2 静态路由表

选择菜单**路由功能**→**静态路由表**，您可以在下图 38 界面中设置的静态路由信息。

静态路由是一种特殊的路由，在网络中使用合适的静态路由可以减少路由选择问题和路由选择数据流的过载，提高数据包的转发速度。通过设定目的IP地址、子网掩码和网关地址可以确定一个路由条目，其中目的IP地址和子网掩码用来确定一个目标网络/主机，之后300M无线路由器会通过网关将数据包发往指定的目标网络/主机。

静态路由表

本页面用于查看当前静态路由表信息，并通过点击相应按钮进行静态路由表配置。

<input type="checkbox"/>	目的网络地址	子网掩码	网关	状态	编辑
<input type="button" value="增加新的条目"/> <input type="button" value="生效所选条目"/> <input type="button" value="失效所选条目"/> <input type="button" value="删除所选条目"/>					

图 38 静态路由表

- 目的网络地址：用来标识希望访问的目标地址或目标网络。
- 子网掩码：该项与目的IP地址一起来标识目标网络，把目标地址和网络掩码逻辑与即可得到目标网络。
- 网关：数据包被发往的300M无线路由器或主机的IP地址。
- 状态：显示该条目是否生效，只有状态为生效时，此路由条目才起作用。
- 增加新的条目：点击该项，您可以在下图中添加静态路由条目。如图39。
- 生效所选条目：单击该按钮，您可以使表中的所选条目生效。
- 失效所选条目：单击该按钮，您可以使表中的所选条目失效。
- 删除所选条目：单击该按钮，您可以删除表中所选条目。

静态路由表

本页面设置路由器的静态路由信息。

目的网络地址：

子网掩码：

默认网关：

使用接口：

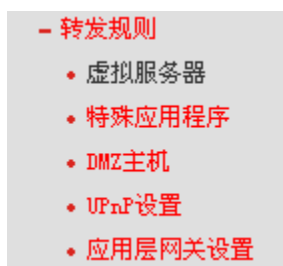
状态：

图 39 添加静态路由条目

完成设置后，点击**保存**按钮。

4.9 转发规则

选择菜单**转发规则**，您可以看到：



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。

4.9.1 虚拟服务器

选择菜单**转发规则**→**虚拟服务器**，您可以在下图 40 界面中设置虚拟服务器条目。

MW313R可配置为虚拟服务器，它能使通过公共IP地址访问Web或FTP等服务的远程用户自动转向到局域网中的本地服务器。

MW313R内置的防火墙特性能过滤掉未被识别的包，保护您的局域网。在路由器默认设置下，局域网中所有的计算机都不能被外界看到。如果希望在保护局域网内部不被侵袭的前提下，某些LAN中的计算机在广域网上可见，请使用虚拟服务器。

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改发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。



图 40 虚拟服务器

- 服务端口：此项为路由器提供给广域网的服务端口，广域网用户通过向该端口发送请求来获取服务。可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。
- IP地址：局域网中被指定提供虚拟服务的服务器地址。
- 协议：虚拟服务所用的协议，可供选择的有：TCP、UDP和ALL。若对采用的协议不清楚，可以选择ALL。
- 状态：该项显示该条目状态“生效”或“失效”，只有状态为生效时，本条目的设置才生效。

- WAN 接口：虚拟服务器条目对应的网络接口。远程用户只有通过指定的 WAN 接口才能访问局域网中的本地服务器。

例1：如果希望广域网用户通过端口21访问您的FTP服务器，FTP服务器在局域网中的IP地址为192.168.1.100，协议选择为TCP，则您可以按照如下步骤设置：

第一步：在图40界面中单击**增加新的条目**按钮。

第二步：在图41界面中单击“常用服务端口号”下拉菜单，查找FTP服务，选中“FTP”服务。

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。

注意：只有可用接口不为空时，才可进行虚拟服务器设置。如果开启了远端管理功能，则虚拟服务器规则中的对应端口将失效。

使用接口：	<input type="text" value="pppoe_eth1_d"/>	
服务端口号：	<input type="text" value="21"/>	(XX-XX or XX)
IP 地址：	<input type="text" value="192.168.1.100"/>	
协议：	<input type="text" value="TCP"/>	
状态：	<input type="text" value="生效"/>	
常用服务端口号：	<input type="text" value="FTP"/>	

图 41 添加虚拟服务条目

- 常用服务端口号：在“常用服务端口号”中，列出了常用协议的端口，您可以直接从中选择一个，系统则会将该服务的端口号、协议类型，自动添加到对应序列的“服务端口号”和“协议”项中，您只需要再为其指定服务器IP地址并启用即可。对于常用服务端口中没有列出的端口，如果需要，也可以在服务端口处手动添加。

第三步：输入IP地址为“192.168.1.100”，设置条目状态为“生效”。

第四步：单击**保存**按钮。

设置好以后，您只要在局域网的服务器上进行相应的设置，广域网的计算机就可以访问到您局域网的服务器上了。

例2：如果希望广域网用户通过端口80访问您的Web服务器，Web服务器在局域网中的IP地址为192.168.1.101，协议选择为ALL，则您可以按照如下步骤设置：

第一步：在图40界面中单击**添加新的条目**按钮。

第二步：在图41界面中设置服务端口为“80”，输入IP地址为“192.168.1.101”，选择协议为“ALL”。

第三步：单击**保存**按钮。

例1和例2设置完成后生成的虚拟服务列表为：

<input type="checkbox"/>	服务端口	IP地址	协议	状态	WAN接口	编辑
<input type="checkbox"/>	21	192.168.1.100	TCP	生效	pppoe_eth1_d	编辑
<input type="checkbox"/>	80	192.168.1.101	TCP	生效	pppoe_eth1_d	编辑

注意：

- 1) 如果设置了服务端口为80的虚拟服务器，则需要将系统管理→管理控制的“管理服务设置”设置为80以外的值，如88，否则会发生冲突，从而导致虚拟服务器不起作用。
- 2) 例1中的服务在“常用服务端口”中已经提供，对于“常用服务端口”中没有提供的服务，可参照例2来添加。

4.9.2 特殊应用程序

选择菜单转发规则→特殊应用程序，您可以在下图 42 界面中设置特殊应用程序条目。

某些应用如Internet网络游戏、视频会议、网络电话等需要多条连接，但由于防火墙而无法正常工作。当这些应用程序向触发端口发起连接时，特殊应用程序将打开对应的所有开放端口，以备后续连接。

特殊应用程序

某些程序需要多条连接，如Internet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路由下工作。特殊应用程序使得某些这样的应用程序能够在NAT路由下工作。

<input type="checkbox"/>	触发端口	触发协议	开放端口	开放协议	状态	编辑
<input type="checkbox"/>						

图 42 特殊应用程序

- 触发端口：该端口是应用程序首先发起连接的端口，只有在该端口上发起连接，开放端口中的所有端口才可以开放，否则开放端口是不会开放的。
- 触发协议：代表触发端口上使用的协议，可以选择ALL、UDP或TCP。若不清楚采用哪种协议，可以选用ALL。
- 开放端口：当向触发端口上成功发起连接后，对应的开放端口会打开，应用程序便可以向该开放端口发起后续的连接。此处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：代表开放端口上使用的协议，可以选择ALL、UDP和TCP。若不清楚采用哪种协议，可以选用ALL。
- 状态：该项显示该条目状态“生效”或“失效”，只有状态为生效时，本条目的设置才生效。

在图 42 界面中单击**添加新的条目**按钮，您可以在下图 43 界面中添加新的特殊应用程序条目。

特殊应用程序

某些程序需要多条连接，如Internet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路由下工作。特殊应用程序使得某些这样的应用程序能够在NAT路由下工作。

注意：只有可用接口不为空时，才可进行特殊应用程序设置。

使用接口：	pppoe_eth1_d
触发端口：	7175
触发协议：	ALL
开放端口：	51200-51201, 51210
开放协议：	ALL
状态：	生效
常用服务端口号：	---请选择---

保存 返回

图 43 添加特殊应用程序条目

- 使用接口：请在下拉菜单中选择网络接口。
- 常用服务端口号：在“常用服务端口号”中，列出了常用的应用程序，您可以直接从中选择一个，系统则会自动将该常用应用程序的触发端口号和开放端口号添加到对应的“触发端口”和“开放端口”项中，并且会启用该条目。对于常用应用程序中没有列出的程序，您可以手动添加。

完成设置后，单击**保存**按钮。

4.9.3 DMZ主机

选择菜单**转发规则**→**DMZ 主机**，您可以在下图 44 界面中设置 DMZ(非军事区)主机。

局域网中设置DMZ主机后，该主机将完全暴露给广域网，可以实现双向无限制通信。具体设置时，只需输入局域网中指定为DMZ主机的IP地址，然后选中启用并单击保存即可。向DMZ添加客户机可能会给客户机带来不安全因素，因此请不要轻易使用这一选项。

DMZ主机	
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。	
DMZ 状态：	<input type="radio"/> 启用 <input checked="" type="radio"/> 不启用
DMZ主机IP地址：	0.0.0.0

保存

图 44 DMZ 主机

4.9.4 UPnP设置

选择菜单**转发规则**→**UPnP 设置**，您可以在下图 45 界面中查看 UPnP 信息。

通常情况下局域网中所有的计算机都不能被外界看到，外部主机（应用程序）需要访问内部主机上的资源时，需通过设置300M无线路由器进行特定的端口转发。UPnP（Universal Plug and Play）通用即插即用协议，可以根据应用程序的需要自动打开相应的端口，而不需要用户手动去添加端口转发，使得外部主机能够在需要时访问内部主机上的资源，对于一些端口不固定的应用将会更加方便。

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。



图 45 UPnP 设置

- 应用描述：应用程序向路由器发出的UPnP请求中，包含的有关应用程序的描述。
- 外部端口：路由器为应用程序打开的外部端口。
- 协议类型：表明是对TCP还是UDP进行端口转换。
- 内部端口：路由器为本地主机打开的内部端口。
- IP地址：需要进行端口转换的本地主机的IP地址。
- 状态：该项显示端口是否已经启用。
- 刷新：单击该按钮，可以刷新当前的UPnP列表信息。

UPnP 的使用方法如下：

1. 单击**开启**按钮启用 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。
3. 不使用时请单击**关闭**按钮关闭 UPnP 功能。

☞ 注意：

- 1) 现阶段版本的UPnP协议的安全性还未得充分保证，在不必要时请关闭UPnP功能。
- 2) 只有支持UPnP协议的应用程序和操作系统才能使用本功能，操作系统如Windows XP/ME/Vista，应用程序如MSN Messenger。

4.9.5 应用层网关设置

选择菜单**转发规则**→**应用层网关设置**，您可以在下图 46 应用层网关设置界面。

图 46 应用层网关设置

- 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 300M 无线路由器连接到远程 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 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”。

完成设置后，单击**保存**按钮。

4.10 家长控制

选择菜单**家长控制**，您可以在下图 47 界面中对小孩的上网时间和访问的网站进行控制。

家长控制

作为家长，您可以通过本页面进行设置，控制小孩的上网行为，使得小孩的PC只能在指定时间访问指定的网站。

开启家长控制

家长PC的MAC地址：

当前PC的MAC地址：

90:2B:34:65:39:3E

[设为家长PC](#)

[保存](#)

小孩MAC地址 - 1：

小孩MAC地址 - 2：

小孩MAC地址 - 3：

小孩MAC地址 - 4：

当前局域网中PC的MAC地址：

90:2b:34:65:39:3e



填充到

请选择



计划时间段：

每天



开始时间：

00:00



结束时间：

24:00



[添加](#)

时间	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00
周日															
周一															
周二															
周三															
周四															
周五															
周六															

[清空时间表](#)

添加URL地址：

[添加](#)



[详细信息](#)

[删除所选条目](#)

(只有保存后，您的删除操作才能生效)

[保存](#)

图 47 家长控制设置

- 开启家长控制：选择是否开启家长控制功能。
- 家长PC的MAC地址：设定不受控制的PC的MAC地址。
- 设为家长PC：单击此按钮可以把当前正在管理此WEB页面的PC的MAC地址复制到“家长PC的MAC地址”中。
- MAC地址 -1/2/3/4：设定小孩PC的MAC地址，您可以在“当前局域网中PC的MAC地址”下拉列表中选择小孩PC的MAC地址，并复制到“MAC地址 -1/2/3/4”。
- 计划时间段，开始/结束时间：您可以通过下列菜单选择允许小孩访问指定网站的时间段，也可以通过单击时间表内的灰色框设置。
- 添加URL地址：输入允许小孩访问的网站地址，最多可输入200条URL地址。

完成更改后，单击**保存**按钮。

4.11 防火墙

选择菜单**防火墙**，您可以看到：



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。

4.11.1 规则管理

选择菜单**防火墙**→**规则管理**，您可以在下图 48 界面中设置对内网主机上网行为的控制规则。

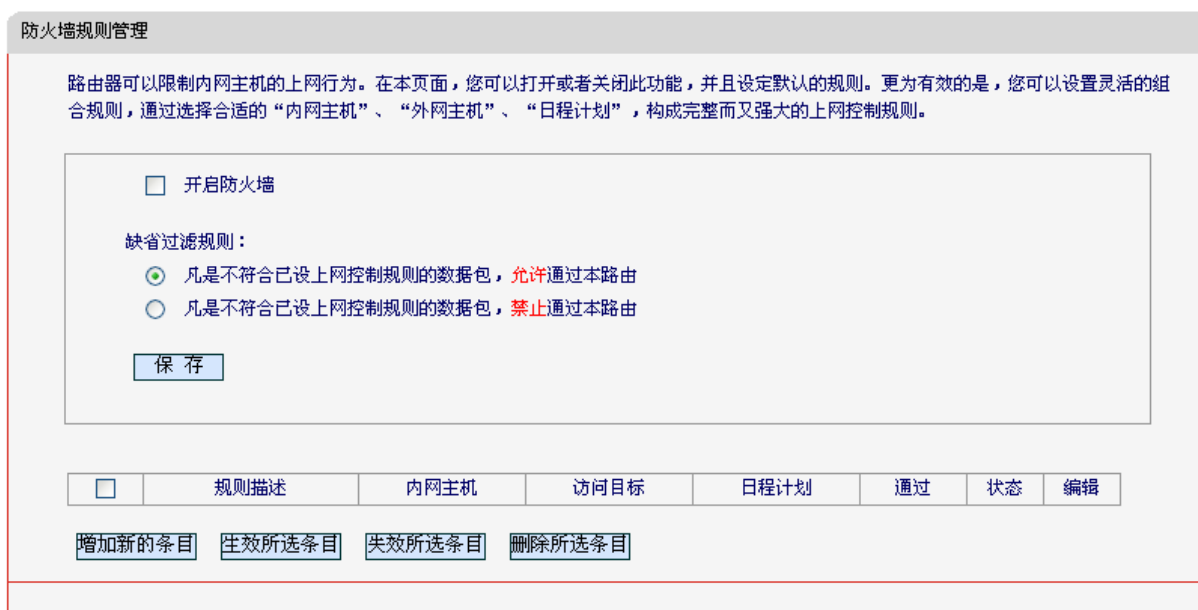


图 48 防火墙规则管理

- 开启防火墙：选中时开启防火墙功能。
- 凡是不符合已设上网控制规则的数据包，允许通过本路由：选择此项，则凡是和您设置的上网控制规则不符的数据包，均可以通过本300M无线路由器。
- 凡是不符合已设上网控制规则的数据包，禁止通过本路由：选择此项，则凡是和您设置的上网控制规则不符的数据包，均不能通过本300M无线路由器。

完成更改后，单击**保存**按钮。

- 增加新的条目：单击此按钮，可以在下图49界面中设置新的上网控制条目。

防火墙规则管理

本页设置一条上网控制综合条目。

条目描述：	<input style="width: 100%;" type="text"/>	
内网主机：	任意主机 ▼	添加内网主机
外网主机：	任意主机 ▼	添加外网主机
日程计划：	任何时间 ▼	添加日程计划
动作：	禁止通过 ▼	
状态：	生效 ▼	
方向：	IN ▼	
协议：	ALL ▼	

图 49 防火墙规则设置

- 条目描述：对该上网控制条目的简单描述，此描述必须是唯一的。
- 内网主机：此条目要控制的内网主机。如果您已在**防火墙→内网主机**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**添加内网主机**进入内网主机列表设置对话框进行设置。有关内网主机列表的设置请参阅本文档[4.11.2 内网主机](#)部分。
- 外网主机：允许或禁止“主机列表”中的主机访问的IP地址、MAC地址或网站域名，即访问目标。如果您已在**防火墙→外网主机**中设置好了外网主机信息，请直接在下拉列表中选择，否则请单击**添加外网主机**进入外网主机设置对话框进行设置。有关外网主机的设置请参阅本文档[4.11.3 外网主机](#)部分。
- 日程计划：允许或禁止“内网主机”中的主机访问“外网主机”的时间段。如果您已在**防火墙→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**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[4.11.4 日程计划](#)部分。
- 动作：对符合上述控制规则的情况，允许或禁止上网。
- 状态：该上网控制条目是否生效。
- 方向：IN 或 OUT，IN 表示外网主机对内网主机的访问，OUT 表示内网主机对外网主机的访问。
- 协议：访问外网主机的服务器所使用的协议。如果您对采用的协议不清楚，推荐选择 ALL。

完成更改后，单击**保存**按钮。此时图 48 所示上网控制规则管理界面的列表中将显示您刚刚设置的控制条目的信息，单击“编辑”列中的**编辑**，可以修改相关信息。

- 生效所选条目：单击该按钮，可以使列表中的所有选定条目生效。
- 失效所选条目：单击该按钮，可以使列表中的所有选定条目失效。
- 删除所选条目：单击该按钮，可以一次性删除列表中的所有选定条目。

例 1：如果您希望限制局域网中 IP 地址为 192.168.1.88 的计算机（假设该计算机的主人为小明）只能在周六、周日的 8:00—12:00 访问网易网站（www.163.com），而局域网中的其它主机（假设 IP 地址为 192.168.1.89—192.168.1.91）不受任何控制，请按照以下步骤进行设置：

第一步：在**内网主机**中添加两个条目，其一：主机名为小明的计算机，IP 地址为 192.168.1.88；其二：主机名为其他计算机，IP 地址为 192.168.1.89—192.168.1.91。

第二步：在**外网主机**中添加一个列表，其规则描述为网易，模式选择 URL 地址并填入 www.163.com。

第三步：在**日程计划**中添加一个列表，日程描述为周末上午 8-12 点，在日程表中选择时间。

第四步：回到上网控制规则管理设置界面，启用上网控制功能，选择缺省过滤规则为“凡是不符合已设上网控制规则的数据包，禁止通过本 300M 无线路由器”，单击**保存**按钮。

第五步：点击**增加新的条目**按钮，按下图 50 所示进行设置并保存。

防火墙规则管理

本页设置一条上网控制综合条目。

条目描述：	<input type="text" value="小明周末可上网"/>	
内网主机：	<input type="text" value="小明的计算机"/> ▼	添加内网主机
外网主机：	<input type="text" value="网易"/> ▼	添加外网主机
日程计划：	<input type="text" value="周末上午8-12点"/> ▼	添加日程计划
动作：	<input type="text" value="允许通过"/> ▼	
状态：	<input type="text" value="生效"/> ▼	
方向：	<input type="text" value="IN"/> ▼	
协议：	<input type="text" value="ALL"/> ▼	

图 50 上网控制规则设置示例一

第六步：点击**增加新的条目**按钮，按下图 51 所示进行设置并保存。

防火墙规则管理

本页设置一条上网控制综合条目。

条目描述：

内网主机： [添加内网主机](#)

外网主机： [添加外网主机](#)

日程计划： [添加日程计划](#)

动作：

状态：

方向：

协议：

图 51 上网控制规则设置示例二

完成以上设置之后，您看到的规则列表将是：

<input type="checkbox"/>	规则描述	内网主机	访问目标	日程计划	通过	状态	编辑
<input type="checkbox"/>	小明周末可上网	小明的计算机	网易	周末上午8-12点	允许	生效	编辑
<input type="checkbox"/>	其他主机上网	其他计算机	任何目标	任何时间	允许	生效	编辑

4.11.2 内网主机

选择菜单**防火墙**→**内网主机**，您可以在下图 52 界面中设置受控的内网主机列表。

内网主机

<input type="checkbox"/>	条目描述	地址信息	编辑
<input type="checkbox"/>	小明的计算机	192.168.1.88	编辑

图 52 内网主机列表

单击**增加新的条目**按钮，可以在下图 53 界面中设置新的受控主机的信息。

内网主机

请选择模式：

条目描述：

IP 地址： -

端口： -

图 53 内网主机设置示例

- 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。
- 条目描述：给受控主机的一个简单描述，不同主机列表条目中的条目描述不能相同。
- IP 地址：输入一个外网主机的 IP 地址或连续的访问目标 IP 地址段。
- 端口：允许或限制访问的外网主机 IP 地址的服务端口，可以为一个端口号或连续的端口段。

完成更改后，单击**保存**按钮。此时图 52 所示界面的列表中将显示您刚刚设置的主机条目的信息，单击“配置”列中的**编辑**可修改已设主机条目的相关信息。单击**删除所选条目**按钮，可以一次性删除列表中的所有选定条目。

4.11.3 外网主机

选择菜单**防火墙**→**外网主机**，您可以在下图 54 界面中设置允许或禁止受控主机访问的外网主机信息。

外网主机

<input type="checkbox"/>	条目描述	详细信息	编辑
<input type="checkbox"/>	IP地址	202.114.71.2	编辑
<input type="checkbox"/>	小王的电脑	40:61:FC:86:74:32	编辑
<input type="checkbox"/>	网易	www.163.com	编辑

图 54 外网主机设置

单击**增加新的条目**按钮，可以在下图 55 界面中设置新的外网主机的信息。

外网主机

请选择模式：

条目描述：

IP 地址： -

端口： -

图 55 访问目标列表设置—IP 地址模式

- 请选择模式：选择描述外网主机信息的模式，有 IP 地址、MAC 地址和 URL 地址三个选项。如果您选择了 MAC 地址模式，此设置页面将如图 56 所示；如果您选择了 URL 地址模式，此设置页面将如图 57 所示。
- 条目描述：给外网主机的一个简单描述，此描述必须是唯一的。
- IP 地址：输入一个外网主机的 IP 地址或连续的访问目标 IP 地址段。
- 端口：允许或限制访问的外网主机 IP 地址的服务端口，可以为一个端口号或连续的端口段。

外网主机

请选择模式：

条目描述：

MAC地址：

图 56 外网主机列表设置—MAC 地址模式

- MAC 地址：输入一个外网主机的 MAC 地址。

外网主机

请选择模式：

条目描述：

添加URL地址：

<input type="checkbox"/>	详细信息
<input type="checkbox"/>	www.163.com

(只有保存后，您的删除操作才能生效)

图 57 外网主机列表设置—URL 地址模式

- 添加 URL 地址：输入一个 URL 地址，单击添加，您可以添加多条 URL 地址。

4.11.4 日程计划

选择菜单**防火墙**→**日程计划**，您可以在下图 58 界面中设置允许或禁止受控主机上网的时间段。在设置之前，请确保您 300M无线路由器的时间是正确的，有关 300M无线路由器的时间设置请参阅本文档[4.14.9 时间设置](#)部分。



<input type="checkbox"/>	条目描述	编辑
<input type="checkbox"/>	周末上午8-12点	编辑

图 58 日程计划设置

单击**增加新的条目**按钮，可以在下图 59 界面中设置新的日程计划。

日程计划

本页进行日程计划条目的设置。您可以在时间表中点击时间点进行时间设置，也可以通过选择时间段进行时间设置。

条目描述：

计划时间段： 开始时间： 结束时间：

周一 周二 周三 周四 周五 周六 周日

时间	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	1:00	2:00
周日									■	■	■	■			
周一															
周二															
周三															
周四															
周五															
周六									■	■	■	■			

图 59 日程计划设置示例

- 条目描述：给日程计划的简单描述，此描述必须是唯一的。
- 计划时间段，开始/结束时间：您可以通过下列菜单选择允许小孩访问指定网站的时间段，也可以通过单击时间表内的灰色框设置。

完成更改后，单击**保存**按钮。此时图 58 所示界面的列表中将显示您刚刚设置的日程计划的信息，单击“配置”列中的**编辑**可修改已设日程计划的相关信息。单击**删除所选条目**按钮，可以一次性删除列表中的所有已选条目。

4.11.5 攻击防护

选择菜单**防火墙**→**攻击防护**，您可以在下图 60 界面中开启 DoS(拒绝服务)攻击防范。完成更改后，单击**保存**按钮。

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。

攻击防护

本页面用于设置DDOS功能参数。

DOS防护： 开启 关闭
(注：流量统计开启时DOS防护功能才生效。)

开启 ICMP-Flood 攻击过滤
ICMP-Flood 报文数阈值（5~3600）： 包/秒

开启 UDP-Flood 攻击过滤
UDP-Flood 报文数阈值（5~3600）： 包/秒

开启 TCP-SYN-Flood 攻击过滤
TCP-SYN-Flood 报文数阈值（5~3600）： 包/秒

拒绝LAN口ping包

图 60 高级安全选项

- DoS 防护：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 报文数阈值：当开启 ICMP-Flood 功能后，如果在指定时间间隔内 ICMP 包达到了指定的数目，防范措施则立即启动。
- 开启 UDP-Flood 攻击过滤：若需要防范 UDP-Flood，请选择此项。
- UDP-Flood 报文数阈值：当开启 UDP-Flood 功能后，如果在指定时间间隔内 UDP 包达到了指定的数目，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 报文数阈值：当开启 TCP-SYN-Flood 功能后，如果在指定时间间隔内 TCP 的 SYN 包达到了指定的数目，防范措施则立即启动。
- 拒绝 LAN 口 ping 包：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。
- 被禁 DoS 主机列表：点击该按钮，你可以查看被禁止的主机列表，如图 61。单击刷新按钮可以更新列表信息。若希望被禁主机能够重新上网，可以点击删除按钮；若需要释放所有被禁主机，可以点击清空列表按钮。

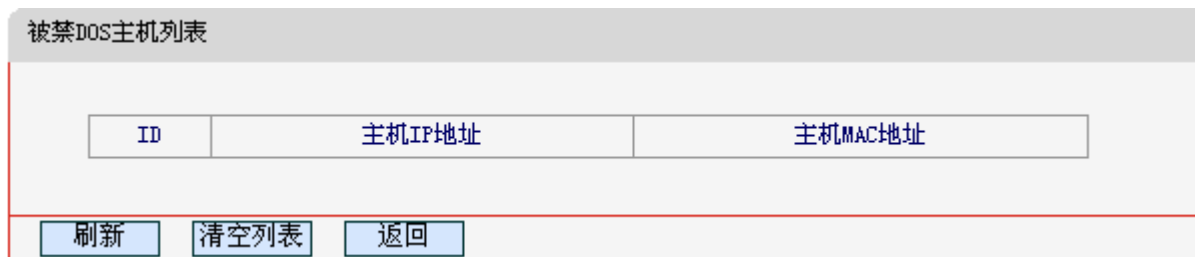


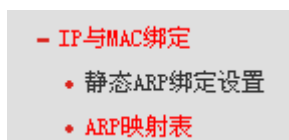
图 61 DoS 被禁主机列表

注意:

只有在开启了运行状态→流量统计中的流量统计功能后，DoS 攻击防范才能正常生效。

4.12 IP与MAC绑定

选择菜单 IP 与 MAC 绑定菜单，您可以看到：



单击某个子项，您即可进行相应功能的设置，下面将详细讲解两个子项的功能。

4.12.1 静态ARP绑定设置

选择IP与MAC绑定→静态ARP绑定设置，即可进入图 62的设置界面设置静态ARP绑定条目。

ARP 绑定主要是将主机的 IP 地址与相应的 MAC 地址进行绑定，是防止 ARP 欺骗的有效方法。在路由器中设置静态 ARP 绑定条目，可以维护内网用户的上网安全。当主机向路由器发送 ARP 请求时，路由器会根据主机的 IP 地址去查看 ARP 静态绑定列表，若列表中的 MAC 地址与主机的 MAC 地址相同，则路由器会允许该 ARP 请求，否则将不允许该请求。

要使用 ARP 绑定功能，您需要先设置以下项目：



图 62 静态 ARP 绑定设置

- ARP 绑定：该项用来开启 ARP 绑定功能，只有选择“启用”时，列表中的设置才能生效。

- MAC 地址：该项显示被绑定主机的 MAC 地址。
- IP 地址：该项显示被绑定主机的 IP 地址。
- 绑定：该项显示条目状态，只有选中该项，该条绑定条目才能生效。

例1：如果您希望将某台主机的IP地址和MAC地址进行绑定，其IP地址为192.168.1.100，MAC地址为00:19:66:80:54:36，这时您可以按照如下步骤设置：

第一步：在图62界面中点击**增加单个条目**。

第二步：在下图界面设置MAC地址和IP地址。

图 63 添加静态 ARP 绑定条目

第三步：设置完成后，选中“绑定”，并单击**保存**按钮。

4.12.2 ARP映射表

选择菜单**IP与MAC绑定**→**ARP映射表**，您可以在下图界面中查看ARP绑定条目信息。

<input type="checkbox"/>	MAC地址	IP地址	状态
<input type="checkbox"/>	90:2b:34:65:39:3e	192.168.1.105	已导入

图 64 ARP 映射表

- 导入所选条目：该项用来将指定映射条目添加到静态 ARP 列表中(见 图 62)。
- 删除所选条目：该项用来删除 ARP 映射列表中的选中条目。
- 刷新：单击该按钮，您可以更新 ARP 映射列表中的条目信息。

👉 注意：

在进行导入操作时，如果该条目与 ARP 静态绑定表中的某条目冲突，则会显示冲突提示，不会添加该条目。

4.13 动态DNS

选择菜单**动态DNS**，您可以在图 65 界面中进行相应的功能设置。

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。

本路由器提供的DDNS服务为花生壳DDNS，该DDNS的服务提供者是www.oray.net。在图 65界面中注册成功后，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。

动态DNS

本页设置“Oray.net花生壳DDNS”的参数。

服务商链接：[花生壳动态域名解析服务申请](#) [花生壳动态域名解析服务帮助](#)

服务商： [注册...](#)

用户名：

密码：

启用DDNS：

连接状态：未连接

服务类型：---

域名信息：无

图 65 花生壳 DDNS 设置

- 服务商链接：如果您还未在 DDNS 上注册，请选择该选项进行注册。
- 服务商：该项是提供 DDNS 的服务器。
- 用户名、密码：请正确填写在 DDNS 上注册的用户名和密码。
- 启用 DDNS：该项用来启用花生壳 DDNS 服务。
- 连接状态：当前与 DDNS 服务器的连接状态。
- 服务类型：当您成功登录后，该项会显示您注册时帐号所对应的服务类型。
- 域名信息：当前从 DDNS 服务器获得的域名服务列表。
- 登录/退出：点击该按钮，您可以登录/退出 DDNS 服务。

4.14 系统管理

选择菜单**系统管理**，您可看到：



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。

4.14.1 系统日志

选择菜单**系统管理**→**系统日志**，可以在下图 66 中查看路由器的日志信息。该界面记录了路由器的系统日志，可以通过查询日志了解网络情况和快速定位设备故障。

系统日志

选择要查看的日志类型： 选择要查看的日志等级：

索引	时间	类型	等级	内容
1	1970-01-01 04:03:13	DHCPD	Notice	Recv INFORM from 40:61:86:E5:C5:B3
2	1970-01-01 04:03:06	DHCPD	Notice	Send ACK to 192.168.1.103
3	1970-01-01 04:03:06	DHCPD	Notice	Recv REQUEST from 40:61:86:E5:C5:B3
4	1970-01-01 04:03:06	DHCPD	Notice	Send OFFER with ip 192.168.1.103
5	1970-01-01 04:03:06	DHCPD	Notice	Recv DISCOVER from 40:61:86:E5:C5:B3
6	1970-01-01 04:03:01	DHCPD	Notice	Send NAK
7	1970-01-01 04:03:01	DHCPD	Notice	REQUEST ip c0a80166 already reserved by E0:3F:49:11:36:C0
8	1970-01-01 04:03:01	DHCPD	Notice	Recv REQUEST from 40:61:86:E5:C5:B3
9	1970-01-01 03:59:02	DHCPD	Notice	Recv INFORM from E0:3F:49:11:36:C0
10	1970-01-01 03:54:02	DHCPD	Notice	Recv INFORM from E0:3F:49:11:36:C0
11	1970-01-01 03:49:02	DHCPD	Notice	Recv INFORM from E0:3F:49:11:36:C0
12	1970-01-01 03:43:12	DHCPD	Notice	Recv INFORM from E0:3F:49:11:36:C0
13	1970-01-01 03:42:08	DHCPD	Notice	Recv INFORM from E0:3F:49:11:36:C0
14	1970-01-01 03:41:04	DHCPD	Notice	Recv INFORM from E0:3F:49:11:36:C0
15	1970-01-01 03:39:59	DHCPD	Notice	Recv INFORM from E0:3F:49:11:36:C0
16	1970-01-01 03:38:55	DHCPD	Notice	Recv INFORM from E0:3F:49:11:36:C0
17	1970-01-01 03:37:51	DHCPD	Notice	Recv INFORM from E0:3F:49:11:36:C0
18	1970-01-01 03:36:46	DHCPD	Notice	Recv INFORM from E0:3F:49:11:36:C0
19	1970-01-01 03:35:42	DHCPD	Notice	Recv INFORM from E0:3F:49:11:36:C0
20	1970-01-01 03:34:37	DHCPD	Notice	Recv INFORM from E0:3F:49:11:36:C0

刷新 清空日志 保存日志 日志设置

图 66 系统日志

- 刷新：点击此按钮，路由器将刷新页面，显示最新的日志列表。
- 清空日志：点击此按钮，路由器中的日志将被永久删除。

- 保存日志：点击此按钮，路由器中的日志可以保存至本地。

4.14.2 诊断工具

选择菜单**系统管理**→**诊断工具**，您可以在下图界面中通过使用单击“**开始诊断**”按钮来测试路由器和其它主机（包括网络设备）的连接情况。

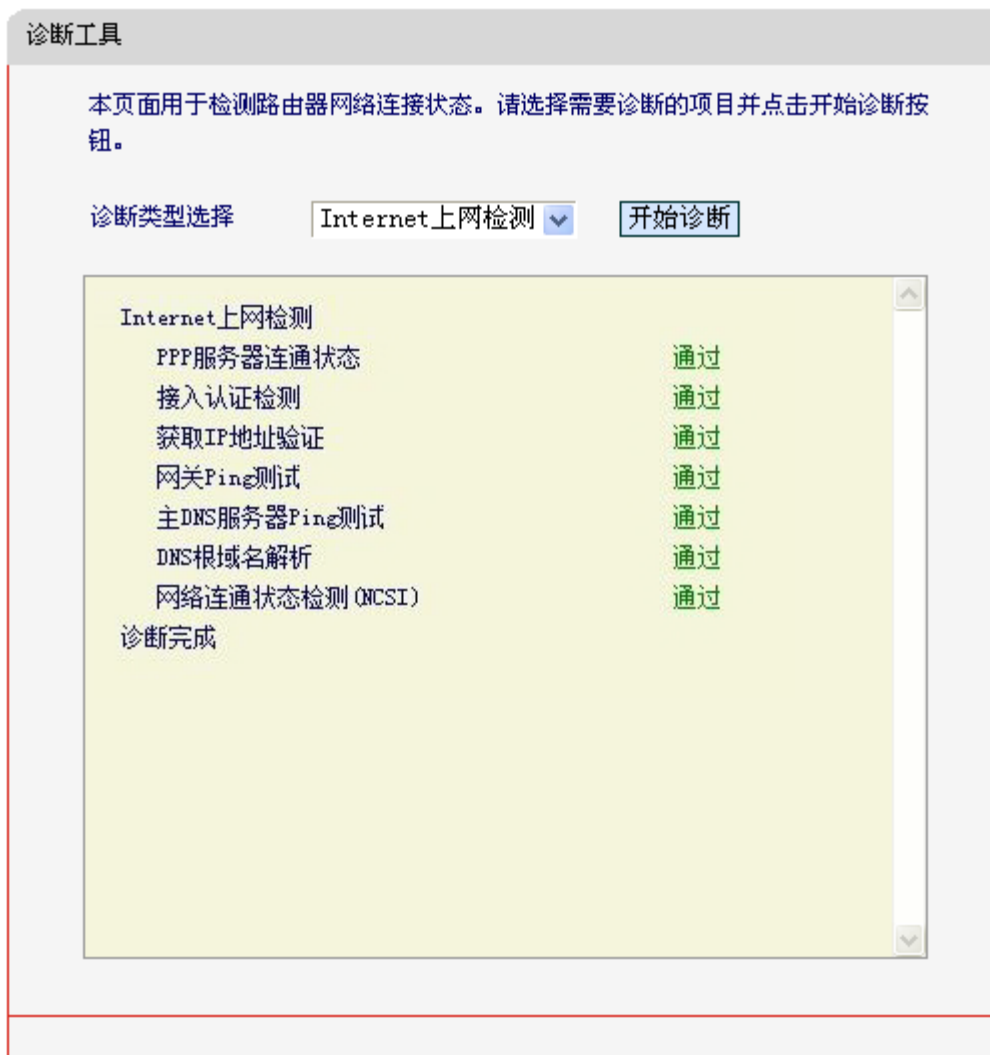


图 67 诊断工具

4.14.3 流量统计

选择菜单**系统管理**→**流量统计**，您可以在图 68 中查看路由器的流量信息。单击**刷新**按钮，您可以更新流量统计表；单击**重置**按钮，您可以重新设置统计粒度；单击**删除**按钮，您可以删除指定的流量统计信息。



图 68 流量统计

- 统计间隔：该数值决定了统计路由器当前流量的时间间隔。
- IP地址：被统计主机的IP地址，此处也会显示该主机的MAC地址。
- 总计：该项分别用数据包个数和字节数来统计路由器接收和发送数据的总流量。
- 当前：该项显示在不同的统计单位下，路由器在当前10秒钟内接收和发送不同数据的总流量。

☞ 注意：

若要查看路由器的流量信息，必须先开启路由器的流量统计功能。如无需流量统计，可以关闭该功能，这样可以提高路由器的数据处理能力。

4.14.4 软件升级

选择菜单**系统管理**→**软件升级**，您可以在图 69界面中升级本路由器的软件版本。

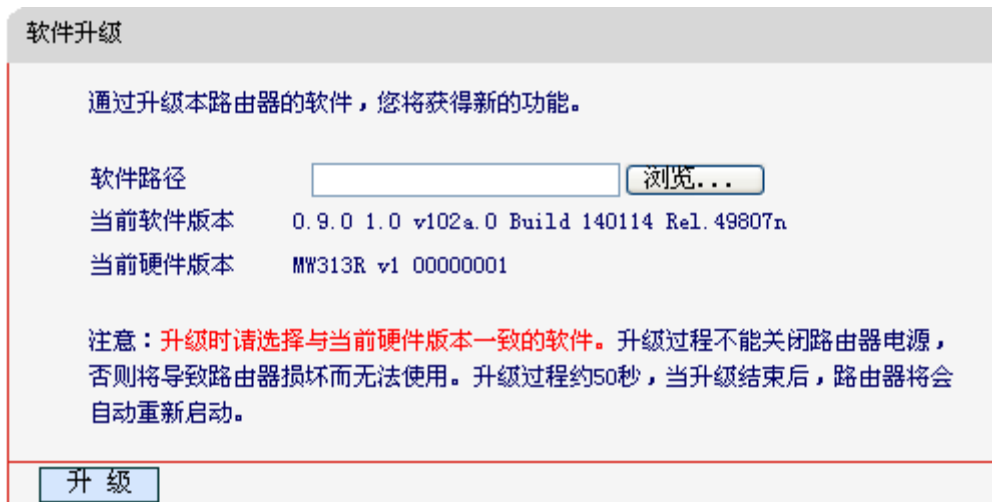


图 69 软件升级

软件升级步骤：

- 第一步：登录本公司的网站(www.mercurycom.com.cn)，下载最新版本的软件。
- 第二步：在“软件路径”文本内填入已下载文件的全路径文件名，或用浏览按钮选择文件。

第三步：单击**升级**进行软件升级。

第四步：升级完成后，300M 无线路由器将自动重启。

注意：

- 1) 升级时请选择与当前硬件版本一致的软件。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。当升级结束后，路由器将会自动重启。
- 2) 软件升级后，路由器可能会恢复到出厂默认设置。

4.14.5 恢复出厂设置

选择菜单**系统管理**→**恢复出厂设置**，您可以将路由器的所有设置恢复到出厂时的默认状态。恢复出厂设置后，路由器将自动重启，如下图。



图 70 恢复出厂设置

单击**恢复出厂设置**按钮，路由器的所有设置将恢复到出厂时的默认状态。其中：

- 默认的 IP 地址：192.168.1.1
- 默认的子网掩码：255.255.255.0

4.14.6 备份和载入配置

选择菜单**系统管理**→**备份和载入配置**，您可以在图 71 中备份或载入路由器配置文件。

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；在升级路由器软件或在载入新的配置文件前备份路由器的原有配置，可以有效防止升级软件或载入新配置文件过程中丢失原有配置的问题。

配置载入功能则可以将先前保存的或已编辑好的配置文件重新载入。如果需要为多台路由器配置相同的设置，则可以先配置一台路由器，保存其配置文件后，再将其载入到其它的路由器中，这样可以有效节省配置时间。

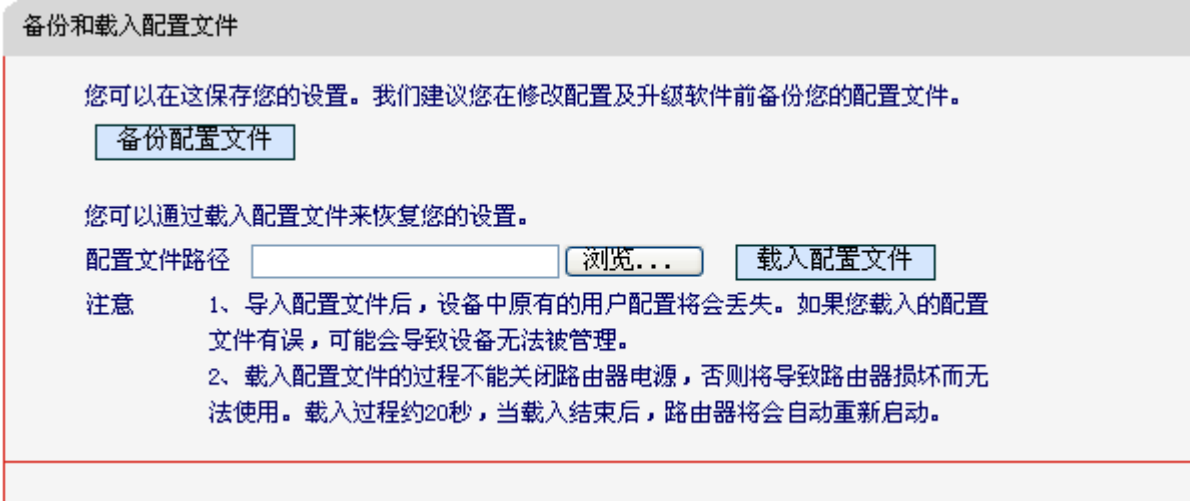


图 71 配置文件备份与载入

例1：如果您希望备份现有路由器的配置文件到C:\Router\backup，您可以按照如下步骤操作。

第一步：在图 71 界面中点击**备份配置文件**。

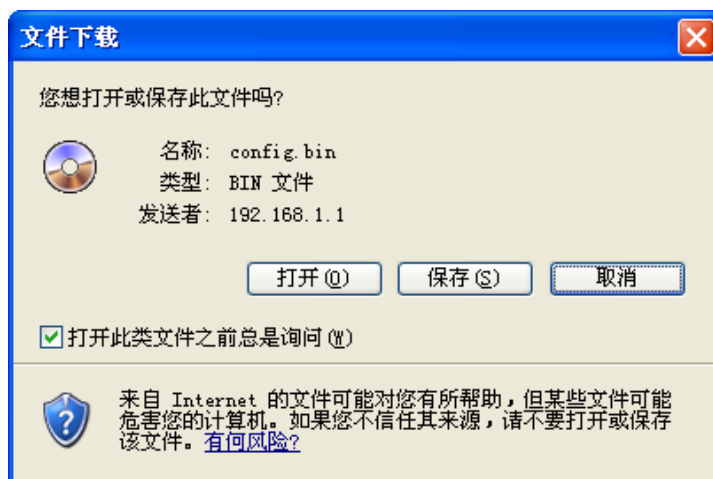


图 72 备份配置文件-文件下载

第二步：在图 72 界面中点击**保存**按钮。

第三步：在图 73 界面中选择文件存放路径“C:\Router\backup”，然后点击**保存**按钮即可完成文件备份。

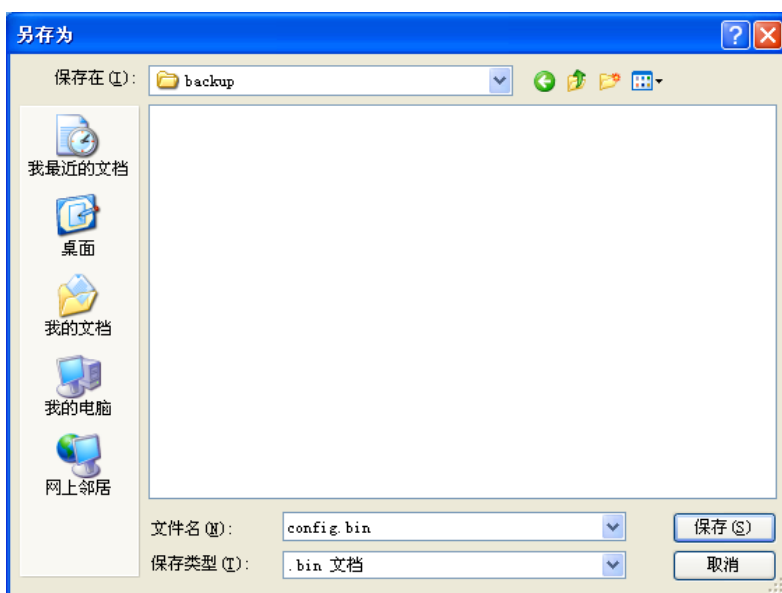


图 73 备份配置文件-选择文件存放路径

例2: 如果您希望将C:\Router\backup目录下的config.bin文件载入到路由器中，您可以按照如下步骤操作。

第一步：在图 71界面中输入文件的全路径“C:\Router\backup\config.bin”；此处也可以单击**浏览**按钮来选定该文件。

第二步：在图 71 界面中点击**载入配置文件**按钮。

☞ 注意：

- 1) 载入配置文件后，设备中原有的配置信息将会丢失，所以在导入配置文件前请先备份配置。如果您载入的配置文件有误，可重新载入先前备份的文件。
- 2) 配置文件载入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，路由器将会自动重新启动。如果载入有错，请根据提示信息自己选择是否保存配置，最好重启路由器。

4.14.7 重启路由器

选择菜单**系统管理**→**重启路由器**，您可以将路由器重新启动，如图 74。



图 74 重启路由器

4.14.8 管理控制

选择菜单**系统管理**→**管理控制**，您可以在图 72 下图界面中查看当前用户状态并进行相应的设置。

管理控制

当前用户状态

用户类型：	Admin
用户名：	admin
用户主机IP地址：	192.168.1.105
用户主机MAC地址：	90:2B:34:65:39:3E

管理帐户设置

原密码：	<input style="width: 100%;" type="password"/>
新密码：	<input style="width: 100%;" type="password"/>
新密码确认：	<input style="width: 100%;" type="password"/>

管理服务设置

	HTTP服务	限定主机 (IP或MAC)
本地管理	端口 <input style="width: 50px;" type="text" value="80"/>	<input style="width: 100%;" type="text"/>
远端管理	<input type="checkbox"/> 开启 <input type="checkbox"/> 端口 <input style="width: 50px;" type="text" value="80"/>	<input style="width: 100%;" type="text"/>

图 75 修改登录口令

- 当前用户状态：显示当前用户类型、用户名、用户主机 IP 地址以及 MAC 地址。
- 管理帐户设置：此处您可以设置新的用户名和密码，用于登录 300M 无线路由器管理页面。
- 管理服务设置：此处您可以更改 300M 无线路由器 Web 管理界面的端口，并且限定主机通过指定端口访问 Web 管理界面。

完成更改后，单击**保存**按钮。

👉 注意：

- 1) 300M无线路由器默认的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1025)，则您必须用“IP地址:端口”的方式(例如http://192.168.1.1:1025)才能登录300M无线路由器执行WEB界面管理。
- 2) 300M无线路由器远端WEB管理默认不开启，点击“开启”，默认的远端WEB管理IP地址为空，在此默认状态下，广域网中所有计算机都能登录300M无线路由器执行远端WEB管理。如果您改变了默认的远端WEB管理IP地址，则广域网中只有具有该指定IP地址的计算机才能登录300M无线路由器执行远端WEB管理。
- 3) 如果WEB管理端口与“转发规则”中虚拟服务器条目的端口产生冲突，当您保存配置时，存在端口冲突的虚拟服务器条目将被自动禁用。

例 1: 如果您希望广域网中 IP 地址为 202.96.134.13 的计算机能够访问 300M 无线路由器，执行远端 WEB 管理功能，WEB 管理端口为 80。则您可以进行如下设置：

第一步：设置 WEB 管理端口为“80”。

第二步：设置远端 WEB 管理 IP 地址为“202.96.134.13”。

这样，该计算机访问 300M 无线路由器管理界面时应该输入 300M 无线路由器 WAN 口 IP 地址即可。

4.14.9 时间设置

选择菜单**系统管理**→**时间设置**，您可以在下图界面中设置路由器的系统时间。您可以选择手动设置时间也可以选择从互联网上获取标准的GMT时间。

图 76 时间设置

- **优先使用 NTP 服务器：**该项用来设置 NTP 服务器的 IP 地址(最多可以输入两个)。NTP 服务器是网络时间服务器，用于互联网上的计算机时间同步。该路由器中内置了一些常用的 NTP 服务器地址，一旦与 Internet 连接后，路由器可以自动获取系统时间。但是，若此处设置了该项，则当路由器获取 GMT 时间时，将优先从已设置的时间服务器上获取。

时间设置步骤：

手动设置时间：首先请选择您所在的时区，然后在日期和时间栏内填入相应值，最后单击**保存**按钮即可完成系统时间的设置。

获取GMT时间：首先请连接互联网，然后选择您所在的时区，最后单击**获取GMT时间**按钮即可从互联网上获取标准的GMT时间。

注意：

- 1) 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。
- 2) 您必须先连上Internet获取GMT时间或在此页手动设置系统时间后，路由器其他功能(如防火墙)中的时间限定才能生效。
- 3) 当选择手动设置时间时，若要查看当前的系统时间，请刷新时间设置页面。

附录A FAQ

1、ADSL用户如何设置上网？

- 1) 首先，将ADSL modem设置为桥模式(RFC 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“上网账号”及“上网口令”，单击**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。

2、如何获取正确的DNS服务器地址？

- 1) 咨询您的网络服务商(ISP)，获取DNS参数；
- 2) 在操作了路由器成功拨号后，登陆到路由器的管理界面，选择菜单**运行状态**，然后便可查看DNS参数并记录。

3、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) 如果希望能接收对方的NetMeeting呼叫，则需要设置虚拟服务器或DMZ主机。假设本地主机192.168.1.102希望接收对方的NetMeeting呼叫。
- 3) 若采用虚拟服务器来实现，设置方法为：进入管理界面，选择菜单**转发规则**→**虚拟服务器**，单击**添加新条目**按钮，然后在随后的界面中设置“服务端口号”为“1720”，这是NetMeeting的连接端口，然后在“IP地址”栏内填入计算机的IP地址(假设IP地址是192.168.1.102)，再在状态栏选择**启用**，单击**保存**按钮即可。如图1中第三条虚拟服务器条目。



图 1

- 4) 若采用DMZ主机来实现，设置方法为：进入管理界面，选择菜单**转发规则**→**DMZ主机**，在“DMZ主机IP地址”栏填入您计算机的IP地址(IP地址是192.168.1.102)，再选中**启用**复选框，

单击**保存**按钮即可。如图2。

DMZ主机

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。

DMZ 状态： 启用 不启用

DMZ主机IP地址：

图2

4、怎样在局域网构建Web服务器？

- 1) 若要在局域网构建其它服务器，只需要参照问题3的第三点设置虚拟服务器即可。
- 2) 若要构建Web服务器，如果Web的服务端口与路由器Web管理界面的缺省端口相同，都是80时，就会引起冲突。这里的解决办法是更改路由器Web管理界面的端口。具体操作如下：
登录路由器管理界面，选择菜单**系统管理**→**管理控制**，在“管理服务设置”栏输入80以外的值，如88。然后单击**保存**并重启路由器。如图3。

管理控制

当前用户状态

用户类型：	Admin
用户名：	admin
用户主机IP地址：	192.168.1.105
用户主机MAC地址：	90:2B:34:65:39:3E

管理帐户设置

原密码：	<input type="text"/>
新密码：	<input type="text"/>
新密码确认：	<input type="text"/>

管理服务设置

	HTTP服务		限定主机 (IP或MAC)
本地管理	端口	<input type="text" value="80"/>	<input type="text"/>
远端管理	开启 <input type="checkbox"/>	端口 <input type="text" value="80"/>	<input type="text"/>

图3

注意：

若要再次登录路由器管理界面，需要在浏览器的地址栏输入路由器WAN口的IP地址和管理端口号才能进行，输入形式为：<http://61.141.186.224:88>(假设路由器WAN口的IP地址是61.141.186.224)。

地址

- 3) 登录路由器管理界面，选择菜单**转发规则**→**虚拟服务器**，单击**添加新条目**按钮，在随后的界面中设置服务端口为“80”，这是Web服务器的连接端口；然后在IP地址栏填入Web服务器的IP地址(假设你指定的Web服务器的IP地址是192.168.1.101)；最后在状态栏选择**启用**并单击**保存**按钮即可。如图4中虚拟服务器中的第二条：



图 4

5、无线信号受哪些因素的影响？

- 1) 家庭的空间都比较拥挤，空间不够开阔，其中房间中的墙壁是最主要的障碍物。由于无线局域网采用的是无线微波频段。微波的最大特点就是近乎直线传播，绕射能力非常弱，因此身处障碍物后面的无线接收设备会接到很微弱的信号，或没有收到信号。
- 2) 物理的障碍物，不仅阻挡微波无线信号，它还能把电磁的能量给吸收掉，生成弱电流泄流掉，因此，无无线信号在家庭环境中最大的金属物体的障碍物是内有钢筋网的楼板，这个方向的信号几乎没有穿透的可能。要能穿透，信号也是非常的弱。
- 3) IEEE 802.11b/g标准的工作频段为2.4GHz，而工业上许多设备也正好工作在这一频段如：微波炉、蓝牙设备、无绳电话、电冰箱等。如果附近有较强的磁场存在，那么无线网络肯定会受到影响。
- 4) 如果在无线环境中存在多台无线设备还有可能存在频道冲突，无线信号串扰的问题。
- 5) 距离无线设备及电缆线路100米内的无线电发射塔、电焊机、电车或高压电力变压器等强信号干扰源，也可能对无线信号或设备产生强干扰。
- 6) 信号实在室外传播天气情况对无线信号影响也很大，如果是在雷雨天或天气比较阴沉的时候信号衰减比较厉害，而晴天里信号能传输的距离会更远。

6、如何改善信号传输质量？

- 1) 为无线路由选择一个最佳的放置地点。这个放置地点的要求如下：一、位置应偏高一些，以便在较高地方向下辐射，减少障碍物的阻拦，尽量减少信号盲区；二、位置地点选择时应使信号尽量少穿越隔墙，最好是房间中的无线客户端能与无线路由之间可视。

- 2) 修改频道，减少无线串扰。注意：设置自己无线信号发射频道时也要尽量保证离别人无线信号频道5个以上。
- 3) 减少居家电器干扰，保证信号畅通无阻。放置无线路由时尽量远离上述设备。
- 4) 如果无线路由天线是可拆卸的，可以通过更换天线达到增强无线信号的目的。

附录B IE浏览器设置

1. 打开 IE 浏览器，选择菜单工具→Internet 选项，如下图 5 示。



图 5

2. 在 Internet 选项界面中选择**连接**，将“拨号和虚拟专用网络设置”中的设置内容全部删除(下图中该内容为空)，如图 6 示。

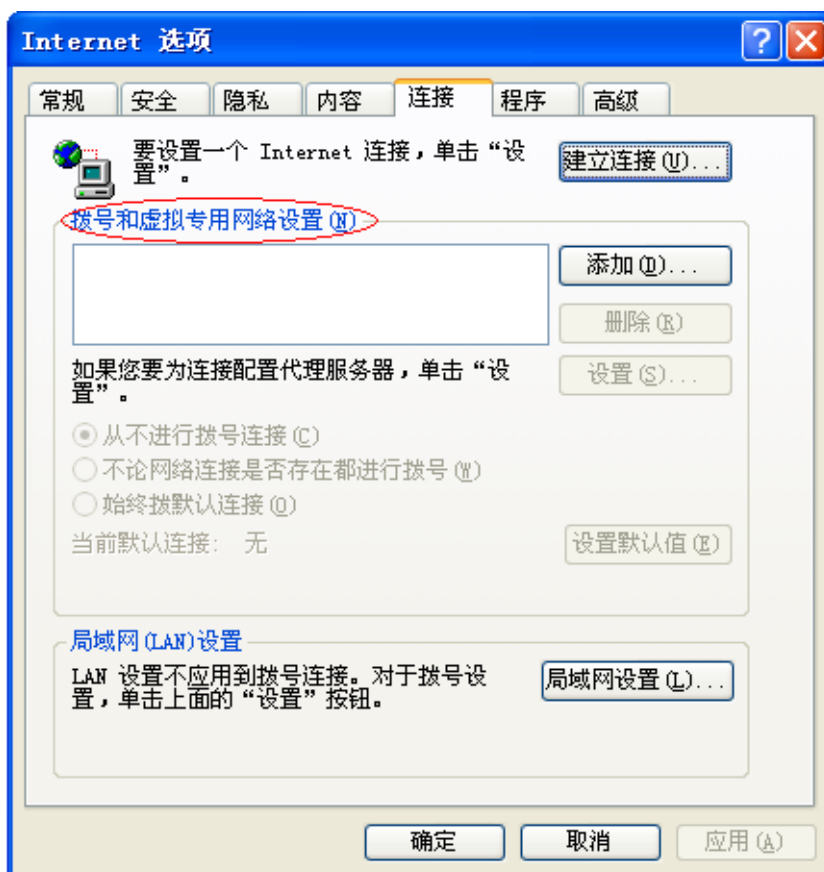


图 6

3. 选择**局域网设置**，按照下图 7 界面所示进行配置。之后单击**确定**按钮返回。

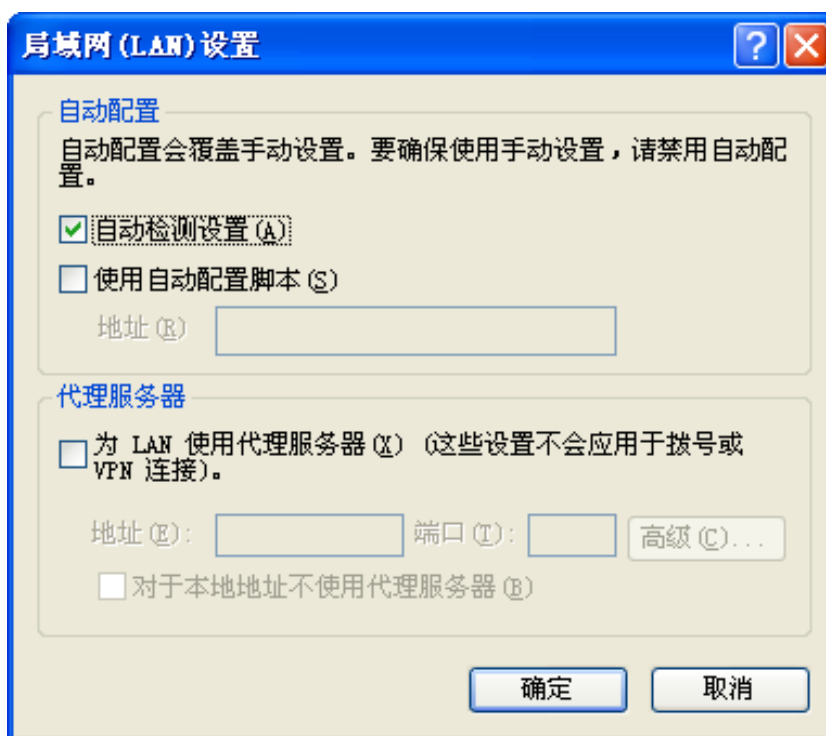


图 7

4. 回到 IE 浏览器界面，选择菜单**文件**，将下拉菜单中的**脱机工作(W)**取消(单击该项将前面的√去掉)，若该项没有启用，则不用设置。如下图 8 示。

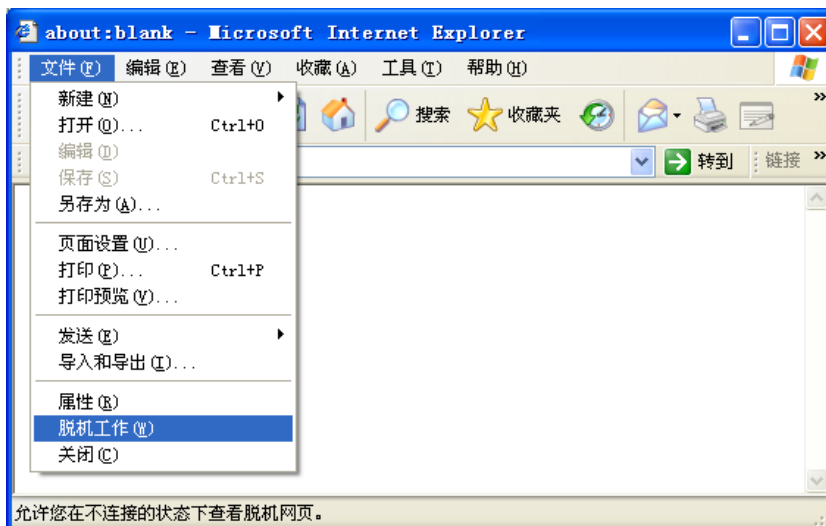


图 8

附录C 规格参数

支持的标准和协议		IEEE 802.11g、IEEE 802.11b、IEEE 802.11n (Draft 2.0)、IEEE 802.3、IEEE 802.3u、IEEE 802.3x、IEEE 802.14X、CSMA/CA、CSMA/CD、TCP/IP、DHCP、ICMP、NAT、PPPoE
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)
无线参数	频率范围	2.4~2.4835GHz
	传输速率	11n: 300M (最大值) 11g: 54/48/36/24/18/12/9/6M (自适应) 11b: 11/5.5/2/1M (自适应)
	工作信道数	13
	展频技术	DSSS (直接序列展频)
	数据调制方式	11g/11n: QPSK,BPSK,16-QAM,64-QAM 11b: CCK,DQPSK,DBPSK
	介质接入协议	CSMA/CA with ACK
	数据加密	支持 WPA/WPA-PSK、WPA2/WPA2-PSK 安全机制, 64/128 位 WEP 加密
网络介质	10Base-T	3 类或 3 类以上 UTP
	100Base-TX	5 类 UTP
LED 指示	端口	WAN, 1/2/3/4 (LAN) (指示各端口的 Link/Act 状态)
	其它	系统状态指示灯
使用环境	工作温度	0 °C ~ 40 °C
	存储温度	-40 °C ~ 70 °C
	工作湿度	10% ~ 90% RH 不凝结
	存储湿度	5% ~ 90% RH 不凝结