

版 权 声 明

IP-COM™是深圳市联科通网络技术有限公司注册商标。这里提及的其它产品和产品名称均是其所属公司的商标或注册商标。本产品的所有部分（包括配件和软件），其版权属于深圳市联科通网络技术有限公司所有，在未经过深圳市联科通网络技术有限公司许可的情况下，不得任意拷贝、抄袭、仿制或翻译。

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

目 录

第一章 产品概述	1
1.1 产品简介.....	1
1.2 主要特性.....	1
1.3 产品规格.....	3
1.4 物品清单.....	4
第二章 硬件描述	5
2.1 面板布置.....	5
2.1.1 前面板.....	5
2.1.2 后面板.....	6
2.2 系统需求.....	6
2.3 安装环境要求.....	6
2.4 硬件安装步骤.....	7
第三章 快速安装	8
3.1 计算机配置.....	8
3.2 验证连通性.....	10
3.3 快速安装.....	11
3.3.1 PPPoE.....	13
3.3.2 动态IP.....	14
3.3.3 静态IP.....	14
第四章 配置说明	16
4.1 运行状态.....	17
4.1.1 WAN口状态.....	17
4.1.2 LAN口状态.....	18

4.1.3 系统信息.....	18
4.2 快速设置.....	19
4.3 局域网设置.....	19
4.3.1 LAN口设置.....	20
4.3.2 域名服务器.....	21
4.3.3 路由器访问限制.....	21
4.4 广域网设置.....	23
4.4.1 WAN口设置.....	23
4.4.1.1 动态IP.....	23
4.4.1.2 静态IP.....	24
4.4.1.3 PPPoE.....	24
4.4.2 MAC地址克隆.....	26
4.4.3 WAN口参数.....	27
4.5 DHCP服务器.....	27
4.5.1 DHCP服务设置.....	27
4.5.2 DHCP客户列表.....	28
4.5.3 静态地址分配.....	29
4.6 ARP表.....	30
4.6.1 IP与MAC绑定.....	30
4.6.2 ARP表.....	31
4.7 虚拟服务器.....	31
4.7.1 端口映射.....	32
4.7.2 DMZ主机.....	33
4.7.3 ALG应用.....	34
4.7.4 UPnP设置.....	35
4.8 安全设置.....	36
4.8.1 客户端过滤.....	36

4.8.2 URL过滤	38
4.8.3 MAC地址过滤	40
4.8.4 ARP防御	42
4.8.5 攻击防护	43
4.8.6 攻击禁止表	46
4.9 带宽设置	46
4.10 连接数设置	47
4.11 流量统计	49
4.12 路由设置	50
4.12.1 系统路由表	50
4.12.2 静态路由	50
4.13 动态DNS	51
4.14 系统工具	52
4.14.1 时间设置	53
4.14.2 远端WEB管理	53
4.14.3 备份/恢复设置	54
4.14.4 软件升级	55
4.14.5 恢复出厂设置	56
4.14.6 重启路由器	56
4.14.7 修改登录口令	57
4.15 系统日志	57
4.15.1 日志设置	58
4.15.2 邮件配置	58
4.16 退出登录	59
附录一 TCP/IP地址设置方法（以WINDOWS XP为例）	60
附录二：常用命令介绍	64

第一章 产品概述

1.1 产品简介

真诚感谢您购买 R5/R7 企业/网吧安全网关路由器。它高达 300MHz（R5）/高达 400MHz（R7）的 CPU 处理，超强 NAT 转发性能，能够保证网络快速、安全、稳定的运行。

R5/R7 除包含所有宽带路由器常见功能外，还支持 IP-MAC 地址绑定功能，有效防止非授权用户接入；防止 ARP、洪水、碎片等攻击，保证带宽稳定性；支持基于协议端口、MAC 地址、URL 及多种特殊应用访问控制，使用户轻松管理网络；支持弹性带宽管理，固定带宽管理，使网络资源得到最大的利用；支持端口转换的虚拟服务器功能，使广域网的用户可以通过路由器的 WAN 口 IP 地址访问多个同类型的内网服务器。可限制单机带宽、连接数，有效防止用户使用 P2P 等特殊应用过度占用网络资源，让网络游戏更顺畅，并提供详细的流量统计列表。

R5/R7 是专门针对网吧、小区、学校、酒店等网络环境比较复杂的用户定义的一款高安全、高性价比产品。

1.2 主要特性

- 符合 IEEE 802.3、IEEE 802.3u、IEEE 802.3x 等标准；
- 提供 1 个 10/100M 自适应以太网（WAN）接口，可接 xDSL/Cable 等设备；
- 提供 4 个 10/100M 自适应以太网（LAN）接口，与内部局域网相连接；
- 支持 IP-MAC 地址绑定功能，有效防止 ARP 攻击、ARP 欺骗和非

授权用户接入：

- 支持基于端口（协议）、MAC、URL 及多种特殊应用访问控制，使用户轻松管理网络；
- 支持弹性带宽管理、固定带宽管理、支持单机限速，保证带宽稳定性,使网络资源得到最大有效的利用；
- 高达 300MHz（R5）/高达 400MHz（R7）的 CPU 处理，超强 NAT 转发性能，支持更多的用户使用
- 支持虚拟服务器、DMZ 主机、ALG 应用
- 支持 VPN 穿透、静态路由功能
- 支持 MAC 地址修改与克隆
- 支持动态域名解析 DDNS 功能
- 提供系统安全日志和流量统计功能
- 支持远程 Web 管理，全中文配置界面
- 内建 DHCP 服务器，同时可进行静态地址分配
- 防止 ARP、洪水、碎片等攻击，保证网络安全稳定
- 支持通用即插即用（UPnP），真正实现 MSN 语音视频通讯
- 内建防火墙，可以精确控制上网时间，支持域名过滤和 MAC 地址过滤

1.3 产品规格

支持的标准和协议		IEEE 802.3、IEEE 802.3u、IEEE 802.3x、TCP/IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS、ARP
网络介质		10Base-T: 3类或3类以上UTP 100Base-TX: 5类UTP
端口和LED指示灯	WAN口	1个“WAN”指示灯和1个“100M”指示灯 (仅R7有100M指示灯)
	LAN口	4个“LAN”指示灯和4个“100M”指示灯 (仅R7有100M指示灯)
	其它	Power (电源指示灯) SYS (系统状态指示灯)
外形尺寸 (L x W x H)		294mm x 180mm x 44mm (R7) 158mm x 105mm x 27mm (R5)
使用环境		工作温度: 0°C 到 40°C; 存储温度: -40°C 到 70°C; 工作湿度: 10%到 90% RH 无凝结; 存储湿度: 5%到 90% RH 无凝结
电源及功耗		R5 输入: DC 9V 1A 功耗: 4W R7 输入: AC 220V 50Hz 功耗: 4W
带机量		R5 (约 30-50 台) R7 (约 50-80 台)

1.4 物品清单

小心打开包装盒，检查包装盒里是否有以下配件：

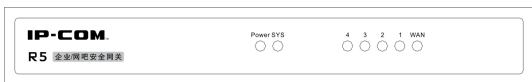
- ✓ R5 或者 R7 企业/网吧安全网关路由器一台
- ✓ 电源适配器（R5）/一条电源线（R7）
- ✓ 一本用户手册
- ✓ 一张保修卡
- ✓ 脚垫四个

如果发现有所损坏或有任何配件短缺的情形，请及时与当地经销商联系。

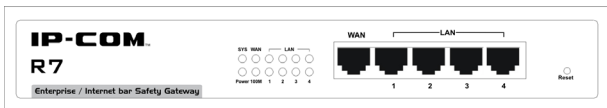
第二章 硬件描述

2.1 面板布置

2.1.1 前面板



R5 的前面板



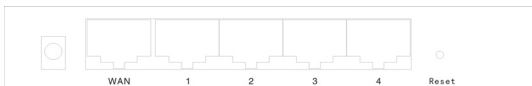
R7 的前面板

- 1) Reset：复位按钮。按住此按钮 5 秒钟后，您设定的资料将被删除，路由器将恢复出厂设置，并自动重启。
- 2) 指示灯：

指示灯	描述	功能
POWER	电源指示灯	供电正常，指示灯常亮
SYS	系统状态指示灯	闪烁表示系统正常 常亮或常灭表示系统不正常
WAN/LAN	广域网和局域网状态指示灯	常亮表示相应端口已正常连接 闪烁表示相应端口正在进行数据传输
100M	广域网和局域网速度指示灯	100M 灯常亮表示相应端口位于 100M 工作模式（仅 R7 有 100M 指示灯）

- 3) WAN: 1 个广域网端口 (RJ-45)。连接 xDSL Modem/Cable Modem 或以太网。
- 4) 局域网端口: 4 个 LAN 端口 (RJ-45)。连接至计算机的以太网网卡, 也可级联交换机。

2.1.2 后面板



R5 的后面板



R7 的后面板

电源: 使用随机附带的是电源适配器 (R5) 或者专用电源线 (R7)。

2.2 系统需求

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

2.3 安装环境要求

- 请不要将路由器放在不稳定的箱子或桌子上, 万一跌落, 会对路由器

造成严重损害。

- 路由器要在正确的电压下才能正常工作，请确认工作电压同路由器所标示的电压相符。
- 在路由器工作时不要打开外壳，即使在不带电的情况下，也不要随意打开路由器机壳。
- 确认路由器的入风口及通风口处留有空间，以利于路由器的散热。

2.4 硬件安装步骤

在安装路由器前，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，请先和您的网络供应商（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路由器。

➤ 建立局域网连接

将路由器 LAN 口和局域网中的交换机或者 Hub 连接。您也可以将路由器 LAN 口直接和您的计算机网卡连接。

➤ 建立广域网连接

将 xDSL 或以太网接入五类线和路由器 WAN 口相连。

➤ 连接电源

将电源连接好，路由器将自行启动。

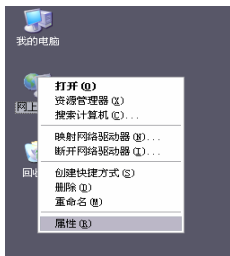
第三章 快速安装

3.1 计算机配置

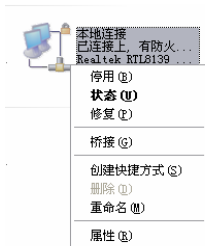
路由器默认 IP 地址是：192.168.0.1，可根据您的需要进行改变，但是我们在这本说明书上将按照默认值进行设置。

将您的计算机连接到路由器的 LAN 口，并按照下面步骤进行设置：

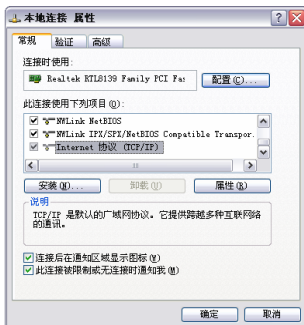
- 在您正在使用的桌面上，用右键单击“网上邻居”，在弹出的菜单中选择“属性”；



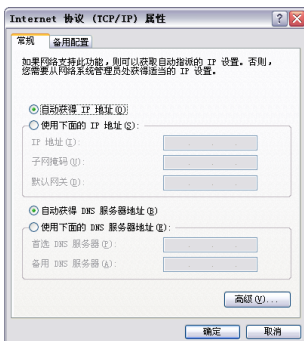
- 在随后打开的窗口里，用鼠标右键点击“本地连接”，选择“属性”；



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



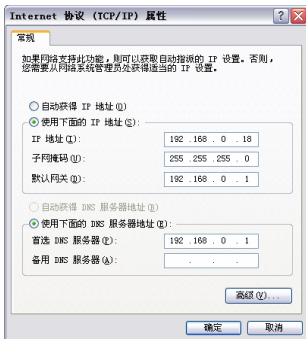
- 在随后打开的窗口里，您可以选择“自动获得 IP 地址（O）”或者是“使用下面的 IP 地址（S）”；
- ✓ “自动获得 IP 地址（O）”如图：



✓ “使用下面的 IP 地址 (S)”

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

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



3.2 验证连通性

设置好 TCP/IP 参数后, 您可以使用 Ping 命令检查您的计算机和路由器之间是否连通:

- 选择“开始——运行”, 在运行对话框输入“cmd”然后点击确定。
- 按图格式输入“ping 192.168.0.1”并回车, 如能得到图示的回应, 则表明您的计算机与路由器连接正常。否则请检查路由器是否通电, 计算机到路由器的网线是否连接好。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\skyng>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=32
Reply from 192.168.0.1: bytes=32 time<1ms TTL=32
Reply from 192.168.0.1: bytes=32 time<1ms TTL=32
Reply from 192.168.0.1: bytes=32 time<1ms TTL=32

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\skyng>
```

3.3 快速安装

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

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

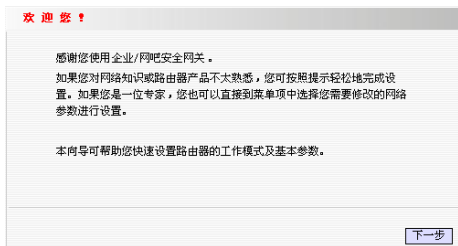


连接建立后，您会看到登录界面。您需要以系统管理员的身份登录，输入用户名和密码（用户名和密码出厂设置均为“admin”），为方便下次快速进入路由器管理页面，请选择“记住我的密码”。

⚠注意：为了路由器的安全，请正确登录后修改系统默认的用户名和密码！

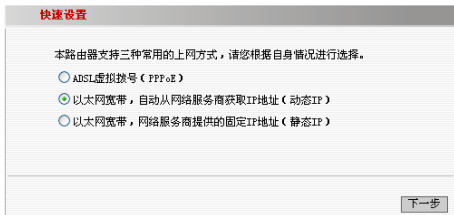


如果您输入的用户名和密码正确，浏览器将进入管理员模式的画面，并出现一个快速设置向导，点击“下一步”，进入上网方式选择画面。



本路由器支持最常见的三种上网方式，（路由器的默认接入方式为动态IP接入）：

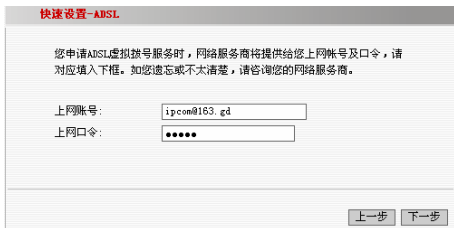
- PPPoE 拨号上网（ADSL）：采用 PPPOE 虚拟拨号来进行 Internet 连接。
- 动态 IP：宽带网络或者有线通（例如：长城宽带）通过 DHCP 服务为用户分配 IP 地址。
- 静态 IP：以太网宽带接入方式 ISP（例如：长城宽带）提供的固定 IP 地址。



可根据自身情况进行选择, 然后单击“下一步”填写上网所需的基本网络参数。

3.3.1 PPPoE

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



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

3.3.2 动态 IP

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

3.3.3 静态 IP

如果您的上网方式为“静态 IP”，输入 ISP 提供给您固定 IP 地址，子网掩码，网关地址以及主 DNS、备用 DNS 地址；点击“下一步”保存即可。

快速设置-静态IP

您申请以太网宽带服务，并具有固定IP地址时，网络服务商将提供给您一些基本的网络参数，请对应填入下框。如您遗忘或不太清楚，请咨询您的网络服务商。

IP地址:

子网掩码:

网关:

DNS服务器:

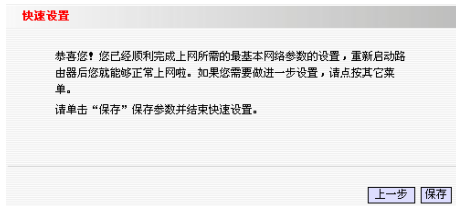
备用DNS服务器: (可选)

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



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

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



当设置完成以后可以到“运行状态”中“WAN口状态”中查看配置信息。

WAN口状态

连接状态	已连接
连接方式	静态 IP
WAN IP	192.168.250.249
子网掩码	255.255.255.0
网关	192.168.250.1
域名服务器	192.168.250.1
备用域名服务器	0.0.0.0
WAN MAC 地址	00:80:0C:52:02:F1
WAN口流量	下行 3.46KB/s 上行 0.07KB/s

第四章 配置说明

本章介绍路由器各种功能在 Web 界面的配置方法，使用户能够轻松使用和管理路由器。在 Web 管理界面中分以下 16 个菜单栏介绍路由器的各个功能：

- 运行状态
- 快速设置
- 局域网设置
- 广域网设置
- DHCP 服务器
- ARP 表
- 虚拟服务器
- 安全设置
- 带宽设置
- 连接数设置
- 流量统计
- 路由设置
- 动态 DNS
- 系统工具
- 系统日志
- 退出登录

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

4.1 运行状态

4.1.1 WAN 口状态

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

WAN口状态	
连接状态	已连接
连接方式	静态 IP
WAN IP	192.168.250.249
子网掩码	255.255.255.0
网关	192.168.250.1
域名服务器	192.168.250.1
备用域名服务器	0.0.0.0
WAN MAC 地址	00:BD:0C:52:02:F1
WAN口流量	下行 3.29KB/s 上行 0.07KB/s

- WAN 口连接状态：显示 WAN 口的连接状态。
未连接：表示 WAN 口未接网线；
连接中：表示 WAN 口已接通，正在获取 IP 地址；
已连接：表示路由器与 ISP 已正常接通；
- 连接方式：表示当前您选的接入方式。
- WAN IP：从 ISP 获取的 IP 地址。
- 子网掩码：从 ISP 获取的子网掩码。
- 网关：从 ISP 获取的网关。
- 域名服务器：从 ISP 获取的域名服务器。
- 备用域名服务器：从 ISP 获取的备用域名服务器。
- WAN 口 MAC 地址：显示 WAN 口的 MAC 地址。
- WAN 口流量：表示当前路由器已使用的带宽，单位为 KB/s。

4.1.2 LAN 口状态

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

LAN口状态	
IP地址	192.168.0.1
子网掩码	255.255.255.0
LAN MAC 地址	00:BD:0C:52:02:F0
DHCP 服务器	允许
NAT/NAT连接数	允许 / 8

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

4.1.3 系统信息

显示路由器当前运行时间、系统时间、已连接客户端、系统版本、引导程序版本、硬件版本号、系统资源。

系统信息	
运行时间	00:20:03
系统时间	2009-04-21 19:40:20
已连接的客户端	1
系统版本	1.0.0.0
引导程序版本	1.0.0.0
硬件版本号	1.0.0.0
系统资源	CPU使用: 0% 内存使用: 45%

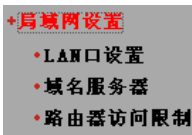
- 运行时间：显示系统正常启动后的运行时间；
- 系统时间：显示系统更新时间；
- 已连接客户端：显示已连接的计算机数（一般只显示通过 DHCP 服务器获得的客户端口的数量）；
- 系统版本：显示路由器的软件版本；
- 引导程序版本：显示路由器的程序版本；
- 硬件版本号：显示路由器的硬件版本；
- 系统资源：显示 CPU 和内存的使用情况；

4.2 快速设置

请参照第三章的快速安装。

4.3 局域网设置

在“局域网设置”菜单下面，共有“LAN 口设置”、“域名服务器”“路由器访问限制”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。



4.3.1 LAN 口设置

LAN口设置

本页面设置LAN口的基本网络参数

MAC地址：您的网关对应的MAC地址。IP地址：当关闭DHCP服务器后，只有手动设置您计算机上的网关为此地址后，才能通过本路由器连接上Internet。

子网掩码：对应网关的网络位和主机位的计算标准，您设置越低的子网掩码，表示您可以获得更多的局域网IP地址。

MAC 地址	00:10:18:01:02:04
IP地址	<input type="text" value="192.168.0.1"/>
子网掩码	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/>

- MAC 地址：显示路由器 LAN 口的 MAC 地址。
- IP 地址：本路由器对局域网的 IP 地址。该 IP 地址的出厂设置为 192.168.0.1，您可以根据需要改变它。
- 子网掩码：该路由器对局域网中的子网掩码。

注意：

1. 如果您修改了该 IP 地址，您必须用新的 IP 地址才能登录路由器进行 WEB 界面管理，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. 路由器 WAN 口获取或指定的 IP 地址和路由器 LAN 口 IP 地址在同一网段，将会影响路由器的使用，导致路由器无法正常工作。紧急时，请使用面板上的复位键进行复位。

4.3.2 域名服务器

域名服务器


在Internet上将网址翻译成IP地址的服务器，您只有设置域名服务器后，才能正常的解析网址并访问网站，在默认情况下，本路由器代理域名服务器功能，当然，您也可以自己设置您需要的域名服务器。

域名服务设置 启用

主DNS服务器

备用DNS服务器(可选)

- 域名服务设置：默认为关闭，启动后，计算机将获取到下面填写的DNS服务器地址；
- DNS服务器：填入ISP提供给您的DNS服务器，不清楚可以向ISP询问。
- 备用域名服务器：可选项，填入ISP提供给您的备用DNS服务器，不清楚可以向ISP询问。

 **注意：** DNS的主要作用是把我们输入的域名(网址)解析为对应的IP地址。

4.3.3 路由器访问限制

为了增加路由器管理的安全性，您可以指定计算机的IP地址和更改路由器端口号来进行管理。

路由器访问限制

为了保护路由器的设置参数不被其他非法用户恶意篡改，本功能将指定特定的用户和使用特定的端口才能访问到本管理界面。


注意：设置本功能后，其它用户将不能登录到本设置界面。建议网吧或企业网络管理员启用此功能。

启用指定访问路由器WEB的主机和端口功能。

IP地址:

端口:

- 启用：开启访问路由器 WEB 限制功能。
- IP 地址：输入局域网中计算机的 IP 地址。
- 端口：默认端口为 80，输入您访问路由器 WEB 界面的端口号。

 **注意：**设置指定IP地址之后，其它地址的主机将不能登陆路由器WEB界面。例如：路由器的IP地址为默认的 192.168.0.1，您仅允许IP地址为 192.168.0.11 的客户机，通过端口 8888 访问路由器WEB界面，则需要设置如下参数，且路由器的访问地址也更改为：<http://192.168.0.1:8888>。

路由器访问限制

为了保护路由器的设置参数不被其他非法用户恶意篡改，本功能将指定特定的用户和使用特定的端口才能访问到本管理界面。

注意：设置本功能后，其它用户将不能登录到本设置界面。建议网吧或企业网络管理员启用此功能。

启用指定访问路由器WEB的主机和端口功能。

IP地址:

端口:

4.4 广域网设置

在“广域网设置”菜单下面，共有“WAN 口设置”、“MAC 地址克隆”“WAN 口参数”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。



4.4.1 WAN 口设置

根据您选择的 WAN 口连接类型，即您的上网方式，可做相应的修改。本路由器默认的上网方式为“动态 IP”。

4.4.1.1 动态 IP

如果您的上网方式为动态 IP，即您可以自动从网络服务商（例如：中国电信、长城宽带）获取 IP 地址。



➤ MTU 默认值为 1500，请根据实际情况进行修改。

4.4.1.2 静态 IP

如果您的上网方式为静态 IP，即您拥有网络服务商（例如：中国电信、中国网通）提供的固定 IP 地址，MTU 默认值为 1500。

WAN口设置

WAN口连接类型：静态IP

IP地址：

子网掩码：

网关：

DNS服务器：

备用DNS服务器：

MTU (如非必要，请勿改动，默认值1500)

➤ MTU 默认值为 1500，请根据实际情况进行修改。

4.4.1.3 PPPoE

如果您的上网方式为 ADSL 虚拟拨号方式，在该页面您可以更改、设置其它参数。

WAN口设置

WAN口连接类型: PPPoE

上网账号:

上网口令:

MTU: (如非必要, 请勿改动, 默认值1492)

服务名: (如非必要, 请勿填写)

服务器名称 (AC NAME): (如非必要, 请勿填写)

根据您的需要, 请选择对应连接模式:

自动连接, 在开机和断线后自动进行连接。

手动连接, 由用户手动进行连接。

按需连接, 在有访问数据时自动进行连接。

自动断线等待时间: (60-3600, 秒) (0表示不自动断线)

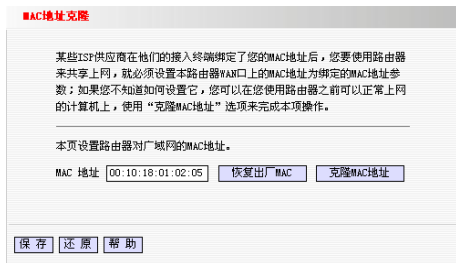
定时连接, 在指定的时段自动进行连接。

注意: 只有当路由器连上Internet, 并获取到标准时间后, “定时连接”功能才能生效。

连接时段: 从 时 分到 时 分


- 上网帐号: 也就是您的上网帐号, 填入 ISP 为您指定的 ADSL 上网帐号。
- 上网口令: 填入 ISP 为您指定的 ADSL 上网口令, 不清楚可以向 ISP 询问。
- 服务名称: 填入 ISP 为您提供的登陆服务名称。(可选)
- MTU: 默认值为 1492, 可根据您的需要进行修改, MTU 值最大不能超过 1492。
- 自动连接: 在开机和断线后自动进行连接。
- 手动连接: 由用户手动进行连接。
- 按需连接: 在有数据访问时自动进行连接。
- 定时连接: 在指定的时段自动进行连接。

4.4.2 MAC 地址克隆

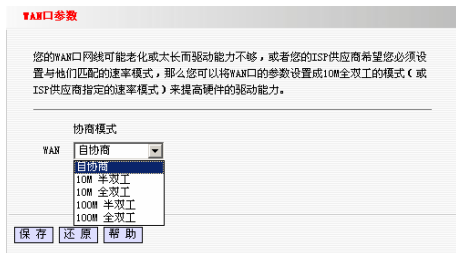


某些 ISP 服务商会绑定用户计算机的 MAC 地址，请将当前管理者的计算机的 MAC 地址，复制到 WAN 口 MAC 地址栏或手动更改 MAC 地址。修改此值后，运行状态中的 WAN 口 MAC 地址将会改变。

- MAC 地址: 默认显示路由器的 WAN 口 MAC 地址, 可手动输入 MAC 地址。
- 恢复出厂 MAC: 点击后 MAC 地址栏会显示路由器的出厂 MAC 地址。
- 克隆 MAC 地址: 点击后 MAC 地址栏会显示当前计算机的 MAC 地址。

 **注意:** 修改 WAN 口 MAC 地址后, 需重新启动路由器才会生效, 如 ISP 没有绑定您的路由器的 MAC 地址, 请不要使用此功能, 以免出现其它问题。

4.4.3 WAN 口参数



您可以按照需要设置 WAN 口的协商模式：自协商、10M 半双工、10M 全双工、100M 半双工、100M 全双工。

4.5 DHCP 服务器

在“DHCP 服务器”菜单下面，有“DHCP 服务设置”、“DHCP 客户端列表”、“静态地址分配”三个子项。下面将详细讲解各子项的功能。

- ◆ DHCP 服务器
 - ◆ DHCP 服务设置
 - ◆ DHCP 客户列表
 - ◆ 静态地址分配

4.5.1 DHCP 服务设置

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

DHCP 服务器设置

DHCP 服务器为 LAN 口上的每台计算机自动分配 IP 地址、网关、域名服务器地址（DNS），如果您关闭了 DHCP 服务器，那么您需要在您的网卡 TCP/IP 协议里手动添加与路由器 LAN 口同一网段的 IP 地址、网关和域名服务器地址（DNS）信息。

DHCP 服务器 启用

IP 池开始地址

IP 池结束地址

过期时间 (1~2880分钟)

主 DNS 服务器

备用 DNS 服务器 (可选)

- DHCP 服务设置：如果您想使用 DHCP 的自动配置 TCP/IP 参数功能，请勾选该选项。
- IP 池开始地址：DHCP 服务器所自动分配的 IP 的起始地址。
- IP 池结束地址：DHCP 服务器所自动分配的 IP 的结束地址。
- 过期时间：DHCP 服务器分配的 IP 地址租期，默认为 2880 分钟。
- 主 DNS 服务器和备用 DNS 服务器：此值随“局域网设置”→“域名服务器设置”中的主 DNS 服务器和备用 DNS 服务器变化而变化，如您需要更改此值，请到“局域网设置”→“域名服务器”页面中进行更改。

 **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”。

4.5.2 DHCP 客户列表

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

DHCP客户端列表

打印DHCP服务器为您的内网用户分配的信息，显示主机名、分配的IP地址、主机MAC地址以及租约时间的对应关系。

刷新

主机名	IP 地址	MAC 地址	租约时间
A1A24D9F96D846F	192.168.0.100	00:B0:0C:77:68:00	1天 23:59:56

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

4.5.3 静态地址分配

为了方便您对局域网中的计算机 IP 地址进行管理，本路由器内置了静态地址分配功能，该功能可以为具有指定 MAC 地址的计算机保留静态的 IP 地址，之后，此计算机请求 DHCP 服务器获得 IP 地址时，DHCP 服务器将给它分配此预留的 IP 地址。

静态地址分配

当您设置静态地址之后，DHCP服务器每次给指定的主机都分配您设置的IP地址，而不会因为空闲关系随机分配，这一功能常常结合虚拟服务器的端口映射来使用。

静态分配

IP 地址

MAC 地址

 : : : : :

添加

序号	IP 地址	MAC 地址	清除
----	-------	--------	----

保存

还原

帮助

- MAC 地址：预留 IP 地址的计算机的 MAC 地址。
- IP 地址：预留的 IP 地址。
- 添加：将预留的 IP 地址和 MAC 地址添加到表中。
- 清除：将已建立的静态分配信息清除。

4.6 ARP 表

4.6.1 IP 与 MAC 绑定

本页设置单机的 MAC 地址和 IP 地址的匹配规则，防止其他非法 IP 和非法 MAC 接入网络，防止 ARP 欺骗。

指定 IP 地址与 MAC 地址的一一对应关系，路由器查看接收到的数据包中的 IP 地址与 MAC 地址，如果与绑定的对应关系不一致，则视为非法，不允许通过和连接上路由器。

如果你想启用 IP-MAC 绑定，请点击勾选启动 IP-MAC 绑定。

IP-MAC 绑定

您的内网用户可能恶意占用他人的IP地址来逃避您设置的过滤规则，在启用此功能后，如果路由器检测到有非法占用IP地址的情况（没有在列表里允许的用户，或是访问的用户IP地址和MAC地址对应关系有错误），将不被授权访问Internet。建议您将局域网中每一台计算机的MAC地址和IP地址绑定；此举也可以防止来自内网和外网的ARP攻击与欺骗从而提升本地网络的安全性。

启用IP-MAC绑定

ARP列表:

IP地址:

MAC地址:

备注:

序号	IP地址	MAC地址	备注	删除
0	192.168.0.135	00:B0:0C:77:88:00	135	<input type="button" value="删除"/>

- ARP 列表：显示 ARP 表中相对应的 IP 和 MAC 地址，如需增加 IP 和 MAC 地址，需在 ARP 列表中选择“手动设置”选项。

- IP 地址：需绑定的 IP 地址。
- MAC 地址：需绑定的 MAC 地址。开启绑定后，只有实现绑定表中的 IP 和 MAC 地址的一一对应才可以访问网络。
- 备注：对该绑定条目的简单描述。
- 添加绑定到列表：点击将需绑定的 IP 和 MAC 添加到列表中。
- 删除：点击删除绑定。

4.6.2 ARP 表

ARP列表

本页面显示局域网所有用户的IP地址和MAC地址的对应消息（DHCP客户端列表仅显示DHCP分配下的对应消息），您可以在此列表里选择“绑定”，方便的进行IP地址与MAC地址的绑定规则。

序号	IP地址	MAC地址	绑定
0	192.168.0.100	00:B0:0C:77:88:00	<input type="button" value="绑定"/>
1	192.168.0.1	00:10:A3:0A:6E:76	<input type="button" value="绑定"/>

ARP 列表中显示了网段内客户端对应的 IP 地址和 MAC 地址，如果直接点击“绑定”按钮即可轻松实现绑定。如果需要删除，请点击“IP-MAC 绑定”，在选择列表中选择“删除”按钮即可删除绑定。

4.7 虚拟服务器

在“虚拟服务器”菜单下面，有“端口映射”、“DMZ 主机”“ALG 应用”、和“UPnP 设置”四个子项。单击某个子项，您即可进行相应的功能查看与设置。

- + 虚拟服务器
 - 端口映射
 - DMZ 主机
 - ALG 应用
 - UPnP 设置

4.7.1 端口映射

端口映射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。端口映射允许建立各种公共服务，例如 WEB 服务器、FTP 服务器等。

端口映射

当您在局域网设置了服务器并希望Internet上的用户能访问到您的服务器，您还需要将您的服务器通过路由器映射出去。每个服务器都有不同的服务端口，例如WEB服务器使用80端口，Telnet使用23端口。

端口映射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重定位给通过IP地址指定的局域网网络服务器。

WAN端口: 常用服务: HTTP (80) ▼

LAN端口:

内网IP:

协议: TCP ▼

启用:

[添加到列表](#)

虚拟服务器列表						
编号	WAN端口	LAN端口	内网IP	协议类型	状态	操作
1	40	80	192.168.0.10	tcp	启用	修改 删除


[保存](#) [还原](#) [帮助](#)

- ✧ **WAN 端口:** WAN 服务端口，即提供外网服务的端口
常用服务: 常用服务的选项中列举了一些常用协议的端口，如 DNS (53)、FTP (21)、GOPHER(70)、HTTP(80)、NNTP(1190)、POP3(110)、PPTP(1723)、SMTP(25)、SOCK(1080)、TELNET(23)。对于常用服务端口中没有列出的端口，您也可以手动添加。
- ✧ **LAN 端口:** 局域网中的服务器发布服务所使用的端口；
- ✧ **内网 IP:** 局域网中作为服务器的计算机的 IP 地址；
- ✧ **协议:** 包含 TCP、UDP 和全部。当您对使用的协议不确定时，可以选择全部。

- ◇ **启用**：只有选中该项后本条目所设置的规则才能生效。
- ◇ **修改**：对对应的编号的端口映射进行修改
- ◇ **删除**：删除选定的端口映射规则。

举例说明：

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

 **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“远端 WEB 管理”项设置为 80 以外的值，如 8080，否则会发生冲突，而导致虚拟服务器不生效。

4.7.2 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主机

在某些应用下，您局域网的服务器可能需要将所有的应用端口全部映射到 Internet 上，以实现双向通信，此时，您可以设置该计算机为 DMZ 主机。
注意：设置计算机为 DMZ 主机之后，该计算机将不受路由器的保护，同时路由器上设置的过滤规则将不对该计算机生效。

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。
(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。)

DMZ 主机 IP 地址： 启用

设置步骤：首先在 DMZ 主机 IP 地址输入需设为 DMZ 主机的局域网计算机的 IP 地址，然后点击“启用”完成 DMZ 主机的设置。

 **注意：** 设置 DMZ 之后，与该 IP 地址相关的 WAN、LAN 口防火墙将不起作用。

4.7.3 ALG 应用

ALG(Application Layer Gateway)即应用层网关。一些早期设计的应用层协议，比如 FTP、TFTP，在穿越 NAT 设备后往往不能正常工作。在这种情况下，您可以在本页面启用相应协议的 ALG，来克服这些问题。



ALG 应用设置

应用层网关ALG(Application Level Gateway)，能识别应用层中的信息，在应用运行的时候建立适当的映射，以此增强对应用的支持。可以根据实际应用的需要来进行选择。

FTP 启用

TFTP 启用

PPTP 启用

IPSec 启用

L2TP 启用

FTP、TFTP 这些应用层协议，客户端会先通过某个知名端口连接到服务器，进行控制交互。在这个过程中，客户端的报文里通常会携带有自己机器本身的 IP 地址和端口号，告知服务器后续数据发往报文里的指定的 IP 地址和端口号。如果客户端是经过 NAT 设备接入 Internet 的话，那么服务器将无法直接访问到客户端指定的地址和端口。ALG 正是为了解决这个问题而设计的，它可以将报文里客户端的 IP 地址和端口改成 NAT 设备的 IP 地址和一个空闲的端口号，后续服务器发往 NAT 设备的数据将会被正确

地转发到内网的客户端。路由器缺省情况下，以下协议的 ALG 已经启用，建议保留缺省设置，不做修改。

4.7.4 UPnP 设置

支持最新的 Universal Plug and Play (UPnP 通用即插即用网络协议)，此功能需要 Windows ME/Windows XP 以上的操作系统(注：系统需集成，安装 Directx9.0 或更新版本)或支持 UPnP 的应用软件才能生效。例如：Windows XP 系统上安装了迅雷等 P2P 软件，在上传和下载时可以利用 UPnP 协议。启用 UPnP 功能后，当启用迅雷时就可以看到端口转换信息，端口转换信息由应用程序发出请求时提供。

UPnP 设置

UPnP 允许自动发现和设置联机在网络上的设备，此功能主要应用在自动端口映射，使迅雷、FlashGet、BitTorrent、eMule、BitComet 等 P2P 软件获得最佳的应用。

启用 UPnP

UPnP 映射表

ID	远端主机	外部端口	内部主机	内部端口	协议	描述
1	192.168.100.135	13949	192.168.0.100	13949	TCP	Thunder5
2	192.168.100.135	13949	192.168.0.100	30791	UDP	Thunder5

- ID：表示建立表项的序号。
- 远端主机：接受或发出响应的远端主机的描述。
- 外部端口：端口转换使用的路由器端口号。
- 内部主机：接受或发出响应的内部主机的描述。
- 内部端口：需要进行端口转换的主机端口号。

- 协议：表明是对 TCP 还是 UDP 进行端口转换。
- 描述：映射端口及软件信息。

4.8 安全设置

在“安全设置”菜单下面，共有“客户端过滤”、“URL 过滤”、“MAC 地址过滤”、“ARP 防御”、“攻击防护”和“攻击禁止表”六个子项。下面将详细讲解各子项的详细功能。



4.8.1 客户端过滤

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

过滤模式	局域网IP段	广域网端口段	类型	时间	星期	操作
					日 一 二 三 四 五 六	

- 过滤模式：有“仅禁止”和“仅允许”两种选项。

仅禁止：只禁止符合规则的数据包通过路由器，其它没有被限制的数据包，可以正常通过路由器。过滤规则只对对应的 IP 或 IP 段生效。

仅允许：只允许符合规则的数据包通过路由器，其它没有被限制的数据包，不能通过路由器。过滤规则只对对应的 IP 或 IP 段生效。

- 注释：即为此配置文件定义的简单描述。
- 局域网 IP 段：填入局域网中被控制的计算机的 IP 地址，您可以使用一个 IP 地址范围。
- 广域网端口段：填入的端口号，您可以指定一个端口范围，为空表示所有端口 1-65535。
- 类型：选择被控制的数据包所使用的协议（“全部”包括 TCP/UDP）；
- 时间：您希望本条规则生效的起始时间和终止时间。如果不设置时间，默认显示为全 0，表示为 24 个小时。
- 日期：根据自身的要求选择相应的选项。
- 添加过滤规则：点击将该条规则添加到列表中。
- 保存：完成设置。



注意：过滤规则，只对对应的 IP 或 IP 段生效，对于其他不符合过滤规则的 IP 不做限制。

例如 1：如果您希望局域网中 IP 地址为 192.168.0.11-192.168.0.22 的计算机在每天的 8:00-18:00 时间段内不能浏览 WEB 网站，对局域网中其它计算机则不做任何限制，这时您需要设置如下参数：

客户端过滤

启用客户端过滤

过滤模式: 访问Internet

注释:

局域网IP段:

广域网端口段:

类型:

时间: : ~ :

日期: 每天 星期日 一 二 三 四 五 六

过滤模式	局域网IP段	广域网端口段	类型	时间	星期							操作				
					日	一	二	三	四	五	六					
仅禁止	192.168.0.11-192.168.0.22	80-80	全部	08:00-18:00	√	√	√	√	√	√	√	√	√	√	修改	删除

例如 2: 如果您希望局域网中 IP 地址为 192.168.0.100-192.168.0.200 的计算机在每天的 8:00-18:00 时间段内仅允许收发邮件, 对局域网中其它计算机则不做任何限制, 这时您需要设置如下参数:

客户端过滤

启用客户端过滤

过滤模式: 访问Internet

注释:

局域网IP段:

广域网端口段:

类型:

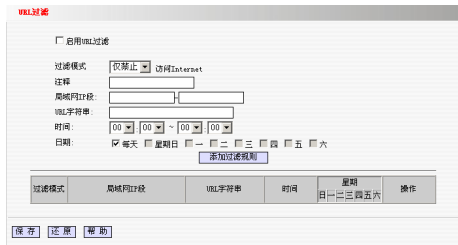
时间: : ~ :

日期: 每天 星期日 一 二 三 四 五 六

过滤模式	局域网IP段	广域网端口段	类型	时间	星期							操作			
					日	一	二	三	四	五	六				
仅允许	192.168.0.100-192.168.0.200	25-25	全部	08:00-18:00	√	√	√	√	√	√	√	√	√	修改	删除
仅允许	192.168.0.100-192.168.0.200	110-110	全部	08:00-18:00	√	√	√	√	√	√	√	√	√	修改	删除

4.8.2 URL 过滤

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



- 过滤模式：只能选择“仅禁止”和“仅允许”中的任何一项，不能混合选择过滤模式。

仅禁止：只禁止符合规则的数据包通过路由器，其它没有被限制的数据包，可以正常通过路由器。过滤规则只对对应的 IP 或 IP 段生效。

仅允许：只允许符合规则的数据包通过路由器，其它没有被限制的数据包，不能通过路由器。过滤规则只对对应的 IP 或 IP 段生效。

- 注释：即为此配置的简单描述。
- 局域网 IP 段：开始 IP 到结束 IP。
- URL 字符串：填入被过滤的域名和域名的一部分。
- 时间：设置您希望本条规则生效的起始时间和终止时间，如果不设置时间，默认显示为全 0，表示为 24 个小时。
- 日期：根据自身的要求选择相应的选项。
- 添加过滤规则：点击将该条规则添加到列表中。
- 保存：完成设置。

⚠注意：过滤规则，只对对应的 IP 或 IP 段生效，对于其他不符合过滤规则的 IP 不做限制。

例如 1：如果您不允许局域网中 IP 地址为 192.168.0.100~192.168.0.200 的计算机浏览包含“sex”字符串的 WEB 网

站，对局域网中其它计算机则不做任何限制，您需要设置如下参数：

URL过滤

启用URL过滤

过滤模式: **禁止** 访问Internet

注释:

局域网IP地址:

URL字符串:

时间: : : ~ :

日期: 每天 星期日 一 二 三 四 五 六

过滤模式	局域网IP地址	URL字符串	时间	星期							操作	
				日	一	二	三	四	五	六		
禁止	192.168.0.100-192.168.0.200		00:00:00-00:00:00	√	√	√	√	√	√	√	修改	删除

例如 2: 如果您只允许局域网中 IP 地址为 192.168.0.10~192.168.0.20 的计算机，可以浏览包含“sina”，“baidu”，“163”字符串的 WEB 网站，而不能访问其它网站，且其它计算机可以正常浏览所有的 WEB 网站。您需要设置如下参数：

URL过滤

启用URL过滤

过滤模式: **禁止** 访问Internet

注释:

局域网IP地址:

URL字符串:

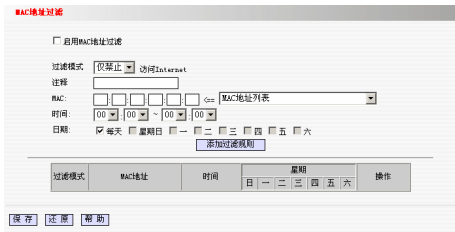
时间: : : ~ :

日期: 每天 星期日 一 二 三 四 五 六

过滤模式	局域网IP地址	URL字符串	时间	星期							操作	
				日	一	二	三	四	五	六		
禁止	192.168.0.10-192.168.0.20	sina, baidu, 163	00:00:00-00:00:00	√	√	√	√	√	√	√	修改	删除

4.8.3 MAC 地址过滤

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



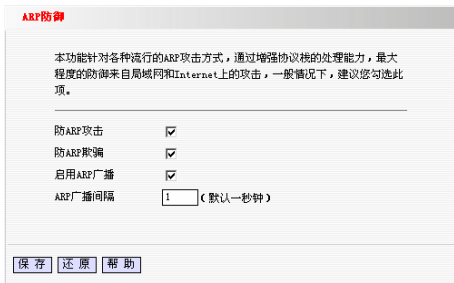
- 过滤模式：只能选择“仅禁止”和“仅允许”中的任何一项，不能混合选择过滤模式。

仅禁止：只禁止所设置的规则的数据包禁止通过路由器，其它没有被限制的数据包通过路由器。

仅允许：仅允许所设置的规则的数据包通过路由器，其它数据包全部禁止通过路由器。

- 注释：即为此配置的简单描述。
- MAC:输入您要控制的 MAC 地址或直接从后面的路由器已学习到的 MAC 地址表中导入。
- 时间：设置您希望本条规则生效的起始时间和终止时间，如果不设置时间，默认显示为全 0，表示为 24 个小时。
- 日期：根据自身的要求选择相应的选项。
- 保存：完成该设置。
- 删除：删除对应的该条规则。

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



4.8.5 攻击防护

在“攻击防护”页面, 共有“应用安全过滤”、“DDOS 攻击过滤”和“常见病毒过滤”三个子项, 下面将详细讲解各子项的详细功能。

a) 应用安全过滤

应用安全过滤, 主要是为了管控影响网络健康的应用、异常行为和不安全服务。勾选对应的选项, 即可实现对某些应用程序和服务的过滤。



b) DDOS 攻击过滤

当局域网内遭遇流氓软件、病毒和木马的攻击时，上网稳定性和网络效能会极大降低，并可能引发掉线；当遭遇 DDOS 攻击时，会造成网络拥塞，使受害主机无法正常和外界通讯，严重时会造成系统死机。为了保障局域网的稳定性，建议您勾选此类过滤。

DDOS攻击过滤

许多网页中都包含了流氓软件、病毒和木马，当局域网中部分计算机中包含这些威胁时，上网稳定性和网络效能会极大降低，并可能引发掉线；遭遇DDOS攻击时：
被攻击主机上有大量等待的TCP连接
网络中充斥着大量的无用的数据包，源地址为假
制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯
利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求
严重时会造成系统死机
针对各种Distribution Denial of service (分布式拒绝服务攻击)进行保护。一般情况下，建议您勾选此项。

忽略WAN口的PING包
 禁止PING网关
 忽略端口扫描报文
 阈值(2000 - 1000000) : 微秒
 启用ICMP-Flood攻击防御
 ICMP-Flood数据包阈值(5-3000) : 包/秒
 启用TCP-SYN-Flood攻击防御
 TCP-SYN-Flood数据包阈值(5-3000) : 包/秒
 启用UDP-Flood攻击防御
 UDP-Flood数据包阈值(5-3000) : 包/秒

- **忽略来自 WAN 口 Ping:** 启用此功能后路由器将不再回应来自 WAN 口的 Ping 检测。勾选后启用此功能。
- **禁止 PING 网关:** 启用可防冲击波病毒攻击。路由器可以防御 DDos 攻击、冲击波、震荡波等病毒。勾选后启用此功能。
- **忽略端口扫描报文:** 这是指在小于规定的时间内，源 IP 发送 TCP SYN 包到同一目的地址的 10 个不同端口，则被认为此源地址正在进行端口扫描攻击。阈值选择范围为 2000-1000000 微秒。勾选后

启用此功能。

- **启用 ICMP-Flood 攻击防御：**这是指在一秒钟内，如果一个目的 IP 收到超过规定数量的 ICMP 请求包，则认为此目的 IP 正受到 ICMP Flood 的攻击。阈值选择范围为 5-3000 包/秒。勾选后启用此功能。
- **启用 TCP-SYN-Flood 攻击防御：**这是指在一秒钟内，如果一个目的 IP 的某一端口收到超过规定数量的 TCP SYN 包，则认为此目的 IP 的此端口正受到 SYN Flood 的攻击。阈值选择范围为 5-3000 包/秒。勾选后启用此功能。
- **启用 UDP Flood 攻击防御：**这是指在一秒钟内，如果一个目的 IP 的某一端口收到超过规定数量的 UDP 包，则认为此目的 IP 的此端口正受到 UDP Flood 的攻击。阈值选择范围为 5-3000 包/秒。勾选后启用此功能。

c) 常见病毒过滤

木马、钓鱼网站等网络病毒的攻击，会威胁网络安全，降低网络稳定性。启用此功能，可以防御一些常见网络病毒的攻击和渗透。

常见病毒过滤

本功能可防御木马、钓鱼网站等一些常见网络病毒的攻击和渗透。
注意：本功能开启后可能会导致某些网络应用失效。

启用病毒过滤

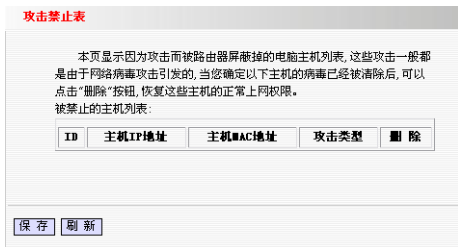


注意：

启用过滤功能，可能会导致某些网络应用失效，请慎用。

4.8.6 攻击禁止表

本页显示因为攻击而被路由器屏蔽掉的电脑主机列表,这些攻击一般都是由于网络病毒攻击引发的,当您确定以下主机的病毒已经被清除后,可以点击"删除"按钮,恢复这些主机的正常上网权限。



路由器一旦发现有电脑存在病毒或制造恶意攻击,自动将其 IP 地址和 MAC 地址显示在列表中,如果您开启了此功能,那么该表中的计算机将无法正常上网。

4.9 带宽设置

宽带控制可以限制内网计算机上网的通信流量,设备可以最多设置 20 条限制规则,最多同时支持 254 台 PC 的流量限制,并支持地址段的配置方式。

带宽控制

本页面设置您的局域网用户通过路由器所能拥有的实际上传速率和下载速率。您可以：

- 弹性设置单个IP或群组IP的最小带宽或最大带宽；
- 设置每一群组IP的带宽优先级；
- 根据您的网络实际使用不同的带宽控制策略；

注意：为了使您的设置更有效，请在WAN口带宽限制中填写您的ISP供应商给您提供的带宽。类型设置中的“独立”是指您的上传/下载限制对每个用户单独生效；“共享”是指您的上传/下载限制对用户组内的整体数据量传输生效。

启用带宽控制

局域网IP段：

上行带宽范围： KB/s

下行带宽范围： KB/s

类型：

启用：

序号	局域网IP段	上行速率	下行速率	类型	启用	删除

- ✧ **启用带宽控制：** 开启和关闭内网 IP 带宽控制功能。默认为关闭。
- ✧ **局域网 IP 段：** 流量控制的主机 IP 地址范围，可以是单个 IP，也可以是一个 IP 段。
- ✧ **上行/下行带宽范围：** 允许指定 IP 范围内的主机上传/下载的最小到最大数据流量，单位是 KByte/s。
- ✧ **类型：** 选择流量限制的服务类型。分为二种：独立和共享。
- ✧ **启用：** 启用当前编辑规则。如果没选，虽然存在这条规则，但不生效。
- ✧ **添加带宽规则：** 编辑完成后，点击“添加带宽规则”按钮可以把当前编辑的带宽控制规则加入规则表中。
- ✧ **保存：** 用户单击“保存”后，当前所编辑的规则才能生效。

4.10 连接数设置

本页设置单机的连接数限制。对指定 IP 地址的计算机连接数进行限

制，超过限制的新连接不允许通过路由器，未指定的计算机可以不受限制的建立连接。

连接数设置

本页面设置您的局域网用户通过路由器所能拥有的实际NAT连接数。
注意：类型设置中的“独立”是指您的连接数限制对每个用户单独生效；
“共享”是指您的连接数限制对用户组内的整体数据传输生效。
一般情况下，如果不希望局域网用户进行P2P软件进行上传和下载，我们推荐您设置每个用户的连接数为150~200。

启用连接数限制

起始IP

终止IP

类型

连接数限制 (范围: 1~9999)

起始IP	终止IP	类型	连接数	删除
------	------	----	-----	----

- **启用连接数限制：**选择后启用此功能。
- **起始/终止 IP：**输入要控制的 IP 地址段。
- **类型：**选择连接数限制的类型。分为二种：独立和共享。
独立：是指对每个用户单独生效，限制每个用户的最大连接数；
共享：是指对组内的整体数据生效，限制整个用户组的连接数总和。
- **连接数限制：**该计算机允许的最大连接数，设置范围为 1-9999。
- **添加连接数限制：**将此规则添加到连接数列表中。

例如：您需要限制的计算机的 IP 地址为 192.168.0.100-192.168.0.200，允许的最大连接为 200，限制类型为共享，这时您需要做如图配置：

连接数设置

本页面设置您的局域网用户通过路由器所能拥有的实际NAT连接数。
注意：类型设置中的“独立”是指您的连接数限制对每个用户单独生效；
“共享”是指您的连接数限制对用户组内的整体数据流传输生效。
一般情况下，如果不希望局域网用户进行P2P软件进行上传和下载，我们推荐您设置每个用户的连接数为150~200。

启用连接数限制

起始IP
终止IP
类型
连接数限制 (范围: 1~9999)

起始IP	终止IP	类型	连接数	删除
192.168.0.100	192.168.0.200	共享	200	<input type="button" value="删除"/>

4.11 流量统计

流量统计

本页面统计您局域网内每个用户的上传/下载数据量，以及即时的上传/下载流量和连接数。

启用流量统计

速率单位：KB/s (千字节/秒)

IP地址	MAC地址	↑包数	↑字节数	↓包数	↓字节数	↑速率	↓速率	连接数
192.168.0.135	00:80:0C:77:88:00	11115	784012	13201	9473123	0.43	0.21	97

- **启用流量统计：**选择后启用此功能。系统默认为关闭，如不需流量统计，请关闭此功能，可提高路由器的数据包处理能力。
- **刷新：**点击更新统计列表。

4.12 路由设置

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

+ 路由设置

- 系统路由表
- 静态路由

4.12.1 系统路由表

本页显示路由器核心路由表的内容。

系统路由表

本页面显示路由器的路由信息表。

目的IP	子网掩码	网关	metric	接口
239.255.255.250	255.255.255.255	0.0.0.0	0	br0
192.168.0.0	255.255.255.0	0.0.0.0	0	br0
192.168.136.0	255.255.255.0	0.0.0.0	0	eth2.2
0.0.0.0	0.0.0.0	192.168.136.1	0	eth2.2

4.12.2 静态路由

本页设置路由器的静态路由功能，您可以指定静态路由规则。

静态路由

本页面可手动为路由器添加路由信息表。

目的网络 IP	子网掩码	网关	操作
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="添加"/>

- 目的网络 IP：目的主机的 IP 地址或目的网络的 IP 地址。
- 子网掩码：目的地址的子网掩码，一般为 255.255.255.0。
- 网关：下一跳路由器入口的 IP 地址。
- 添加：点击将此条目添加中列表中。

 **注意：**

- ◇ 网关 IP 必须是与 WAN 或 LAN 属于同一个网段。
- ◇ 目的 IP 地址如果是一台主机 IP 地址，则子网掩码为 255.255.255.255。
- ◇ 目的 IP 地址如果为 IP 网段，则须与子网掩码匹配。例如，如果目的 IP 为 10.0.0.0，则子网掩码为 255.0.0.0；如果目的 IP 为 10.1.2.0，子网掩码为 255.255.255.0。

4.13 动态 DNS

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

动态DNS

通过动态DNS功能，您可以快速使用您注册的域名来获得路由器WAN口的IP地址，免去记录IP地址的烦恼。本功能一般结合虚拟服务器来使用。

开启动态DNS

服务提供商: 3322.org 注册去

用户名:

密码:

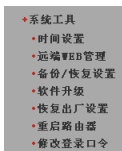
域名信息: (选项)

连接状态: 未连接

- 开启动态 DNS：选择后启用此功能。
- 服务提供商：选择提供 DNS 的服务提供商，Dyndns.org、88ip.cn、freedns.afraid.org、zoneedit.com、no-ip.com、3322.org。
- 用户名：在 DDNS 服务器上注册的用户名。
- 密码：在 DDNS 服务器上注册的密码。
- 域名信息：当前从 DDNS 服务器获得的域名，也可手动输入。
- 连接状态：当前从 DDNS 服务器的连接状态。

4.14 系统工具

在“系统工具”菜单下面，共有“时间设置”、“远程 WEB 管理”、“备份/恢复设置”、“软件升级”、“恢复出厂设置”、“重启路由器”“修改登录口令”七个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。



4.14.1 时间设置

时间设置

本页设置路由器的系统时间，您可以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，当您下次开机连上Internet后，路由器将会自动获取GMT时间。您必须先到此页设置时间并连上Internet获取GMT时间后，其他功能（如防火墙）中的时间限定才能生效。

启用网络校时 校时周期:

时区:

(注意：仅在连上互联网后才能获取GMT时间。)

请输入日期与时间:

年 月 日 时 分 秒

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

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

4.14.2 远端 WEB 管理

通常来讲，只有局域网内的用户才能管理路由器。假如有特殊需要，这个功能将使您能在远程管理路由器。

远端WEB管理

远端WEB管理可允许指定的用户通过Internet来访问到本路由器的WEB管理界面。本功能一般用于远程技术支持。

启用

IP 地址

端口

 **注意:**

- ◇ 路由器默认的远程管理可以根据需求进行修改，您必须用“IP 地址（此 IP 地址为路由器 WAN 口 IP 地址）：端口”的方式（例如 http://192.168.1.2:8080）才能登录路由器执行远程管理。
- ◇ 路由器默认的远端 WEB 管理 IP 地址为 0.0.0.0，当启用时，广域网中所有计算机都能登录路由器执行远端 WEB 管理，如果您改变了默认的 IP 地址（例如改为 58.60.111.221），则广域网中只有具有指定 IP 地址（例如 58.60.111.221）的计算机才能登录到路由器管理页面。

4.14.3 备份/恢复设置

在这里您可以备份当前或恢复以前的路由器设置。

备份/恢复设置

您可以备份/恢复路由器的当前设置

需选择你要保存配置参数的文件目录:

选择你想要导入的配置文件:

备份/恢复设置步骤:

- 单击“备份”，便出现导出配置页面，请指定保存配置文件的路径！选择确定可以在指定目录生成一个系统配置的备份文件。
- 同样道理，单击浏览，我们只需要选择正确的上传的系统配置文件点击恢复，重新启动路由器后将可以恢复到以前的系统配置。

4.14.4 软件升级

通过升级本路由器的软件，您将获得更加稳定的路由器版本及增值的路由功能。

软件升级

通过升级本路由器的软件，您将获得新的功能。


选择固件文件:

当前系统版本: 1.0.0.0; 发布日期: Apr 27 2009

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

软件升级步骤:

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

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

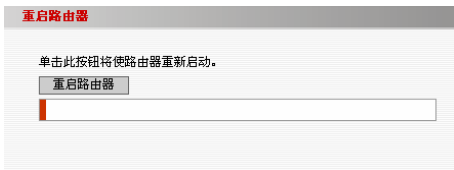
4.14.5 恢复出厂设置



单击“恢复出厂设置”按钮，将使路由器的所有设置恢复到出厂时的默认状态。其中：

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

4.14.6 重启路由器



点击“重启路由器”按钮，将使一些需要重新启动路由才能生效的设置生效。路由器在重启前，会自动断掉网络连接。


4.14.7 修改登录口令

修改登录口令

本页修改系统管理员的用户名及口令。

原用户名	<input type="text" value="admin"/>
原口令	<input type="password" value="•••••"/>
新用户名	<input type="text"/>
新口令	<input type="password" value="•••••"/>
确认新口令	<input type="password" value="•••••"/>

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

 **注意：**出于安全考虑，我们强烈推荐您改变初始系统员用户名和密码。

4.15 系统日志

在“系统日志”菜单下面，共有“日志查看”、“邮件配置”两个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

- + 系统日志
 - 日志查看
 - 邮件配置

4.15.1 日志设置

在系统日志里，您可以查看系统启动出现的各种情况，也可以查看有无网络攻击发生。

- 清除日志：点击清除系统日志。
- 刷新：刷新当前系统日志

日志查看

索引	日志内容		
1	2000-01-01 00:00:07	system	系统初始化完成
2	2009-05-07 13:53:29	system	时间同步成功

4.15.2 邮件配置

在路由器默认的情况下，当系统日志满 256 条后，旧的记录将会被自动清除。为了更完整的了解路由器的运行状态，邮件管理功能将把上网记录以邮件的形式发送到指定的邮箱。

邮件配置

启用邮件管理功能

接收邮件地址：

SMTP服务器地址：

发送邮件地址：

电子邮件用户名：

电子邮件密码：

邮件发送间隔： 分钟 (范围：30-1440分钟)

记录触发间隔： 条 (范围：10-256条)

- 启用邮件管理功能：选择后启用此功能。
- 接收邮件地址：在此输入接收邮件的邮箱地址。例如：
test@sina.com.cn
- SMTP 服务器地址：在此输入发送邮件有效的 SMTP 服务器地址，如不清楚自己使用邮件的 SMTP 服务器地址，可以到注册邮箱的帮助页面找到相关内容。

例如：smtp.sina.com.cn, smtp.163.com 等。

- 发送邮件地址：在此输入发送邮件的邮箱地址。
- 电子邮件用户名：在此输入发送邮箱的注册用户名。
- 电子邮箱密码：在此输入发送邮箱的注册密码。
- 邮件发送间隔：设置发送邮件的时间间隔，时间间隔为 30~1440 分钟。

例如：设置为 30 分钟，则表示每隔 30 分钟路由器都会把记录以邮件的形式，从“发送邮件地址”发送到设置的“接收邮件地址”。然后页面记录将全部清除，重新记录访问信息。

- 记录触发间隔：设置触发发送邮件的记录数。触发记录数目范围为 10~256。

例如：设置为 10，则表示记录超过 10 条时，就以邮件发邮件方式，从“发送邮件地址”发送到设置的“接收邮件地址”，然后页面记录将全部清除，重新记录访问信息。

4.16 退出登录

各项设置完成后请从“退出登录”安全的完全退出路由器的 WEB 管理页面。

附录一 TCP/IP 地址设置方法(以 Windows XP 为例)

依次点击“开始—控制面板”，打开控制面板。（如图 1）。



图 1

单击“网络和 Internet 连接”，进入网络和 Internet 连接页面(如图 2)。



图 2

单击“网络连接”，进入网络连接页面（如图 3）。

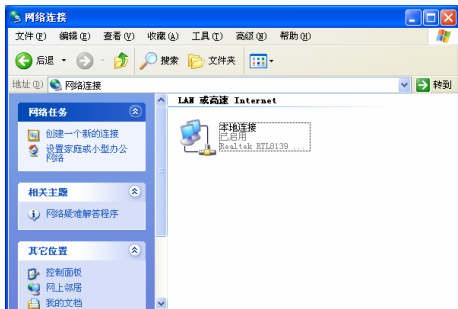


图 3

选择“本地连接”，点击鼠标右键，选择“属性”（如图 4）。



图 4

在弹出的对话框里，先选择“Internet 协议 (TCP/IP)”，再用鼠标点击“属性”按钮（如图 5）。

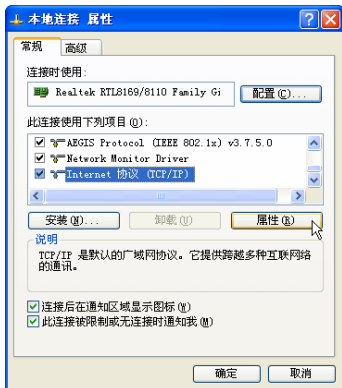


图 5

方法 1: 选择“自动获得 IP 地址”“自动获得 DNS 服务器地址” 点击“确定”（如图 6）。

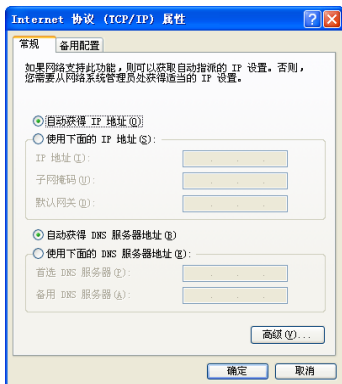


图 6

方法 2: 选择“使用下面的 IP 地址”, 填写 IP 地址为: 192.168.0.xxx. (xxx 为 2~254 中除了 1 的任意数值), 子网掩码为 255.255.255.0, 网关 192.168.0.1, 首选 DNS 服务器: 192.168.0.1, 如果您知道当地 DNS 服务器地址可直接输入 (如图 7)。

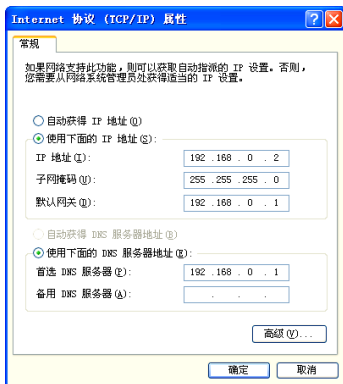


图 7

点击“确定”回到“本地连接 属性”对话框。

再点击“确定”退出设置界面。

在这一节中, 我们介绍了如何为您的个人计算机配置 TCP/IP 协议。请您确认已经在您的计算机中成功安装了网卡, 如果没有, 请参阅网卡的 用户手册, 正确安装网卡硬件及驱动程序。

附录二：常用命令介绍

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