IP-COM®

说明书

450M企业无线上网行为管理路由器

www.ip-com.com.cn

X5

V1.0

版权声明

目录

第一章　　产品介绍

1.1　产品简介

IP-COM 推出 450M 无线覆盖王路由器 X5，其采用 IEEE802.11N 无线技术，外置三根 5dBi 可拆卸高增益全向天线，无线传输速率高达 450Mbps，提供 4 个千兆 WAN 口、1 个千兆 LAN 口和 2 个 USB 2.0 标准接口。带机数量为有线 60 台、无线 20 台，具备 VPN、智能带宽控制、ARP 防护和攻击防护、访客 网络、电子公告、即插即用、邮件密送、地址伪装、多 WAN 口负载均衡等丰富的软件功能特性，还支持 USB 存储共享和打印。适用于企业网络应用环境，让其组建高性价比、高安全、易管控的无线网络。

主要特性：

- 支持 IEEE802.11n, IEEE802.11g, IEEE 802.11b
- 提供 4 个千兆 WAN 口，1 个千兆 LAN 口，LAN、WAN 口数量可根据实际情况修改
- 无线传输速率高达 450Mbps
- 二个 USB 接口，提供网络存储，打印
- 支持 WEP、WPA-PSK、WPA2-PSK 多种加密与安全机制,可有效防止蹭网
- 支持访客网络
- 支持隐藏无线 SSID 功能和基于 MAC 地址的访问控制
- 支持 WMM，让您的语音、视频更流畅
- 支持 WDS 无线网络扩展
- 提供高级策略路由与负载均衡
- 支持端口镜像功能
- 支持智能带宽管理，保证带宽稳定性,使网络资源得到合理的利用
- 支持 PPTP、L2TP、IPSEC VPN 技术，有效保证安全接入和数据传输
- 支持 IP-MAC 地址绑定功能，有效防止 ARP 攻击、欺骗和非授权用户接入
- 支持基于协议端口、MAC、URL 及多种特殊应用访问控制
- 支持虚拟服务器、DMZ 主机
- 内建 DHCP 服务器，同时可进行静态地址分配
- 支持通用即插即用（UPnP），真正实现 MSN 语音视频通讯
- 高效无线覆盖，精确控制上网时间、访问的域名和上网 PC 的 MAC 地址
- 支持 QQ、MSN、飞信、阿里旺旺等软件过滤，另外可以设置例外 QQ 通过
- 支持动态域名解析 DDNS 功能
- 支持系统监控功能，能够实时监控 UDP/TCP 等数据包上下流量，统计 IP 实时数据包流量、监控最大连接数
- 支持实时监控 CPU 和系统内存，易于维护
- 高达 600MHz 的 CPU 处理，超强 NAT 转发性能，支持更多的用户使用
- 支持远程 Web 管理，全中文配置界面

1.2 包装清单

在包装盒完整的情况下，开启包装盒。盒内应包含以下各项：

- 一台 X5 企业无线无线覆盖王路由器
- 三根外置可拆卸 5dBi 高增益全向天线
- 一条电源线
- 一本说明书
- 一张保修卡
- 一条网线
- 四个脚垫

注意：如果发现有任何配件的损坏或遗漏，请及时与当地经销商联系。

1.3 硬件描述

◆ 前面板介绍

图：X5 前面板示意图

Reset：复位按钮。按住此按钮 7 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。

指示灯：

指示灯	描 述	功 能
POWER	电源指示灯	常亮表示电源供电正常
SYSTEM	系统状态指示灯	闪烁表示系统正常 常亮或不亮表示系统异常
WiFi	无线状态指示灯	常亮表示无线功能开启，闪烁表示正在进行无线数据传输

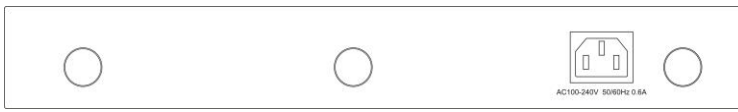
Link/Act	广域网和局域网状态指示灯	黄色常亮表示相应端口连接速率为 100Mbps 或 10Mbps 绿色常亮表示相应端口连接速率为 1000Mbps 闪烁表示相应端口正在进行数据传输 熄灭表示未连接
USB	USB 指示灯	常亮表示工作正常

USB：2 个 USB 2.0 标准接口。用于 USB 接口外挂存储器，网络共享存储内容和 USB 打印。

WAN：4 个千兆广域网端口（RJ-45）。可根据需要更改 WAN 口数。连接 ADSL Modem/Cable Modem 或以太网。

LAN：1 个千兆局域网端口（RJ-45）。可根据需要更改 LAN 口数。连接至计算机的以太网网卡，也可级联至集线器和交换机。

◆ 后面板介绍



1.4 系统需求

最低系统需求如下：

- 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 ADSL/Cable Modem/以太网接入)

1.5 安装环境要求

- 请不要将本产品放置在潮湿、粉尘的环境中；
- 请不要将本产品置于阳光下暴晒或置于其他热源附近。

推荐使用环境：

工作温度：0℃到 40℃；
存储温度：-40℃到 70℃；
工作温度：10%到 90%不凝结；

存储温度：5%到 90%不凝结。

提示：为了您的安全，安装时请关闭电源，拔掉电源插头，保持双手干燥！

第二章　　快速安装指南

2.1　硬件安装步骤

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

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

2.2　配置计算机网络设置

2.2.1　打开路由器电源，等待片刻，当路由器前面板的 system 灯匀速闪烁以后，表示路由器已经进入工作状态，可以开始配置了。

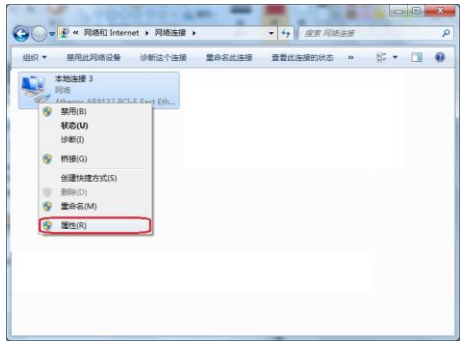
2.2.2　首先需要将您的电脑与路由器的 LAN 口用网线连接起来，正确配置计算机的网络设置，并加载 TCP/IP 协议。

2.2.3　下面将以 Win7 为例介绍具体的设置方法：

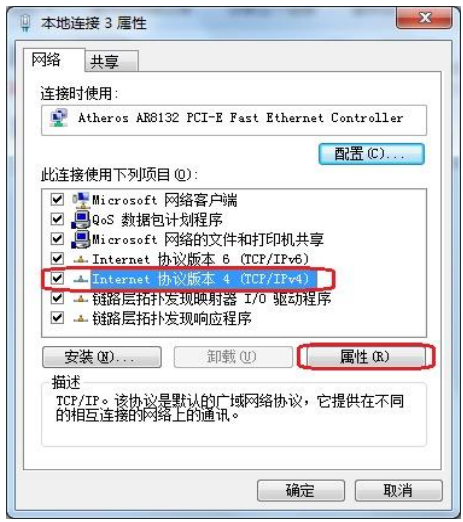
- 在您正在使用的桌面上，用右键单击“网络”，在弹出的菜单中选择“属性”；

- 在随后打开的窗口里，点击“更改适配器设置”；

- 用鼠标右键点击“本地连接”，选择“属性”；

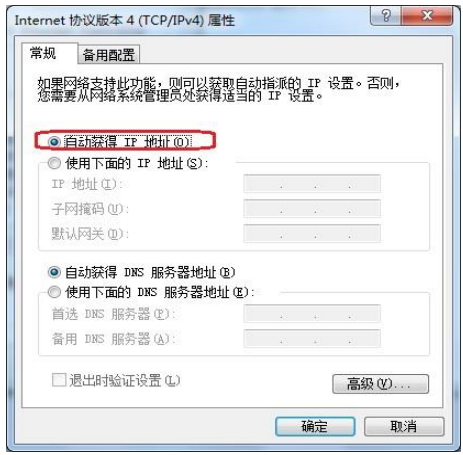


➢ 在弹出的对话框里，先选择“Internet 协议版本 4（TCP/IPv4）”，再用鼠标点击“属性”按钮；

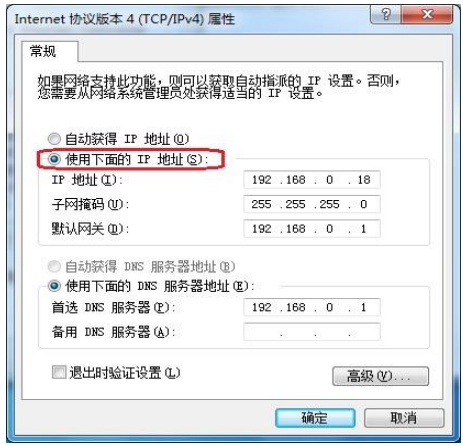


➢ 在随后打开的窗口里，您可以选择“自动获得 IP 地址（O）”或者是“使用下面的 IP 地址（S）”；

✓ “自动获得 IP 地址（O）”如图：



✓ “使用下面的 IP 地址（S）”



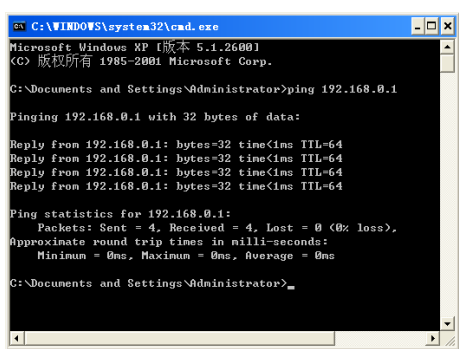
设置您计算机的 IP 地址为 192.168.0.xxx(xxx 为 2~254)，子网掩码：255.255.255.0，网关：192.168.0.1，DNS 服务器：您可以填写您当地的 DNS 服务器地址（可咨询您当地的网络服务提供商）也可以由路由器作为 DNS 代理服务器。设置完成后点击“确定”提交设置，再在本地连接“属性”中点击“确定”保存设置。

- 点击“确定”回到“本地连接 属性”对话框。再点击“确定”退出设置界面。

2.2.4 使用 Ping 命令检查您的计算机和路由器之间是否连通，具体步骤如下：

- 选择“开始”，在“搜索程序和文件”对话框中输入“cmd”然后回车。

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

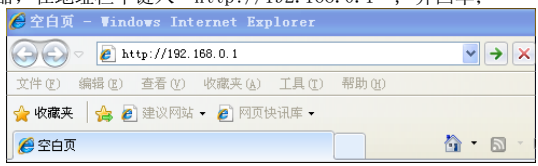


2.3 配置路由器设置

2.3.1 登录设备

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。具体步骤如下：

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

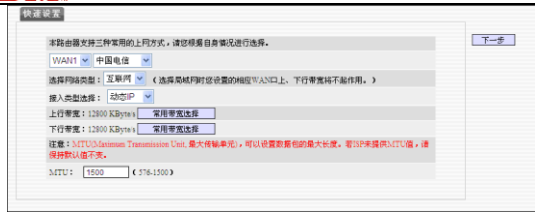


连接建立后，您会看到登录界面。您需要以系统管理员的身份登录，输入用户名和密码（用户名和密码出厂设置均为“admin”）。

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，点击“设置向导”→“快速设置”，进入上网方式选择画面。



2.3.2 配置上网

本路由器支持最常见的三种上网方式，默认接入方式为动态 IP 接入：

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

⚠注意：

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

  上行带宽 512Kbps = 64KByte/s

  下行带宽 2Mbps = 2048Kbps = 256KByte/s。

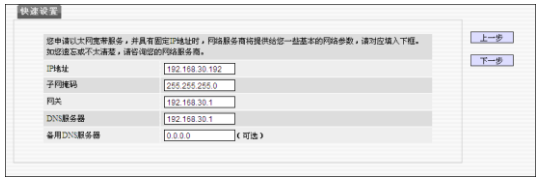
根据自身情况选择需要接入的 WAN 口并选择正确的接入方式，然后填写正确的上下行带宽，最后单击“下一步”填写上网所需的基本网络参数。

2.3.1.1 动态 IP

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

2.3.1.2 静态 IP

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



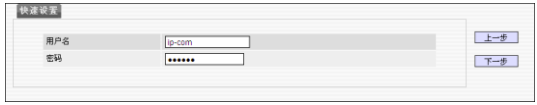
- IP 地址：本路由器对广域网的 IP 地址，即 ISP（网络服务商）提供给您的 IP 地址，不清楚可以向 ISP（网络服务商）询问。
- 子网掩码：本路由器对广域网的子网掩码，即 ISP（网络服务商）提供给您的子网掩码，不清楚可以向 ISP（网络服务商）询问。
- 网关：填入 ISP（网络服务商）提供给您的网关，不清楚可以向 ISP（网络服务商）询问。
- DNS 服务器：填入 ISP（网络服务商）提供给您的 DNS 服务器，不清楚可以向 ISP（网络服务商）询问。
- 备用 DNS 服务器：可选，如果 ISP（网络服务商）提供两个 DNS 服务器地址，您可以将另一个 DNS 服务器地址填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

⚠注意：

当路由器 WAN 口指定的 IP 地址和路由器 LAN 口 IP 地址在同一网段时，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

2.3.1.3 PPPoE

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



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

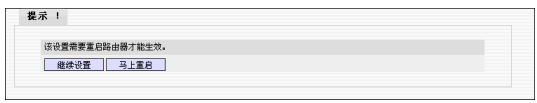
2.3.3 无线配置

在填写完上网的基本网络参数后，点击“下一步”您将来到无线网络基本参数的设置页面。

如果不需要修改无线设置，直接点击下一步。（无线设置可以参考 3.4 节无线基本设置部分）

在填写完无线网络基本参数后，您将来到设置向导的完成画面，点击“保存”完成设置。

点击“保存”按钮后，系统提示是否马上重新启动路由器。



当路由器重新启动后，可以到“运行状态”中“WAN 状态”中查看配置信息。


WAN状态
LAN状态
无线状态
系统信息
WAN1状态 已启用，已连接
连接方式 动态 IP
WAN IP 192.168.30.192
子网掩码 255.255.255.0
网关 192.168.30.1
域名服务器 192.168.30.1
MAC 地址 A8:AA:35:00:01:6B
WAN口流量 下行：0.00KB 上行：0.00KB
连接时间 01:08:39
更新
释放
WAN2状态 已启用，网线未插好
连接方式 动态 IP
WAN IP 0.0.0.0
子网掩码 0.0.0.0
网关 0.0.0.0
域名服务器 0.0.0.0
MAC 地址 A8:AA:35:00:02:6C
WAN口流量 下行：0.00KB 上行：0.00KB
连接时间 00:00:00
更新
释放
WAN3状态 未启用
连接方式 PPPoE
WAN IP 0.0.0.0
子网掩码 0.0.0.0
网关 0.0.0.0
域名服务器 0.0.0.0
MAC 地址 00:00:00:00:00:00
WAN口流量 下行：0.00KB 上行：0.00KB
连接时间 0
连接
断开
WAN4状态 未启用
连接方式 PPPoE
WAN IP 0.0.0.0
子网掩码 0.0.0.0
网关 0.0.0.0
域名服务器 0.0.0.0
MAC 地址 00:00:00:00:00:00
WAN口流量 下行：0.00 KB 上行：0.00 KB
连接时间 0
连接
断开

第三章　　路由器详细设置

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11个菜单栏介绍路由器的各个功能：

- 系统状态
- 设置向导
- 网络参数
- 无线设置
- 行为管理
- 安全设置
- 高级设置
- USB应用
- VPN设置
- 系统监控
- 系统工具

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

3.1　　系统状态

WAN状态

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

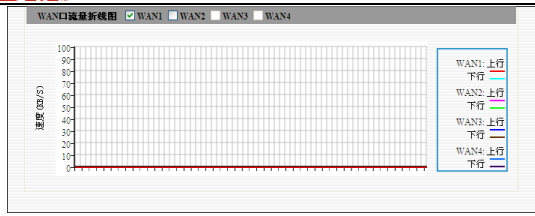
- WAN 状态：显示 WAN 口的连接状态。

  已启用，网线未插好：表示 WAN 口未接网线；

  已启用，连接中：表示 WAN 口已接通，正在获取 IP 地址；

  已启用，已连接：表示路由器与 ISP（网络服务商）已正常接通；
- 连接方式：表示当前您选的接入方式。
- WAN IP：从 ISP（网络服务商）获取的 IP 地址。
- 子网掩码：从 ISP（网络服务商）获取的子网掩码。
- 网关：从 ISP（网络服务商）获取的网关。
- 域名服务器：从 ISP（网络服务商）获取的主 DNS。
- MAC 地址：显示 WAN 口的 MAC 地址。
- 连接时间：表示路由器与 ISP（网络服务商）连接的时间（动态 IP 和 PPPoE 接入方式）

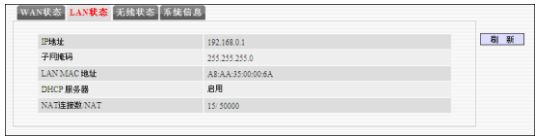
WAN 口流量折线图



- WAN 口流量：表示路由器当前 WAN 口的实时速率，单位为 KB/s。
- 您可以根据实际情况勾选 WAN 口查看各个 WAN 口的实时速率

LAN 状态

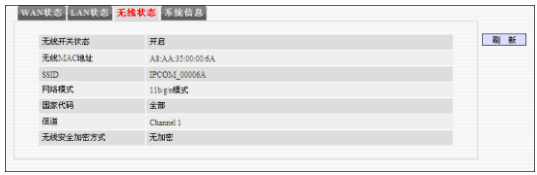
此处显示当前路由器的 IP 地址、子网掩码、LAN MAC 地址、DHCP 服务器是否启用和 NAT 连接数/NAT。



- 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 连接数/NAT：已使用的 NAT 数/路由器的 NAT 总连接数；

无线状态

此处显示路由器的无线开关状态、无线 MAC 地址、SSID、网络模式、国家代码、信道和无线安全加密方式。

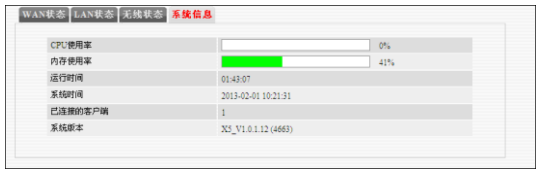


- 无线开关状态：路由器无线的运行状态，开启或关闭；

- 无线 MAC 地址：路由器无线的 MAC 地址；
- SSID：路由器使用的网络标识符；
- 网络模式：路由器无线工作的模式；
- 国家代码：路由器无线的国家代码；
- 信道：路由器无线的当前工作信道；
- 无线安全加密方式：路由器无线的加密方式。

系统信息

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



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

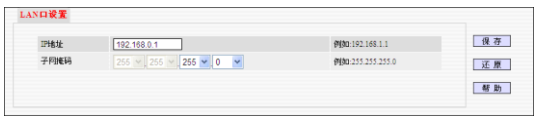
3.2 设置向导

快速设置过程，请参考第 2.3 节。

3.3 网络参数

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

3.3.1 LAN 口设置



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

⚠注意：

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

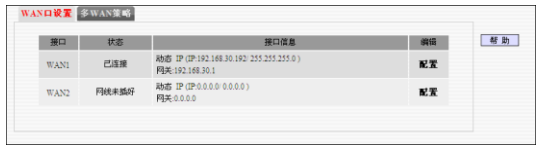
路由器 WAN 口获取或指定的 IP 地址和路由器 LAN 口 IP 地址在同一网段，会导致路由器无法正常工作。紧急时，请使用面板上的复位键进行复位。

3.3.2 WAN 口设置

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

WAN 口设置

本界面显示所有 WAN 口的接入状态和接口参数。



选择您要设置的 WAN 口，点击“配置”，即可进入 WAN 口参数设置界面。每个 WAN 口都支持三种连接方式，静态 IP，动态 IP，PPPOE 拨号。

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

- ISP： WAN 口连接线路的 ISP 名称。
- IP 地址：申请的线路的广域网 IP 地址，由网络服务商提供，可以向网络服务商询问获得。
- 子网掩码：当前 IP 所对应的子网掩码，由网络服务商提供，可以向网络服务商询问获得。
- 缺省网关：当前 IP 所对应的网关，由网络服务商提供，可以向网络服务商询问获得。
- 主 DNS 服务器/备用 DNS 服务器：填入网络服务商提供的 DNS 服务器 IP 地址，可以向网络服务商询问获得。
- 线路带宽：申请的 WAN1 口静态线路的带宽，可以向网络服务商询问获得。

- MTU 设置：MTU（最大传输单元），系统默认使用 1500 字节。注意：通常情况下这个参数不用设置，不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

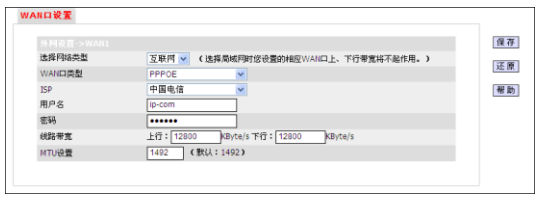
2）动态 IP：如果您的上网方式为动态 IP，即您可以自动从网络服务商获取 IP 地址。

- ISP： WAN 口连接线路的 ISP 名称。
- 线路带宽：申请的 WAN 口动态 IP 线路的带宽，可以向网络服务商询问获得。
- MTU 设置：最大传输单元设置，系统默认使用 1500 字节。

⚠注意：

通常情况下，MTU 设置不要更改，不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

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



- ISP： WAN 口连接线路的 ISP 名称。
- 用户名：填入网络服务商提供的 PPPOE 账号，可以向网络服务商询问获得。
- 密码：填入网络服务商提供的 PPPOE 密码，可以向网络服务商询问获得。
- 线路带宽：申请的账号带宽，可以向网络服务商询问。
- MTU 设置：MTU（最大传输单元），系统默认使用 1492 字节。

⚠注意：

通常情况下，MTU 设置不要更改，不恰当的 MTU 设置可能导致网络性能变差甚至无法使用。

多 WAN 策略

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

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

  注意：系统默认的工作模式为智能负载均衡。
- 按比例负载均衡：用户根据自己的实际需要，将流量按比例分配到对应 WAN 口，以达到带宽的合理利用。在此工作模式下，您可以根据实际情况定义需要的负载设置。
- ISP 策略路由：您可以根据实际情况选择开启或关闭 ISP 策略路由。
- 用户自定义策略：用户根据自己的实际需要，针对特定的源地址和目的端口指定特定的 WAN 口。在此工作模式下，您可以根据实际情况定义需要的策略模式。

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

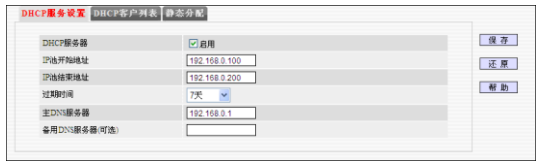
3.3.3 DHCP 服务器

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

DHCP 服务设置

TCP/IP 协议设置包括 IP 地址、子网掩码、网关、以及 DNS 服务器等。为您局域网中所

有的计算机正确配置 TCP/IP 协议并不是一件容易的事，幸运的是，DHCP 服务器提供了这种功能。如果您使用本路由器的 DHCP 服务器功能的话，您可以让 DHCP 服务器自动替您配置局域网中各计算机的 TCP/IP 协议。



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

注意：

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

DHCP 客户列表

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

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

3.3.4 静态分配

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

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

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

3.3.5 访客网络 DHCP 服务器

在“访客网络 DHCP 服务器”菜单下面，有“访客网络 DHCP 服务设置”和“访客网络 DHCP 客户列表”二个子项。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。

访客网络 DHCP 服务设置

访客网络 DHCP 服务器默认为关闭状态，当在无线设置页面开启访客网络后将自动启用，访客网络 DHCP 服务器将自动替您配置访客网络中各计算机的 TCP/IP 协议（TCP/IP 协议设置包括 IP 地址、子网掩码、网关以及 DNS 服务器等），而免去手动设置 TCP/IP 相关参数。

- DHCP 服务器：默认为关闭状态，当开启访客网络后将自动设置为“启用”状态。
- IP 池开始地址：DHCP 服务器所自动分配的 IP 的起始地址。
- IP 池结束地址：DHCP 服务器所自动分配的 IP 的结束地址。
- 过期时间：客户端获得 IP 地址的使用时间。
- 主 DNS 服务器：分配的 DNS 服务器地址。
- 备用 DNS 服务器：分配的 DNS 服务器地址（可不填）。

⚠注意：

为了使用本路由器的访客网络 DHCP 服务器功能，访客网络计算机的 TCP/IP 协议必须设置为“自动获得 IP 地址”。

访客网络 DHCP 客户列表

该客户列表显示了所有访客网络通过 DHCP 获得 IP 的主机名、IP 地址、MAC 地址、租约时间。

- 主机名：访客网络客户端的主机名。
- IP 地址：访客网络客户端申请到的 IP 地址。
- MAC 地址：访客网络申请到该 IP 地址的计算机的 MAC 地址。

租约时间：访客网络主机通过 DHCP 所获得的 IP 的使用时间。

3.3.6 访问控制

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

LAN 口访问控制

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

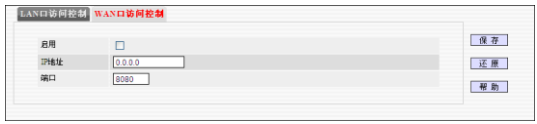
⚠注意：

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

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

WAN 口访问控制

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



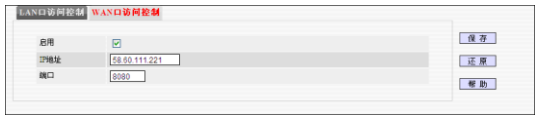
- 启用：开启 WAN 口访问控制路由器功能。
- IP 地址：输入访问控制路由器 WAN 口的 IP 地址。

- 端口：默认端口为 8080，输入您访问路由器 WEB 界面的端口号。

注意：

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

例如：路由器的 WAN 口的 IP 地址为默认的 58.251.88.90，您仅允许 IP 地址为 58.60.111.221 的客户机，通过端口 8080 访问控制路由器 WEB 界面，则需要设置如下参数，且路由器的访问地址也更改为：http:// 58.251.88.90:8080

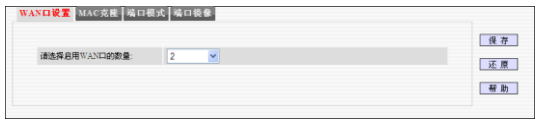


3.3.7 端口参数设置

在“端口参数设置”菜单下面，有“WAN 口设置”、“MAC 克隆”、“端口模式”、“端口镜像”四个子项，单击某个子项，您即可进行相应的功能设置。

WAN 口设置

本页可以修改路由器 WAN 口数量。默认情况下，路由器开启 2 个 WAN 口，您可以根据实际情况进行修改，未开启的 WANN 端口作为 LAN 口使用。



MAC 克隆

本页设置路由器各个接口的 MAC 地址。

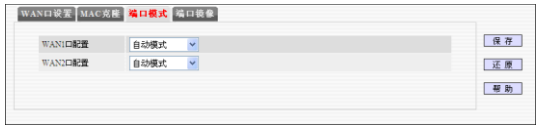
- LAN 口 MAC 地址：显示路由器的 LAN 口 MAC 地址，可手动输入 MAC 地址。
- WAN 口 MAC 地址：显示路由器的 WAN 口 MAC 地址，可手动输入 MAC 地址。
- 恢复出厂 MAC：把路由器对广域网的 MAC 地址值还原到出厂默认值。
- 克隆 MAC 地址：设置计算机 MAC 地址为路由器对广域网的地址。

⚠注意：

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

端口模式

本页设置各 WAN 口工作模式。



您可以按照需要分别设置各 WAN 口的端口模式：自动模式、10M 半/全双工、100M 半/全双工、1000M 全双工。

⚠注意：

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

端口镜像

为了方便对一个或多个网络端口的流量进行分析，可以通过端口镜像功能把一个或多个端口的数据转发到某一个端口来实现对网络的监听。

- 监控设置：选择开启或禁用端口镜像功能。
- 监控端口：对应于路由器的物理端口，监听被监控端口的数据流。
- 被监控端口：对应于路由器的物理端口，采用复选方式选择或不选。当选择某端口后，该端口的数据将被转发至监控端口。其中端口 2 对应 LAN4，端口 3 对应 LAN3，端口 4 对应 LAN2，LAN 口对应 LAN1。当端口 2、3、4 为 WAN 口时，不能被监控。

例如：在 LAN 口监听 LAN2、LAN3 的数据流，您只需做如下的配置，点击保存即可。

3.4 无线设置

在“无线设置”菜单下面，共有“基本设置”、“访客网络”、“无线安全”、“高级设置”、“访问过滤”、“WDS 设置”和“连接状态”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。

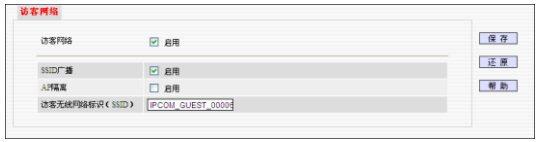
3.4.1 基本设置

无线基本设置用来管理您的无线网络，可以更改国家区域代码、无线网络名称、无线工作模式、信道等相关参数。

- 无线网络：“勾选”后，启用无线功能，如果您不想使用无线，可以取消选择，所有与无线相关的功能将禁止；
- 无线发射功率：默认为中，根据实际情况分高、中、低三种情况选择。
- SSID 广播： 默认为“开启”。选择“关闭”禁止路由器广播 SSID，无线客户端将无法扫描到路由器的 SSID。选择“关闭”后，客户端必须知道路由器的 SSID 才能与路由器进行通讯。
- 无线网络标识（SSID）：无线信号的网络名称，您可以根据个人喜好进行修改。
- 模式：根据无线客户端类型选择其中一种模式。默认为 11b/g/n 混合模式。
- 信道：路由器当前使用的信道，可以从下拉列表中选择其它有效的工作信道。
- 信道带宽：选择信道带宽以提高无线性能。当无线网络中同时有 11b/g 和 11n 客户端时，可以选择宽带为 20/40M 的 802.11n 模式；无线网络中只有非 11n 客户端时，可以选择带宽为 20M 模式。如果无线网络模式为 11n 模式，请选择 20/40M 频带，以提高其吞吐量。
- 扩展信道：用于确定 11n 模式时本网络工作的频率段。
- WMM-Capable：开启时可以提高无线多媒体数据传输性能（如：视频或在线播放）。
- ASPD Capable：启用或禁用自动省电模式。

3.4.2 访客网络

您的访客可以通过该无线网络标识（SSID）连接到您的网络。通过访客网络连接的无线客户端，只能访问互联网或该 SSID 下其他无线客户端，不允许访问路由器管理界面和主 SSID 上的客户端以及 LAN 口下的客户端或者设备。

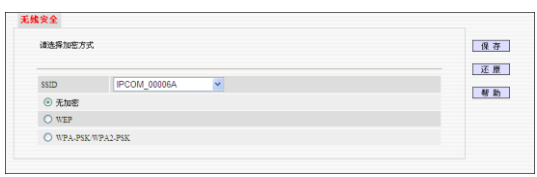


- 访客网络：启用或禁用此功能；
- SSID 广播：默认为“开启”。选择“关闭”，将禁止路由器广播访客 SSID，无线客户端将无法扫描到该 SSID。选择“关闭”后，客户端必须知道该 SSID 才能与路由器进行通讯；
- AP 隔离：启用 AP 隔离后，同时连接到该网络（此 SSID）的客户端之间将无法相互访问；
- 访客无线网络标识（SSID）：无线网络中所有设备共享的网络名称，您可以根据个人喜好进行修改。

3.4.3 无线安全

通过无线加密功能，可以防止他人未经同意私自连入您的无线网络，占用网络资源，同时也可以防止非法用户窃听或侵入无线网络。

加密方式分为主网络与访客网络加密方式，点击 SSID 下拉列表可以选择主网络或访客网络，如您想对路由器的主网络进行加密，请在 SSID 下拉框里面选择主网络 SSID 进行加密设置。



加密类型共分为“无加密”、“WEP”、“WPA-PSK”、“WPA2-PSK”共四种加密类型。

1、无加密

无线连接上路由器时不需要输入密码。

2、 WEP

有线等效保密（WEP）协议是对在两台设备间无线传输的数据进行加密的方式，用以防止非法用户窃听或侵入无线网络。WEP 安全技术是基于 RC4 的数据加密技术。为无线网络通信提供数据机密性、完整性及认证功能。

- 认证类型：从列表中选择相应的认证类型，开放系统或共享密钥。
- WEP 密钥格式：从列表中选择相应的 WEP 密钥格式，十六进制或 ASCII 码。
- 密钥选择： 可以从预先设置好的 4 组密钥中选择一个作为当前有效密钥。

3、WPA-PSK

WPA 是一种基于标准的可互操作的 WLAN 安全性增强解决方案，可大大增强现有无线局域网系统的数据保护和访问控制水平。WPA 源于 IEEE802.11i 标准并将与之保持前向兼容。WPA 可保证 WLAN 用户的数据受到保护，并且只有授权的网络用户才可以访问 WLAN 网络。WPA 采用比 WEP 更强的加密算法。

- 认证类型：可以选择 WPA-PSK 或 WPA2-PSK，此时选择 WPA-PSK。
- 加密算法：可以选择 AES（高级加密标准）模式、TKIP（时间密钥完整性协议）+AES 模式。
- PSK 密码：请输入您想使用的加密字符串，密钥字符最短为 8 个字符，最长为 63 个 ASCII 码字符或 64 个 16 进制字符。
- 密钥更新周期：为您设定的密钥生成一个有效期。

4、WPA2-PSK

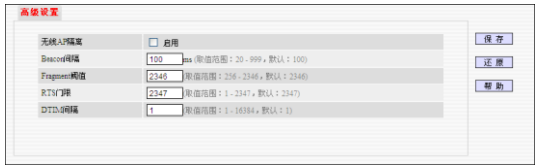
WPA2 能提供比 WEP 或 WPA 更佳的安全性。

- 认证类型：可以选择 WPA-PSK 或 WPA2-PSK，此时选择 WPA2-PSK。
- 加密算法：选择数据加密类型，支持 AES（高级加密标准）模式、TKIP（时间密钥完整性协议）+AES 模式。

- PSK 密码：请输入您想使用的加密字符串，密钥字符最短为 8 个字符，最长为 63 个 ASCII 码字符或 64 个 16 进制字符。
- 密钥更新周期：为您设定的密钥生成一个有效期。

3.4.4 高级设置

使用高级设置可以详细地设置无线功能，高级设置包含了无线基本设置之外的设置项，包括无线 AP 隔离、Beacon 间隔、Fragment 阈值、RTS 门限和 DTIM 间隔等。



- 无线 AP 隔离:主 SSID 下客户端之间的隔离。
- Beacon 间隔：设置 AP 发送 Beacon 包频率，默认值为 100，建议不要更改默认值。
- Fragment 阈值:设定一个分片阈值,一旦无线数据包超过这个阈值将其分成多个片段，片段的大小和分片阈值，默认值为 2346，建议不要更改默认值。
- RTS 阈值：当数据包的大小超过这个阈值时，使用 RTS/CTS 机制，降低发生冲突的可能性。在存在干扰、长距离客户端接入情况下，可以设置相对较小的 RTS 值，在一般 Soho 办公场所建议不要更改默认值，否则会影响路由器的性能。
- DTIM 间隔，用于通知客户端下一个监听广播和多播信息的窗口。当路由器缓冲了发送到客户端的广播或多播信息，它发送下一个 DTIM 及 DTIM 间隔，唤醒客户端接收这些信息。

3.4.5 访问过滤

访问过滤功能是以 MAC 地址为条件允许或禁止指定的客户端接入到无线网络。

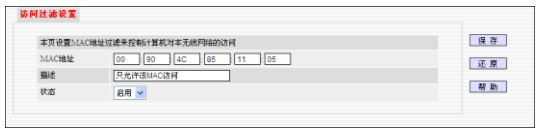
- 启用过滤：不勾选表示不启用访问过滤，勾选表示启用访问过滤。
- 禁止：表示只禁止列表中客户端接入。
- 允许：表示只允许列表中客户端接入。

点击“添加过滤规则”，会出现如下界面：

- MAC 地址：设置为您要允许或禁止无线客户端的 MAC 地址。
- 描述：即为此配置文件定义的简单描述。
- 状态：启用或关闭。

举例：您只允许无线网卡 MAC 地址为 00:90:4C:85:11:05 的计算机接入您的无线网络。

1、点击“添加过滤规则”按钮，在 MAC 地址栏里输入 00:90:4C:85:11:05，描述中输入自定义的标识，状态选择“启用”，保存，如下图



2、页面转跳回过滤设置首页，并且显示刚才添加的规则，选择“允许”，并启用过滤，如下图：

3.4.6 WDS

无线分布式系统（WDS），用来扩大现有无线网络覆盖范围。在 WDS 模式的下拉列表中选择“无线接入点”模式，WDS 状态选择“启用”，将进入如下图设置界面：

- WDS 模式：可以选择无线接入点和无线桥模式。
- WDS 状态：可以选择“启用”和“禁用”。
- 扫描：启用 WDS 功能后点击扫描可以搜索到处于同一信道的无线设备的 SSID 与 BSSID。
- 远端桥 MAC 地址：对端设置的无线 MAC 地址。

举例：本例以两个 X5 做网桥(WDS)。

选择 WDS 模式为无线接入点，再将 WDS 状态选择启用，如图所示：

1．如果知道对端路由器的无线 MAC 地址，则可以直接在 MAC 地址输入框填入对端设备的无线 MAC 地址，然后点击“确定”。

2．也可以通过扫描,搜索到对端无线路由器的信号。

1）点击"扫描"选择扫描到的信号，并点击"连接"按钮，会自动添加相应无线信号的 MAC 地址。

2）MAC 地址添加后再点击“保存”，如图所示

添加成功后，还需要对另一台 X5 按以上步骤进行操作。两台路由器互相填写对方 MAC 地址后即可连接成功。

注意：

1、 **WDS 功能需要两台路由器均支持此功能，而且 SSID、信道、加密方式和密码必须与对端路由器的相同。**

2、 **如果需要对无线客户接入进行安全认证，请在“无线设置->加密方式”中进行设置。设置完成保存后，请重新启动路由器后，才能使 WDS 设备之间正常通讯。**

3、 **WDS 桥接数最好不要超过 3 台**

3.4.7 连接列表

这个页面显示了无线客户端的接入信息和它们的状态，如下图所示：

3.5 行为管理

在“行为管理”菜单下面，共有“组设置”、“端口过滤”、“URL 过滤”、“网址分类过滤”、“协议特征过滤”和“带宽设置”六个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

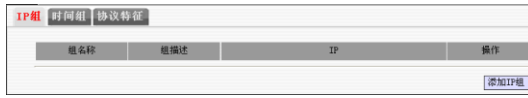
3.5.1 组设置

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

用户组

您可以通过添加 IP 组名称、IP 组描述以及合适的 IP 或者 IP 段来设置 IP 组。设置好

的 IP 组将与无线覆盖王的各个子功能配合使用。



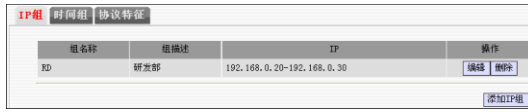
比如公司研发部的 IP 段为：192.168.0.20-192.168.0.30，将研发部配置为一个 IP 组的方法为，点击“添加 IP 组”。

1、 IP 组名称：RD

2、 IP 组描述：添加注释“研发部”。

3、 添加 IP：192.168.0.20-192.168.0.30

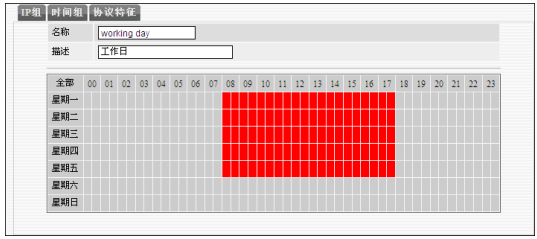
4.点击“添加”并保存后出现如下的界面



时间组

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

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



1、名称：Working day

2、描述:工作日

3、时间段：星期一到星期五的 8：00-18:00

4、点击保存会出现如下界面

协议特征

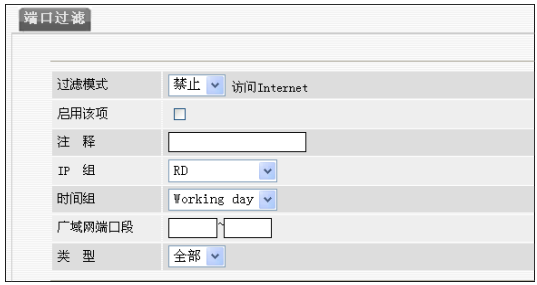
协议特征表中可以查看到每个应用类型所包含的不同应用程序，方便用户了解路由器系统能够自动识别的应用程序。

编号	对象名	备注
1	网络电视	QQLive
2	网络电视	PPLive
3	网络电视	PPStream
4	网络电视	UUSee
5	网络电视	皮皮高清影视
6	网络电视	风行
7	WEB视频	优酷网
8	WEB视频	土豆网
9	WEB视频	百度视频搜索
10	WEB视频	酷6网
11	WEB视频	56网
12	WEB视频	迅雷看看

3.5.2 端口过滤

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

点击“添加过滤规则”，会出现如下界面：

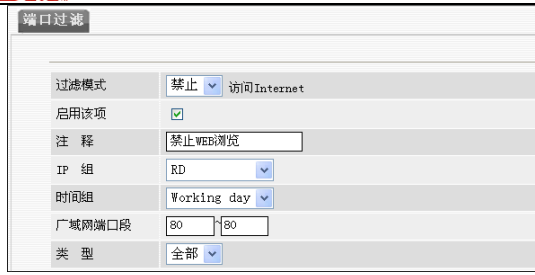


- 过滤模式：更改客户端过滤模式，有“禁止”和“允许”两种选项。

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

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

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

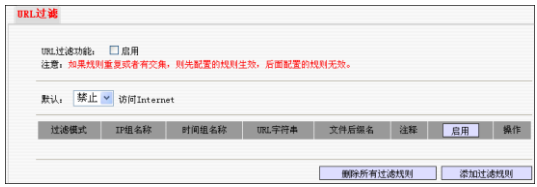


点击保存，出现如下界面

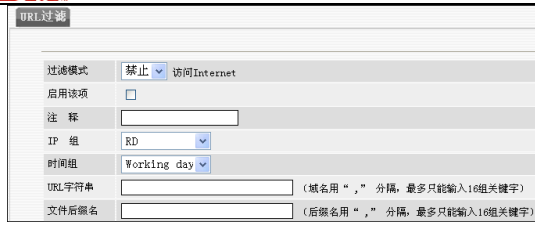
将默认规则设置成“允许”访问 Internet，勾选“启用”端口过滤功能并保存，即可实现。

3.5.3 URL 过滤

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



点击“添加过滤规则”，会出现如下界面：



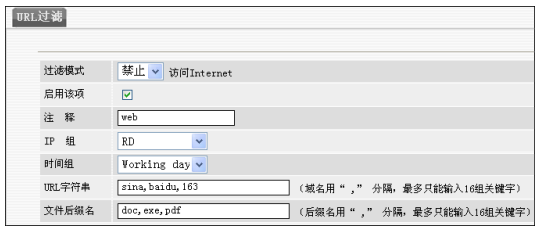
- 过滤模式：更改 URL 过滤的过滤模式，有“禁止”和“允许”两种选项。

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

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

- 注释：即为此配置的简单描述。
- IP 组：选择用户组里面添加的 IP 组。
- 时间组：选择用户组里面添加的时间组。
- URL 字符串：填入需过滤的域名或域名关键字。
- 文件后缀名：下载文件的后缀名，如.html、.exe、.pdf。

例如：如果您只禁止局域网中 IP 地址为 192.168.0.20~192.168.0.30（IP 组 RD）的计算机在星期一到星期五的 8:00-18:00(时间组 Working day)，不允许浏览包含“sina”,”baidu”,”163”字符串的 WEB 网站,，不允许通过 WEB 下载后缀名为.dos,.exe,.pdf 的文件，而可以访问其它网站，且其它计算机可以正常浏览所有的 WEB 网站。您需要设置如下参数：



点击保存，出现如下界面

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

3.5.4 网址分类过滤

您可以通过设置网址分类过滤，可以达到阻断/记录/警告访问相关类型网址的用户。

阻断：用户不能访问相关类型的网址，会提示无法找到该网址

记录：用户可以访问相关类型的网址，但是路由器会将用户的访问动作记录在系统日志里面。

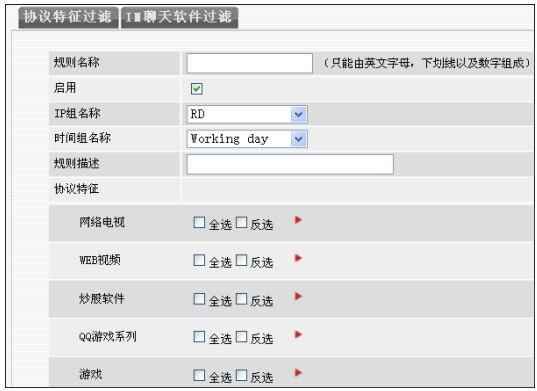
警告：用户不可以访问相关类型的网址，系统会提示路由器不允许访问此网址

3.5.5 协议特征过滤

在“协议特征过滤”菜单下，有“协议特征过滤”和“IM 聊天软件过滤”两个子项。

协议特征过滤

选择“协议特征过滤”子项，点击“添加协议特征过滤”，添加过滤规则：



规则名称：过滤规则的名称。

启用：是否启用此规则。

IP 组名称：选择需要的 IP 地址组。

时间组名称：选择需要的时间组。

规则描述：对该规则的简单描述。

协议特征：需要过滤的相应类型的应用。

全选：选择全部的分类或应用程序。

反选：选择之前没有选中的分类或应用程序。

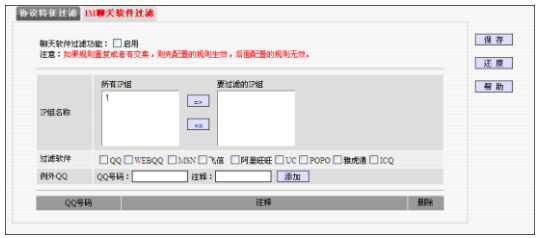
在协议特征选项中，共分为网络电视，WEB 视频，炒股软件，QQ 游戏系列和游戏五大类，每一个分类包含多个应用软件，可点击右边的三角形展开后查看，也可以查看“行为管理”—“组设置”—“协议特征”库。

例如：如果禁止局域网中 IP 地址为 192.168.0.20~192.168.0.30（IP 组 RD）的计算机在星期一到星期五的 8:00-18:00(时间组 Working day)，看网络电视，可以做如下图所示的设置：

点击“保存”按钮启用过滤规则。

IM 聊天软件过滤

IM 聊天软件过滤项可设置用户不能使用相应的聊天工具，如 QQ，WEBQQ,MSN，飞信，阿里旺旺，UC，POPO，雅虎通和 ICQ，也可以让某此特殊的 QQ 号码不受限制，可以正常使用。



启用聊天软件过滤：启用设置的规则。

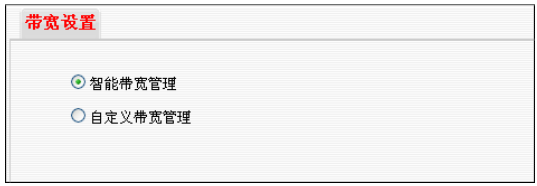
IP 组名称：需要做过滤限制的 IP 地址组。

过滤软件：需要做过滤限制的聊天软件。

例外 QQ：设置的 QQ 将不会被过滤。

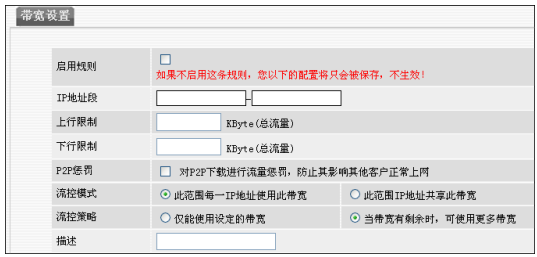
3.5.6 带宽设置

带宽设置一共有两种模式：智能带宽管理和自定义带宽管理。



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

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



- 启用规则：启用该带宽设置规则。
- IP 地址段：流量控制的主机 IP 地址范围，可以是单个 IP，也可以是一个 IP 段。
- 上行限制：总流量，允许指定 IP 范围内的主机上传的最大总流量。
- 下行限制：总流量，允许指定 IP 范围内的主机下载的最大总流量。
- P2P 惩罚：对 P2P 下载进行流量惩罚，防止其影响其他客户正常上网。
- 流控模式：选择此范围内 IP 地址独享/共享带宽。
- 流控策略：选择此范围内 IP 地址固定/弹性带宽。
- 描述：对该规则的简单描述。

⚠注意：

1. 上行限制/下行限制设置时请注意流量单位。

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

配置的带宽限制范围内。

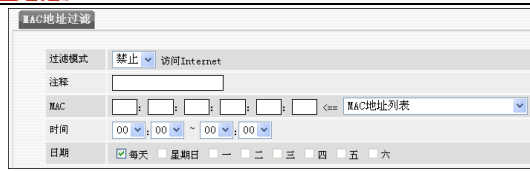
3.6 安全设置

在“安全设置”菜单下面，共有“MAC 地址过滤”、“攻击防御”和“IP-MAC 地址绑定”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。

3.6.1 MAC 地址过滤

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

点击“添加过滤规则”，会出现如下界面：



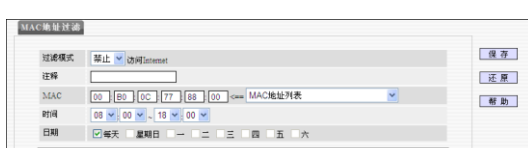
- 过滤模式：更改 MAC 地址过滤的过滤模式。

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

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

- 注释：即为此配置的简单描述。
- MAC:输入您要控制的 MAC 地址或直接选择 MAC 地址列表中的 MAC。
- 时间：填入您希望本条规则生效的起始时间和终止时间，如果不设置时间，默认显示为全 0，表示为 24 个小时。
- 日期：根据自身的要求选择相应的日期。

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



点击保存后，将出现如下的界面。

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

3.6.2 攻击防御

在“攻击防御”页面，共有“ARP 防御”、“DDOS 防御”和“IP 选项防御”三个子项，下面将详细讲解各子项的详细功能。

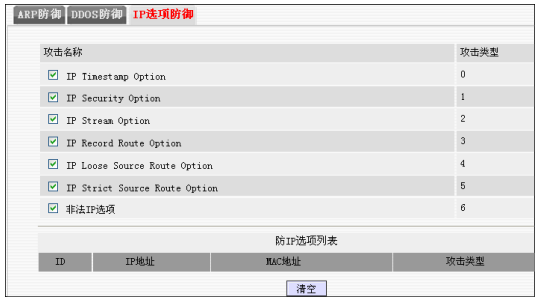
ARP 防御

ARP 防御可以防止内网发生 ARP 攻击、欺骗，路由器默认关闭此功能。ARP 广播间隔默认为一秒钟，可设置范围为 1-60 秒钟。

DDOS 防御

- ICMP Flood：这是指在一秒钟内，如果一个目的 IP 收到超过规定数量的 ICMP 请求包，则认为此目的 IP 正受到 ICMP Flood 的攻击。
- UDP Flood：这是指在一秒钟内，如果一个目的 IP 的某一端口收到超过规定数量的 UDP 包，则认为此目的 IP 的此端口正受到 UDP Flood 的攻击。
- SYN Flood：这是指在一秒钟内，如果一个目的 IP 的某一端口收到超过规定数量的 TCP SYN 包，则认为此目的 IP 的此端口正受到 SYN Flood 的攻击。

IP 选项防御



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

3.6.3 IP-MAC 地址绑定

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

IP-MAC 地址绑定

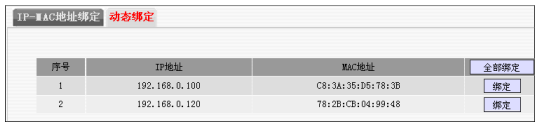
本功能用于实现内网计算机的 IP 地址与 MAC 地址之间的绑定。地址绑定一旦配置完成，指定的 IP 地址就只能被指定的计算机使用，解决了局域网中 IP 地址被随意改动而导致的 IP 地址冲突。

- 启动 IP-MAC 绑定：启动 IP-MAC 地址绑定功能。

点击“添加绑定”，会出现如下界面：

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

动态绑定



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

3.7 高级设置

在“高级设置”菜单下面，共有“虚拟服务器”、“DMZ”、“UPnP”、“DDNS”、“路由表”、“电子公告”、“即插即用”、“邮件密送”和“地址伪装”九个子项。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。

3.7.1 虚拟服务器

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

点击“添加虚拟服务器”按钮，添加设置：

✧ WAN 口：选择端口映射的 WAN 口。

✧ WAN 端口：WAN 服务端口，局域网内部 PC 端口对应映射到外部的端口。

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

对于常用服务端口中没有列出的端口，您也可以手动添加。

✧ LAN 端口：LAN 服务端口，即局域网内部 PC 的端口；

✧ 内网 IP：局域网中作为服务器的计算机的 IP 地址；

✧ 协议：包含 TCP、UDP 和全部。当您对使用的协议不确定时，可以选择全部。

✧ 启用：只有选中该项后本条目所设置的规则才能生效。

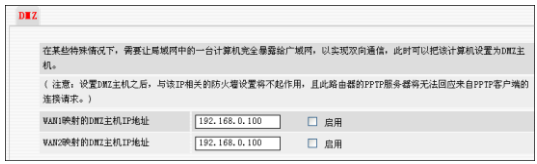
例如：您在内部局域网 IP 为 192.168.0.10 的计算机上搭建了一个 WEB 服务器，服务器使用端口为 80，如果需要实现在广域网以 http://x.x.x.x:40 访问到 WEB 服务器（x.x.x.x 为路由器 WAN2 IP 地址），就可以在此页面中的“WAN 端口”中输入 40，“LAN 端口”中输入 80，“内网 IP”设置为 192.168.0.10，“协议”选择全部，选择启用，添加到列表保存后，即可生效。

⚠注意：

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

3.7.2 DMZ

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



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

⚠注意：

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

3.7.3 UPnP

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

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

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

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

3.7.4 DDNS

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

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

- 开启动态 DNS：选择是否开启此功能。
- 服务提供商：选择提供 DDNS 的服务提供商，可选择 3322.org，88IP.cn 和金万维。
- 用户名：在 DDNS 服务器上注册的用户名。
- 密码：在 DDNS 服务器上注册的密码。
- 域名信息：在 DDNS 服务器注册的域名。
- 连接状态：当前和 DDNS 服务器的连接状态。

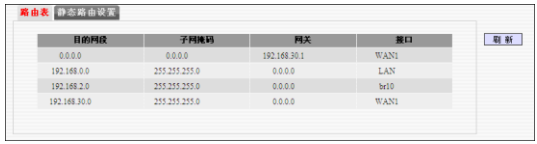
3.7.5 路由表

在“路由表”菜单下面，共有“路由表”和“静态路由设置”两个子项，下面将详细讲

解各子项的详细功能。

路由表

本页显示路由器路由表的内容。



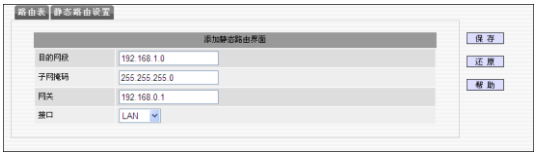
静态路由设置

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

- 目的网段：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。
- 接口：指定接口。

要实现局域网内不同网段的 pc 进行通信，您需要进行如下的配置：

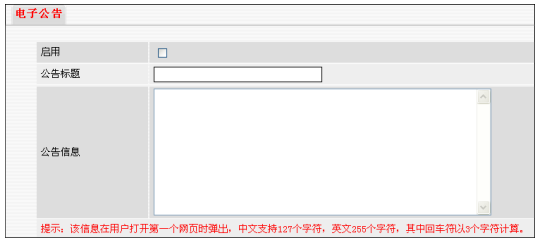
例如：局域网内分别位于 192.168.0.0/24,192.168.1.0/24 网段的 PC1（192.168.0.11），PC2(192.168.1.11)进行通讯，您需要在静态路由器设置界面进行如下的配置：



PC2 的网关设置为 192.168.0.1。这样配置之后，PC1 和 PC2 就可以互相通讯。

3.7.6 电子公告

公告信息在用户打开第一个外网网页时弹出。

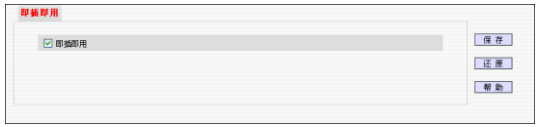


- 启用：是否启用电子公告功能。
- 公告标题：公告信息的标题。
- 公告信息：公告的具体信息。

注意：

1. 使用电子公告功能，需在行为管理-组设置中添加 IP 组、时间组。

3.7.7 即插即用



启用此功能后，连接到路由器的 PC 只要具有 IP 地址、子网掩码、网关地址和 DNS 就可以上网。

注意：

1. ARP 防御攻击会导致该功能失效。

3.7.8 邮件密送

- 启用：是否启用邮件密送功能。
- 监控邮件地址：路由器下所有主机发送的邮件都将被发送至监控邮件地址。

注意：

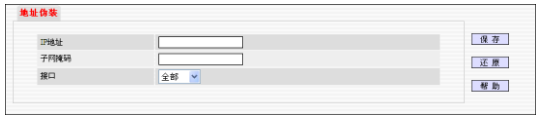
1. 邮件密送只对邮箱客户端软件有效（如：Outlook，Foxmail 等），对网站邮箱无效。

3.7.9 地址伪装

地址伪装配合使用静态路由 LAN 口设置可以实现路由器 LAN 口下不同网段的 PC 上网

- ID：伪装列表的序列号。
- IP 地址：与路由器 LAN 口不同网段的需要伪装上网的 IP 地址或 IP 段。
- 子网掩码：需要伪装上网的 IP 地址或 IP 段的子网掩码。
- 接口：指定接口。

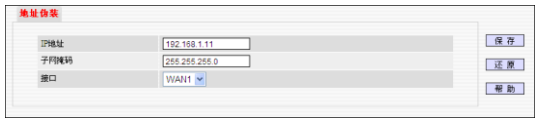
点击“添加”按钮，将出现如下的界面：



例如：要实现局域网不同网段的 PC1（192.168.1.11/24）的上网功能，您需要进行如下的配置：

1 添加静态路由器：

2 添加地址伪装：



点击“保存”按钮之后，局域网不同网段的 PC1(ip 地址：192.168.1.11，子网掩码：255.255.255.0，网关：192.168.0.1，DNS 服务器：192.168.0.1)的上网功能。

3.8 USB 应用

本路由器提供两个 USB 接口，用于连接 USB 设备，可同时支持储存设备的共享和 USB 打印功能。在“USB 应用”菜单下，包含“网络邻居共享”和“USB 打印功能”两个子项。

3.8.1 网络邻居共享

通过启用共享实现 USB 存储文件资料共享。

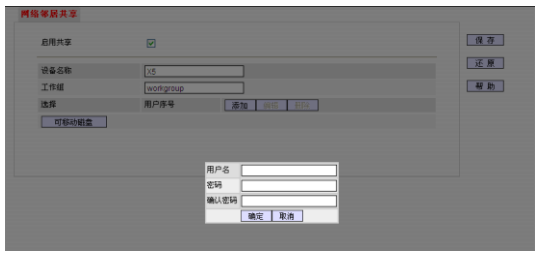
- 启用共享:启用、禁用网络邻居共享；
- 设备名称：给该设备定义一个网络名；
- 工作组：给该设备定义一个工作组名；
- 添加：添加用户账号，最多可添加五个用户；
- 编辑：编辑已添加的用户账号；
- 删除：删除已添加的用户账号；

操作说明：

在开始共享 USB 存储文件共享之前需先新建一个用户账号。

1、 新建账户：

点击用户序号列表中的“添加”按钮，将出现如下对话框：



输入访问共享文件时客户端提供的账号名称与密码，重新输入密码以确认。点击“确定”按钮后如下图：

2、 设置权限

选择您要设置访问权限的账号，点击“盘符”——“sda1”，在文件列表中，选择您要设置的访问权限。

读/写：对文件有读取、写入的权限；

只读:对文件仅有读取的权限；

无权限:无法共享此文件；

点击本页面“保存”按钮，应用所有配置。

3、 客户端访问

在连接到路由器的电脑中双击“我的电脑”——在地址栏中输入：\\192.168.0.1，进行访问共享文件。

3.8.2 USB 打印功能

USB 打印功能允许您设置连接在无线路由器上的 USB 打印机，并允许您网络内的客户端共享使用 USB 打印机。USB 打印机与无线路由器连接成功后，路由器可自动识别打印机设备。

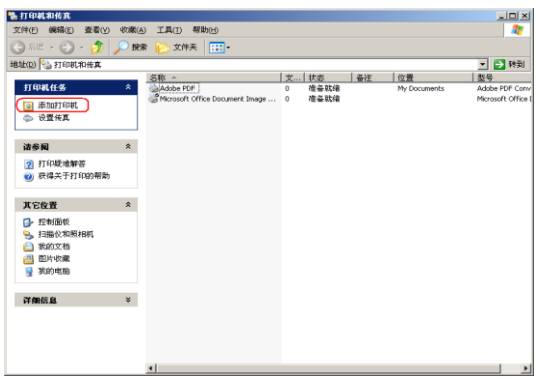
➢ 启用打印服务：启用或者禁用 USB 打印功能。

操作说明：

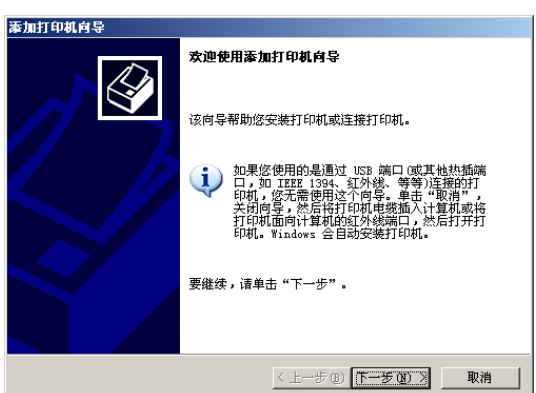
1、 USB 打印机与路由器 USB 接口正常连接；

2、 启用打印服务功能；

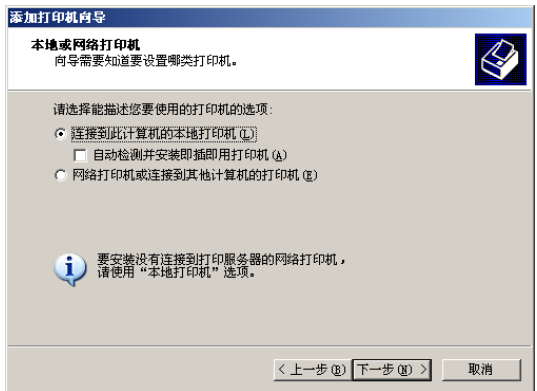
3、 在与此路由器连接的电脑上，点击“开始”——“设置”——“打印机和传真”，在弹出的对话框中选择“添加打印机”；



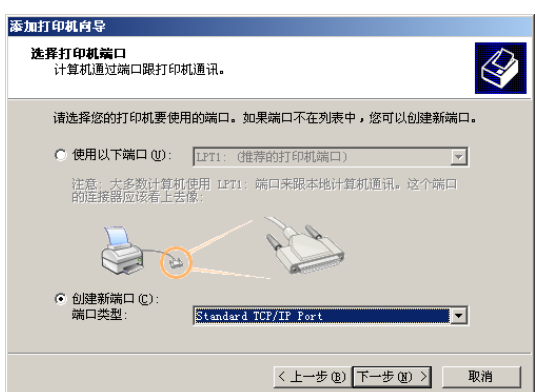
4、 点击“下一步”进行添加；



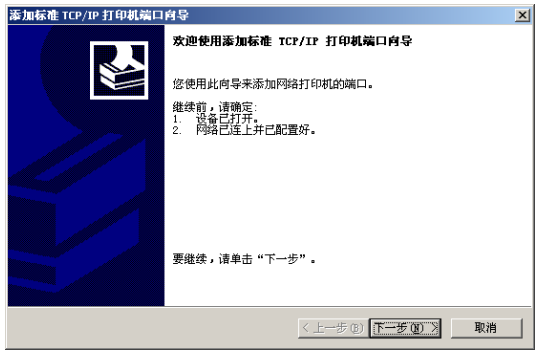
5、 选择“连接到此计算机的本地打印机”，点击“下一步”；



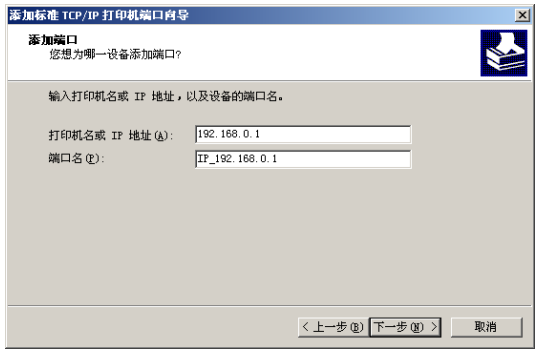
6、 选择“创建新端口”，端口类型为：Standard TCP/IP Port，点击“下一步”；



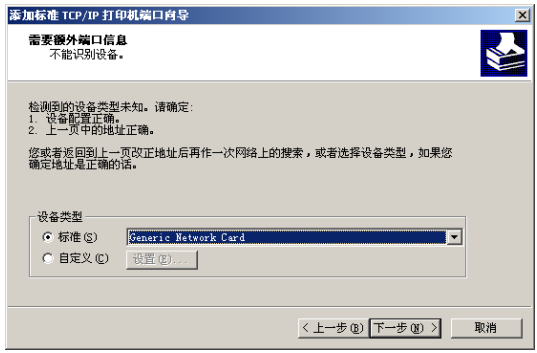
7、 点击“下一步”按钮；



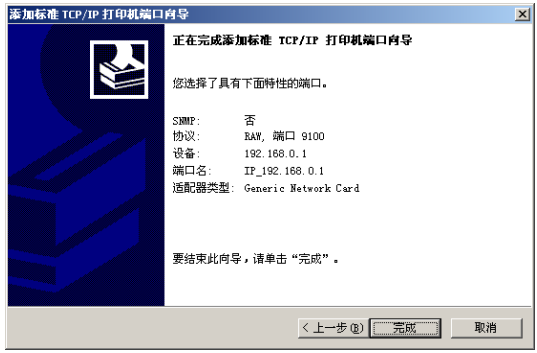
8、 输入路由器的管理 IP 地址；点击“下一步”；



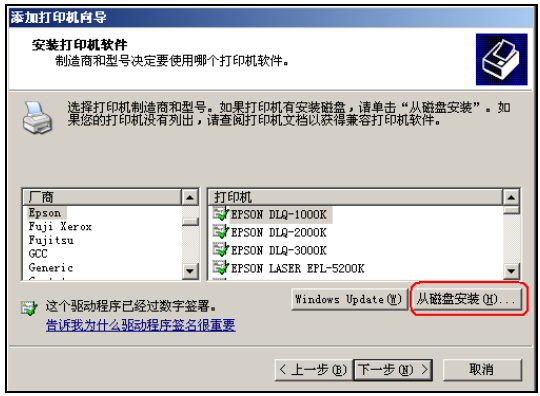
9、 选择设备类型为标准的 Generic Network Card,点击“下一步”；



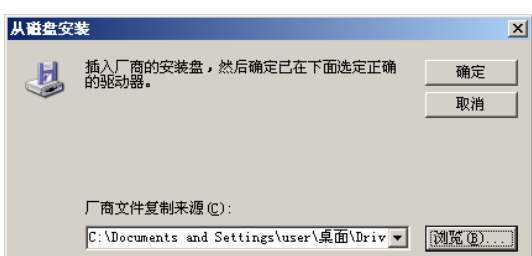
10、 点击“完成”按钮，完成端口添加；



11、 选择“从磁盘安装”；

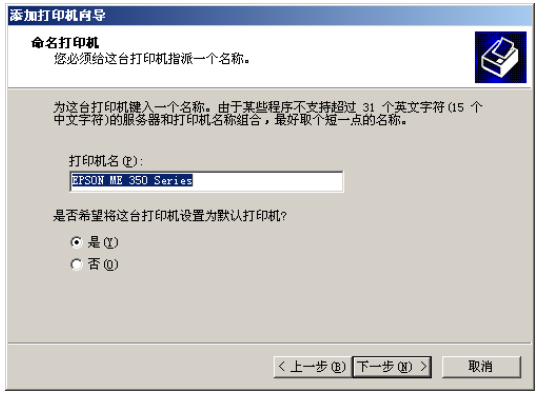


12、 点击“浏览”，在弹出的对话框中，选择设备驱动文件，再点击“打开”，确定文件目录后，点击“确定”按钮；

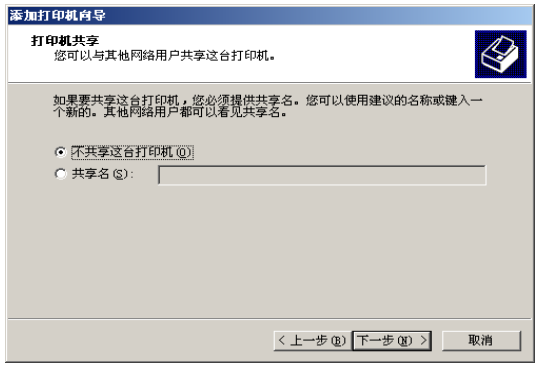


13、 点击“下一步”；

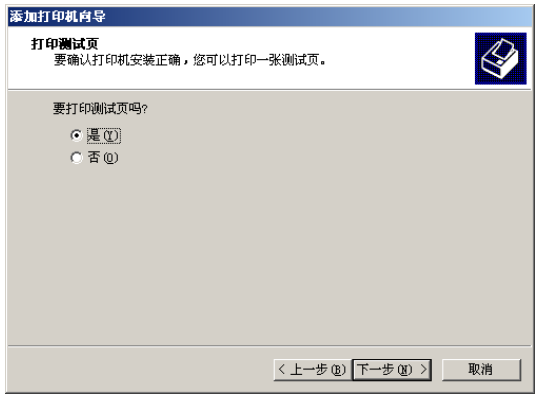
14、 设置打印机名称，点击“下一步”；



15、选择是否共享此打印机，请根据您的需要来设置是否共享打印机；



16、为确保您的打印机安装正确，选择“是”按钮打印测试页；



17、点击“完成”按钮完成添加；

3.9 VPN 设置

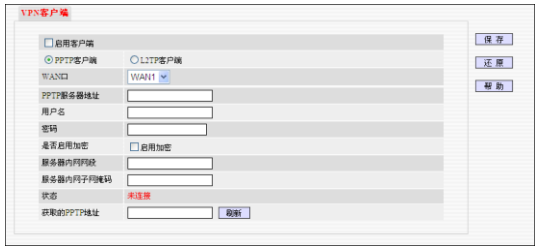
在“VPN 设置”菜单下面，有“VPN 客户端”、“VPN 服务器”、“证书管理”和“证书管理”四个子项。单击某个子项，您即可进行相应的功能设置，下面将详细介绍各子项的功能。

3.9.1 VPN 客户端

VPN 客户端包含 PPTP 客户端和 L2TP 客户端。支持从 VPN 路由器客户端连接到 VPN 路由器服务端。比如：企业分支机构与企业总部之前需要实现简单安全的信息互访，可以在分支

机构路由器中使用 PPTP 客户端完成上述操作。

PPTP 客户端配置界面：



- WAN 口：指定 WAN 口
- 启用客户端：是否启用 PPTP 客户端功能。
- PPTP 服务器地址：需要连接的 PPTP 服务器 IP 地址。
- 用户名/密码：PPTP 服务器分配给您的用户名和密码。
- 是否启用加密：是否启用数据加密。需要与服务器设置一致。
- 服务器内外网段：PPTP 服务器端的局域网网段。
- 服务器内外子网掩码：PPTP 服务器端的局域网子网掩码。
- 状态：显示当前 PPTP 客户端的连接状态。
- 获取的 PPTP 地址：PPTP 连接成功后，从 PPTP 服务器获取的 IP 地址。

L2TP 客户端配置界面：

- WAN 口：指定 WAN 口
- 启用客户端：是否启用 L2TP 客户端功能。
- L2TP 服务器地址：需要连接的 L2TP 服务器 IP 地址。
- 用户名/密码：L2TP 服务器分配给您的用户名和密码。

- 服务器内外网段：L2TP 服务器端的局域网网段。
- 服务器内外子网掩码：L2TP 服务器端的局域网子网掩码。
- 状态：显示当前 L2TP 客户端的连接状态。
- 获取的 PPTP 地址：L2TP 连接成功后，从 L2TP 服务器获取的 IP 地址。

⚠注意：

PPTP 与 L2TP 客户端不能同时开启，一个开启后另一个会自动关闭。

3.9.2 VPN 服务器

VPN 服务器包含 PPTP 服务器和 L2TP 服务器。VPN 服务器设置页面共有“VPN 服务器”，“VPN 用户设置”和“拨入列表”三个子项。PPTP 与 L2TP 服务器不能同时开启，一个开启后另一个会自动关闭。

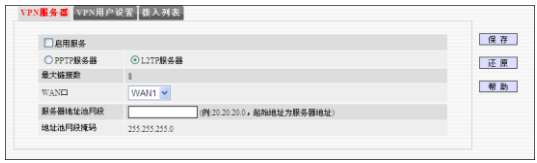
PPTP 服务器

此页面设置 PPTP 服务器参数：

- 启用服务器：是否启用 PPTP 服务器。
- 最大 PPTP 链接数：可以接入的最大客户端数量，系统固定为 8 个。
- WAN 口：PPTP 服务器应用的 WAN 口，用于客户端接入。
- 服务器地址池网段：分配给 PPTP 客户端的 IP 地址段，IP 地址段开始的第一个地址即为 PPTP 服务器地址，从第二个地址开始分配给 PPTP 客户端。如：PPTP 客户端的 IP 地址段为 20.20.20.0，PPTP 服务器地址即为 20.20.20.1， 20.20.20.2 分配给第一个连接上的 PPTP 客户端。
- 是否启用加密：是否加密 PPTP 通信的数据。

L2TP 服务器

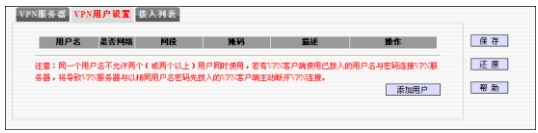
此页面设置 L2TP 服务器参数：



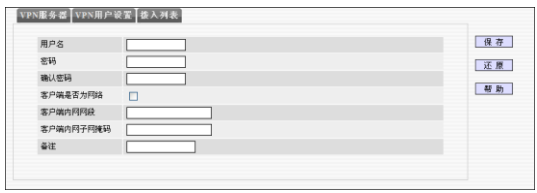
- 启用服务器：是否启用 L2TP 服务器。
- 最大 L2TP 链接数：可以接入的最大客户端数量，系统固定为 8 个。
- WAN 口：L2TP 服务器应用的 WAN 口，用于客户端接入。
- 服务器地址池网段：分配给 L2TP 客户端的 IP 地址段，IP 地址段开始的第一个地址即为 L2TP 服务器地址，从第二个地址开始分配给 PPTP 客户端。如：L2TP 客户端的 IP 地址段为 20.20.20.0，PPTP 服务器地址即为 20.20.20.1， 20.20.20.2 分配给第一个连接上的 L2TP 客户端。

VPN 用户设置

此页面显示已经设置的 VPN 账号信息。



点击“添加用户”，进行客户端账号的添加：

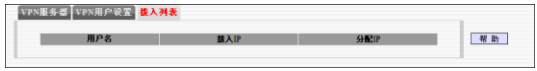


- 用户名/密码：客户端连接到 VPN 服务器使用的账号。
- 客户端是否为网络：VPN 客户端是一个网络时，需要启用，并且需要设置 VPN 客户端的网段和掩码。
- 网段/掩码：VPN 客户端的局域网网段和子网掩码。

- 备注：描述设置的信息。

拨入列表

显示当前已经连接到此 PPTP 服务器的客户端信息。



⚠注意：

设置 PPTP 客户端和服务器端的参数时，有以下几点需要注意：

1. 确保路由器可以与外网成功通信。
2. VPN 客户端设置时，配置的 VPN 服务器地址为服务器端的 WAN 口 IP 地址，而不是在 VPN 服务器设置页面中配置的 IP 地址。
3. PPTP 服务器端和客户端需要同时设置加密或者不加密。
4. 如果 VPN 服务器和客户端都有自己的局域网，并且需要相互访问，需要正确添加相关的子网：服务器端添加的是客户端的子网信息，客户端添加的是服务器端的子网信息。

3.9.3 证书管理

在证书管理页面共有“本地证书管理”，“服务器证书管理”两个子项。单击某个子项，您即可进行相应的功能设置，本模块结合 IPSEC 模块使用。下面将详细介绍各子项的功能。

本地证书服务器

此页面主要是传入本地端的证书，有直接上传和手动生成两种方式，其中保存到 Flash 按钮是为了保证传入的证书在重启路由后不会丢失

点击 “生成证书”按钮生成一对证书密钥对

- 证书名称:生成证书的命名
- 证书规格:生成证书的密钥长度(长度越长更安全但速率会相应变慢)
- 国　家:选择自己的国家
- 省或州名:填写自己的省或州名
- 地区或城市:填写自己的地区或城市
- 组织/单位/姓名：填写自己的组织、单位和姓名
- 电子邮件:填写自己的电子邮箱
- 仅生成证书请求：路由器会为您生成一个私钥和一个证书请求，您可以在证书管理页面进行下载此证书请求，并通过 CA（证书管理中心）签名后开成证书，再次导入路由器
- 生成自签发的证书:路由器会为您生成一个自己签名的证书，您可以在证书管理页面进行下载。

⚠**注意：**仅生成证书请求只会生成证书请求的初始配置档,您必须到特定的证书服务器网站上申请证书,所以正常情况下不建议使用该操作

点击“导入证书”按钮导入一对证书密钥对

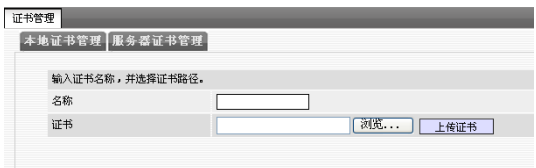
- 名称:填入证书的名称
- 证书:导入证书
- 密钥:导入密钥

⚠**注意：**因该操作必须要您手中有配对的证书和密钥才能起作用,所以一般情况下不建议使用,直接点选生成证书按钮能自动为您生成配对的证书和密钥

服务器证书：

此页面主要是传入远端服务器发给您的证书，有“上传证书”和“保存到 Flash 中”按钮，其中保存到 Flash 按钮是为了保证传入的证书在重启路由后不会丢失

点击“上传证书”按钮进入上传证书按钮



- 名称:填入证书的名称
- 证书:导入远端服务器的证书

3.9.4 IPSEC 设置

本产品的 IPsec 默认为隧道模式，在隧道模式下，整个原数据包被当作有效载荷封装了起来，外面附上新的 IP 报头。其中“内部 IP 报头”（原 IP 报头）指定最终的信源和信宿地址，而“外部 IP 报头”（新 IP 报头）中包含的常常是做中间处理的安全网关地址。

点击“添加 IPSEC 隧道”按钮添加条 IPSEC 规则

- WAN 口：选择本地接口，将 IPSec 配置绑定到指定接口上，那么所有经过该接口的数据包将被 IPSec 检查，以确定是否对该数据包进行加密和解密操作。（接口可以是以太网口，或 PPPoE 拨号连接，还可以是 L2TP 拨号连接。）
- 连接名称：为一条 IPSec 隧道命名，名称必须唯一。
- 隧道协议：

  ESP(Encapsulating Security Payload)：在端对端的隧道通信中该协议会对整个数据包进行加密，用户可选使用带密钥的哈希算法保证报文的完整性和真实性（该协议在各

网关产品中使用较广泛，兼容性较好）。

AH(Authentication Header)：该协议会对整个数据包完整性检查，包括"外部"IP 报头，不对数据进行加密，若数据包在传输过程中数据被修改，则该数据包会被丢弃。

ESP+AH：兼具 ESP 与 AH 两个协议加密与完整性检查的功能。

- 远端安全网关 IP（域名）：IPSec 隧道远端网关的 IP 地址（或域名）。设置为域名时，需要在设备上设置 DNS 服务器，此时设备会定期解析该域名，若 IP 地址变化，设备将重新协商 IPSec 隧道。
- 本地内网 IP/掩码：本地受保护的内网的任一 IP 地址和子网掩码。
- 远端内网 IP/掩码：隧道远端受保护的内网的任一 IP 地址和子网掩码。若远端是移动单机用户，则这个参数设置为该设备的 IP 地址/32。
- 密钥协商方式：

手动设置：SA（安全联盟）的建立需要用户设置加密/认证算法及密钥，手动建立的 SA 没有生存周期限制，永不过期，除非手工删除，因此有安全隐患。该方式常用于调试阶段。

自动协商：SA 的自动建立、动态维护和删除是通过 IKE(Internet Key Exchange)进行的，自动建立的 SA 有生命期。如果安全策略（SP）要求建立安全、保密的连接，但又不存在与该连接相应的 SA，IPSec 的内核会立即启动 IKE 来协商 SA。

- ESP 认证算法：（可选，提供数据包完整性保证服务）

NONE：ESP 认证算法为空，不需要填入认证密钥。

MD5：ESP 认证算法为 MD5 时，认证密钥长度必须为 16 个 ASCII 码或 32 个十六进制数。

SHA1：ESP 认证算法为 SHA1 时，认证密钥长度必须为 20 个 ASCII 码或 40 个十六进制数。

- AH 认证算法：

MD5：AH 认证算法为 MD5 时，认证密钥长度必须为 16 个 ASCII 码或 32 个十六进制数。

SHA1：AH 认证算法为 SHA1 时，认证密钥长度必须为 20 个 ASCII 码或 40 个十六

进制数。

- 认证方法：

  共享密钥：双方事先通过某种方式商定好一个双方共享的字符串。

  X.509 认证：双发利用数字证书来表示身份，利用数字签名算法计算出　　一个签名来验证身份。

  本地证书：本地数字证书，可在证书管理页面中生成自签发证书也可以从证书发行机构获得您自己的数字证书，通信前需将本地证书与远端共享。

  远端证书：远端的数字证书，通信前需要通过某种方式获得远端的数字证书。

- 预共享密钥：协商所用的预共享密钥，最长为 128 字符。
- 协商模式（第一阶段）：主模式、积极模式（野蛮模式）。
- 加密认证算法（第一阶段）：可供第一阶段协商使用的首选加密和认证算法。
- Diffie-Hellman 分组（第一阶段）：Diffie-Hellman 公共密钥算法中需要的参数，与远端保持相同即可。
- 生存时间（第一阶段）： IKE SA 的生存时间，至少 600 秒，当剩余时间为 540 秒时，将重新协商 IKE SA。
- PFS（完美转发安全）：PFS 是提议者向接收者提供建议的属性，如果协商就支持，否则就不支持。它的作用是在快速模式中重新协商 DH 密钥。这允许使用新的密钥进行 IPSec 加密，而不是使用第一阶段生产的密钥。
- Diffie-Hellman 分组（第二阶段）：Diffie-Hellman 公共密钥算法中需要的参数，与远端保持相同即可。
- 加密认证算法（第二阶段）：可供第二阶段协商使用的首选加密和认证算法。
- 生存时间（第二阶段）：IPSec SA 的生存时间，至少 600 秒，当剩余时间为 540 秒时，将重新协商 IPSec SA。

可以将密钥协商方式设置为手动模式

- ESP 加密算法：

  3DES：加密算法为 3DES 时，密钥长度必须为 24 个 ASCII 码或 48 个十六进制数。

  DES：加密算法为 DES 时，密钥长度必须为 8 个 ASCII 码或 16 个十六进制数。

  AES-128：加密算法为 AES-128 时，密钥长度必须为 16 个 ASCII 码或 32 个十六进制数。

  AES-192：加密算法为 AES-192 时，密钥长度必须为 24 个 ASCII 码或 48 个十六进制数。

  AES-256：加密算法为 AES-256 时，密钥长度必须为 32 个 ASCII 码或 64 个十六进制数。

- ESP 认证算法：（可选，提供数据包完整性保证服务）

  NONE：ESP 认证算法为空，不需要填入认证密钥。

  MD5：ESP 认证算法为 MD5 时，认证密钥长度必须为 16 个 ASCII 码或 32 个十六进制数。

  SHA1：ESP 认证算法为 SHA1 时，认证密钥长度必须为 20 个 ASCII 码或 40 个十六进制数。

- AH 认证算法：

  MD5：AH 认证算法为 MD5 时，认证密钥长度必须为 16 个 ASCII 码或 32 个十六进制数。

  SHA1：AH 认证算法为 SHA1 时，认证密钥长度必须为 20 个 ASCII 码或 40 个十六

进制数。

- SPI（Security Parameter Index）：是 32 位的安全参数索引，用于标识具有相同 IP 地址和相同安全协议的不同的 SA。为保证安全联盟的唯一性，建议使用不同的 SPI 来配置安全联盟；使用 IKE 协商产生安全联盟时，SPI 将随机生成。

  ESP 外出 SPI：与远端的 ESP 进入 SPI 相同。

  ESP 进入 SPI：与远端的 ESP 外出 SPI 相同。

  AH 外出 SPI：与远端的 AH 进入 SPI 相同。

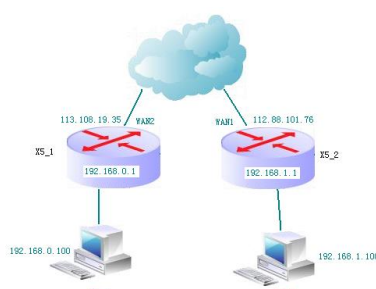
  AH 进入 SPI：与远端的 AH 外出 SPI 相同。

增加实例

⚠注意：

IPSEC 是路由器的两端互作为客户端和服务器，因此两端配置的认证和加密方式必须保持一致若想更安全，建议密钥协商方式不要使用手动设置

下面举例说明怎么使用 IPSEC VPN。



使用预共享密钥建立 IPSEC VPN

1. 两台 X5 的 LAN IP 不能是同一网段。X5 默认 LAN IP 为 192.168.0.1，请将其中一台 X5 的 LAN IP 改成其他网段。我们这里将 X5_2 的 LAN IP 改成 192.168.1.1

2. X5_2 的 WAN2 口 PPPoE 拨号，获取到的 IP 为 112.88.101.76； X5_1 的 WAN1 口 PPPoE 拨号，获取到的 IP 为 113.108.19.35。PC_A 能 Ping 通 112.88.101.76，PC_B 能 Ping 通 113.108.19.35。

3. X5_2 上添加一条 IPSEC 隧道，配置如下

4. X5_2 上也添加一条 IPSEC 隧道，配置如下

5. 当两台 X5 都添加了 IPSEC 隧道的配置后，IPSEC 进程就启动了，但 IPSEC VPN 实际上还没有建立，只是配置配好安全策略 SP 而已，安全联盟 SA 并没有协商建立。只有当其中一台 X5 的内网 PC 发送数据到另一台 X5 的内网时，开始协商 SA，SA 协商好后，

IPSEC 隧道即建立成功。

6. PC_A Ping 192.168.1.100，X5_1 收到第一个 Ping 包时，IPSEC 进程发现是发往已有的安全策略的另一方的，就会启动 IKE 与 X5_2 协商 SA。

7. 因双方的配置匹配，SA 几秒内即可协商出来，协商的速度根据设置的算法而定，一般需要 2～5 秒左右的时间。所以 PC_A Ping 192.168.1.100，前一两个包 Time out，后续的包就可以 Ping 通了，也就说明 IPSEC VPN 建立成功了。

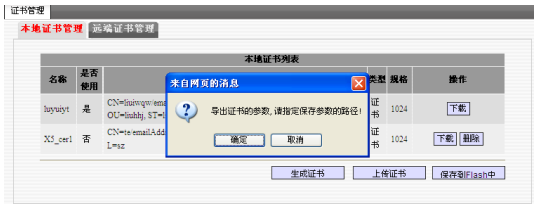
使用数字证书建立 IPSEC VPN

接上一个例子接着往下设置。

1、 X5_1 生成一个自签发的证书，证书名称为 X5_cer1。

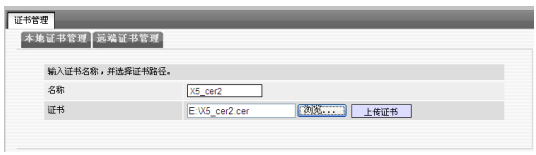
2、 X5_2 也生成一个自签发的证书，证书名称为 X5_cer2。

3、 PC_A 将 X5_1 的证书 X5_cer1 下载到本地电脑，PC_B 将 X5_2 的证书 X5_cer2 也下载下来。

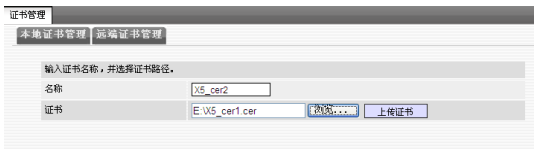


4、 PC_A 和 PC_B 将自己的证书通过邮件的方式发给对方。

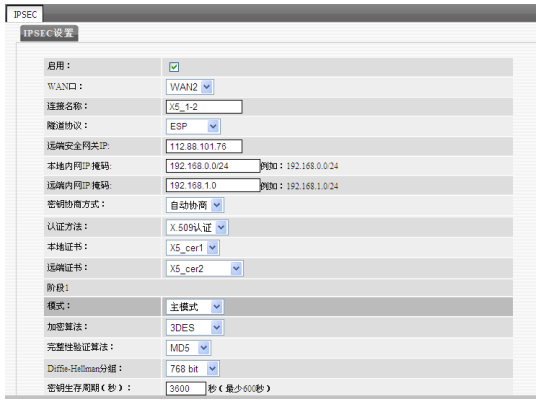
5、 PC_A 将 X5_2 的数字证书导入 X5_1 的远程证书管理列表里。



6、 PC_B 将 X5_1 的数字证书导入 X5_2 的远程证书管理列表。



7、 如果添加一条 IPSEC 隧道，需要将隧道 X5_1-2 先删除，因为一个远端内网只能建立一条 IPSEC 隧道。我们这里采用修改现有隧道的方法进行配置。修改 X5_1 的 IPSEC 隧道，将认证方式改成 X.509，本地证书选择 X5_cer1，远端证书选择 X5_cer2，其他配置保持不变。



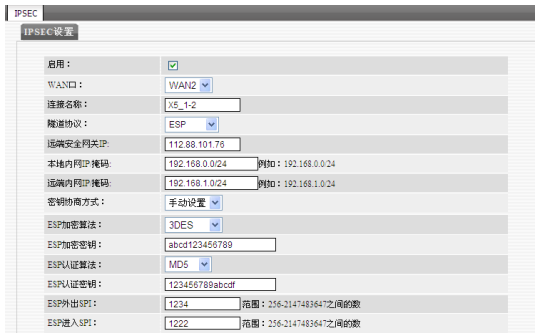
8、 修改 X5_2 的 IPSEC 隧道，将认证方式改成 X.509，本地证书选择 X5_cer2，远端证书选择 X5_cer1，其他配置保持不变。

9、 当 IPSEC 隧道的配置被修改再次保存后，IPSEC 进程会重启，之前的 SA 会被清除。PC_A 和 PC_B 再次通信时，会用新的配置重新协商 SA，即使用证书建立 IPSEC VPN。

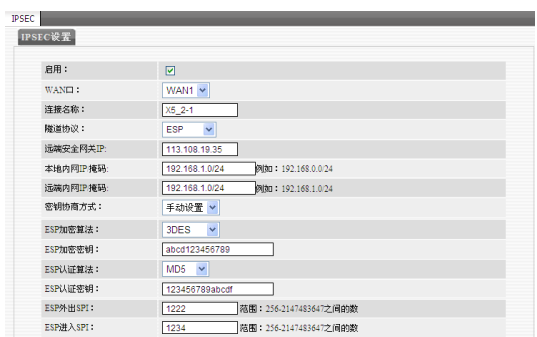
使用手动设置建立 IPSEC VPN

接上一个例子接着往下设置。

1、 修改 X5_1 的 IPSEC 隧道，将密钥协商方式改为“手动设置”，照下图设置其他参数。



2、 修改 X5_2 的 IPSEC 隧道，将密钥协商方式改为“手动设置”，照下图设置其他参数。



3、 当 IPSEC 隧道的配置被修改再次保存后，IPSEC 进程会重启，之前的 SA 会被清除。PC_A 和 PC_B 再次通信时，IPSEC VPN 会使用手动配置的 SA 进行加解密。

⚠注意：

1． 双方添加 IPSEC 隧道配置后，VPN 还未建立，当有数据通信时才开始协商建立 IPSEC VPN。

2． 当一方保存配置、插拔网线或重启系统后，IPSEC 进程都会重启，IPSEC 隧道即被中断。此时这一方没有 SA，另一方仍使用之前的 SA，另一方的内网 PC 会一直 Ping 不通这一方的内网 PC。只有当这一方的内网 PC 再次与另一方的内网 PC 通信时，这一方才会主动开始与另一方协商密钥建立 VPN。

3． 使用数字证书建立 IPSEC VPN 时，须先自己生成证书，并将证书与远端路由器共享。

3.10 系统监控

在“系统监控”菜单下面，共有“流量统计”、“日志查看”” 和“日志设置”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。

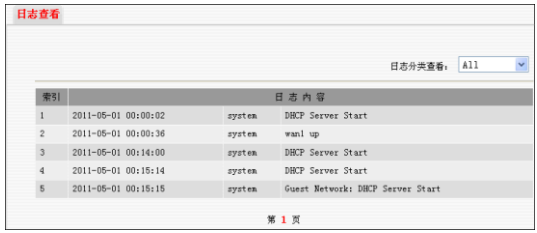
3.10.1 流量统计

在此页面中，显示局域网中各 IP 地址当前的数据包流量信息。

- 启用流量统计：是否启用对内网用户的流量统计功能。如果没有必要，建议关闭此功能。
- 刷新：更新列表中的信息。

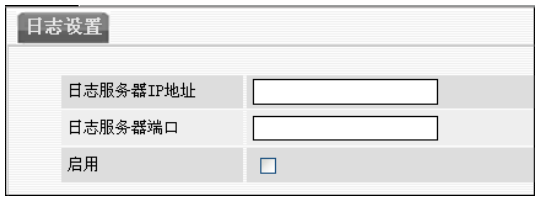
3.10.2 日志查看

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



3.10.3 日志设置

默认的情况下，当系统日志满 200 条后，旧的记录将会被路由器自动清除。为了更完整的了解路由器的运行状态，日志设置功能可以把路由器的日志信息传给日志服务器，点击“添加日志设置”，显示的页面如下：



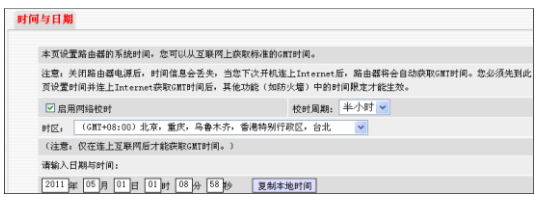
- 日志服务器 IP 地址：搭建日志服务器的 IP 地址。
- 日志服务器端口：日志服务器开启的服务端口。
- 启动：启动日志服务功能。

3.11 系统工具

在“系统工具”菜单下面，共有“时间与日期”、“软件升级”、“策略升级”、“备份与恢复”、“恢复出厂设置”、“用户名与密码”和“重新启动”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。

3.11.1 时间与日期



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

- 启用网络校时：系统时间从网络上自动获取。
- 校时周期：系统时间从网络校时周期，请根据您的需要进行选择，系统默认校时周期为半个小时。
- 时区：选择您当地的时区。
- 复制本地时间：将您电脑的时间设置到路由器上。

3.11.2 软件升级

通过升级本路由器的软件，您将获得更加稳定的路由器版本及增值的路由功能。

软件升级步骤：

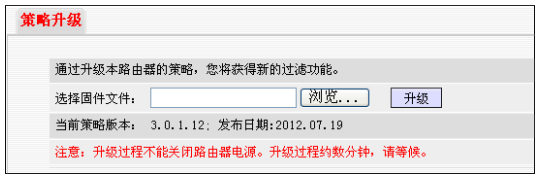
- 浏览选择升级文件的路径，单击“升级”进行软件升级。
- 升级完成后，路由器将自动重新启动。

⚠注意：

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

3.11.3 策略升级

通过升级本路由器的策略文件，您将获得更加稳定的过滤功能。



策略升级步骤：

- 点击“浏览”选择策略文件的路径，单击“升级”进行策略升级。

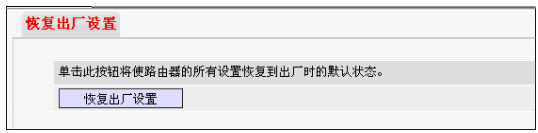
3.11.4 备份与恢复

在这里您可以备份当前或恢复以前的路由器设置。

备份/恢复设置步骤：

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

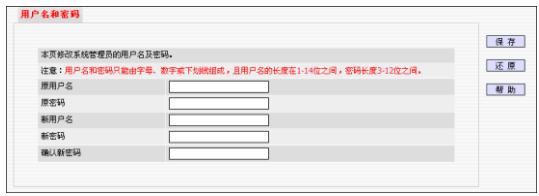
3.11.5 恢复出厂设置



单击“恢复出厂设置”按钮，将使路由器的所有设置恢复到出厂时的默认状态。

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

3.11.6 用户名和密码



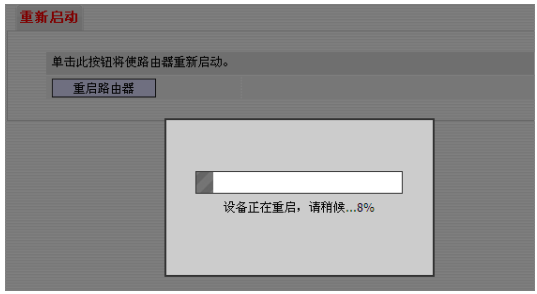
- 本页修改系统管理员的用户名和密码。
- 请您首先输入原用户名和原密码，然后输入您希望使用的新用户名和密码 ，如果您原来的用户名和密码无误的话，单击“保存”即可成功修改系统的用户名和密码。

⚠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。

3.11.7 重新启动

本界面提供的功能是从软件上重启路由器，路由器的重启过程大概需要一分钟。界面如下图所示：

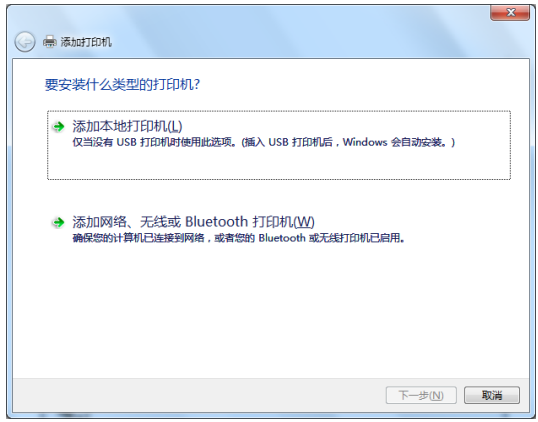


点击“重启路由器”按钮，将使一些需要重新启动才能生效的设置生效。路由器在重启前，会自动断掉网络连接。

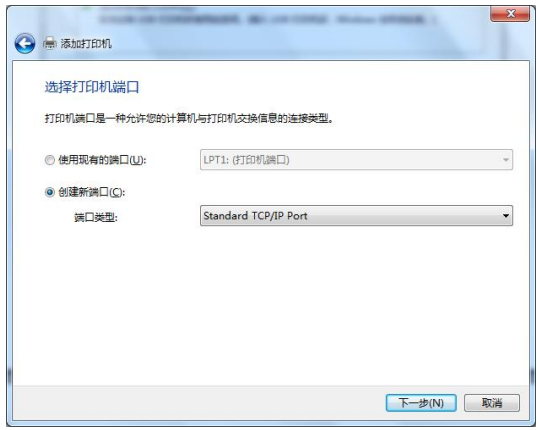
附录一　添加打印机的设置方法（以 Windows 7 为例）

1、在与此路由器连接的电脑上，点击“开始”——“设备和打印机真”，在弹出的对话框中选择“添加打印机”；

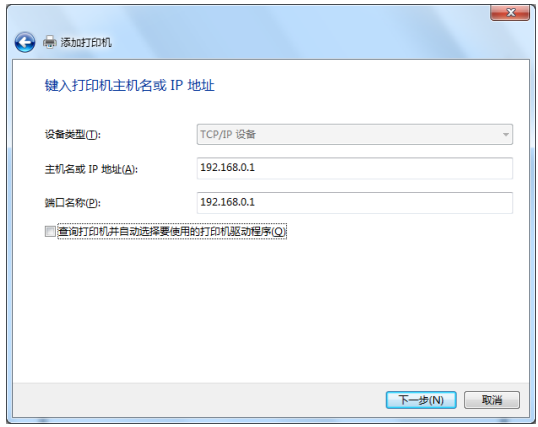
2、选择“添加本地打印机”，点击“下一步”；



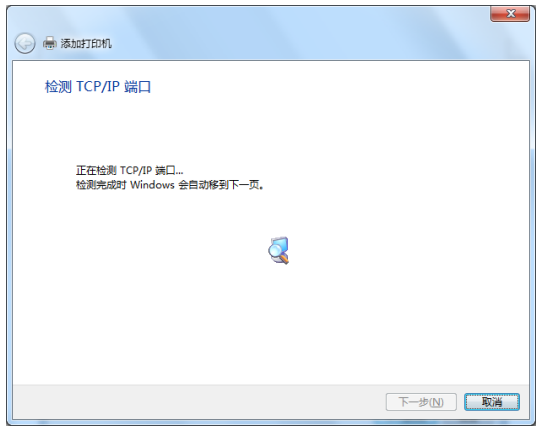
3、选择“创建新端口”，端口类型为：Standard TCP/IP Port，点击“下一步”；



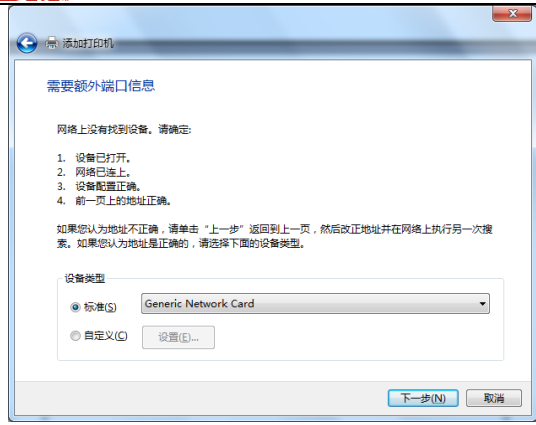
4、 输入路由器的管理 IP 地址；点击“下一步”；



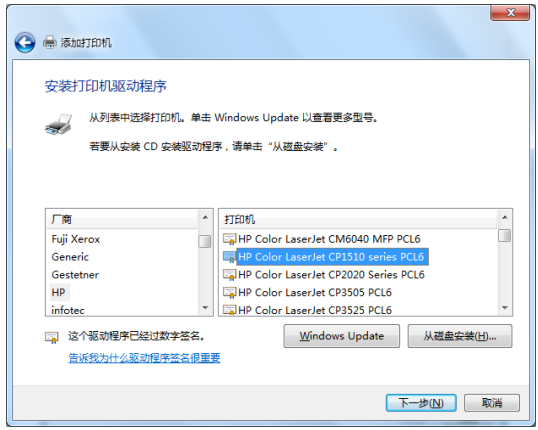
5、与路由器相连的电脑自动检测 TCP/IP 端口；



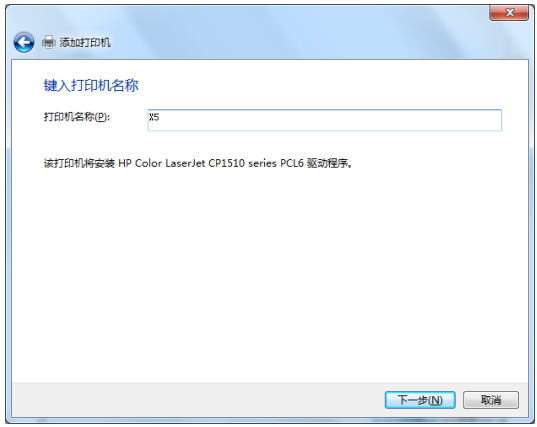
6、 选择设备类型为标准的 Generic Network Card,点击“下一步”；



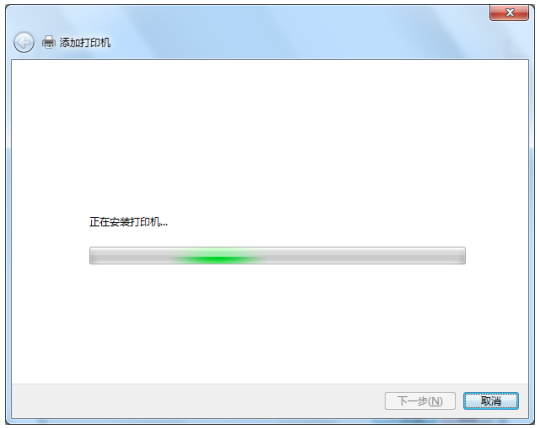
7、 完成端口添加后为打印机安装驱动，选择正确的打印机驱动，如果没找到对应型号，可以从磁盘手动添加驱动文件选择“从磁盘安装”；



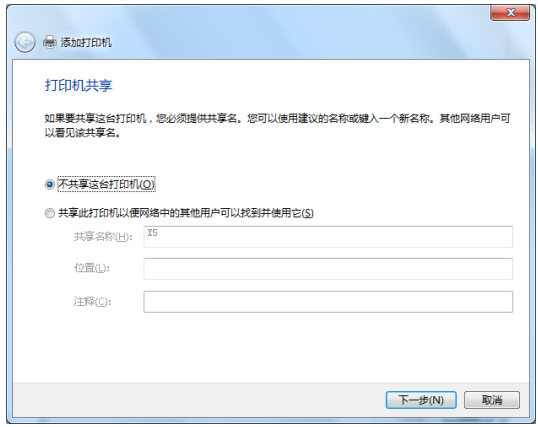
8、 设置打印机名称，点击“下一步”；



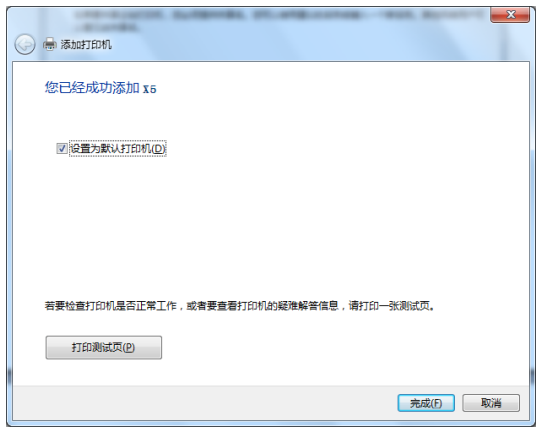
9、出现正在安装打印机；



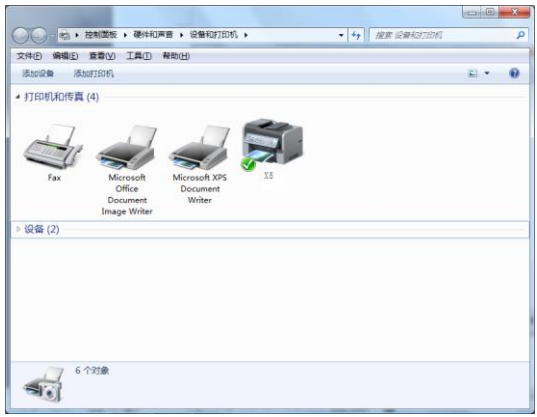
10、选择是否共享此打印机，请根据您的需要来设置是否共享打印机；



11、根据您的需要是否将将打印机设置为默认打印机，为确保您的打印机安装正确，选择“打印测试页”按钮打印测试页；



12、点击“完成”按钮完成添加；



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。

电子信息产品有毒有害物质申明

部件名称	有毒有害物质或元素					
	铅（pb）	汞（Hg）	镉（Cd）	六价铬（Cr6+）	多溴联苯（PBB）	多溴二苯醚（PBDE）
结构件	×	○	○	○	○	○
单板/电路模块	×	○	○	○	○	○
电源适配器	×	○	○	○	○	○
线缆	×	○	○	○	○	○
连接器	×	○	○	○	○	○
附件	×	○	○	○	○	○

1. “○”表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T11363-2006标准规定的限量要求以下。
2. “X”表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T11363-2006标准规定的限量要求。
3. 由于中国限量标准中没有豁免条例，故标识为“X”并不一定表示为对人体有害。
4. 对生产制造的产品，可能包含这些欧洲豁免的物质。
5. 在所售产品中可能包含所有部件也可能不包含所有部件。

免责声明：此为工业级产品，非用户端设备。在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对干扰采取切实可行的措施。