# BiPAC 6200NXL

## 3G/802.11n 无线宽带路由器

# 用户手册

发行版本: 1.00d-1

最后修改时间: 2009.9

# 目录

# 第一章: 产品入门

## 产品介绍

欢迎使用 BiPAC 6200NXL 路由器。这是一款多合一的路由器，包括宽带路由器，以太网交换机和 USB 端口，可以满足您使用 3G 连接到 Internet 的需求。

BiPAC 6200NXL 支持 3G, PPPoE, DHCP 和使用固定 IP 地址，用以连接到 ISP。

BiPAC 6200NXL 提供了完美的解决方案让几个PC 连接到高速的宽带Internet，使得多个用户可以同时享用高速的Internet 接入。

这款路由器还可以用作 Internet 防火墙，可以保护您的网络防止外界非授权的用户访问。它不仅仅支持网络地址转换（NAT）的基本防火墙功能，还支持高级的防火墙功能以保护您的网络。所有进入的数据包都将被监控和过滤。您还可以配置路由器阻挡用户访问Internet。

BiPAC 6200NXL 支持两种安全级别。首先，它使得Internet上的外部用户无法看见LAN IP地址，所以就更难让网络中的设备成为黑客的攻击目标。其次，它可以阻挡和重定向某些端口以限制外部用户访问的服务。若要确保游戏和其它Internet应用可以正常运行，您必须为外部用户打开特定的端口以便让其访问内部网络的服务。

在路由器启动后，集成的DHCP（动态主机控制协议）客户端和服务器功能可以让用户自动获取IP地址。只需要把本地计算机设置成DHCP客户端就可以动态获取从DHCP服务器分配的IP地址。只要本地计算机的电源是开着的，路由器就可以识别它然后分配一个IP地址给它让其立即连接到LAN。

对高级用户来说，虚拟服务器（端口映像）功能可以对外部用户开放有限可见的端口使得本地计算机可以提供专门的服务。例如，一台专业的Web服务器可以通过路由器连接到Internet，然后路由器接收入站的Web页面请求并重新路由到本地的Web服务器，即使服务器拥有不同的IP地址。

虚拟服务器还可以用于分配多台服务器的服务。例如，您可以设置路由器支持独立的 FTP，Web 和多玩家游戏服务器分享同一个Internet 可见的IP 地址，同时也能够保护服务器和LAN用户防止黑客入侵。

# 功能特性

### 3G

基于 3G 的 Internet 连接（需要一个 3G USB 调制解调器），具有自动故障切换功能，保证出现 Internet 服务故障时仍保持 Internet 连接。基于 web 浏览器的配置可以简化安全 WLAN 的设置，不论您在办公桌旁还是旅途中，只要可以使用 3G，就能随时访问 Internet。

### 支持 WPA 的 802.11n 无线 AP

路由器中集成了 802.11n 无线接入点，可以在有线网络，无线网络和宽带连接之间进行简单快捷地接入，使用户拥有了单一设备的简单性和灵活性。除了支持 300 Mbps 的 802.11n 标准以外，还能够向下兼容现有的支持 802.11g 和 802.11b 标准的设备。支持的无线网络安全存取(WPA)和无线对等加密(WEP)功能加强了数据保护的安全级别和无线局域网的访问控制。

### 快速以太网交换机

集成的 3 个端口 10/100Mbps 快速以太网交换机可以在 10Base-T 和 100Base-TX 端口的 MDI 和 MDI-X 之间自动切换，自动侦测后允许您使用直通线或交叉线。

### EWAN

除了通过 3G 可以连接到 Internet， BiPAC6200NXL 还可以把 LAN 1 端口当作 WAN 端口，用于连接光纤线缆。这样的选择性，给用户以更加快速而灵活的方式去连接 Internet。

### USB 服务器

BiPAC 6200NXL 提供了两个 USB 2.0 端口，设备除了可以使用户共享有线网络还可以共享基于 3G 的无线网络连接。USB 端口还可以连接打印机，网络摄像头和硬盘，通过 USB 端口 BiPAC 6200NXL 就可以作为一个多功能服务器，帮助您组建一个自己的网络。您可以使用在办公室网络中的打印机，通过网络摄像头监测家中的每个角落，与同事或者朋友共享文件,甚至在您出行的时候还可以下载或者上传或者下载 FTP 或者 BT 文件。如果您想兼顾企业办公、家庭安全以及个人娱乐，内置 USB 端口的 BiPAC 6200NXL 可以满足您的需求。

### 3G 管理中心

通过 BiPAC 6200NXL 可以很容易的监控 3G 连接状态。 Billion 3G 管理中心是一款独特的基于 Web GUI 的实用工具，为用户提供了可视的 3G 信号状态页面，使用连接速度尽可能的最

大化。用户还可以监测当前上传可下载所占的带宽，同时此工具还记载了 3G 上网每月使用的总的小时数和总的数据流量，方便用户管理 3G 的包月上网服务。BiPAC 6200NXL 提供的 Web 配置界面使用户安装及网络管理更加简便。内置 DHCP 客户端与服务器端，系统管理员可以轻松地利用现有的网络，管理和分配 IP 地址。

### 用多协议建立连接

BiPAC 6200NXL EWAN 功能支持 PPPoE, DHCP 和使用固定 IP 地址，用以连接到 ISP。

### 通用即插即用(UPnP)和 UPnP NAT *TRA*versal

此协议用于在不同厂商的独立设备和 PC 之间建立简单健全的连接，使网络的安装变得简单而可以普及。除了在网络设备之间控制和数据传输之外，UPnP 体系结构还利用了 TCP/IP 和 Web 启用了邻近组网。启用这个功能，您可以无缝地连接到 NetMeeting 或 MSN Messenger。

### 网络地址转换

网络地址转换(NAT)允许多个用户同时使用一个 IP 地址/一个 Internet 帐户访问外部资源。其支持多个应用层网关(ALG)，例如 Web 浏览器，ICQ，FTP，Telnet，E-mail，News，Net2phone，Ping，NetMeeting，IP 电话和其它。

### 防火墙

NAT 技术支持了简单的防火墙功能，并且提供了阻挡外部 Internet 访问的选项，如 Telnet，FTP，TFTP，Web，SNMP 和 IGMP。

### 域名解析系统中继

域名解析系统(DNS)中继提供了简单的方法映射一个用户友好的域名，如www.google.com到一个IP地址。当本地计算机设定把DNS服务器设定成路由器的IP地址，那么每个从PC到这个路由器的DNS转换请求包都会被转发到外部网络的真实DNS。

### 动态域名解析系统 (DDNS)

动态DNS服务允许您给动态IP地址映像一个静态主机别名。动态IP地址就是WAN接口的IP地址。若要使用这个功能，您必须先从DDNS服务那儿申请一个账户，如 http://www.dyndns.org/.

### 以太网上的 PPP (PPPoE)

BiPAC 6200NXL 内置的 PPPoE 客户端功能用于建立连接。在分享相同的 ISP 账户并为此支付费用的时候，您不需要更改操作观念就可以获得更高的访问速度。而且本地计算机不需要安装 PPPoE 客户端软件。其还支持自动重新连接和超时断开(空闲时间)功能。

### 服务质量(QoS)

QoS 可以让您使用路由器完全控制哪种出站数据流能够优先，以确保重要数据，如游戏包，客户信息或管理信息以闪电般的速度通过路由器，甚至在高负载下也可以实现。QoS 功能可以配置的信息包括内部 IP 地址，外部 IP 地址，协议和端口。您可以限制通过路由器的不同类型的出站数据流的速度，以确保 P2P 用户不会使上传带宽拥塞或在不会给办公室的用户浏览网页造成停顿。另外，或许您可以仅仅改变上传数据的不同类型的优先级，然后让路由器找出它们实际的速度。

### 虚拟服务器

您可以指定哪些服务对外部用户是可见的。路由器侦测入站的服务请求，然后转发到指定的本地计算机。例如，您可以让 LAN 中的 PC 作为内部的 Web 服务器，并把它暴露在外部网络上。外部用户可以在 Web 服务器上直接浏览，然后却是受 NAT 保护的。一个 DMZ 主机设定可以把本地计算机暴露在外部 Internet 网络上。

### 动态主机控制协议(DHCP)客户端和服务器

在 WAN 端，DHCP 客户端可以从 Internet 服务提供商(ISP)自动获取 IP 地址。在 LAN 端，DHCP 服务已分配一个客户 IP 地址范围，包括子网掩码和 DNS 的 IP 地址，并把他们分发到本地计算机。这提供了一个简单的方式管理本地 IP 网络。

### 丰富的包过滤功能

这个功能基于 IP 地址和端口号过滤数据包。过滤来往 Internet 的数据包，提供了高级别的安全控制。

### 基于 Web 的 GUI

基于 Web 的 GUI 提供了简单的配置和管理。还支持为远程用户配置和管理设备用的远程管理功能。

### 可升级的 Firmware

您可以通过基于 Web 的 GUI 把路由器升级到最新的 Firmware 版本。

# 第二章: 产品概述

BiPAC 6200NXL 是一款支持 3.75G 和 802.11n 的无线宽带路由器。这是一款多合一的路由器，可以使 SOHO 或者办公用户在家中、办公室或者旅途中自由的享受安全、高速、便捷的 Internet 连接。因为集成了 USB 2.0 端口, 设备除了可以使用户共享有线网络还可以使用户共享基于 3G 的无线网络连接。

随着 3G 标准日益普及，通过 BIPAC6200NXL 通信变的越来越方便和实用，您可以将 3G USB 调制解调器连到 BiPAC 6200NXL 内置 USB 端口，使您能够通过 3.5G / HSDPA,3.75G / HSUPA, HSPA+,UMTS, EDGE, GPRS, 或者 GSM 网络连接到 Internet，其下行速度高达 14.4Mbps。您可以在路途中观看电影、下载音乐；在会议中或是在高速的跨国列车上，也可以查收电子邮件。内置的自动故障排除功能，确保了正在使用的有线连接连接失败时快速顺利的切换到 3G 网络，使 网络中断带来的损失最小化。当有线连接恢复时 BiPAC 6200NXL 又会自动切换到有线连接，最大限度的降低网络连接成本。

USB 端口还可以连接打印机，网络摄像头和硬盘，通过 USB 端口 BiPAC 6200NXL 就可以作为一个多功能服务器，帮助您组建一个自己的网络。您可以使用在办公室网络中的打印机，通过网络摄像头监测家中的每个角落，与同事或者朋友共享文件,甚至在您出行的时候还可以下载或者上传或下载 FTP 或者 BT 文件。如果您想兼顾企业办公、家庭安全以及个人娱乐，内置 USB 端口的 BiPAC 6200NXL 可以满足您的需求。

路由器提供了一个 Ethernet WAN 端口, 因此 BiPAC 6200NXL 可以作为一个有线的 ADSL/Cable 调制解调器。同时配备一个可选的 12V 车载电源线，将电源线连接到车载电源为 BiPAC 6200NXL 供电，即使您开车在路途中网络连接也不受任何限制。 同时您可以通过 Billion 的增值应用程序-3G 管理中心随 时监测 3G 的连接状态。

路由器内置了支持 802.11n 草案的无线接入点，这款路由器可以达到以往支持 802.11b/g 设备 6 倍的速率以及 3 倍的覆盖。接入速率高达 300Mbps，因此家中或者办公室中的任何地方都可以进行无线存取。无线保护接入(WPA-PSK / WPA2-PSK)和无线对等加密(WEP)功能加强了数据保护的安全级别和无线局域网的访问控制。这款路由器还支持 Wi-Fi 保护设置(WPS)标准，只需轻点一个按键就可以让用户建立一个安全的无线网络. 如果你的网络需要更大的覆盖，内置无线中继功能(WDS)不需要电线或光缆可以帮你实现。多个 SSID 允许用户从一个接入点访问不同的网络，网管可以为每个 SSID 分配不同的权限和功能，增加了网络结构的灵活性和效率。然而，请记住墙壁、屋顶或其它物体的数量，厚度和位置影响会影响穿过的无线信号。

保证 BiPAC 6200NXL 和其它网络设备之间的墙壁和屋顶的数量最小化——每堵墙壁或每个屋顶都可以减少无线产品 3-90 英尺（1-30 米）的覆盖范围。

把设备放置在最少数量墙壁或屋顶的地方。要知道在网络设备之间是直线的。把设备放置在可以直接（而不是有角度地）发送信号通过墙壁或屋顶的地方，以便更好地接收。建筑材料会阻挡无线信号——一扇金属门或铝制饰钉可能会对覆盖范围有所影响。

尝试放置无线设备和装有无线适配器的计算机，让信号可以穿过干燥的墙壁或打开的门而不是其它材料。让您的设备远离产生极大 RF（电波频率）噪声的电子设备（至少 3-6 英尺或 1-2 米）。

# 产品使用注意事项

警告

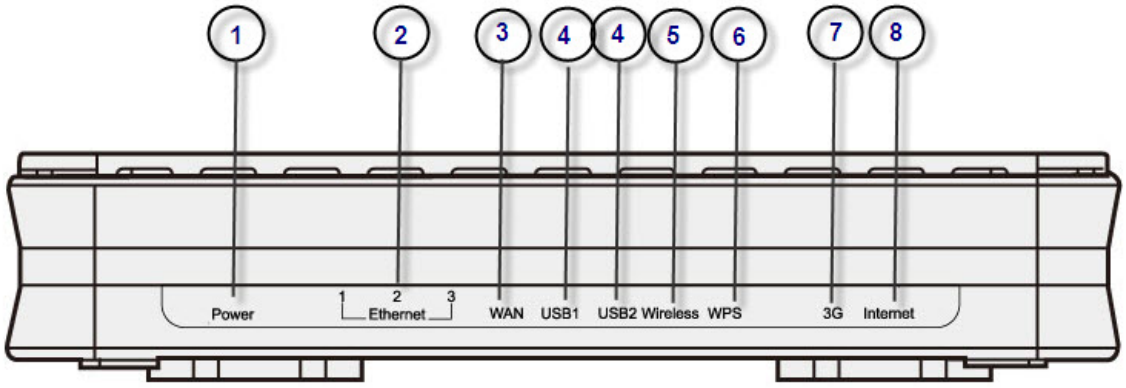
- 不要在高湿度或高温度环境中使用路由器。
- 不要让路由器和其它设备共享相同的电源。
- 不要自己打开或维修设备。如果路由器太烫了，请立即关掉电源然后把它送到有资质的服务中心去维修。
- 避免在户外使用产品和其附件。

# 产品列表

- **BiPAC 6200NXL 3G** 无线路由器
- 包含在线手册的 **CD-ROM**
- 以太网 **(CAT-5)** 线缆
- 电源适配器
- 快速安装向导
- 天线 **(2** 件**)**

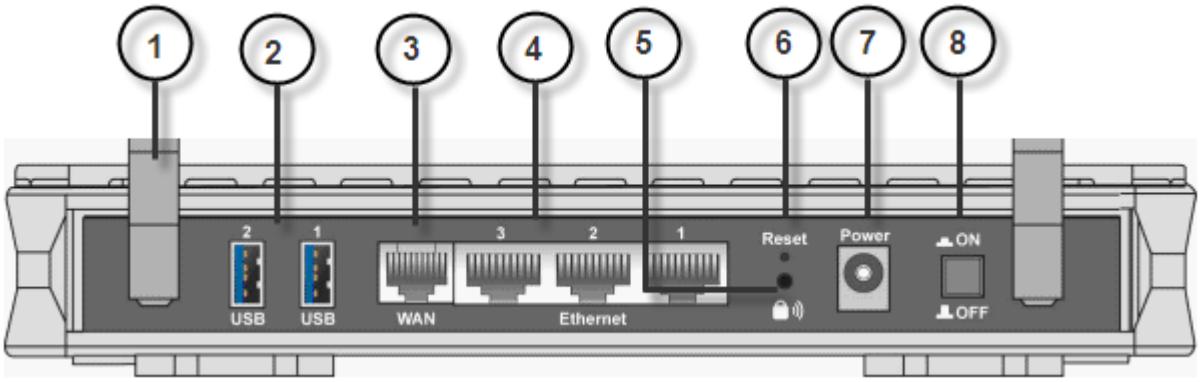
# 设备描述

## 前端面板的 LED




| LED | | 描述 |
|---|---|---|
| 1 | **Power** | 当电源插上的时候灯是橙色；<br>当系统就绪的是时候灯是绿色；<br>红灯亮表示系统出现故障。<br>重启设备或联系 Billion 以获得技术支持。 |
| 2 | **Ethernet Port** | 其中一个 LAN 端口连接到以太网设备时灯亮。<br>绿灯表示传输速度达到 100Mbps；<br>橙色灯表示传输速度达到 10Mbps；<br>灯闪表示正在传输/接收数据。 |
| 3 | **WAN** | 连接到 modem 或光纤 modem 灯为绿色。 |
| 4 | **USB** | 设备连接到 USB 设备时灯为绿色。<br>闪烁表示正在发送/接收数据。（USB1 和 USB2 无区别） |
| 5 | **Wireless** | 当已建立无线连接的时候灯是绿色。<br>灯闪表示正在发送/接收数据。 |
| 6 | **WPS** | 当 WPS 在运行时会闪烁 |
| 7 | **3G** | 当接收到 3G 信号时灯为红色。<br>绿灯表示拨号成功。<br>当设备成功获取 IP 地址时 Internet 灯亮。 |
| 8 | **Internet** | 绿灯表示 WAN 端口成功获得 IP 地址；<br>绿灯闪烁表示 WAN 端口成功获得 IP 地址并且有流量通过设备；<br>红灯表示 WAN 端口无法获得 IP 地址；<br>灯不亮表示设备处于桥接模式或 WAN 连接不存在。 |

## 后端面板的端口




| | | |
|---|---|---|
| **1** | **Antenna** | 连接到可拆分的天线。 |
| **2** | **USB** | 连接 USB设备。<br>插入 3G/ HSDPA USB modem 以便访问 Internet；<br>亦可连接打印机，网络摄像头和硬盘，使路由器作为网络中共享的打印机服务器，网络摄像头服务器和FTP服务器。（USB1和USB2无区别。） |
| **3** | **WAN** | 10/100M Ethernet 端口 (支持自动跨越);<br>连接 调制解调器。 |
| **4** | **Ethernet** | 连接一根 UTP 以太网线缆（Cat-5 或 Cat-5e）到四个 LAN 接口中的一个，把另一端连接到 PC 或 10Mbps/100Mbps 的办公室/家庭网络。 |
| **5** | **WPS** | 按下 WPS 键去触发 WPS 功能。 |
| **6** | **RESET** | 保证设备已经打开，按 RESET 按钮：<br>**1-3 秒钟：**快速重设设备。<br>**超过 6 秒钟，设备断电后再次通电：**恢复到出厂默认设置。（无法登录到路由器或忘记用户名/密码。按住 RESET 按钮超过 6 秒钟）。<br>**注意：**按住 RESET 按钮超过 6 秒钟后，保证设备再次通电。 |
| **7** | **Power** | 用于连接电源适配器的插孔。 |
| **8** | **Power Jack** | 电源开关。 |

# 布线

引起问题的最常见原因之一：线缆或 Ethernet 线使用不当。确保所有连接的设备是打开的。在产品的前端面板是一排 LED。确保 LAN Link 和 WAN Link  LED 是亮的。如果他们不亮，检查您是否使用的是合适的线缆。

# 第三章: 基本安装

可通过 web 浏览器配置路由器。Web 浏览器作为标准应用包含在以下操作系统中：Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista 等。该产品提供简单、易用、用户友好的配置界面。检查 PC 网络组件。必须安装 TCP/IP 协议栈和以太网卡。如果未安装，请参照与 Windows 或其他操作系统有关的手册。

要与路由器连接，可以通过外部中继器或集线器连接到路由器或直接与 PC 相连接。不过，在连接到路由设备前，确保您的 PC 上已正确安装了以太网接口。必须对 PC 进行配置以通过 DHCP 服务器获取一个 IP 地址或固定 IP 地址，IP 地址必须与路由器在同一子网中。路由器的默认 IP 地址是 192.168.1.254，子网掩码是 255.255.255.0（如，任何相连接的 PC 都必须在同一子网中，且 IP 地址范围在 192.168.1.1 ~ 192.168.1.253 之间）。最佳也最简单的方法是：将 PC 配置为使用 DHCP 从路由器自动获取一个 IP 地址。

如果在访问路由器时出现问题，建议您卸载 PC 上的防火墙软件，因为他们会造成不能访问路由器 IP 地址（192.168.1.254）的问题。用户应当自己决定如何更好地保护网络。

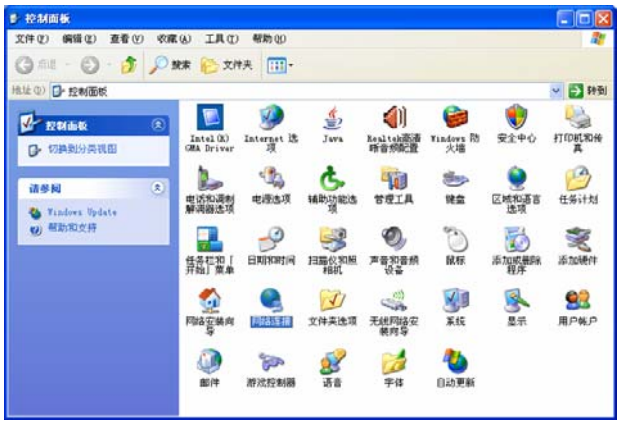
请按照以下的步骤在您的 PC 网络环境中进行安装。首先，检查您的 PC 网络的组件。TCP/IP 协议栈和以太网适配器必须正确安装。如果不是，请参考基于 Windows 或其它操作系统的手册。


任何装有 TCP/IP 的工作站都可以和或通过该产品通讯。
若要配置工作站的其他类型，请参考制造商提供的文档。

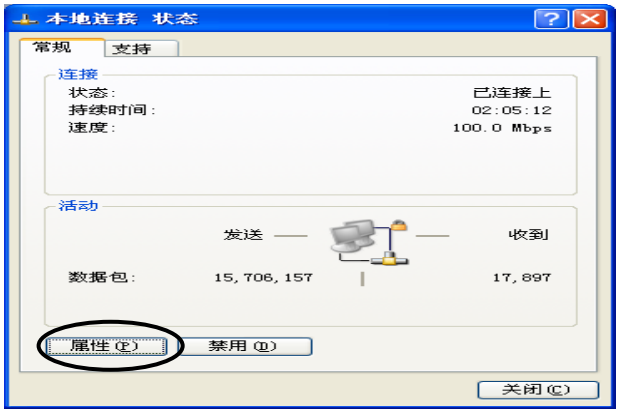
# 网络配置

## 在 Windows XP 中配置 PC

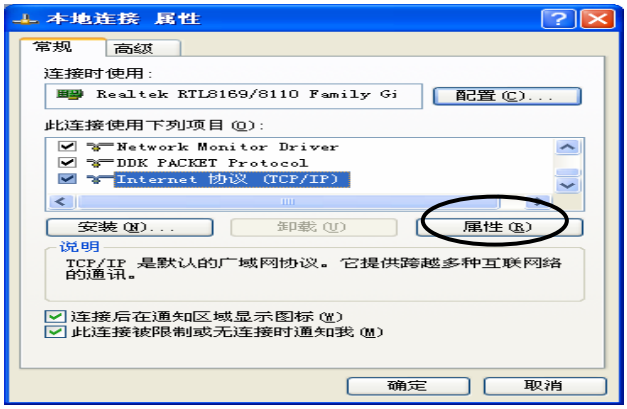
1. 点击**开始/控制面板**（经典视图）。在控制面板中，双击**网络连接**。
2. 双击**本地连接**。



3. 在**本地连接状态**窗口中，点击**属性**。

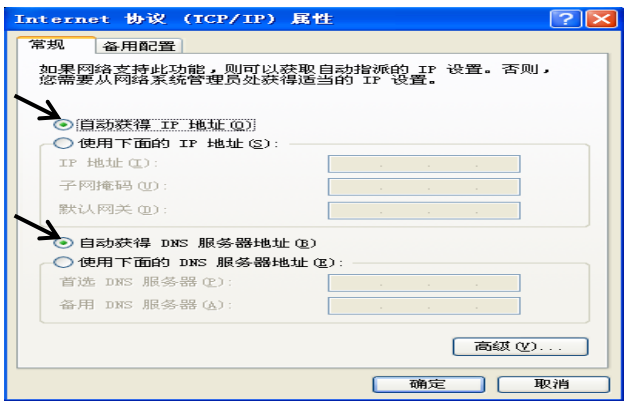



4. 选择 **Internet 协议(TCP/IP)** 并点击**属性**。



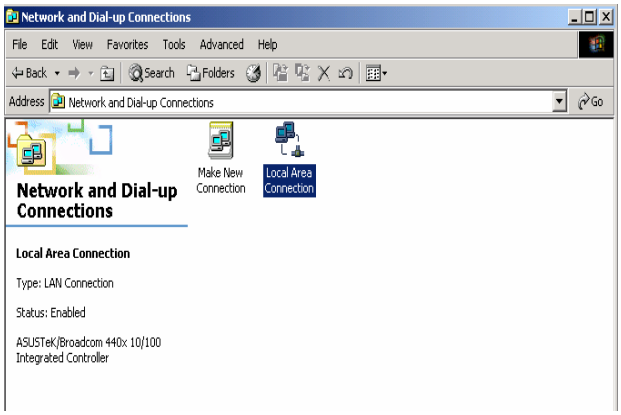

5. 选择**自动获得 IP 地址**和**自动获得 DNS 服务器地址**。

6. 点击**确定**完成配置。



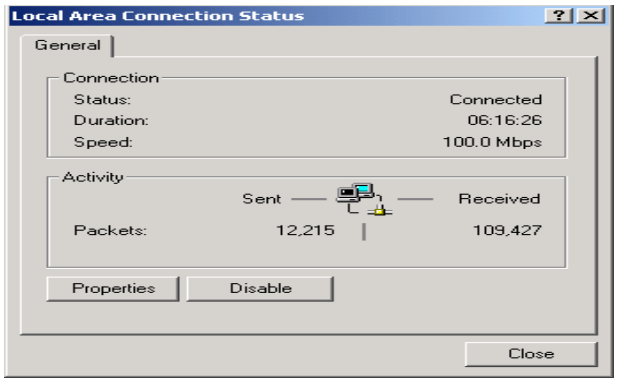
# 在 Windows 2000 中配置 PC

1. **开始/设置/控制面板**。在控制面板中，双击**网络和拨号连接**。

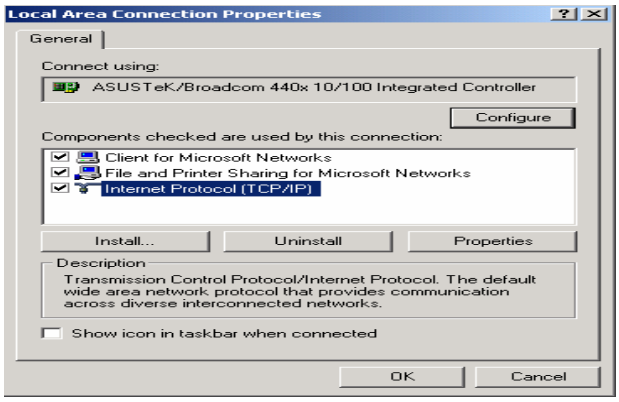



2. 双击**本地 (LAN) 连接**。

3. **本地连接状态**窗口中，单击**属性**。

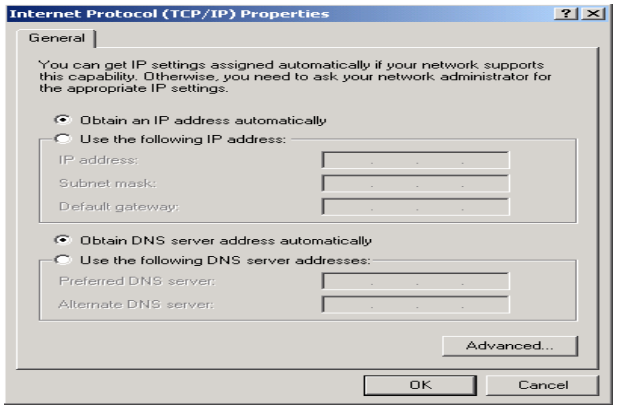



4. 选择 **Internet 协议 (TCP/IP)** 并单击**属性**。



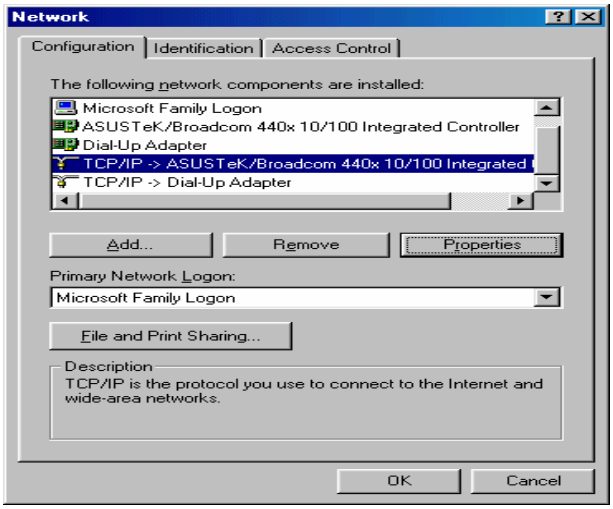

5. 选择**自动获得 IP 地址**和**自动获得 DNS 服务器地址**。

6. 单击**确定**完成配置。



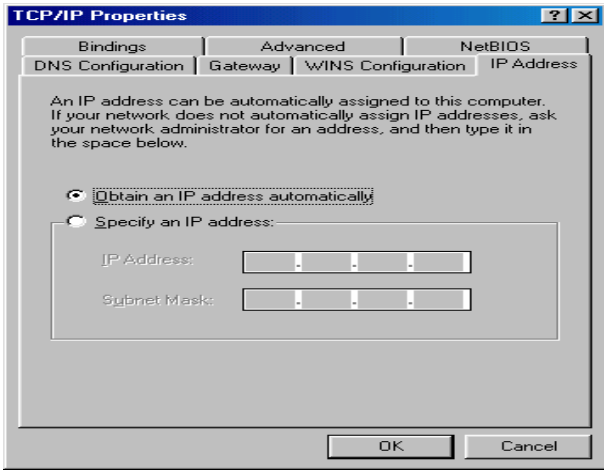
# 在 Windows 95/98/Me 中配置 PC

**1.** 转到**开始/设置/控制面板**。在控制面板中，
双击**网络**，然后选择**配置**选项卡。



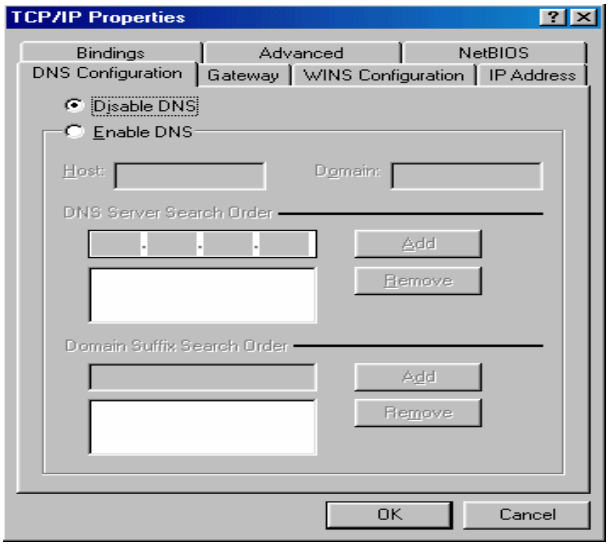

**2.** 选择 **TCP / IP -> NE2000 兼容**，或任何 PC 的
网卡名称。

**3.** 选择**自动获得 IP 地址**单选按钮。




**4.** 选择 DNS 配置选项卡。

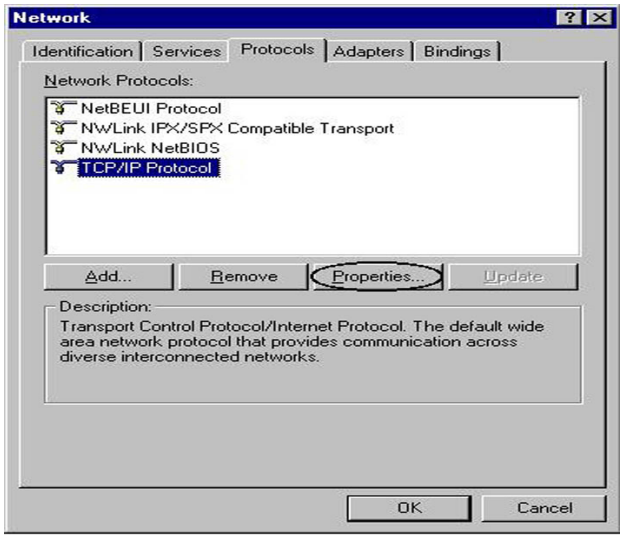
**5.** 选择**关闭 DNS** 单选按钮，然后单击**确定**，完成配置。



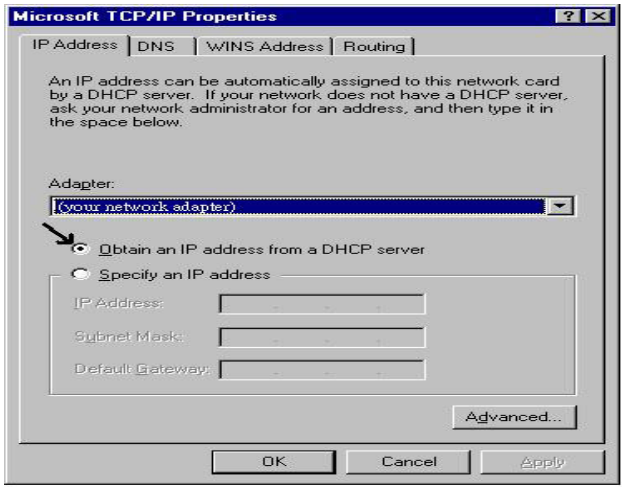
# 在 Windows NT4.0 中配置 PC

**1.** 转到**开始/设置/控制面板**。在控制面板中，
双击**网络**，然后选择**配置**选项卡。

**2.** 选择 **TCP/IP 协议**，然后单击**属性**。




**3.** 选择**通过 DHCP 服务器获得 IP 地址**单选按钮，然后单击**确定。**



# 出厂默认设置

在配置 BiPAC 6200NXL 以前，您必须知道下列默认设置。

### Web 界面（用户名和密码）

- 用户名： admin
- 密码： admin

默认的用户名和密码分别是 “**admin**”和 “**admin**”。

*注 意*

**如果您忘记登录路由器的用户名和密码，请按住 RESET 按钮 6 秒钟，然后松开让其恢复到出厂默认设置。**

**注意**：在按住 RESET 按钮超过 6 秒后松开，要确保设备重新启动。

### LAN 接口的 IP 设置

- IP 地址：192.168.1.254
- 子网掩码：255.255.255.0

### WAN 端的 ISP 设置

- PPPoE

### DHCP 服务器

- DHCP 服务器是开启的。
- 开始 IP 地址：192.168.1.100
- 地址池容量：100

### LAN 和 WAN 接口

LAN 和 WAN 接口的参数是厂商事先设置好的。默认值如下：

| **LAN 端口** | | **WAN 端口** |
|---|---|---|
| **IP 地址** | 192.168.1.254 | 启用 PPPoE 功能可以自动获得 ISP 提供的 WAN 接口配置。 |
| **子网掩码** | 255.255.255.0 | |
| **DHCP 服务器功能** | 在端口 1，2 和 3 中启用 | |
| **分配给 PC 的 IP 地址** | 100 个从 192.168.1.100 到 192.168.1.199 的 IP 地址 | |

# ISP的信息

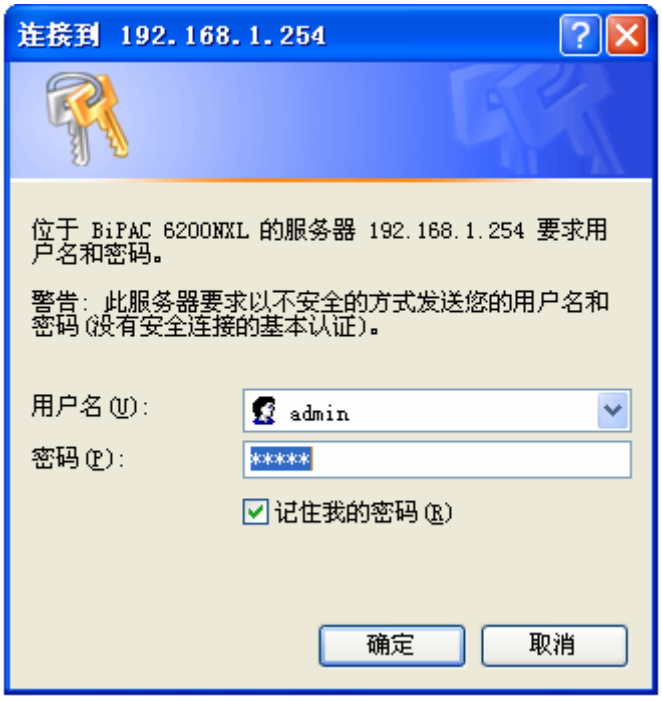
在配置设备之前，您必须检查您的 ISP（Internet 服务提供商）提供的服务种类，如 DHCP（自动获得 IP 地址）、静态 IP（固定 IP 地址）或 PPPoE。

获取下表中列出的信息作为参考。

| | |
|---|---|
| **PPPoE** | PPPoE (PPP over Ethernet)主要用于拨号服务。它将宽带服务融入到当前广泛的部署中，提供类似于使用 PPP 拨号服务的接入控制和计费功能。 |
| **DHCP(自动获取 IP 地址)** | 配置 WAN 端口使用 DHCP 客户端协议从您的 ISP 自动获取 IP 地址。您的 ISP 提供给路由器动态的 IP 地址。 |
| **静态 IP(固定 IP 地址)** | 配置 WAN 端口使用分配的静态 IP 地址。这个 IP 地址由您的 ISP 提供。 |

# Web 浏览器配置

打开 web 浏览器，输入路由器的 IP 地址，默认是 **192.168.1.254**，然后点击**转到**，随后出现提示输入用户名和密码的窗口。默认的用户名和密码是 **admin** 和 **admin**。




**恭喜！您已成功登录了 BiPAC6200NXL 路由器！**

# 第四章: 配置

通过配置页面左侧的导航栏，可以链接到所有配置页面。配置页面如下所示：

- **高级**（切换到高级配置模式）
- **状态**
- **快速启动**
- **WAN**
- **WLAN**

# 状态


**设备信息**

- **模块名称:** 用于识别的路由器名称。
- **系统运行时间：** 记录了系统运行的时间。
- **硬件版本：** 设备的硬件版本。
- **软件版本：** 固件的版本。

**端口状态**

- **端口状态：** 用户可以查看设备连接的以太网，3G 或无线的信息。

**WAN**

- **端口：** WAN 连接的名称。
- **协议：** PPPoE, DCHP 或者静态 IP
- **操作：** 当前可进行的操作。
- **连接：** 当前连接的时间。
- **IP 地址：** WAN 接口的 IP 地址。
- **子网掩码：** WAN 接口的 IP 子网掩码。
- **网关：** 输入默认网关的地址。
- **主用 DNS：** 主用 DNS 服务器的 IP 地址。

# 快速启动


## 配置无线网络


**无线局域网服务：**默认是**开启**的。

**ESSID:** ESSID 是无线接入点（AP）的唯一名称，可以区别于其它无线网络。为了安全的目的，要更改内置于路由器的无线 AP 的唯一 ID 名称。这是大小写敏感的，不能超过 32 个字符。确保您的无线客户端拥有设备准确的 ESSID，这样才能连接到网络中。

**通道 ID：** 选择您想使用的通道。

**安全模式：**您可以关闭或开启 WPA 或 WEP 保护您的网络。默认的无线安全模式是**关闭**。

# WAN

## EWAN


## 3G

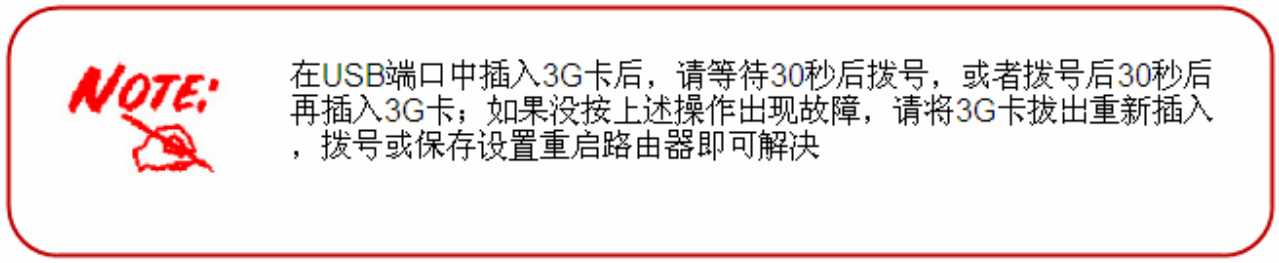

**APN:** APN 类似于 WWW 的 URL，是拨打 GPRS / UMTS 电话的设备。任何服务都可以连接到 APN，以建立数据连接。APN 分配的要求随服务提供商的不同而不同。大都数服务提供商都有一个连接到 DHCP 服务器的门户网站，通过它可以访问 internet。例如，有些 3G 运营商使用 APN ‘internet’ 作为他们的门户网站。APN 的默认值是 “internet”。

**用户名：**输入ISP提供的用户名。

**密码：**输入ISP提供的密码。

**鉴权协议:** 如果您知道服务器使用的认证类型，或者您希望客户端连接时使用您指定的认证类型（作为服务端时），可以手动指定 CHAP（挑战握手协议）或 PAP（密码认证协议）。使用 PAP 时，密码是未加密发送的；而 CHAP 会在发送前对密码进行加密，因为要确保客户端在不同时段都不会被入侵者取代。

**PIN:** PIN 代表个人识别号码。PIN 码是一个数值，在有些系统中作为密码进行登录和认证。在手机中，PIN 码是锁定 SIM 卡的，直到您输入正确的密码。如果连续三次输入的 PIN 码都不正确，SIM 卡将被锁定，必须使用网络/服务提供商提供的 PUK 码才能解锁。



# WLAN


● **无线局域网服务：**默认设定是**开启**的。

● **ESSID:** ESSID 是无线接入点（AP）的唯一名称，可以区别于其它无线网络。为了安全的目的，要更改内置于路由器的无线 AP 的唯一 ID 名称。这是大小写敏感的，不能超过 32 个字符。确保您的无线客户端拥有设备准确的 ESSID，这样才能连接到网络中。

**注意：**ESSID 是大小写敏感的，不能超过 32 个字符。

● **隐藏：**这个功能是当无线客户端在网络中搜索在空间中传输的 ESSID 的时候是否能够发现并识别路由器。默认值是**关闭**。

⊙ **开启：**如果您不想泄露您的 ESSID 就可以选择**开启**。选择**开启**以后，没有人可以发现您路由器的接入点(AP)。

⊙ **关闭：**选择**关闭**，您就可以允许任何有无线客户端的用户找到您路由器的接入点(AP)。

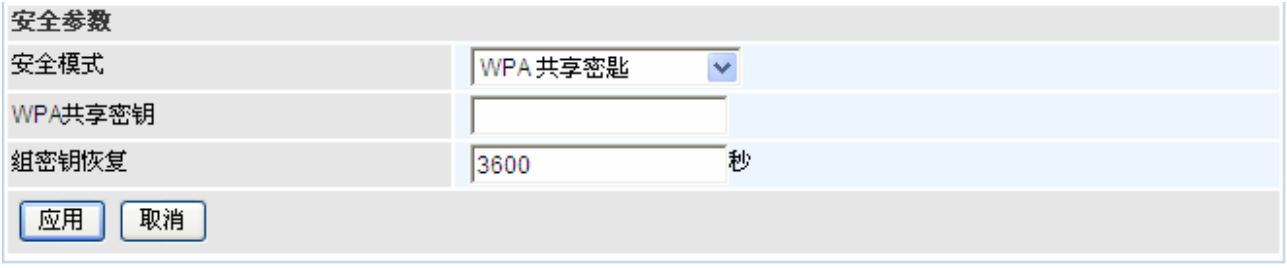
● **规则域：** 您可以在下拉选项种选择七种规则域，包括**北美**，**欧洲**，**法国**等等。不同的通道 ID 有不同的设置。

● **通道 ID：**选择您想使用的通道。

● **安全模式：**您可以关闭或开启 WPA 或 WEP 保护您的网络。默认的无线安全模式是**关闭**。

安全参数

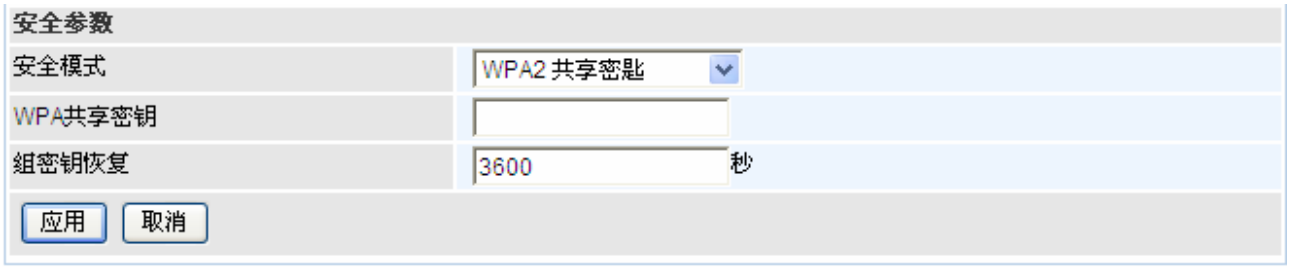
### WPA 共享密钥




**WPA 共享密钥：**这个密钥是用于网络认证。输入的格式是密钥的长度要在 8 到 63 个字符之间。

**组密钥恢复：**在无线客户端和接入点(AP)之间更改安全密钥的恢复周期。这个过程是自动的。

### WPA2 共享密钥




**WPA2 共享密钥：**这个密钥是用于网络认证。输入的格式是密钥的长度要在 8 到 63 个字符之间。

**组密钥恢复：**在无线客户端和接入点(AP)之间更改安全密钥的恢复周期。这个过程是自动的。

## WEP


**WEP 认证：**防止未授权的无线工作站访问网络上传输的数据，这种路由器提供的安全数据加密就是 WEP。如果您要求更高级别的安全性，下面有三个选项可以选择：**开放系统**，**共享密钥**或**双方**。

**默认使用的 WEP 密钥：**选择加密密钥 ID，请参考下面的密钥 1-4。

**Passphrase:** 基于输入的字符串自动生成 WEP 密钥，预定义的算法是 WEP64 或 WEP128。您可以在 AP 和客户卡设定中输入相同的字符串以生成相同的 WEP 密钥。请注意在开启 **Passphrase** 之后不要输入**密钥 1-4**。

**Key (1-4): 密钥 1-4：**输入无线数据加密的密钥。若要允许加密的数据传输，在所有无线工作站上的 WEP 加密密钥值必须和路由器上相同。这儿可以选择四个密钥。输入的格式是 Hex 或 ASCII，WEP64 和 WEP128 分别需要输入 5 和 13 个密码——不包含任何分隔符。

# 第五章: 高级配置

通过 web 浏览器登录了 BiPAC 6200NXL 路由器，您就可以开始根据要求配置了。 通过配置页面左侧的导航栏，可以链接到所有配置页面。配置页面如下所示：

- **基础** (切换到基础配置模式)
- **状态** (3G 状态， ARP 表， DHCP 表， 系统日志， 防火墙日志， UPnP 端口映射)
- **快速启动**
- **配置** (LAN， WAN，系统， USB 服务器， 防火墙， QoS， 虚拟服务器， 时间表， 从 LAN 唤醒 和高级)

下面的部分将介绍如何配置路由器。

# 状态


**设备信息**

- **模块名称：**设备的模块名称。
- **主机名称：**用于识别的路由器名称。可以在主机名称字段修改路由器名称。点击**主机名称**进入下面的界面。


- **系统运行时间：**记录了系统运行的时间。
- **当前时间：**设定当前时间。查看时区的部分获取更多的信息。
- **硬件版本：**设备的硬件版本。
- **软件版本：**固件的版本。
- **MAC 地址：**LAN 接口的 MAC 地址。

端口状态

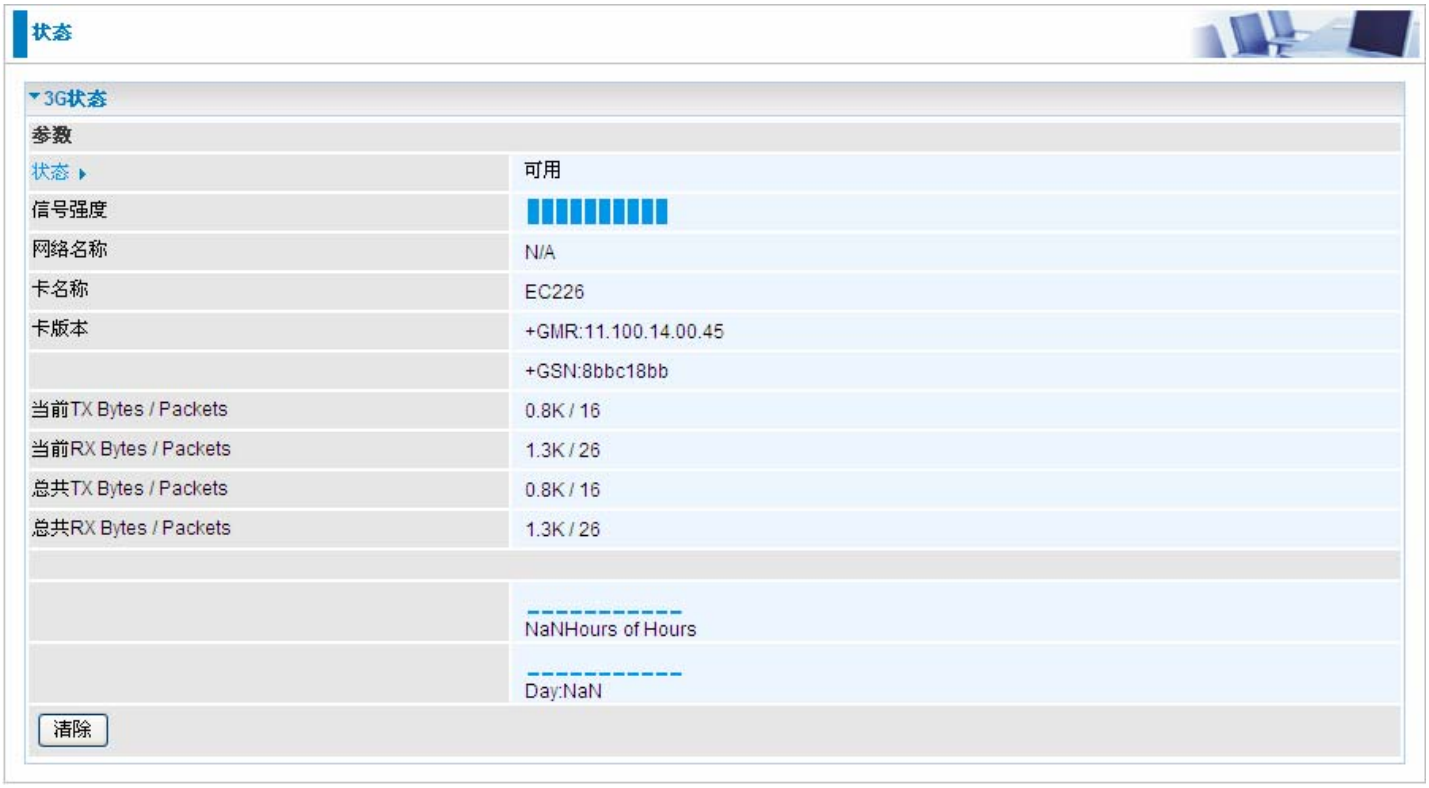
- **端口状态：**用户可以查询他们是否已连到以太网，EWAN，3G 或者无线网络。

**WAN**

- **端口：** WAN 连接的名称。
- **操作：** 当前可进行的操作。
- **连接：** 当前连接的时间。
- **IP 地址：**WAN 接口的 IP 地址。
- **子网掩码：**WAN 接口的 IP 子网掩码。
- **网关：**输入默认网关的地址。
- **主用 DNS：**主用 DNS 服务器的 IP 地址。

# 3G 状态

显示 3G 卡的所有状态信息，如当前信号强度、当前数据传输和总的数据传输的统计信息。




- **状态**：3G 卡的当前状态。
- **信号强度**：表示当前 3G 信号强度的信号强度条。
- **网络名称**：设备连接到的网路的名称。
- **数据卡名称**：3G 卡的名称。
- **数据卡固件版本**：3G 卡的当前固件版本。
- **当前 TX Bytes / Packets**：通话时传输数据的字节/数据包统计。
- **当前 RX Bytes / Packets**：通话时接收到数据的字节/数据包统计。
- **总共 TX Bytes / Packets**：系统就绪后，传输数据的总字节/总数据包统计。
- **总共 RX Bytes / Packets**：系统就绪后，接收到数据的总字节/总数据包统计。

# ARP 表

这部分将介绍 ARP（地址解析协议）表，显示 IP 地址与 MAC 地址之间的映射关系。这对于快速确定 PC 网络接口的 MAC 地址，并用作**防火墙 – MAC 地址过滤**功能是很有用的。参考本手册中的防火墙部分，获取更多信息。


- **IP 地址：**显示 LAN（局域网）设备的 IP 地址列表。
- **MAC 地址：**显示所有 LAN 设备的 MAC（介质访问控制）地址。
- **接口：**该 IP 地址连接到的接口名称（路由器）
- **静态：**ARP 表条目的静态状态。

  **“否”**表示动态生成的 ARP 表条目。

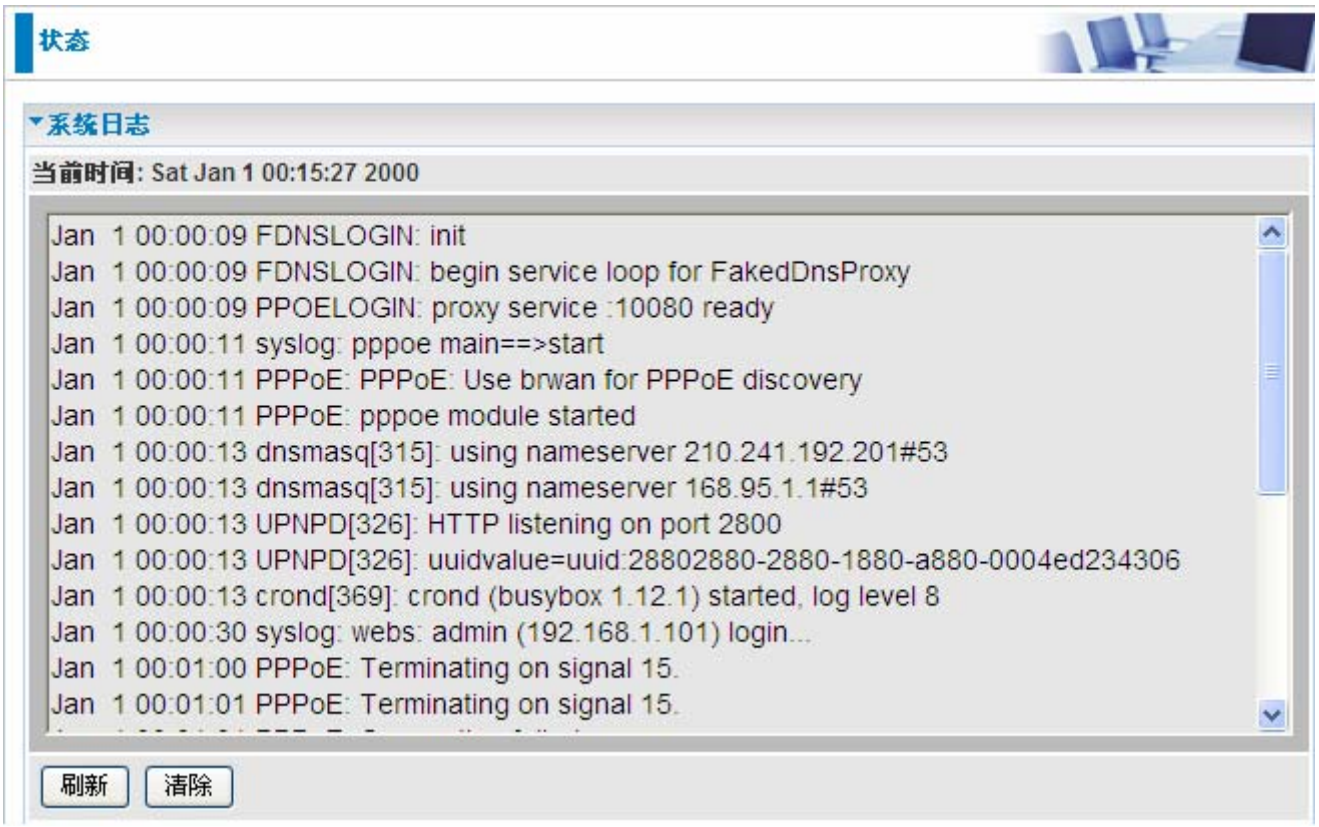
  **“是”**表示用户增加的静态 ARP 表条目。

# DHCP 表


- **IP地址：**设备当前DHCP服务器分配的IP地址。
- **MAC 地址：** 内部 DHCP 客户端的 MAC 地址。
- **客户端主机名称：** DHCP 客户端的主机名称。
- **注册信息：**注册的时间信息。

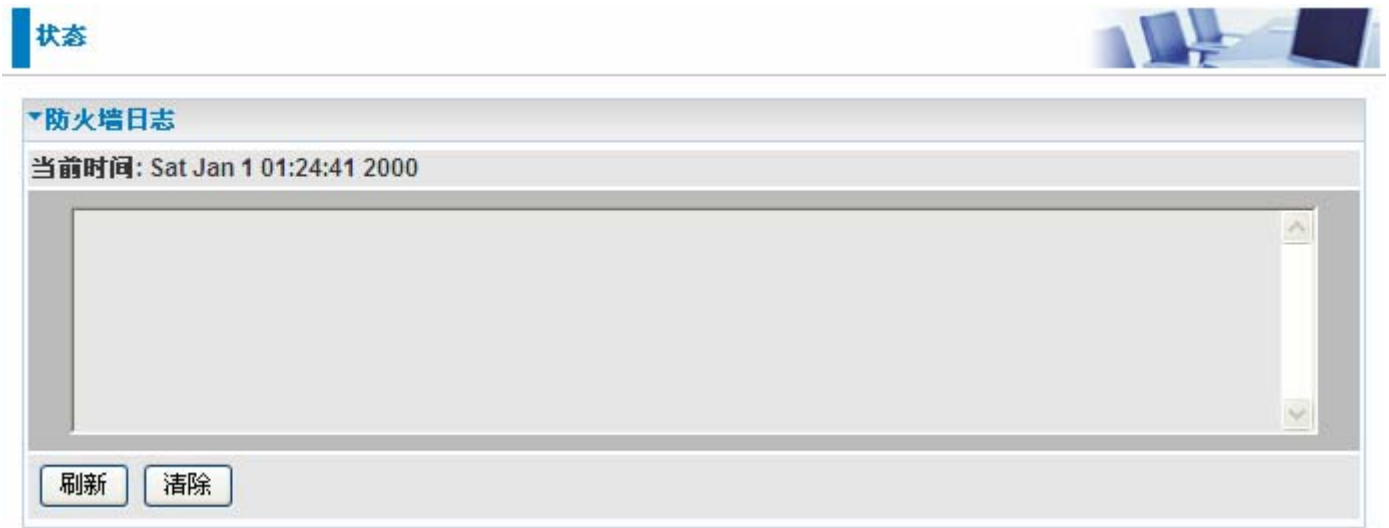
# 系统日志

显示当前所有的系统日志。您可以用这个功能查找历史信息。




# 防火墙日志

防火墙日志显示了所有防火墙不期望操作的日志信息。这个页面显示了防火墙日志的条目。日志将显示您在**配置-防火墙**中启用的入侵检测或阻塞 WAN PING 的日志条目。请参考本手册的**防火墙**部分获取启用防火墙日志的详细信息。



# UPnP 端口映射

这部分列出了所有使用 UPnP（通用即插即用）建立的端口映射。请参考本手册的高级部分获取更多 UPnP 和路由器 UPnP 配置选项的详细信息。

# 快速启动

**3G**


- **连接模式:** 3G
- **TEL No.:** GPRS / 3G 用户用来拨打网络互连电话的拨号串。由移动服务提供商提供。
- **用户名：**输入ISP提供的用户名。
- **APN:** APN 类似于 WWW 的 URL，是拨打 GPRS / UMTS 电话的设备。任何服务都可以连接到 APN，以建立数据连接。APN 分配的要求随服务提供商的不同而不同。大都数服务提供商都有一个连接到 DHCP 服务器的门户网站，通过它可以访问 internet。例如，有些 3G 运营商使用 APN ‘internet’ 作为他们的门户网站。APN 的默认值是 “internet”。

**EWAN**


- **连接模式:** EWAN
- **协议:** 设备当前使用的协议。

点击 **继续** 选择连接 EWAN 的协议 或者点击**转到无线网络设置**，使用协议：自动获得 IP 地址连接同时设置无线网络设置。

**自动获得 IP 地址**

当链接到 ISP 的时候，BiPAC 6200NXL 还可以作为一个 DHCP 客户端。如果 ISP 确定此信息通过 DHCP，BiPAC 可以自动获得一个 IP 地址，子网掩码，网关地址和 DNS 服务器地址。.


**协议:** 设备当前的 ATM 协议。

点击 **继续** 等待连接。


如果连接成功将会显示下面的画面

**固定 IP 地址**

选择此选项可以设置静态 IP 信息，您需要输入 ISP 提供给你的连接类型，IP 地址，子网掩码和网关地址。在这个区域中输入的必须是由圆点分隔成的 4 个 IP 字段的正确的 IP 地址形式(x.x.x.x)。如果不是这种形式路由器将不会接受这个 IP 地址。


- **协议：**设备当前的 ATM 协议。
- **IP：**您的 WAN 接口 IP 地址。保持 0.0.0.0 将自动从 ISP 获取 IP 地址。
- **子网掩码:** 默认是 0.0.0.0。用户可以更改称其它的，如 255.255.255.0。输入 ISP 分配的子网掩码。
- **网关:** 必须指定一个网关 IP 地址(ISP 提供)

点击 **继续** 等待连接


如果连接成功将会显示下面的画面

**PPPoE**

PPPoE（以太网上的 PPP）提供类似于使用 PPP 拨号服务的接入控制和计费功能。


- **协议：**设备当前的 ATM 协议。
- **用户名：**输入 ISP 提供的用户名。您可以输入最多 **128** 个字符（大小写敏感）。格式是“username@ispname”，而不是“username”。
- **密码：**输入 ISP 提供的密码。您可以输入最多 **128** 个字符（大小写敏感）。
- **服务名称：**这个字段用于鉴定。如果需要，您的 ISP 提供了这个信息。最多输入 15 个字符。
- **IP：**您的 WAN 接口 IP 地址。保持 0.0.0.0 将自动从 ISP 获取 IP 地址。
- **认证协议：**默认是**自动**。您的 ISP 可能会使用 **Chap** 或 **Pap**。

点击 **继续** 等待连接


如果连接成功将会显示下面的画面

## 设置无线属性


- **无线局域网服务：**默认是**开启**的。
- **ESSID：**ESSID 是无线接入点（AP）的唯一名称，可以区别于其它无线网络。为了安全的目的，要更改内置于路由器的无线 AP 的唯一 ID 名称。这是大小写敏感的，不能超过 32 个字符。确保您的无线客户端拥有设备准确的 ESSID，这样才能连接到网络中。
- **通道 ID：** 选择您想使用的通道。
- **安全模式：**您可以关闭或开启 WPA 或 WEP 保护您的网络。默认的无线安全模式是**关闭**。

# 配置

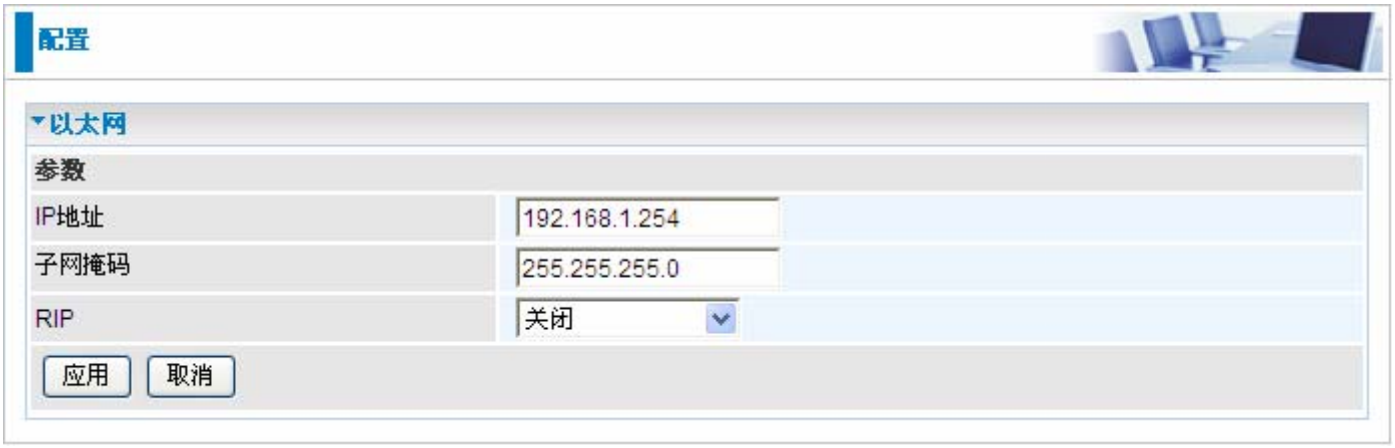
点击这个菜单可以访问以下子菜单配置 3G 路由器：**LAN**，**WAN**，**系统**，**USB**，**防火墙**，**QoS**，**虚拟服务器**，**从 LAN 唤醒**，**时间表**和**高级**。

以下部分介绍了这些功能。

## LAN (局域网)

局域网 (LAN)是许多计算机通过中间媒体相连分享通讯的系统，通常是在一幢楼或楼房的一层中使用。LAN 部分有 6 个选项：**以太网**，**IP 别名**，**无线**，**无线网络安全**，**WPS** 和 **DHCP 服务器**。

### 以太网




LAN 中的路由器支持多个以太网 IP 地址，您可以在同一时间从不同的 LAN 子网中访问 Internet。用户常常只有一个 LAN 子网。路由器的默认 IP 地址是 192.168.1.254。

- **IP 地址**：路由器的默认 IP 地址。
- **子网掩码**：路由器的默认子网掩码。
- **RIP**：RIP v1， RIP v2 Broadcast，RIP v2 Multicast 和 RIP v1+v2 Broadcast。

### IP 别名

允许在路由器上创建多个虚拟 IP 接口。可以用来连接两个或多个本地网络到 ISP 或远程节点。在这种情况下，不需要内部路由器。


- **IP 地址**：指定虚拟接口的 IP 地址。
- **子网掩码**： 指定虚拟接口的子网掩码。

# 无线


## 参数

- **无线局域网服务：**默认是**开启**的。

- **模式：**默认是 **802.11g+n**（混合模式)。如果您不知道或者同时拥有 802.11g 和 802.11n 设备，那么就保持默认值。如果您只有 802.11g 卡，那么从下拉选项中可以选择 802.11g。如果您只有 802.11b 卡，那么从下拉选项中可以选择 802.11b。如果您只有 802.11n 卡，那么从下拉选项中可以选择 802.11n。

- **活动的 SSID 数:** 您可以选择 SSID 号。

- **SSID No.:** 当前支持 SSID 连接的数目。

- **ESSID:** ESSID 是无线接入点（AP）的唯一名称，可以区别于其它无线网络。为了安全的目的，要更改内置于路由器的无线 AP 的唯一 ID 名称。这是大小写敏感的，不能超过 32 个字符。确保您的无线客户端拥有设备准确的 ESSID，这样才能连接到网络中。

注意：ESSID 是大小写敏感的，不能超过 32 个字符。

**隐藏：**这个功能是当无线客户端在网络中搜索在空间中传输的 ESSID 的时候是否能够发现并识别路由器。默认值是**关闭**。

⊙ **开启：**如果您不想泄露您的 ESSID 就可以选择**开启**。选择**开启**以后，没有人可以发现您路由器的接入点(AP)。

⊙ **关闭：**选择**关闭**，您就可以允许任何有无线客户端的用户找到您路由器的接入点(AP)。

**规则域：** 您可以在下拉选项种选择七种规则域，包括**北美**，**欧洲**，**法国**等等。不同的通道 ID 有不同的设置。

**通道 ID：**选择您想使用的通道。

**信道宽度:** 信道带宽选择 **20 MHz** 或者 **20/40 MHz** ， 带宽越高表现越好。

**Tx 功率发射强度：**加强无线传输信号强度的功能。用户可以调整的范围是 0-100。

注意：功率发射强度因用户假定接入网络的不同而不同，请选择适合您网络的强度。

**AP 的 MAC 地址：**访问点的硬件地址。

**AP 的版本：**访问点的固件版本。

**WPS 服务:** 开启/ 关闭

**WPS 状态:** 访问点的当前 WPS 状态。 它用于 WCN (Windows Connect Now).

⊙ **已配置:** 访问点已通过 WPS 进行配置。它不允许通过 WCN 配置。

⊙ **未配置:** 访问点未通过 WPS 进行配置。它可以通过 WCN 来配置。

**无线分配系统 (WDS)**

无线访问点模式开启了和其它访问点通讯的无线连接。这很容易安装，只要定义连接的 AP 的对等 MAC 地址就行。使用 WDS 很灵活并且节约成本，不需要在访问点之间架设无线客户端设备进行桥接就可以扩展有线或无线基础网络以创建一个大网络。

**WDS 服务：** 默认是**关闭**的。勾选**开启**可以激活该功能。

**1. WDS 点的 MAC 地址：**AP 的 MAC 地址。您的对等 AP 必须彼此包含双方 MAC 地址，以便彼此确认和通讯。

**2. WDS 点的 MAC 地址：**AP 的第 2 个 MAC 地址。

**3. WDS 点的 MAC 地址：**AP 的第 3 个 MAC 地址。

**4. WDS 点的 MAC 地址：**AP 的第 4 个 MAC 地址。

注意：MAC 地址必须包含分号(：)或破折号(—)。

## 无线网络安全

您可以关闭或开启 WPA 或 WEP 保护您的无线网络。默认的无线安全模式是**关闭**。


- **SSID：**选择您想设置的 SSID 编号。
- **安全模式：**共有 5 个选型可以选择。

### WPA 预共享密钥


- **WPA 算法：**TKIP（临时密钥完整性协议）/AES（高级加密标准）使用一个更加强大的加密算法和合并消息完整性编码(MIC)可以提供保护防止黑客入侵。
- **WPA 共享密钥：**网络认证的密钥。输入的格式是字符，密钥的大小应该在 8-63 个字符之间。
- **组密钥恢复：**自动在无线客户端和访问点(AP)更改安全密钥的恢复时间。

## WPA2 预共享密钥


**WPA 算法：**TKIP（临时密钥完整性协议）/AES（高级加密标准）使用一个更加强大的加密算法和合并消息完整性编码(MIC)可以提供保护防止黑客入侵。

**WPA 共享密钥：**网络认证的密钥。输入的格式是字符，密钥的大小应该在 8-63 个字符之间。

**组密钥恢复：**自动在无线客户端和访问点(AP)更改安全密钥的恢复时间。

## WEP


**WEP 认证：**防止未授权的无线工作站访问网络上传输的数据，这种路由器提供的安全数据加密就是 WEP。如果您要求更高级别的安全性，下面有三个选项可以选择：**开放系统**，**共享密钥**或**双方**。

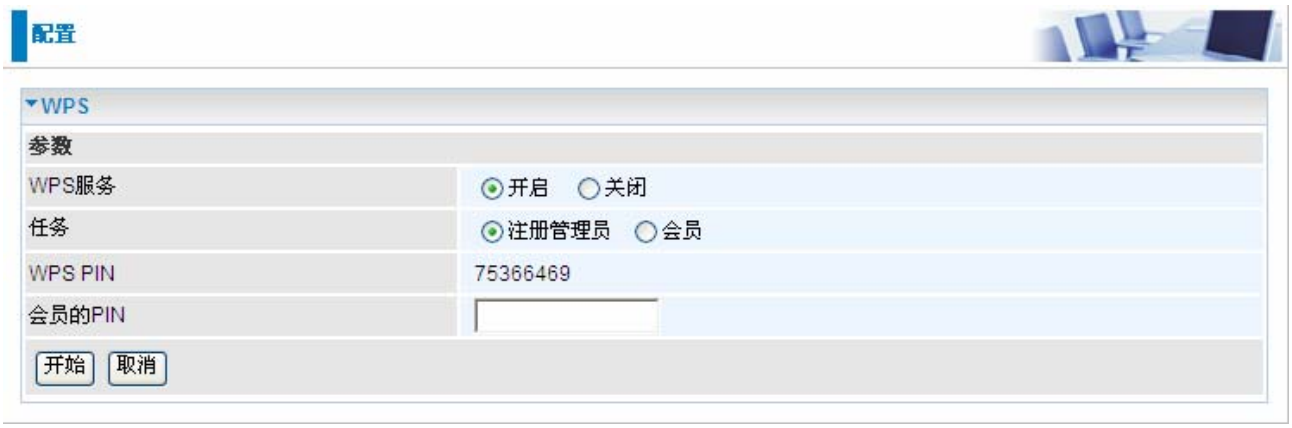
**默认使用的 WEP 密钥：**选择加密密钥 ID，请参考下面的密钥 1-4。

**Passphrase（产生密钥）：**基于输入的字符串自动生成 WEP 密钥，预定义的算法是 WEP64 或 WEP128。您可以在 AP 和客户卡设定中输入相同的字符串以生成相同的 WEP 密钥。请注意在开启 **Passphrase** 之后不要输入**密钥 1-4**。

**密钥 1-4：**输入无线数据加密的密钥。若要允许加密的数据传输，在所有无线工作站上的 WEP 加密密钥值必须和路由器上相同。这儿可以选择四个密钥。输入的格式是 Hex 或 ASCII，WEP64 和 WEP128 分别需要输入 5 和 13 个密码——不包含任何分隔符。

## WPS

WPS 的特点是遵循 Wi-Fi 联盟的标准，在家庭和小型办公环境中很方便的建立安全加密的 Wi-Fi 网络。减少了用户配置网络的一般步骤，并支持两种大多数消费者所熟悉的配置网络和启用安全密钥的方法。

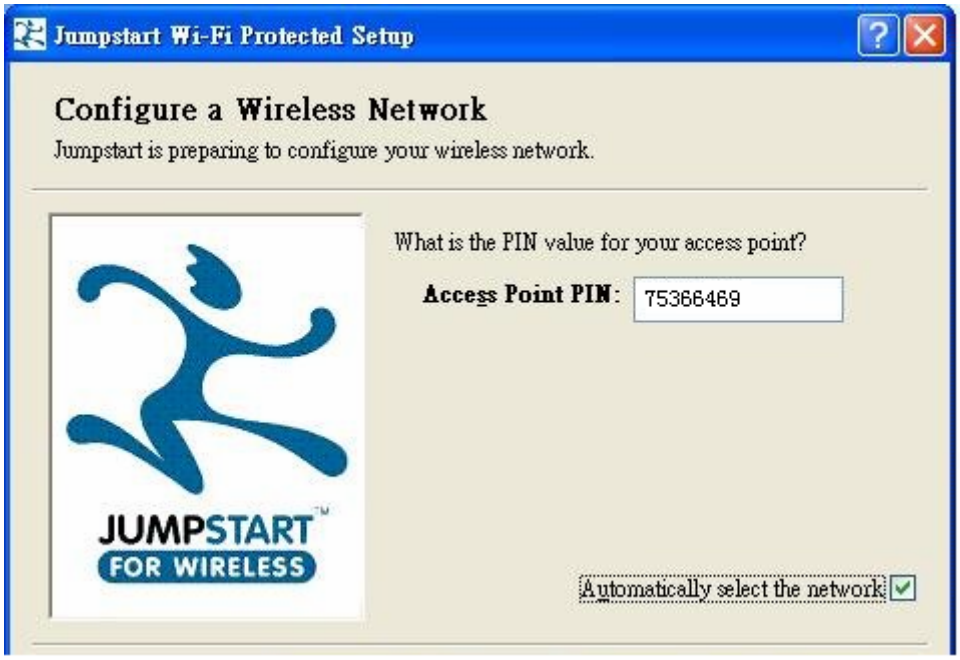


## 建立安全加密的 Wi-Fi 网络

**步骤 1:**记下接入点的 PIN 码(如：75366469)

**步骤 2:** 打开无线客户端应用程序(如： Atheros Jumpstart WPS utility), 选择“Configure a wireless network”点击“next”

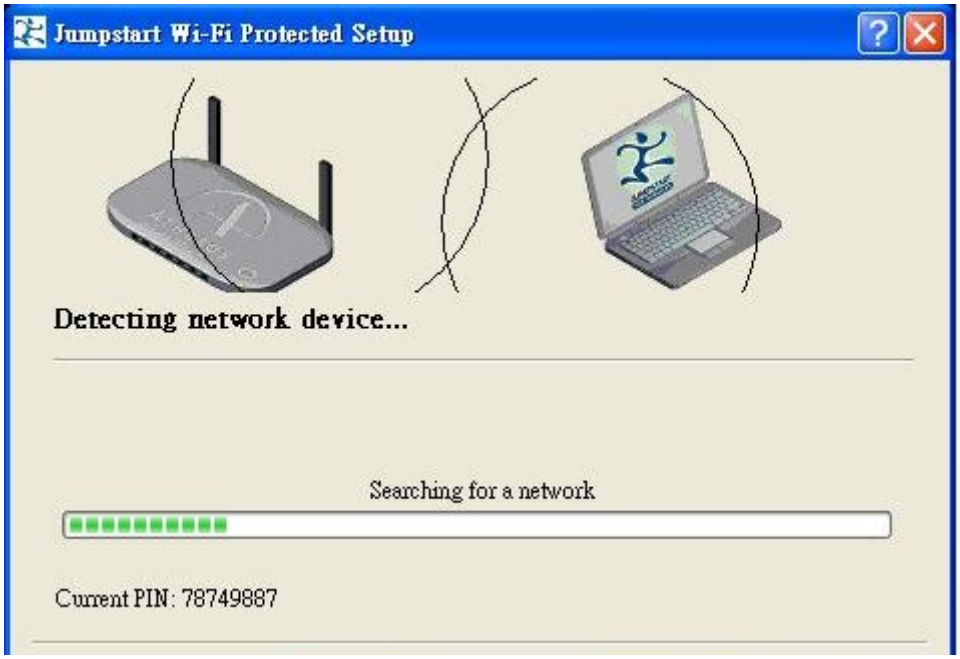

**步骤 3:** 输入接入 PIN 码点击“next”



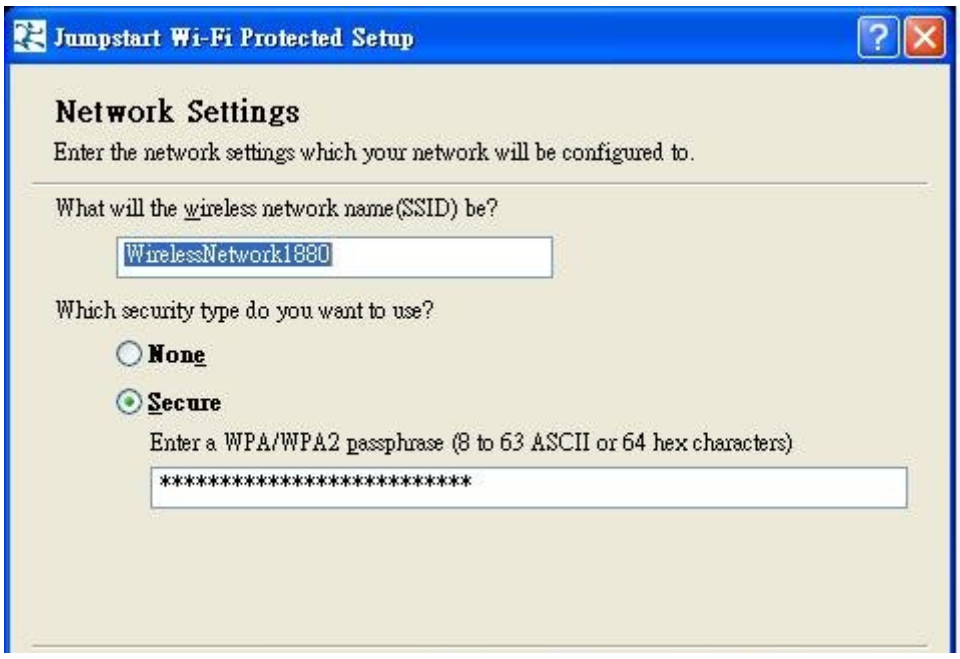

**步骤 4:** 为会员提供了两种连接 AP 的方法，您可以选择其中一种：

- 按下 WPS 按钮一秒钟后释放
- 在 WPS 配置页面，选择“会员”然后点击“开始”


**步骤 5:** Jumpstart WPS utility 搜索 WPS 接入点




**步骤 6: SSID** 和 **Secure** 会自动生成 (您可以更改)点击下一步



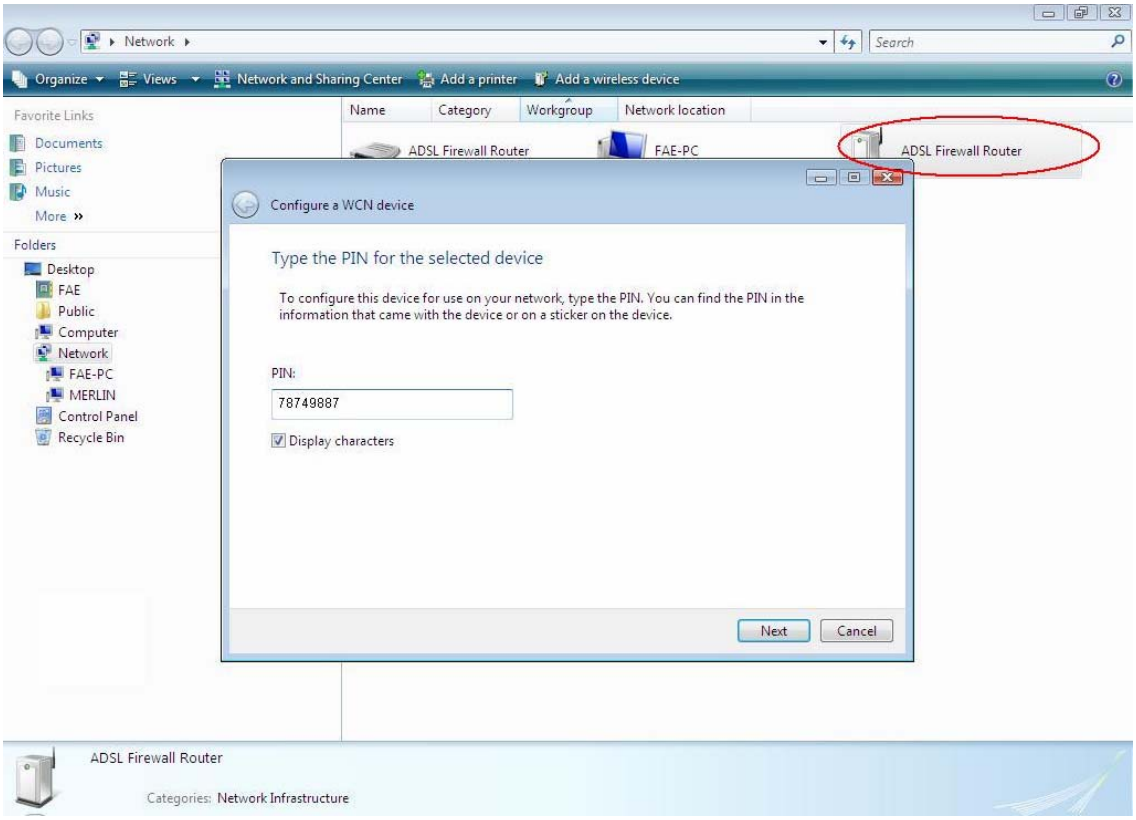
**步骤 7:** WPS 设置完成。您已经建立了安全加密的 Wi-Fi 网络

## 在 **Vista** 系统中用建立安全加密的 **Wi-Fi** 网络

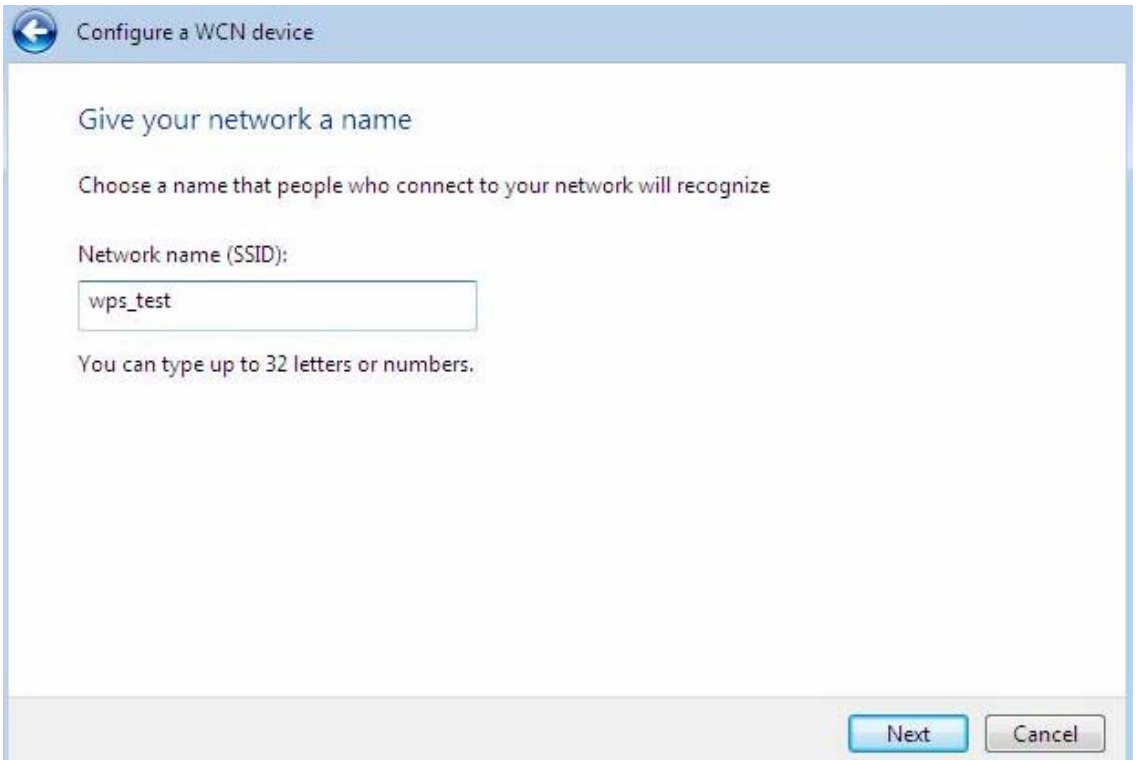
**步骤 1:** 记下 AP 的 PIN 码(如：75366469)

**步骤 2:** 在无线页面将 WPS 状态设置为“未配置”点击“应用”

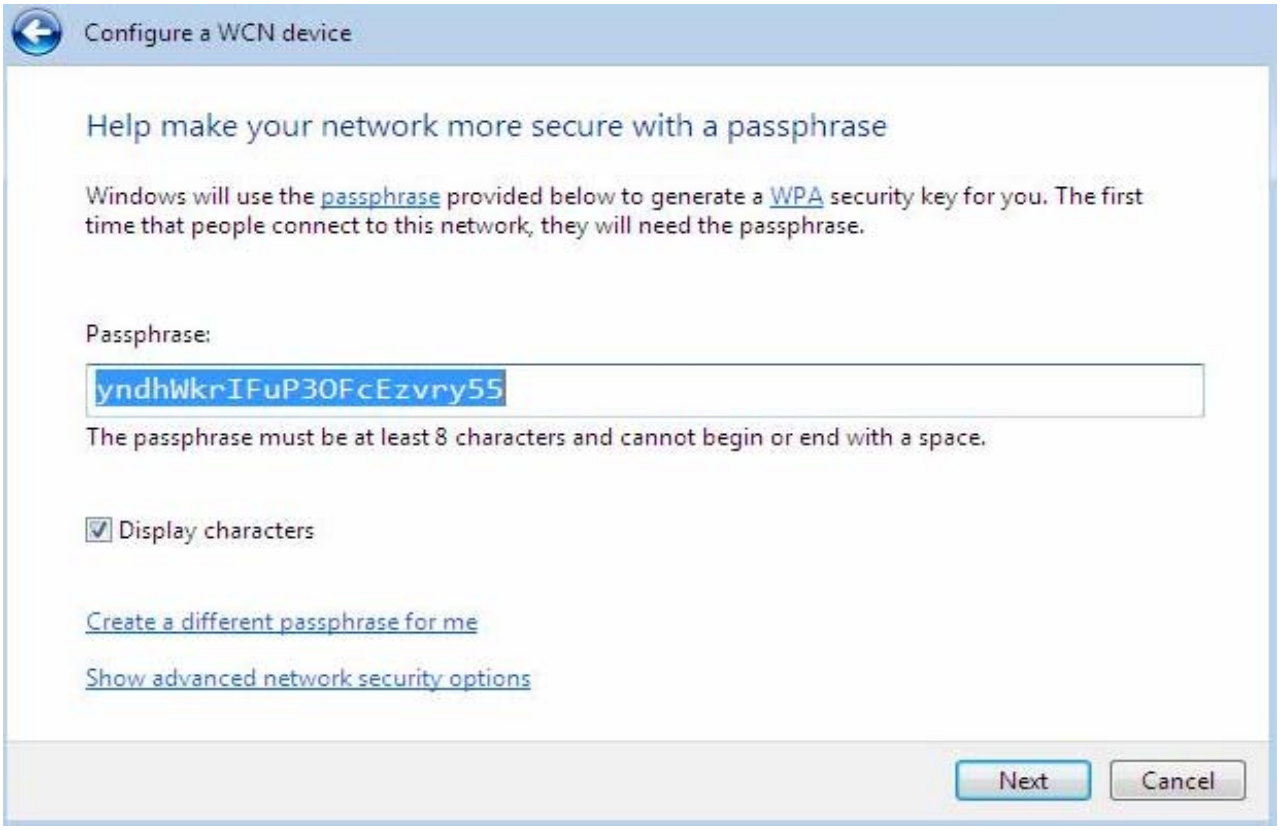

**步骤 3:** 在 Vista 控制面板中，选择 **Network and Internet and** choose **View network computers and devices**. 双击 “ADSL 防火墙路由器”输入 PIN 码点击“下一步”



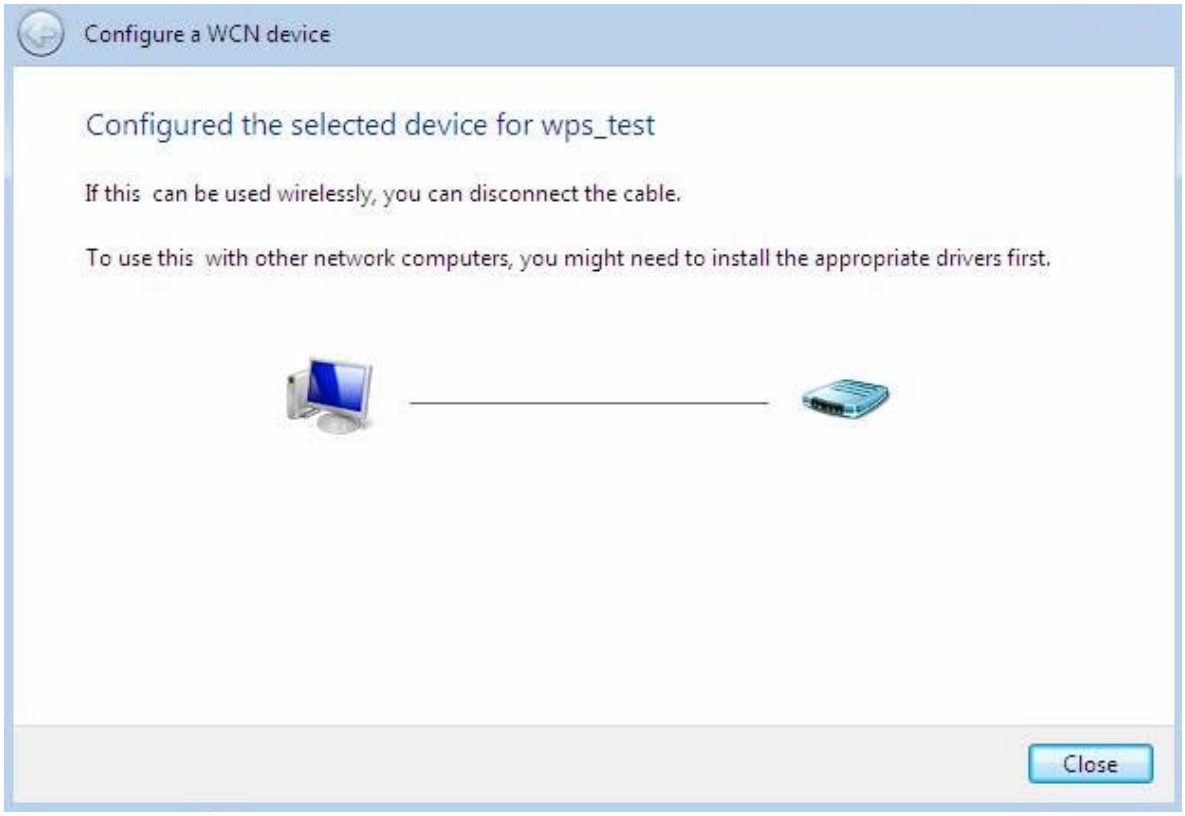

**步骤 4:** 输入 SSID 点击“下一步”



**步骤 5:** 输入密钥点击“下一步”




**步骤 6:** WCN 安装完成。您已经建立了安全加密的 Wi-Fi 网络

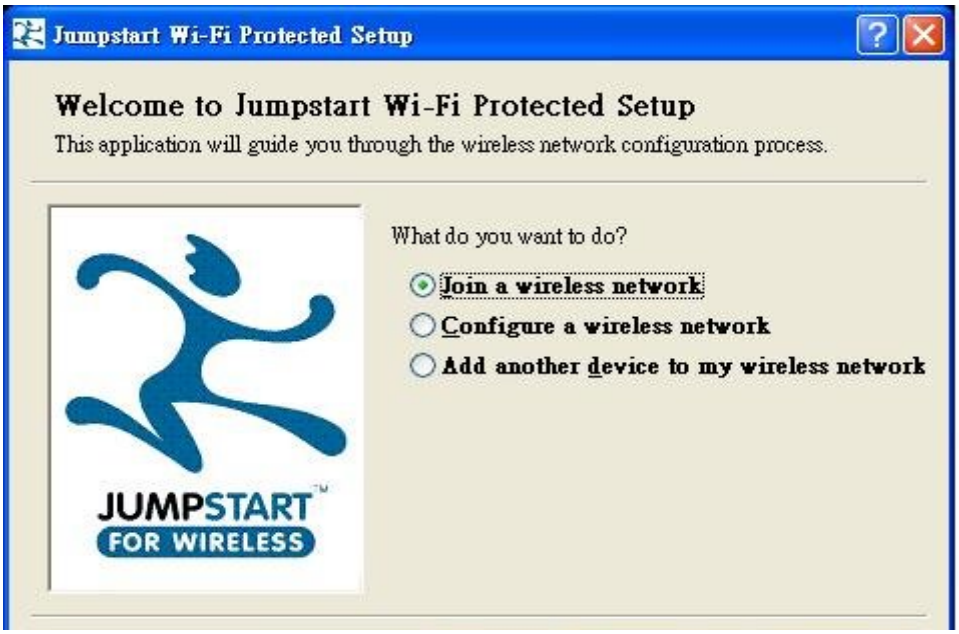


**在网络中添加一个 WPS 设备（无线客户端）——通过按钮配置**

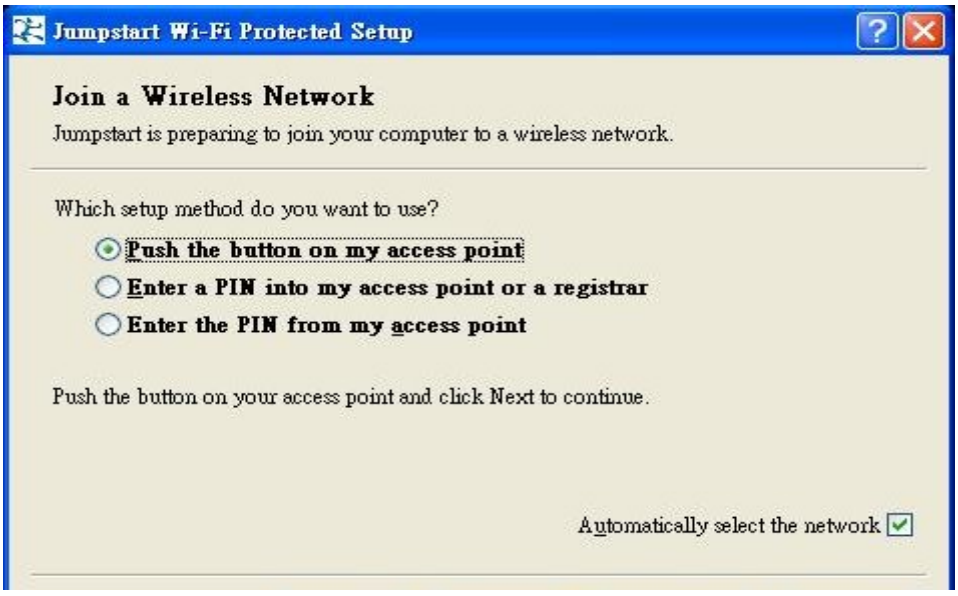
**步骤 1:** 按下 WPS 按钮超过一秒，您将会发现 WLAN 的 led 将会闪烁

**步骤 2:**打开无线客户端 WPS 应用程序，选择 “join a wireless network”点击“next”

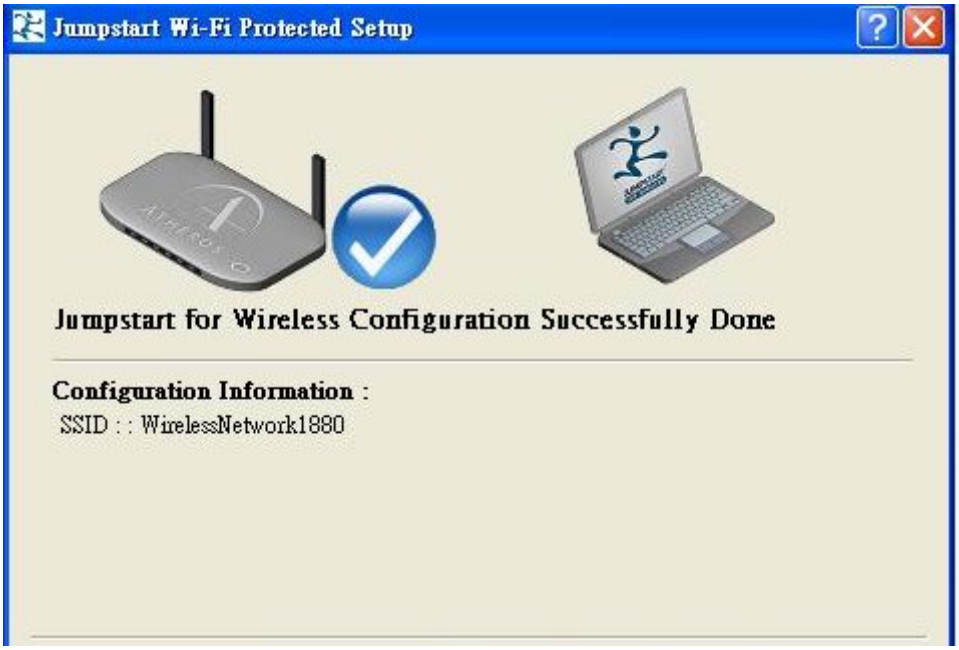
**注意：**当按下 WPS 按钮之后，以下步骤应在 2 分钟内完成。




**步骤 3:** 选择“Push the button on my access point” 点击“next”



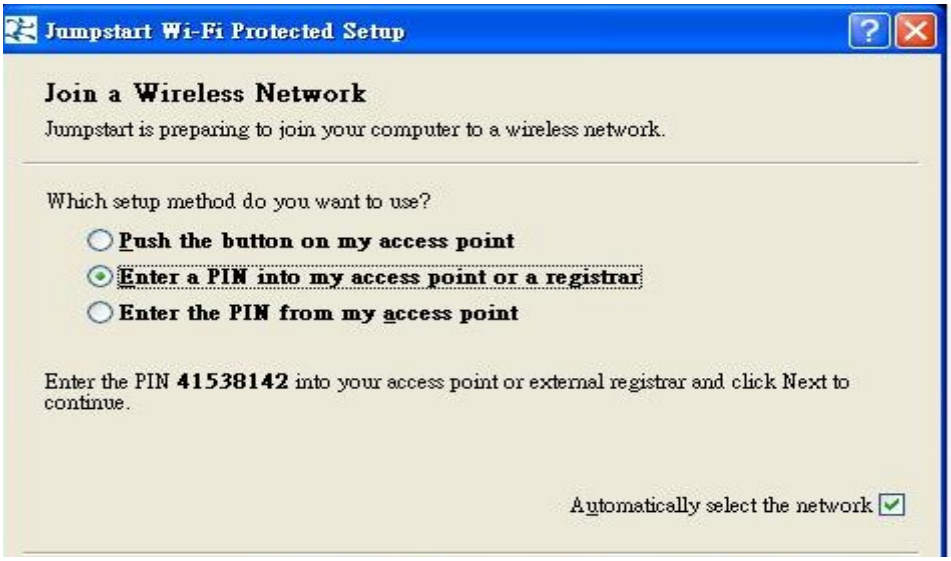
**步骤 4:** WPS 设备已经添加到了无线网络




**在网络中添加一个 WPS 设备（无线客户端）——通过输入 PIN 码配置**

**Step 1:** 打开无线客户端 WPS 应用程序，选择 “join a wireless network”点击“next”

**步骤 2:** 记下无线客户端的 PIN 码 (如： 41538142) 点击“start”激活无线客户端 WPS PIN 码




**步骤 3:** “在会员的 PIN”中输入无线客户端的 PIN，点击“开始”

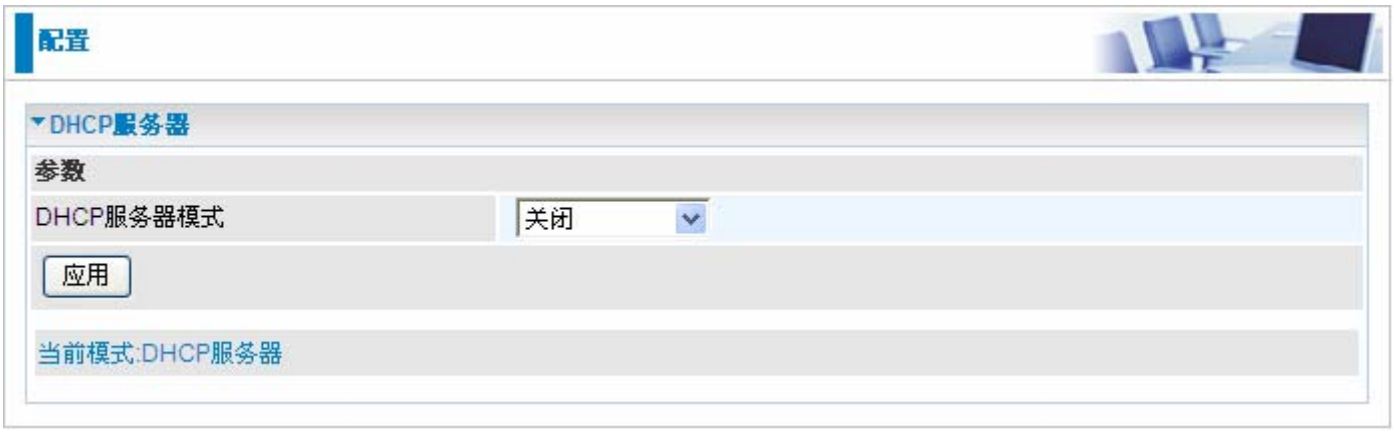

**步骤 4:** 新的 WPS 设备已经添加到了无线网络

## DHCP 服务器

您可以关闭或开启 DHCP（动态主机配置协议）服务器或开启路由器的 DHCP 中继功能。DHCP 协议允许您的路由器为网络中的 PC 动态分配 IP 地址，如果配置成自动获取 IP 地址。

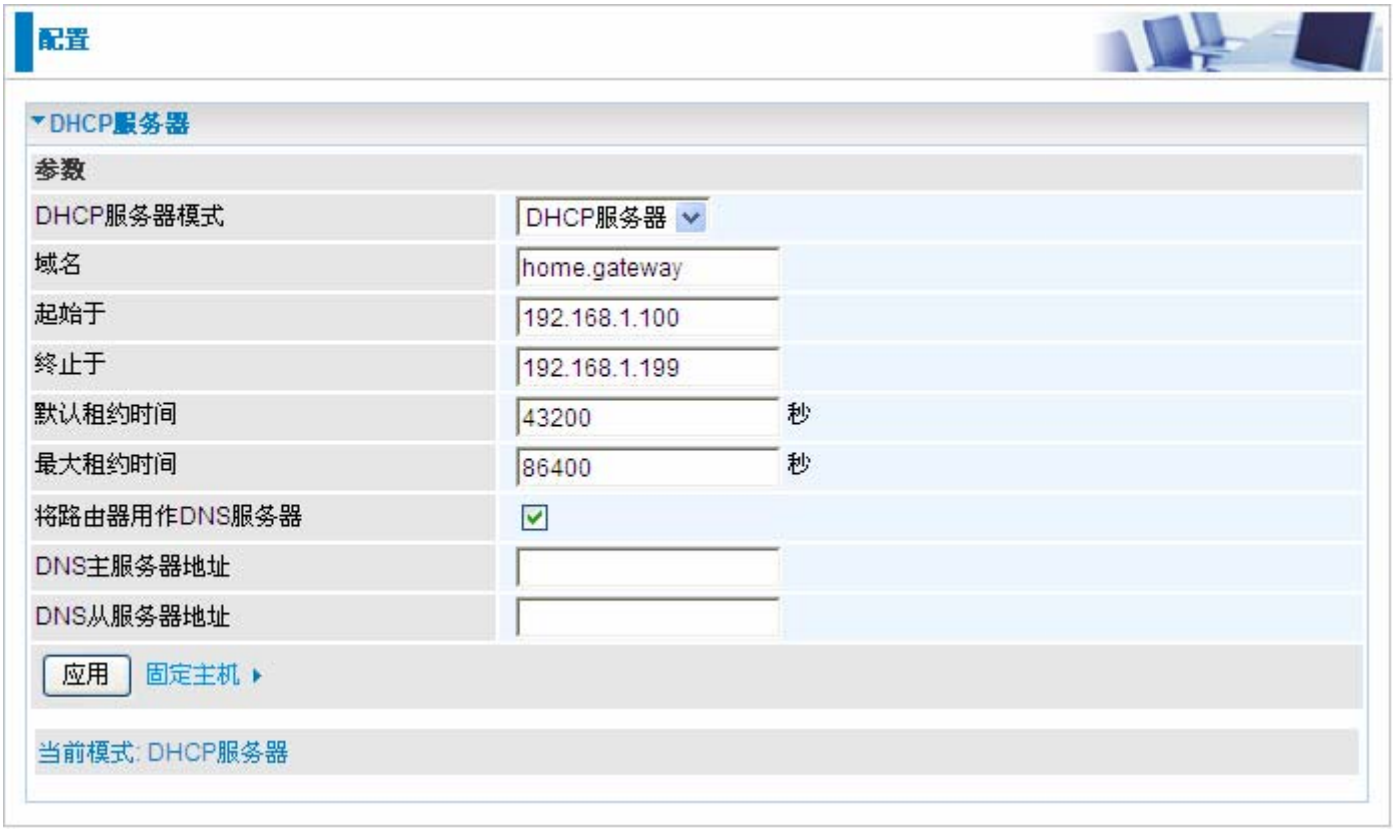
### DHCP 服务器模式：关闭

若要关闭 DHCP 服务器，选择**关闭**然后点击**应用**。当 DHCP 服务器是关闭的，您将需要手工分配固定的 IP 地址给网络中每台 PC，并且要为每个 PC 配置默认网关是路由器的 IP 地址。（默认是 192.168.1.254）



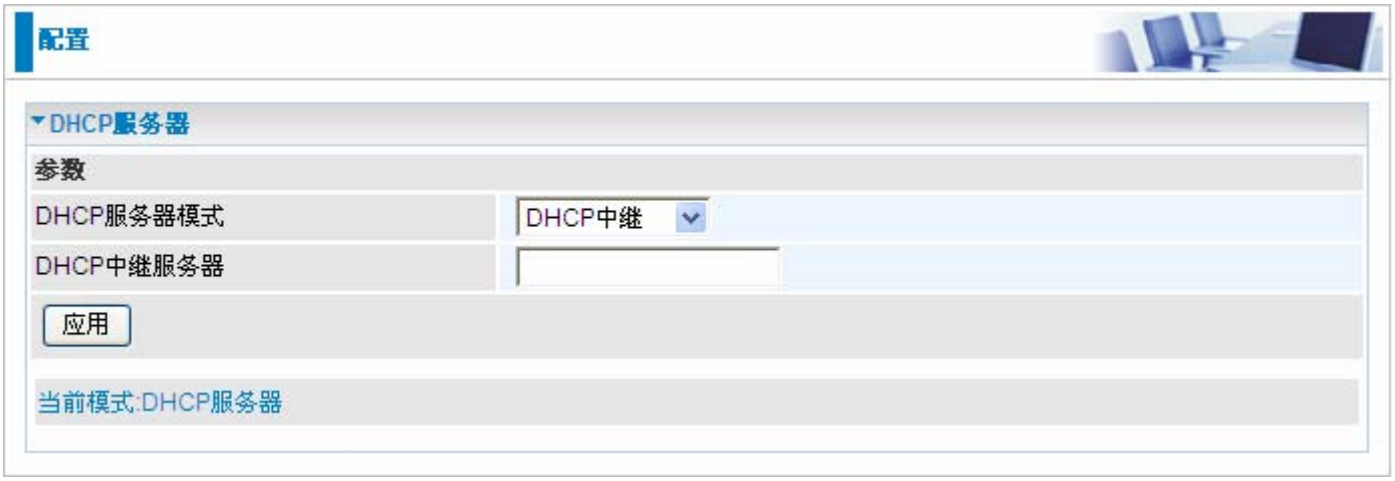

### DHCP 服务器模式：DHCP 服务器

若要配置路由器的 DHCP 服务器，选择 **DHCP 服务器**。您可以配置 DHCP 服务器的参数，包括 IP 地址池（分配给 PC 的开始 IP 地址和结束 IP 地址），每个分配的 IP 地址的租约时间（有效的 IP 地址分配时间），DNS 服务器的 IP 地址和网关的 IP 地址。这些详细信息都要分配给 DHCP 客户端（例如您的 PC），当 DHCP 客户端向 DHCP 服务器请求 IP 地址的时候。点击**应用**可以开启此功能。如果勾选了**将路由器用作 DNS 服务器**，那么这个路由器将执行 DNS 查询，将自动从外部网络查找 IP 地址，然后反馈到 LAN 中的发起请求的 PC。




**DHCP 服务器模式：DHCP 中继**

如果选择了 **DHCP 中继**，您必须输入第三方 DHCP 服务器地址。如果网络管理员或 ISP 需要用的时候可以使用这个功能。点击**应用**可以开启此功能。



# WAN (广域网)

WAN（广域网）是到另一网络或 Internet 的外部连接。**WAN** 部分包括：**WAN 接口**和 **WAN 外部形态**。

## WAN Interface


## WAN 外部形态

### 主端口 – EWAN

BiPAC 6200NXL 提供了一个 WAN 口 Ethernet port 1，通过它可以连接到电缆调制解调器和光纤上，使用户上网享受快速且灵活性的连接。

## 自动获得 IP 地址 (EWAN)

当链接到 ISP 的时候，BiPAC 6200NXL 还可以作为一个 DHCP 客户端。如果 ISP 确定此信息通过 DHCP，BiPAC6200NXL 可以自动获得一个 IP 地址，子网掩码，网关地址和 DNS 服务器地址。


- **带宽 ：**以千字节每秒的单位设定了连接时的上行速率和下行速率
- **NAT:** NAT（网络地址转换）功能允许多个用户通过一个 ISP 帐户访问 Internet，共享一个 IP 地址。如果 LAN 中的用户有公网 IP 地址并且可以直接访问 Internet，那么就关闭 NAT 功能。
- **获得 DNS：**勾选可以自动获得 DNS。
- **主用/备用：**输入 DNS 服务器的 IP 地址。DNS 服务器将和 IP 地址和子网掩码一起传到 DHCP 客户端。
- **MAC Spoofing:** 选择**开启**并输入一个 MAC 地址，路由器的 MAC 地址将会暂时的变为您输入的地址。如果不想改变路由器的 MAC 地址就不要开启。

## PPPoE (EWAN)

PPPoE（以太网上的 PPP）提供类似于使用 PPP 拨号服务的接入控制和计费功能。


- **带宽 ：**以千字节每秒的单位设定了连接时的上行速率和下行速率。
- **用户名：**输入 ISP 提供的用户名。您可以输入最多 **128** 个字符（大小写敏感）。格式是“username@ispname”，而不是“username”。
- **密码：**输入 ISP 提供的密码。您可以输入最多 **128** 个字符（大小写敏感）。
- **服务名称:**连接时输入一个名字。
- **NAT:** NAT（网络地址转换）功能允许多个用户通过一个 ISP 帐户访问 Internet，共享一个 IP 地址。如果 LAN 中的用户有公网 IP 地址并且可以直接访问 Internet，那么就关闭 NAT 功能。
- **IP 地址：**WAN 口的 IP 地址。保持 0.0.0.0 将自动从 ISP 获取 IP 地址。
- **认证协议:** 默认是自动。您的 ISP 可能会使用 **Chap** 或 **Pap**。
- **获得 DNS：**勾选可以自动获得 DNS。
- **主用/备用 DNS：**输入 DNS 服务器的 IP 地址。DNS 服务器将和 IP 地址和子网掩码一起传到 DHCP 客户端。
- **MAC Spoofing:** 选择**开启**并输入一个 MAC 地址，路由器的 MAC 地址将会暂时的变为您输入的地址。如果不想改变路由器的 MAC 地址就不要开启。
- **连接:**

  **永续：**如果想在路由器启动时建立会话，以及在 ISP 断开连接时能够自动重新建立 PPPoE 会话。

- **空闲时间：**如果预定义时间内没有进行任何通话，将自动断开连接。 最小值为 10 分钟。
- **MTU:** 最大传输单元。IP 试图通过接口传输的最大数据报（不包括特定于媒体的报头）的长度。

## 固定 IP 地址 (EWAN)

选择此选项可以设置静态 IP 信息，您需要输入 ISP 提供给你的连接类型，IP 地址，子网掩码和网关地址。在这个区域中输入的必须是由圆点分隔成的 4 个 IP 字段的正确的 IP 地址形式(x.x.x.x)。如果不是这种形式路由器将不会接受这个 IP 地址。


- **带宽:** 以千字节每秒的单位设定了连接时的上行速率和下行速率
- **NAT:** NAT（网络地址转换）功能允许多个用户通过一个 ISP 帐户访问 Internet，共享一个 IP 地址。如果 LAN 中的用户有公网 IP 地址并且可以直接访问 Internet，那么就关闭 NAT 功能。
- **IP 地址：** WAN 口的 IP 地址。保持 0.0.0.0 将自动从 ISP 获取 IP 地址。
- **子网掩码：**默认是 0.0.0.0。用户可以更改称其它的，如 255.255.255.0。输入 ISP 分配的子网掩码。
- **网关：**必须指定一个网关 IP 地址(ISP 提供)。
- **获得 DNS：**勾选可以自动获得 DNS。
- **主用/备用 DNS：**输入 DNS 服务器的 IP 地址。DNS 服务器将和 IP 地址和子网掩码一起传到 DHCP 客户端。
- **MAC Spoofing:** 选择**开启**并输入一个 MAC 地址，路由器的 MAC 地址将会暂时的变为您输入的地址。如果不想改变路由器的 MAC 地址就不要开启。

## 主端口 - 3G

在USB端口中插入 3G/HSDPA 卡， 接 入 3G/ HSDPA, UMTS, EDGE, GPRS, 或者 GSM 网络连接，下载速度可达 14.4 Mbps。


**模式: 选择** 3G 服务提供商。

**电话号码：**GPRS / 3G 用户用来拨打网络互连电话的拨号串。由移动服务提供商提供。

**接入点名称：**APN 类似于 WWW 的 URL，是拨打 GPRS / UMTS 电话的设备。任何服务都可以连接到 APN，以建立数据连接。APN 分配的要求随服务提供商的不同而不同。

**用户名：**输入服务提供商提供的用户名。

**密码：**输入服务提供商提供的密码。

**鉴权协议：**如果您知道服务器使用的认证类型，或者您希望客户端连接时使用您指定的认证类型（作为服务端时），可以手动指定 CHAP（挑战握手协议）或 PAP（密码认证协议）。

使用 PAP 时，密码是未加密发送的；而 CHAP 会在发送前对密码进行加密，因为要确保客户端在不同时段都不会被入侵者取代。

- **PIN**：PIN 代表个人识别号码。PIN 码是一个数值，在有些系统中作为密码进行登录和认证。在手机中，PIN 码是锁定 SIM 卡的，直到您输入正确的密码。如果您连续三次输入的 PIN 码都不正确，SIM 卡将被锁定，必须使用网络/服务提供商提供的 PUK 码才能解锁。

注意：如果连续三次输入的 PIN 码都不正确，SIM 卡将被锁定，必须使用网络/服务提供商提供的 PUK 码才能解锁。

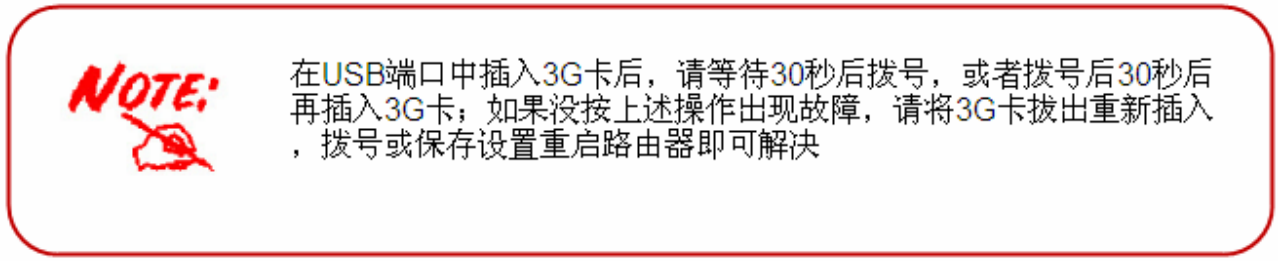
- **连接:**

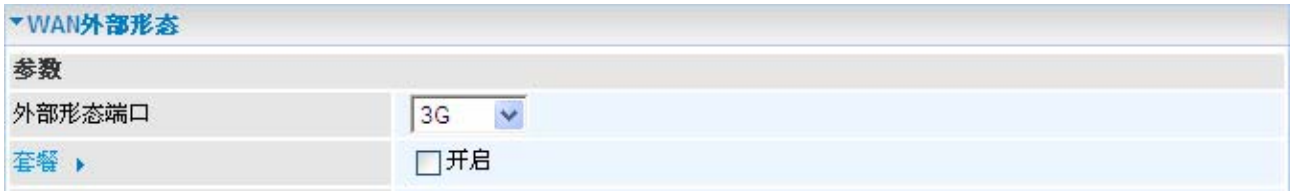
  **永续:** 路由器启动时将拨打 UMTS/GPRS 电话。启用**总是连接**后，您可以选择是否启用**保持连接**。

  **在请求时连接:** 如果您只想在有封包请求访问 Internet 时（如：计算机上的某个程序想要访问 Internet 时）拨打 UMTS/GPRS 电话，选择**按需连接**。这种模式下，您必须同时设置空闲时间。启用**按需连接**后，您必须设置**空闲时间**选项。

- **空闲时间**：如果预定义时间内没有进行任何通话，将自动断开连接。
- **自动获取 DNS**：选择该复选框，使用 DNS。
- **主用 DNS 服务器/备用 DNS 服务器**：输入 DNS 服务器的 IP 地址。将 DNS 服务器和 IP 地址以及子网掩码一起发送给 DHCP 客户端。

***注：如果您不知道如何设置这些值，请保留默认值。***

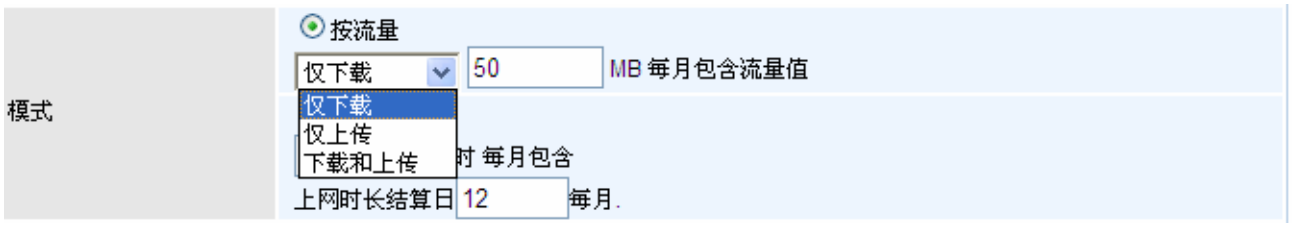





点击 **套餐** 进入套餐配置页面。


为了方便在线时间查询和使用流量查询，您可以设置以下选项：

- **模式:** 提供两种统计方式，**按流量**和**按时间**。
- **按流量:** 如果选择按流量，可以看到使用的总的流量。I



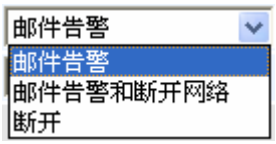

**仅下载:** 只统计下载流量。

**仅上传:** 只统计上传流量。

**下载和上传：** 统计上传和下载的总流量。

- **按时间:** 如果选择按时间，可以看到使用的总的时间。您也可以分配结算周期。


**超过套餐限制:** 如果在线时间或者使用流量超过了您设置的参数，系统会根据以下设置进行操作。




**保存统计数据:** 选择保存统计的时间间隔。您可以选择**每小时**，或者禁用该项功能。

# 系统

在**系统**部分包括六个部分：**时区**，**版本升级**，**备份/恢复**，**重启**，**用户管理** 和 **邮件告警**。

## 时区


路由器的主板上使用的不是真实的时间，而是使用简单网络时间协议 (SNTP) 从外部网络的 SNTP 服务器获得当前的时间。选择本地时区，点击**开启**，然后点击**应用**按钮就可以了。在成功连接到 Internet 以后，路由器会从指定的 SNTP 服务器获取正确的本地时间。如果您要自定义一个 SNTP 服务器而不是从下拉选项中选择，只要在空白处写上 IP 地址就可以了。您的 ISP 会提供 SNTP 服务器供您使用。

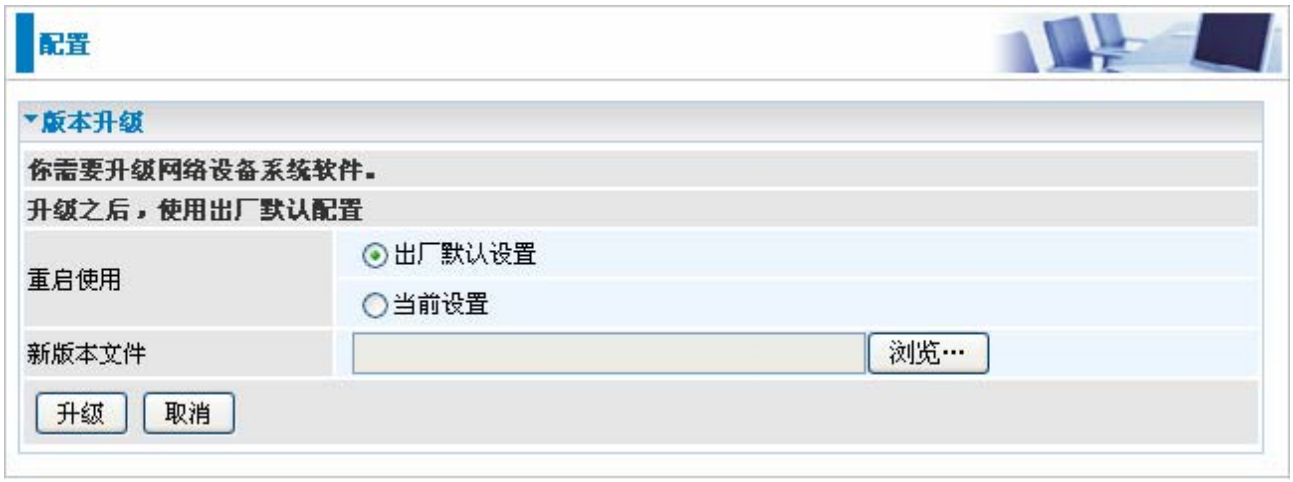
**日光节约时间**又称***夏时制***。世界上许多国家都在夏季采用夏时制，将当地标准时间的日照时间提前 1 小时。勾选**自动**框自动设置当地时间。

**同步时间**（分钟）是路由器在与 SNTP 服务器同步时间以前等待的时间。若要避免在 SNTP 服务器不必要的负载，那就尽可能的延长同步时间，将时间设置成几小时或几天。

## 版本升级

您的路由器的固件是一种可以供您对路由器功能进行操作的软件。把您的路由器想象成专用的计算机，固件就是这台计算机运行的软件。这个软件可能随着时间的推移不断改进和更新。您的路由器可以让您升级这个软件以使用新的功能。

点击**浏览**可以让您选择新下载的固件文件。选择以后，点击升级可以升级您的路由器。




- **重启使用：**选择出厂设置或当前设置可以让您在升级到新的固件的时候恢复出厂默认设置或保持当前设置。（强烈建议恢复出厂默认设置）
- **新版本图像：**输入上传文件的位置，或点击**浏览**定位此文件。
- **浏览...：**点击**浏览**可以找到**.afw** 扩展名的固件文件。要记得从压缩文件(.zip)中解压缩以后才能进行升级。
- **升级：**点击升级可以开始进行升级。这个过程估计要花 3 分钟。

*警告*

在这个过程中不要关闭路由器或中断固件的升级。不适当的操作可能会损坏路由器。

## 备份 / 恢复


这个功能可以让您保存并备份路由器的当前设置到您的 PC 上，或者恢复先前保存的备份。如果您想用不同的设置进行试验就会非常有用，您有一个备份在手边就可以防止任何错误。建议在对路由器做任何重大的更改之前备份您的路由器设置。

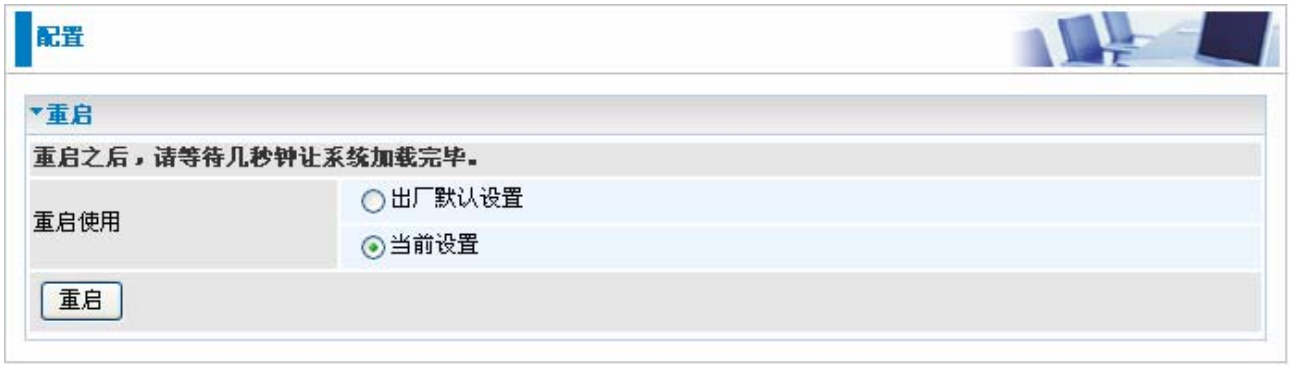
点击**备份**可以在您的 PC 上保存配置文件。您还可以更改保存的文件名以便保存多个备份。

点击**浏览**可以从 PC 找到备份的文件进行恢复。您只能恢复先前在路由器**当前版本**下备份的文件。**保存的备份文件不要进行任何形式的编辑。**

选择备份的文件，点击**恢复**就可以恢复路由器的配置。

## 重启

点击**重启**并选择**当前设置**可以重新启动路由器并保存当前的设备配置文件。




如果您想要使用出厂默认设置重新启动路由器（例如，在升级固件以后或保存了错误的配置文件以后），请选择**出厂默认设置**。

## 用户管理


为了防止未授权的用户访问您路由器的配置界面，就需要让所有登录的用户使用密码。您可以设置多个用户帐户，让他们拥有各自的密码。

- **有效的：**可以勾选以决定用户帐户是否激活。
- **用户：**输入用户帐户的名称。
- **密码/确认：**输入并确认用户帐户的密码。
- **登录模式：**可以选择**基础**让用户登录以后进入基础配置界面，选择**高级**可以让用户登录以后进入高级配置界面。
- **等级：**可以选择**超级**可以让用户登录以后进入基础或高级配置界面，选择**普通**可以让用户登录以后进入基础配置界面。

您可以**编辑**现有的用户或**添加**新的用户访问设备的配置界面。一旦您在编辑字段点选了您想编辑的帐户，就会显示出此帐户的信息。您可以更改帐户的**密码**，可以决定帐户是否**有效**。这些选项和创建用户帐户的时候除了不能更改用户名，其它都是一样的。更改完参数以后点击**编辑/删除**保存设定。您不能删除默认的用户帐户，但是可以在删除字段勾选创建的其它帐户，然后点击**编辑/删除**。

强烈建议您更改默认的 **admin** 帐户密码，如果忘记密码可以按住 reset 按钮恢复到出厂默认设置。

## 邮件警告

邮件警告目的是让管理员或者其他相关人员在能够更有效率的监测到计算机或者服务器发生的意外事件。可以用适当的办法来解决可能产生的问题，以便服务器得到妥善的维修。


- **SMTP Server：** 输入发送邮件的 SMTP 服务器。
- **用户名：**输入在SMTP服务器上使用的Email账户名。.
- **密码：**输入邮箱账户密码。
- **Sender’s Email：**输入您的邮箱地址。
- **Recipient’s Email ：**输入接收告警邮件的Email地址。

# USB 服务器

USB Server 集中了 FTP 服务器，打印机服务器和网络摄像头监控功能。通过 FTP 服务器和 Samba 可以设置账户上传下载权限。打印机服务器 支持 Internet printe protocol,允许用户远程打印。

USB 部分有 5 个选项： **用户管理, 存储设备, Samba 服务器, FTP 服务器** 和 **打印机设置**

## 管理


- **用户设置:** 在次栏目中输入要创建的账户名和密码。
- **FTP 设置:**

  **FTP 服务器:** 启用这项功能，创建的账户就有访问 FTP 服务器的权限。

  **重复登录:** 允许与多个账户同时登陆 FTP 服务器。启用这项功能才可以设置**最大登录数。**

  **最大登录数:** 这个选项设定了同时登陆 FTP 服务器的最大用户数（包括匿名登录和不是匿名登录用户）。

**下载:** 从 FTP 服务器上下载文件权限。

**上传:** 上传文件到 FTP 服务器上的权限。

**写:** 改写 FTP 服务器上文件的权限。.

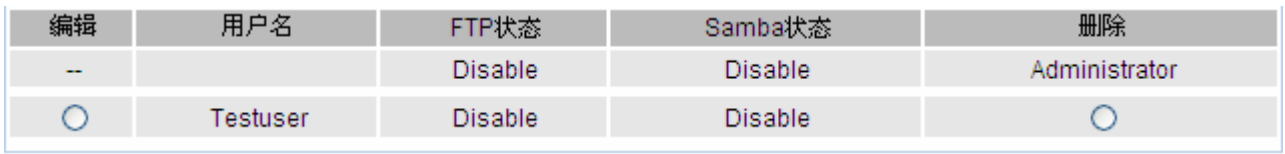
**删除:** 删除 FTP 服务器上文件的权限。

- **Samba 设置:** 启用或禁用创建的用户使用 Samba 服务器的功能。
- **添加:** 点击添加按钮添加的新的账户将显示在下面的表格中。
- **编辑/删除:** 选择您想编辑/删除的用户，点击编辑/删除即可。

**编辑/删除用户:**

1. 输入用户名和密码


2. 点击添加，新的用户将在下端表格中显示。




3. 选择您想编辑的账户，您就可以编辑它的参数设置，点击编辑/删除保存设置。


4. 选择您想删除的用户，点击编辑/删除即可删除。

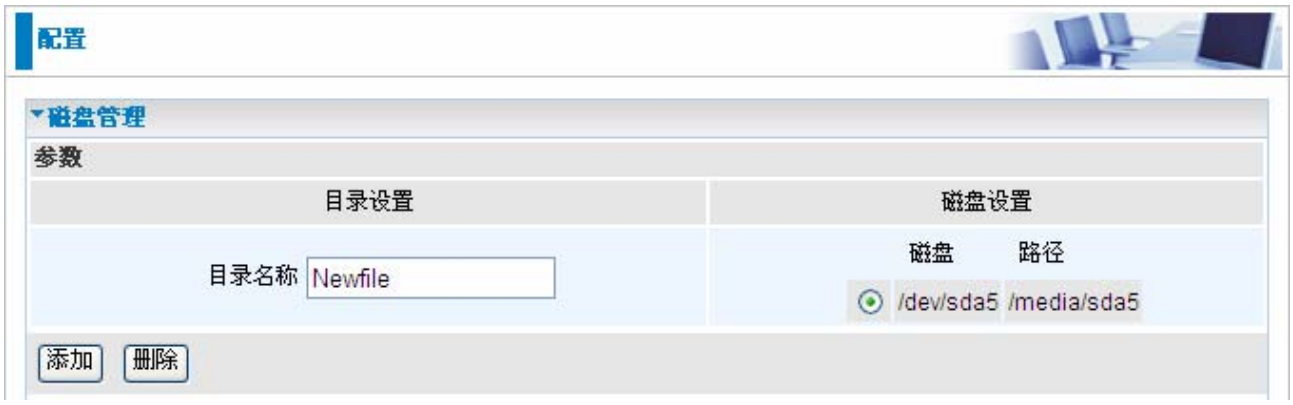
## 存储设备

此页面显示连接到 USB 端口的存储设备的信息。 例如目录设置，磁盘路径等等。用户可以设置存储设备也可以将其格式化。


- **目录设置:** 输入要创建的目录文件的名称。
- **磁盘设置:** 选择要编辑的磁盘路径。
- **FAT32 格式:** FAT 32 方式格式化选择的磁盘。
- **NTFS 格式:** NTFS 方式格式化选择的磁盘。
- **移除硬盘:** 点击此按键移除选择的磁盘路径。

**添加/删除 目录:**

1. 在目录名称栏中输入目录名并选择其磁盘路径。

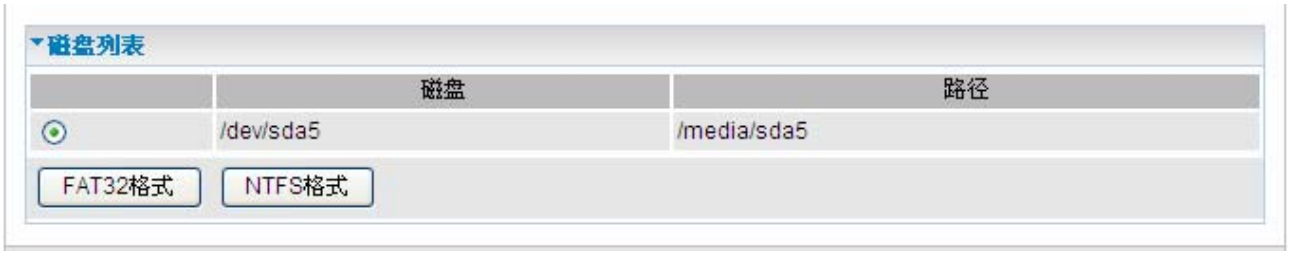



2. 点击添加，新的目录将在下端磁盘列表中显示。

3. 选择要删除的目录，点击删除即可移除该目录。


**磁盘列表:**

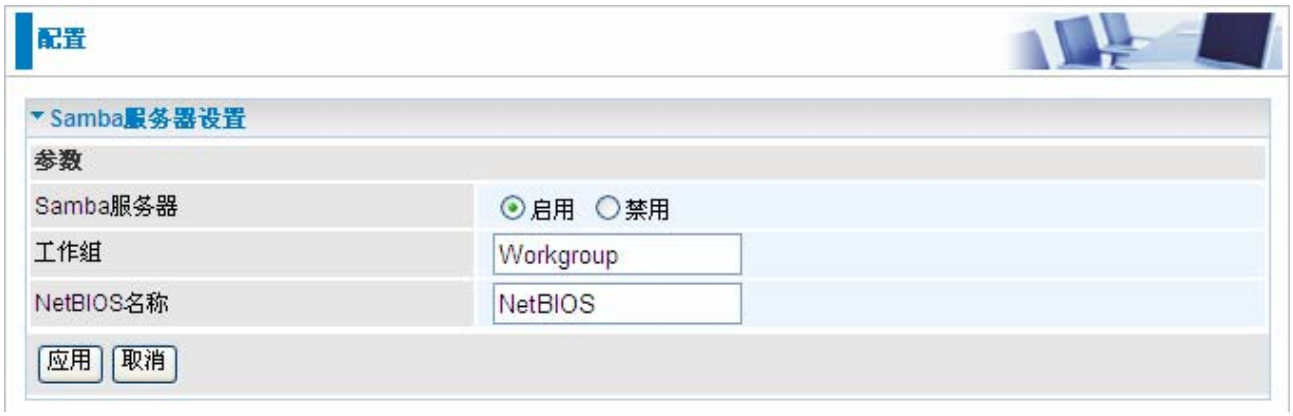
选择磁盘路径，点击 FAT32/ NTFS 格式，将会用 FAT32/NTFS 方式格式化所选的磁盘。



## Samba 服务器


配置
Samba服务器设置
参数
Samba服务器
启用
禁用
工作组
Workgroup
NetBIOS名称
NetBIOS
应用
取消
共享目录列表设置
参数
访问目录设置
访问用户设置
访问路径设置
目录名称
访问用户
Testuser
admin
test
路径
磁盘
/media/sda5/Recycled
/dev/sda5
/media/sda5/Newfile
/dev/sda5
/media/sda5/arm
/dev/sda5
/media/sda5/Red Hat Linux
/dev/sda5
/media/sda5/System Volume Information
/dev/sda5
添加
删除
删除
目录名称
目录路径
允许访问用户

**Samba 服务器设置:**




- **SAMBA 服务器:** 启用或禁用 SAMBA 服务器功能。默认设置是**禁用**。
- **工作组:** 在工作组栏目中输入工作组名称，默认名称是 Workgroup.
- **NetBIOS 名称:** 在 NetBIOS 名称栏目中输入 NetBIOS 名称，默认名称是 NetBIOS。

点击**应用**保存设置。

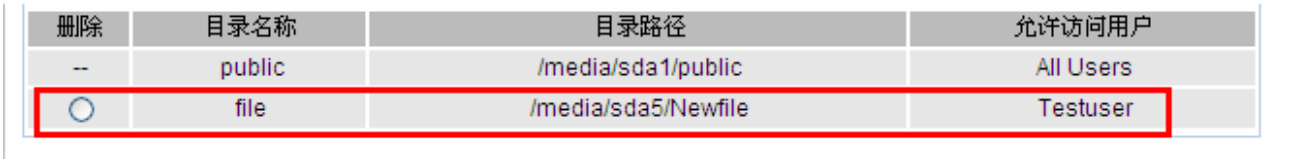
**共享目录列表设置**


- **目录名称:** 输入在服务器上显示的镜像目录名称。
- **访问用户:** 选择允许访问目录的用户。
- **路径 磁盘:** 选择用户可以访问的路径。
- **添加:** 点击添加按钮增加新的设置，新增的设置将会在下端列表中显示。

**添加/删除 目录:**

1. 在目录名称栏中输入镜像目录名称，选择可访问的用户和磁盘路径。


2. 点击**添加**，新的目录将在下端列表显示。




点击**应用**保持设置。

3. 选择要删除的路径，点击**删除**即可移除。

## FTP 服务器

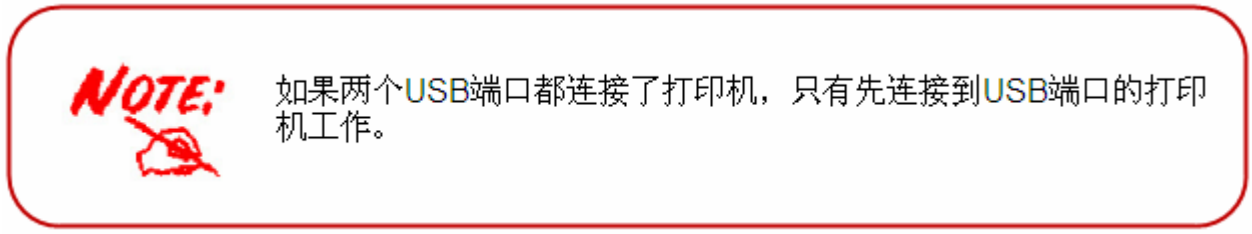

- **FTP 服务器:** 启用或禁用 FTP 服务器功能。默认设置是禁用。
- **匿名登录:** 启用或禁用匿名登录功能。默认设置是禁用。
- **FTP 端口:** 在此栏目中输入 FTP 端口号；请注意不要和其他端口号冲突。
- **最大用户数:** 限定了可设置的最大用户数。
- **登陆超时:** 输入登录超时时间数值。登录超时选项设置从尝试登陆到服务器到返回登录失败的时间间隔。 默认值是 120 秒。
- **空闲超时:**输入空闲超时时间数值。如果在这个时间段内无任何操作将于服务器自动断开连接。默认值是 240 秒。

点击**应用**保存设置。

## 打印机设置

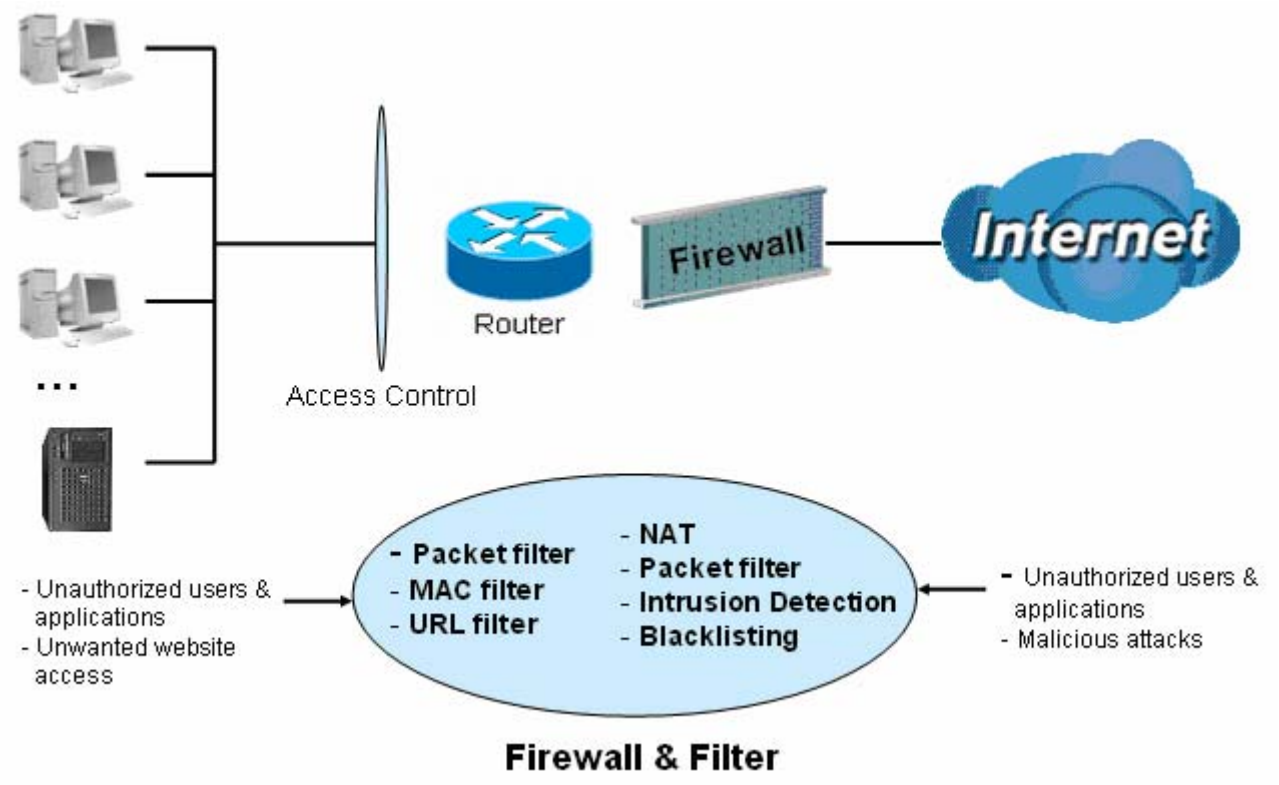

- **启用打印机:** 开启或关闭打印机服务器功能。默认设置是关闭的。
- **启用从 WAN 口访问打印机:** 开启或关闭启用从 WAN 口访问打印机功能。默认设置是关闭的。
- **打印机型号:** 显示打印机的型号。
- **打印机名称:** 设置打印机的别名。
- **打印机描述:**输入打印机的相关信息。

点击**应用**保存设置。



# 防火墙和访问控制

您的路由器支持 SPI（状态封包检测）防火墙功能，可以控制从 LAN 的 Internet 访问，防止黑客的攻击。除此之外，NAT（网络地址转换）是路由器的天然 Internet 防火墙，因为 LAN 中的 PC 使用私有 IP 地址不能直接访问到 Internet。请参考 **WAN** 配置获取更多关于 NAT 的信息。




**防火墙：** 防止外部网络的访问。

**NAT 天然防火墙：**这使得 LAN 中的用户 IP 在 Internet 中不可见，让黑客更难于攻击网络中的计算机。开启 NAT 功能就可以使用天然防火墙。

NOTE:

当使用虚拟服务器（端口映射），您的 PC 就会把特定的端口暴露在 Internet。

**防火墙和策略 (中心设定)：**入站包过滤规则防止未授权的计算机或应用程序从 Internet 访问本地网络。

**入侵检测：**开启入侵检测可以侦测，防止，记录恶意攻击。

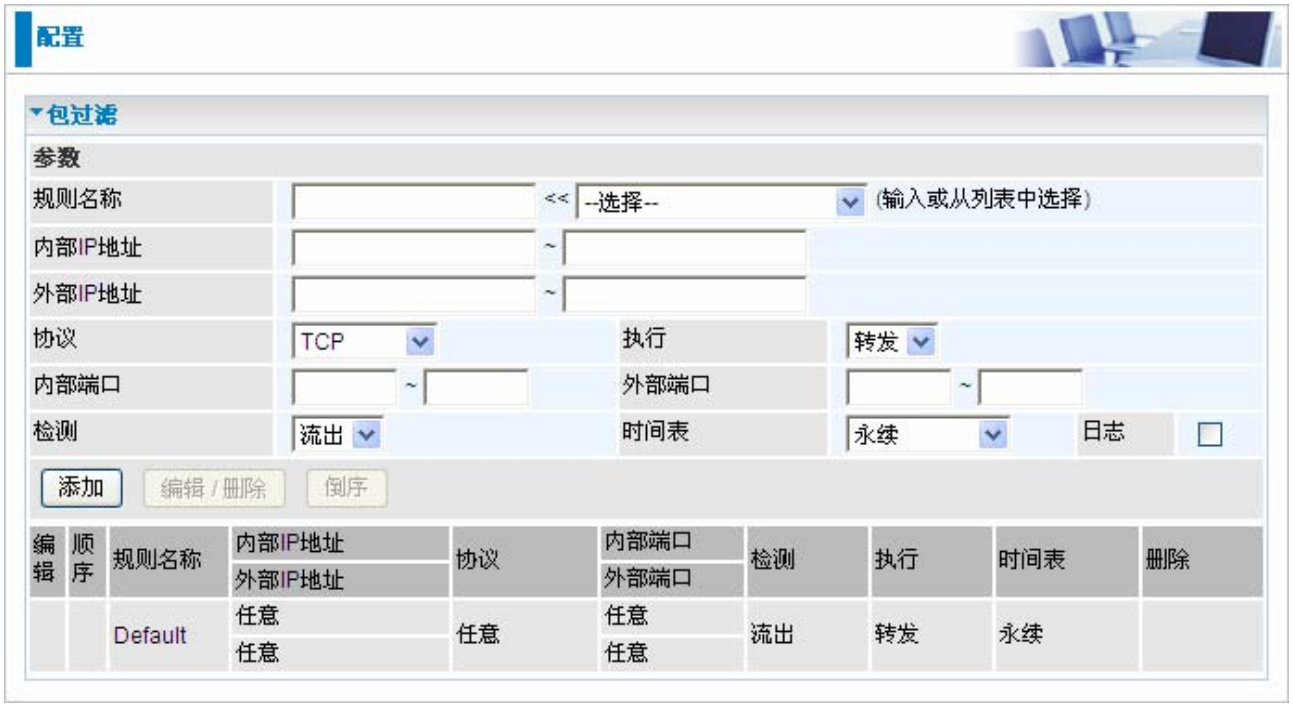
**MAC 地址过滤：**防止 Internet 的非授权计算机访问。

**URL 过滤：**可以阻塞本地网络中的 PC 访问限制站点。

**防火墙**包括以下五部分：**包过滤，MAC 地址过滤，入侵检测，阻塞**和 **URL 过滤**。

## 包过滤

包过滤可以让您配置路由器阻塞指定的内部/外部用户（IP 地址）访问 Internet/Intranet，或者可以阻塞指定的服务请求（端口号）去/来自于 Internet。这个配置程序可以让你为不同的用户设置 6 种不同的基于 IP 地址或端口号的过滤规则。在所有过滤规则之间是**或**的关系。这意味着路由器将从头到尾按顺序检查过滤规则。一旦匹配一个规则，那么就会执行相应的动作。




**规则名称：**用户定义的描述名称。最大长度是 32 个字节，可以从旁边的下拉选项中选择。

**内部IP地址/外部IP地址：**这是地址过滤用于阻塞出入的特定IP地址。输入想过滤的IP地址范围。如果不填写或填写 0.0.0.0，这表示所有IP地址。

- **协议：** 指定规则应用的协议类型 (TCP，UDP，ICMP等)。如果您想搜索基于连接的使用端口号的远程应用服务，请选择TCP。或者如果您想搜索无连接的使用端口号的远程应用服务，请选择UDP。
- **执行：** 如果与包过滤规则映射，可以**转发 （允许数据包通过）**或**丢弃 （不允许数据包通过）** this packet.
- **内部端口：** 端口范围定义了允许远程/WAN连接的应用服务。默认范围是 **0-65535**。建议高级用户配置此选项。
- **外部端口：** 端口范围定义了允许内部访问的应用服务。
- **检测：** 决定规则是用于出站数据流还是入站数据流。
- **时间表：** 用户定义的时间表。用于指定应用包过滤规则的时间。若要设置详细信息，请参考**时间表**部分。
- **日志：**勾选**日志**，当包过滤规则匹配的时候就会产生日志。
- **添加：** 点击这个按钮可以添加包过滤规则，并且添加到包过滤列表的底部。
- **编辑/删除：** 在编辑字段选择包过滤规则，然后更改参数，最后点击**编辑/删除**可以进行编辑。在删除字段选择包过滤规则，然后点击**编辑/删除**可以进行删除。

| 编辑 | 顺序 | 规则名称 | 内部IP地址<br>外部IP地址 | 协议 | 内部端口<br>外部端口 | 检测 | 执行 | 时间表 | 删除 |
|---|---|---|---|---|---|---|---|---|---|
| ○ | ↓ | FTP | 任意<br>任意 | TCP | 任意<br>21~21 | 流出 | 转发 | 永续 | ☐ |
| ○ | ↑ | HTTP | 任意<br>任意 | TCP | 任意<br>80~80 | 流出 | 转发 | 永续 | ☐ |

*注意*

如果 DHCP 是开启的，您必须小心过滤分配的私有 IP 地址范围，以避免冲突，因为您不知道 LAN 中的 PC 分配的 IP 地址。最简单和最安全的方式是不允许指定的 PC 访问外部资源，如 Internet。您可以手动配置 PC 的 IP 地址，但是要和路由器在同一子网。

## MAC 地址过滤

MAC（媒介访问控制）地址是网络中每台 PC 接口（如网卡）的唯一网络物理标识。使用 MAC 地址过滤功能可以阻塞 LAN 端访问的指定计算机。

没有预先定义的 MAC 地址过滤规则，您可以根据要求添加 MAC 地址过滤规则。


**MAC 地址：**输入需要过滤的 MAC 地址。

**时间表：**用户定义的时间表。用于指定应用包过滤规则的时间。若要设置详细信息，请参考**时间表**部分。

## 入侵检测

如果想检测非授权访问计算机的入侵者，请选择入侵检测。如果开启这个功能路由器将自动检测并阻塞 DoS（拒绝式服务）攻击。这种攻击不是访问网络中的机密数据，而是中断指定的设备或整个网络。如果发生这种情况，用户不能访问网络资源。


- **入侵检测：**选择开启可以检测非授权访问您计算机的入侵者。
- **最大 TCP 开放握手数量：**这是 SYN 泛洪攻击出现时的最大值。默认是每秒 100 个 TCP SYN 数。
- **最大 PING 数量：**这是 ICMP Echo 风暴出现时的最大值。默认是每秒 15 个 ICMP Echo 请求（PING）。
- **最大 ICMP 数量：**这是 ICMP 泛洪出现时的最大值。默认是每秒 100 个 ICMP 数据包（除了 ICMP Echo 请求（PING）。
- **日志：**勾选日志，当入侵检测规则匹配的时候就会产生日志。

表：**IDS** 可以识别的黑客攻击类型

| 入侵名称 | 检测参数 | 黑名单 | 阻塞持续时间类型 | 丢弃数据包 | 记录日志 |
|---|---|---|---|---|---|
| **Ascend Kill 攻击** | Ascend Kill 数据 | 源 IP | DoS | 是 | 是 |
| **WinNuke 攻击** | TCP<br>135, 137~139 端口,<br>标记: URG | 源 IP | DoS | 是 | 是 |
| **Smurf 攻击** | ICMP 类型是 8<br>目标 IP 是广播 | 目标 IP | 入侵防护 | 是 | 是 |
| **Land 攻击** | 源 IP=目标 IP | | | 是 | 是 |
| **Echo/CharGen 扫描** | UDP Echo 端口和 CharGen 端口 | | | 是 | 是 |
| **Echo 扫描** | UDP 目标端口 t = Echo(7) | 源 IP | 扫描 | 是 | 是 |
| **CharGen 扫描** | UDP 目标端口 = CharGen(19) | 源 IP | 扫描 | 是 | 是 |
| **X'mas Tree 扫描** | TCP 标记: X'mas | 源 IP | 扫描 | 是 | 是 |
| **IMAP SYN/FIN 扫描** | TCP 标记: SYN/FIN<br>目标端口：IMAP(143)<br>源端口 t: 0 or 65535 | 源 IP | 扫描 | 是 | 是 |
| **SYN/FIN/RST/ACK 扫描** | TCP,<br>没有当前会话和扫描超过 5 台主机 | 源 IP | 扫描 | 是 | 是 |
| **Net Bus 扫描** | TCP<br>没有当前会话<br>目标端口 = Net Bus 12345,12346, 3456 | 源 IP | 扫描 | 是 | 是 |
| **Back Orifice 扫描** | UDP, 目标端口 = Orifice Port (31337) | 源 IP | 扫描 | 是 | 是 |
| **SYN 泛洪** | 最大 TCP 开始握手数（默认是 100 次/秒） | | | | 是 |
| **ICMP 泛洪** | 最大 ICMP（默认是 100 次/秒） | | | | 是 |
| **ICMP Echo 风暴** | 最大 PING Count (默认是 15 次/秒) | | | | 是 |

**Src IP**：源 IP　　**Src Port:** 源端口　　**Dst Port**：目标端口　　**Dst IP**：目标 IP

## 阻塞

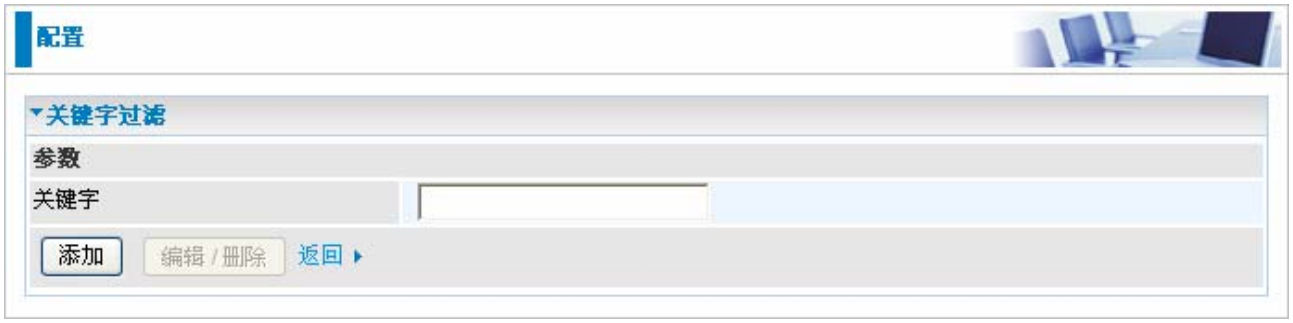
选择开启可以阻塞路由器 WAN 接口的 PING 请求。


## URL 过滤

URL（统一资源定位— 例如**http://www.example.com** 的地址形式）过滤规则可以让您阻塞网络中的用户通过URL访问网站。默认没有预定义的URL过滤规则，您可以根据需要增加过滤规则。


**关键字过滤：**允许您在 URL 中指定关键字，而不是全部的 URL（例如阻塞任何叫做”advertisement.gif”的图片） 开启这个功能可以让任何 URL 中的关键字匹配关键字列表的时候，连接将会被阻塞。要注意，URL 过滤只是阻塞 80 端口的 HTTP 连接。

例如，这个URL http://www.abc.com/abcde.html 将会被阻塞，因为出现了abcde关键字。



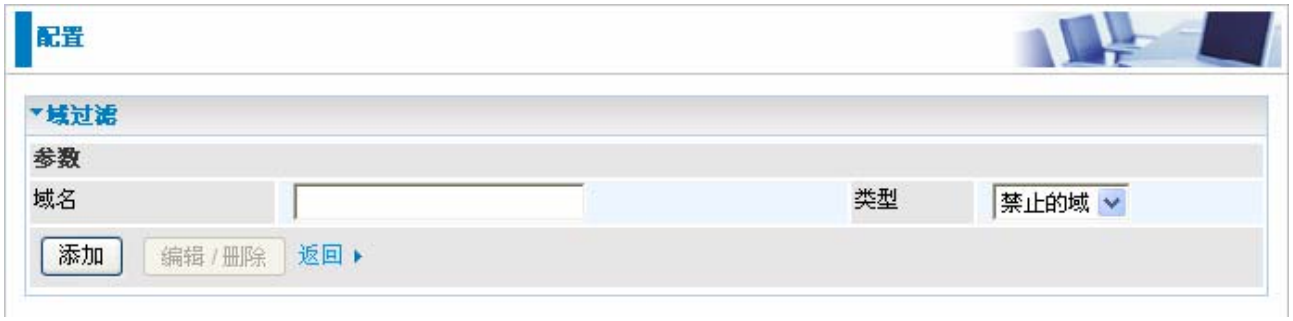

**域过滤：**勾选开启可以根据域名列表阻塞或允许指定域名的 URL。如果匹配了，URL 请求 将会被转发（信任的）或丢弃（禁止的）。检查步骤如下：

1. 检查 URL 中的域名决定是否是信任的 URL。如果是的，连接将会被转发。

2. 如果不是信任的，而是禁止的。那么连接将会被丢弃。

3. 如果没有匹配的也将被转发。

4. 请注意，完整的URL是www+域名。例如阻塞数据流到www.google.com.au，可以输入“www.google” 或 “www.google.com”。




**限制 URL 过滤：** 这个功能可以加强 URL 规则的过滤。

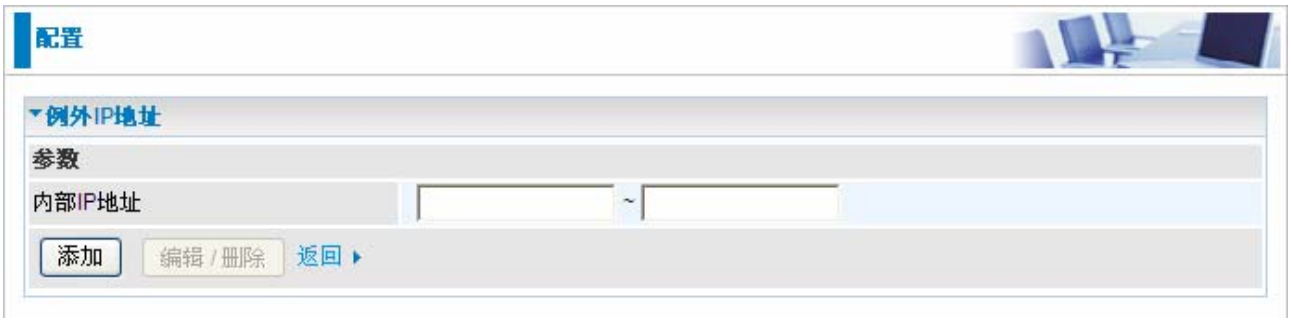
⊙ **阻塞 Java Applet:** 阻塞 Java Applet 可以阻塞一些人通过标准的 HTTP 协议更改您的系统。

⊙ **阻塞 ActiveX：**阻塞 ActiveX。

⊙ **阻塞 Cookies：**阻塞 Cookies。

⊙ **阻塞 Proxy：**阻塞代理。

**例外 IP 地址：**




**时间表：** 用户定义的时间表。用于指定应用包过滤规则的时间。若要设置详细信息，请参考时间表部分。

**日志：** 勾选日志，当包过滤规则匹配的时候就会产生日志。

# QoS (服务质量)

## 服务质量介绍

如果您曾经发现您的网速非常缓慢，那是因为家人在使用 P2P 软件共享您的带宽。您要明白为什么服务质量功能是家庭使用和办公室使用中的突破。

### QoS：让您的网络连接能够快速响应

服务质量(QoS)能够让您配置内部 IP 地址，外部 IP 地址，协议和端口，通过给定优先级给予您完全控制出站数据流，确保如游戏数据的带宽消耗的应用，如语音的延迟敏感的应用，甚至重要任务文件甚至在高负载下以闪电般的速度进行传输。

## QoS 配置

在**配置**中选择 **QoS** 显示下面界面。


在点击 QoS 以后，您可以添加/编辑/删除一个 QoS 策略。这个界面显示了您添加或编辑的策略的简要信息。这个界面还以百分比显示了总共可供分配的可用的带宽（非分配的）。

- **应用：** 输入策略的名称。
- **检测：** QoS 策略控制的数据流方向。

路由器中提供了两种方向：

⊙ **LAN to WAN**：可以控制从本地网络到外部网络的数据流，例如使用 QoS 策略控制本地网络的 FTP 服务器的有限的数据速率。所以，您要增加一个 LAN to WAN 的方向。

⊙ **WAN to LAN**：可以控制从 WAN 到 LAN 的数据流。（连接要么是 LAN to WAN，要么就是 WAN to LAN。）

**协议**：用于控制协议。对于 GRE 协议，就不需要指定 IP 地址或应用端口。对于其他协议，至少需要给出一个数值。

⊙ **任意**：不指定协议类型。

⊙ **TCP**

⊙ **UDP**

⊙ **ICMP**

⊙ **GRE:** 用于 PPTP VPN 连接。

**DSCP 标记**： 差分服务编码点(DSCP)，ToS 字节的前 6 位。 DSCP 标记允许用户根据 DSCP 值分类数据流，然后发送数据流到下一跳路由器。

**注意**： 要确保骨干网的路由器有能力执行和检查 QoS 网络的 DSCP。

| DSCP 映射表 | |
|---|---|
| **3G 路由器** | **标准 DSCP** |
| 关闭 | None（空） |
| 最大努力 | 最大努力(000000) |
| 保险 | 快速转发(101110) |
| 黄金服务(L) | 等级 1，黄金 (001010) |
| 黄金服务(M) | 等级 1，白银 (001100) |
| 黄金服务(H) | 等级 1，青铜 (001110) |
| 白银服务(L) | 等级 2，黄金(010010) |
| 白银服务(M) | 等级 2，白银(010100) |
| 白银服务(H) | 等级 2，青铜(010110) |
| 青铜服务(L) | 等级 3，黄金(011010) |
| 青铜服务(M) | 等级 3，白银(011100) |
| 青铜服务(H) | 等级 3，青铜(011110) |

**速度类型：**提供 2 种类型

⊙ **受限的（最大）：**为策略指定一个受限的数据速率。这同样也是策略的最大速率。如上面的 FTP 服务器案例，您可能想把 FTP 的出站速率限制成 256K 的 20%，您可以使用此类型。

⊙ **有保证的（最小）：**为策略指定一个最小的数据速率。例如，您想要为外部客户访问内部 FTP 服务器提供一个有保证的数据速率，至少是总带宽的 20%。您可以使用此类型。那么，如果有未使用的带宽，这个策略允许通过下列优先级分配使用该带宽。

**比率：**为策略控制分配比率。例如，我们要允许数据传输速率的 20%用于 LAN-toWAN 方向的 FTP 数据流。然后我们能指定速率=20。如果您有一条 256Kbps 的线路，根据这个策略的估算速率是 20%*256*0.9 = 46kbps。（0.9 是 LAN to WAN 的线路的有效数据传输的估算因

子，如果是 WAN to LAN 那就是 0.85-0.8 之间）。

- **优先级：** 指定未使用带宽的优先级。例如，您可以指定 2 个不同的策略用于不同的应用。两个应用都需要最小带宽和更多带宽，除了分配的以外，可以使用任何未使用的带宽。所以，您可以指定什么样的应用才对拥有使用未使用带宽的高优先级。

  - ⊙ **高**
  - ⊙ **普通：**默认值。
  - ⊙ **低**

此案例中对于不同策略分配的优先级，运行的是先进先出的机制。

- **内部 IP 地址：**想要控制的本地 LAN 计算机的 IP 地址。（LAN to WAN 的 IP 数据包的源 IP 地址，WAN to LAN 的 IP 数据包的目的 IP 地址）
- **内部端口：**想要控制的本地 LAN 计算机的应用端口号。（LAN to WAN 的 TCP/UDP 数据包的源端口号，WAN to LAN 的 TCP/UDP 数据包的目的端口号）
- **外部 IP 地址：** 想要控制的远程 WAN 计算机的 IP 地址。（LAN to WAN 的 IP 数据包的目的 IP 地址，WAN to LAN 的 IP 数据包的源 IP 地址）
- **外部端口：**想要控制的远程 WAN 计算机的应用端口号。（LAN to WAN 的 TCP/UDP 数据包的目的端口号，WAN to LAN 的 TCP/UDP 数据包的源端口号）
- **时间表：**策略的优先时间表。

# 虚拟服务器

TCP 和 UDP 网络端口是 16 位的数字，主要用于识别应用服务的，以决定如何转发。一些端口已经由 IANA（Internet 地址指派机构）预先分配，请参考知名端口部分。服务器通常都遵循知名端口的定义，所以客户端可以找到他们。

如果您在网络上运行一个可以从 WAN 访问到的服务器（例如从 Internet 上的其他计算机），或接受进入连接的任何应用程序（例如，对等/P2P 软件，如即时消息应用程序和 P2P 文件共享应用程序），和使用的 NAT（网络地址转换），您要配置路由器使用指定的端口转发这些进入连接到网络中运行此程序的 PC。如果您想架设一台网络游戏服务器，您还要使用端口转发功能。

原因是，在使用 NAT 的时候，您的公用可访问 IP 是路由器在使用并指向路由器，它需要传送所有数据流到您 PC 使用的私有 IP 地址。请参考本手册的 WAN 配置部分的 NAT 信息。

Internet 地址指派机构(IANA)是为 Internet 协议分配唯一的参数值的主要协调员。端口号范围是 0-65535，但是只有 0-1023 保留给专有服务，也就是熟知的知名端口。注册的端口是从 1024-49151。剩下的端口都是动态端口或私有端口，范围是 49152-65535。

下面是知名端口和注册端口的例子，若要获取进一步的信息，请参考IANA的网站 http://www.iana.org/assignments/port-numbers

**熟知的端口和注册端口列表**

| 端口号 | 协议 | 描述 |
|---|---|---|
| 20 | TCP | FTP 数据 |
| 21 | TCP | FTP 控制 |
| 22 | TCP & UDP | SSH 远程登录协议 |
| 23 | TCP | Telnet |
| 25 | TCP | SMTP（简单邮件传输协议） |
| 53 | TCP & UDP | DNS（域名解析系统） |
| 69 | UDP | TFTP（简单文件传输协议） |
| 80 | TCP | HTTP |
| 110 | TCP | POP3（邮局协议 v3） |
| 119 | TCP | NEWS （网络新闻传输协议） |
| 123 | UDP | NTP（网络时间协议） |
| 161 | TCP | SNMP |
| 443 | TCP & UDP | HTTPS |
| 1503 | TCP | T.120 |
| 1720 | TCP | H.323 |
| 4000 | TCP | ICQ |
| 7070 | UDP | RealAudio |

## 端口映射


- **应用：**选择想配置的服务。
- **协议：** 当从下拉选项种选择应用或协议。
- **外部端口&内部端口：**输入想要配置的端口号和范围。
- **内部 IP 地址：** 输入内部服务器的 IP 地址，用来响应指定端口发送的请求。
- **添加：** 点击可以添加一条虚拟服务器规则。
- **编辑：** 点选虚拟服务器规则进行编辑，然后点击**编辑/删除**。
- **删除：**点选虚拟服务器规则进行删除，然后点击**编辑/删除**。

既然 NAT 是 Internet 防火墙的天然防火墙，您的路由器就可以保护您的网络防止外部用户访问。因为所有进入连接都指向您的路由器，除非您创建虚拟服务器规则转发特定端口服务到网络中的 PC。当您的路由器需要允许外部用户访问内部服务器的时候，例如 web 服务器，FTP 服务器，Email 服务器或游戏服务器，路由器就好像是个虚拟服务器。您可以安装制定的端口号用于本地服务器的指定服务，例如 web/HTTP（80 端口），FTP（21 端口），Telnet（23 端口），SMTP（25 端口）或 POP3（110 端口）。当路由器接收到访问的请求，它就会转发到相应的内部服务器。

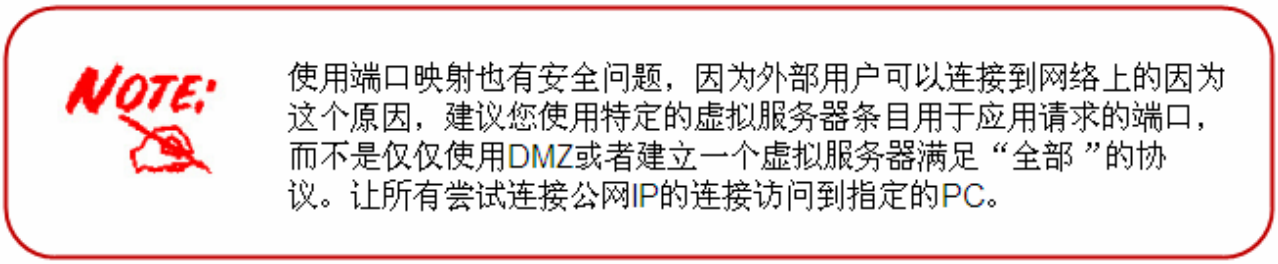
例如，如果设置 80 端口(Web/HTTP)映射到 IP 地址 192.168.1.2，然后所有从外部用户发送

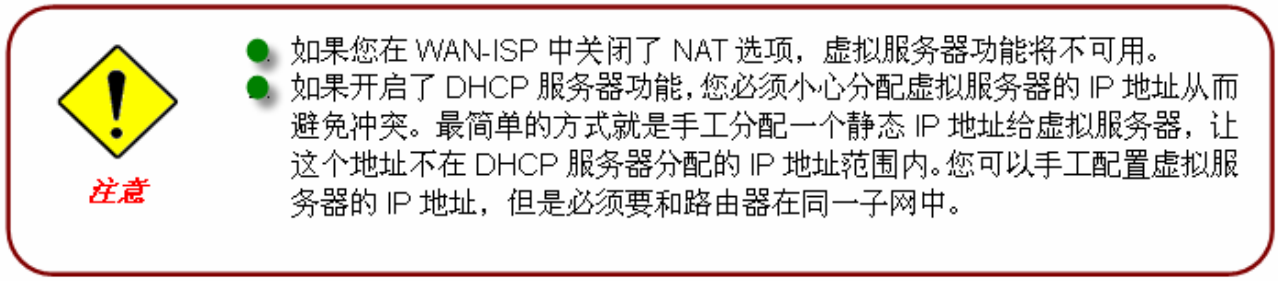
的 HTTP 请求都将被转发到 192.168.1.2 的这台本地服务器(PC)。如果端口号没有列在预定义的应用中，需要手动添加。


除了指定使用的端口号以外，您还要指定使用的协议。协议通常由特定的应用决定。大多数应用使用 TCP 或 UDP，然而您可以从**协议**下拉选项中选择其他协议。

## DMZ

DMZ 主机就是暴露在 Internet 上的本地主机。当设置一个特定的内部 IP 地址的 DMZ 主机，所有的进入数据包都将被防火墙和 NAT 算法检查，然后数据包被转发到 DMZ 主机上而不使用其他虚拟服务器规则条目使用的端口号。

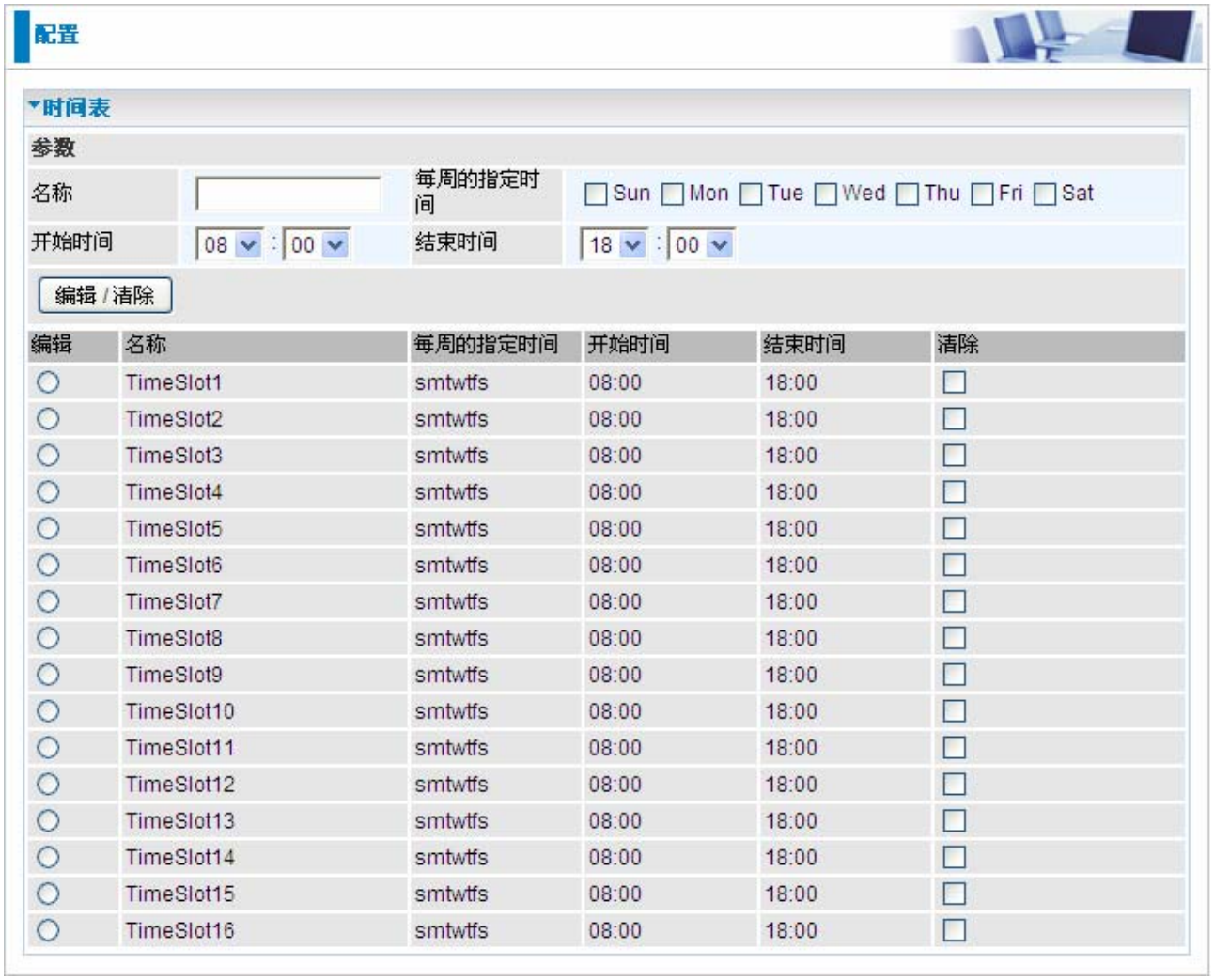
# 从 LAN 唤醒

从LAN唤醒 (WOL) 这项功能为远程站点打开/启动计算机提供了很大的灵活性。.


- **MAC 地址：**输入目标计算机的MAC 地址，您可以从 MAC 地址的下拉菜单中直接选择。
- **Select:** 您可以从列表中选在MAC地址。

# 时间表

时间表最多支持 16 个时间槽，可以帮助管理 Internet 连接。在每个时间配置文件中，您可以指定特定的时间段，例如从周一到周日限制或允许用户或应用程序使用 Internet。
这个时间表和路由器的时间息息相关，因为路由器主板上的时钟不是真实的时间，需要使用简单网络时间协议 (SNTP) 从 Internet 的 SNTP 服务器获得当前时间信息。参考**时区**获取详细信息。您的路由器时间应该设定为当地时间。如果时间设定不正确，您的时间表将不能正常工作。




- **名称：**用户自定义的时间表描述名称。
- **每周的指定时间：**指定时间表应用的具体时间。默认是全选的。
- **开始时间：** 可以指定时间表的开始时间，默认是 8:00 AM。
- **结束时间：**可以指定时间表的结束时间，默认是 18:00 AM。

# 高级

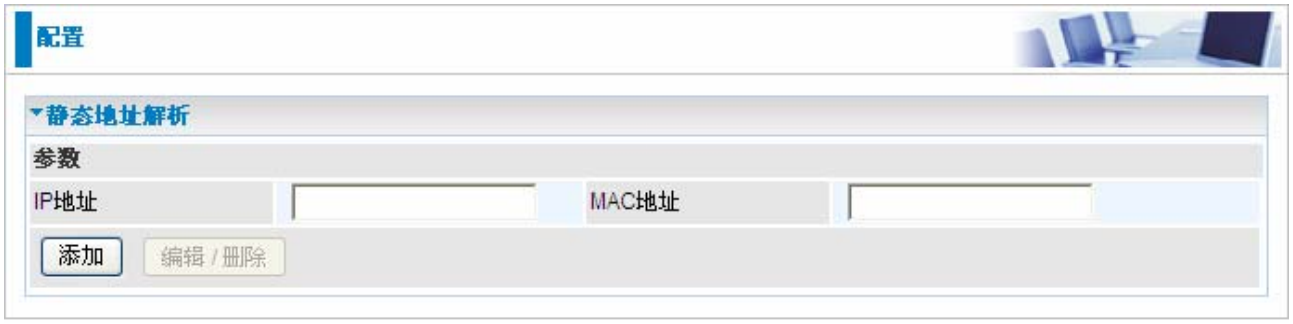
用户可以在**高级**配置选项中配置路由器的高级功能。如果用户不清楚这项功能，在没有技术支持人员的帮助下最好不要重新配置路由器。

**高级**菜单下有 8 个子菜单：**静态路由**，**静态地址解析**，**动态域名解析**，**VLAN**，**设备管理**，**IGMP**，**SNMP** **接入控制**和**远程接入**。

## 静态路由


- **目的地：**目的子网地址。
- **子网掩码：**与目的子网地址相关的子网掩码。
- **网关：**转发数据包的下一跳地址。
- **接口：**选择转发数据包的接口。
- **开销：**路由传输的开销。这个数字可以根据实际情况进行定义，输入范围是 0-65535。

## 静态 ARP




- **IP 地址:** 填写发送数据包的主机的 IP 地址。
- **MAC 地址:** 填写转发数据包的主机的 MAC 地址。

## 动态域名解析

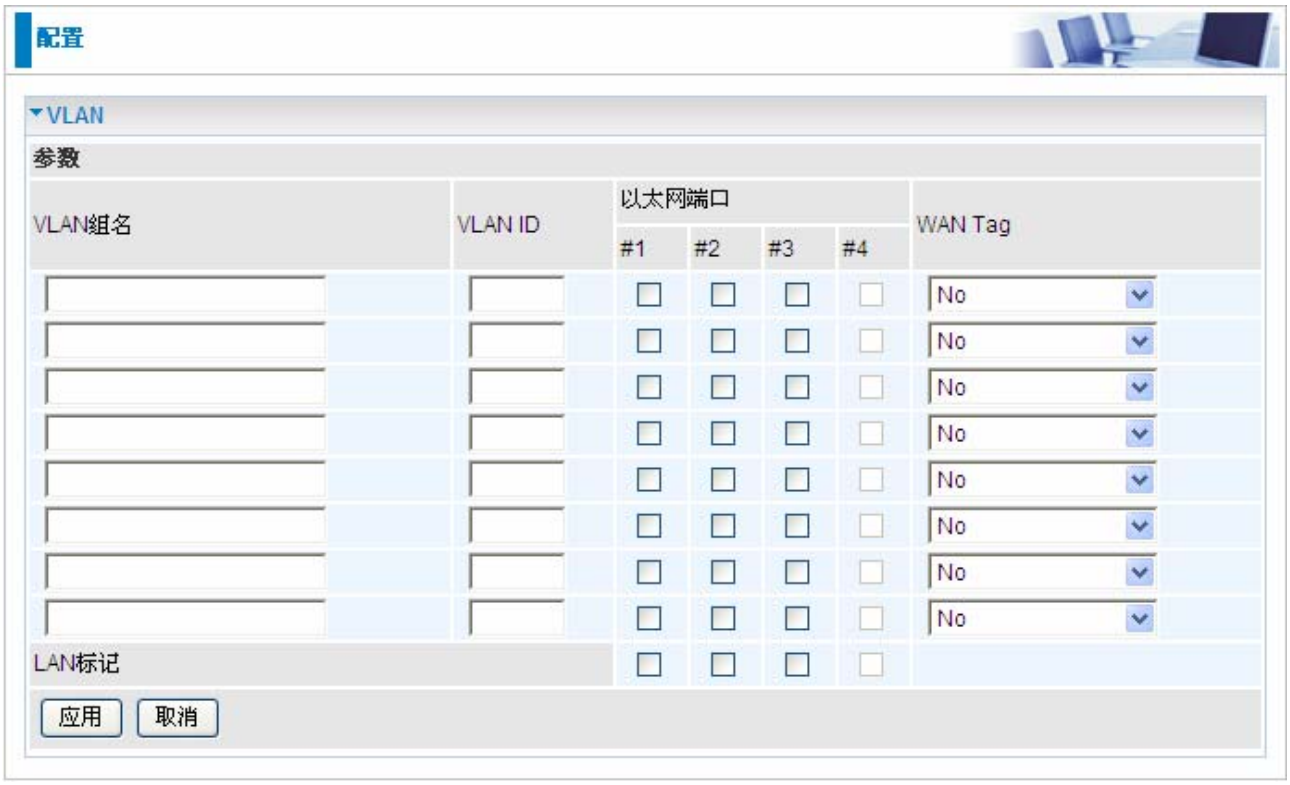
动态域名解析功能让您为动态的 IP 地址映射一个静态的主机名，所以如果您的 ISP 即使不分配静态的 IP 地址，您仍然可以使用 DNS 名称进行访问。这通常用于通过动态 IP 连接的主机，使得任何人可以通过 DNS 名访问到你，而不是通过随时会变得动态 IP 地址。动态 IP 地址是 ISP 分配给您的路由器 WAN 接口的 IP 地址。

您首先需要使用DDNS提供商的网站，例如http://www.dyndns.org/，去注册一个DDNS帐户。


- **关闭：**勾选可以关闭动态域名解析功能。
- **开启：**勾选可以开启动态域名解析功能。
- **动态域名解析服务器：**选择您申请帐号的 DDNS 服务器。
- **通配符：**勾选这个选项开启 DDNS 通配符。
- **域名，用户名和密码：**输入注册服务的域名，用户名和密码。
- **周期：**设置路由器和 DDNS 服务器交换信息的时间。除了定期更新以外，在动态 IP 地址更改以后还将执行路由器更新。

## VLAN

VLAN（虚拟局域网）是在不同的物理 LAN 网段中能够互相通讯的一组设备，就好像是在同一个物理 LAN 网段中进行通讯。



## 设备管理

高级配置的设备管理允许您控制路由器的安全选项和设备的监控功能。


**内置 Web 服务器：**

**HTTP 端口：**路由器内置的 Web 服务器的端口是用于基于 web 的配置。标准 HTTP 端口的默认值是 80。如果您在 LAN 中的 PC 上运行 web 服务器，您可以改变这个默认端口。

**例如：**把HTTP端口改成 **100**，指定他们的IP地址是 **192.168.1.55**，然后设置到期自动注销时间是 100 分钟。这样就只能允许用户A在浏览器中输入**http://192.168.1.254:100**从 **192.168.1.55** 的IP地址访问。100 分钟以后，设备将自动注销用户A。

**即插即用(UPnP)：**

UPnP 给 PC 和其他网络设备提供了对等网络的连通性，并在设备之间提供了数据控制和传输的功能。通过使用 UPnP NAT Traversal，UPnP 给使用 NAT 路由器的用户提供了很多优势，并且在支持的系统上，通过让应用程序控制必要的设定，移除用户对控制设备高级配置的需要，来让端口转发等任务变得更加容易。

除了路由器支持以外，用户操作系统和相关应用程序都必须支持 UPnP。Windows XP 和 Windows Me 本来就支持 UPnP（在安装这个组件以后），Windows 98 用户可能需要安装 Windows XP 的 Internet 连接共享客户端来支持 UPnP。Windows 2000 不支持 UPnP。

**关闭：**可以关闭路由器的 UPnP 功能。

**开启：**可以开启路由器的 UPnP 功能

**UPnP端口：** 默认端口是2800。强烈建议使用默认端口。

如果这个端口和其他使用中的端口冲突，您就必须更改端口。

## 参考以下步骤在 Windows XP 中安装 UPnP

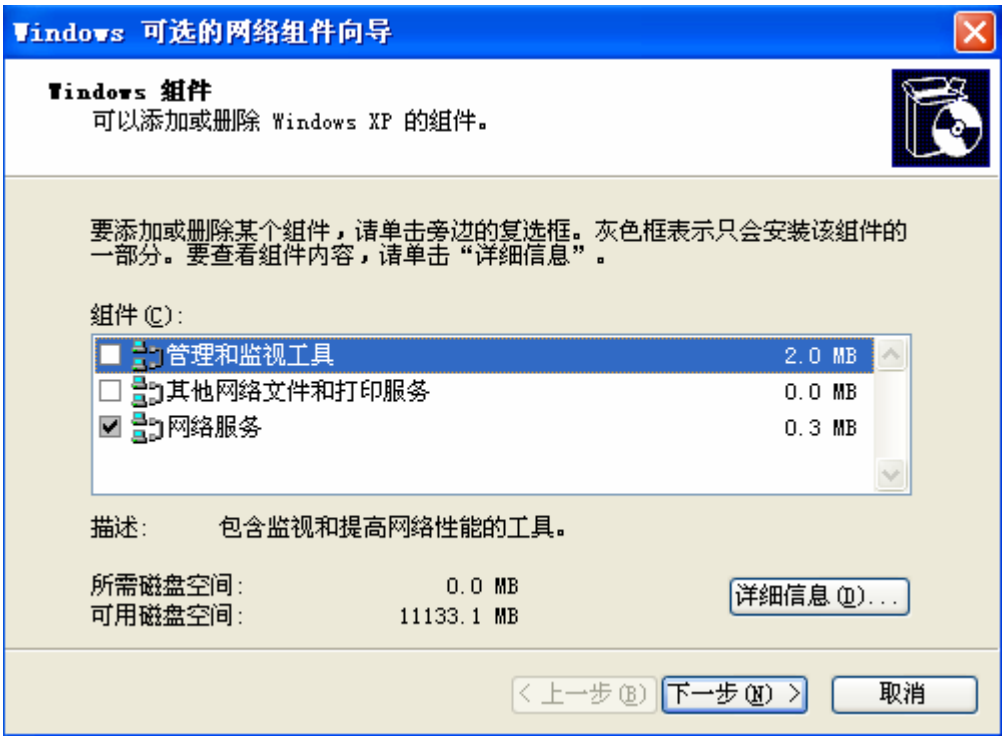
**步骤1：**点击开始和控制面板。

**步骤2：**双击网络连接。

**步骤3：**在网络连接窗口中，在菜单栏中点击高级并选择可选网络组件…

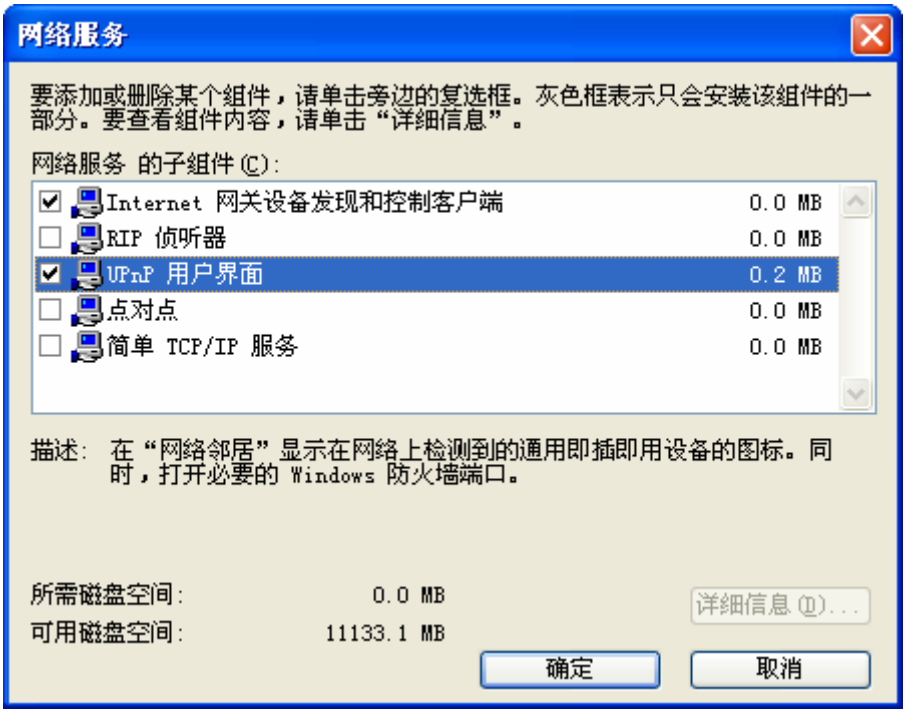

显示Windows可选的网络组件向导窗口。

**步骤4：**在组件中选择网络服务并点击详细信息。




**步骤5：**在网络服务窗口选择UpnP用户界面。

**步骤6：**点击**确定**回到Windows可选的网络组件向导窗口，然后点击**下一步**。

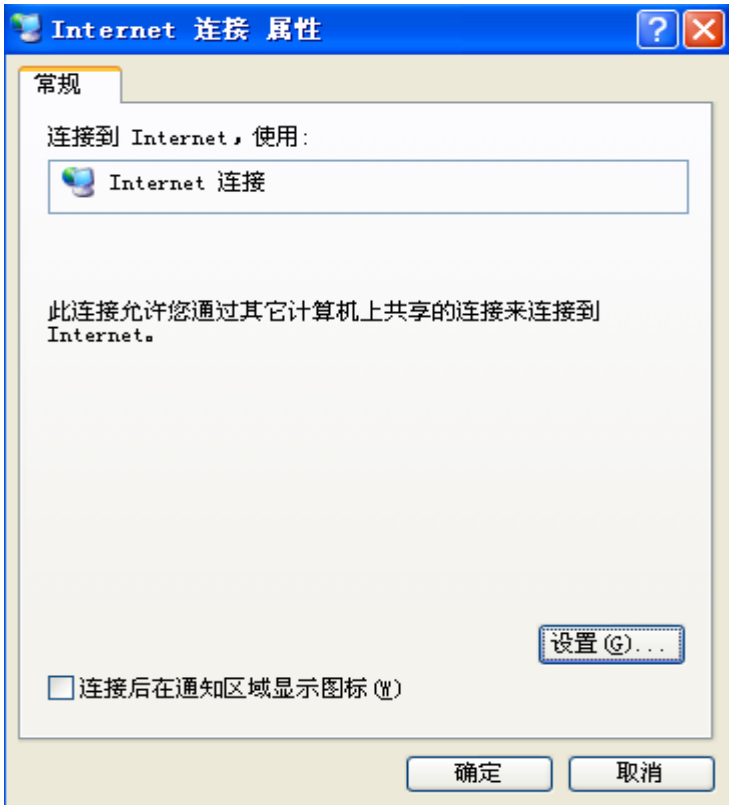


**自动发现启用 UPnP 的网络设备**

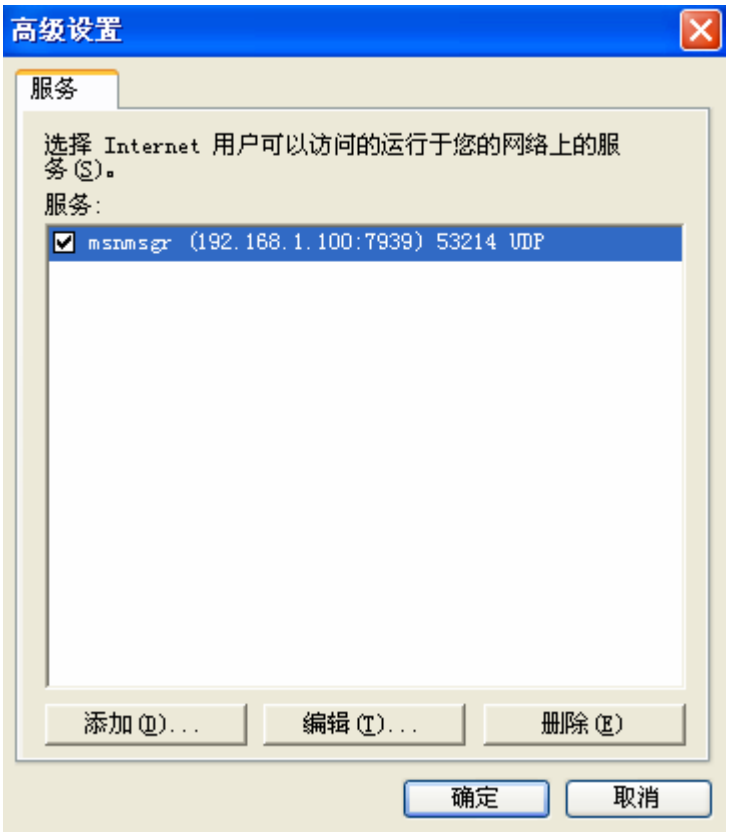
**步骤1：**点击开始和控制面板。双击网络连接。 会在Internet网关下显示了一个图标。

**步骤2：**右键点击这个图标，然后选择属性。


**步骤3：**在Internet连接属性窗口中点击设置查看自动创建的端口映射。

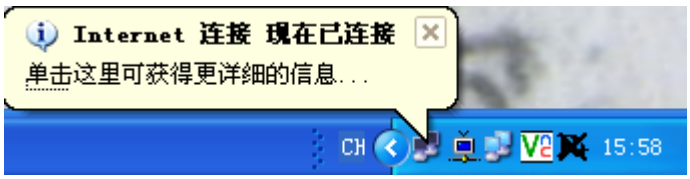


**步骤 4：**您可以编辑或删除端口映射或点击添加手动添加端口映射。





**步骤5：**选择**在连接后通知区域显示图标**然后点击**确定**。在系统托盘处可以看到该图标。



**步骤6：**双击图标显示当前Internet连接状态。

**简单访问 Web 配置器**

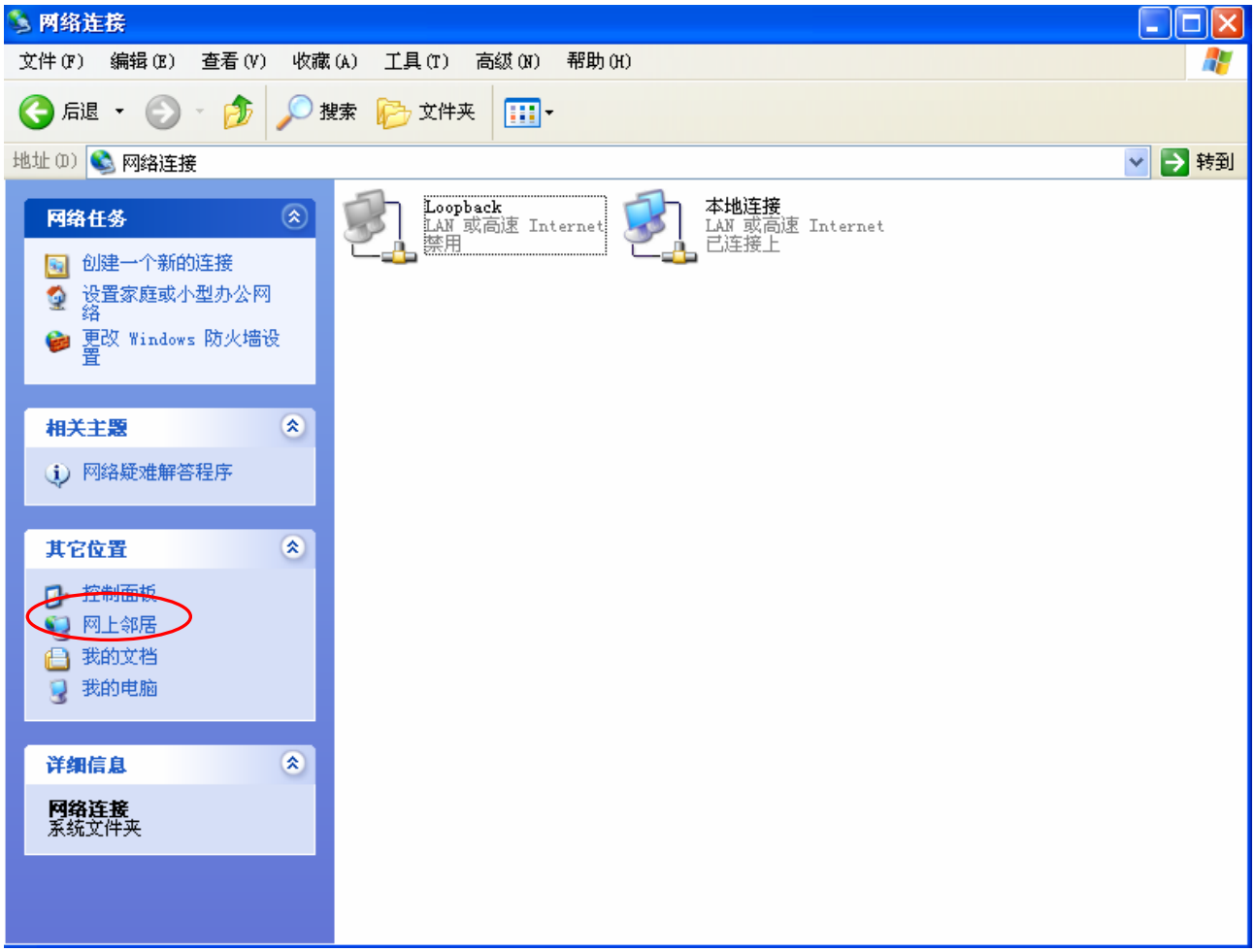
使用UPnP，您不需要找出路由器的IP地址就可以访问BiPAC 6200NXL 的web配置界面。

参考以下步骤访问web配置界面。

**步骤1：**点击开始然后点击控制面板。

**步骤2：**双击网络连接。

**步骤3：**在其他位置栏点击网上邻居。




**步骤4：**在本地网络中会显示一个图标表示启用UPnP的设备。

**步骤5：**右击BiPAC 6200NXL的图标然后选择调用。这样就可以进入web配置的登录界面。

**步骤6：**右击BiPAC 6200NXL的图标然后选择属性。 属性窗口将会显示BiPAC 6200NXL的基本信息。

## IGMP

GMP 全称 Internet 组管理协议，用于群播群组的管理。


- **IGMP Proxy**：接收组播数据包。默认是**关闭**的。
- **IGMP Snooping**：允许交换的以太网/无线网络检查并做出正确的转发决定。默认是**关闭**的。

## SNMP 接入控制

LAN 中的 PC 需要软件支持这个功能——简单网络管理协议。


**SNMP V1 and V2:**

**读社区：**指定读社区的名称和 IP 地址。根据输入配置文件的字符串检查这个社区字符串。一旦字符串名称相符，用户的这个 IP 地址就可以查看数据。

**写社区：**指定写社区的名称和 IP 地址。根据输入配置文件的字符串检查这个社区字符串。一旦字符串名称相符，用户的这个 IP 地址就可以更改数据。

**SNMP V3:**

指定认证的用户名和密码。然后定义认证 IP 地址的访问权限。一旦认证成功，用户的那个 IP 地址就可以查看和更改数据。

**SNMP 版本：SNMPV2c 和 SNMPv3**

SNMPv2c 是没有 SNMPv2 安全功能的加强协议功能的组合。”c”来源于 SNMPv2c 为了安全而使用 SNMPv1 的社区字符串参数，但这却是普遍承认的 SNMPv2 标准。

SNMPv3 是一种强有力的认证机制，能够为远程监控提供细粒度的认证。

以下列出了支持的 MIB。

**RFC 1213 (MIB-II)：**

☑ 系统组

☑ 接口组

☑ 地址翻译组

☑ IP 组

☑ ICMP 组

☑ TCP 组

☑ UDP 组

☒ EGP（不可用）

☑ 传输

☑ SNMP 组

**RFC1650 (EtherLike-MIB)：**

☑ dot3Stats

**RFC 1493 (Bridge MIB)：**

☑ dot1dBase 组

☑ dot1dTp 组

☑ dot1dStp 组（如果配置生成树）

**RFC 1471 (PPP/LCP MIB)：**

☑ pppLink 组

☒ pppLqr 组

**RFC 1472 (PPP/Security MIB)：**

☑ PPP 安全组

**RFC 1473 (PPP/IP MIB)：**

☑ PPP IP 组

**RFC 1474 (PPP/Bridge MIB)：**

☑ PPP 桥接组

**RFC1573 (IfMIB)：**

☑ ifMIBObjects 组

**RFC1695 (atmMIB)：**

☑ atmMIBObjects

**RFC 1907 (SNMPv2)：**

仅支持 snmpSetSerialNo OID

## 远程接入


**远程接入控制:**

**开启：**选择开启允许远程接入（大多数情况下是从 Internet）。

**持续时间：**设定时间参数允许远程接入的持续时间。0 表示永续。

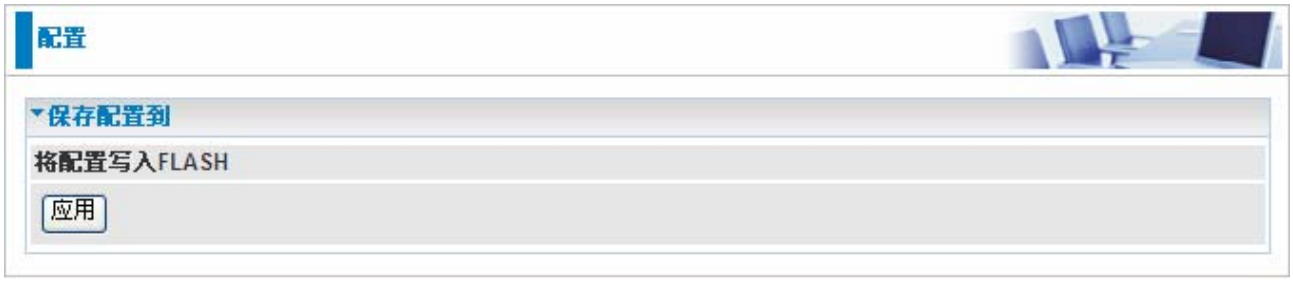
**允许接入 IP 地址范围：**

**有效：**选择有效允许此 IP 地址范围中的主机远程接入。

**IP 地址范围：**指定允许远程接入的 IP 地址。点击添加可以增加 IP 地址列表。

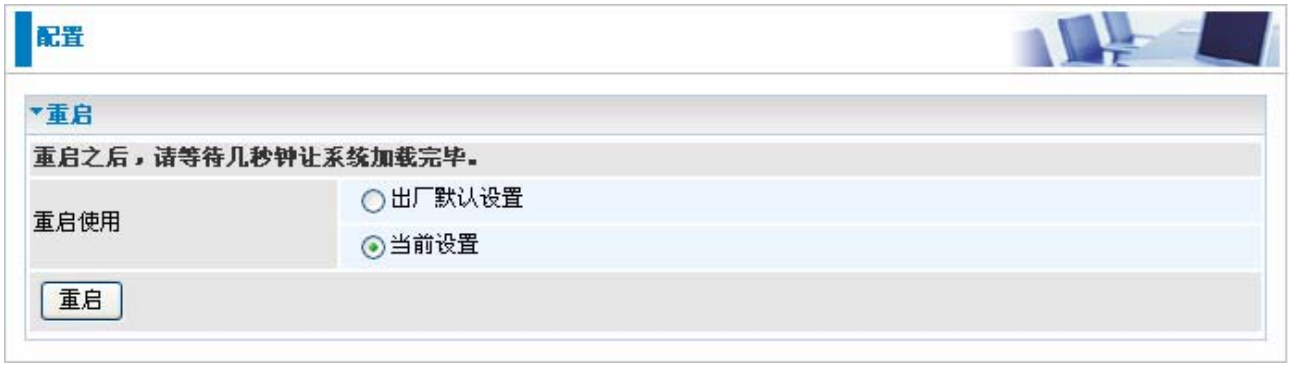
# 保存设置到 Flash

在更改路由器的配置以后，您必须把配置参数保存在 FLASH 中，防止在关闭或重启路由器以后丢失这些参数。点击 “**保存设置**“ 然后点击 “**应用**” 保存配置信息到 FLASH。




# 重启

点击**重启**，然后选择**当前设置**重新启动路由器。（恢复到上次保存的路由器配置）




如果您想重启路由器并恢复到出厂默认设置（例如，在升级过固件以后或者在保存了错误的配置信息以后），选择**出厂默认设置**把路由器重置到出厂默认设置。

# 注销

要退出路由器的 web 管理界面，点击**注销**。请在注销之前保存配置。

要注意路由器在同一时间只能允许一台 PC 访问 web 配置界面，在当前 PC 没有注销之前其他的 PC 都不能访问。如果先前的 PC 忘记注销，那么第二台 PC 只有在用户定义的自动注销时间过去以后才能访问，默认是 3 分钟。您可以通过 web 管理界面的**高级-设备管理**来配置这个数值。请参考本手册的**高级**部分获取更多信息。

# 第六章: 故障排除

如果 3G 路由器不能够正常工作，您可以参考本章在联系服务提供商或 Billion 技术之前进行简单的故障排错。

## 路由器启动的问题

| 问题 | 建议解决办法 |
| --- | --- |
| **当您打开路由器的时候所有的 LED 都不亮** | 检查网络适配器和路由器之间的连接。如果仍然出现错误，您可能遇到硬件问题。如果是这样，请与服务提供商或联系技术支持。 |

## LAN 接口的问题

| 问题 | 建议解决办法 |
| --- | --- |
| **在 LAN 端无法 Ping 通任何 PC** | 检查前端面板的以太网 LED。如果有 PC 相连，LED 应该是亮的。如果不亮，请检查路由器和 PC 之间的网线是否正确廉洁。确保在 卸载了所有软件防火墙之后进行故障排错。<br>确保路由器和工作站之间的 IP 地址和子网掩码是一致的。 |