BiPAC 74XX

3G/VoIP/ (802.11g/802.11n)
宽带/ADSL2+ (VPN) 防火墙路由器

用户手册

发行版本：5.53.S6

最后修改时间：2-22-10

目 录

第 1 章：产品入门

产品介绍

欢迎使用 74XX 系列防火墙路由器。这是一款多合一的路由器，包括 ADSL 调制解调器，ADSL/宽带路由器和以太网交换机，可以满足您使用 ADSL/ 宽带连接到 Internet 的需求。通过 ADSL/宽带快速安装向导和 DHCP 服务器，您只要简单配置就可以登录，满足了新用户对高级功能以及 Internet 连接和网络管理的要求。

功能特性

- **快速的 Internet 接入**

产品符合 ADSL 全球标准。ADSL2/2+ 标准支持最高可达 12/24 Mbps 的下行速率，ADSL 支持最高可达 8Mbps 的下行速率。用户不但能够享用高速的 ADSL 服务，还能够享用多种宽带多媒体应用，如互动游戏，视频流媒体和实时音频媒体，而且比以往更加简单快捷。路由器支持多种模式标准 (ANSI T1.413，Issue 2，G.dmt (ITU G.992.1)，G.hs (ITU G994.1)，G.dmt.bis (ITU G.992.3) 和 G.dmt.bisplus (ITU G.992.5)。

- **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 802.11g/802.11n 无线 AP（仅适用于无线路由器）**

路由器集成了 802.11g/802.11n 无线接入点，可以在有线网络，无线网络和宽带连接 (ADSL) 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 54Mbps 的 802.11g 标准以外，还能够向下兼容现有的支持 802.11b 标准的设备。支持的 Wi-Fi 网络安全存取 (WPA) 和有线对等保密 (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**

除了通过 3G/ADSL 可以连接到 Internet， BiPAC74XX 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。

- **EWAN**

集成的 4 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。

- **用多协议建立连接**

路由器支持 PPPoA（RFC 2364 – PPP 在 ATM 适配层 5），RFC1483 ATM 上的多协议封装（桥接或路由），PPP 在以太网上 (RFC2516)，用以连接到 ISP。还可以支持基于 VC 和 LLC 的多路复用。

快速安装向导

支持 WEB 用户图形界面，实现快速安装。通过快速安装向导，用户输入 ISP 提供的信息后，即可进行网上冲浪。

通用即插即用 (UPnP) 和 UPnP NAT 穿透

此协议用于在不同厂商的独立设备和 PC 之间建立简单而稳定的连接，使网络的安装变得简单，使费用在用户可以承受的范围之内。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 实现无缝的邻近组网。利用这个功能，您可以无缝地连接到 NetMeeting 或 MSN Messenger。

网络地址转换 (NAT)

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。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 电话等。

具有 DoS 和 SPI 的 SOHO 防火墙

除了内置 NAT 天然防火墙外，路由器还提供高级黑客过滤保护功能。它能自动检测和阻止拒绝服务 (DoS) 攻击。路由器具有状态封包检查功能，决定是否允许数据包通过防火墙进入 LAN 中。

域名解析系统中继

域名解析系统 (DNS) 中继提供映射域名（用户友好的域名，如 www.yahoo. com）到 IP 地址的简单方法。当本地计算机把 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中的真实 DNS。

动态域名解析系统 (DDNS)

动态 DNS 服务允许您给动态 IP 地址映射一个静态主机别名。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 服务那儿申请一个帐户，如 http://www.dyndns.org/。能够支持超过 5 个 DDNS 服务器。

服务质量 (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（端口转发）

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。

丰富的包过滤功能

这个功能不仅过滤基于 IP 地址和端口号的数据包，还过滤来往 Internet 的数据包，提供了高级别的

安全控制。

动态主机配置协议 (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 服务器可以分配一系列客户端 IP 地址，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。

静态路由和 RIP1/2 路由

具有路由功能，提供简易的静态路由表或 RIP1/2 路由协议。

简单网络管理协议 (SNMP)

这是一种通过 SNMP 远程管理路由器的简单方法。

基于 Web 的 GUI

支持基于 web 的 GUI 用户友好界面提供了简单的配置、管理以及联机帮助。还为远程用户配置和管理设备提供远程管理功能。

可升级的固件

您可以通过基于 WEB 的 GUI 把路由器升级到最新的固件版本。

丰富的管理端口

提供灵活的管理端口，包括本地控制端口、LAN 端口以及 WAN 端口。用户可以通过控制端口使用终端应用配置和管理设备，或通过 LAN 或 WAN 端口使用 Telnet、WEB GUI 以及 SNMP 配置和管理设备。

虚拟专用网 (VPN)

允许用户直接与远程站点之间建立安全传输数据的隧道。用户可以使用路由器本身提供的 PPTP、L2TP 客户端程序/服务端程序、IKE 以及 IPSec，建立 VPN 连接。由于路由器已提供了建立 VPN 连接的 IPSec 和 PPTP 穿透功能，若用户想在本机上运行 PPTP 客户端程序，就可以直接运行了。

BiPAC 74xx/64xx Series Firewall Routers Feature Comparison Table

	BiPAC Model											
	7402 X	7402 XL	7402G X	7402G XL	7402N X	7402 NXL	7404 VGPX	7404V GOX	7404 VNOX	7404 VNPX	6404 VGO X	6404 VGPX
Wireless			●	●	●	●	●	●	●	●	●	●
VPN	●		●		●			●	●		●	
3G	●	●	●	●	●	●	●	●	●	●	●	●
QoS	●	●	●	●	●	●	●	●	●	●	●	●
VoIP							●	●	●	●	●	●
Firewall	●	●	●	●	●	●	●	●	●	●	●	●
Virtual Server	●	●	●	●	●	●	●	●	●	●	●	●
Time Schedule	●	●	●	●	●	●	●	●	●	●	●	●
Remote Access	●	●	●	●	●	●	●	●	●	●	●	●
Static Route	●	●	●	●	●	●	●	●	●	●	●	●
Static ARP	●	●	●	●	●	●	●	●	●	●	●	●
DDNS	●	●	●	●	●	●	●	●	●	●	●	●
IGMP	●	●	●	●	●	●	●	●	●	●	●	●
VLAN Bridge	●	●	●	●	●	●	●		●	●	●	●
Device Management	●	●	●	●	●	●	●	●	●	●	●	●
Web Firmware Upgrade	●	●	●	●	●	●	●	●	●	●	●	●
User Management	●	●	●	●	●	●	●	●	●	●	●	●

第 2 章：产品安装

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。
- 不要和其他设备共用相同的电源。
- 不要自己打开或维修设备。如果产品太烫了，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及其附件。

注意

- 请把产品放置在平稳的平面。
- 只可以使用包装中的电源适配器。使用不同额定电压的电源适配器可能会导致路由器损坏。

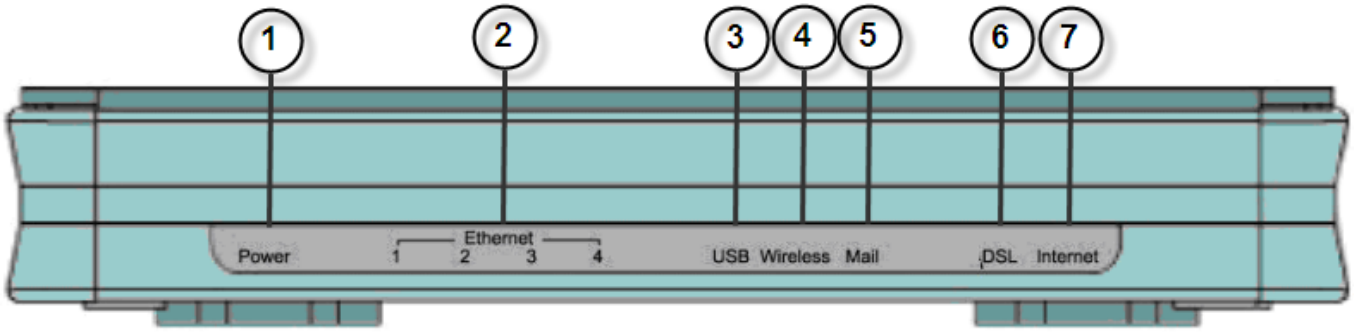
产品列表

- **3G/VoIP/(802.11g/802.11n) 宽带/ADSL2+ (VPN) 防火墙路由器**
- 包含在线手册的 **CD-ROM**
- **RJ-11 ADSL/电话线**
- 以太网 **(CAT-5)** 线缆
- **RJ-45 到 RS-232 转接头**
- 电源适配器
- 可拆分天线
- 快速安装向导

设备描述

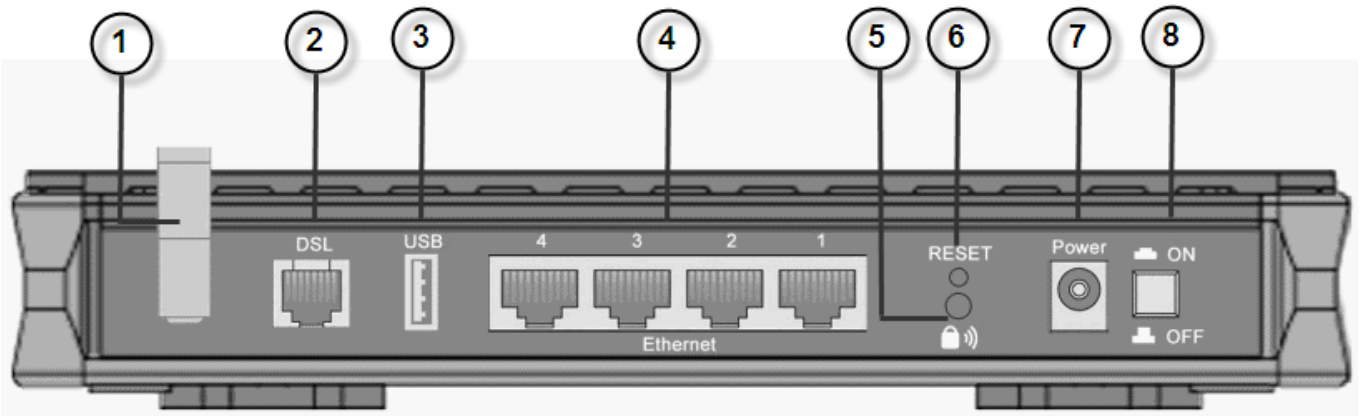
7402X/7402XL/7402GX/7402GXL

前端面板的 **LED**



LED		描述
1	**Power**	当电源插上的时候灯是橙色； 当系统就绪的是时候灯是绿色； 红灯亮表示系统出现故障。重启设备或联系 Billion 以获得技术支持。
2	**LAN 端口** **1X - 4X** （RJ-45 连接器）	LAN 端口连接到以太网设备时，灯亮。 绿灯表示传输速度达到 100Mbps； 橙色灯表示传输速度达到 10Mbps。 灯闪表示正在传输/接收数据。
3	**USB**	当连接到 USB 设备的时候灯是绿色。 灯闪表示正在发送/接收数据。
4	**Wireless**	当已建立无线连接的时候灯是绿色。 灯闪表示正在发送/接收数据。
5	**Mail**	绿灯亮表示收件箱中有邮件。
6	**DSL**	当成功连接到 ADSL DSLAM（线路同步）的时候灯是绿色。
7	**Internet**	绿灯表示 WAN 端口成功获得 IP 地址； 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； 红灯表示 WAN 端口无法获得 IP 地址； 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

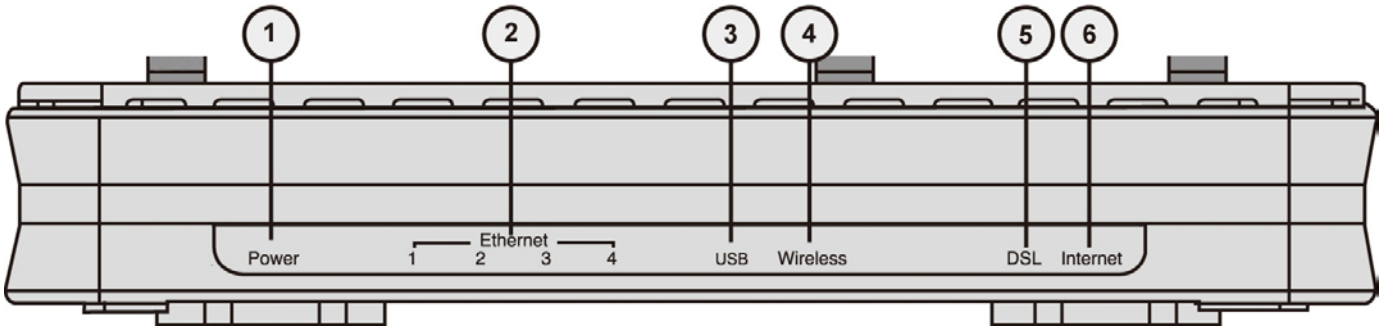


NOTE: 以太网端口 **4** 可以作为控制端口使用。需要专门的控制工具（已包含在产品清单中）来连接 **LAN** 端口 **4** 和 **PC** 的 **RS-232** 端口（**9** 针串行端口）。

端口		描述
1	天线（仅限无线路由器）	连接到可拆分的天线。
2	**DSL**	如果连接的是 ADSL/电话网络，另一端连接到 RJ-11 电话线缆。
3	**USB**	连接 USB 线缆。
4	**Ethernet** **1X — 4X** （RJ-45 连接器）	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。 注：端口 4 可以是 LAN 端口或控制端口，但不能同时是。 端口 1 可以当作 EWAN 端口。
5	**WPS**	按住 WPS 按钮，启用 Wi-Fi 保护设置功能。
6	**RESET**	保证设备已经打开 → 按 RESET 按钮： **1-3 秒钟：**快速重设设备。 **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）。 注：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 Switch**	电源开关

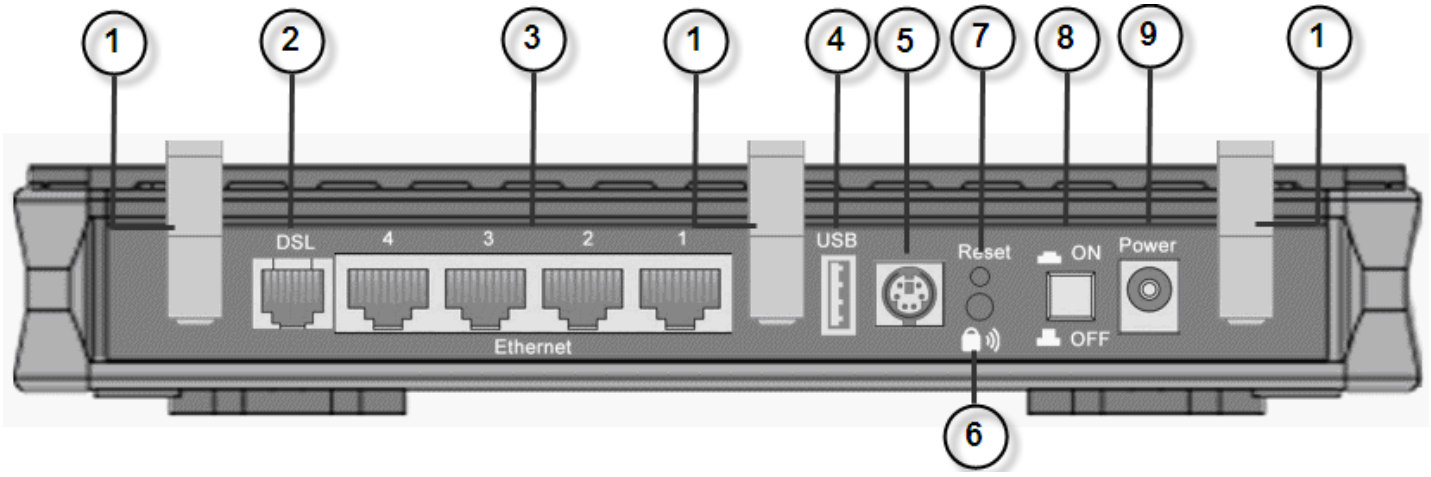
7402NX/7402NXL

前端面板的 LED



LED		描述
1	**Power**	当电源插上的时候灯是橙色； 当系统就绪的是时候灯是绿色； 红灯亮表示系统出现故障。重启设备或联系 Billion 以获得技术支持。
2	**LAN 端口** **1X - 4X** （RJ-45 连接器）	LAN 端口连接到以太网设备时，灯亮。 绿灯表示传输速度达到 1000Mbps； 橙色灯表示传输速度达到 100Mbps。 如果传输速度为 10Mbps，灯不亮。 灯闪表示正在传输/接收数据。
3	**USB**	当连接到 USB 设备的时候灯是绿色。 灯闪表示正在发送/接收数据。
4	**Wireless**	当已建立无线连接的时候灯是绿色。 灯闪表示正在发送/接收数据。
5	**DSL**	当成功连接到 ADSL DSLAM（线路同步）的时候灯是绿色
6	**Internet**	绿灯表示 WAN 端口成功获得 IP 地址； 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； 红灯表示 WAN 端口无法获得 IP 地址； 灯不亮表示设备处于桥接模式或 WAN 连接不存在。

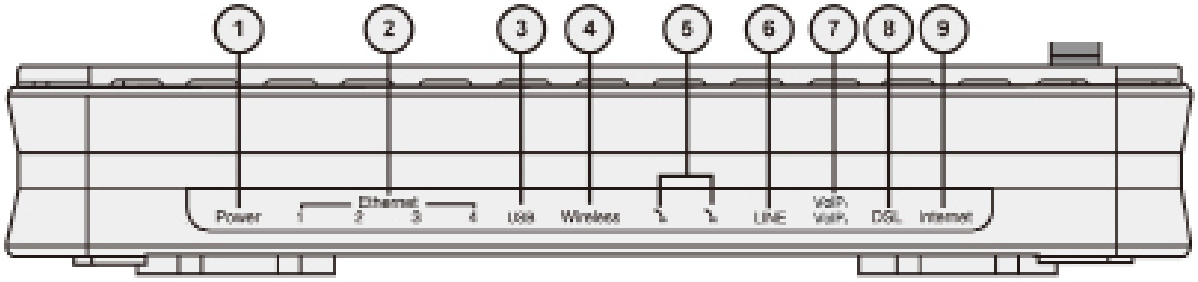
后端面板的端口



端口		描述
1	天线	连接到可拆分的天线。
2	**DSL**	连接的是 ADSL/ 电话网络，另一端连接到 RJ-11 电话线缆。
3	**Ethernet** **1X - 4X** （RJ-45 连接器）	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。 注：端口 4 可以是 LAN 端口或控制端口，但不能同时是。 端口 1 可以当作 EWAN 端口。
4	**USB**	连接 USB 线缆。 Internet 接入的 3G/ HSDPA USB 调制解调器备份。
5	**Console**	插入控制线缆。
6	**WPS**	按住 WPS 按钮，启用 Wi-Fi 保护设置功能。
7	**RESET**	保证设备已经打开 → 按 RESET 按钮： **1-3 秒钟：**快速重设设备。 **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）。 注：按住 RESET 按钮超过 6 秒钟后，保证设备再次通电。
8	**Power Switch**	电源开关
9	**Power**	用于连接电源适配器的插孔。

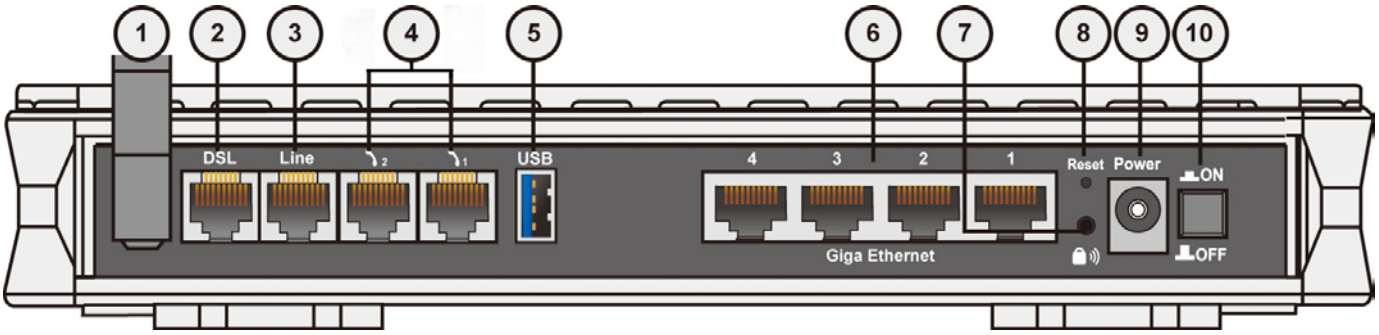
7404VGOX/7404VGPX/6404VGOX/6404VGPX

前端面板的 **LED**



LED		描述
1	**Power**	当电源插上的时候灯是橙色； 当系统就绪的是时候灯是绿色； 红灯亮表示系统出现故障。重启设备或联系 Billion 以获得技术支持
2	**以太网端口 1X - 4X（RJ-45 连接器）**	LAN 端口连接到以太网设备时，灯亮。 绿灯表示传输速度达到 100Mbps； 橙色灯表示传输速度达到 10Mbps。 灯闪表示正在传输/接收数据。
3	**USB**	当连接到 USB 设备的时候灯是绿色。 灯闪表示正在发送/接收数据。
4	**Wireless**	当已建立无线连接的时候灯是绿色。 灯闪表示正在发送/接收数据。
5	**电话 1x-2x（RJ-11 连接器）**	当电话摘机时灯是绿色。
6	**LINE（仅限带有 LINE 端口的路由器）**	当通过 PSTN 传输呼入和呼出电话时灯是绿色
7	**VoIP 1x-2x（RJ-11 连接器）**	SIP 注册好后 当电话 1 摘机时绿灯亮； 当电话 2 摘机时橙色灯亮。 ***注：橙色灯亮表示同时注册了电话 1 和电话 2。***
8	**DSL**	当成功连接到 ADSL DSLAM (“line synch”) 时是灯是绿色。 当有 PPPoA / PPPoE 连接时灯是橙色。
9	**Internet**	绿灯表示 WAN 端口成功获得 IP 地址； 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； 红灯表示 WAN 端口无法获得 IP 地址； 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

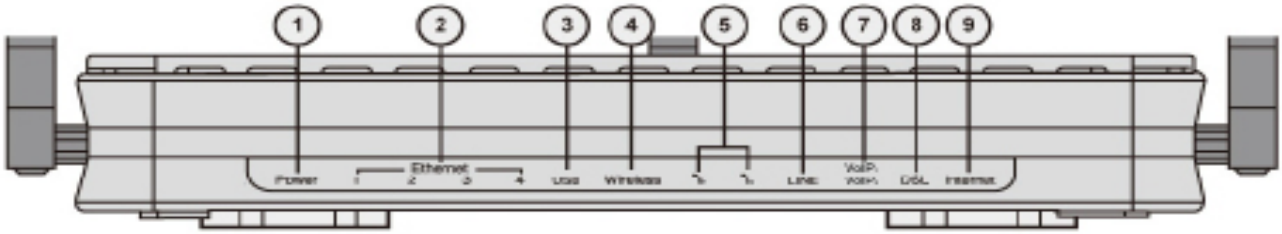


以太网端口 4 可以作为控制端口使用。需要专门的控制工具（已包含在产品清单中）来连接 LAN。

端口		描述
1	天线（仅限无线路由器）	连接到可拆分的天线。
2	**DSL**	连接的是 ADSL/电话网络时，另一端连接到 RJ-11（电话）线缆。
3	**LINE（仅限带有 LINE 端口的路由器）**	连接的是壁式电话插座时，另一端连接到 RJ-11 线缆。
4	**电话 1X - 2X** （RJ-11 连接器）	连接的是模拟电话机时，另一端连接到 RJ-11 线缆。
5	**USB**	连接 USB 线缆。
6	**Ethernet 1X - 4X** （RJ-45 连接器）	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。 注：端口 4 可以是 LAN 端口或控制端口，但不能同时是。 端口1可以当作EWAN端口。
7	**WPS**	按住 WPS 按钮，启用 Wi-Fi 保护设置功能。
8	**RESET**	保证设备已经打开 → 按 RESET 按钮： **1-3 秒钟：**快速重设设备。 **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）。 注：按住 RESET 按钮超过 6 秒钟后，保证设备再次通电。
9	**Power**	连接到提供的电源适配器。
10	**Power Switch**	电源开关

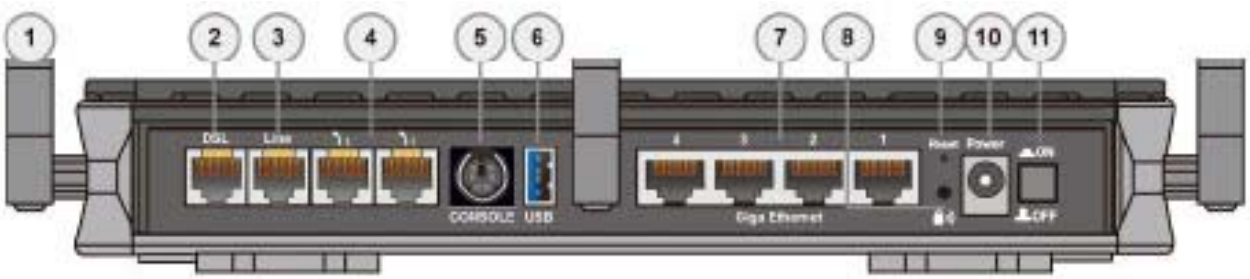
7404VNOX/7404VNPX

前端面板的 LED



LED		描述
1	**Power**	当电源插上的时候灯是橙色； 当系统就绪的是时候灯是绿色； 红灯亮表示系统出现故障，重启设备或联系 Billion 以获得技术支持。
2	**以太网端口** **1X - 4X** **（RJ-45 连接器）**	LAN 端口连接到以太网设备时，灯亮。 绿灯表示传输速度达到 1000Mbps； 橙色灯表示传输速度达到100Mbps； 传输速度为 10Mbps 时，灯不亮； 灯闪表示正在传输/接收数据。
3	**USB**	当连接到 USB 设备的时候灯是绿色。 绿灯闪表示正在发送/接收数据。
4	**Wireless**	当已建立无线连接的时候灯是绿色。 绿灯闪表示正在发送/接收数据。
5	**电话 1x-2x（RJ-11 连接器）**	当电话摘机时灯是绿色。
6	**LINE（仅限带有 LINE 端口的路由器）**	当通过 PSTN 传输呼入和呼出电话时灯是绿色
7	**VoIP 1x-2x** **（RJ-11 连接器）**	SIP 注册好后 当电话 1 摘机时绿灯亮； 当电话 2 摘机时橙色灯亮。 ***注：橙色灯亮表示同时注册了电话 1 和电话 2。***
8	**DSL**	当成功连接到 ADSL DSLAM (“line synch”) 时是灯是绿色。 当有 PPPoA / PPPoE 连接时灯是橙色。
9	**Internet**	绿灯表示 WAN 端口成功获得 IP 地址； 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； 红灯表示 WAN 端口无法获得 IP 地址； 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



NOTE: **以太网端口 4 可以作为控制端口使用。需要专门的控制工具（已包含在产品清单中）来连接 LAN。**

端口		描述
1	天线	连接到可拆分的天线。
2	**DSL**	连接的是 ADSL/ 电话网络，另一端连接到 RJ-11 电话线缆。
3	**LINE（仅限带有 LINE 端口的路由器）**	连接的是壁式电话插座时，另一端连接到 RJ-11 线缆。
4	**电话 1X - 2X**（RJ-11 连接器）	连接的是模拟电话机时，另一端连接到 RJ-11 线缆。
5	**Console**	插入连接控制端口的线缆。
6	**USB**	连接 USB 线缆。
7	**Ethernet 1x - 4x** （RJ-45 连接器）	连接到 10Mbps、100Mbps 或 1000Mbps 的 PC 或办公室/家庭网络时，UTP 以太网电缆（Cat-5 或 Cat-5e）连接到其中一个 LAN 端口。 注：端口 4 可以是 LAN 端口或控制端口，但不能同时是。 端口 1 可以当作 EWAN 端口。
8	**WPS**	按住 WPS 按钮，启用 Wi-Fi 保护设置功能。
9	**RESET**	保证设备已经打开 → 按 RESET 按钮： **1-3 秒钟：**快速重设设备。 **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）。 注：按住 RESET 按钮超过 6 秒钟后，保证设备再次通电。
10	**Power**	电源开关

11	**Power Switch**	用于连接电源适配器的插孔。

布线

引起问题的最常见原因之一：线缆或 ADSL/ 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 ADSL LED 是亮的。如果他们不亮，检查您是否使用的是 合适的线缆。

确保其他连接到同一个电话线的设备（例如电话，传真机，模拟调制解调器）都像您的路由器一样在墙壁的接口和他们之间连接着一个线路过滤器（除非您在使用一个有资质和认证的电工安装的中心分离器或中心过滤器）。要确保线路过滤器被正确安装。如果不安装或错误安装线路过滤器会造成 ADSL 连接问题，导致频繁断线。

第 3 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。

请按照以下步骤，进行 PC 网络环境安装。

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。

连接路由器

1.将路由器连接到 **LAN**（局域网）和 ADSL/电话 (**ADSL**) 网络。

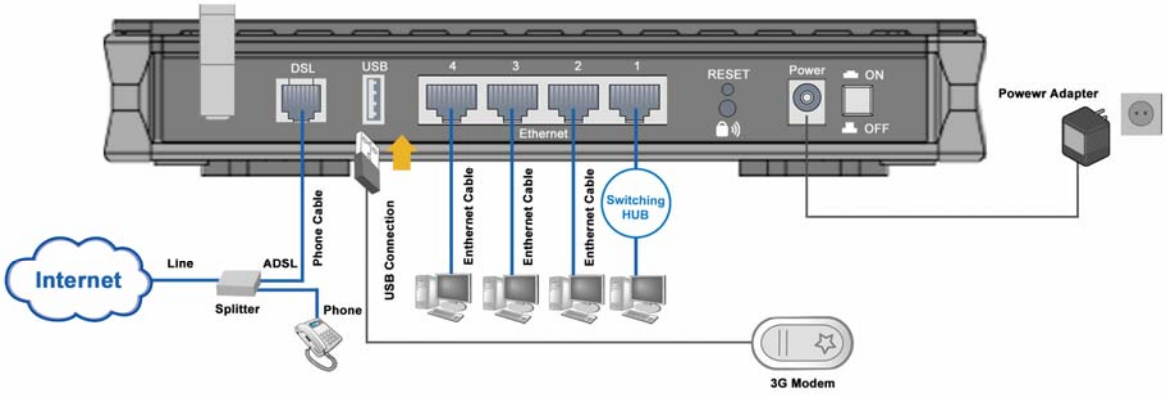
2.接通设备电源。

3.确保 **Power** 灯一直亮着，同时 **LAN** 灯也亮。

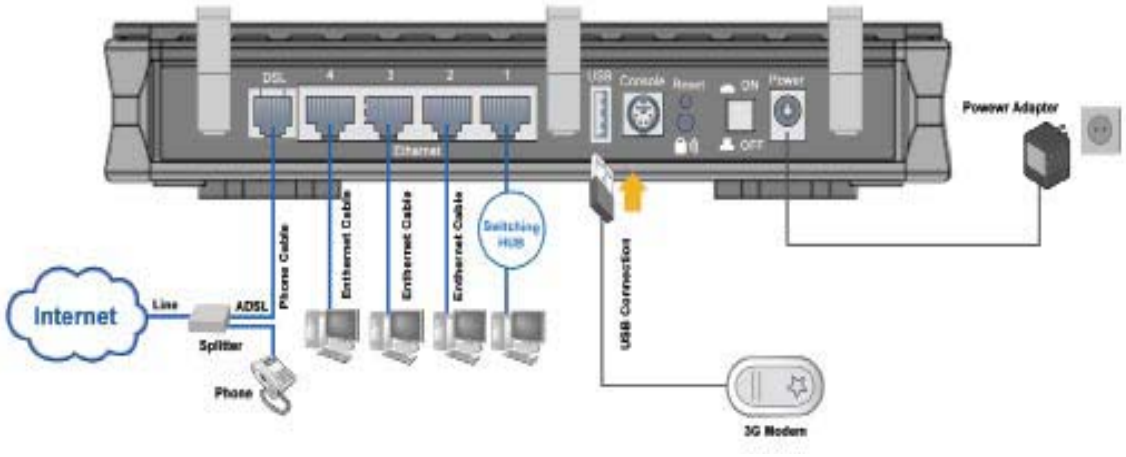
4.通过 RJ-11 线缆将路由器连接到电话壁式插座。

5.连接 USB 2.0 线缆。

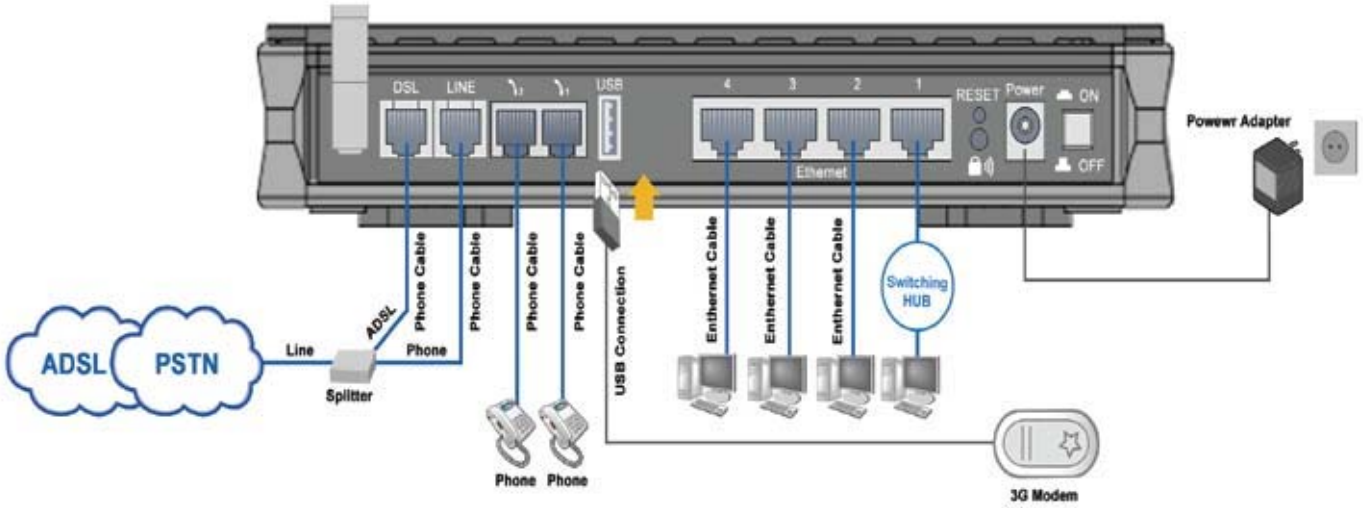
BiPAC 7402X/7402XL/7402GX/7402GXL



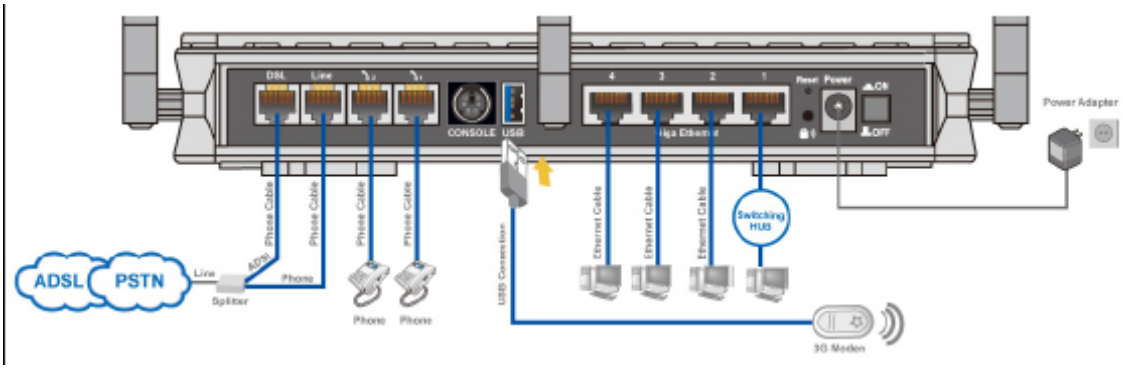
BiPAC 7402NX/7402NXL



BiPAC 7404VGOX/7404VGPX/6404VGOX/6404VGPX



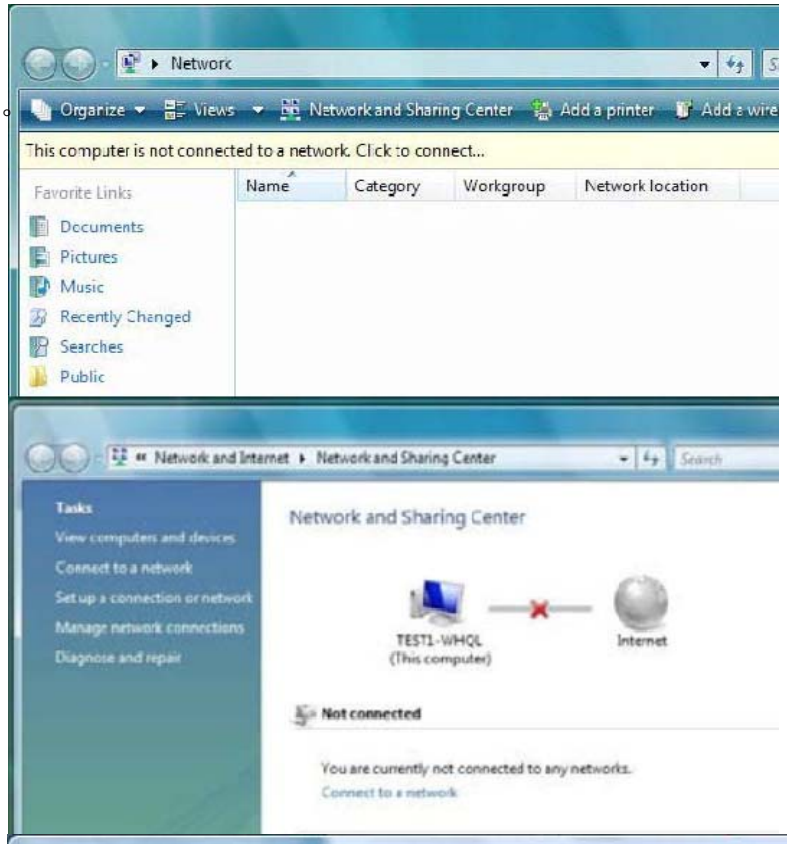
BiPAC 7404VNOX/7404VNPX



网络配置

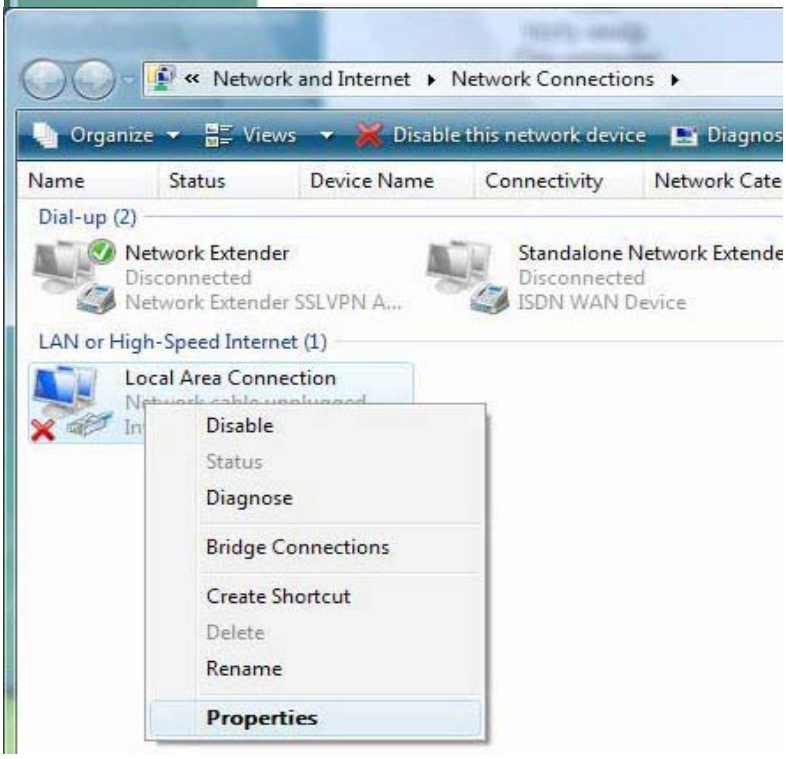
在 Windows Vista 中配置 PC

1. 转到**开始**。单击**网络**。
2. 然后单击顶部工具栏中的**网络和共享中心**。

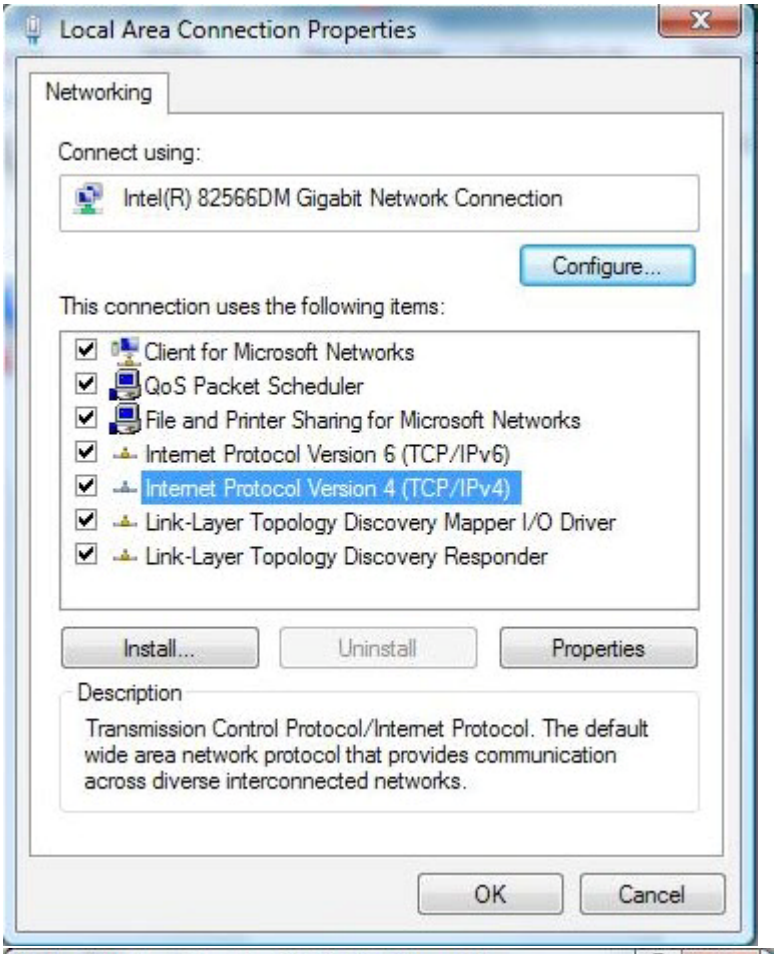


3. **网络和共享中心**窗口弹出后，选择并单击位于左侧的**管理网络连接**。

4. 选择**本地连接**，然后右键单击该图标，选择**属性**。

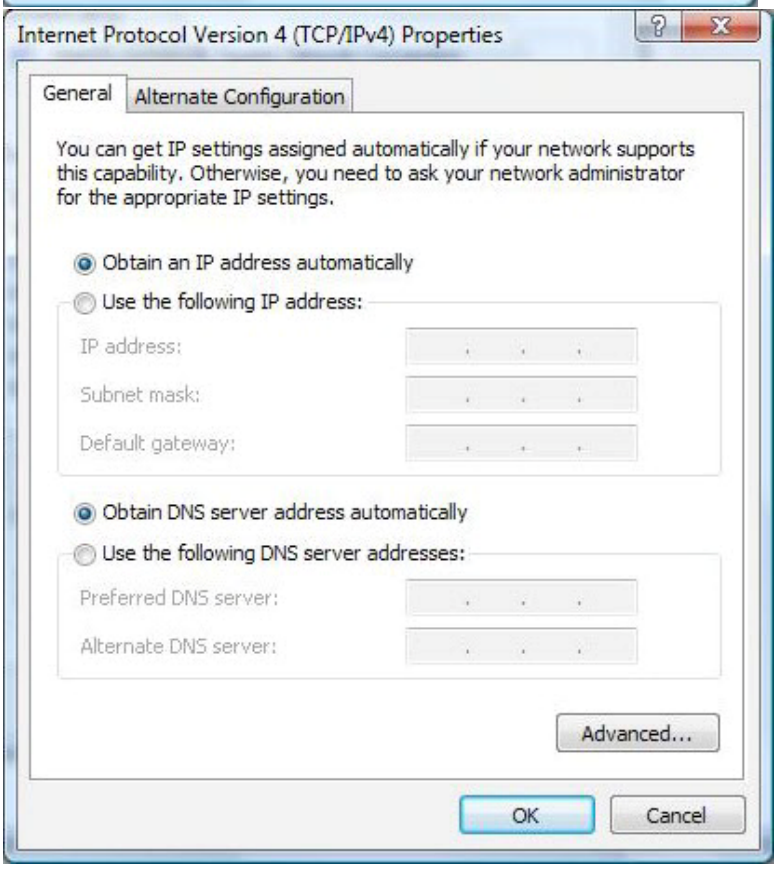


5. 选择 Internet 协议第 4 版 (TCP/IPv4)，然后单击**属性**。



6. 在 TCP/IPv4 属性窗口中，选择**自动获得 IP 地址和 DNS 服务器地址**单选按钮。然后单击**确定**，退出设置。

7. 再次在**本地连接属性**窗口中单击**确定**，应用新的配置。



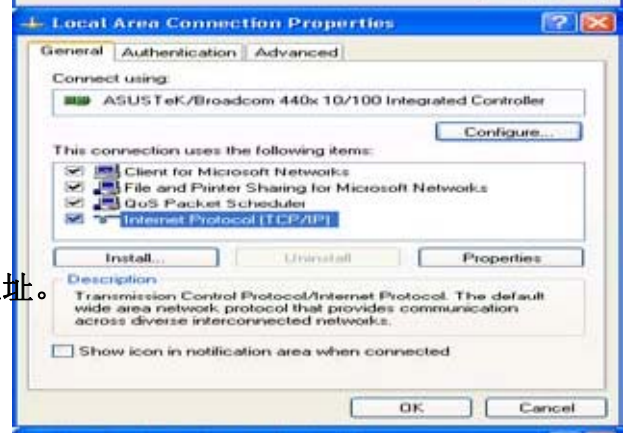
在 Windows XP 中配置 PC

1. 转到**开始/控制面板**（经典视图模式下）。
   在**控制面板**中，双击**网络连接**。

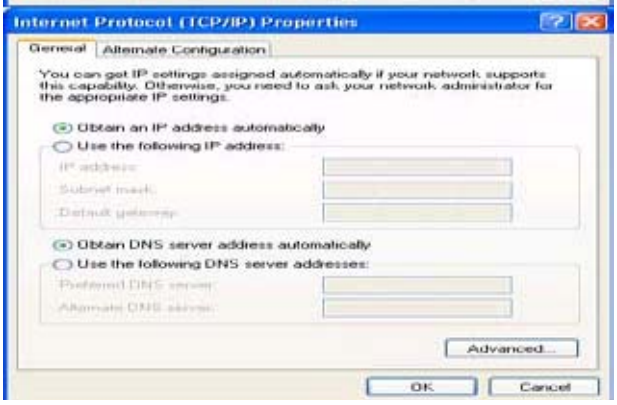
2. 双击**本地连接**。

3. 在**本地连接状态**窗口中，单击**属性**。

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

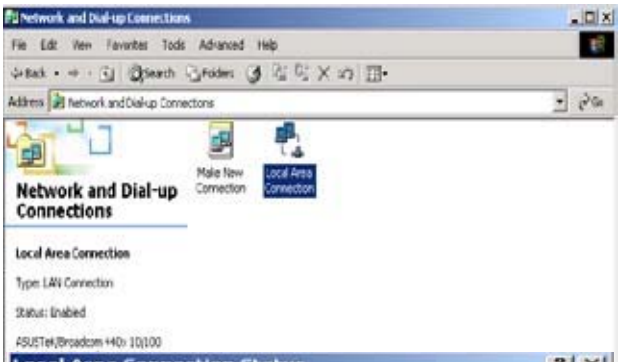


5. 选择自动获得 **IP 地址和自动获得 DNS 服务器地址。**
6. 单击**确定**完成配置。



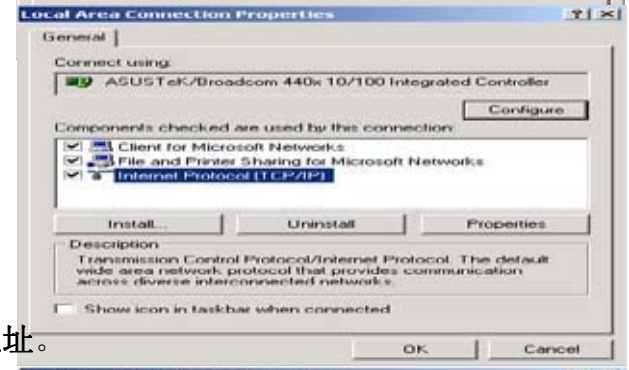
在 Windows 2000 中配置 PC

1. 转到**开始/设置/控制面板**。在控制面板中，双击**网络和拨号连接**。
2. 双击**本地 (LAN) 连接**。

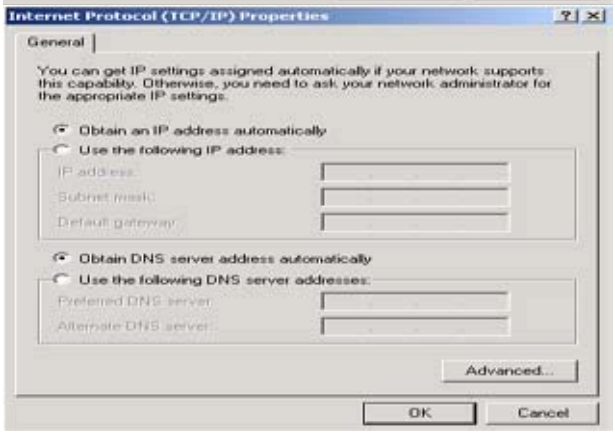


3. 在**本地连接状态**窗口中，单击**属性**。

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

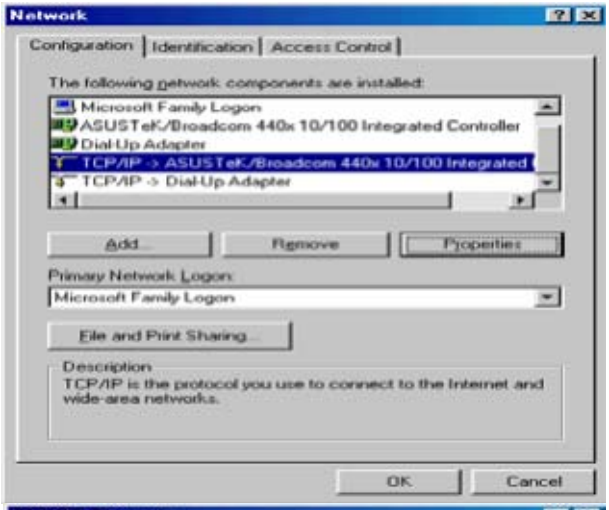
1. 转到**开始/设置/控制面板**。在控制面板中，双击**网络，**然后选择**配置**选项卡。

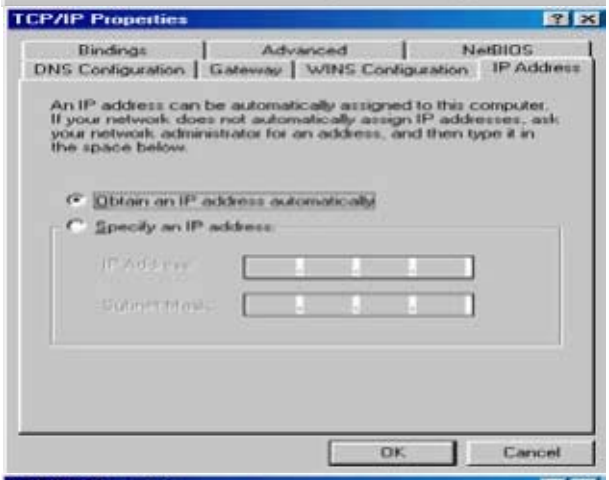
2. 选择 **TCP / IP -> NE2000 兼容**，或任何 PC 的网卡名称。

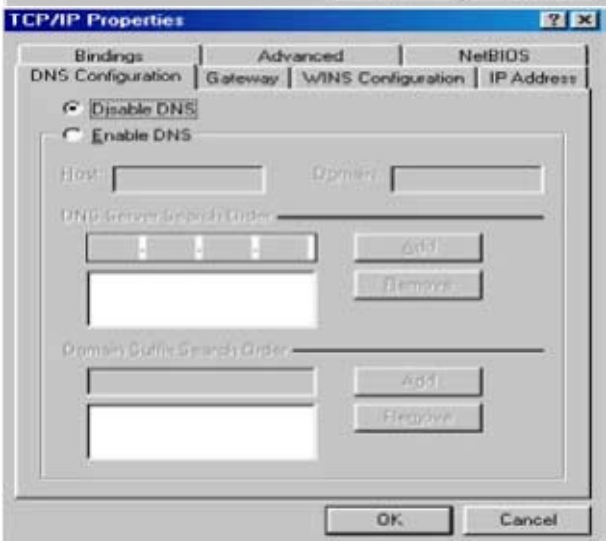
3. 选择**自动获得 IP 地址**单选按钮。

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

在配置之前，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

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。

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

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	
DCP 服务器功能	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(RFC2516)	VPI/VCI，基于 VC/LLC 的多路复用，用户名，密码，服务名和域名解析系统（DNS） 服务器的IP地址（在您连接 ISP 的时候会自动分配或手工设定）。
PPPoA(RFC2684)	VPI/VCI，基于 VC/LLC 的多路复用，用户名，密码和域名解析系统 (DNS) 服务器的IP地址（在您连接 ISP 的时候会自动分配或手工设定）。
MPoA(RFC1483/ RFC2684)	VPI/VCI，基于 VC/LLC 的多路复用，IP 地址，子网掩码，网关地址和域名解析系统 (DNS) 服务器的 IP 地址（它是个固定 IP）。
IPoA(RFC1577)	VPI/VCI，基于 VC/LLC 的多路复用，IP 地址，子网掩码，网关地址和域名解析系统 (DNS) 服务器的 IP 地址（它是个固定 IP）。
纯桥接	VPI/VCI，基于 VC/LLC 的多路复用使用桥接模式。

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**。（**参阅图 3.14**）

图 3.14：用户名和密码弹出窗口

恭喜！您已成功登录了 3G/VoIP/(802.11g/n) (VPN) 宽带防火墙路由器！

第 4 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。

状态

ADSL 表

3G 状态

ARP 表

DHCP 表

路由表

NAT 会话

UpnP 端口映射

PPTP 状态

IPSe 状态

L2TP 状态

Email 状态

VoIP 状态

VoIP 呼叫记录

事件日志

错误日志

分析

快速启动

配置

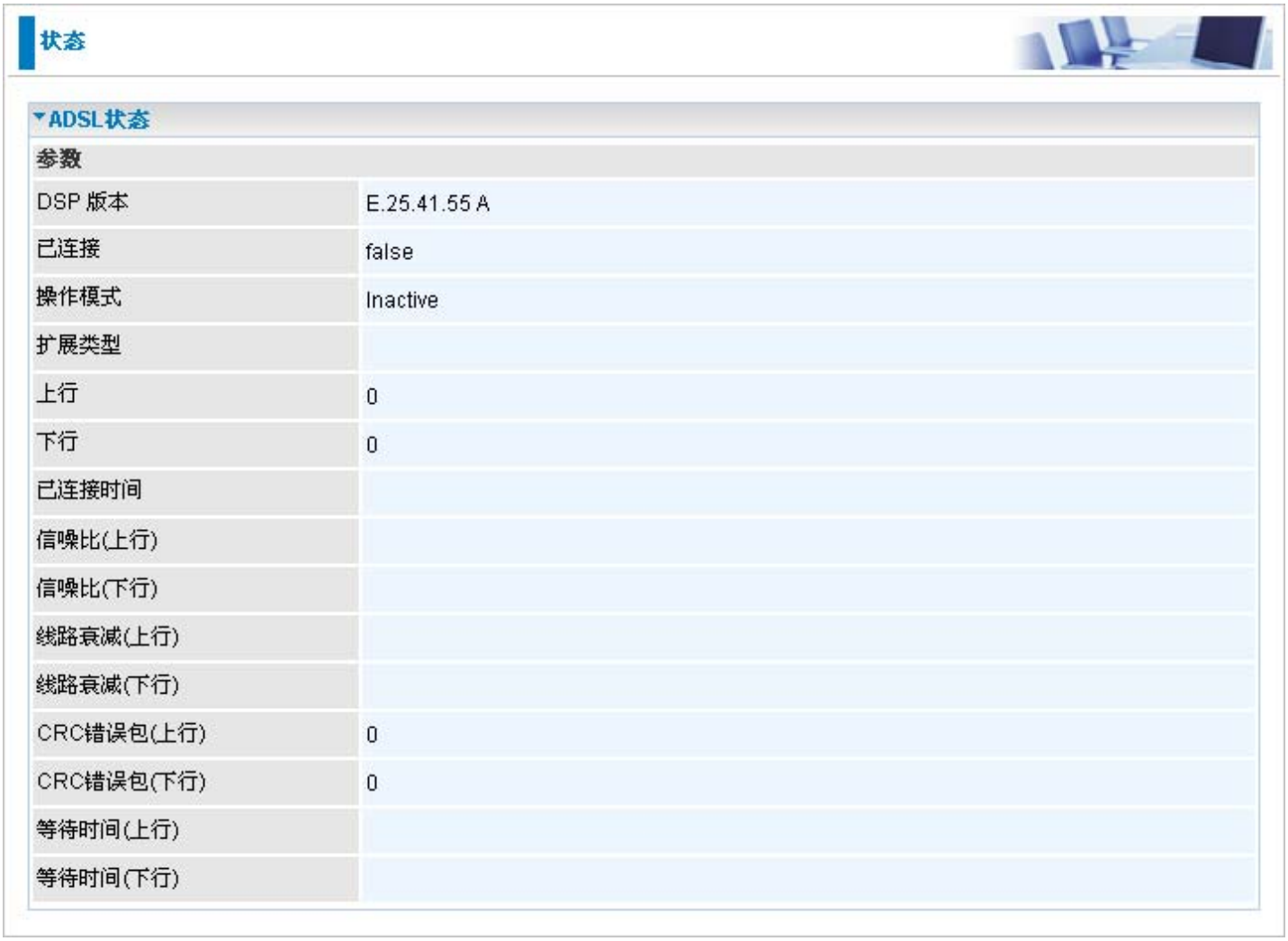
LAN
WAN
系统
防 火 墙
VPN
VoIP
QoS
虚拟服务器
时间表
高级

语言（提供英文和法文的用户界面）

状态

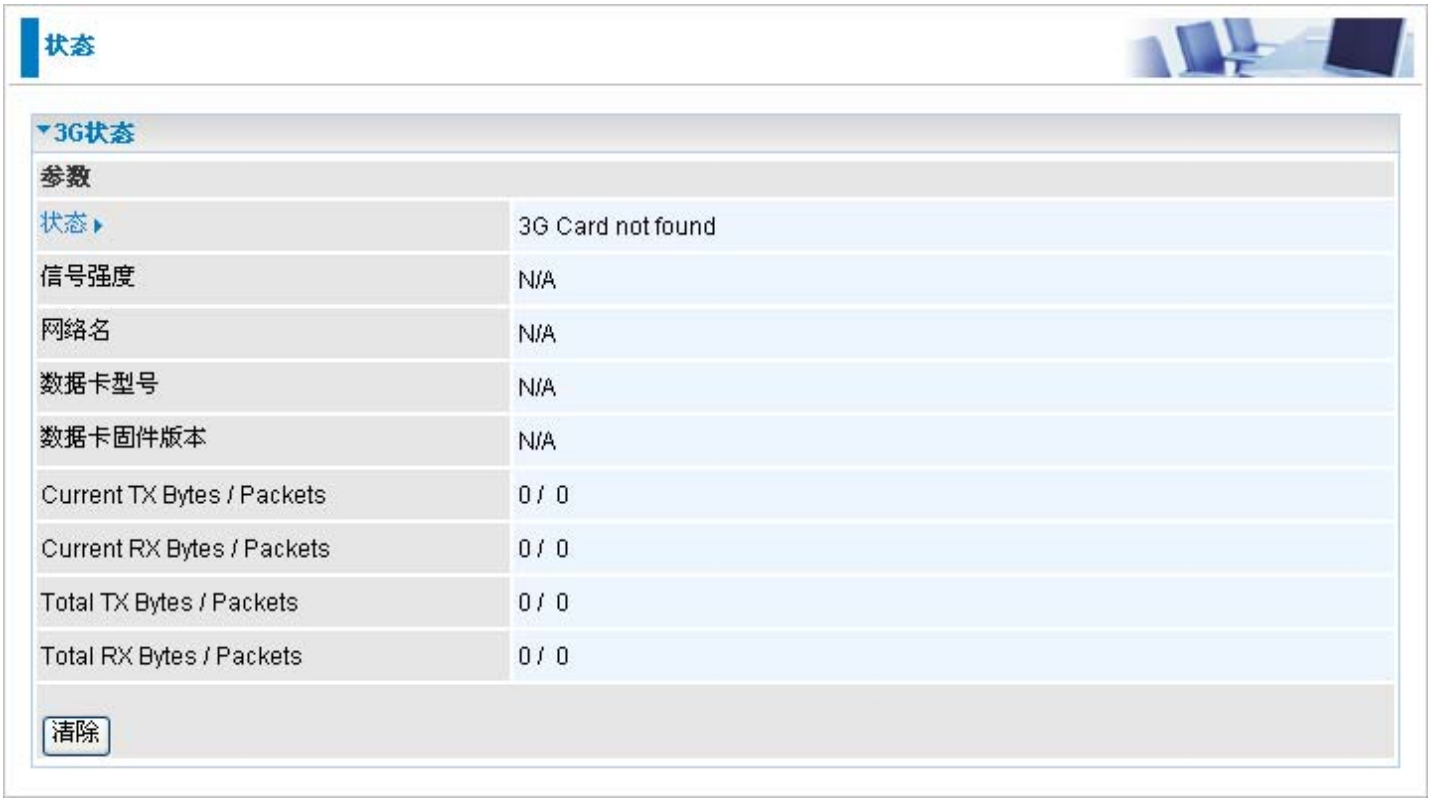
ADSL 状态

这里将所有的 ADSL 状态信息，如 DSP 固件版本、操作模式、上行速率/下行速率、噪声容限、线路衰减、CRC 错误包以及等待时间。



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。

Current TX Bytes / Packets：通话时传输数据的字节/数据包统计。

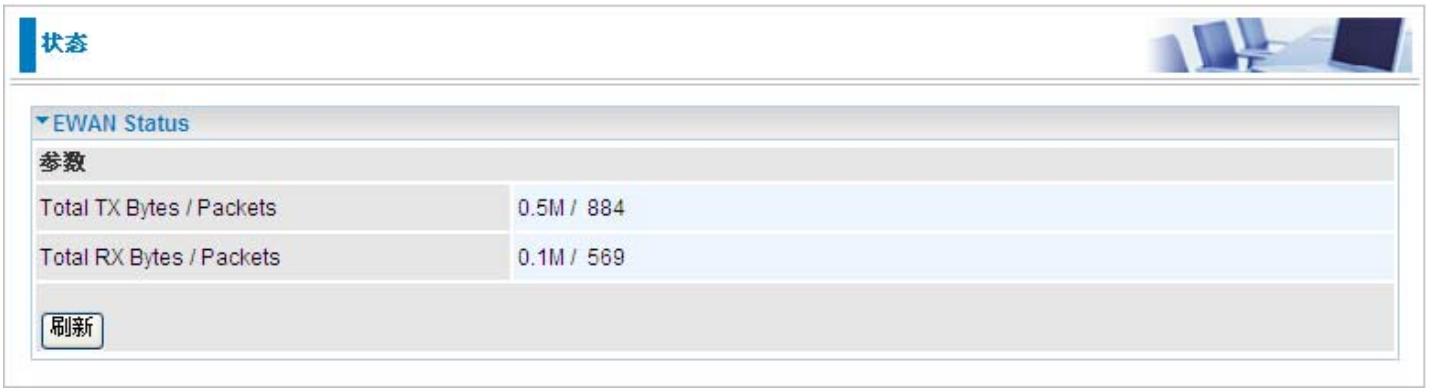
Current RX Bytes / Packets：通话时接收到数据的字节/数据包统计。

Total TX Bytes / Packets：系统就绪后，传输数据的总字节/总数据包统计。

Total RX Bytes / Packets：系统就绪后，接收到数据的总字节/总数据包统计。

EWAN Status

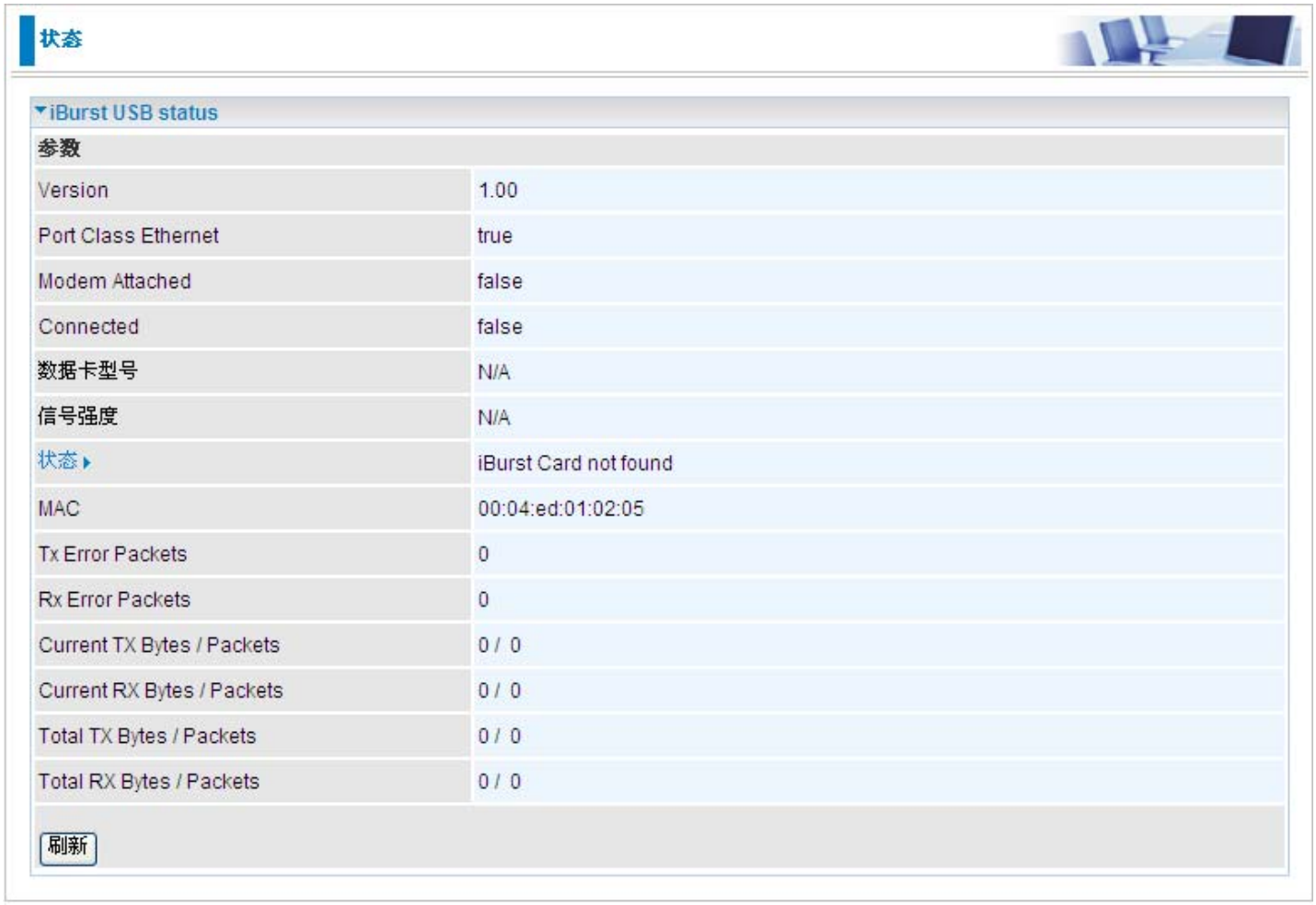
除了能通过 3G/ADSL 连接到互联网上，该路由器还提供了一个WAN 口Ethernet port 1，通过它可以连接到电缆调制解调器上，使用户上网享受快速且机动性的连接。



Total TX Bytes / Packets: 系统就绪后，传输数据的总字节/总数据包统计。
Total RX Bytes / Packets: 系统就绪后，接收到数据的总字节/总数据包统计

IBurst Status

当配置3G状态时启用iBurst 功能时，显示3G状态更多的信息。例如card name, connection status and port class Ethernet.



数据卡型号：卡的型号。

信号强度：表示当前 3G 信号强度的信号强度条。

Current TX Bytes / Packets：通话时传输数据的字节/数据包统计。

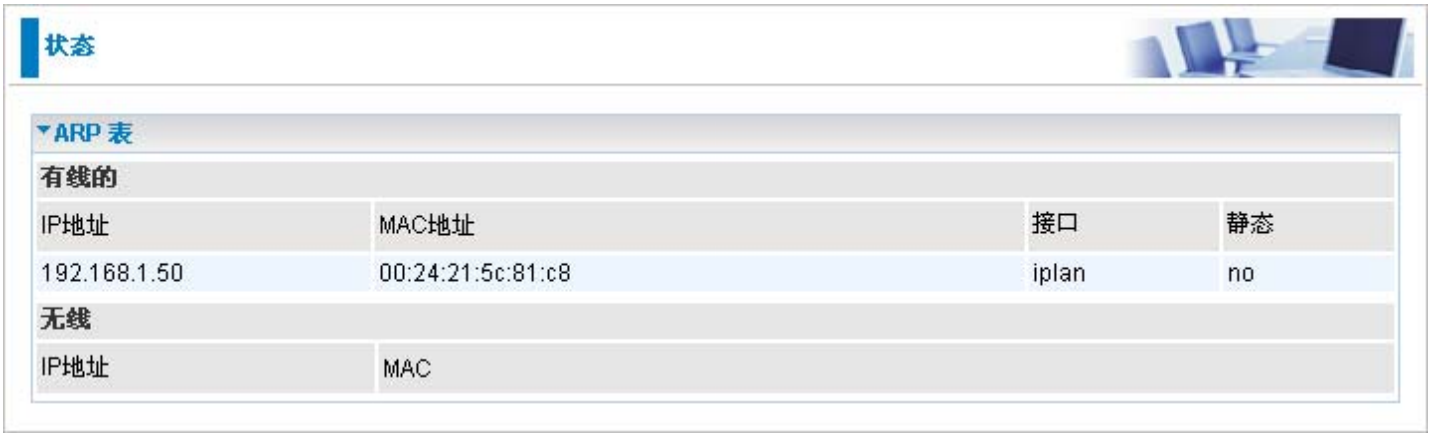
Current RX Bytes / Packets：通话时接收到数据的字节/数据包统计。

Total TX Bytes / Packets：系统就绪后，传输数据的总字节/总数据包统计。

Total 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

租用：DHCP 指定的 IP 地址信息。

到期：到期 IP 地址的信息。

固定：固定主机映射信息。

租用表

IP 地址：分配给客户端的 IP 地址。

MAC 地址：客户端的 MAC 地址。

客户端主机名：客户端的主机名称（计算机名）。

到期：当前客户端的租用时间。

路由表

路由表

有效的：复选标记表示成功的路由状态。

目标地址：显示目标网络的 IP 地址。

子网掩码：显示目标网络的子网掩码。

网关/接口：路由器使用的接口或网关的 IP 地址。

成本：跳数就是路由的成本。

RIP 路由表

目标地址：目标网络的 IP 地址。

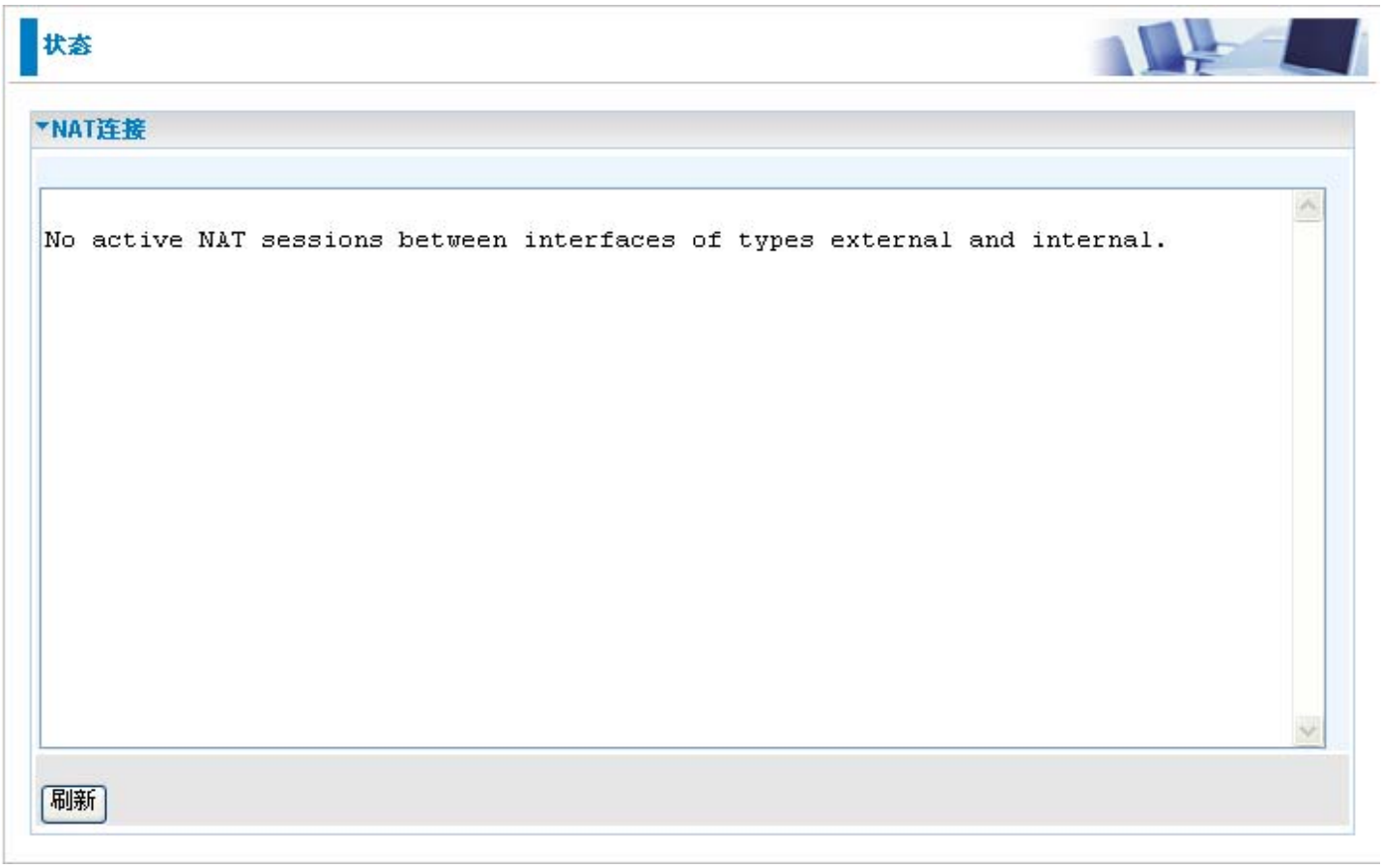
子网掩码：目标网络的子网掩码。

网关：路由器使用的网关的 IP 地址。

成本：跳数就是路由的成本。

NAT 会话

这里列出了外部端口 (WAN) 与内部端口 (LAN) 之间的当前所有 NAT 会话。



UPnP 端口映射

这里列出所有使用 UPnP（通用即插即用）建立的端口映射。有关 UPnP 以及路由器 UPnP 配置选项的更多信息，请参阅手册中的**高级**部分。

PPTP 状态

下图显示配置 PPTP VPN 连接的详细信息。

名称：配置 VPN 时，分配给特定 PPTP 连接的名称。

类型：连接类型（拨入/拨出）。

启用：此时是否已启用连接。

激活：此时是否已激活连接。

隧道连接：VPN 隧道是否已连接。

会话连接：VPN 入口的会话是否已连接。

加密：VPN 连接所使用的加密类型。

注：只有 7402X、7402GX、7404VGOX、7404VNOX、6404VGOX 具有 PPTP 状态。

IPSec 状态

下图显示配置 IPSec VPN 连接的详细信息。

名称：分配给 VPN 入口的名称。

激活：VPN 连接此时是否已激活。

连接状态：VPN 是否连接或断开。

统计信息：VPN 连接的统计信息。

本地子网：正在使用的本地 IP 地址或子网。

远程子网：远程站点的子网。

远程网关：远程网关的 IP 地址。

SA：VPN 入口的安全关联。

L2TP 状态

下图显示配置 L2TP VPN 连接的详细信息。

名称：配置 VPN 时，指定给特定 L2TP 连接的名称。

类型：连接类型（拨入/拨出）。

启用：此时连接是否已启用。

激活：此时连接是否已激活。

通道连接：此时 VPN 通道是否已连接。

呼叫连接：VPN 入口的会话是否已连接。

加密：VPN 连接所使用的加密类型。

注：只有 7402X、7402GX、7404VGOX、7404VNOX、6404VGOX 具有 L2TP 和 IPSec 状态。

VoIP 状态

下表显示激活 VoIP 功能后电话端口的状态。显示域名以及 VoIP 设备的名称与电话号码信息。

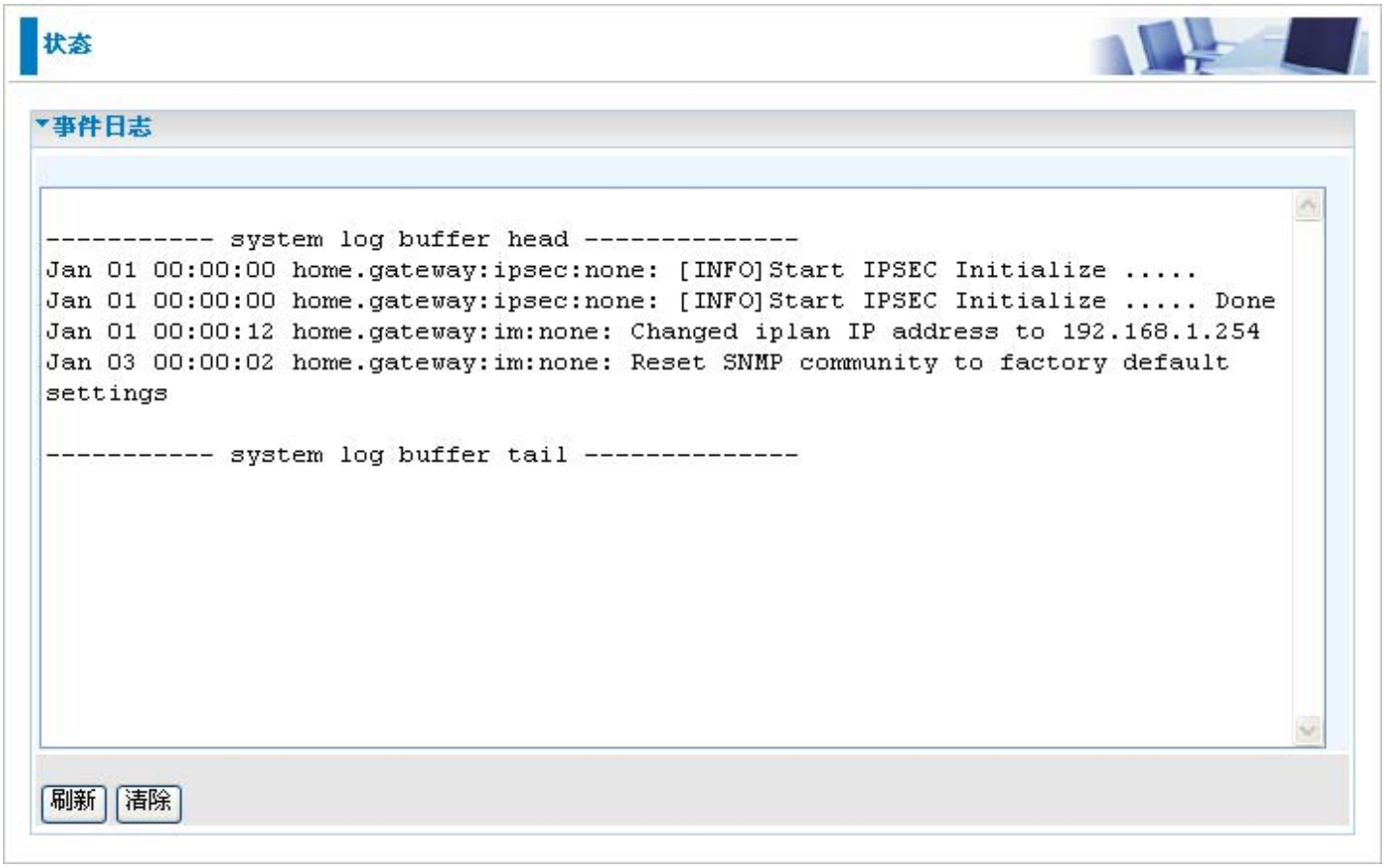
VoIP 呼叫记录

呼叫记录记录的是 VoIP 设备的数据信息，如拨出电话的日期/时间、通话持续时间、未接来电以及打进电话的信息。

注：只有 7404VGPX、7404VGOX、7404VNOX、7404VNPX、6404VGO(P)X 具有 VoIP 功能。

事件日志

该页显示路由器的所有事件日志条目，如路由器与 ADSL 连接断开，以及防火墙触发**入侵**或**阻止日志**事件。关于如何启用防火墙日志的详细信息，请参阅该手册中的**防火墙**部分。

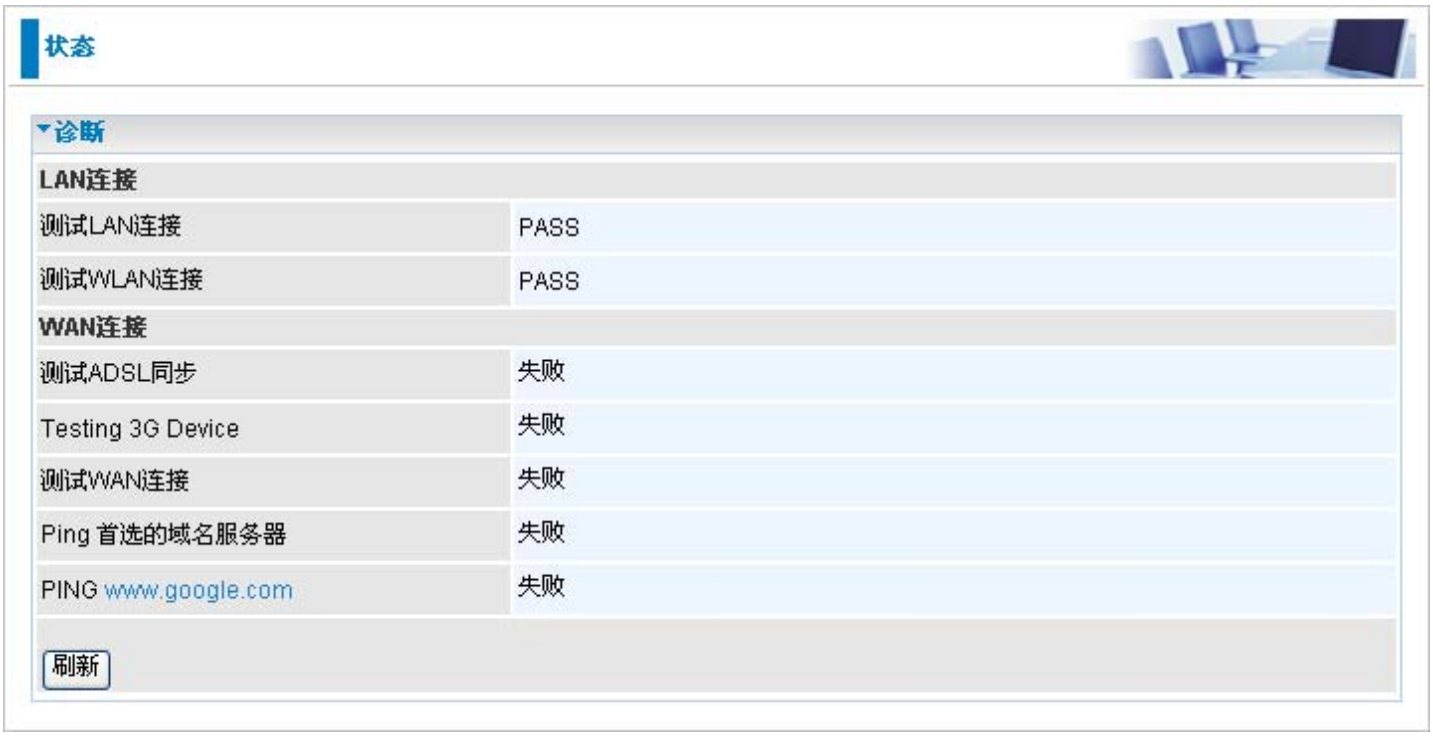


错误日志

所有路由器错误（如，条目名称无效）都记录在下面的窗口中。

诊断

检测计算机与 LAN 端口的连接以及与 WAN Internet 端口的连接。如果显示**无法** PING 通 **www.google.com**，而其他的都显示**可以**，则必须检查 PC 的 DNS 设置是否正确。

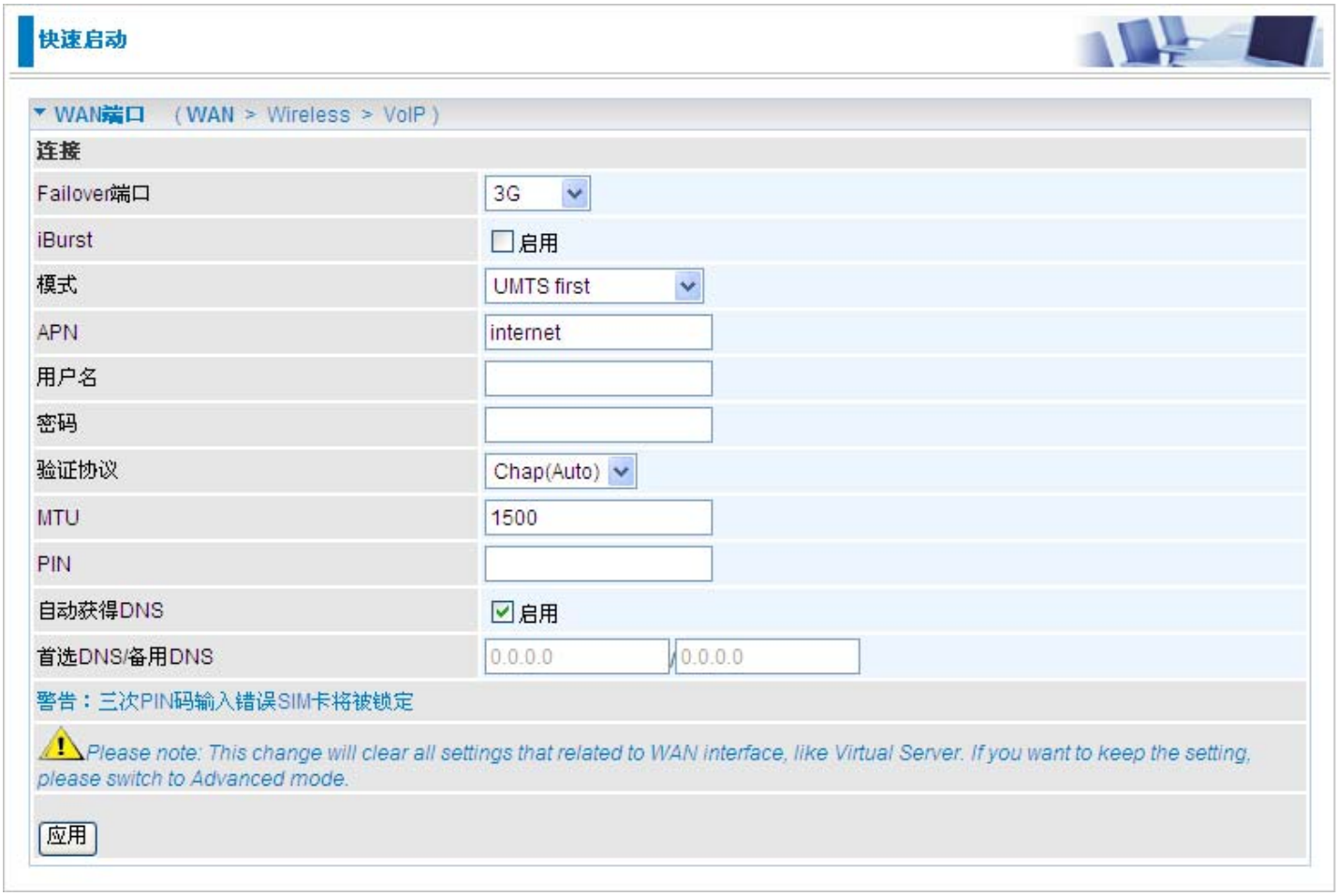


快速启动

1. 单击快速启动。选择连接方式。有两个选项可选择：ADSL，EWAN 或 3G。 **（对于 6404VGO(P)X，连接方式是 EWAN 和 3G，而不是 ADSL）**

3G

1) 从下拉菜单中选择 3G 模式，然后单击**继续**。



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。

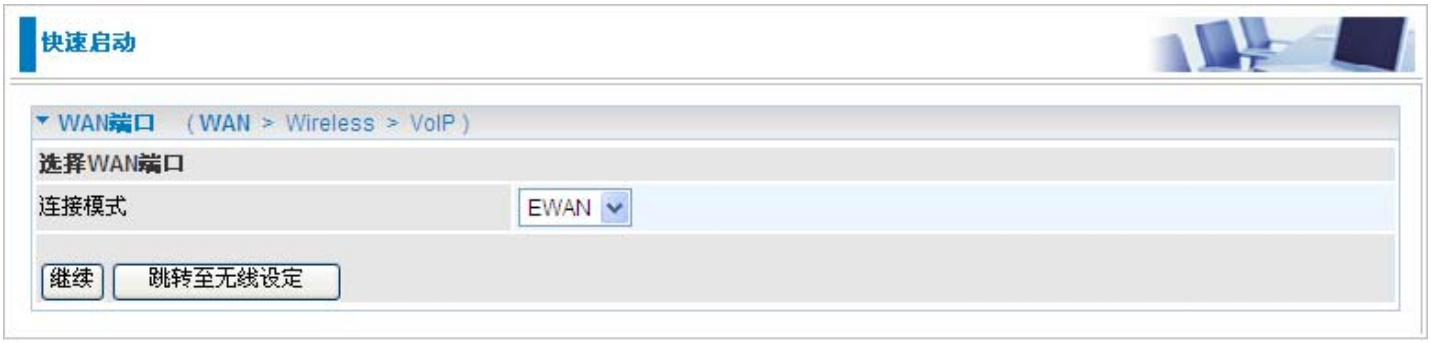
验证协议：如果您知道服务器使用的认证类型，或者您希望客户端连接时使用您指定的认证类型（作为服务端时），可以手动指定 CHAP（挑战握手协议）或 PAP（密码认证协议）。使用 PAP 时，密码是未加密发送的；而 CHAP 会在发送前对密码进行加密，因为要确保客户端在不同时段都不会被入侵者取代。

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。

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。

EWAN

1) 从下拉菜单中选择 EWAN 模式



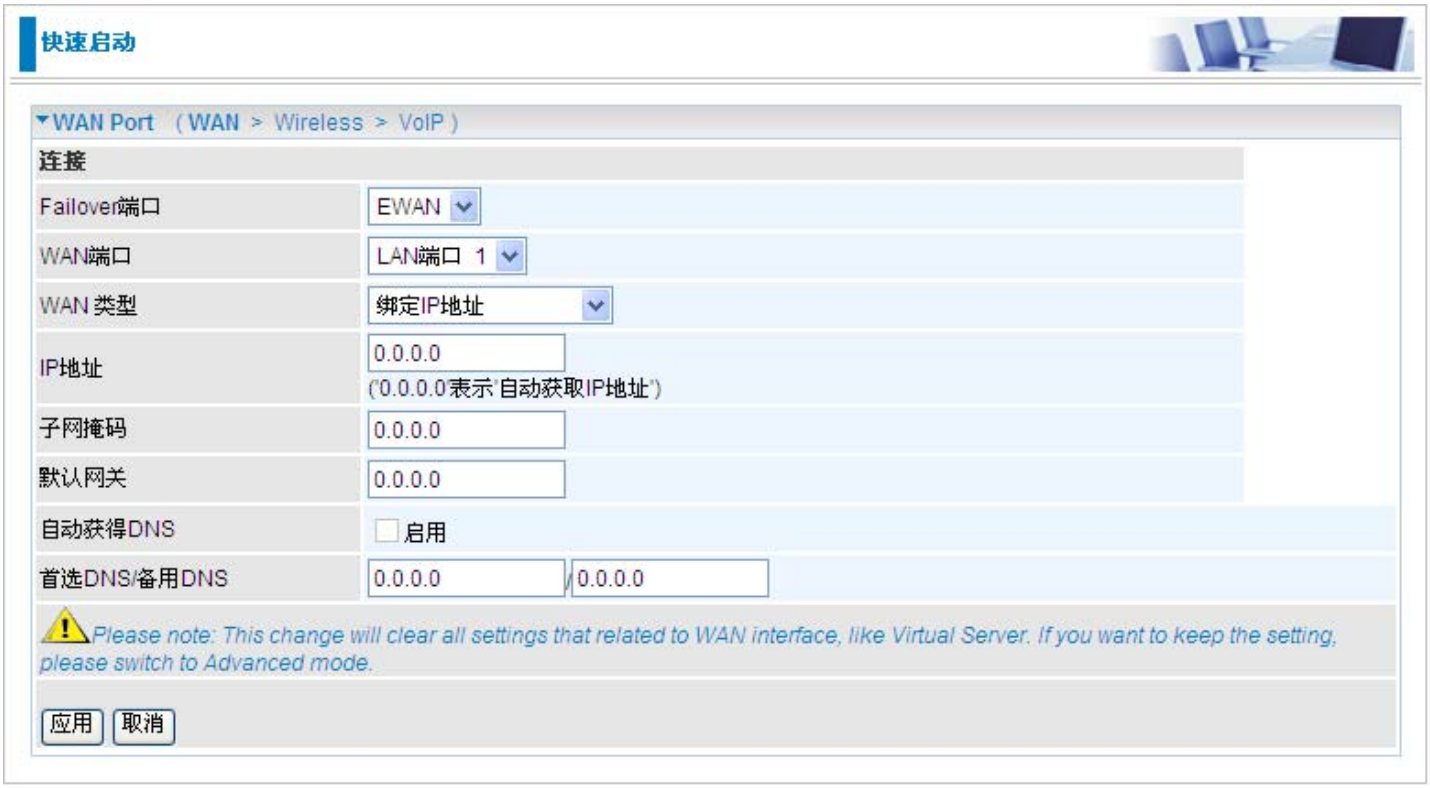
2) 单击**继续**

自动获取IP地址

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

绑定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。



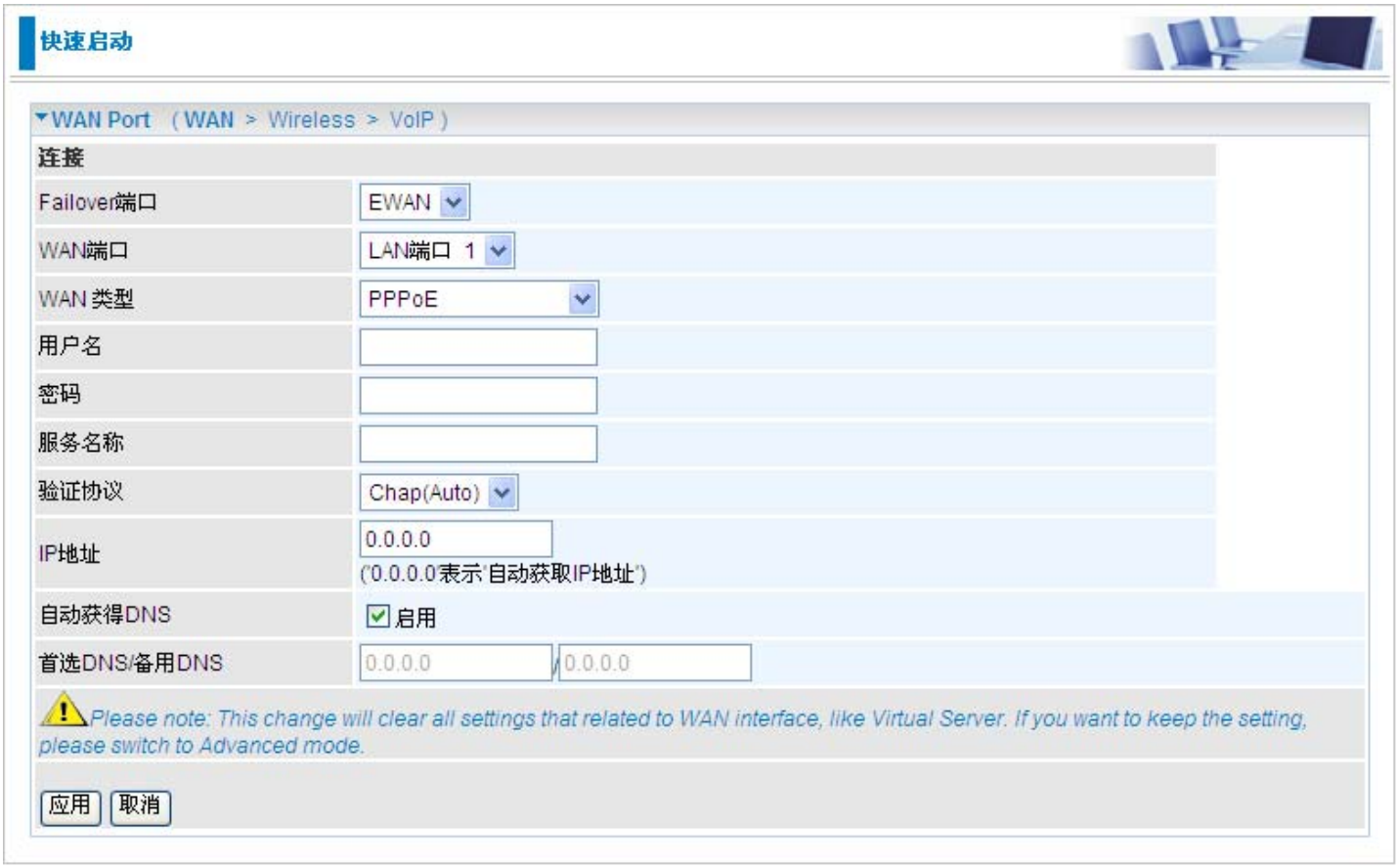
IP地址： WAN 口的 IP 地址。保持 0.0.0.0 将自动从 ISP 获取 IP 地址。

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)。

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。



用 户 名 ： 输入ISP 提供的用户名。您可以输入最多**128** 个字符（ 区分大小写）。格式是“username@ispname”，而不是“username”。

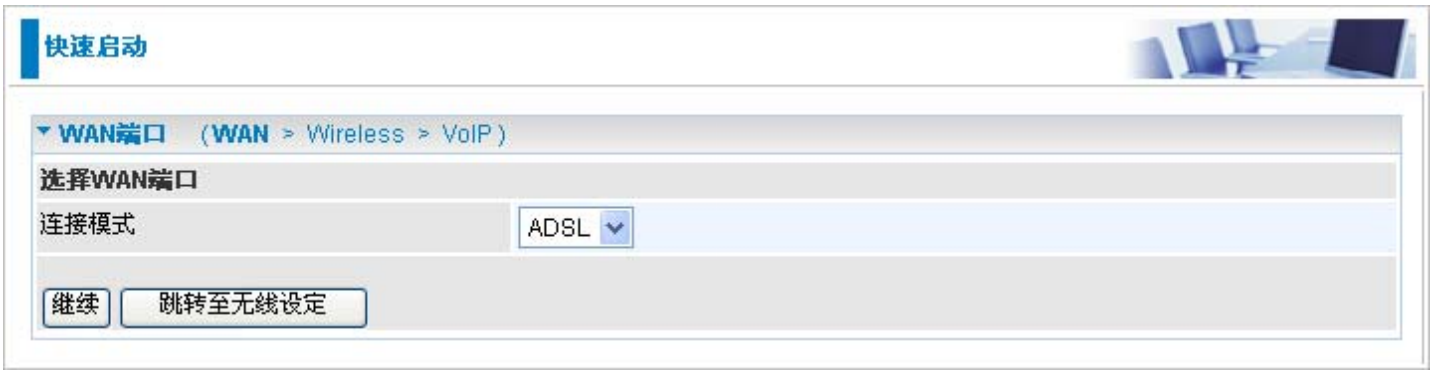
密码：输入ISP提供的密码。您可以输入最多**128**个字符（区分大小写）。

服务名称:连接时输入一个名字。

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。

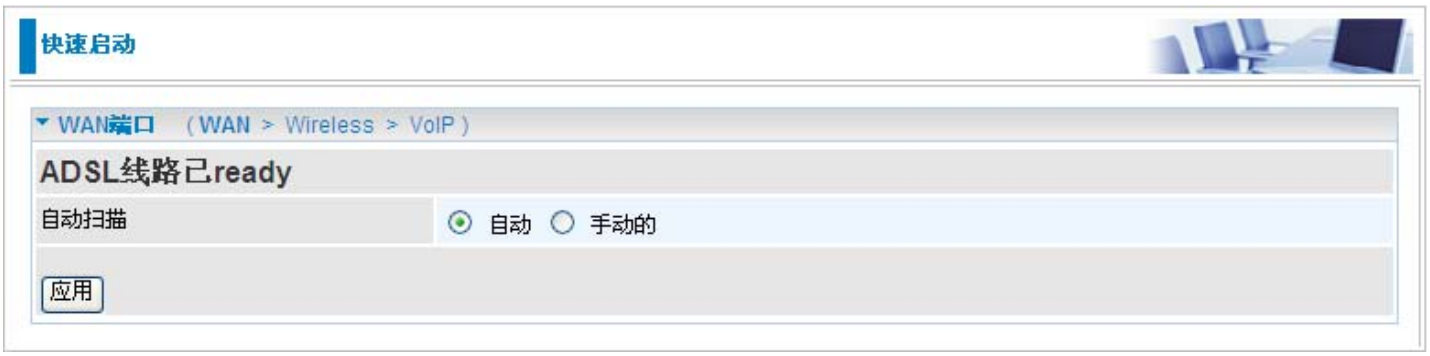
ADSL

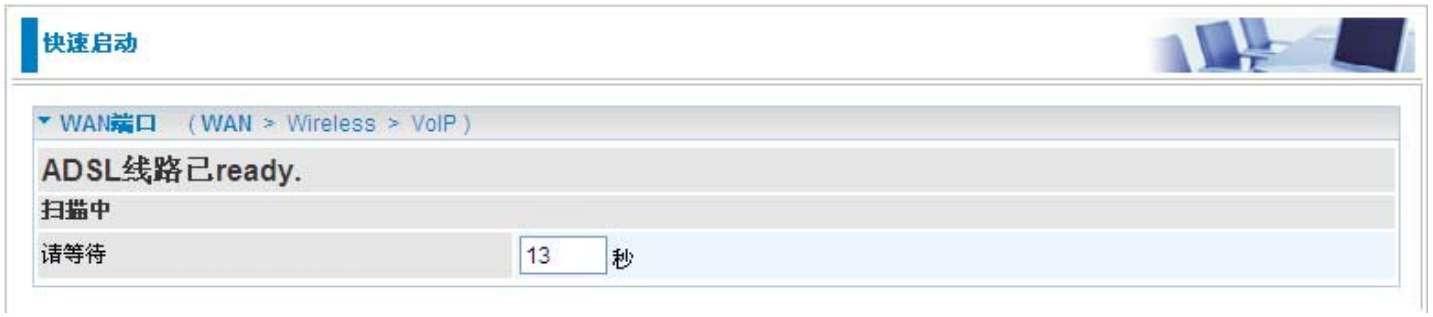
1) 从下拉菜单中选择ADSL 模式



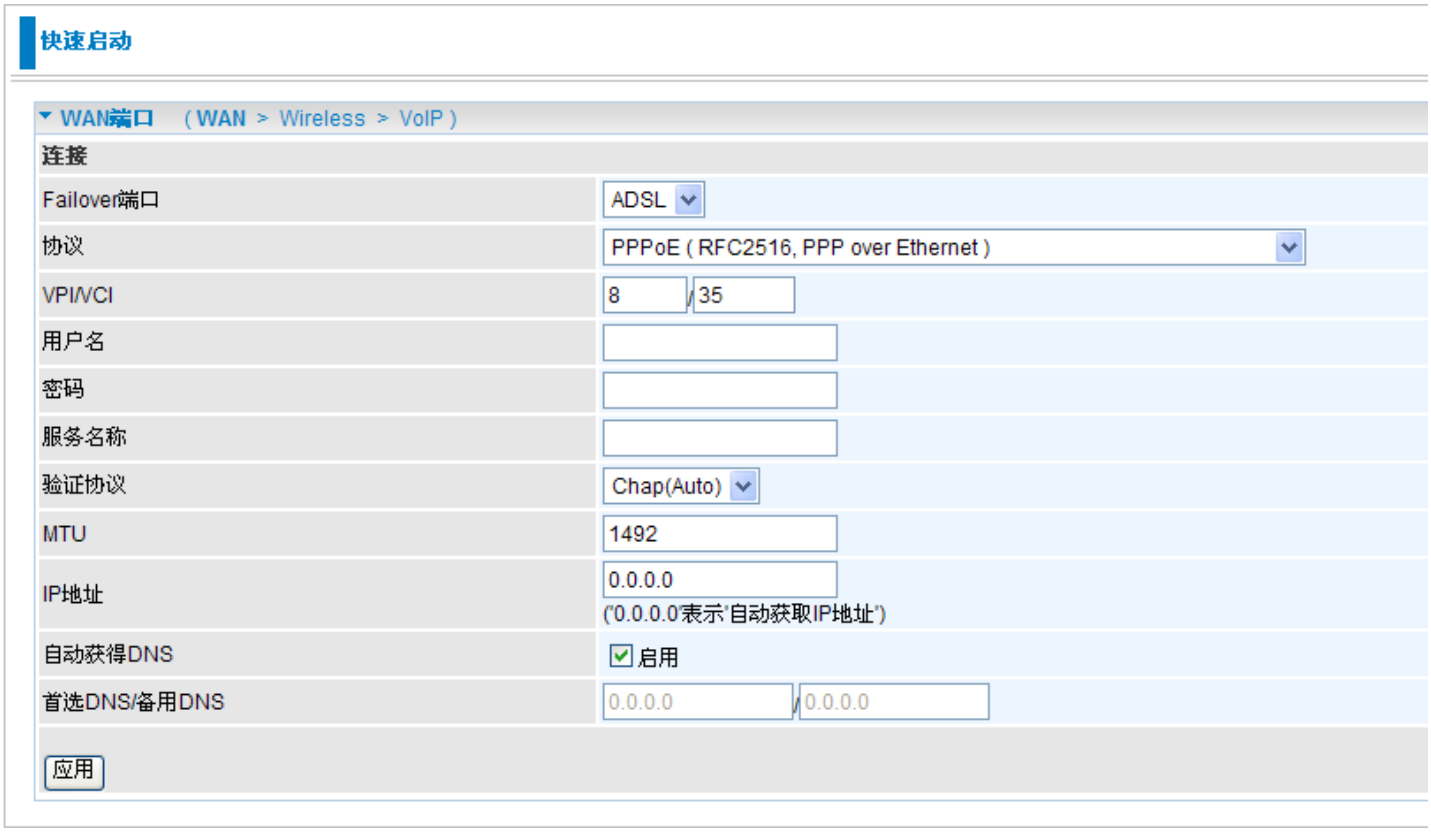
2) 如果 ADSL 线路未准备就绪，您需要检查 ADSL 线路是否已经设置好。

3) 如果 ADSL 线路已准备就绪，屏幕上会显示 ADSL 线路已准备就绪。选择**自动**单选按钮，然后单击**应用**，便自动扫描推荐的模式。手动模式需要您手动设置 ADSL 线路。（如果选择**手动**，您可以直接转到第 5 步。）





4) 输入 ISP（Internet 服务提供商）提供的“用户名”和“密码”，然后单击**应用**以继续。



配置端口：选择连接模式。可以选择 ADSL。

协议：选择协议模式。默认模式为 PPPoE。

VPI/VCI：输入 ISP 提供的 VPI 和 VCI 信息。

用户名：输入 ISP 提供的用户名。

密码：输入 ISP 提供的密码。

服务名称：这个字段起标识作用。需要的话，由 ISP 提供。

认证协议：默认为**自动**。ISP 会建议您使用 **Chap** 还是 **Pap**。

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。
自动获得 DNS：单击以激活 DNS，使系统自动检测 DNS。

首选 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。

2. 配置无线 LAN 设置。**（7402X 和 7402XL 不具有此功能）**

WLAN 服务：默认设置为**启用**。如果网络中要使用无线 802.11g 和 802.11b 设备，可以选择**启用**。

ESSID：ESSID 是区分不同无线接入点 (AP) 的名称。为了安全起见，将路由器无线接口的内置 AP 改成唯一的 ID 名称。它是区分大小写的，不得超过 32 个字符。保证无线客户端拥有和设备一样的 ESSID，这样才能连接到网络中。

ESSID 广播：其功能是将 ESSID 发射到空中，当无线客户端搜索网络时，能够发现并识别路由器。默认设置为**启用**。

启用：选择**启用**后，允许任何无线客户端都能找到路由器的接入点 (AP)。

禁用：如果不想广播您的 ESSID，那么任何无线客户端不管进行怎样的无线设置，都无法发现路由器的接入点 (AP)。

区域：有七个区域供选择，包括：北美、欧洲、法国等等。区域不同，设置的通道 ID 也不同。

通道 ID：选择您想使用的 ID 通道。

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

3. 设置 VoIP。**（7402 系列不具有此功能）**

SIP：使用 VoIP SIP 作为 VoIP 呼叫的信号协议。默认设置为***禁用***。

区域：用户可以从下拉列表中选择使用 VoIP 设备的国家。选择一个国家后，有关国家的参数将自动加载。

SIP 服务提供商：允许您选择服务提供商。选择后，以下相关参数将自动显示。

电话号码：此参数包含 VoIP SIP 注册服务器中用户的注册 ID。

用户名：如果用户名和电话号码一样，则不填。若不一样，在空白处填写 VoIP 提供商提供的用户名。

密码：此参数包含 VoIP SIP 注册服务器中用于认证的密码。

显示名称：名称将显示在来电显示上。

4. 等待配置

5. ADSL 线路同步时，会显示“勾号”。

配置

单击此项时，将展开显示其中的子项，使您可以进一步配置路由器。

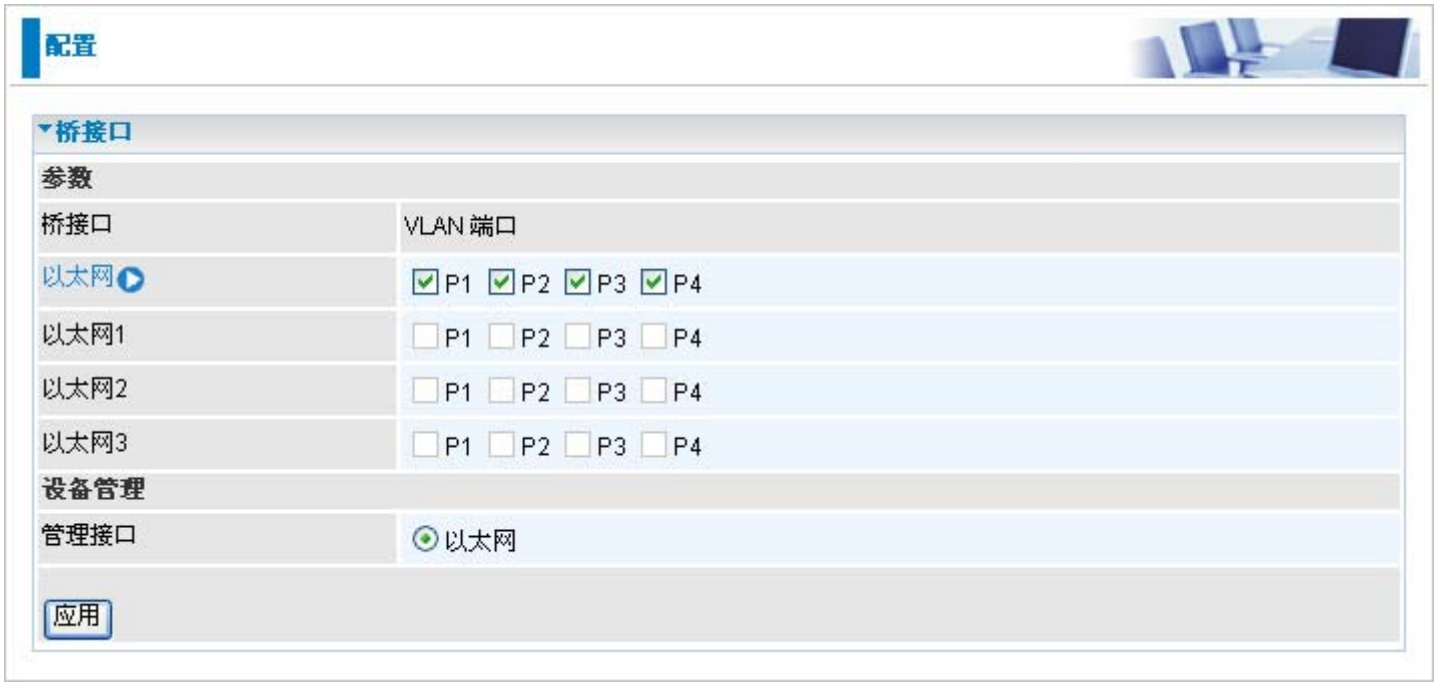
LAN、WAN、系统、防火墙、VPN、VoIP、QoS、虚拟服务器、Wake on LAN、计划时间和**高级设置**

下面将介绍各个配置子项的功能。

LAN – 局域网

LAN 包括以下几部分：**桥接口、以太网、IP 别名、以太网客户端过滤、无线、无线安全、无线客户端过滤、端口设置**以及 **DHCP 服务器。**

桥接口



您可以在桥接口部分设置各个 VLAN 组的成员端口。

以太网：P1 & P2 (Port 1, 2)

以太网 1：P3、P4 和无线（端口 3、4 和无线）。首先取消选中以太网 VLAN 端口中的 P3、P4、无线。

注：设置 VLAN 组时须注意：所有桥接口都是按这个顺序排列的。

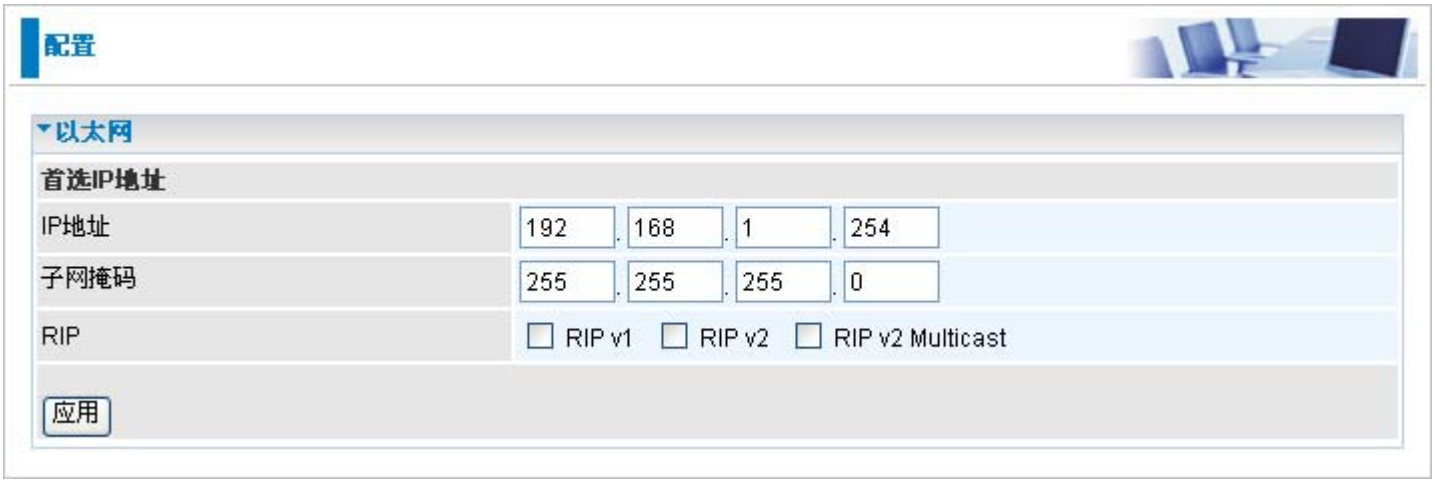
桥接口	端口（总是以...开）
以太网	P1 / P2 / P3 / P4
以太网 1	P2 / P3 / P4
以太网 2	P3 / P4
以太网 3	P4

管理接口：指定哪个 VLAN 组可能执行设备管理（如同执行 web 管理一样）。

注：NAT/NAPT 仅适用于管理接口。

以太网

LAN 中的路由器支持多个以太网 IP 地址，从而支持同一时间有多个 Internet 访问。通常 LAN 中的用户只有一个子网。路由器的默认 IP 地址为 192.168.1.254。



首选 IP 地址

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 以及 RIP v2 多播。选中以启用 RIP 功能。

IP 别名

此功能支持创建多个路由器虚拟 IP 接口。用来将两个或多个局域网连接到 ISP 或远程节点。这样就不需要内部路由器了。

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。

安全接口：指定虚拟接口的防火墙设置。

内部：将 NAT 应用于网络。如果已启用 NAT，则向 Internet 发送数据流量时，将进行网络地址转换。

外部：外部 IP 接口没有直接连接到 Internet 的 NAT。通常，当 ISP 提供多个公共 IP 地址时，会使用 NAT。这样您就可以在局域网中使用公共 IP 地址，网关 IP 地址指向该接口的 IP 地址。

DMZ：指定网络的 DMZ 区。DMZ 区不具有 NAT 功能。

以太网客户端过滤

以太网客户端过滤支持多达 16 台以太网设备，通过它接收来自指定授权设备的数据流、或限制某些设备访问局域网，从而实现网络控制。

如果没有预定义的以太网 MAC 地址过滤规则；您可以添加过滤规则，以满足您的要求。

以太网客户端过滤：默认设置为**禁用**。

允许：在空白处插入 MAC 地址或单击“候选表”，选中“**允许**”允许指定设备访问您的局域网。确保您 PC 的 MAC 地址在该列表中。

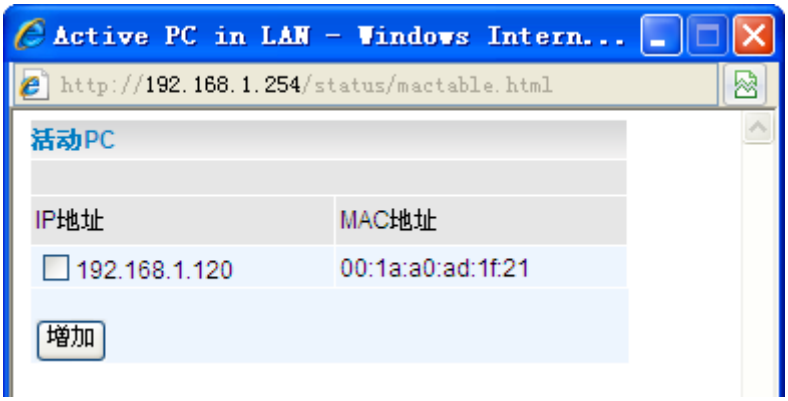
阻止：在空白处插入 MAC 地址或单击“候选表”，选中“**阻止**”阻止未经允许的设备访问您的局域网。确保您 PC 的 MAC 地址不在列表中。

最多可以有 16 个客户端。MAC 地址长度为 6 个字节，而且只能采用 16 进制字符表示。可以使用数字 0-9 以及字母 a – f。

注：MAC 地址采用 xx:xx:xx:xx:xx:xx 格式。必须包含分号(:)。

候选表：自动检测通过以太网连接到路由器的设备。

单击**候选表**按钮，访问 **LAN 中的活动 PC** 窗口。



LAN 中的活动 PC：显示每个连接到路由器的以太网设备的 IP 地址和 MAC 地址列表。

您只要选中要阻塞或允许 IP 地址旁边的选方框。然后单击**添加**插入到以太网客户端过滤表中。以太网客户端最多为 16。

无线

参数

WLAN 服务：默认是**开启**的。如果网络中没有无线设备，那么选择**禁用**。

模式：默认设置为 **802.11b+g+n**（混合模式）。如果不知道网络中是否有 11g 和 11b 设备，保持默认设置为**混合模式**。如果只有 11g 网卡，从下拉列表中选择 **802.11g**。如果只有 11b 网卡，选择 **802.11b**。如果有 11n 卡，选择 802.11n。

ESSID：ESSID 是区分不同无线接入点 (AP) 的名称。为了安全起见，要更改内置于路由器的无线 AP 的唯一 ID 名称。它是区分大小写的，不得超过 32 个字符。保证无线客户端拥有和设备一样的 ESSID，这样才能连接到网络中。
注：区分大小写，且最多不超过 32 个字符。

ESSID 广播：其功能是将 ESSID 发射到空中，当无线客户端搜索网络时，能够发现并识别路由器。默认设置为**允许**。

禁用：如果不想广播您的 ESSID，那么任何无线客户端不管进行怎样的无线设置，都无法发现路由器的接入点 (AP)。

允许：任何客户端通过任何设置都能够找到接入点 (AP)。

区域：您可以从下拉列表中选择七个区域，包括北美、欧洲、法国等等。区域不同，设置的通道 ID 也将不同。

通道 ID：选择无线连接时要使用的 ID 通道。通过*扫描通道使用*，选择未被占用的无线通道。

扫描通道使用：无线通道扫描用时 14 秒，扫描网络中的通道 ID。扫描结果会显示所有正被使用或未被使用的 ID 通道。

注：如果选择的 ID 通道正在被其他接入点 (AP) 使用，那么无线的性能将会有所降低。

发射功率等级：其功能是增强无线传输信号强度。用户可以在 0~255 之间调整功率等级。

注：网络不同，功率等级也会不同。选择最适合您网络的功率等级。

已连接：以**真**或**假**表示，是系统和内置无线网卡之间的连接状态。

AP MAC 地址：它是接入点的唯一硬件地址。

AP 固件版本：接入点固件版本。

无线分布式系统 (WDS)

它是无线接入点模式，实现与其他接入点的无线连接和无线通信。安装很容易，只要指定连接的对端 AP 的 MAC 地址。WDS 可以节约成本并具有灵活性：两个接入点之间无需其他无线客户端设备就可以连接，可将现有的有线或无线架构的网络进行扩展，以构建一个大型网络。它可以同时连接 4 个 AP 扩展无线网络覆盖范围。

此外，WDS 可以增强 WEP 模式下的连接安全。两个 AP 的 WEP 密钥加密方式必须相同。

WDS 服务：默认设置为**禁用**。选中**启用**单选按钮以激活该功能。

1. 对端 WDS MAC 地址：它是关联的 AP 的 MAC 地址。为了与另一端的 AP 进行应答和通信，对端 AP 必须包含您的 MAC 地址，这很重要。

2. 对端 WDS MAC 地址：它是第二个关联的 AP 的 MAC 地址。

3. 对端 WDS MAC 地址：它是第三个相关联的 AP 的 MAC 地址。

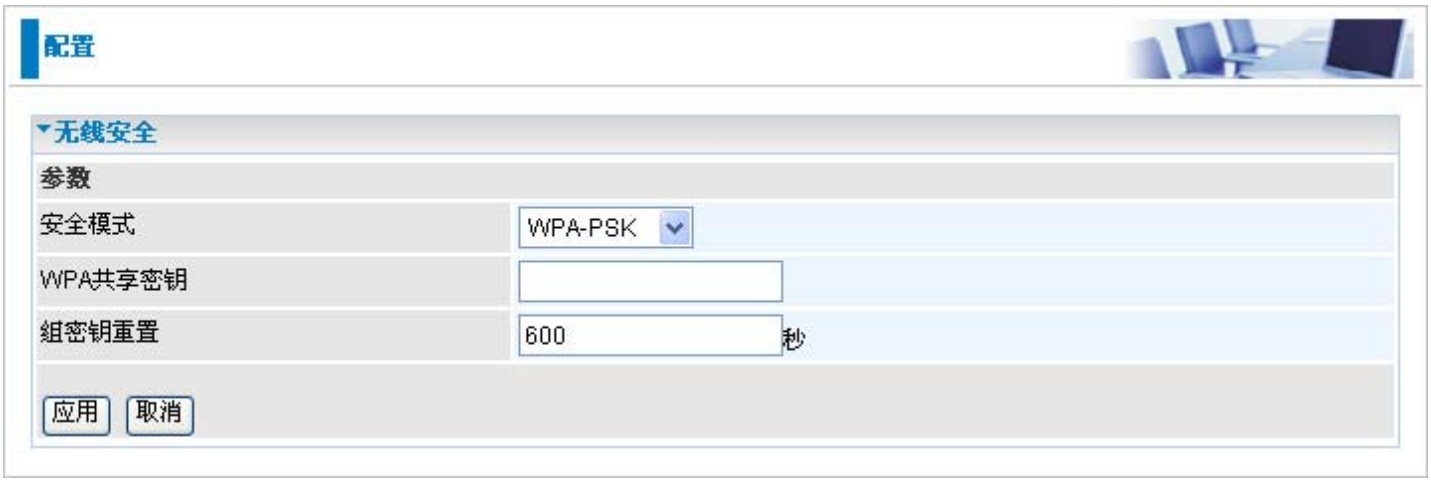
4. 对端 WDS MAC 地址：它是第四个关联的 AP 的 MAC 地址。

注：MAC 地址必须包含冒号(：)

无线安全

您可以关闭或开启 WPA 或 WEP 来保护您的网络。默认无线安全模式为**关闭**。

WPA-PSK / WPA2-PSK



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

WPA 共享密钥：该密钥用于网络认证。输入格式为字符样式，且密钥的长度必须在 8 到 63 个字符之间。

组密钥重置：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。默认为 600 秒。

WEP

WEP 认证：为了阻止未授权无线工作站访问网络中的数据，路由器提供高安全性的数据加密，也叫做 WEP。如果传输需要更高安全性，可以选择**开放式系统、共享密钥。**

WEP 加密：为了阻止未授权无线工作站访问网络中的数据，路由器提供高安全性的数据加密，也叫做 WEP。如果传输需要更高安全性，可以选择 **WEP 64 和 WEP 128。**WEP 128 提供的安全性比 WEP 64 好。

产生密钥：根据输入的字符串自动生成 WEP 密钥，预定义算法是 WEP64 或 WEP128。

默认使用的 WEP 密钥：选择加密密钥 ID，请参照下面的密钥 **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的相同。有四个密钥可以选择。输入格式为十六进制，WEP64 和 WEP128 分别需要输入 10 位和 26 位十六进制密码。

无线用户过滤

MAC 地址支持 16 台无线网络设备，通过它接收来自指定授权设备的数据流、或限制某些设备访问您的局域网，从而实现网络控制的目的。

如果没有预定义的以太网 MAC 地址过滤规则；您可以添加过滤规则以满足要求。

无线客户端过滤器：默认设置为**禁用**。

允许：在空白处插入 MAC 地址或单击“候选表”，选中“**允许**”允许指定设备访问您的局域网。确保您的 PC 的 MAC 地址在该列表中。

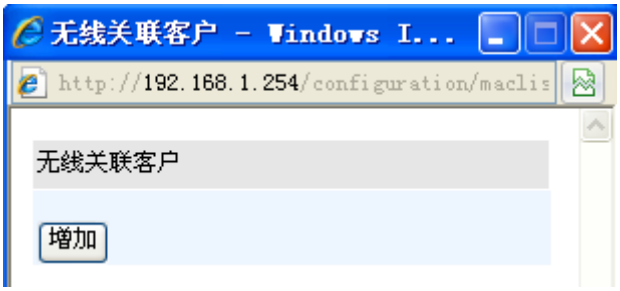
阻止：在空白处插入 MAC 地址或单击“候选表”，选中“**阻止**”阻止未经允许的设备访问您的局域网。确保您 PC 的 MAC 地址不在列表中。

最多可以有 16 个客户端。MAC 地址长度为 6 个字节，而且只能采用 16 进制表示。可以使用数字 0-9 以及字母 a – f。

注：MAC 地址采用 xx:xx:xx:xx:xx:xx 格式。必须包含分号(:)。

候选表：自动检测通过无线连接到路由器的设备。

单击**候选表**按钮，访问**相关联的无线客户端**窗口。

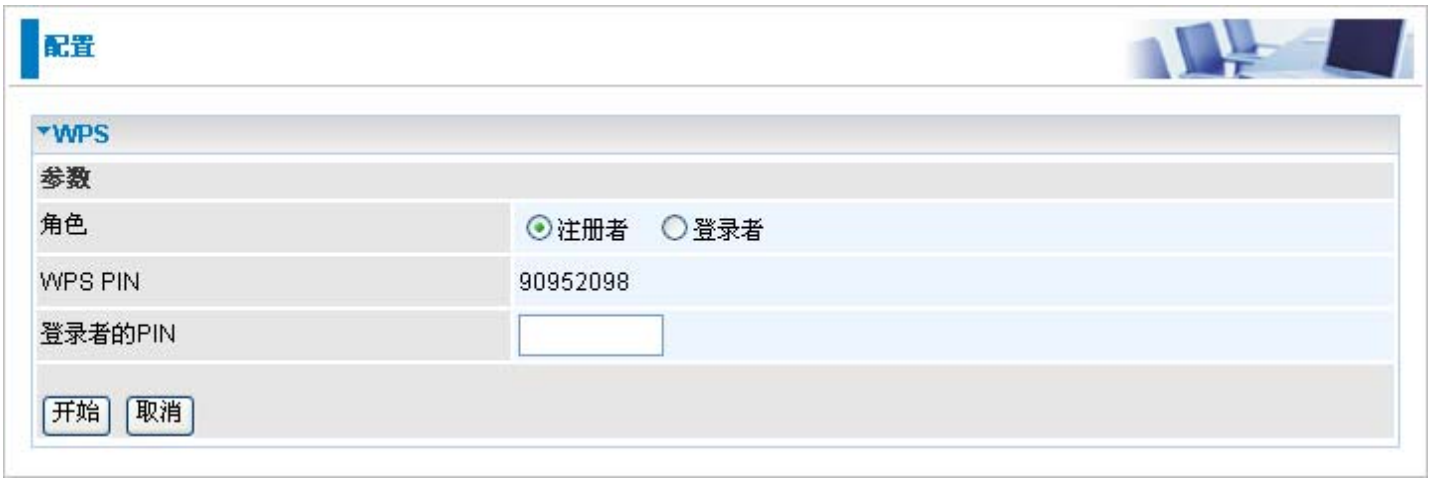


关联无线客户端：显示当前连接到路由器的所有无线设备的 MAC 地址列表。

您只要选中要阻塞或允许的 IP 地址旁边的方框。然后单击**添加**，插入到无线客户端过滤器表中。无线客户端最多可以有 16 个。

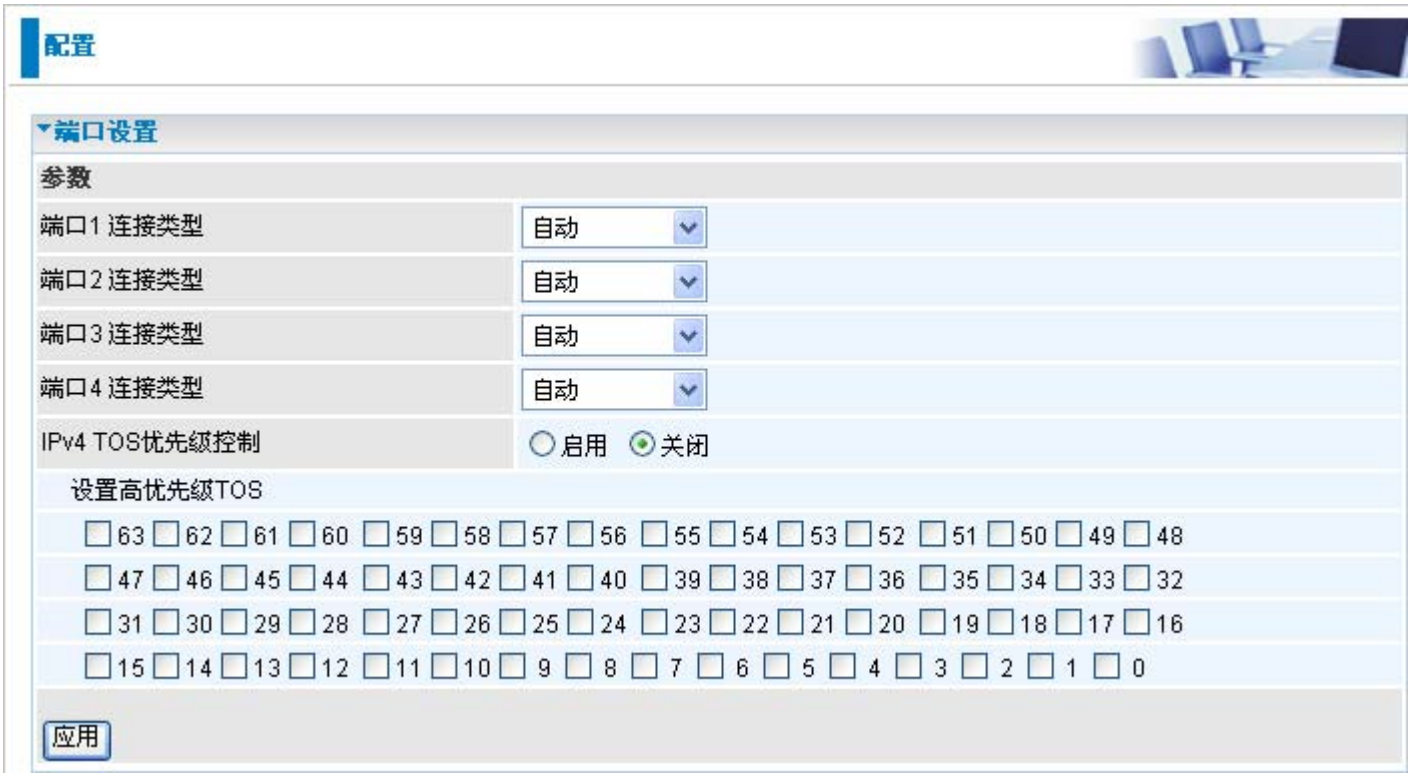
WPS

WPS（WiFi 保护安装）是由 Wi-Fi 联盟创建的标准协议。该协议用于构建家庭/小型办公室 Wi-Fi 网络，简单而又安全。从而简化了 WiFi 保护访问的配置，确保缺乏无线安全意识的用户的网络安全。



端口设置

通过端口设置对路由器的以太网端口进行配置，从而解决连接到 Internet 时可能发生的兼容性问题，用户也可以调整网络性能。



端口连接类型：有六个选项可供选择：自动、禁用、10M 半双工、10M 全双工、100M 半双工、100M 全双工以及禁用。有时，过时的以太网设备会存在以太网兼容性问题，通过配置不同的类型，可以解决这样的问题。默认设置为**自动**，除非出现 PC 无法访问 LAN，否则将保留此默认设置。

IPv4 TOS 优先级控制（高级用户）：TOS 即服务类型，IP 封包的第 2 个八位元组。八位元组的第 6-7 位保留，0-5 位用来指定封包的优先级。

使用第 0-5 位对封包优先级进行分类。如果封包优先级为高，它将第一个通过且不受速率限制。因此启用该功能后，路由器的以太网开关将检查每个 IP 封包的第 2 个八位元组。如果 TOS 字段中的值与表中选中的值（0 到 63）相匹配，则认为该封包的优先级为**高**。

DHCP 服务器

您可以禁用或启用 DHCP（动态主机配置协议）服务器或启用路由器的 DHCP 中继功能。如果配置为自动获取 IP 地址，DHCP 协议将允许路由器为网络中的 PC 动态分配 IP 地址。

要关闭路由器的 DHCP 服务器，选中**关闭**并单击**下一步**，然后再单击**应用**。如果 DHCP 服务器是关闭的，则需要手动分配固定 IP 地址给网络中的每台 PC，并且要将每个 PC 的配置默认网关设置为路由器的 IP 地址。（默认是 192.168.1.254）。

要配置路由器的 DHCP 服务器，选择 **DHCP 服务器**并单击**下一步**。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），被分配的 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。单击**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 ADSL 路由器将执行 DNS 查询，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。

如果选择 **DHCP 中继代理**，并单击**下一步**，您必须输入 DHCP 服务器的 IP 地址，DHCP 服务器再将 IP 地址分配给 DHCP 客户端。仅当网络管理员或 ISP 建议时使用此功能。点击**应用**开启此功能。

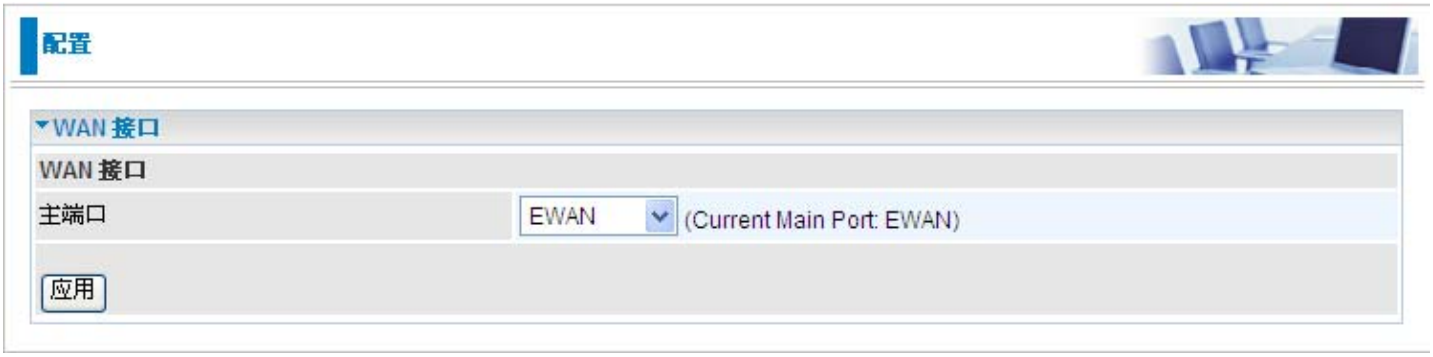
WAN – 广域网

WAN（广域网）指广域网连接，如路由器与 ISP 以及 Internet 的连接。**WAN** 部分包括：**WAN 接口、WAN 配置以及 ADSL 模式。（6404VGO(P)X 没有 ADSL 模式）**

WAN 接口

WAN 连接 – EWAN 模式

默认的连接模式是 EWAN



WAN 连接 – ADSL 模式

WAN 连接 - 3G 模式

如果 ADSL/EWAN 连接不能用（故障转移/故障切换），将会切换到 3G 模式，进行 WAN 连接。然而，3G 模式下，如果不能使用 3G，将无法通过 ADSL 进行 WAN 连接。

WAN 连接 – Dual WAN

主端口：选择 Dual WAN 作为主端口。

Mode：设备使用的模式。

WAN1：从ADSL，3G 和 EWAN三种连接中选择一种。

WAN2：从与WAN1的连接不同的两种连接中选择一种。

计划时间：选择总是连接，或者从TimeSlot1~ TimeSlot16中选择一种。

连接状态：输入探测连接失败的次数。

Failover/Failback 探测周期：输入探测连接的周期。

WAN 配置

ADSL

PPPoE 连接

PPPoE（以太网上点对点协议）提供类似于使用 PPP 拨号的访问控制。

配置端口：选择 ADSL 作为配置端口。

协议：设备使用的 ATM 协议。

描述：指定的连接名称。

VPI/VCI：输入 ISP 提供的信息。

ATM 类：ATM 层的服务质量。

用户名：输入 ISP 提供的用户名。您最多可以输入 **128** 个字母数字字符（区分大小写）。格式为“username@ispname”，而不是“username”。

密码：输入 ISP 提供的密码。最多可以输入 **128** 个字母数字字符（区分大小写）。

服务名称：这个字段起标识作用。需要的话，由 ISP 提供。最多可以输入 15 个字母数字字符。

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，那么关闭 NAT 功能。

IP 地址（0.0.0.0：自动）：WAN 口的 IP 地址。保持 0.0.0.0 将自动从 ISP 获取 IP 地址。

认证协议类型：默认为 Chap（自动）。应由 ISP 建议您使用 Chap 还是 Pap。

连接：

总是连接：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 PPPoA 会话。

按需连接：如果您只想在有封包请求访问 Internet 时建立 PPPoA 会话（如：您计算机上的某个程序想要访问 Internet 时）。

空闲时间：规定时间内网络中没有数据流时，路由器会自动断开宽带防火墙网关。

详细：您可以定义目标端口和封包类型 (TCP/UDP)，而无须通过计时器检查。通过它，您可以设置哪些外出流量将不触发并重置空闲计时器。

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。

RIP：RIP v1、RIP v2 以及 RIP v2 多播。选择以开启 RIP 功能。

TCP MSS Clamp：帮助自动找到最佳的 MTU 大小。默认为开启。

MAC 地址伪装：一些服务提供商要求设置此项。需要时您必须填写由服务提供商指定的 MAC 地址。默认为关闭。

获得 DNS：域名系统 (DNS) 包含域名和 IP 地址的映射表。DNS 帮助查找指定域名的 IP 地址。选中复选框，自动获得 DNS。

首选 DNS：输入首选 DNS。

备用 DNS：输入备用 DNS。

PPPoA 连接

配置端口：选择 ADSL 作为配置端口。

协议：设备使用的 ATM 协议。

描述：指定的连接名称。

VPI/VCI：输入 ISP 提供的信息。

ATM 类：ATM 层的服务质量。

用户名：输入 ISP 提供的用户名。您最多可以输入 **128** 个字母数字字符（区分大小写）。格式为“username@ispname”，而不是“username”。

密码：输入 ISP 提供的密码。最多可以输入 **128** 个字母数字字符（区分大小写）。

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，那么关闭 NAT 功能。

IP 地址（0.0.0.0：自动）：WAN 口的 IP 地址。保持 0.0.0.0 将自动从 ISP 获取 IP 地址。

认证协议类型：默认为 Chap（自动）。应由 ISP 建议您使用 Chap 还是 Pap。

连接：

总是连接：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 PPPoA 会话。

按需连接：如果您只想在有封包请求访问 Internet 时建立 PPPoA 会话（如：您计算机上的某个程序想要访问 Internet 时）。

空闲时间：规定时间内网络中没有数据流时，路由器会自动断开宽带防火墙网关。

详细：您可以定义目标端口和封包类型 (TCP/UDP)，而无须通过计时器检查。通过它，您可以设置哪些外出流量将不触发并重置空闲计时器。

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。

RIP：RIP v1、RIP v2 以及 RIP v2 多播。选择以开启 RIP 功能。

TCP MSS Clamp：帮助自动找到最佳的 MTU 大小。默认为开启。

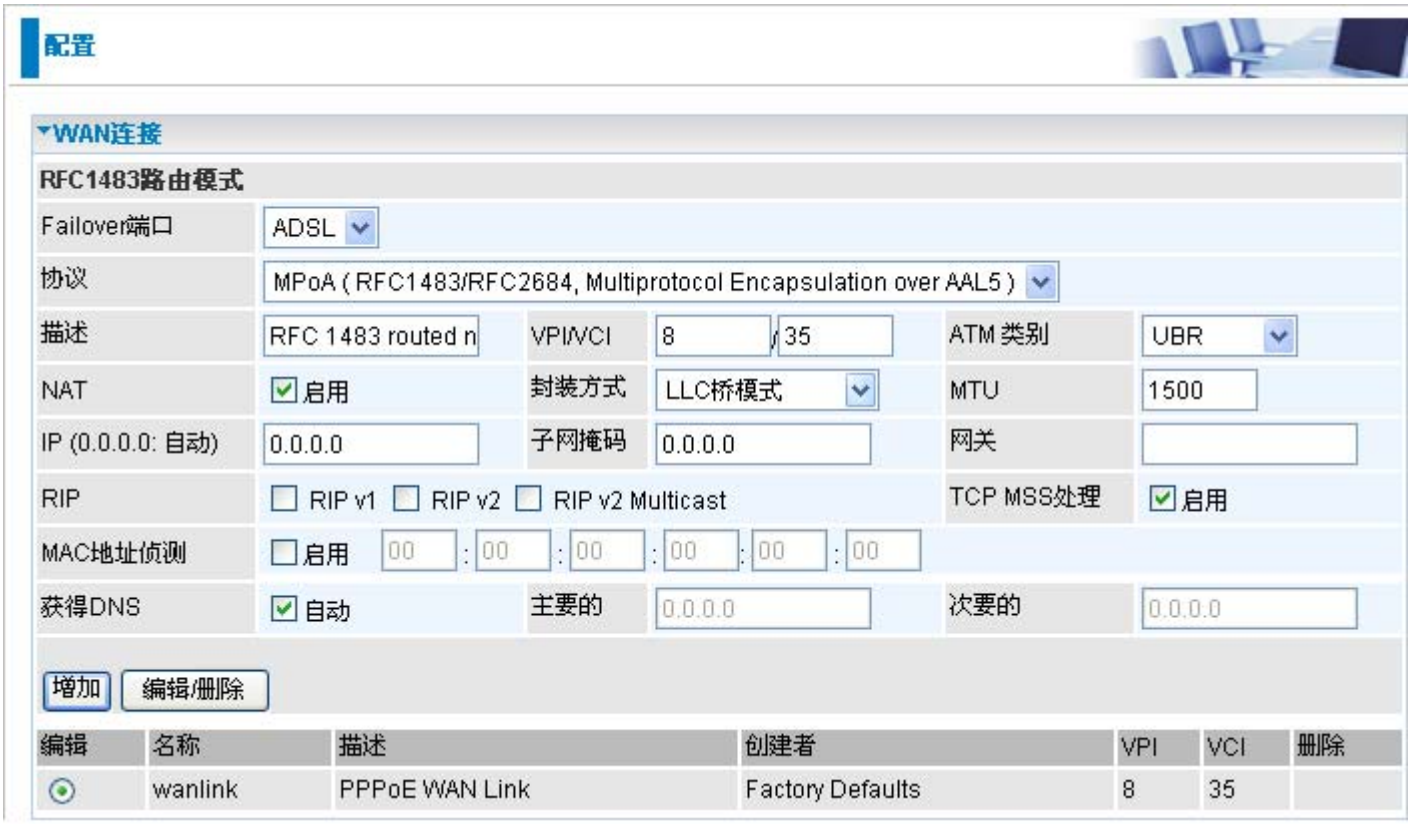
MAC 地址伪装：一些服务提供商要求设置此项。需要时您必须填写由服务提供商指定的 MAC 地址。默认为关闭。

获得 DNS：域名系统 (DNS) 包含域名和 IP 地址的映射表。DNS 帮助查找指定域名的 IP 地址。选中复选框，自动获得 DNS。

首选 DNS：输入首选 DNS。

备用 DNS：输入备用 DNS。

MPoA 连接



配置端口：选择 ADSL 作为配置端口。

协议：设备使用的 ATM 协议。

描述：指定的连接名称。

VPI/VCI：输入 ISP 提供的信息。

ATM 类：ATM 层的服务质量。

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，那么关闭 NAT 功能。

封装方式：选择 WAN 端口数据包的封装方式为桥接还是路由。

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。

IP 地址（0.0.0.0：自动）：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 255.255.255.0。用户可以更改子网掩码，如改成 255.255.255.128。输入 ISP 指定的子网掩码（如果有提供的话）。

网关：输入默认网关的 IP 地址（如果有提供的话）。

RIP：RIP v1、RIP v2 以及 RIP v2 多播。选择以开启 RIP 功能。

TCP MSS Clamp：帮助自动找到最佳的 MTU 大小。默认为开启。

MAC 地址伪装：一些服务提供商要求设置此项。需要时您必须填写由服务提供商指定的 MAC 地址。默认为关闭。

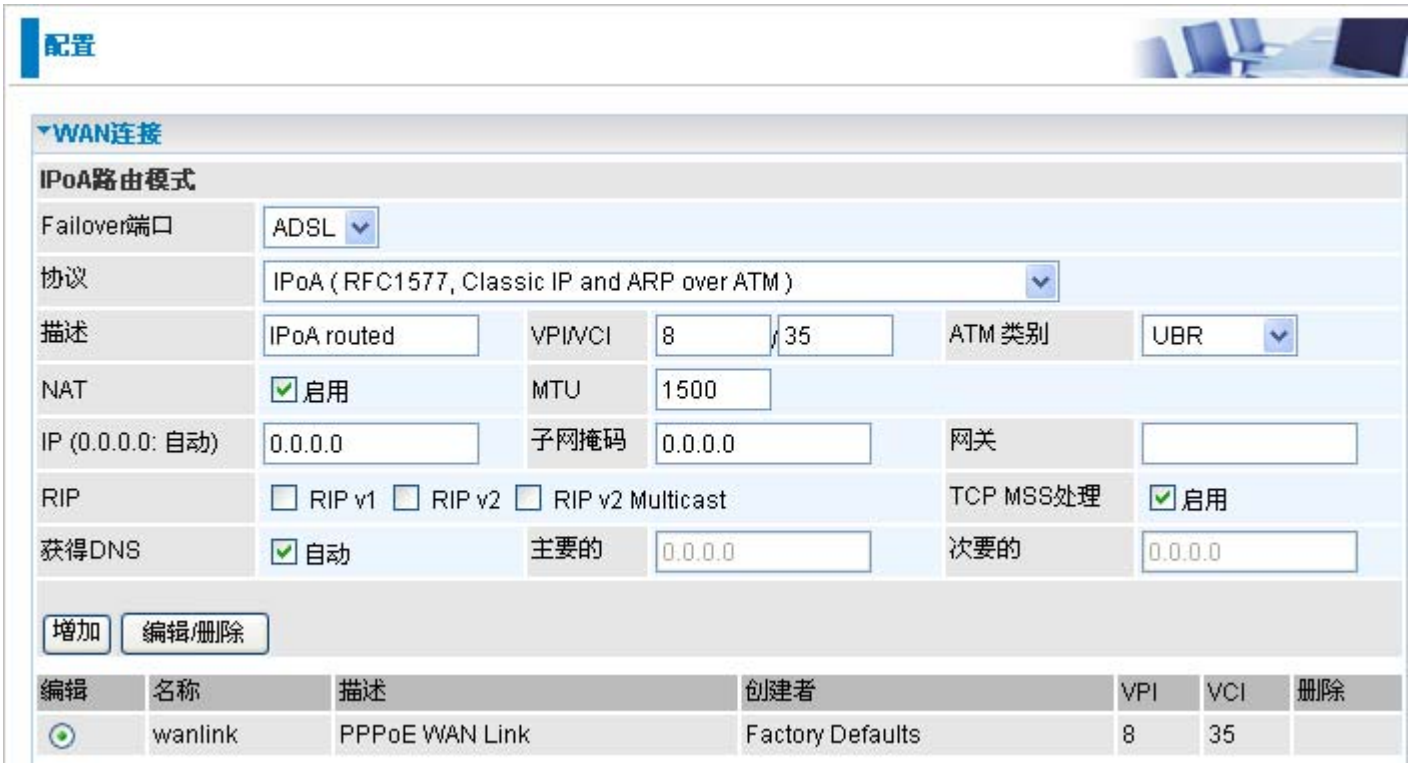
获得 DNS：域名系统 (DNS) 包含域名和 IP 地址的映射表。DNS 帮助查找指定域名的 IP 地址。选

中复选框，自动获得 DNS。

首选 DNS：输入首选 DNS。

备用 DNS：输入备用 DNS。

IPoA 路由连接



配置端口：选择 ADSL 作为配置端口。

协议：设备使用的 ATM 协议。

描述：指定的连接名称。

VPI/VCI：输入 ISP 提供的信息。

ATM 类：ATM 层的服务质量。

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，那么关闭 NAT 功能。

封装方式：选择 WAN 端口数据包的封装方式为桥接还是路由。

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。

IP 地址（0.0.0.0：自动）：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 255.255.255.0。用户可以更改子网掩码，如改成 255.255.255.128。输入 ISP 指定的子网掩码（如果有提供的话）。

网关：输入默认网关的 IP 地址（如果有提供的话）。

RIP：RIP v1、RIP v2 以及 RIP v2 多播。选择以开启 RIP 功能。

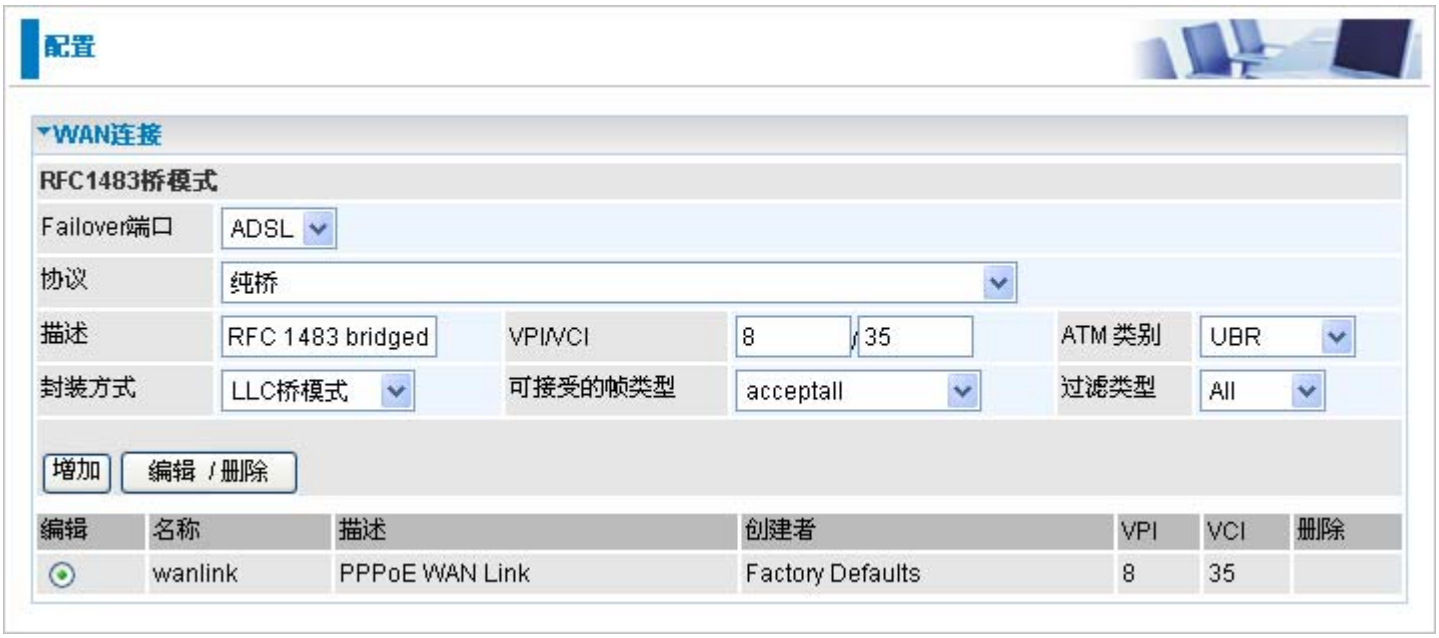
TCP MSS Clamp：帮助自动找到最佳的 MTU 大小。默认为开启。

获得 DNS：域名系统 (DNS) 包含域名和 IP 地址的映射表。DNS 帮助查找指定域名的 IP 地址。选中复选框，自动获得 DNS。

首选 DNS：输入首选 DNS。

备用 DNS：输入备用 DNS。

纯桥接



配置端口：选择 ADSL 作为配置端口。

协议：设备使用的 ATM 协议。

描述：指定的连接名称。

VPI/VCI：输入 ISP 提供的信息。

ATM 类：ATM 层的服务质量。

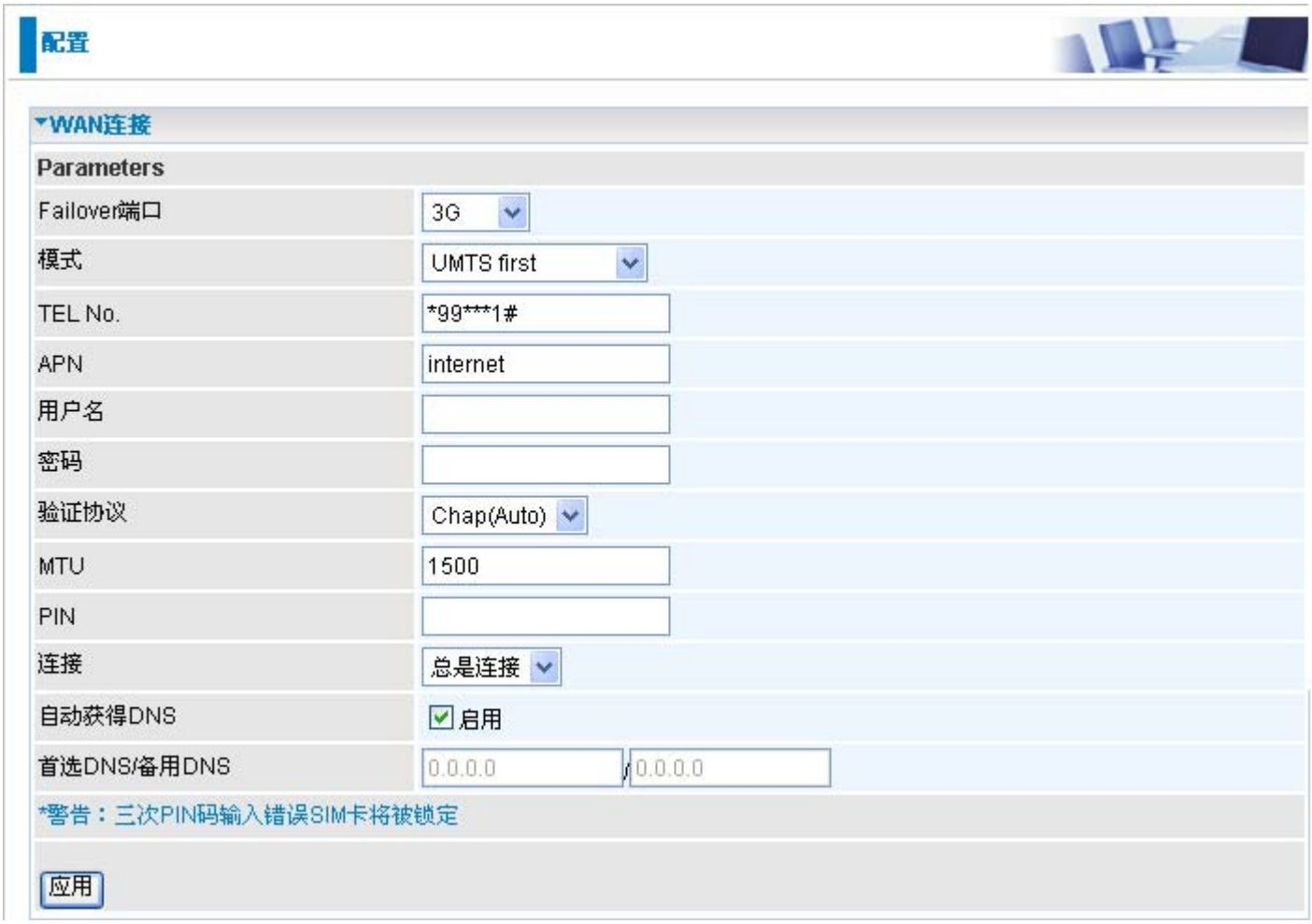
封装方式：选择 WAN 端口数据包的封装方式为桥接还是路由。

可接收帧类型：指定可以通过连接的流量类型，是所有流量还是只有带 VLAN 标记的流量。

过滤类型：规定特定的桥接口采用的以太网过滤类型。

所有	允许所有类型的以太封包通过端口。
Ip	只允许 IP/ARP类型的以太封包通过端口。
Pppoe	只允许 PPPoE类型的以太封包通过端口。

3G



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。

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。

认证类型：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。

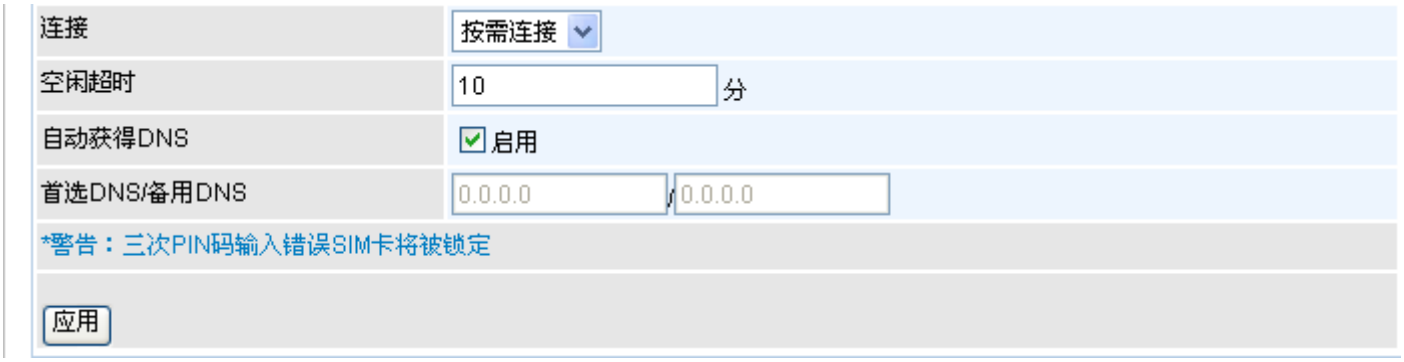
MTU：最大传输单元。IP 试图通过接口传输的最大数据报（不包括特定于媒体的报头）的长度。

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。

连接：

总是连接：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**。

保持连接：设置**启用**后，当 ISP 断开连接时，路由器将自动进行重新连接。



按需连接：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。

自动获得 DNS：选择该复选框，使用 DNS。

首选 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。

EWAN

自动获得IP地址

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

Failover端口：选择 EWAN作为Failover端口。

协议：选择自动获取IP地址协议。

获得 DNS：域名系统 (DNS) 包含域名和 IP 地址的映射表。DNS 帮助查找指定域名的 IP 地址。选中复选框，自动获得 DNS。

主要的/次要的：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。

绑定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。

Failover端口：选择 EWAN作为Failover端口。

协议：选择**绑定IP地址**协议。

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：域名系统 (DNS) 包含域名和 IP 地址的映射表。DNS 帮助查找指定域名的 IP 地址。选中复选框，自动获得 DNS。

主要的/次要的：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。

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。

Failover 端口：选择 EWAN作为Failover端口。

协议：选择PPPoE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（区分大小写）。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（区分大小写）。

服务名称:连接时输入一个名字。

IP ：WAN 口的IP 地址。保持0.0.0.0 将自动从ISP 获取IP 地址。

连接：

总是连接：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 PPPoA 会话。

按需连接：如果您只想在有封包请求访问 Internet 时建立 PPPoA 会话（如：您计算机上的某个程序想要访问 Internet 时）。

空闲时间：规定时间内网络中没有数据流时，路由器会自动断开宽带防火墙网关。

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。

认证协议: 默认是自动。您的ISP 可能会使用**Chap** 或 **Pap**。

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。

获得DNS：勾选可以自动获得DNS。

主要的/次要的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。

纯桥

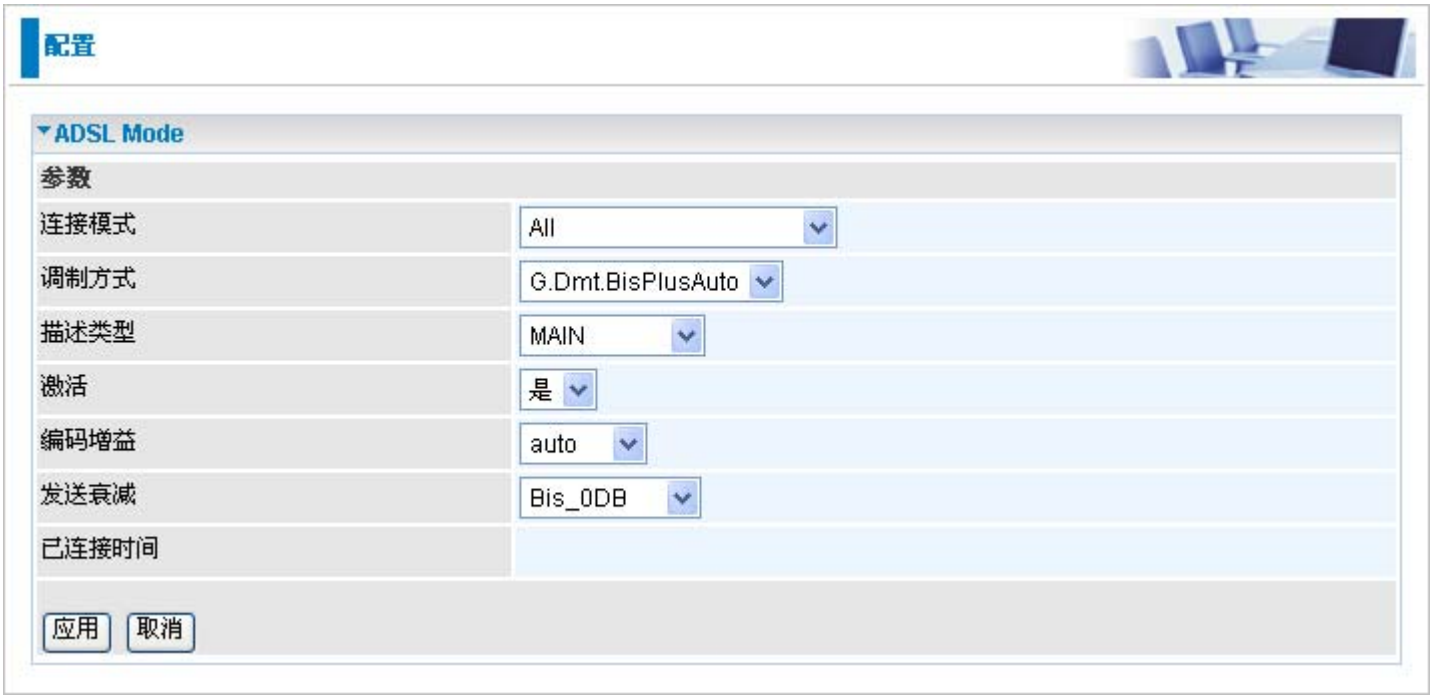
Failover 端口：选择 EWAN作为Failover端口。

协议：选择**纯桥**协议。

可接收帧类型：指定可以通过连接的流量类型，是所有流量还是只有带 VLAN 标记的流量。

过滤类型：规定特定的桥接口采用的以太网过滤类型。

ADSL 模式



连接模式：此模式下会自动检测 ADSL 线路编码：ADSL2+、ADSL2、AnnexM2 和 AnnexM2+、ADSL、所有。除非检测出 ADSL 存在同步问题，否则保留这些默认设置。

调制方式：将自动检测 ADSL 线路的性能。除非检测出 ADSL 存在同步问题，否则保留这些默认设置。

配置类型：除非检测出 ADSL 存在连接速度太低或不稳定问题，否则保留这些默认设置。您也可以更改配置设置，以达到最佳的连接速度，这取决于不同的 DSLAM 和 位置。

激活线路：先断开（假） ADSL 线路然后再激活（真），就可以使**连接模式**设置生效。

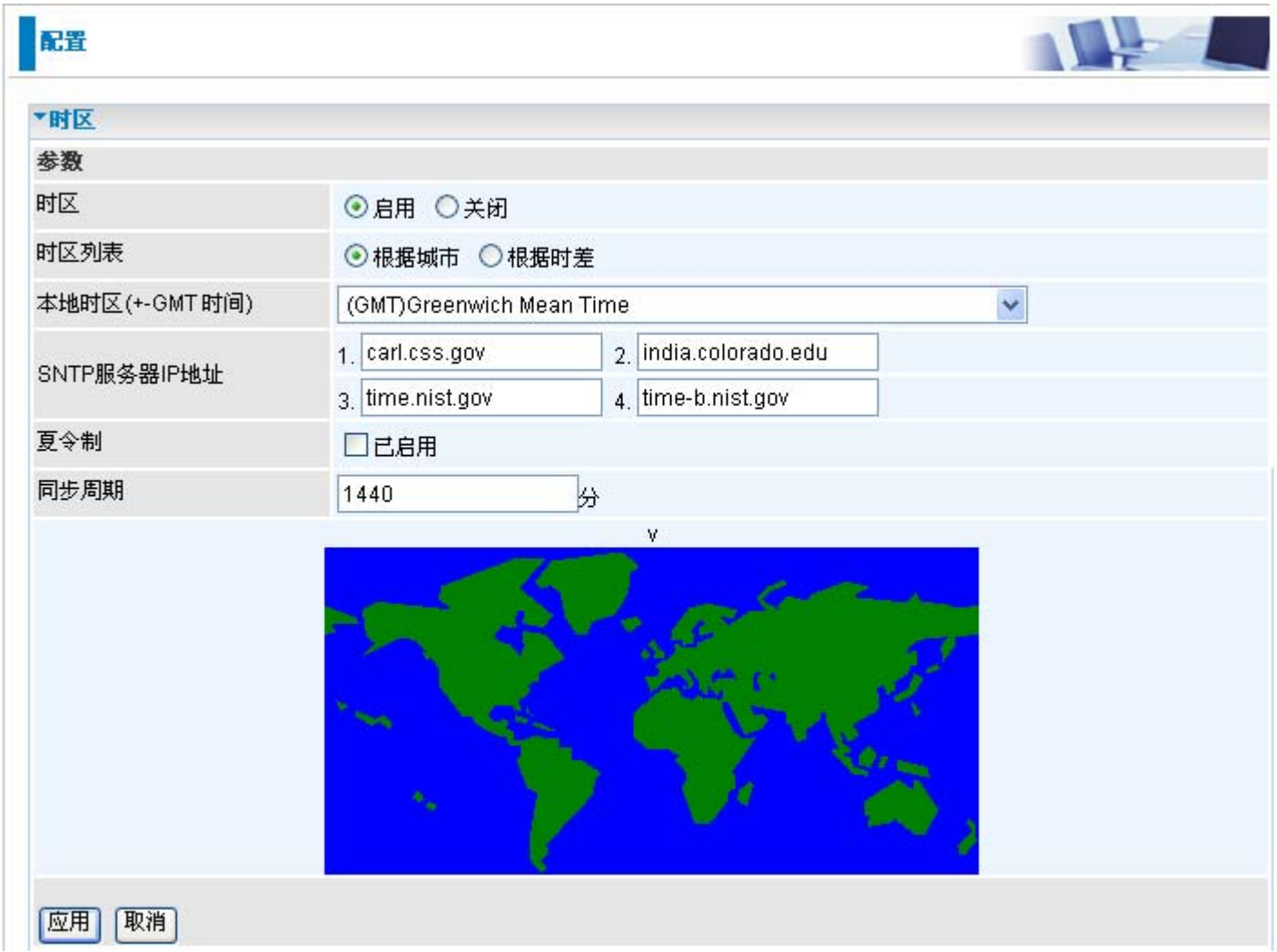
编码增益：它能减弱路由器的传输功率，从而影响路由器的下行速率。增益越高，下行速率越快，但有时会造成 ADSL 线路不稳定。可在 0 dB 到 7dB 配置 ADSL 编码增益，或自动配置。

Tx 衰减：调制解调器使用的 ADSL 传输功率。功率越低，路由器的上行速率越快。

系统

系统部分包括以下几部分：**时区、远程访问、版本升级、备份/还原、重启、用户管理**以及**Mail Alert**。

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。

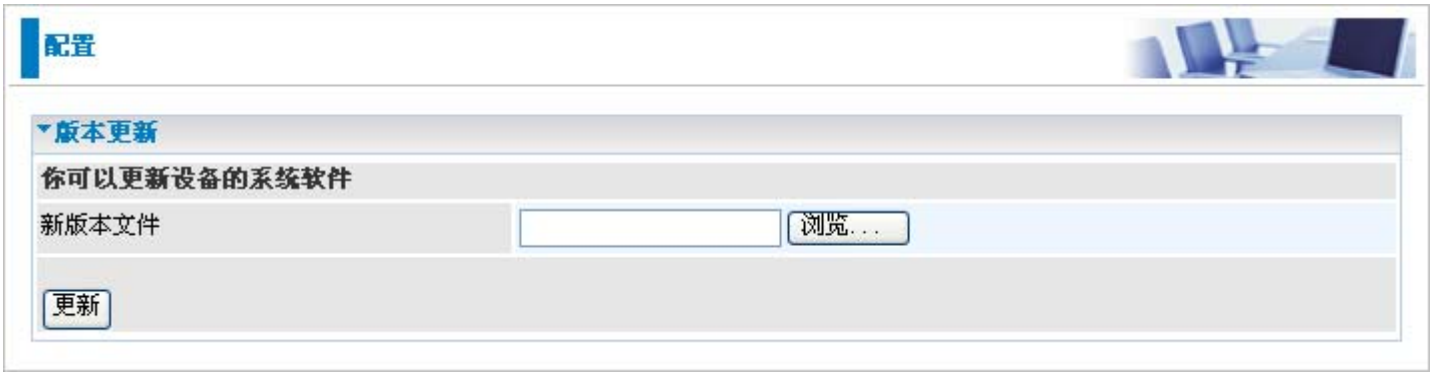
日光节约时间又称***夏时制***。世界上许多国家都在夏季采用夏时制，将当地标准时间的日照时间提前 1 小时。勾选**自动**框自动设置当地时间。

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。

远程访问

若要临时允许远程管理路由器（如从 LAN），选择允许远程访问路由器的时间段，单击**启用**。
使用 GUI 上**高级**部分的**设备管理**选项，更改 web 管理界面上的其他配置选项。
想要永久启用远程访问，将时间段设置为 **0** 分钟。

版本升级



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。选择后，点击**升级**可以升级您的路由器。

警告

升级过程中不要关闭路由器或中断固件升级。操作不当可能会损坏路由器。

备份/还原

通过这些功能，可以将路由器的当前设置保存并备份到您的 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更改之前备份您的路由器设置。

创建路由器配置备份

要备份设置，只要按住**备份**按钮并指定配置文件保存位置。您也可以更改文件名，保存多个备份。

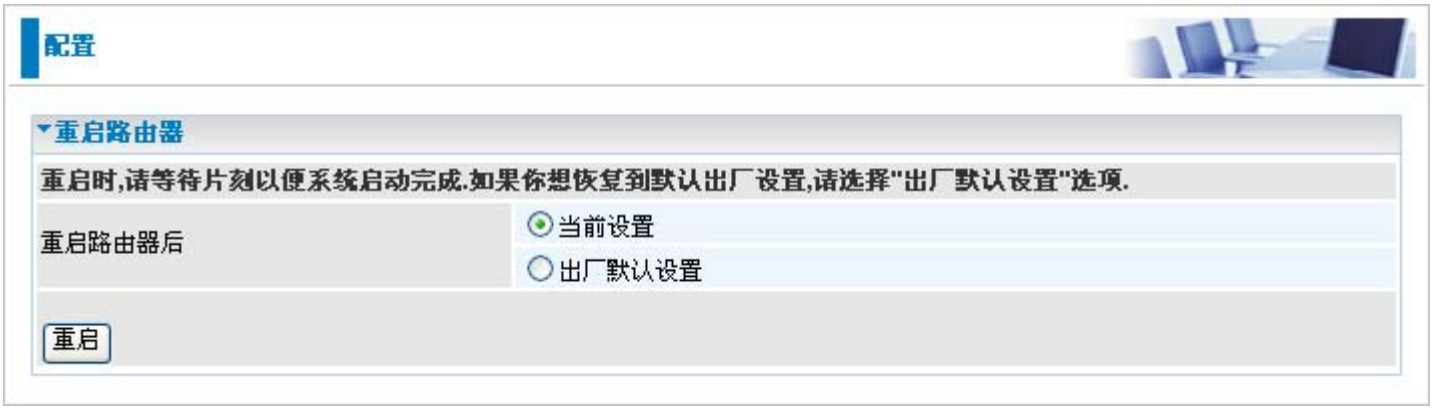
恢复路由器配置

要恢复路由器的配置，按住**浏览**按钮，找到 PC 上的配置文件。找到文件后，单击**文件**，然后单击**恢复**按钮以加载设置。

注：只能通过备份功能恢复创建的文件设置。不得以任何形式对保存到 PC 的设置文件进行手动编辑。

重启路由器

选择**当前设置并**单击**重启**，以重新启动路由器（恢复最后保存的配置）。



如果想重启路由器恢复到出厂默认设置（例如，固件升级后或保存了错误的配置），选择出厂默认设置可以恢复到默认设置。

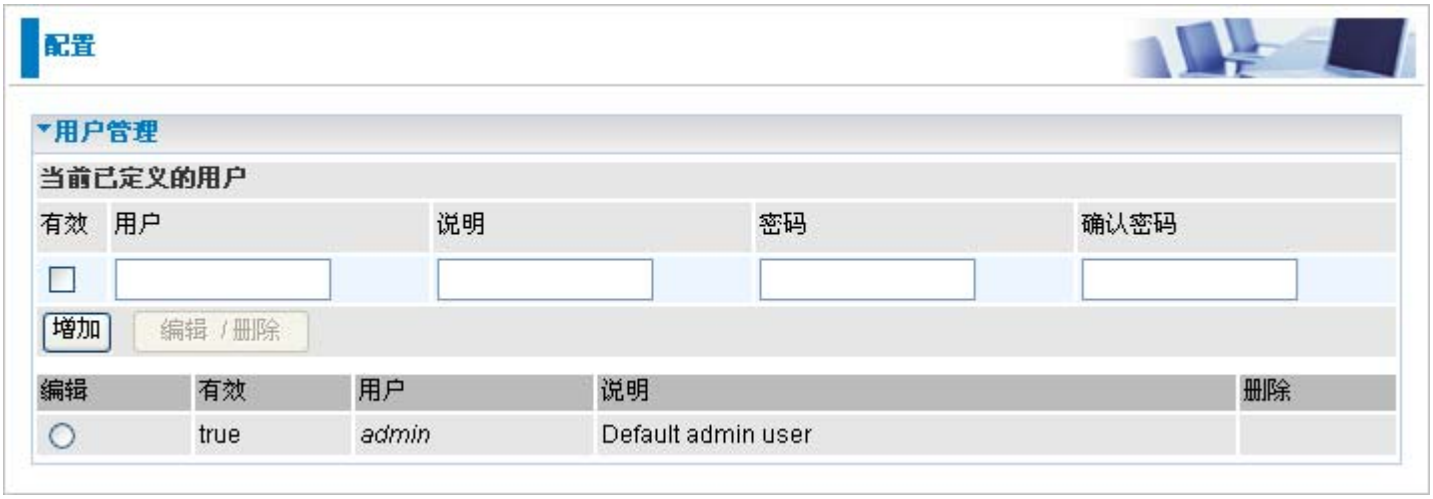
您也可以按住路由器后端面板上的 Reset 针孔按钮超过 6 秒钟，将路由器恢复到出厂默认设置。

注：按住 Reset 按钮超过 6 秒钟后，要保证路由器再次通电。

用户管理

为了防止未授权用户访问路由器的配置界面，用户需要使用密码登录 GUI。您可以设置多个用户账号，每个账号都有对应的密码。

可对现有用户账号进行编辑，或创建可以访问设备配置界面的新用户。

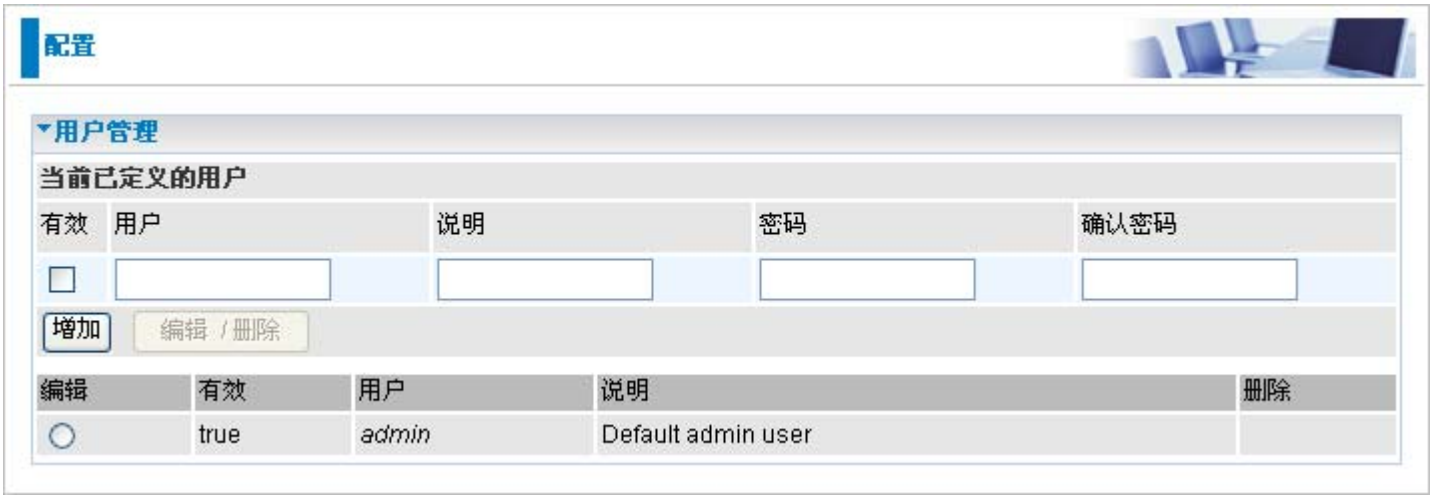


编辑账号信息

您可以更改账号信息（不论账号是处于活动状态还是有效状态）。

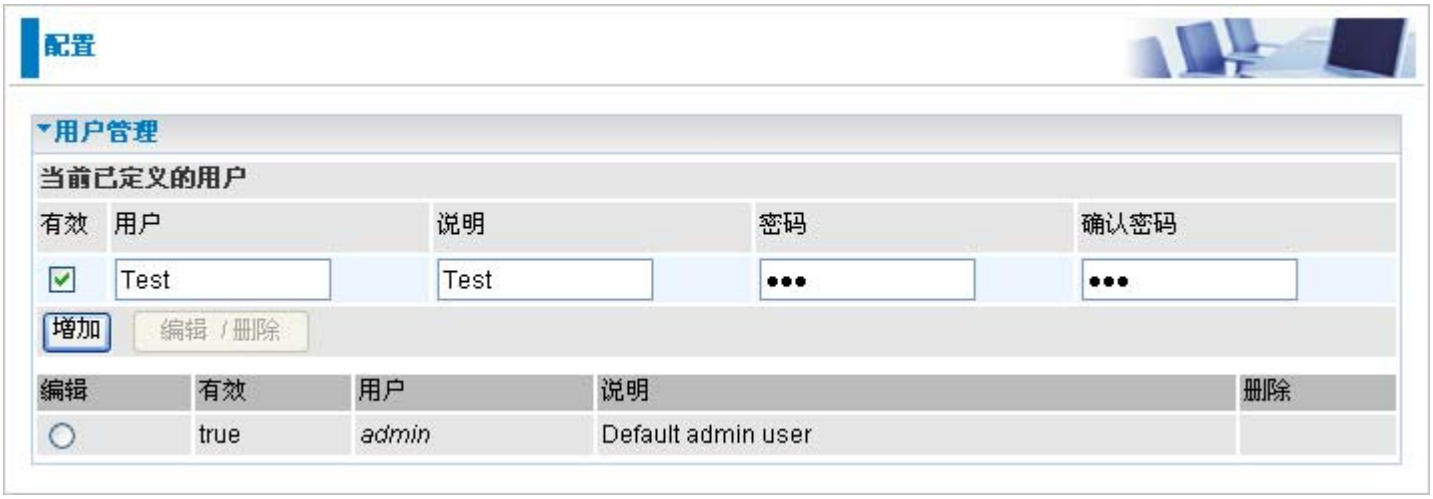
1. 要编辑账号，选择要编辑账号前面的**编辑**单选按钮。一旦选择，将显示该账号的所有信息。
2. 删除要编辑的账号信息，然后用新账号代替。
3. 完成后，单击**编辑/删除**按钮保存更改。

注：为了 GUI 的安全，建议您立即更改密码。



增加账号

1. 选中**有效**复选框，填写信息：用户名、说明（可选）、密码、确认密码。
2. 完成后，单击**增加**按钮。

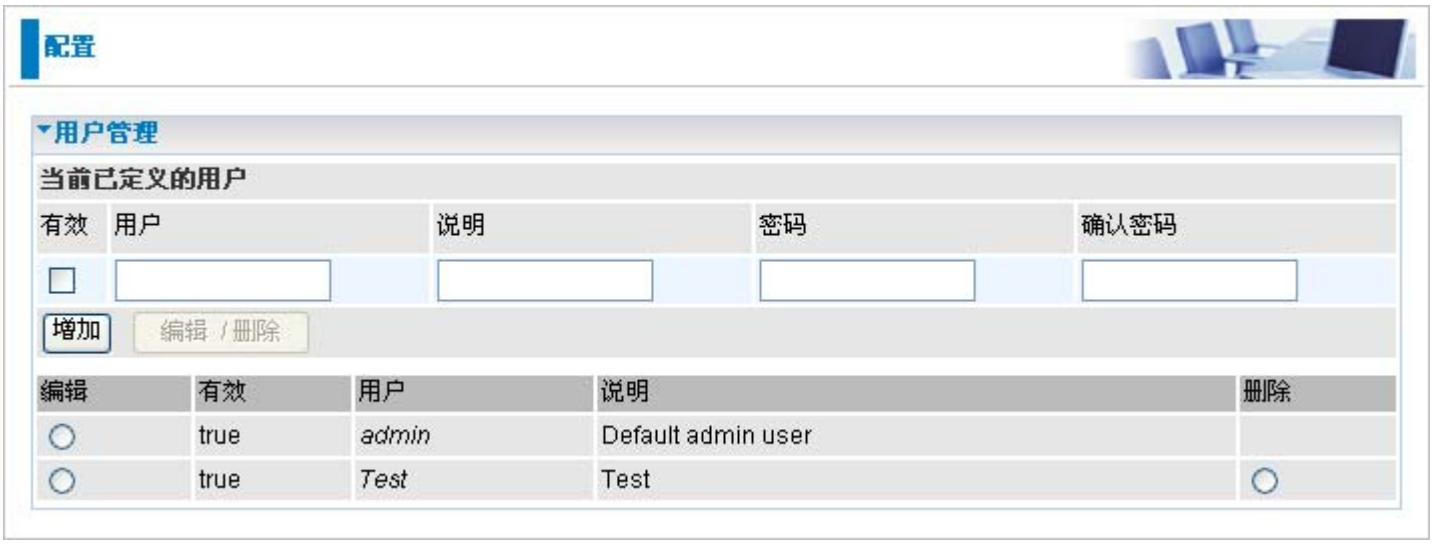


删除用户账号

1.单击您想要删除的账号前面的**删除**单选按钮。

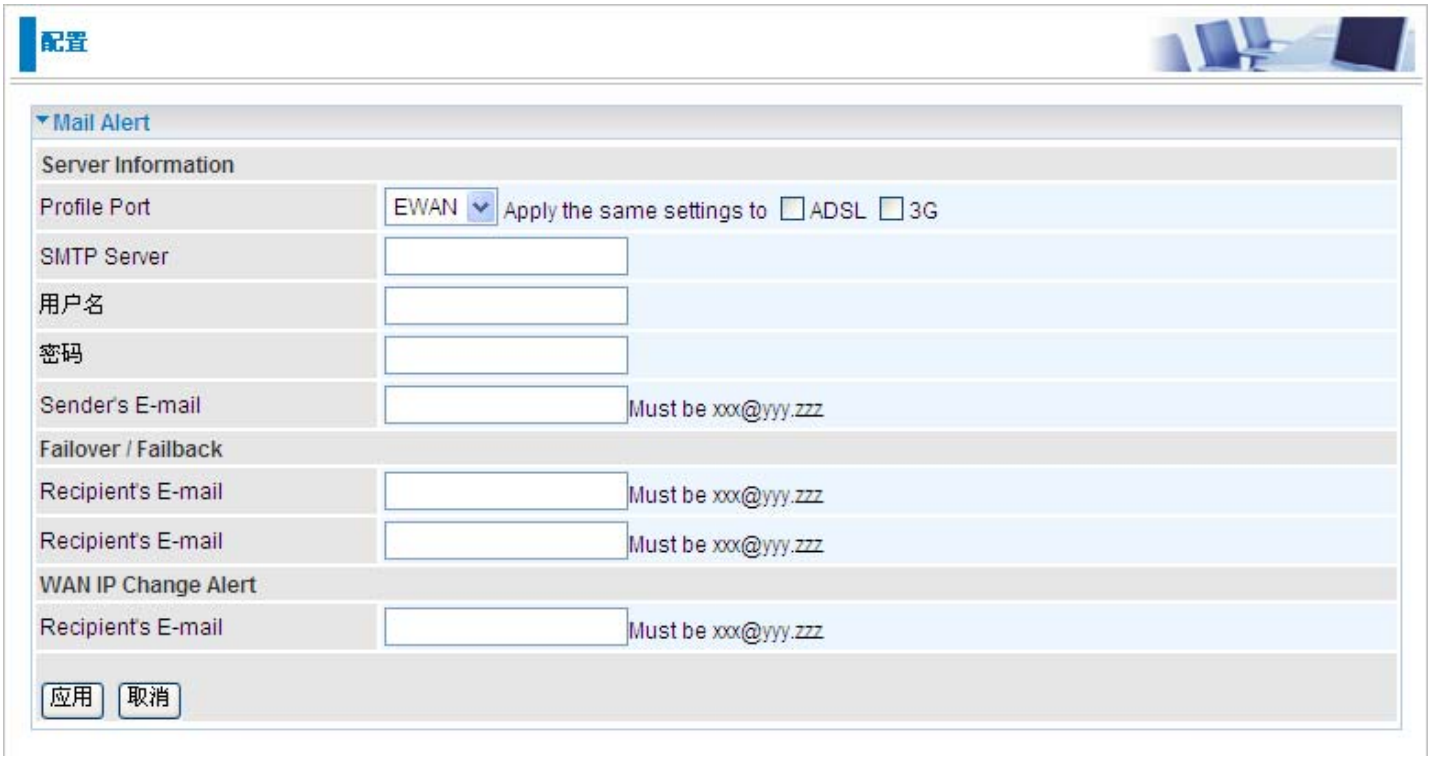
2. 然后单击**编辑/删除**按钮，确认删除。

注：您可以删除默认管理员账号以外的其他任何账号。管理员账号没有删除单选按钮。



Mail Alert

在 WAN IP 被更改或入侵者未经授权访问您的计算机的时候会通过邮件发送日志警告。



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。.

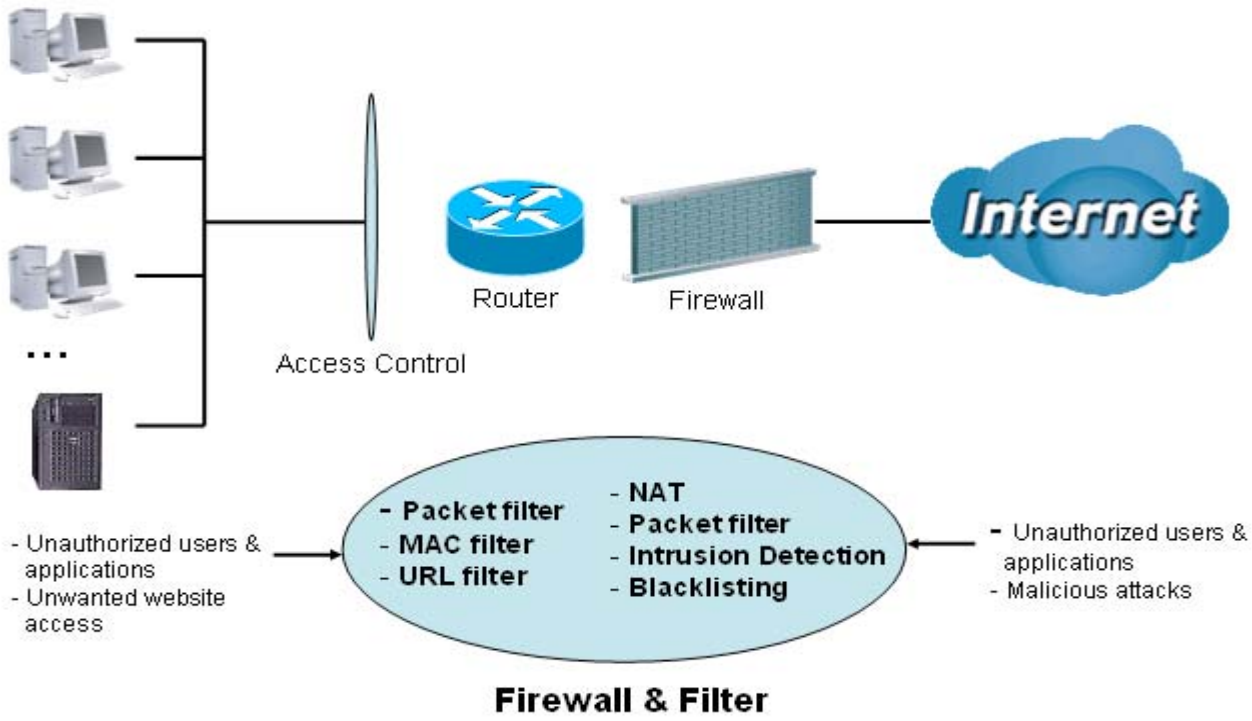
密码：输入邮箱账户密码。

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。

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，控制通过 LAN 访问 Internet，并阻止黑客攻击。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 中的所有 PC 使用私有 IP 地址不能直接访问到 Internet。这款路由器提供三级安全支持。



NAT 天然防火墙：使 LAN 中用户的 IP 在 Internet 中不可见，让黑客更难攻击您网络中的计算机。开启 NAT 功能就可以使用天然防火墙。

防火墙安全和策略（基本设置）：入站包过滤规则防止未授权的计算机或应用程序从 Internet 访问您的本地网络。

入侵检测：开启入侵检测可以侦测、防止和记录恶意攻击。

访问控制：阻止本地网络中的 PC 访问。

防火墙安全和策略（基本设置）：入站包过滤规则防止未授权的计算机或应用程序从 Internet 访问您的本地网络。

URL 过滤：可以阻塞本地网络中的 PC 访问限制站点。

NOTE:

如果在防火墙包过滤设置中将特定端口设置为开放，则使用虚拟服务器时，您的 PC 将根据虚拟服务器的设置，有不同程度的暴露。

防火墙包括以下几部分：**基本设置、包过滤、入侵检测、URL 过滤、阻止 IM/P2P 通信以及防火墙日志。**

基本设置

可以选择不启用防火墙但仍然能够使用 URL 过滤和 IM/P2P 阻塞功能，或使用预设过滤规则启用防火墙，并根据需要修改端口过滤规则。包过滤功能用来过滤基于应用程序（端口）或 IP 地址的包。

有 4 个策略选项可供选择：

阻塞所有流量/用户自定义：默认情况下，如果没有预定义的端口或地址过滤规则，说明所有接收到的数据包（从 Internet 到 LAN）和转发的数据包（从 LAN 到 Internet）都被阻塞。用户要访问 Internet，必须自己添加过滤规则。

高/中/低安全级别：针对**高、中、低**安全等级的预定义端口过滤规则显示在**包过滤端口过滤**中。

选择**高、中、低安全级别，**以启用防火墙。三种安全级别之间唯一不同的是：**包过滤**中预设的端口过滤规则不同。不同安全级别，防火墙功能一样；只有预设端口过滤列表不同。有关预设端口过滤级别的详细信息，请参阅**表 1：预定义的端口过滤。**

如果选择预设的安全级别并添加自定义过滤，过滤规则级别被保存，不需要再重新配置规则（如果您禁用或切换到其他防火墙级别的时候）。

“阻塞 WAN 请求”是独立的功能，与是否启用安全无关。通常用来阻塞来自 WAN 站点黑客的扫描工具。

任何远程用户如果执行此操作，可能导致阻塞通过 Internet 访问、配置和管理设备。

包过滤

只有启用了防火墙并选择了安全等级（阻塞所有、高、中、低）后，才能使用包过滤功能。包过滤中的预设端口过滤规则必须根据所选的防火墙安全等级进行修改。有关详细信息，参阅**表 1：预定义端口过滤**。

实例：预定义的端口过滤规则

针对高、中、低安全级别的预定义端口过滤规则如下。参阅表 1。

注：防火墙 – 阻塞所有I用户自定义，您必须自己定义和创建端口过滤规则。不预先配置预定义过滤规则。

应用	协议	端口号		防火墙 – 低		防火墙 – 中		防火墙 – 高	
		起始	终止	入站	出站	入站	出站	入站	出站
HTTP(80)	TCP(6)	80	80	否	是	否	是	否	是
DNS (53)	UDP(17)	53	53	否	是	否	是	否	是
DNS (53)	TCP(6)	53	53	否	是	否	是	否	是
FTP(21)	TCP(6)	21	21	否	是	否	是	否	否
Telnet(23)	TCP(6)	23	23	否	是	否	是	否	否

SMTP(25)	TCP(6)	25	25	否	是	否	是	否	是
POP3(110)	TCP(6)	110	110	否	是	否	是	否	是
NEWS(NNTP)（网络新闻传输协议）	TCP(6)	119	119	否	是	否	是	否	否
RealAudio/ RealVideo (7070)	UDP(17)	7070	7070	是	是	是	是	否	否
PING	ICMP(1)	N/A	N/A	否	是	否	是	否	是
H.323(1720)	TCP(6)	1720	1720	是	是	否	是	否	否
T.120(1503)	TCP(6)	1503	1503	是	是	否	是	否	否
SSH(22)	TCP(6)	22	22	否	是	否	是	否	否
NTP /SNTP	UDP(17)	123	123	否	是	否	是	否	是
HTTP/HTTP 代理 (8080)	TCP(6)	8080	8080	否	是	否	否	否	否
HTTPS(443)	TCP(6)	443	443	否	是	否	是	不可用	不可用
ICQ (5190)	TCP(6)	5190	5190	是	是	不可用	不可用	不可用	不可用
MSN (1863)	TCP(6)	1863	1863	是	是	不可用	不可用	不可用	不可用
MSN (7001)	UDP(17)	7001	7001	是	是	不可用	不可用	不可用	不可用
MSN VEDIO (9000)	TCP(6)	9000	9000	否	是	不可用	不可用	不可用	不可用

入站：从 Internet 到 LAN

出站：从 LAN 到 Internet

是：允许

否：阻塞

N/A：不可用

包过滤 – 添加 TCP/UDP 过滤

规则名称帮助：用户自定义用来标识该条目的名称，或单击“帮助”，选择现有的预定义规则。名称最大长度不超过 32 个字符。

时间表：自定义的时间段。您必须为优先策略指定一个时间段。有关设置和详细信息，请参阅**时间表**部分。

源 IP 地址/目标 IP 地址：用来允许或阻塞发送/接收来自特定 IP 地址的流量的地址过滤。选择您想要允许或阻塞的 IP 地址的子网掩码；将 IP 地址和子网掩码设置为 **0.0.0.0**，以禁用地址过滤规则。

提示：要阻塞访问外部 IP 或来自外部 IP 的访问，输入要阻塞的 IP 地址作为主机 IP 地址并使用 255.255.255.255 作为主机子网掩码。

类型：应用使用的包协议类型，可以选择 TCP 或 UDP，也可两者都选。

协议号：插入端口号。

源端口：定义允许被远程/WAN 用来连接到应用程序的端口或端口范围。默认设置范围是：**0 ~ 65535**。建议高级用户配置此项。

目标端口：定义应用端口或端口范围。

入站 / 出站：选择**允许**或**阻塞**访问 Internet (**“Outbound”**)或来自 Internet 的访问(**“Inbound”**)。

完成所有更改后，单击**增加**按钮应用更改。

包过滤 – 添加原始 IP 包

转到**类型**下拉菜单，选择**使用协议号**。

规则名称帮助：用户自定义用来标识规则的名称。您也可以从**选择**下拉菜单中选择现有的预定义规则。

时间表：自定义的时间段。您必须为优先策略指定一个时间段。有关设置和详细信息，请参阅**时间表**部分。

源 IP 地址/目标 IP 地址：用来允许或阻塞发送/接收来自特定 IP 地址的流量的地址过滤。选择您想要允许或阻塞的 IP 地址的子网掩码；将 IP 地址和子网掩码设置为 **0.0.0.0，**以禁用地址过滤规则。

提示：要阻塞访问外部单独 IP 或来自外部单独 IP 的访问，输入要阻塞的 IP 地址作为主机 IP 地址并使用 255.255.255.255 作为主机子网掩码。

类型：应用使用的包协议类型，可以选择 **TCP** 或 **UDP，**也可两者都选。

协议号：输入端口号，如 GRE 47。

源端口：定义允许被远程/WAN 用来连接到应用程序的端口或端口范围。默认设置范围是：**0 ~ 65535。**建议高级用户配置此项。

目标端口：定义应用的端口或端口范围。

入站 / 出站：选择**允许**或**阻塞**访问 Internet（**出站**）或来自 Internet 的访问（**入站)**。

完成所有更改后，单击**增加**按钮应用更改。

实例：将防火墙配置为允许公开访问局域网中的 web 服务器

尽管防火墙的安全级别可以设置为高、中、低，但 HTTP（TCP 端口 80）的预定义端口过滤规则是一样的。

防火墙启用后，要设置局域网中的 web 服务器，必须对 HTTP 的端口过滤规则进行配置。

由下图表可以看出，启用防火墙并设置一个安全级别（高/中/低），入站的 HTTP 访问被禁止，意味着无法通过 HTTP 远程访问您的路由器。

注：入站是指通过 Internet 访问 LAN，而出站是指通过 LAN 访问 Internet。

配置包过滤：

1. 单击**包过滤**。您会看到预定义端口过滤规则界面（这里的安全级别为**低**），如下所示：

注：您可以单击编辑预定义规则但不能删除。本例说明如何添加过滤规则。

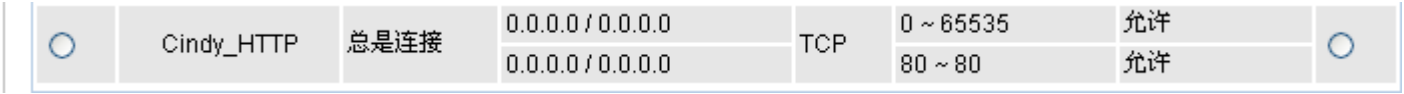
2. 如果想要删除过滤规则，选择想要删除的 HTTP 规则的删除单选按钮。然后单击**编辑/删除**按钮删除规则。

3. 要增加新的规则，输入**规则名称、时间表、源/目标 IP、类型、源/目标端口、入站**和**出站**。然后单击**增加**按钮。

实例：

应用：Cindy_HTTP
时间表：总是连接
源/目标 IP 地址：0.0.0.0（不想激活地址过滤器，而是使用端口过滤）
类型：TCP（请参阅表 1：预定义端口过滤）
源端口：0-65535（允许所有端口都连接到应用）
重定向端口：80-80（这是为 HTTP 定义的端口）
入站/出站：允许

1. HTTP 的新端口过滤规则如下：



2. 配置虚拟服务器（端口转发）设置，将端口 80 收到的 HTTP 请求转发给运行 web 服务器的 PC。

NOTE:

有关如何在虚拟服务器中配置 HTTP，请参阅**虚拟服务器**部分的**增加虚拟服务器**内容，以获取详细信息。

入侵检测

测系统 (IDS) 用来检测来自 Internet 的黑客攻击和入侵行为。如果已启用防火墙的 IDS 功能，将对所有入站数据包进行过滤，并根据是否被检测为可能的黑客攻击、入侵行为或其他路由器认为可疑的连接进行阻塞。

黑名单：如果路由器检测到可能的攻击，源 IP 或目标 IP 地址将被添加到**黑名单**中。在指定**阻塞持续时间内**，任何继续使用该 IP 地址的行为都会被阻塞。该功能默认设置为假（禁用）。如果不使用**黑名单**功能，有些攻击类型会被拒绝，如 *Land 攻击*和 *Echo/CharGen 扫描*。

入侵检测：如果已启用，IDS 将阻塞 Smurf 攻击行为。默认为假。

阻塞持续时间：

入侵防护持续时间：在此期间将阻塞所有 Smurf 攻击。默认值为 600 秒。

扫描攻击阻塞持续时间：在此期间将阻塞试图进行扫描攻击的主机。扫描攻击类型包括：*X'mas 扫描*、*IMAP SYN/FIN 扫描*和类型行为。默认值为 86400 秒。

拒绝访问阻塞持续时间：在此期间将阻塞试图进行**拒绝服务**攻击的主机。要阻塞的拒绝服务攻击包括：*Ascend Kill 和 WinNuke*。默认值为 1800 秒。

最大 TCP 连接次数：这是决定是否发生 *SYN Flood* 行为的阀值。默认值为 100 TCP SYN/秒。

最大 PING 包数：这是决定是否发生 *ICMP Echo Storm* 的阀值。默认值为 15 个 ICMP Echo 请求 (PING)/秒。

最多 ICMP 包数：这是决定是否发生 *ICMP flood* 的阀值。默认值为 100 个 ICMP 包/秒，除 ICMP Echo 请求 (PING) 外。

关于 *SYN Flood*、*ICMP Echo Storm 以及 ICMP flood*，IDS 只能在**事件日志**中警告用户，却不能保护网络不受攻击。

表 2：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	丢包	记录日志
Ascend Kill 攻击	Ascend Kill 数据	源 IP	DoS	是	是
WinNuke 攻击	TCP 端口 135,137~139, 标记：URG	源 IP	DoS	是	是
Smurf 攻击	ICMP 类型 8 目标 IP 是广播	目标 IP	入侵保护	是	是
Land 攻击	源IP=目标IP			是	是
Echo/CharGen 扫描	UDP Echo Port and CharGen Port			是	是
Echo 扫描	UDP 目标端口=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 目标端口： IMAP(143) 源端口：0 或 65535	源 IP	扫描	是	是
SYN/FIN/RST/ACK 扫描	TCP, 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 没有当前会话 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 洪泛	最大 TCP 开始握手数（默认是 100 次/秒）				是
ICMP 洪泛	最大 ICMP 数（默认 100 个/秒）				是
ICMP Echo 风暴	最大 PING 包数 （默认 15 个/秒）				是

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

URL 过滤

URL（统一资源定位 – 例如 http://www.abcde.com 或 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。

启用/禁用：启用或禁用 URL 过滤功能。

阻塞模式：选择用来检查 URL 过滤规则的模式列表。默认设置为**总是连接**。

禁用：该阻塞模式下将不执行阻塞操作。

总是连接：功能被启用。URL 过滤规则将会进行全天监控与检测。

时间槽 1~时间槽 16：自定义的时间段。您可以指定检查 URL 过滤规则的时间段，比如工作时间。详细信息，请参阅**时间表**部分。

关键字过滤：允许根据 URL 中的指定关键字进行阻塞，而无须指定完整的 URL（如，要阻塞所有文件名为“advertisement.gif”的图像）。功能开启后，检查指定关键字，查看是否出现在访问地址中，以决定是否阻塞连接。请注意：URL 过滤只能阻塞 80 端口的 HTTP 连接。

*例如：*URL http://www.abc.com/abcde.html 中出现关键字 abcde，所以会被阻止。

域名过滤：检查所访问的整个 URL（而不是 IP 地址）是否在阻止或允许的域名列表中。如果匹配，URL 请求会被转发（信任的）或丢弃（禁止的）。检查步骤如下：

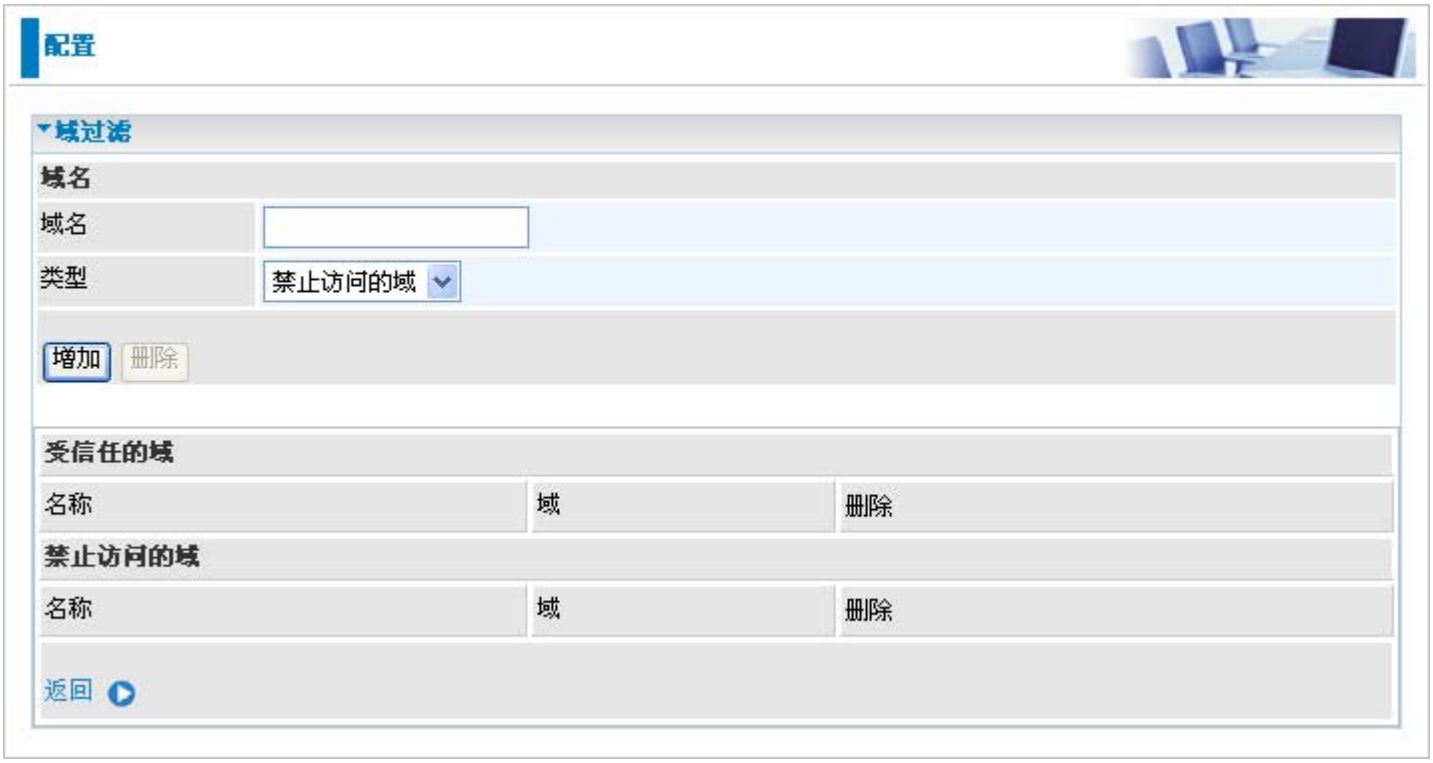
检查 URL 中的域名，决定它否是可信任的。如果是，将连接请求发送到远程 web 服务器。

2. 如果不是信任的，而是禁止的。那么连接请求被丢弃。

3. 如果以上两种情况都不是，将请求发到远程 web 服务器。

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

在以下例子中，URL 请求 www.abc.com 被发送到远程 web 服务器，因为它在信任列表中；而 URL 请求 www.google 或 www.google.com 却被丢弃，因为它在禁止列表中。



例如：想要阻止所有 WEB 流量（信任域名中列出的除外），这将阻止任何人访问其他站点。在*域名过滤*中选择这两种功能后，将对任何人进行阻止。所有人都知道这个功能，*域名过滤*，**只是**阻止除信任域名之外的所有 WEB 流量，**而不是 IP 地址**。如果是这种情况，**通过 IP 地址阻塞网上冲浪**这一功能将会起到帮助作用。这样就可以阻止任何人访问其他站点了。

限制 URL 功能：这个功能可以加强对 URL 规则的限制。

- **阻塞 Java Applet：**该功能可以阻塞包含 Java Applet 的 Web 内容。它将阻止有人通过标准 HTTP 协议破坏您的系统。
- **通过 IP 地址阻塞网上冲浪：**阻止有人使用 IP 地址作为 URL 跳过域名过滤。只有启用域名过滤后，该功能被激活。

阻止IM / P2P通信

IM（即时通讯简称）要求使用客户端程序，使用户通过 Internet 与其他 IM 用户进行实时文本信息通信。P2P 应用（对等网络）就是一组用户通过 Internet 与其他组的用户共享文件。两种应用都会使通信更加快速方便，同时您的网络也越来越不安全。Billion 的 IM 和 P2P 阻塞功能可以帮助用户限制局域网 PC 通过 Internet 访问常用的 IM、Yahoo、MSN、BitTorrent、eDonkey 应用。

IM 阻塞：默认设置为**禁用**。

禁用：不触发 IM 阻塞。不执行任何操作。

总是连接：启用操作。

时间槽 1 ~ 时间槽 16：这是自定义的时间段。您可以指定要触发阻塞的时间段，如在工作时间。关于安装和详细信息，请参阅**时间表**部分。

Yahoo/MSN Messenger：选中以阻塞其中一个或两者都阻塞。保证已启用 *Instant Message 阻塞*。

端对端阻塞：默认设置为**禁用**。

禁用：不触发 IM 阻塞。不执行任何操作。

总是连接：启用操作。

时间槽 1 ~ 时间槽 16：这是自定义的时间段。您可以指定要触发阻塞的时间段，如在工作时间。关于安装和详细信息，请参阅**时间表**部分。

BitTorrent / eDonkey：选中以阻塞其中一个或两者都阻塞。保证已启用*端对端阻塞*。

防火墙日志

防火墙日志显示防火墙设置所出现的任何异常操作。

选中**启用**以激活事件日志。

启用后，可在**状态-事件日志**中查看日志信息。

VPN – 虚拟专用网

（仅适用于 BiPAC 7402X、7402GX、7404VGOX、7404VNOX、6404VNOX）

虚拟专用网是一种通过 Internet 与机构网络之间建立安全通信隧道的方法。此款路由器支持三种类型 VPN（虚拟专用网络）：**PPTP、IPSec** 和 **L2TP。**

PPTP（点对点通道协议）

PPTP 连接 - LAN 到 LAN

支持两种类型的 PPTP VPN；**远程访问**和 **LAN 到 LAN**（详细信息，请参阅下面的内容）。从**类型**下拉菜单中选择LAN 到 LAN。

名称：指定的连接的名称（如连接到办公室）。

连接类型：远程访问或 LAN 到 LAN。

类型：如果想要路由器作为客户端（连接到远程 VPN 服务器，如您办公室的服务器），选中**拨出**，选中**拨入**，路由器作为 VPN 服务端。

将路由器配置为客户端，输入您想要连接到的远程**服务器 IP 地址（或域名）**。

将路由器配置为服务端，输入**分配给拨入用户的私有 IP 地址**。

IP 地址：输入 IP 地址。

远端网络 IP：输入远端网络的 IP 地址。

子网掩码：根据远端网络的 IP 设置，输入远端网络的子网掩码。

用户名：如果您是拨出用户（客户端），输入主机提供的用户名。如果您是拨入用户（服务端），输入您自己的用户名。

密码：如果您是拨出用户（客户端），输入主机提供的密码。如果您是拨入用户（服务端），输入您自己的密码。

认证类型：默认为**自动**，由路由器决定使用的认证类型。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。

数据加密：可以对通过 VPN 发送的数据进行 MPPE 算法加密。默认为**自动**，建立连接时进行加密协商。也可以手动**启用**或**禁用**加密。

密钥长度：使用 MPPE 算法加密数据，密钥长度为 40 位或 128 位。默认为**自动**，建立连接时进行密钥长度协商。128 位密钥比 40 位密钥的加密功能强大。

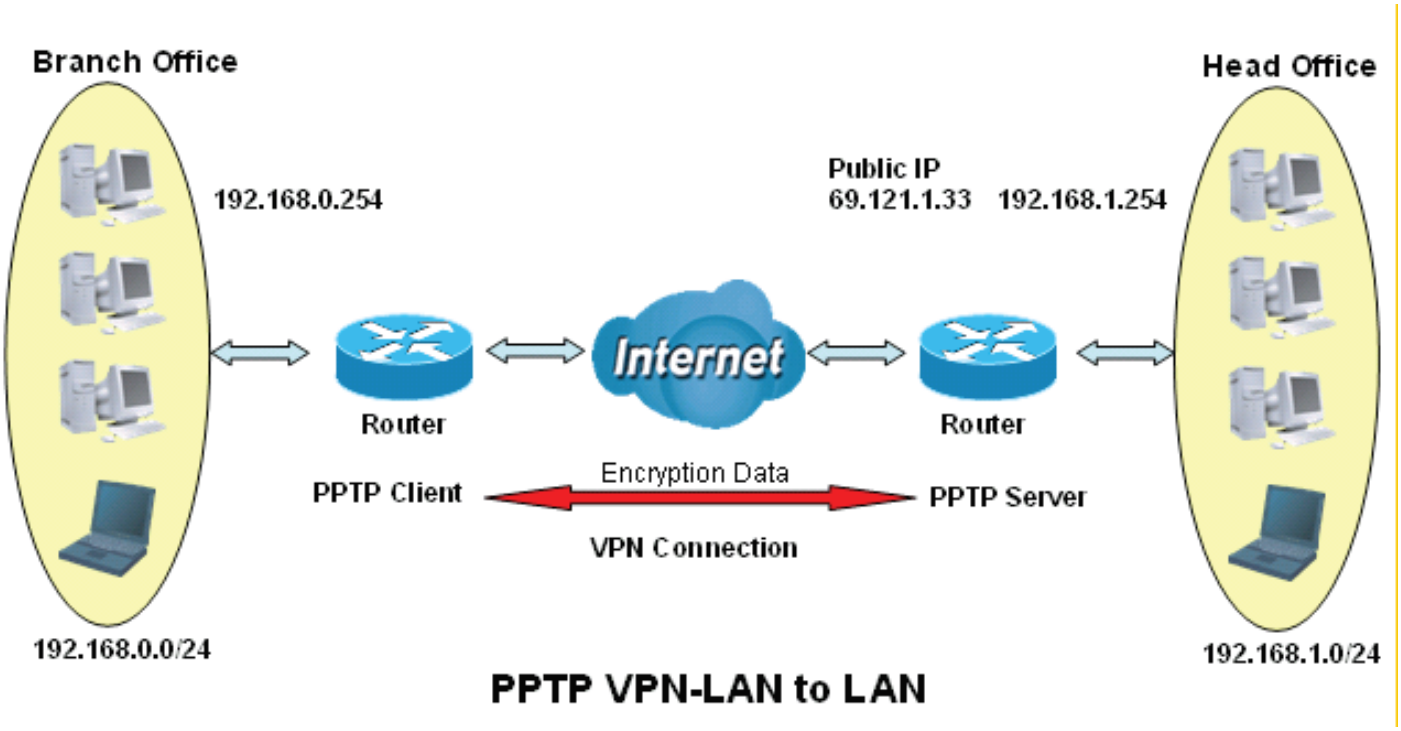
模式：您可以选择密钥状态是 **Stateful 或 Stateless。如果选择** Stateful，密钥在发送了 256 个包后改变。如果选择 Stateless，则每次有一个包发送时，密钥都会改变。

启用为默认路由：常用于**拨出**连接，所有数据包通过 VPN 隧道路由到 Internet，启用该功能会降低 Internet 性能。

单击**编辑/删除**按钮，保存更改。

实例：配置*LAN-to-LAN PPTP VPN* 连接

在分部建立连接到总部的 PPTP VPN 隧道，将 Internet 上的两个专用网连接起来。因此要在总部和分部分别安装路由器。



注意

LAN 到 LAN 应用要求总部和分部的 LAN 必须在不同子网中。

配置总部的 PPTP VPN

将 IP 地址 192.168.1.200 分配给分部路由器。确保该 IP 未被总部局域网使用。

功能		描述
名称	HeadOffice	指定的 PPTP 连接名称
连接类型	LAN 到 LAN	从连接类型下拉菜单中选择 LAN 到 LAN
类型	拨入	从类型下拉菜单中选择拨入
IP 地址	192.168.1.200	指定给分部网络的 IP 地址
远端网络 IP	192.168.0.0	分部网络
子网掩码	255.255.255.0	
用户名	用户名	用来认证分部网络的指定用户名和密码
密码	123456	
认证类型	Chap（自动）	大多情况下，保持默认值，默认值由 PPTP 服务端与客户端自动决定。若要更改设置，详细信息请参阅手册。
数据加密	自动	
密钥长度	自动	
模式	带状态的	

配置分部的 PPTP VPN

位于总部的路由器的**公共 IP** 地址是：69.1.121.33。注册 DDNS（请参阅手册的 DDNS 部分）后，您可以使用域名代替 IP 地址连接到路由器。

功能		描述
名称	BranchOffice	指定的 PPTP 连接名称
连接类型	LAN 到 LAN	从连接类型下拉菜单中选择 LAN 到 LAN
类型	拨出	从类型下拉菜单中选择拨入
IP 地址（或域名）	69.121.1.33	指定给分部网络的 IP 地址
远端网络 IP	192.168.1.0	总部网络
子网掩码	255.255.255.0	
用户名	用户名	用来认证分部网络的指定用户名和密码
密码	123456	
认证类型	Chap（自动）	大多情况下，保持默认值，默认值由 PPTP 服务端与客户端自动决定。若要更改设置，详细信息请参阅手册。
数据加密	自动	
密钥长度	自动	
模式	带状态的	

PPTP 连接 – 远程访问

名称：指定的连接的名称（如连接到办公室）。
连接类型：远程访问或 LAN 到 LAN。

类型：如果想要路由器作为客户端（连接到远程 VPN 服务器，如您办公室的服务器），选中**拨出**，选中**拨入**，路由器作为 VPN 服务端。

将路由器配置为客户端，输入您想要连接到的远程**服务器 IP 地址（或域名）**。

将路由器配置为服务端，输入**分配给拨入用户的私有 IP 地址**。

IP 地址：输入 IP 地址。

用户名：如果您是拨出用户（客户端），输入主机提供的用户名。如果您是拨入用户（服务端），输入您自己的用户名。

密码：如果您是拨出用户（客户端），输入主机提供的密码。如果您是拨入用户（服务端），输入您自己的密码。

认证类型：默认为**自动**，由路由器决定使用的认证类型。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。

数据加密：可以对通过 VPN 发送的数据进行 MPPE 算法加密。默认为**自动**，建立连接时进行加密协商。也可以手动**启用**或**禁用**加密。

密钥长度：使用 MPPE 算法加密数据，密钥长度为 40 位或 128 位。默认为**自动**，建立连接时进行密钥长度协商。128 位密钥比 40 位密钥的加密功能强大。

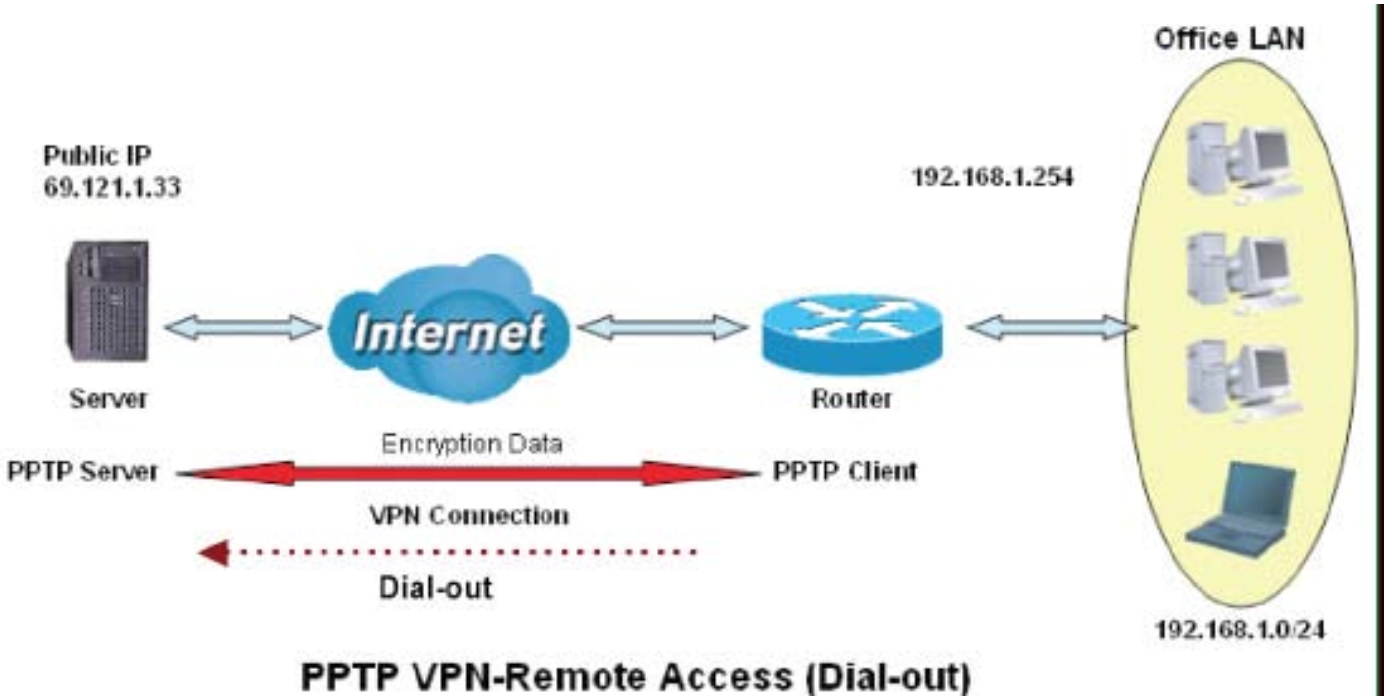
模式：您可以选择密钥状态是 **Stateful 或 Stateless。如果选择** Stateful，密钥在发送了 256 个包后改变。如果选择 Stateless，则每次有一个包发送时，密钥都会改变。

启用为默认路由：常用于**拨出**连接，所有数据包通过 VPN 隧道路由到 Internet，启用该功能会降低 Internet 性能。

单击**编辑/删除**按钮，保存更改。

实例：配置远程访问 PPTP VPN 拨出连接

在公司办公室与放置在另一地方的文件服务器之间建立 PPTP VPN 连接。
路由器安装在办公室内，连接到多台 PC 或服务器。



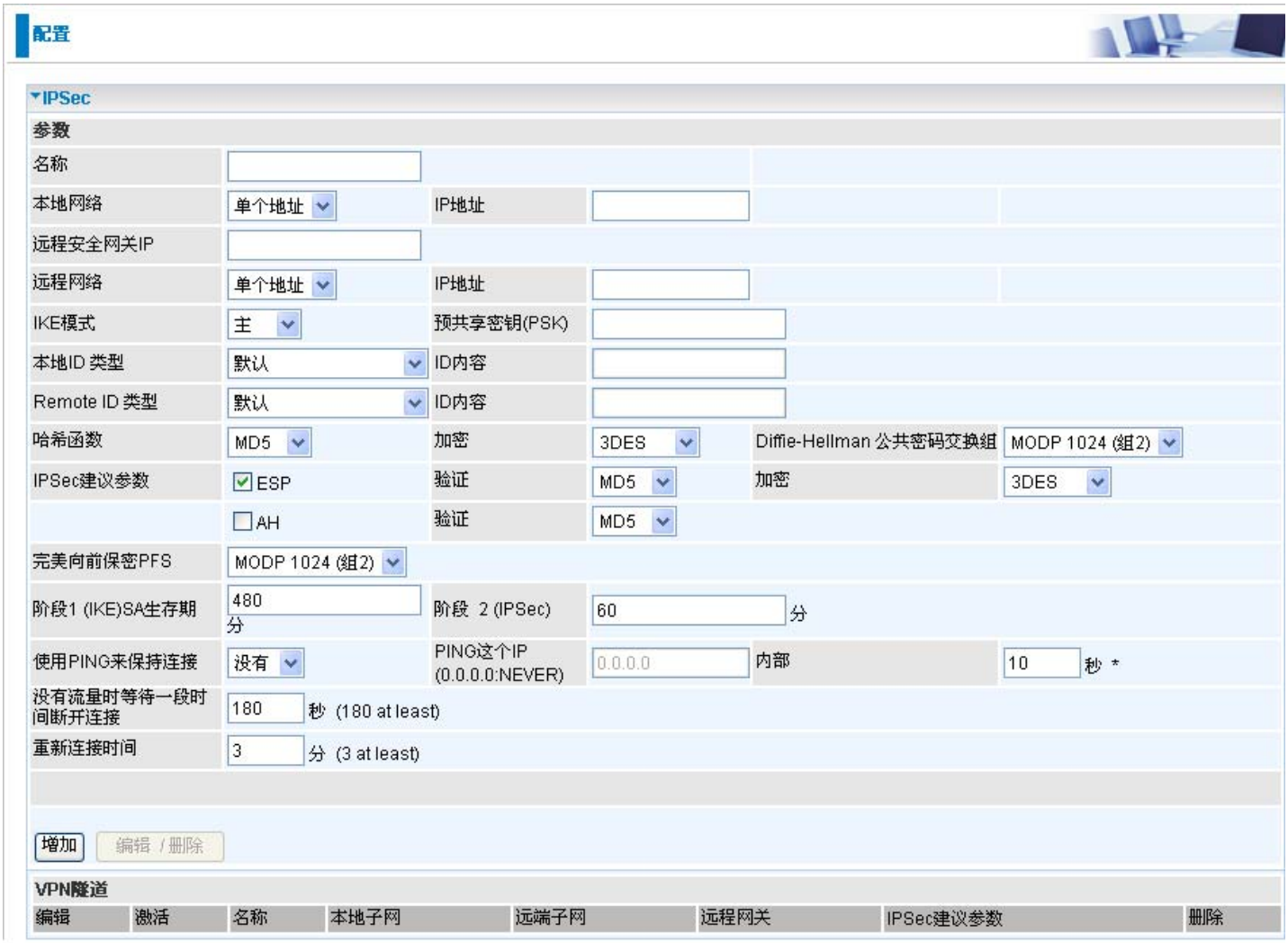
PPTP VPN-Remote Access (Dial-out)

配置办公室的 PPTP VPN

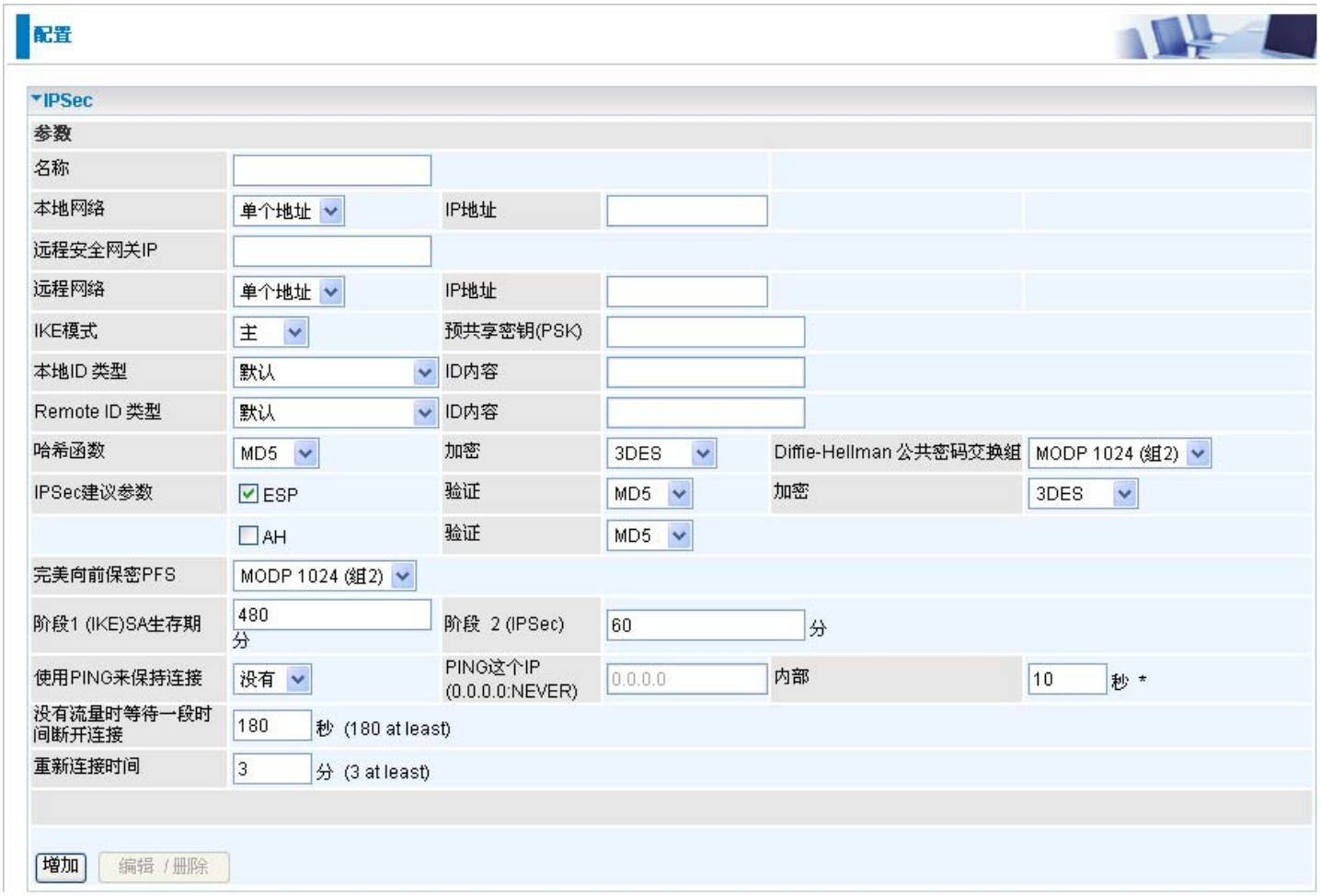
单击配置> VPN > PPTP。从下拉菜单中选择**远程访问**。您可以输入 IP 地址（这里用 69.121.1.33）或主机名连接到服务器。

功能		描述
名称	VPN_PPTP	指定的 PPTP 连接名称
连接类型	远程访问	从连接类型下拉菜单中选择 LAN 到 LAN
类型	拨出	从类型下拉菜单中选择拨出
IP 地址（或域名）	69.121.1.33	呼叫的服务器 IP
用户名	用户名	指定用户名和密码
密码	123456	
认证类型	Chap（自动）	大多情况下，保持默认值，默认值由 PPTP 服务端与客户端自动决定。若要更改设置，详细信息请参阅手册。
数据加密	自动	
密钥长度	自动	
模式	带状态的	

IPSec（IP 安全协议）



IPSec VPN 连接



名称：指定的连接名称（如连接到办公室）。

本地网络：设置本地网络的 IP 地址、子网或地址范围。

单地址：本地主机的 IP 地址。

子网：局域网的子网。如 IP: 192.168.1.0 连同子网 255.255.255.0 表示 C 类子网，起始 IP 地址自 192.168.1.1 开始（如：从 192.168.1.1 到 192.168.1.254）。

IP 范围：局域网的 IP 地址范围。如：起始 IP: 192.168.1.1，结束 IP: 192.168.1.10。

IP 地址：输入 IP 地址。

远程安全网关地址（或域名）：用来连接和建立 VPN 隧道的远程 VPN 设备的 IP 地址或主机名。

远程网络：设置远程网络的 IP 地址、子网或地址范围。

IKE（Internet 密钥交换）模式：选择 IKE 模式为 Main 模式或 Aggressive 模式。IKE 提供安全的密钥生成和管理。

预共享密钥：用于 Internet 密钥交换协议 (IKE) 的字符串，长度为 4~128 个字符。两端必须使用相同的密钥。IKE 用来为需要提供密钥的服务（如 IPSec）建立共享安全策略和认证密钥。在 IPSec 流量通过之前，路由器都必须验证对端身份。可通过手动输入路由器或主机的预共享密钥完成。

本地 ID：

ID 内容：输入 ID 信息，如域名 www.ipsectest.com.

远程 ID：
标识符：输入 ID 信息，如 www.ipsectest.com。

哈希函数：它是将信息长度转换为唯一位集合的信息摘要算法。常被 MD5（信息摘要）和 SHA-1（安全散列算法）使用。SHA1 算法速度较慢，但比 MD5 更能抵御力迫法攻击。

MD5：单向哈希算法，生成一个 128 位散列值。

SHA1：单向哈希算法，生成一个 160 位散列值。

加密：从下拉菜单中选择加密方法。可供选择的选项有：**DES**、**3DES**、**AES (128, 192 和 256)**。3DES 和 AES 算法更高级，但会增加延迟。

DES：数据加密标准，密钥长度为 56 位。

3DES：三重数据加密标准，密钥长度为 168(56*3) 位。

AES：高级加密标准，密钥长度为 128、192 和 256 位。

Diffie-Hellman 组：公钥加密协议，使通信双方可以在不安全通信隧道上建立共享密钥（如，通过 Internet）。共有三种模式：MODP 768 位, MODP 1024 位和 MODP 1536 位。MODP 代表模块指数组。

IPSec 提议：选择 IPSec 安全模式。检验认证信息的方式有两种：AH（认证头）和 ESP（封装安全负载）。使用 ESP 协议加密数据和认证，更加安全。使用 AH 协议，只对数据进行认证但不加密。

认证：认证能够实现数据报文的完整性，并确保在传输过程中，报文不被篡改。有三个选项可选：信息摘要算法 (**MD5**)、安全散列算法 (**SHA1**) 或**无**。SHA1 算法速度比较慢，但抵御力迫法攻击的能力比 MD5 强。

MD：单向哈希算法，生成一个 128 位散列值。

SHA1：单向哈希算法，生成一个 160 位散列值。

加密：从下拉菜单中选择加密方法。可以选择的选项有：**DES**、**3DES**、**AES（128, 192 和 256)**）以及**没有。没有**是指隧道没有加密。3DES 和 AES 算法更加高级，但会增加延迟。

DES：数据加密标准，密钥长度为 56 位。

3DES：三重数据加密标准，密钥长度为 168 (56*3) 位。

AES：高级加密标准，密钥长度为 128、192 或 256 位。

完美向前保密：选择是否启用 PFS，在 VPN 协商第二阶段使用 Diffie-Hellman 公开密钥加密法来更改加密密钥。该功能提供的安全性更好，但会延长 VPN 协调时间。Diffie-Hellman 是一种公钥加密法，通信双方在不安全通信隧道上建立共享密钥（如，通过 Internet）。共有三种模式：MODP 768 位, MODP 1024 位和 MODP 1536 位。MODP 代表模块指数组。

安全关联 (SA) 生存期：在交换新的加密密钥和认证密钥之前，安全关联 (SA) 保持活动的分钟数。IKE 和 IPSec 两者都使用 SA。IKE 代表 IPSec 协商建立 SA，IKE 使用 IKE SA。

第 1 阶段 (IKE)：提出建立新 VPN 隧道的初始连接请求。时间范围为 5 到 15,000 分钟，默认为 480 分钟。

第 2 阶段 (IPSec)：协商建立安全认证。时间范围为 5 到 15,000 分钟，默认为 60 分钟。

短暂的 SA 可以通过强迫双方更新密钥来增强安全性。当 VPN 隧道重新协商时，通过隧道进行的访问临时被断开。

短暂的 SA 可以通过强迫双方更新密钥来增强安全性。当 VPN 隧道重新协商时，通过隧道进行的访问临时被断开。

使用 PING 来保持连接

没有：默认设置为**没有**。这种模式下不检测远程 IPSec 对端是否丢失。实行无流量后断开时间策略，远程 IPSec 在超时设定时间后断开。

PING：这种模式下，通过 PING 指定 IP 地址检测远程 IPSec 对端是否丢失。
DPD：死亡对端探测 (DPD) 是一种保活机制，当路由器和远程 IPSec 对端的连接断开时，检测路由器的活跃状态。

PING IP：可以 Ping 远程 PC 的指定 IP 地址，连接失败时会发出警报。收到警报信息后，路由器断开当前隧道连接。需要重新建立连接。默认设置为 0.0.0.0，默认设置将禁用此功能。

间隔：设置 ***Ping IP*** 的时间间隔，以监测连接状态。默认时间间隔为 10 秒。时间间隔可以设置为 0 到 3600 秒，设置为 0 将禁用此功能。

Ping IP	**间隔（秒）**	**Ping IP 操作**
0.0.0.0	0	否
0.0.0.0	2000	否
xxx.xxx.xxx.xxx （有效的 IP 地址）	0	否
xxx.xxx.xxx.xxx （有效的 IP 地址）	2000	是，每隔 2000 秒激活一次。

没有流量时等待一段时间断开连接：对**无反应**计时。当没有流量的时间超过设定的**断开**时间，路由器将自动中断隧道连接，然后重新建立连接（根据**重新连接时间**设置）。**180 秒**是最短时间间隔。

重新连接时间：对**没有流量**计时后，再重新连接的时间间隔。时间间隔至少为 **3 分钟**。

选择**应用**按钮更新设置。

实例：配置 IPSec LAN 到 LAN VPN 连接

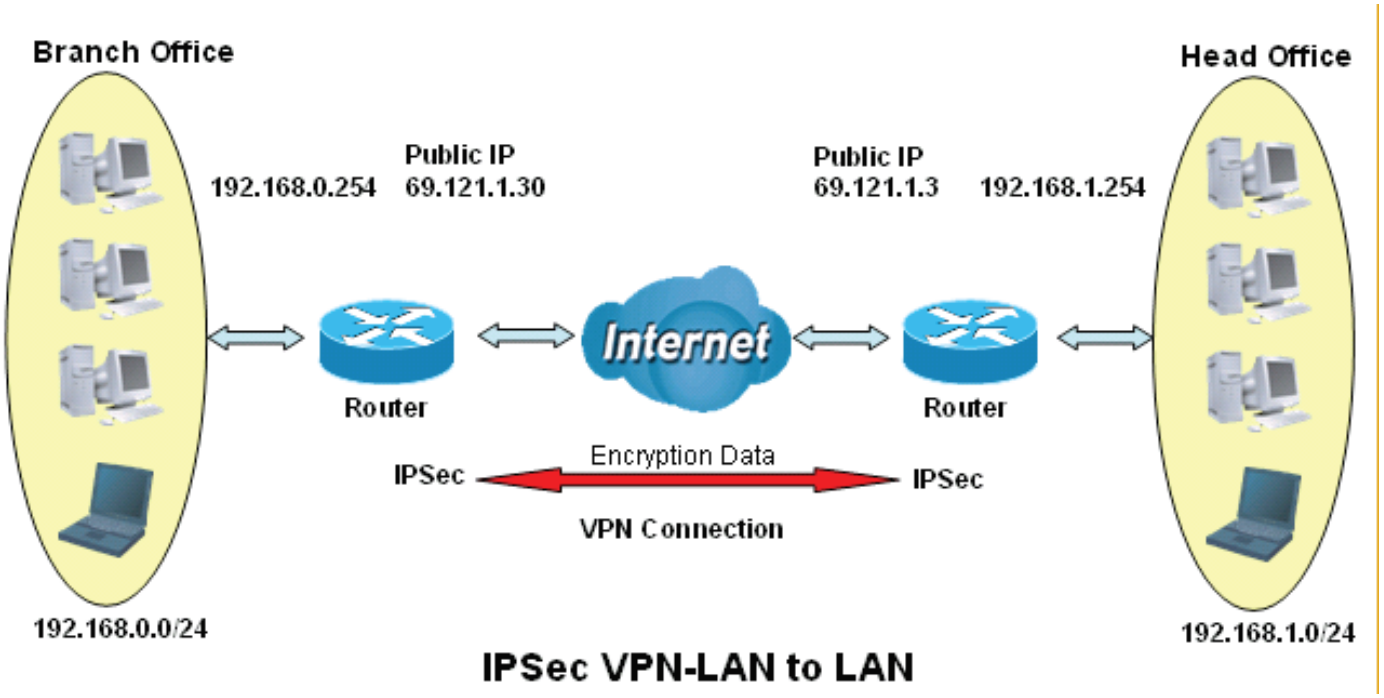


表 3：网络配置和安全计划

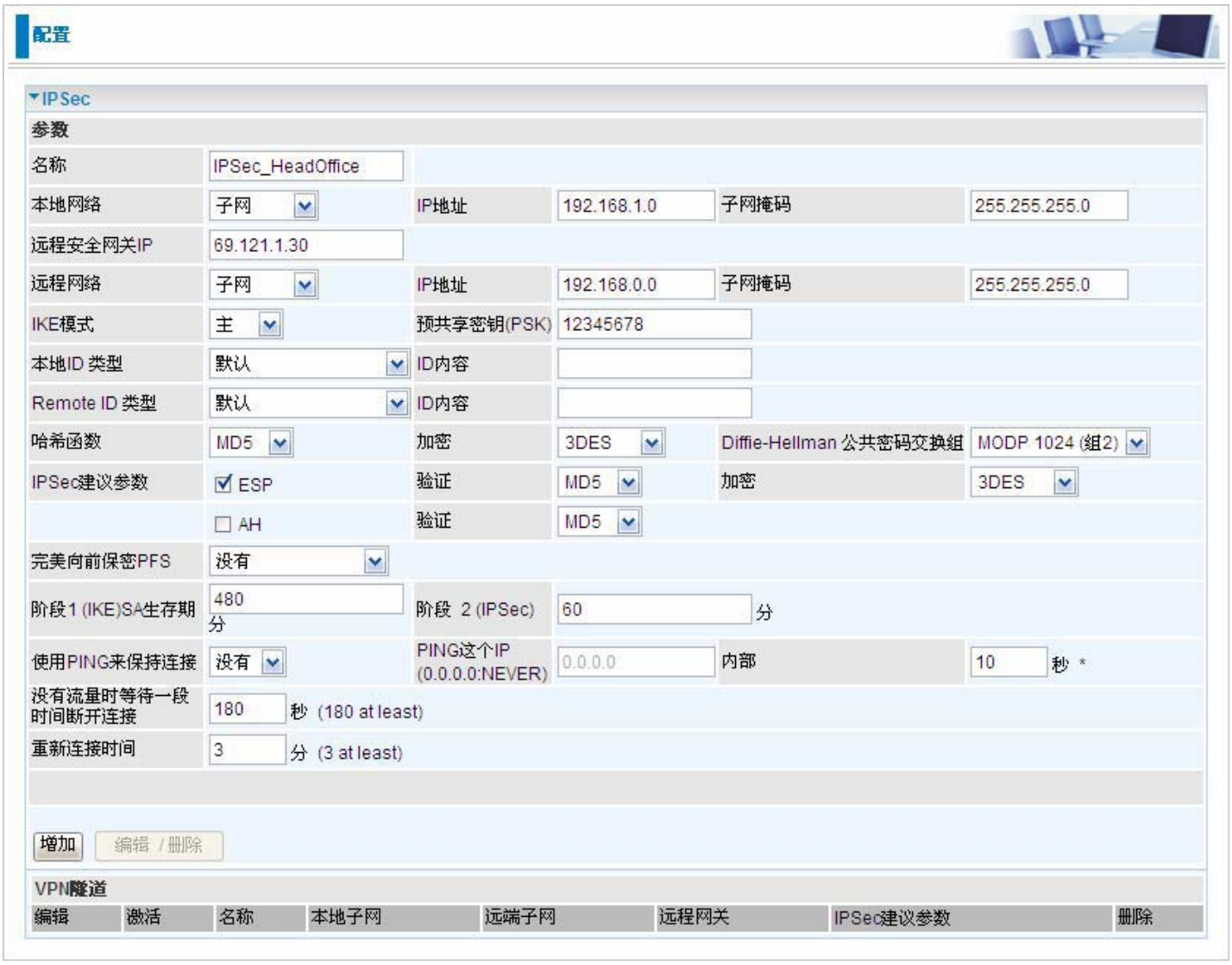
	Branch Office	**Head Office**
局域网 ID	192.168.0.0/24	192.168.1.0/24
本地路由器 IP	69.1.121.30	69.1.121.3
远程网络 ID	192.168.1.0/24	192.168.0.0/24
远程路由器 IP	69.1.121.3	69.1.121.30
IKE 预共享密钥	12345678	12345678
VPN 连接类型	隧道模式	隧道模式
安全算法	ESP：采用 MD5 认证的 AES 加密	ESP：采用 MD5 认证的 AES 加密

注意

LAN 到 LAN 应用要求两个办公室的局域网**必须在不同子网中**。

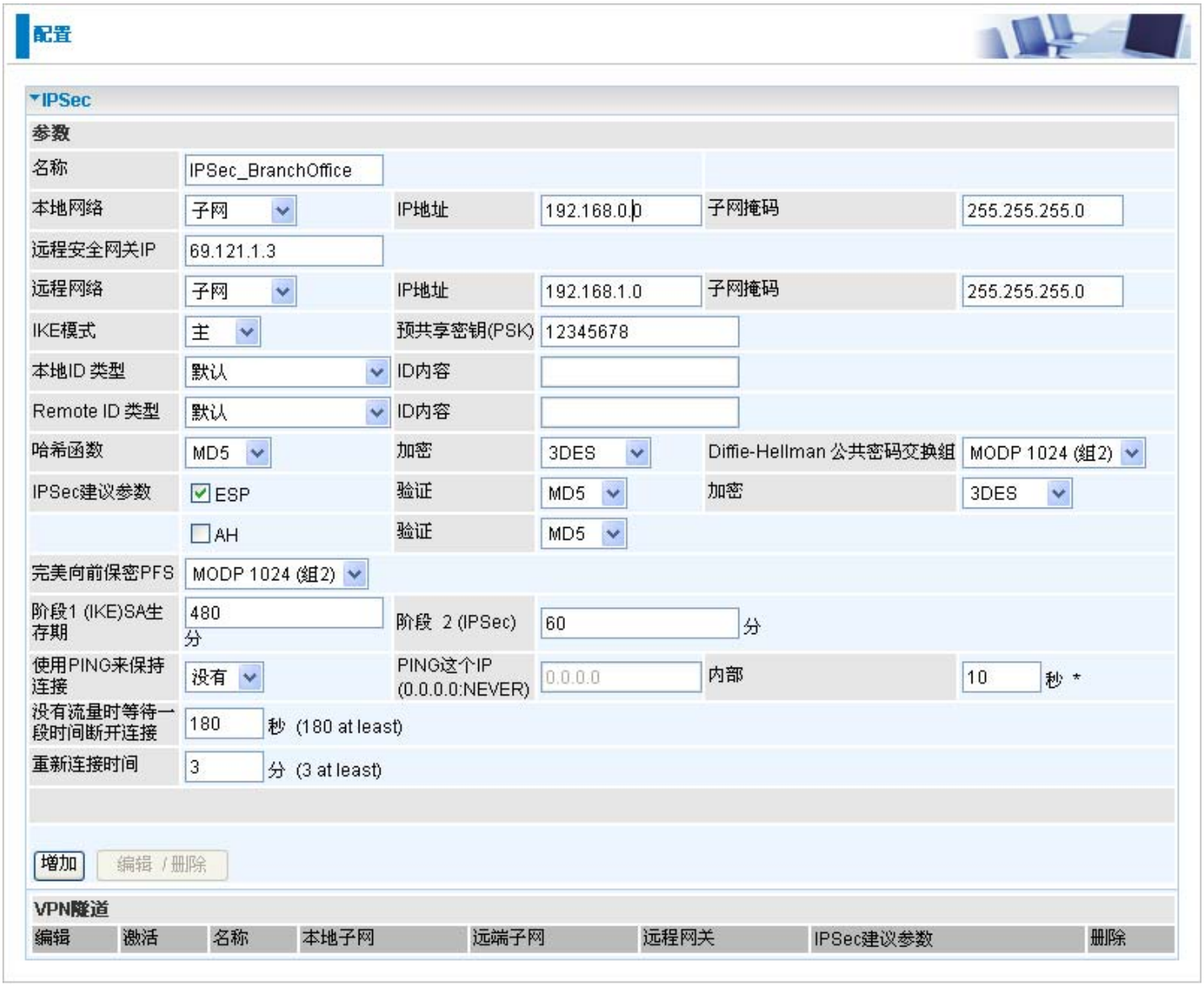
总部和分部必须设置相同的**预共享密钥、VPN 连接类型和安全算法**。

配置总部的 IPSec VPN



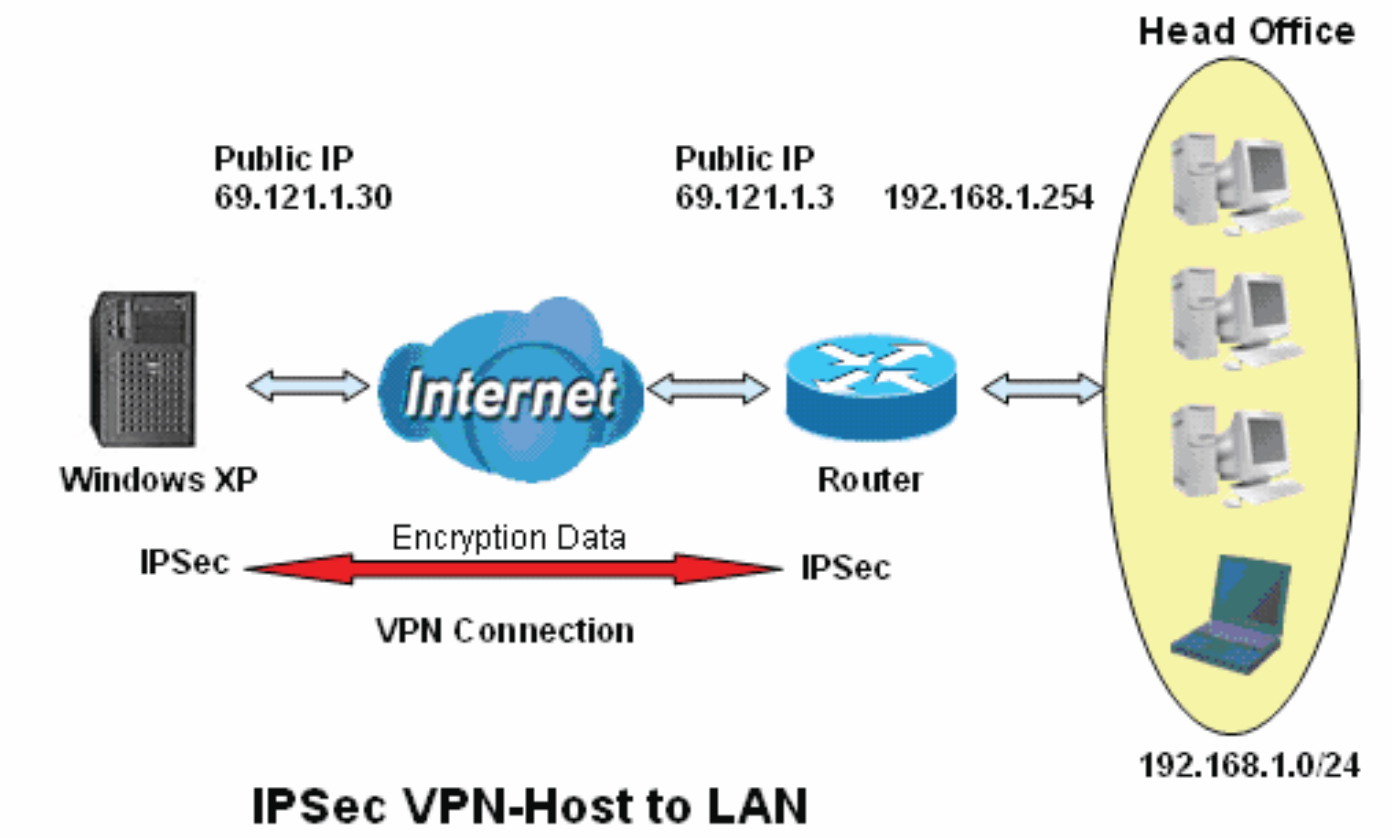
功能		描述
名称	IPSec_HeadOffice	指定的 IPSec 连接名称
局域网	子网	从局域网下拉菜单中选择子网。
IP 地址	192.168.1.0	总部网络
子网掩码	255.255.255.0	
远程安全网关 IP（或主机名）	69.121.1.30	分部路由器的 IP 地址（WAN 端）
远程网络	子网	从远程网络下拉菜单中选择子网
IP 地址	192.168.0.0	分部网络
子网掩码	255.255.255.0	
预共享密钥	12345678	安全计划
认证	MD5	
加密	3DES	
完美向前保密	没有	

配置分部的 IPSec VPN

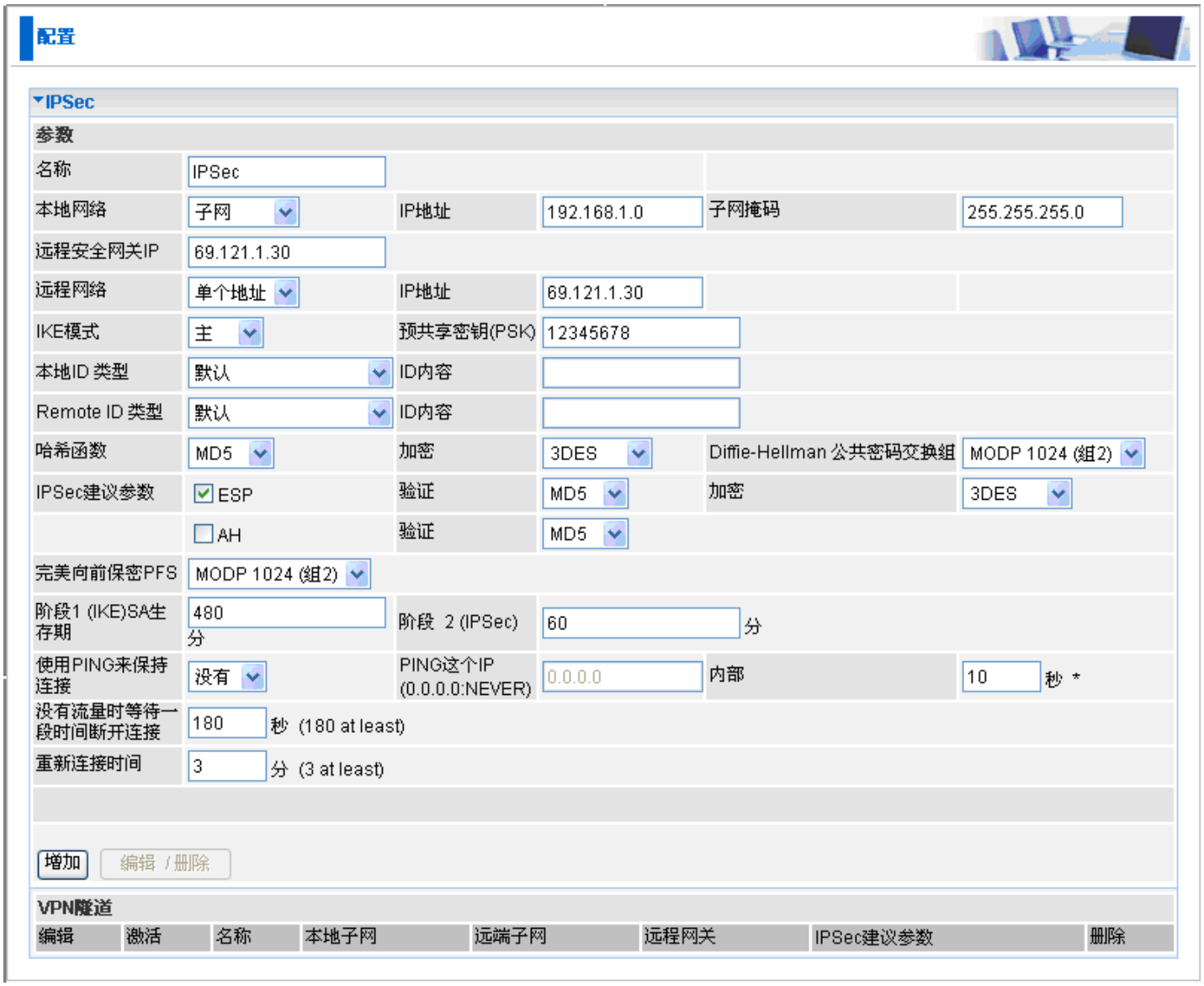


功能		描述
名称	IPSec_BranchOffice	指定的 IPSec 连接名称
局域网	子网	从局域网下拉菜单中选择子网。
IP 地址	192.168.0.0	分部网络
子网掩码	255.255.255.0	
远程安全网关 IP（或主机名）	69.121.1.3	总部路由器的 IP 地址（WAN 端）
远程网络	子网	从远程网络下拉菜单中选择子网
IP 地址	192.168.1.0	总部网络
子网掩码	255.255.255.0	
预共享密钥	12345678	安全计划
认证	MD5	
加密	3DES	
完美向前保密	没有	

实例：配置 **IPSec** 主机到 **LAN VPN** 连接



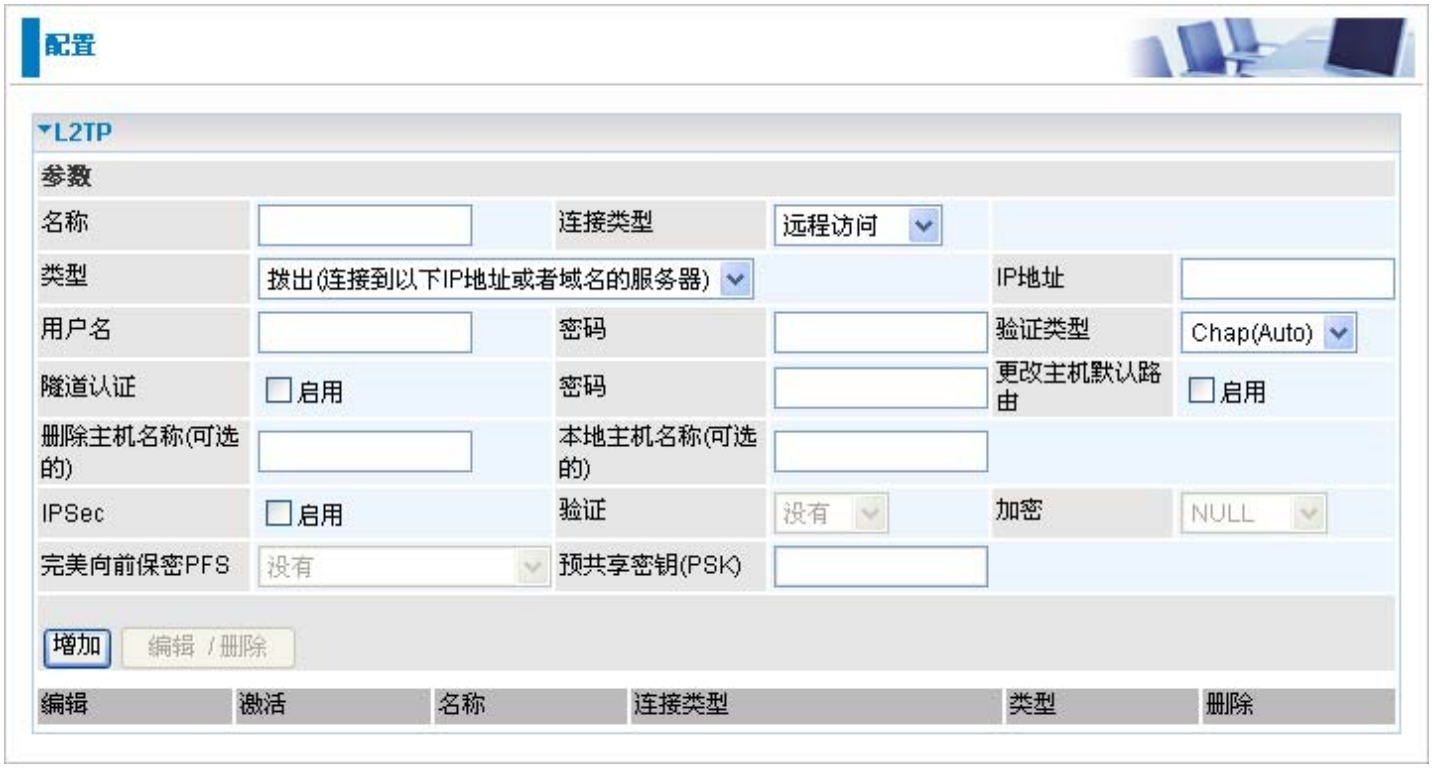
配置办公室的 IPSec VPN



功能		描述
名称	IPSec	指定的 IPSec 连接名称
局域网	子网	从局域网下拉菜单中选择子网。
IP 地址	192.168.1.0	总部网络
子网掩码	255.255.255.0	
远程安全网关 IP（或主机名）	69.121.1.30	分部路由器的 IP 地址（WAN 端）
远程网络	单地址	从远程网络下拉菜单中选择但地址
IP 地址	69.121.1.30	远地人工作人员的 IP 地址
预共享密钥	12345678	安全计划
认证	MD5	
加密	3DES	
完美向前保密	没有	

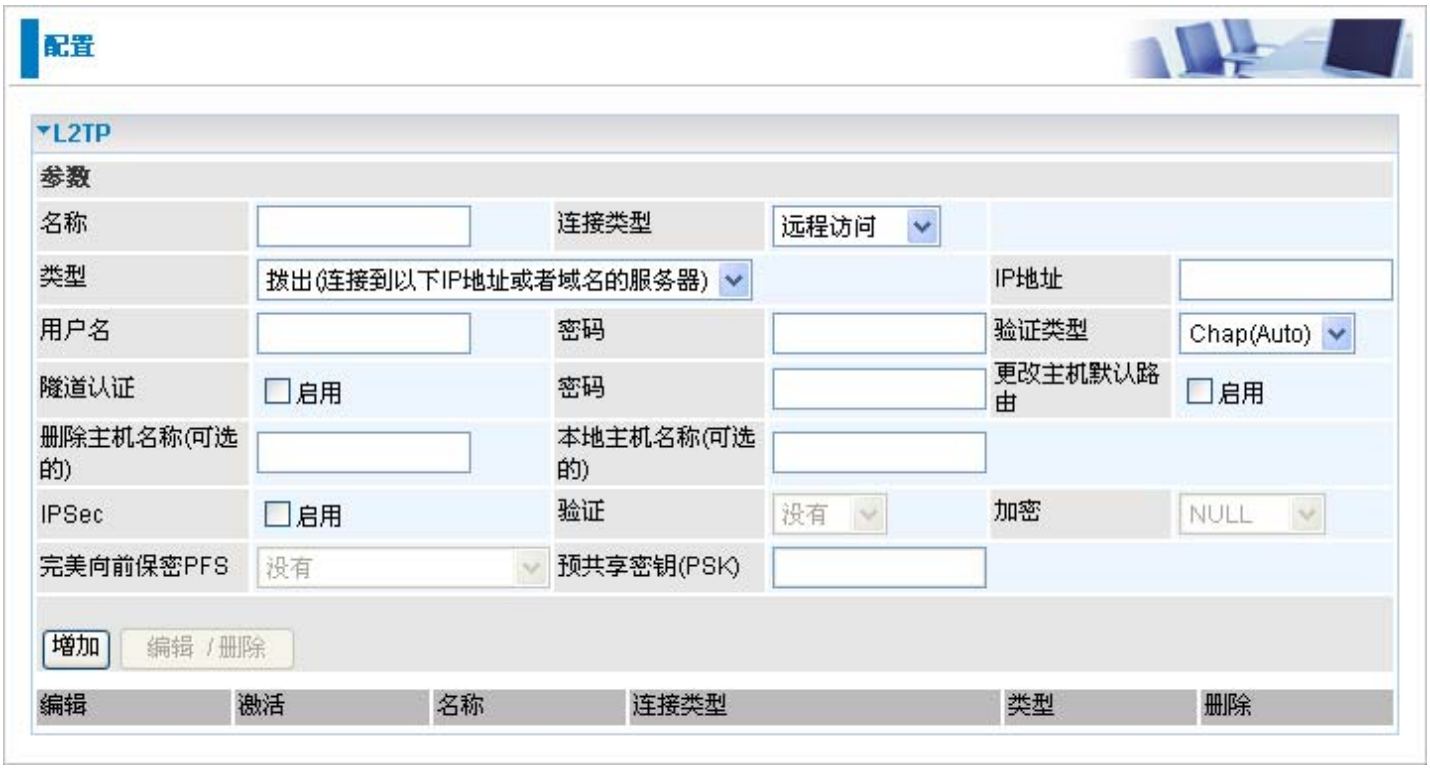
L2TP（第二层隧道协议）

L2TP VPN 支持：远程访问和 LAN 到 LAN（详细信息，请参阅以下内容）。在空白处填写信息，然后单击**增加**创建新的 VPN 连接账号。



L2TP 连接 – 远程访问

连接类型：远程访问或 LAN 到 LAN



名称：指定的连接名称（如连接到办公室）。

连接类型：远程访问或 LAN 到 LAN。

类型：如果想要路由器作为客户端（连接到远程 VPN 服务器，如办公室里的服务器），选中**拨出**；选中**拨入**，路由器作为 VPN 服务端。

将路由器配置为客户端时，输入您想要连接到的远程服务器 IP 地址（或域名）。

将路由器配置为服务端时，输入分配给拨入用户的私有 IP 地址。

IP 地址：输入 IP 地址。

用户名：如果您是**拨出**用户（客户端），输入主机提供的用户名。如果您是**拨入**用户（服务端），输入您自己设置的用户名。

密码：如果您是**拨出**用户（客户端），输入主机提供的密码。如果您是**拨入**用户（服务端），输入您自己的设置的密码。

认证类型：默认为**自动**，由路由器决定使用的认证类型。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。

隧道认证：使路由器对 L2TP 远程和 L2TP 主机进行认证。仅当 L2TP 远程支持该功能时有效。

密钥：安全口令长度必须为 16 个字符，包括字符和数字。

启用为默认路由：常用于拨出连接，所有数据包通过 VPN 隧道路由到 Internet，启用该功能会降低 Internet 性能。

远程主机名（可选）：输入远程 VPN 设备的主机名。主机名是远程 VPN 设备的隧道标识符，与提供的远程主机名进行匹配。如果相匹配，则建立起隧道连接，如果不匹配，则断开连接。

警告：仅针对当路由器作为 VPN 服务端时。只有高级用户可以使用这个选项。

本地主机名（可选）：输入用来连接/建立 VPN 隧道的本地 VPN 设备的主机名。默认情况下，路由器的默认主机名是 **home.gateway**。

IPSec：启用 IPSec 可以增强 L2TP VPN 安全。

认证：认证能够实现数据报文的完整性，并确保在传输过程中，报文不被篡改。有三个选项：信息摘要算法 (**MD5**)、安全散列算法 (**SHA1**) 或**没有**。SHA1 算法速度比较慢，但比 MD5 更能抵御力迫法攻击。

MD5：单向哈希算法，生成一个 128 位散列值。

SHA1：单向哈希算法，生成一个 160 位散列值。

加密：从下拉菜单中选择加密方法。有四个选项可供选择：**DES、3DES、AES (128, 192 和 256)。** 3DES 和 AES 算法更加高级，但会增加延。

DES：数据加密标准，密钥长度为 56 位。

3DES：三重数据加密标准。密钥长度为 168 位。

AES：高级加密标准。密钥长度为 128 位。

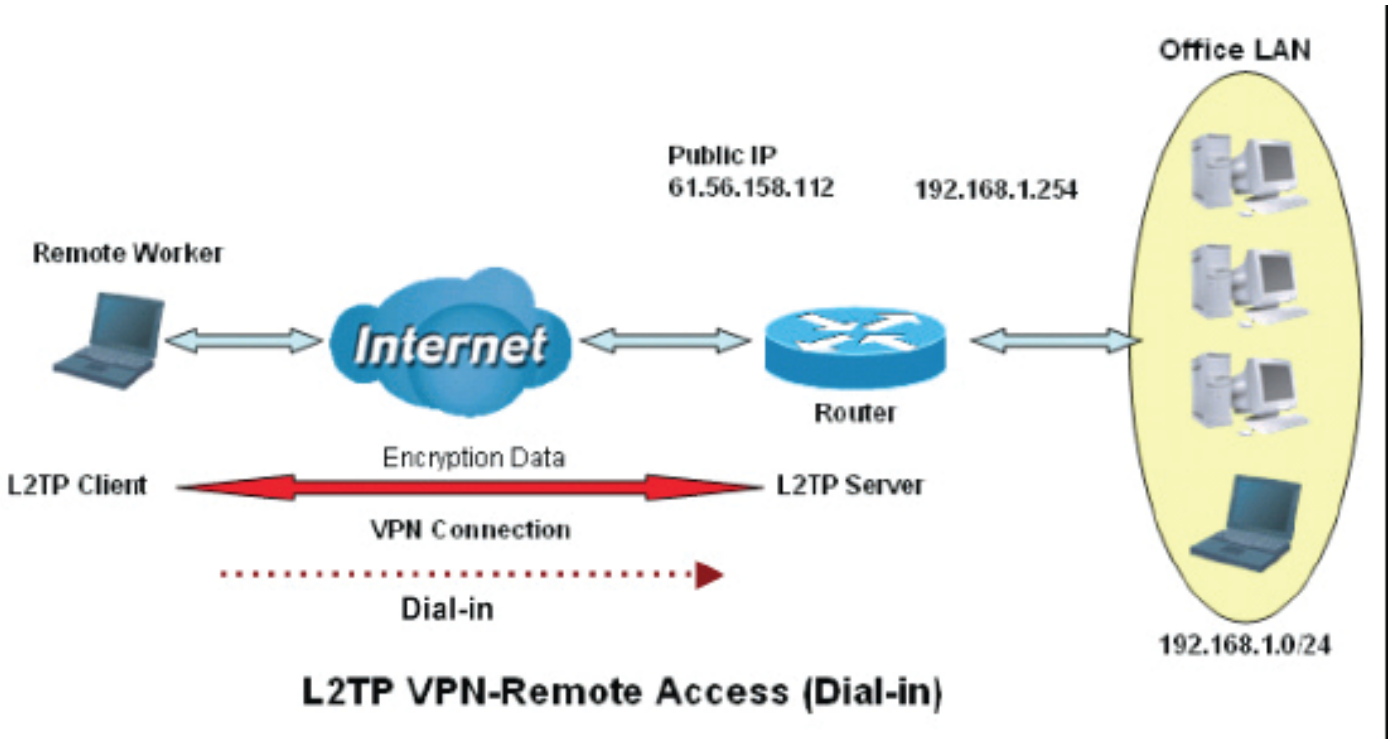
完美向前保密：选择是否启用 PFS，在 VPN 协商第二阶段使用 Diffie-Hellman 公开密钥加密法来更改加密密钥。该功能提供的安全性更好，但会延长 VPN 协商时间。Diffie-Hellman 是一种公钥加密法，通信双方在不安全通信隧道上建立共享密钥（如，通过 Internet）。共有三种模式：MODP 768 位, MODP 1024 位和 MODP 1536 位。MODP 代表模块指数组。

预共享密钥：用于 Internet 密钥交换协议 (IKE) 的字符串，长度为 4~128 个字符。两端必须使用相同的密钥。IKE 用来为需要提供密钥的服务（如 IPSec）建立共享安全策略和认证密钥。在 IPSec 流量通过之前，路由器都必须验证对端身份。可通过手动输入路由器或主机的预共享密钥完成。

单击**编辑/删除**保存更改。

实例：配置 L2TP VPN – 远程访问拨入连接

远地的工作人员通过 Microsoft VPN 适配器（与 Windows XP/2000/ME 一起提供）与总部建立 L2TP VPN 连接。路由器安装在总部，连接到多个 PC 和服务器。



L2TP VPN-Remote Access (Dial-in)

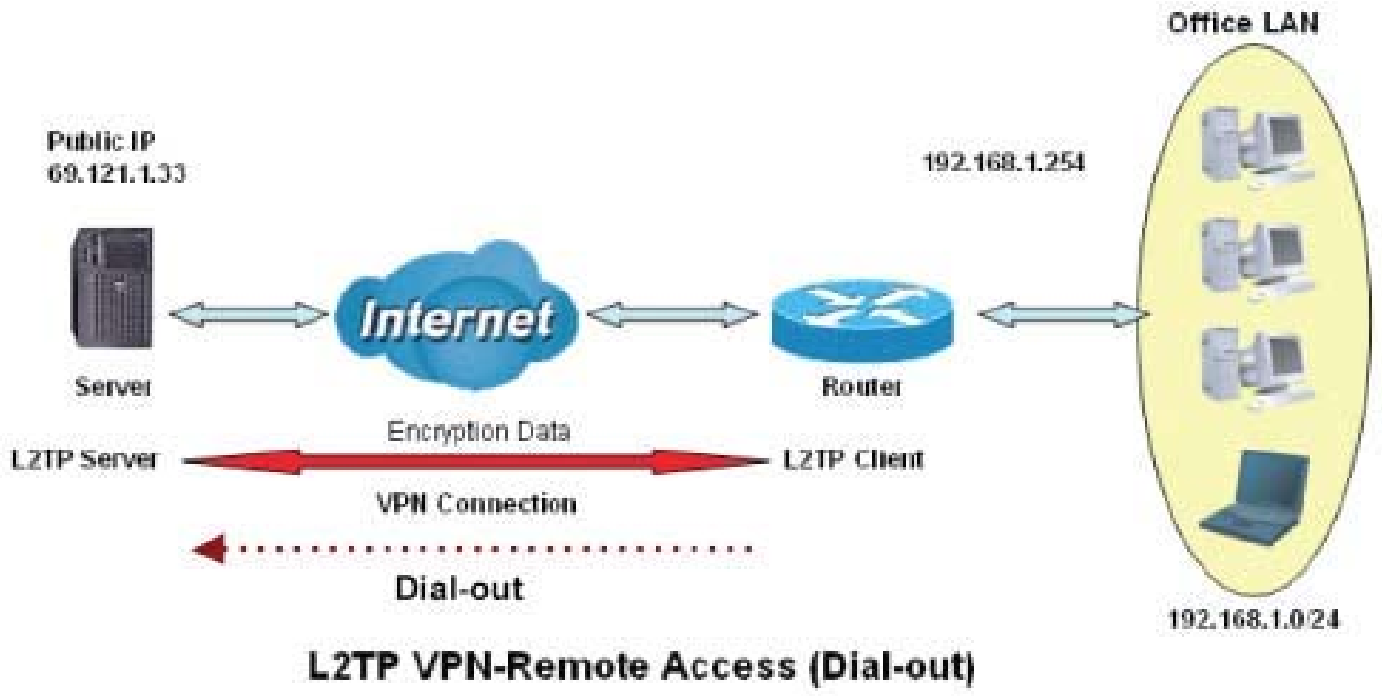
配置办公室的 L2TP VPN

输入的 IP 地址 192.168.1.200 将被分配给远地工作人员。确保这个 IP 没有被办公室 LAN 使用。

功能		描述
名称	VPN_L2TP	指定的 L2TP 连接名称
连接类型	远程访问	从连接类型下拉菜单中选择远程访问
类型	拨入	从类型下拉菜单中选择拨入
IP 地址	192.168.1.200	指定给远程客户端的 IP 地址
用户名	username	输入认证远地工作人员的用户名和密码
密码	123456	
认证类型	Chap（自动）	大多情况下，保持默认值。
IPSec	启用	启用可以增强 L2TP VPN 安全。
认证	MD5	两者必须使用相同值。
加密	3DES	
完美向前保密	没有	
预共享密钥	12345678	

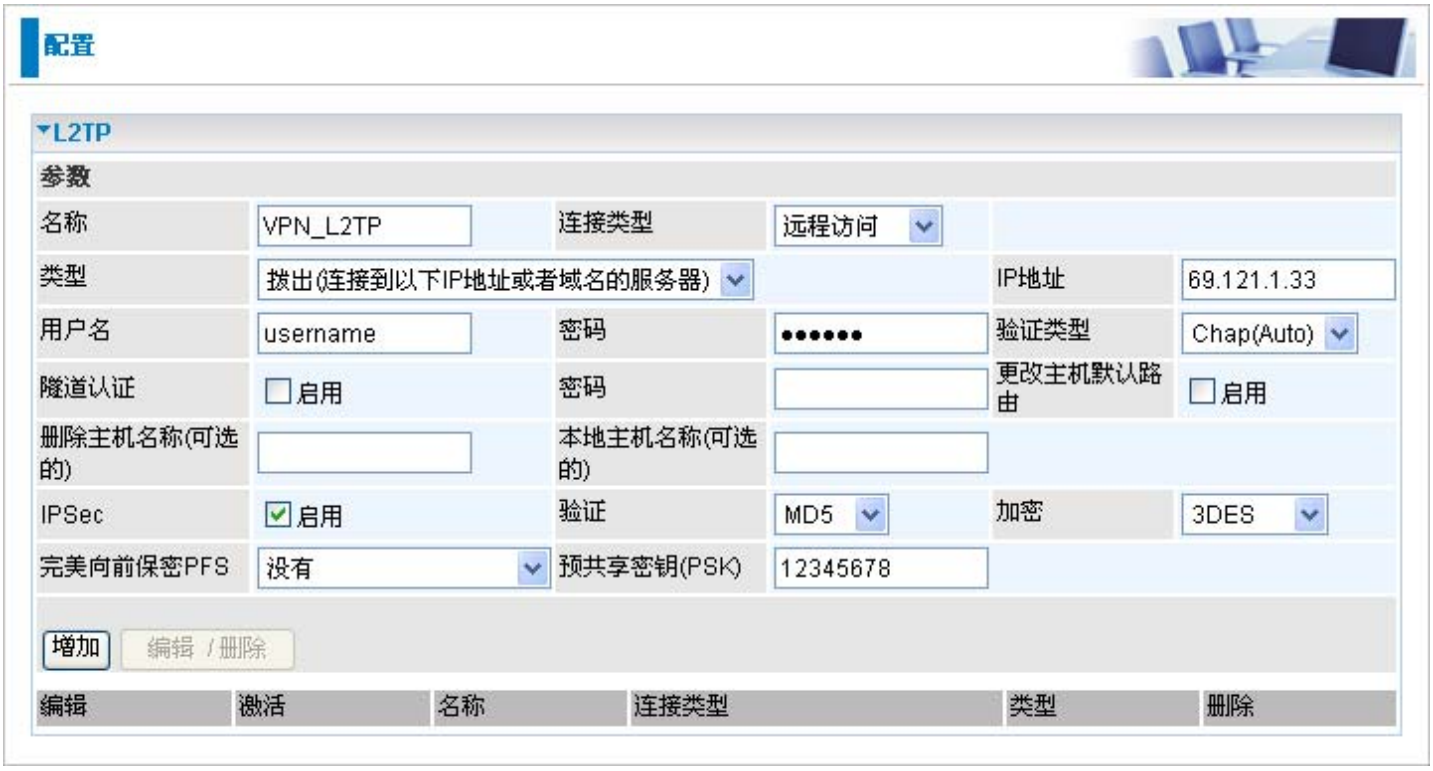
实例：配置远程访问 L2TP VPN 拨出连接

在公司办公室与位于其他地方的文件服务器之间建立 L2TP VPN 连接。路由器安装在办公室内，连接到多个 PC 和服务器。



L2TP VPN-Remote Access (Dial-out)

配置办公室的 L2TP VPN



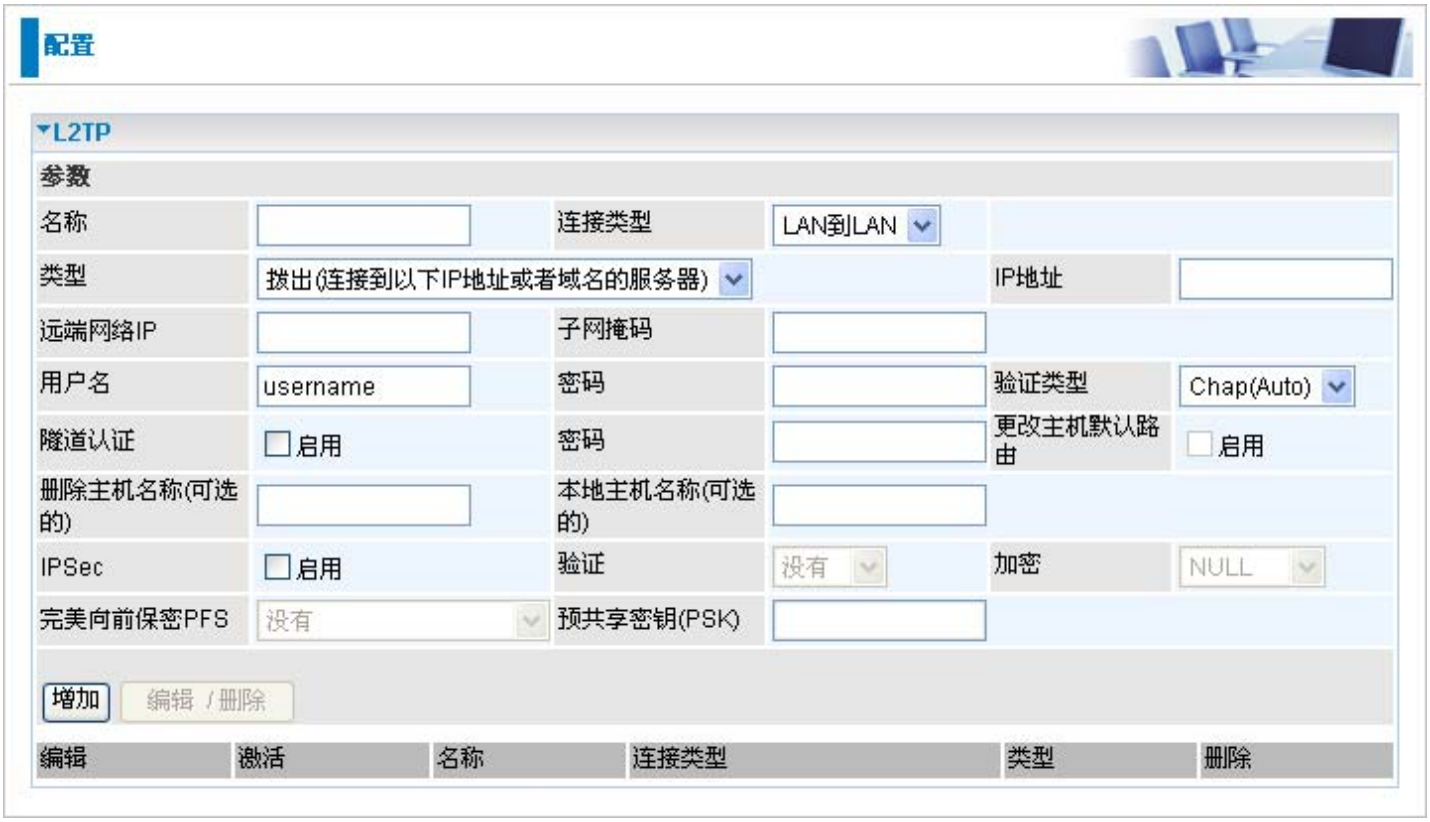
功能		描述
名称	VPN_L2TP	指定的 L2TP 连接名称
连接类型	远程访问	从连接类型下拉菜单中选择拨出
类型	拨出	从类型下拉菜单中选择拨入
IP 地址	69.121.1.33	拨号服务器 IP
用户名	Username	指定的用户名和密码
密码	123456	
认证类型	Chap（自动）	大多情况下，保持默认值。
IPSec	启用	启用可以增强 L2TP VPN 安全。
认证	MD5	两者必须使用相同值。
加密	3DES	
完美向前保密	没有	
预共享密钥	12345678	

实例：配置路由器拨入到服务器

目前的 Microsoft Windows 操作系统不支持外来 L2TP 服务。所以还需要使用其他软件来支持该项服务。

L2TP 连接 - LAN 到 LAN

L2TP VPN 连接



名称：指定的连接名称。

连接类型：远程访问或 LAN 到 LAN。

类型：如果想要路由器作为客户端（连接到远程 VPN 服务器，如办公室服务器），选中**拨出**；选中**拨入**，路由器作为 VPN 服务端。

配置通过路由器建立远程 LAN 连接，输入您想要连接到的远程服务器 IP 地址（或主机名）。

配置路由器作为服务端接收传入的连接，输入分配给拨入用户的私有 IP 地址。

IP 地址：输入 IP 地址。

远端网络 IP：输入远端网络的 IP 地址。

子网掩码：根据远端网络的 IP 设置，输入远端网络的子网掩码。

用户名：如果您是拨出用户（客户端），输入由主机提供的用户名。如果您是拨入用户（服务端），输入您自己的用户名。

密码：如果您是拨出用户（客户端），输入主机提供的密码。如果您是拨入用户（服务端），输入您自己的密码。

认证类型：默认为**自动**，由路由器决定使用的认证类型。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。

隧道认证：使路由器对 L2TP 远程和 L2TP 主机进行认证。仅当 L2TP 远程支持该功能时有效。

密钥：安全口令长度必须为 16 个字符，包括字符和数字。

启用为默认路由：常用于拨出连接，所有数据包通过 VPN 隧道路由到 Internet，启用该功能会降低 Internet 性能。

IPSec：启用 IPSec 可以增强 L2TP VPN 安全。

远程主机名（可选）：输入远程 VPN 设备的主机名。主机名是远程 VPN 设备的隧道标识符，与提供的远程主机名进行匹配。如果相匹配，则建立起隧道连接，如果不匹配，则断开连接。

警告：仅针对当路由器作为 VPN 服务端时。只有高级用户可以使用这个选项。

本地主机名（可选）：输入用来连接/建立 VPN 隧道的本地 VPN 设备的主机名。默认情况下，路由器的默认主机名是 **home.gateway**。

IPSec：启用 IPSec 可以增强 L2TP VPN 安全。

认证：认证能够实现数据报文的完整性，并确保在传输过程中，报文不被篡改。有三个选项：信息摘要算法 (**MD5**)、安全散列算法 (**SHA1**) 或**没有**。SHA1 算法速度比较慢，但比 MD5 更能抵御力迫法攻击。

MD5：单向哈希算法，生成一个 128 位散列值。

SHA1：单向哈希算法，生成一个 160 位散列值。

加密：从下拉菜单中选择加密方法。有四个选项可供选择：**DES**、**3DES**、**AES (128, 192 和 256)**。3DES 和 AES 算法更加高级，但会增加延。

DES：数据加密标准，密钥长度为 56 位。

3DES：三重数据加密标准。密钥长度为 168 位。

AES：高级加密标准。密钥长度为 128 位。

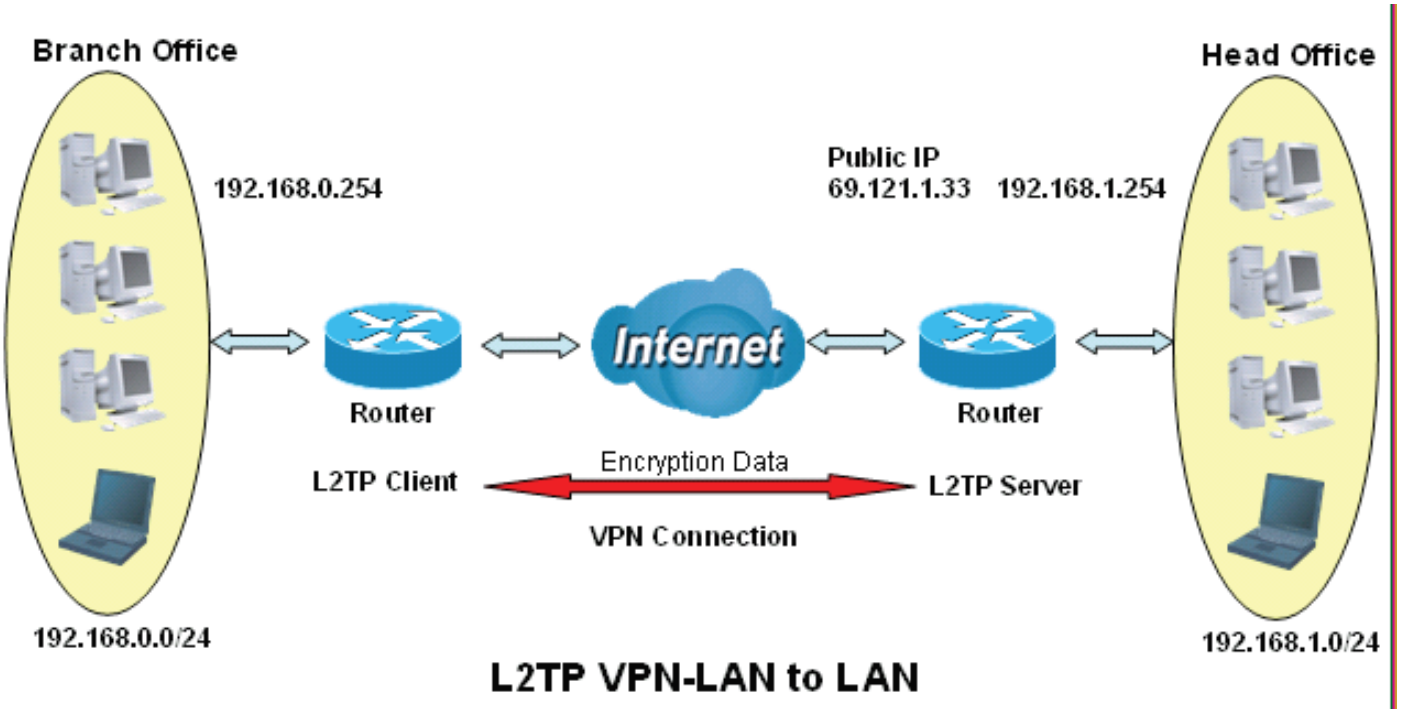
完美向前保密：选择是否启用 PFS，在 VPN 协商第二阶段使用 Diffie-Hellman 公开密钥加密法来更改加密密钥。该功能提供的安全性更好，但会延长 VPN 协商时间。Diffie-Hellman 是一种公钥加密法，通信双方在不安全通信隧道上建立共享密钥（如，通过 Internet）。共有三种模式：MODP 768 位, MODP 1024 位和 MODP 1536 位。MODP 代表模块指数组。

预共享密钥：用于 Internet 密钥交换协议 (IKE) 的字符串，长度为 4~128 个字符。两端必须使用相同的密钥。IKE 用来为需要提供密钥的服务（如 IPSec）建立共享安全策略和认证密钥。在 IPSec 流量通过之前，路由器都必须验证对端身份。可通过手动输入路由器或主机的预共享密钥完成。

单击**编辑/删除**保存更改。

实例：配置 L2TP LAN 到 LAN 连接

通过在分部与总部之间建立 L2TP VPN 隧道，连接 Internet 上的两个专用网。分别在总部和分部安装路由器。



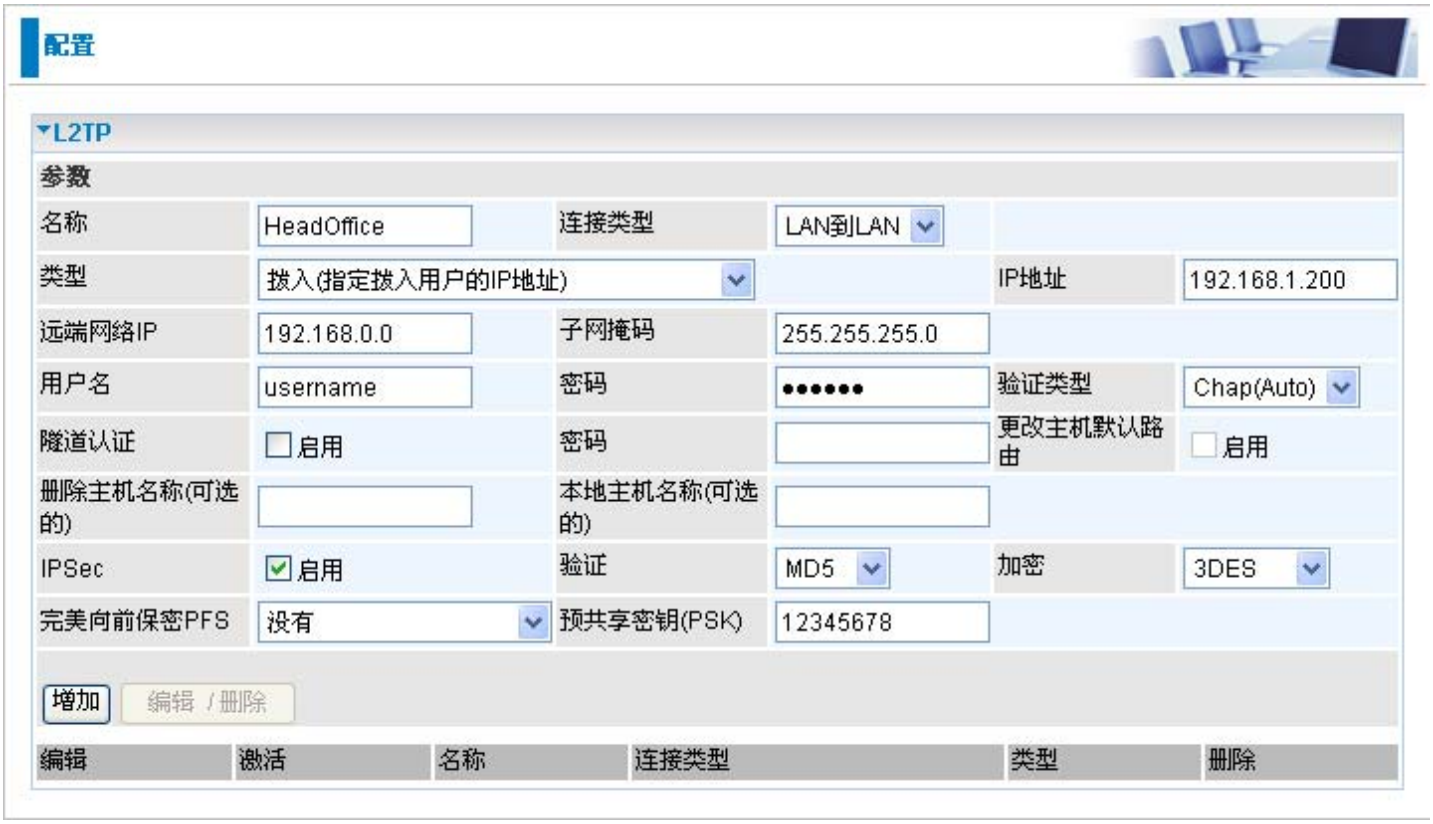
注意

LAN 到 LAN 应用要求分部和总部的 LAN **必须在不同的子网中**。

总部和分部必须设置相同的**预共享密钥、VPN 连接类型和安全算法。**

配置总部的 L2TP VPN

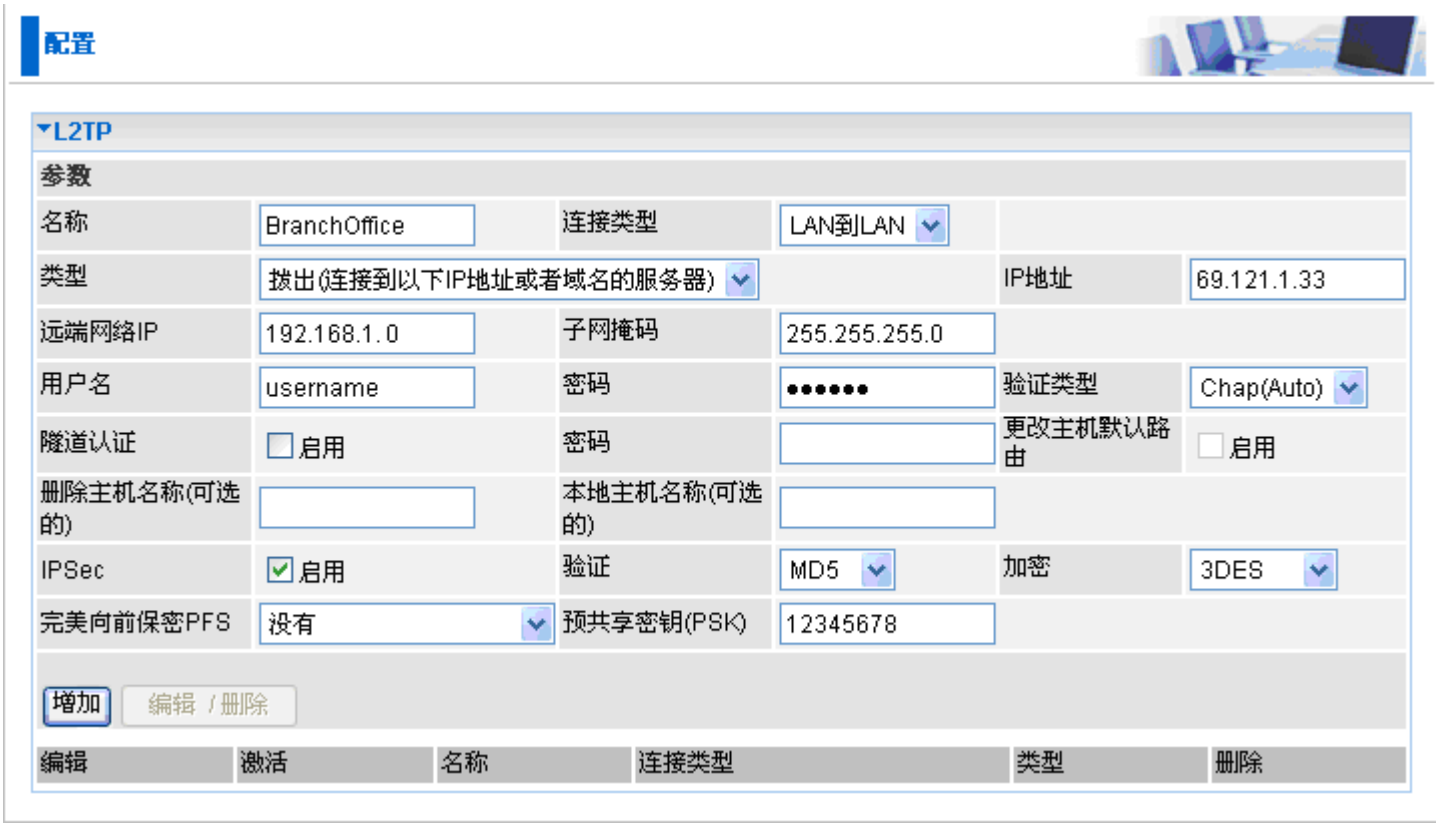
将 IP 地址 192.168.1.200 分配给分部路由器。保证该 IP 地址未被总部 LAN 使用。



功能		描述
名称	HeadOffice	指定的 L2TP 连接名称
连接类型	LAN 到 LAN	从连接类型下拉菜单中选择LAN 到 LAN
类型	拨入	从类型下拉菜单中选择拨入
IP 地址	192.168.1.200	分配给分部网络的 IP 地址
对端网络 IP	192.168.0.0	分部网络
用户名	username	指定的用来认证分部网络的用户名和密码
密码	123456	
认证类型	Chap（自动）	大多情况下，保持默认值。
IPSec	启用	启用可以增强 L2TP VPN 安全。
认证	MD5	两者必须使用相同值。
加密	3DES	
完美向前保密	没有	
预共享密钥	12345678	

配置分部的 L2TP VPN

IP 地址 69.1.121.30 是总部路由器的公共 IP 地址。如果注册了 DDNS（请参阅本手册的 **DDNS** 部分），您还可以使用域名代替 IP 地址连接到路由器。



功能		描述
名称	BranchOffice	指定的 L2TP 连接名称
连接类型	LAN 到 LAN	从连接类型下拉菜单中选择LAN 到 LAN
类型	拨出	从类型下拉菜单中选择拨出
IP 地址	69.121.1.33	分配给分部网络的 IP 地址
对端网络 IP	192.168.1.0	总部网络
子网掩码	255.255.255.0	
用户名	username	指定的用来认证分部网络的用户名和密码
密码	123456	
认证类型	Chap（自动）	大多情况下，保持默认值。
IPSec	启用	启用可以增强 L2TP VPN 安全。
认证	MD5	两者必须使用相同值。
加密	3DES	
完美向前保密	没有	
预共享密钥	12345678	

VoIP – 因特网声传协议

（仅适用于 BiPAC 7404VGO(P)X、7404VNO(P)X、6404VGO(P)X）

VoIP 实现在 Internet 上通话，而不经过 PSTN（公用电话交换网线路）。它不仅成本低廉（尤其对于长途电话），而且通话音质好。

注意

VoIP 配置完成后，记住要应用更改。**保存配置**，然后重启，以激活 VoIP。

VoIP 包括以下几部分：**SIP 设备参数、SIP 账号、电话端口、PSTN 拨号计划、VoIP 拨号计划、呼叫功能、快速拨号**以及**振铃 & 音调。**

SIP 设备参数

提供了 VoIP 服务的简易安装。电话端口 1 和端口 2 可以向不同的 SIP 服务提供商申请。

SIP 设备参数

SIP：使用 VoIP SIP 作为 VoIP 呼叫的信号协议。默认设置为**关闭**。

静默抑制 (VAD)：语音启动侦测将阻止传输耗带宽的背景噪声。语音启动侦测 (VAD) 也叫静默抑制，是一种软件应用，保证只有在真正通话时才使用带宽。默认设置为**开启**。

回声消除：G.168 回声消除器符合 ITU-T 标准，用来隔离通话时产生的回声。使您在通话时不会听到回声。默认设置为**开启**。

RTP 端口：提供媒体端口 (RTP) 的基准值，这些接口被指定给不同端点以及可能分布在端点上的各个会话。（范围在 5100~65535 之间，默认为 5100）

区域：从下拉列表框中选择，允许用户选择使用 VoIP 设备的国家。选择一个国家后，所选的参数将会自动加载。

语音 QoS，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。参阅表 4：DSCP 映射表：

注：确保骨干网中的路由器有能力执行和检查 QoS 网络中的所有 DSCP。

高级 – 参数

VoIP 透传：IP 接口决定发送/接收 VoIP 流量的方向，包括：ipwan 和 iplan。选择接口的简单方法是：检查 SIP 服务器的位置。如果 SIP 服务器在 Internet 中，那么选择 **ipwan**。如果 VoIP SIP 服务器在局域网中，选择 **iplan**。

语音帧大小：可使用的语音帧大小在 10ms 到 60ms。帧大小表示语音包排队和发送需要多少毫秒。理想情况是消除器和接收器中的语音帧同样大。

拨号计划优先级：定义 VoIP 和 PSTN 拨号计划的优先级。

PSTN 自动回环：如果 VoIP SIP 响应的错误及错误代码与**编辑**中的代码匹配，VoiP 通话将自动回退到 PSTN。也就是说，当 VoIP SIP 返回错误代码时，将通过 PSTN 进行呼叫。

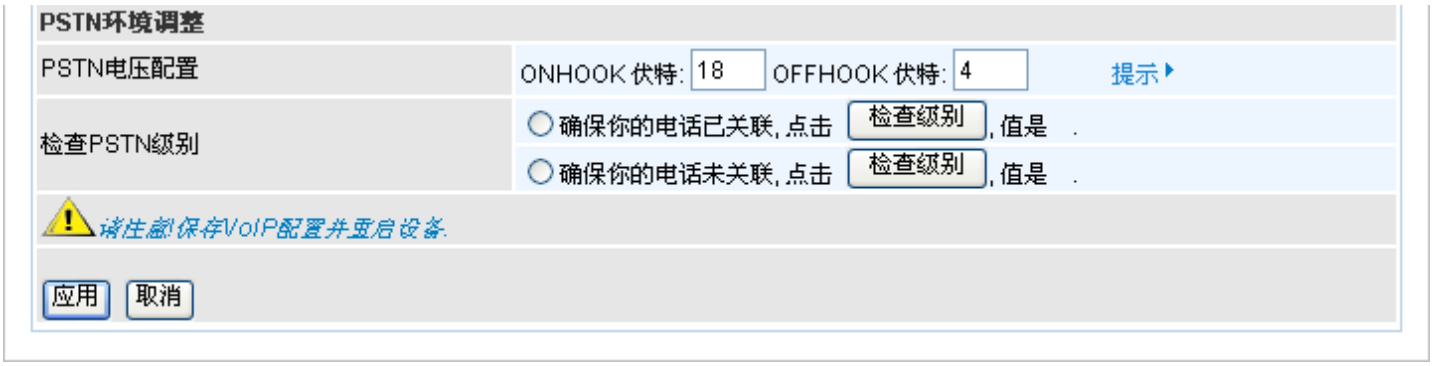
单击**编辑**，添加或删除响应代码。保证代码必须使用逗号 (,) 隔开。

有关 SIP 响应代码的详细信息，请单击**此处**链接到 http://voip-info.org/wiki/view/sip+response+codes，了解所有错误代码的含义。

T.38 传真中继：两台标准的组 3 传真终端可以在 Internet 或其他 IP 网络上实时传输传真文件。只有两端的站点都支持并已启用了该功能，它才能发挥作用。

高级 – PSTN 环境调整

PSTN 环境调整选项用来调整挂机和摘机时的电压检测值。如果默认值不正确，导致无法正确检测 PSTN 通话（如通话在接听后 5 秒钟终止），这时必须调整电压检测值。有效电平由环境来决定，包括所使用电话的数量和型号。



*注：**ONHOOK** 指挂机。*

想要**摘机**，拿起听筒后按闪断 (Hook/Flash)，直到听到正常的 PSTN 拨号音，而不是 VoIP 拨号音。等待数秒钟，然后按**核对电平**。

必须检查所有已连接到这台设备的电话机的 OFFHOOK 值。将所有电话机的 OFFHOOK 电压设置为最低值，比如，如果电话机返回的值是 4、5、7，那么必须将 OFFHOOK 设置为 4。

注：核对电平不会自动设置检测值；测试完所有电话后，您必须输入检测到的最低电平。

SIP 账号

这部分包含 VoIP 模块的基本设置，模块由向导中选择的提供商提供。如果提供的信息不准确，将中断通话。

配置名称：配置文件的标识名称。

注册地址（或主机名）：表示 VoIP SIP 注册服务器的 IP 地址。

注册端口：指定 VoIP SIP 注册服务器上监听 VoIP 设备注册请求的端口。
期限：发送注册信息的截止时间。

用户名：为 VoIP SIP 代理服务器设置不同的域名。

出站代理地址：指定 VoIP SIP 出站代理服务器的 IP 地址。

出站代理端口：指定 VoIP SIP 出站代理服务器上监听信息的端口。

电话号码：此参数包含 VoIP SIP 注册服务器中用户的注册 ID。

用户名：认证用户名就是电话号码。

密码：此参数包含 VoIP SIP 注册服务器中用来认证的密码。

显示名称：名称将显示在来电显示上。

直接拨号：选择 VoIP 电话呼入时使用的电话端口。

电话端口

显示电话端口状态，您可以编辑电话端口的账号信息。单击**编辑**，更新电话端口信息。

端口：您可以更改指定 FXS 端口的设置。

***69（回拨）：**拨 *69 回拨最后一个未接电话。仅对 VoIP 电话适用。

***20（启用请勿打扰）：**拨 *20 可以设置开启**请勿打扰**。来电时，电话将不会响。

***90x（盲呼叫转移）：**拨 *90 + 电话号码将电话转给第三方。该功能默认为开启。

x#快速拨号(x:2..9)：参阅 Web GUI 中的**电话端口**部分。使用**快速拨号**功能之前，请先设置**快速拨号**电话簿。该功能默认为开启。

重新拨号：按 ## 以重新拨打最近拨打的号码。该功能默认为开启。

***74<x><号码>#：**使用电话键盘插入电话号码到**快速拨号**电话薄中。您也可以手动更新**快速拨号**电话薄。详细内容，参阅 Web GUI 中的**电话端口**部分。

***67 匿名电话：**隐藏所有呼叫方的电话号码，使号码不显示在远程站点上。它将应用于输入控制符号以后，下一个打入的电话。详细操作步骤如下：“摘机-> *67 -> 挂机-> 摘机-> 拨号”。 该功能默认为开启。

电话号码 + #：这种拨号是最快的，您可以立即拨号，无须等待。

注：有关详细信息，请参阅本手册中的特殊拨号代码部分。

编解码选择

Codec 是编解码器，用于数据信号转换。设置语音压缩的优先级：1 为最高优先级。

G.729：用来将语音信息编码并解码成但数据包，从而降低带宽消耗。

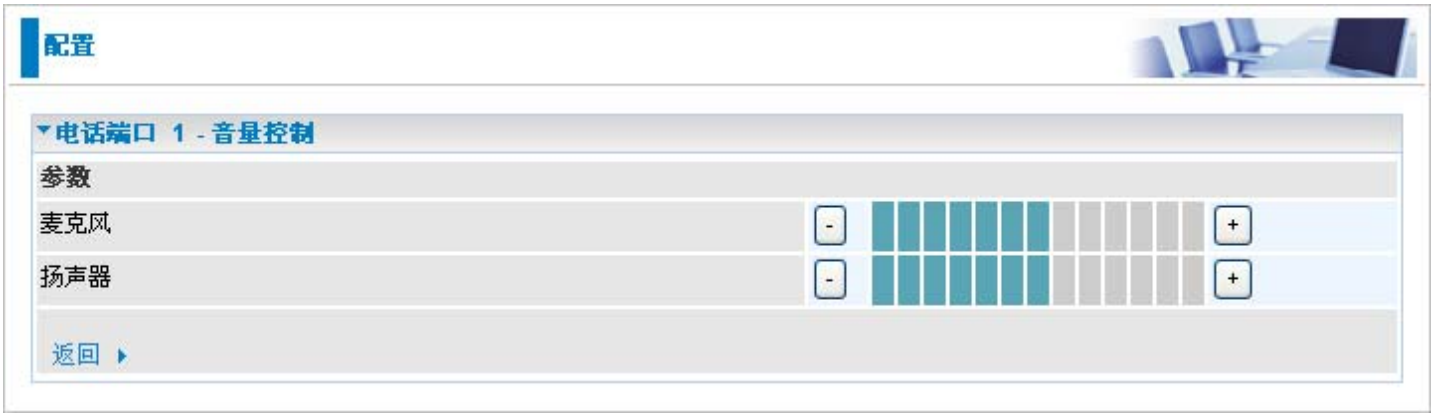
G.711μ-LAW：它是基本非压缩编码和解码技术。μ-LAW 使用脉码调制 (PCM) 编码器和解码器来转换 14 位线性采样。

G.711A-LAW：它是基本非压缩编码和解码技术。A-LAW 使用脉码调制 (PCM) 编码器和解码器来转换 13 位线性采样。

G.726-32：用于将语音信息编码并解码成但数据包，从而降低带宽消耗。目前仅支持比特率 32Kbps。

DTMF 方法：支持 Inband、RFC 2833 以及 SIP INFO (RFC 2976)。

音量控制



音量控制帮助将电话音质调节到最佳舒适听力级。

按减号“-”可减小麦克风或/和扬声器的音量。

按加号“+”可增大麦克风或/和扬声器的音量。

PSTN 拨号计划（仅适用于带有 LINE 端口的路由器）

通过 PSTN 拨号计划，您可以对系统中“具有 PSTN 交换功能的 VoIP”进行配置。您可以定义一系列从 VoIP 到 PSTN 线路的常规呼叫的拨号计划。前缀是区分 VoIP 电话和**常规**电话的关键。如果实际拨打的号码与拨号计划中定义的前缀相匹配，所拨打的号码将被路由到 PSTN 中进行常规呼叫。否则，拨打的号码将被路由到 VoIP 网络中。

提醒：要使用此功能，您必须是已经注册并且已经连接到 SIP 服务器。

前缀：指定要从 VoIP 切换到 PSTN 电话的号码。

号码位数：指定拨出号码的总位数。最多为 15 位。

动作：指定拨打 PSTN 电话的拨号方式。

带前缀拨号：选择以后，拨打常规电话时，将通过 FXO 同时拨号前缀和和电话号码。

注：实际拨打号码的有效位数必须与号码位数字段中的位数相匹配。

不带前缀拨号：选择以后，拨打常规电话时，FXO 将只拨号电话号码。

注：实际拨打号码的有效位数必须与号码位数字段中的位数相匹配。

拨号超时：超时开始时，将通过 FXO 拨号输入的号码和前缀，尽管输入的号码位数与规定的号码位数不匹配。

注：实际拨打号码的有效位数不得超过号码位数字段中的位数。

不带前缀拨号超时：超时开始时，将通过 FXO 端口拨号输入的号码，不包括前缀，尽管输入的号码位数与规定的号码位数不匹配。

注：实际拨打号码的有效位数不得超过号码位数字段中的位数。

警告

下列情况下，电话端口 1和 2 将自动依赖 PSTN 线路：

- **断电。**
- **Internet 服务失误，**如 WAN IP 地址丢失。
- **SIP 选项被禁用。**参阅 *VoIP 基本设置*部分。
- **与 *PSTN 拨号计划* 中定义的规则相匹配的呼叫。**
- **SIP 服务无法使用。**其中不包括：
  - 用户手动禁用注册
  - 用户插入错误的认证用户名或密码
  - 用户拨错 SIP 号码，当且仅当 *PSTN 自动回退*功能未启用时。参阅*VoIP 基本设置/高级*，以获取信息

PSTN 拨号计划实例：

1. 带前缀拨号

如果您拨打 01223 707070，将通过 FXO 拨出号码 01223707070 进行常规通话。

2. 不带前缀拨号

如果您拨打 9102，将通过 FXO 端口拨出号码 9102 进行常规通通话。

3. 拨号超时

如果拨打的号码只有 01223 7070 这几位数字，超时激活后，将通过 FXO 端口拨出号码 012237070 进行常规通话。

即使号码 7070（只有 4 位），与字段中定义的 6 位数不匹配，但因为没有超过 6 位数所以仍是有效的电话号码。

4. 不带前缀拨号超时

如果拨打的号码只有 97070 这几位数字，超时激活后，将通过 FXO 端口拨出号码 7070 进行常规通话。

即使号码 7070（只有 4 位），与字段中定义的 6 位数不匹配，但因为没有超过 6 位数所以仍是有效的电话号码。

VoIP 拨号计划

通过 VoIP 拨号计划，您拨打电话将变的简单方便的多，无须记住每位联系人的号码。VoIP 拨号计划创建起来很很容易，您可以不用记住号码就可以拨打电话。要使用此功能，转至**配置> VoIP > VoIP 拨号计划**。

拨号计划规则

单击**增加**按钮，创建并定义 VoIP 拨号计划规则。

前缀处理：

无条件前置 xxx：拨号时，xxx 号码将被无条件地添加到拨号号码的前面。前缀也可以包含任何数字和/或字符，如 +, *, #。

注：对于带有 +, *, # 的特殊服务，您需要向 VoIP 或当地电话服务提供商核实，以获取相关信息。

如果前缀是 xxx，则删除：拨号前，将前缀 xxx 从拨号号码中删除。

如果前缀是 xxx，则替换为：拨号前，将前缀 xxx 添加到拨号号码的前面。

无前缀：拨号号码前不插入前缀。将其设置为默认设置。

主要数字序列：可以通过 **SIP、PSTN 或 ENUM** 拨打电话。

X：任何 0 到 9 之间的数字。

.（句号）：重复 0 到 9 之间的数字。

***（星号）**：* 是电话键盘上的标准字符。请核实它是否是 VoIP 服务提供商或当地电话服务提供商针对特殊服务而提供的。

#（井号）：* 是电话键盘上的标准字符。请核实它是否是 VoIP 服务提供商或当地电话服务提供商针对特殊服务而提供的。

<@ 当前配置文件>：参阅通过 *VoIP 向导为*端口 1 或 2 *注册* VoIP 账号。

<@ PSTN>：指通过 PSTN 线路呼叫。

<@ENUM>：指通过 E.164 号码 (“ENUM”) 直接呼叫对方。电子号码 (ENUM) 使用基于 DNS 的技术，映射传统电话号码 (PSTN) 和 Internet 地址/ SIP 地址。ENUM 号码必须通过公共 ENUM 站点或向 VoIP 服务提供商注册。

<@ SIPgateway>：用于*智能呼叫路由*功能，您需要在 VoIP 向导页面的 **VoIP 用户自定义配置文件**连接上设置 SIP 账号。有关详细信息，请转到手册中的 *VoIP 向导*部分。

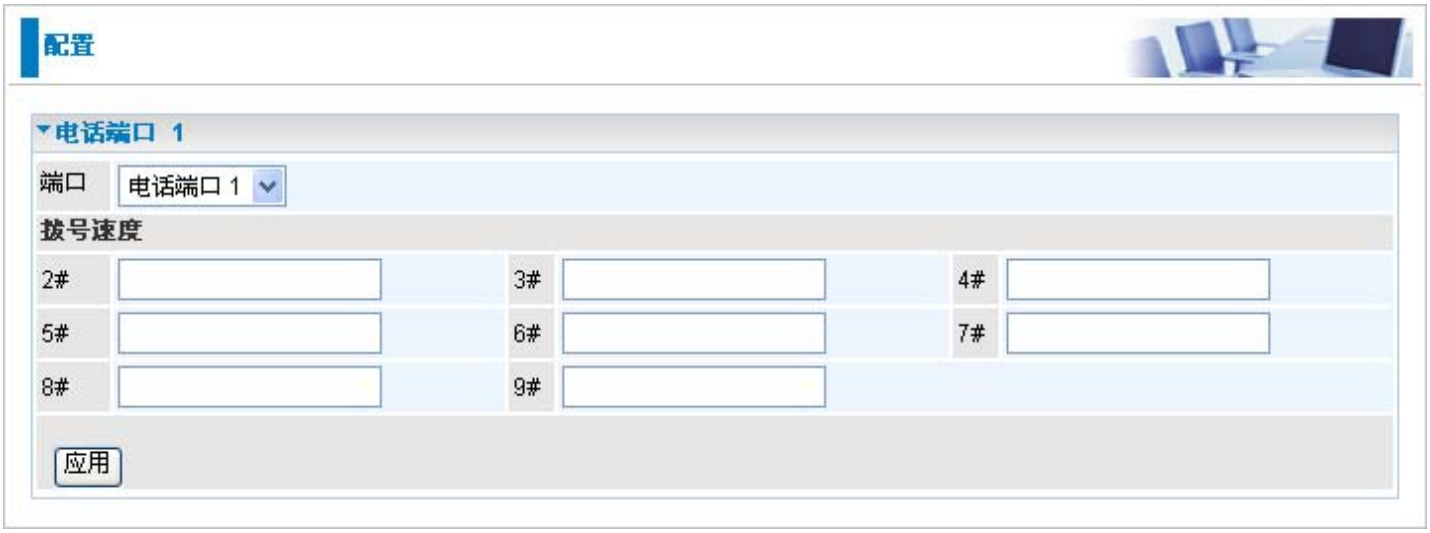
拨号计划示例	描述
x.	任何 0 到 9 之间的数字，长度不等。 最大长度为 16。
xxx	0 到 9 之间的任何 3 位数字。总长度为 3。 ***注：不得包括句号(.)。***
xxxx.	任何 0 到 9 之间的数字，长度不等，但不得少于 3 位数字。最大长度为 16。
123x.	任何以 123 开头的数字(0-9)。最大长度为 16。
[x…x]x. 例如：[124]x.	任何以 1、2 或 4 开头的数字(0-9)。最大长度为 16。
[x-x]x. 例如：[1-3]x.	任何以 1 到 3 开头的数字(0-9)。最大长度为 16。
x[x-x]x. 例如：9[4-6]8x.	任何以 9 为开头、第二位为 4-6、第三位为 8 的数字(0-9)。最大长度为 16。
特殊拨号计划示例	**描述**
*xx*x.	以*+任何两位数字+任何数字(0-9)开头，长度不等。最大长度为 16。
*xx	以*+任何两位数字(0-9)开头。包括*在内的总长度为 3。最大长度为 16。 ***注：不得包括句号(.)。***
**xx*x.	以**+任何两位数字(0-9)+*+任何数字(0-9)开头，长度不等。最大长度为 16。
#xx.	以#+任何数字(0-9)开头，长度不等，但不得少于 1 位。最大长度为 16。
##xx*x.	以##+任何两位数字+*+任何数字(0-9)开头，长度不等，但不得少于 1 位。最大长度为 16。

呼叫功能

VoIP 电话具有传统电话的所有功能。除了提供基本的功能外，VoIP 还提供几个增强型功能，为了符合您的个人要求，您可以进一步自定义呼叫设置，如呼叫转移设置、呼叫等待时间、会议电话、匿名电话以及来电未应答计时器等多个功能。

快速拨号

快速拨号作用很大，可以存储频繁使用的电话号码，按键盘上的数字 0 到 9 和井号键 (#) 即可启用该功能。例如，要快速呼叫条目 9 中的电话号码，只要按下键盘上的 9，再按 **#**。路由器将自动呼叫条目 9 中的号码。



振铃 & 音调

高级用户可以更改各种铃声的当前参数或新定义的参数（拨号音、忙音、应答音等）。

特定于国家的振铃 & 音调

区域：从下拉列表中选择您所在国家的铃声。VoIP 路由器根据不同国家提供不同的默认参数。输入国家名称后，铃声参数将自动显示。如果您所在国家不在此列表中，您可以手动创建铃声参数。

振铃参数

振铃节奏 (ms)：振铃节奏由三组字段定义，频率：打开 1，关闭 1；打开 2，关闭 2；打开 3；关闭 3。频率通过 Hertz 表示。时间以毫秒计。

音调参数

有关此类信息，请向当地电话服务提供商核实。此外，若没有特别要求，建议只有高级用户才配置该选项。
单击**应用**，应用设置。

QoS – 服务质量

QoS 功能针对各个应用，控制从 LAN（Ethernet 和/或无线网络）到 WAN (Internet) 的网络流量。方便您在系统以最高上行速度运行时，控制所有应用的服务质量以及传送速度。

QoS 包括以下几部分：**优先级别、出站 IP 控制 & 入站 IP 控制（带宽管理）。**

优先级别

路由器可以设置 3 个优先级：

高

标准（若没有设置，默认所有流量的优先级为标准）

低

各个优先级的使用比例为：高 (60%)、标准 (30%)、低 (10%)。

要删除应用，单击应用后面的**删除**单选按钮，然后单击**编辑/删除**按钮。

名称：用户自定义用来标识新策略/应用的名称。

时间表：优先策略的时间表。

优先级：各个策略/应用的特定优先级。默认设置为**高**。您也可以调整此设置，以适合您的策略/应用。

协议：支持的协议的名称。

源 IP 地址范围：被监控的发送数据包的源 IP 地址范围。

源端口：被监控的发送数据包的源端口。

目标 IP 地址范围：被监控的接收数据包的目标 IP 地址范围。

目标端口：被监控的接收数据包的目标端口。

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。

参阅表 4。DSCP 映射表：

注：确保骨干网中的路由器有能力执行和检查 QoS 网络中所有 DSCP。

表 4：DSCP 映射表

DSCP 映射表	
路由器	**标准 DSCP**
禁用	无
尽力服务	尽力服务(000000)
优质的	快速转发(101110)
金级服务(L)	一级金级服务(001010)
金级服务(M)	一级银级服务(001100)
金级服务(H)	一级铜级服务(001110)
银级服务(L)	二级金级服务(010010)
银级服务(M)	二级银级服务(010100)
银级服务(H)	二级铜级服务(010110)
铜级服务(L)	三级金级服务(011010)
铜级服务(M)	三级银级服务(011100)
铜级服务(H)	三级铜级服务(011110)

出站 IP 控制（LAN 到 WAN）

通过 IP 控制可以限制 IP 流量的速度。速率限制空白处输入的值将限制应用的流量速度。

名称：用户自定义用来标识创建的策略/应用的名称。

时间表：优先策略的时间表。详细信息，请参阅**时间表**。

协议：支持的协议名称。

速率限制：限制出站流量的速度。

源 IP 地址范围：被监控的发送数据包的源 IP 地址范围。

源端口：被监控的发送数据包的源端口。

目标 IP 地址范围：被监控的接收数据包的目标 IP 地址范围。

目标端口：被监控的接收数据包的目标端口。

入站 IP 控制（WAN 到 LAN）

IP 控制将限制 IP 流量的速度。速率限制空白处输入的值将限制应用的流量速度。

名称：用户自定义用来标识创建的策略/应用的名称。

时间表：优先策略的时间表。详细信息，请参阅**时间表**。

协议：支持的协议的名称。

速率限制：限制出站流量的速度。

源 IP 地址范围：被监控的发送数据包的源 IP 地址范围。

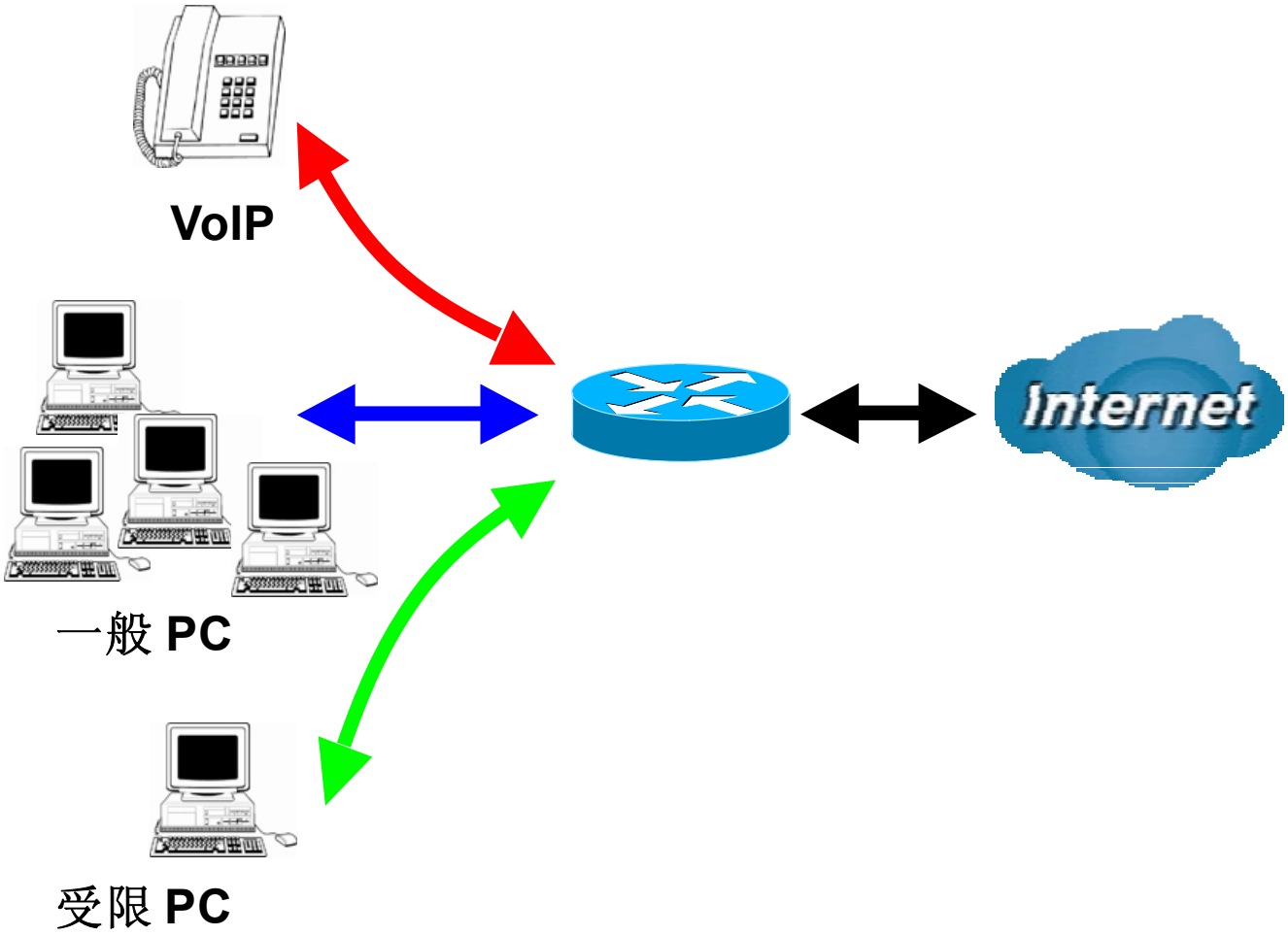
源端口：被监控的发送数据包的源端口。

目标 IP 地址范围：被监控的接收数据包的目标 IP 地址范围。

目标端口：被监控的接收数据包的目标端口。

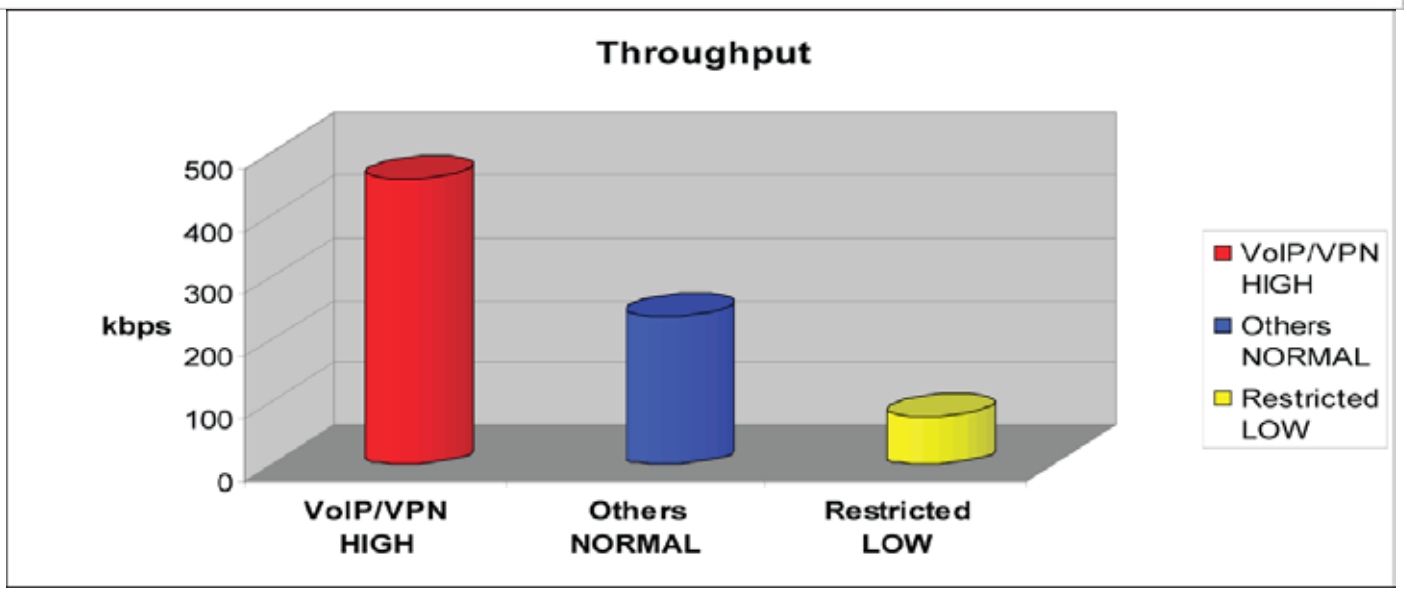
实例：网络的服务质量 (QoS)

连接图



信息与设置

上行流：928 kbps
下行流：8 Mbps
VoIP 用户：192.168.1.1
一般用户：192.168.1.2~192.168.1.5
受限用户：192.168.1.100



关键任务应用

通常，VPN 连接是一种针对关键任务的应用，用来在总部和分部之间进行数据交换。

关键任务应用必须顺利发送出去，不得丢弃。将优先级设置为**高**，以避免任何其它应用占满带宽。

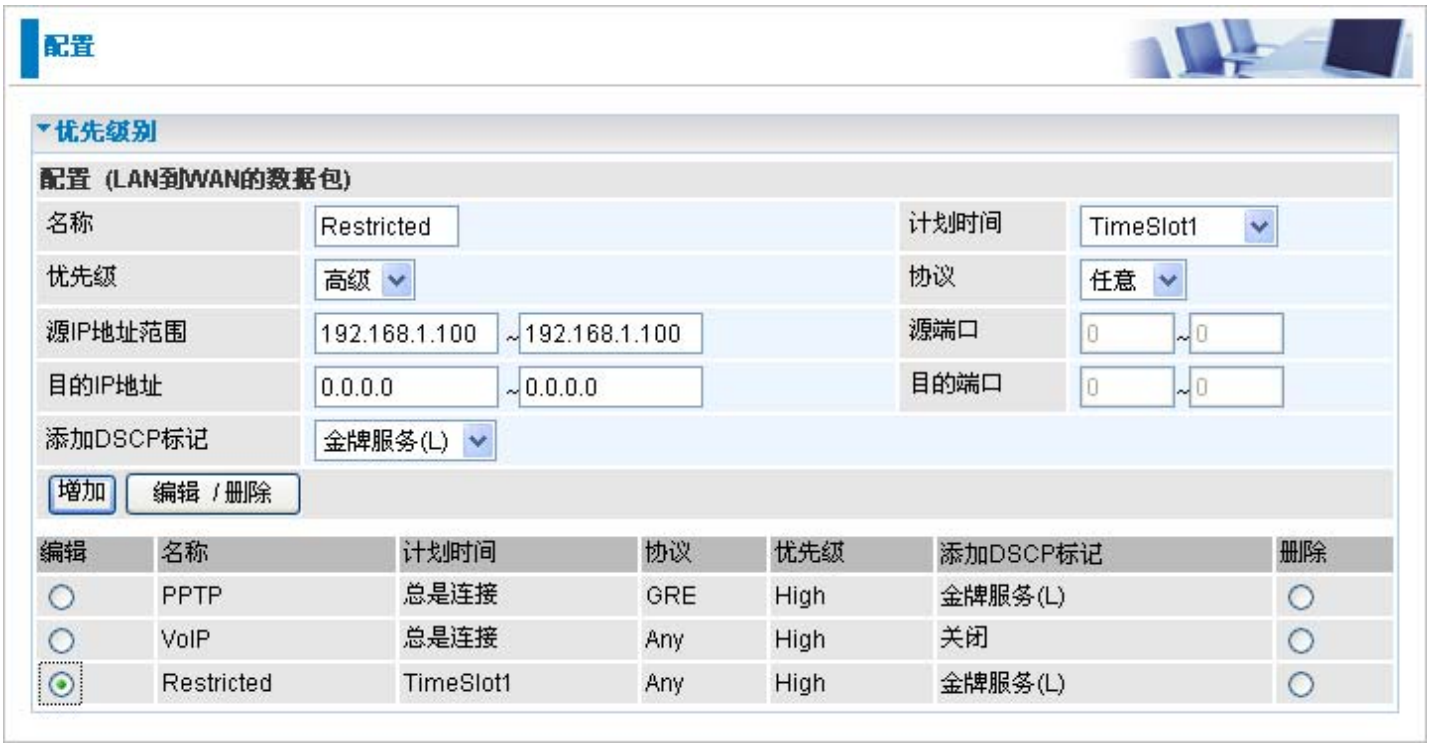
语音应用

语音是延迟敏感的应用。大多数 VoIP 设备使用 SIP 协议，SIP 模块将自动分配端口号。最好使用固定 IP 地址获取高优先级的 VoIP 数据包。

当流量为全载时，以上设置将有助于提高 VoIP 服务质量。

限制应用

有些公司将设置 FTP 服务器设置为仅供客户下载或家庭用户共享文件。



通过以上设置，FTP 上行流使用将受到限制。通过时间表，可以设置只在白天限制上行流的使用。

使用 IP 控制进行高级设置

通过 IP 控制，可以为分配带宽指定更多的信息，甚至是同等级中的应用也可以。

上行流：928kbps (29*32kbps)
关键任务应用：192kbps (6*32kbps)

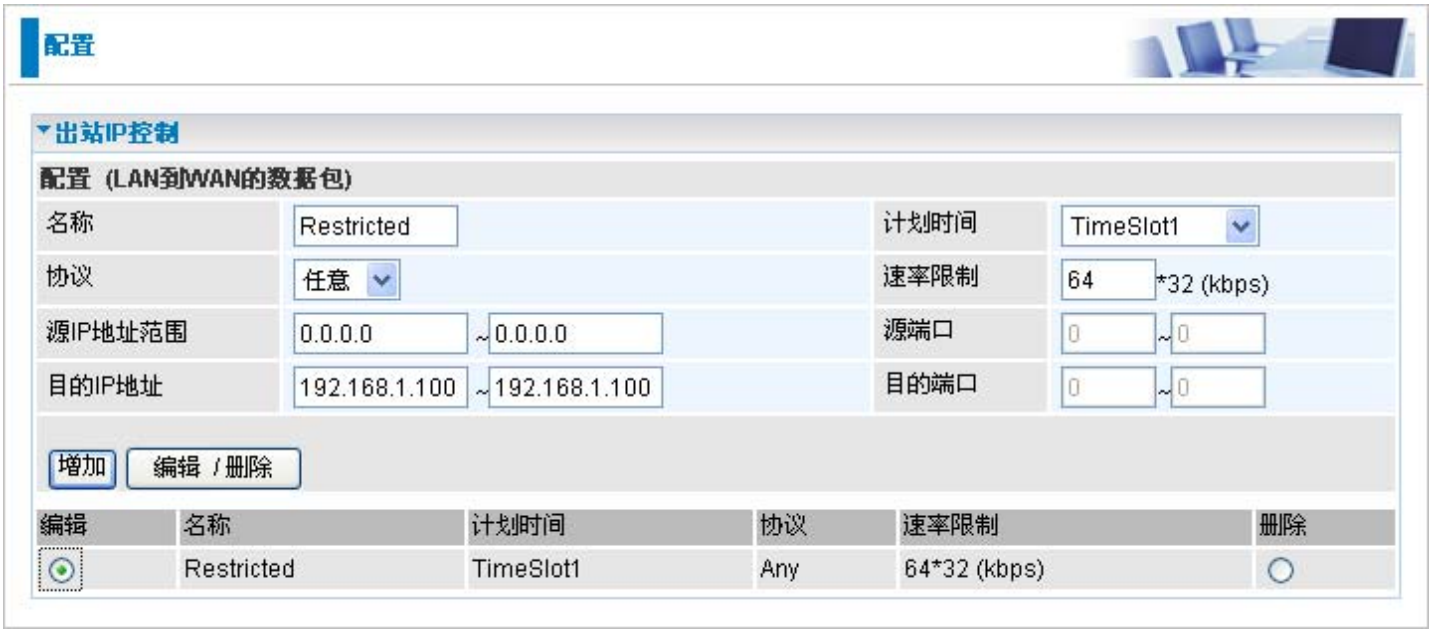
语音应用：128kbps (4*32kbps)

限制应用：160kbps (5*32kbps)

其它应用：448kbps (14*32kbps)

6+4+14+5=29, 29*32kbps=928kbps

您的客户或朋友有时会上传文件到 FTP 服务器，从而占满下行流带宽。以下设置可以对限制应用使用的带宽进行限制。



虚拟服务器（即端口转发）

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，请参考著名端口部分。服务器通常都遵循著名端口的定义，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（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），然后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，您的公共可访问 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。

将设备配置成虚拟服务器，当远程用户通过公共 IP 地址 (WAN) 访问 Web 或 FTP 时，可以自动转到本地 LAN 服务器上。根据所请求的服务（TCP/UDP 端口号），设备将外部服务请求重导向到适当的 LAN 服务器上。

添加虚拟服务器

NAT（网络地址转换）是路由器的天然 Internet 防火墙，使用 NAT 可以阻止外部用户访问您的网络。如果您没有专门创建虚拟服务器条目、将端口转发到网络上的 PC，那么所有外来连接都指向路由器。

如果服务器允许外部用户访问内部服务器，如 web 服务器、FTP 服务器、Email 服务器或游戏服务器，路由器可作为虚拟服务器使用。您可以在本地服务器上设置服务使用的端口号，如 web/HTTP（80 端口）、FTP（21 端口）、Telnet（23 端口）、SMTP（25 端口）或 POP3（110 端口）。当指定端口收到外来访问请求后，便将请求转给相应的内部服务器。

应用：用户自定义用来标识条目的名称。或单击**应用**下拉菜单，选择现有的预定义规则。

选择：有 20 条预定义规则可供选择。选择以后，将填写应用、协议、外部/重定向端口。

协议：虚拟服务器支持的协议。除指定端口外，您还需要指定使用的协议。使用的协议根据特定应用来定。大多数应用使用 TCP 或 UDP 协议。

时间表：用户自定义启用虚拟服务器的时间段。您可以指定虚拟服务器的使用时间表或选择一**直开启**。有关安装及详细信息，请参阅**时间表**部分。

外部端口：访问虚拟服务器时，远程/ WAN 端使用的端口号。

内部 IP 地址：LAN 中的私有 IP，由虚拟服务器应用提供。**选择**下拉菜单中列出了当前所有连接到网络的 PC。您可以通过候选列表为 PC 指定 I P 地址和 MAC 地址。

实例：

如果想一直通过 Web/HTTP 远程访问路由器，则需要启用 80 端口 (Web/HTTP)，并将端口映射到路由器的 IP 地址。所有来自远端的 HTTP 请求将被转发到 IP 地址为 192.168.1.254 的路由器上。由于端口 80 已被预定义，单击“**帮助**”旁边的**应用**。此时将弹出一个预定义规则列表窗口，选择**HTTP_Sever**。

应用：*HTTP_Sever*
时间表：*一直开启*
协议：*tcp*
外部端口：*80-80*
重定向端口：*80-80*
IP 地址：*192.168.1.254*

添加：单击以应用设置。

编辑/删除：单击以编辑或删除虚拟服务器应用。

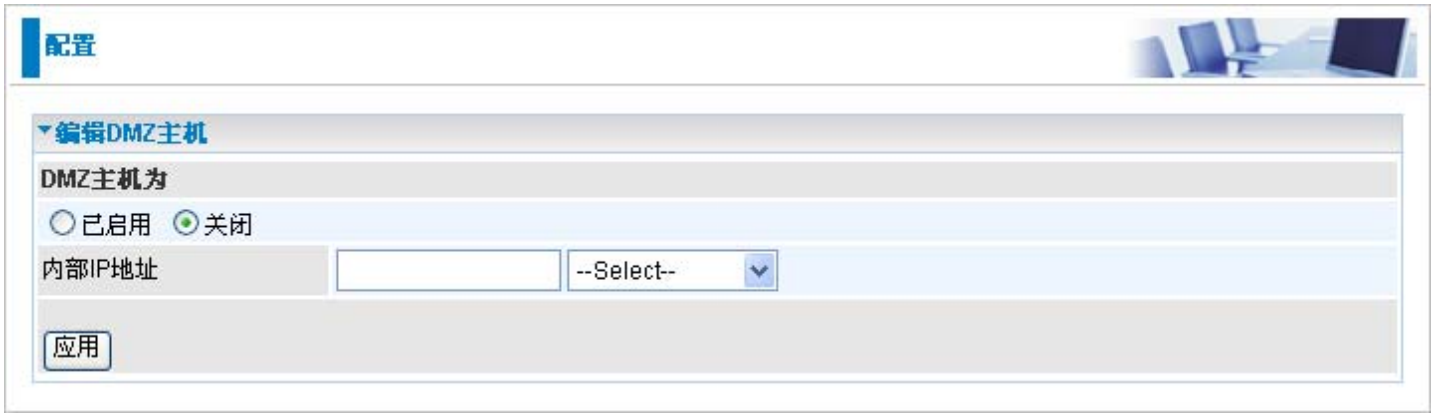
使用端口映射就不能考虑安全性，因为外部用户可以连接到内部网络的 PC。因为这个原因，您需要使用特定的虚拟服务器条目用于应用请求的端口，而不是仅仅使用 DMZ 让所有的连接都能够通过公网 IP 访问到内部的 PC。

编辑 DMZ 主机

DMZ 主机就是暴露在 Internet 中的本地主机。当设置一个特定的内部 IP 地址作为 DMZ 主机，防火墙和 NAT 算法会检查所有进入的数据包，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。

注：暴露在 Inernet 中的本地计算机可能会面临各种安全风险。

转至配置 > 虚拟服务器 > 编辑 DMZ 主机



启用：它将激活 DMZ 功能。

禁用：如默认设置所设，它将禁用 DMZ 功能。

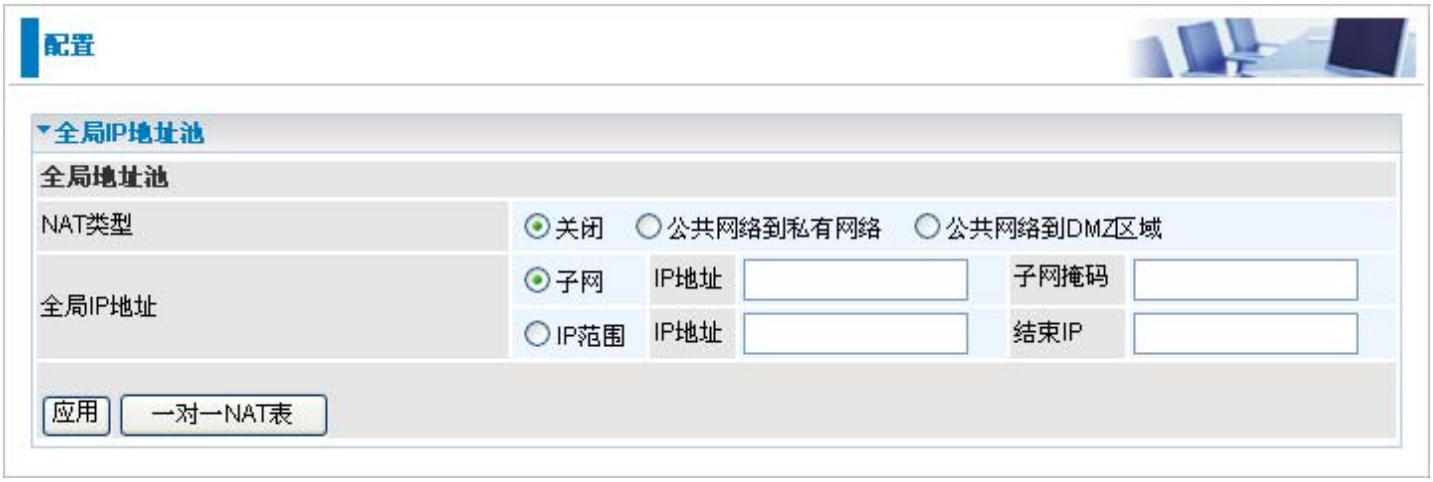
内部 IP 地址：选中**启用**单选按钮，给 DMZ 主机指定静态 IP 地址。请注意，这个 IP 将暴露在 WAN/Internet 中。

候选表：列出当前所有连接到网络的 PC。您可以通过候选列表为 PC 指定 IP 地址。

选择**应用**按钮应用更改。

编辑一对一 NAT（网络地址转换）

一对一 NAT 将特定的私有/本地 IP 地址映射到全局/公共 IP 地址。
如果 ISP 提供多个公共/WAN IP 地址，为了能够使用它们，您可以进行一对一网络地址转换。
转至配置 > 虚拟服务器 > 编辑一对一 NAT



NAT 类型：选择要使用的 NAT 类型。默认情况下，一对一 NAT 功能是**禁用**的。
全局 IP 地址

子网：ISP 提供的公共/WAN IP 地址的子网。如果 ISP 有提供，在这里插入子网地址，如果没有，使用 IP 范围方法。

IP 范围：公共/WAN IP 地址范围。如，起始 IP: 192.168.1.1，终止 IP: 192.168.1.10。
选择**应用**按钮应用更改。

单击一对一 NAT 表，创建新的一对一 NAT 规则：

应用：用户自定义用来标识条目的名称。或单击**选择**下拉菜单，选择现有的预定义规则。

选择：有 20 条预定义规则可供选择。选择后，将填写应用、协议和外部/重定向端口。

协议：虚拟服务器支持的协议。除指定使用的端口外，您还需要指定要使用的协议。使用的协议根据特定的应用来定。大多数应用使用的是 TCP 或 UDP 协议。

时间表：用户自定义启用虚拟服务器的时间段。您可以指定虚拟服务器的使用时间表或选择**一直开启**。有关安装及详细信息，请参阅**时间表**部分。
全局 IP：定义应用的公共/ WAN IP 地址。全局 IP 地址必须在全局 IP 地址字段空白处定义。

外部端口：访问虚拟服务器时，远程/ WAN 端使用的端口号。

重定向端口：LAN 中的本地服务器使用的端口号。

内部 IP 地址：LAN 中的私有 IP，由虚拟服务器提供。候选表列出当前所有连接到网络的 PC。您可以通过候选列表为 PC 指定 IP 地址。

选择**添加**按钮，应用更改。

实例：著名端口和注册端口列表

互联网地址指派机构 (IANA) 是为 Internet 协议分配唯一参数值的中央协调机构。

端口范围从 0 到 65535，但端口 0 到 1023 是具有预定功能的端口，叫做“著名端口”（请参阅表 5）。注册端口从 1024 到 49151。其余端口叫做动态或私有端口，从 49152 到 65535。

有关详细信息，请参阅 IANA 网站：**http://www.iana.org/assignments/port-numbers**

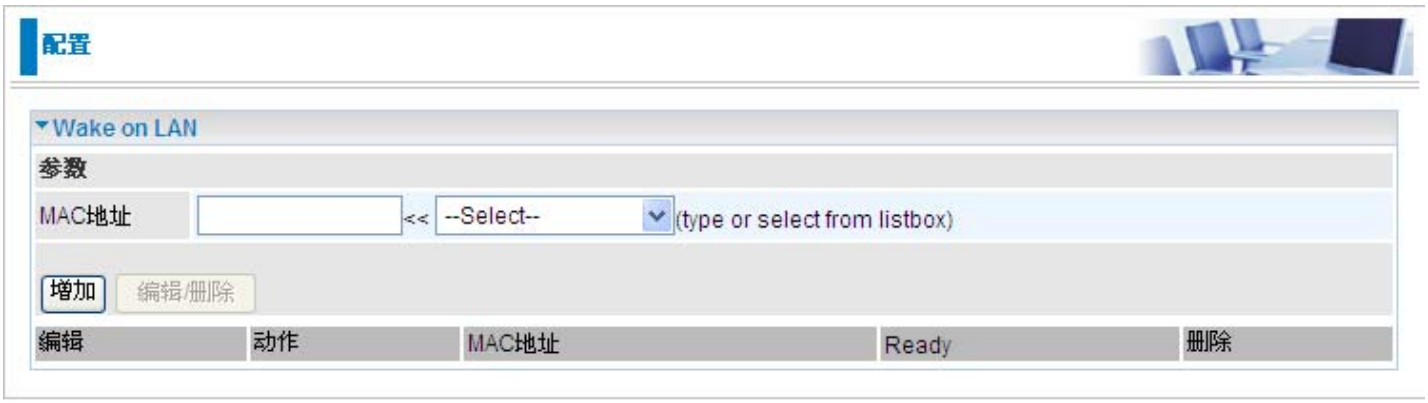
有关如何决定列表上的通用应用该使用哪个私有端口号的帮助，请参阅 **http://www.billion.com** 上的 FAQ（常见问题）。

表 5：著名端口和注册端口

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	远程登录
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	World Wide Web HTTP
110	TCP	POP3（邮局协议第 3 版）
119	TCP	NEWS（网络新闻传输协议）
123	UDP	NTP（网络时间协议）/NTP（简单网络时间协议）
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Wake on LAN

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。



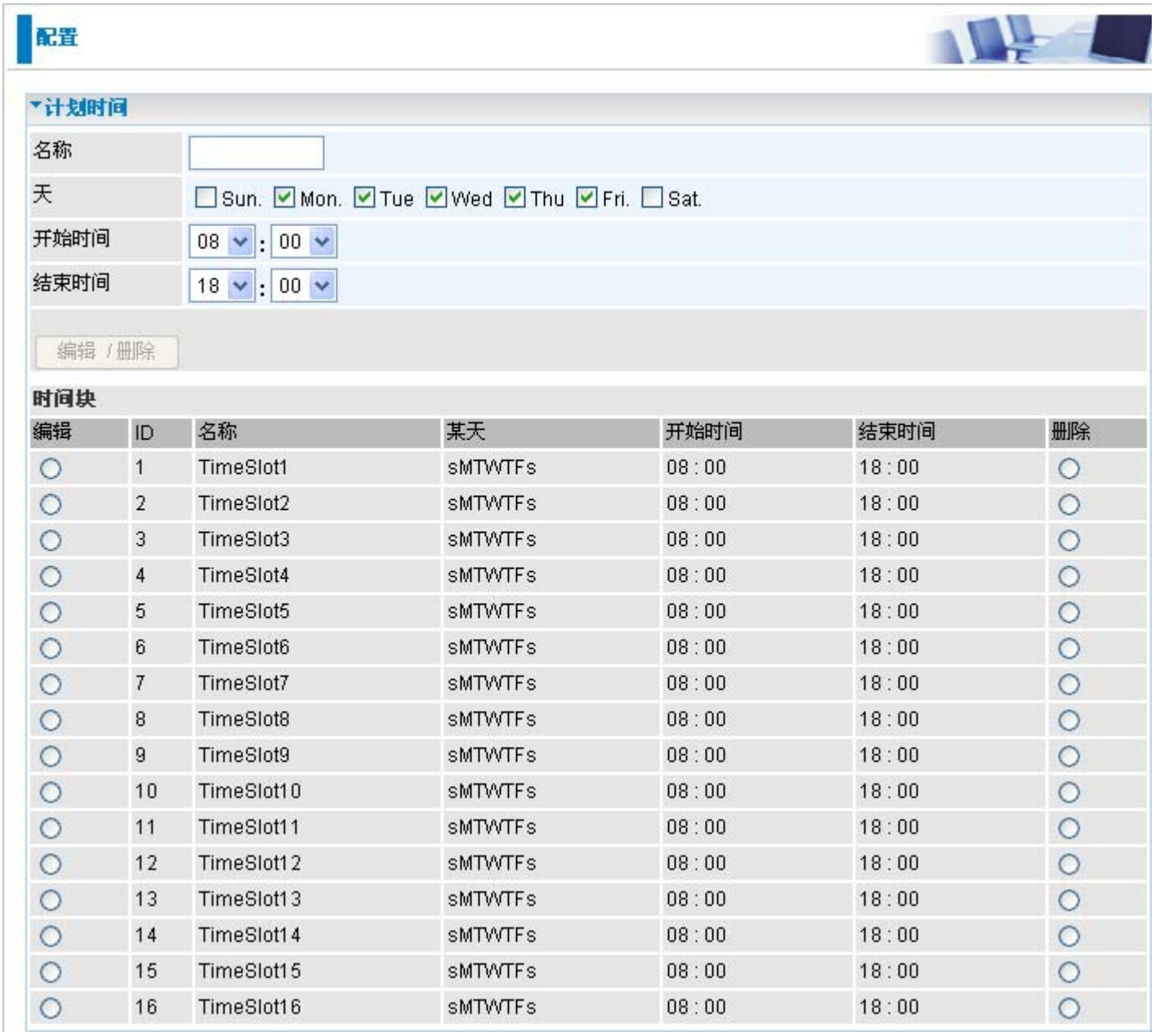
MAC 地址：输入目标计算机的MAC 地址，您可以从 MAC 地址的下拉菜单中直接选择。

：您可以从列表中选在MAC地址。

计划时间

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。



配置时间表

编辑时间槽

1. 选择要编辑的时间槽（ID 1 到 ID 16），单击**编辑**单选按钮。

注：所选择的天数必须以大写字母表示。小写字母表示这一天没有被选择，因此也不会应用任何规则。

2. 详细的时间槽设置如下图所示。

ID：时间槽的编号。
名称：用户自定义的时间表描述名称。
天数：默认设置为星期一到星期五。您可以指定天数。

开始时间：默认是 8:00 AM。您可以指定时间表的开始时间。

结束时间：默认是 18:00 (6:00 PM)。您可以指定时间表的结束时间。

删除时间槽

单击想要删除时间槽前面的**删除**单选按钮，然后单击**编辑/删除**按钮，确认删除了时间配置，如清除了**天数**，并恢复到开始时间/结束时间的默认设置。

高级

用户可以在**高级**配置选项中配置路由器的高级功能。如果用户不明白这个功能可以不用配置路由器，除非有支持人员的支持。

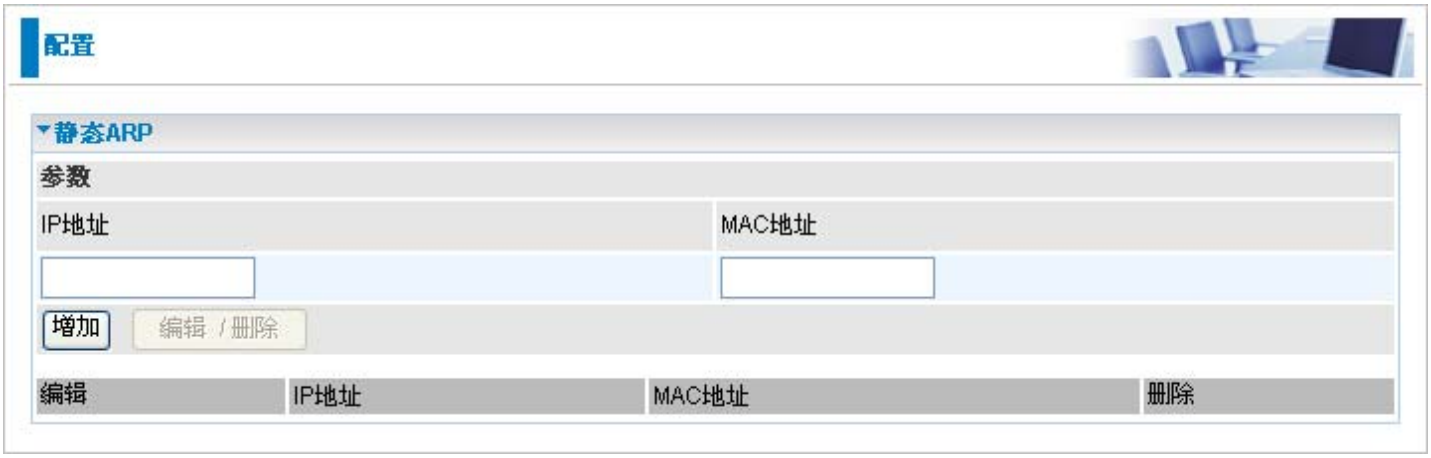
高级部分包括以下几部分：**静态路由、静态 ARP、动态 DNS 系统、检查电子邮件、设备管理、IGMP** 以及 **VLAN 桥接.**

静态路由

转至配置 > 高级 > 静态路由。

目的地：目的子网 IP 地址。
子网掩码：基于目的子网 IP 的子网掩码的目的 IP 地址。
网关：转发数据包的下一跳 IP 地址。
接口：选择转发数据包的接口。
开销：也就是路由的跳数。通常设为 1。

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 ADSL 连接的主机，使得任何人可以通过 DNS 名访问到你，而不是随时会变得动态 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。

首先，您需要到动态域名解析提供商的网站上注册一个账号，比如 **http://www.dyndns.org/**。

支持 5 种动态域名解析服务。

动态域名解析系统：

禁用：选中以禁用动态域名解析功能。

启用：选中以启用动态域名解析功能。以下是必填字段，启用后被激活。

动态域名解析服务器：选择您申请账号的 DDNS 服务器。
域名、用户名和密码：输入注册的域名、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。

设备管理

通过对设备管理进行高级配置，使您可以控制路由器的安全选项和设备监控功能。

设备主机名

主机名：指定主机名称。

注：主机名必须至少由两个单词组成，通过‘.’连接。

实例：
主机名：homegateway ==> 错误
主机名：home.gateway 或 my.home.gateway ==> 正确

内置 web 服务器（2 个管理账号）

HTTP 端口：路由器的内置 Web 服务器（用于基于 web 的配置）使用的端口号。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。

管理 IP 地址：您可以指定用来登录和访问 web 服务器的 IP 地址。将 IP 地址设置为 0.0.0.0，将关闭IP 地址限制，用户可以使用任何 IP 地址登录。

到期自动注销：指定系统自动注销用户配置会话的时间。

例如：

用户 A 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为 100 秒。这样就只允许用户 A 在浏览器中输入 **http://192.168.1.254:100** 从 **192.168.1.55** 访问。100 秒钟以后，设备将自动注销用户 A。

通用即插即用 (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。

禁用：选中以禁用路由器的 UPnP 功能。

开启：选中以开启路由器的 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。

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 和 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。

陷阱社区：为陷阱社区指定名称和 IP 地址。将社区串与配置文件中输入的串进行核对。一旦串名匹配，使用这个 IP 地址的用户将被发送到 SNMP 陷阱。

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。

支持陷阱：冷启动、认证失败。

以下列出了支持的 MIB：

From RFC 1213 (MIB-II)

系统组

接口组

地址转换组

IP 组

ICMP 组

TCP 组
UDP组
EGP （不可用）

SNMP 组

From RFC 1650 (EtherLike-MIB)

dot3stats

From RFC 1493 (Bridge MIB)

dot1 dBase 组

dot1 dTp 组

dot1 dStp 组（如果配置生成树）

From RFC 1472 (PPP/Security MIB)

PPP 安全组

From RFC 1473 (PPP/IP MIB)

PPP IP 组

From RFC 1474 (PPP/Bridge MIB)

PPP 桥接组

From RFC 1573 (IfMIB)

ifMIBObjects 组

From RFC 1695 (atmMIB)

atmMIBObjects

From RFC 1907 (SNMPv2)

only snmpSetSerialNo OID

From RFC 1471 (PPP/LCP MIB)

pppLink 组

pppLgr 组（不可用）

IGMP

IGMP 全称 *Internet 组管理协议*，用于管理组播组中的主机。

IGMP 转发：接收组播数据包。默认为**开启**。

IGMP 探听：允许交换的以太网/无线网络检查并做出正确的转发决定。默认为**禁用**。

VLAN 桥接

您可以创建 VLAN 组并指定组的成员。

编辑：编辑所选 VLAN 组中成员的端口。

创建 VLAN：再创建一个 VLAN 组。

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 5 章：故障排除

如果 ADSL 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。
如果忘记登录用户名或密码。	尝试默认的登录和密码，参阅第 3 章。如果不行，您可以按住路由器后端面板上的 Reset 针孔按钮超过 6 秒钟，将路由器恢复到出厂默认设置。

WAN 接口的问题

问题	建议解决办法
PVC 连接（线路同步）初始化失败	确保从 ADSL 端口到墙上插座的电话线是正确连接的。路由器的前端面板的 ADSL LED 是亮着的。确保您的 VPI，VCI，封装类型和多路复用类型设置和 ISP 提供的一样。重新启动路由器。如果您仍然出现问题，您要与您的 ISP 确认设置。
ADSL 线路同步频繁丢失（断线）	查看是否所有其他设备（例如电话线，传真机，模拟调制解调器）和您的路由器都连接到同一个电话线，且在他们之间安装了线路分离器和墙上插座（除非您在使用中心分离器或由有资质的电工安装的中心分离器），要确保所有线路过滤器都正确安装。没有线路过滤器或线路过滤器安装不正确将导致频繁断线。如果您有返厂警告系统，您应该联系您的安全提供商，让支持人员做必要的更改。

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。请确保在卸载了所有软件防火墙之后进行故障排错。
	确保路由器和工作站之间的 IP 地址和子网掩码是一致的。

附录：产品技术支持和联系信息

大部分问题，可以参阅本手册中的**疑难排解**部分解决。如果仍无法解决，请联系您购买产品的经销商。

联系 Billion

全球网站：

http://www.billion.com