启博 MR 系列 VPN 防火墙用户手册

商标、版权声明

目录

第一章 产品概述

感谢您选用深圳市启博网络有限公司出品的MR系列VPN防火墙网关，本手册以启博MR-5100为例进行设置，由于各型号产品硬件和软件规格存在差异，有涉及产品规格的问题需要和深圳市启博网络有限公司销售部联系确认。

1.1.产品概述

启博MR-5100（包括含MR-1000/1300/1300S/2600等）是针对中小企业量身定制的多功能一体化VPN防火墙网关，集成VPN、防火墙、带宽控制、上网行为管理等功能，主要用于解决企业业务系统（如财务软件、ERP、进销存、OA、邮件系统等）的远程互联、移动办公、远程监控、工业控制等，设备内置启博目录服务寻址技术，不需要客户申请固定IP或动态域名，通过启博VPN的简单设置即可以把企业分布在不同地域的工作人员，连成一个大的局域网

1.2.支持的标准和协议

- IEEE 802.3 10Base-T
- IEEE 802.3u 100Base-TX
- CSMA/CD、pppoE、PPP、IP、ARP、DHCP、TCP、UDP、HTTP、FTP、DNS、PPTP、L2TP、IPSEC、ESP、GRE

1.3. 工作环境

温度：

- 0° 至 50° （工作）
- -40° 至 70° （储存）

湿度：

- 10% 至 90% RH 无凝结（工作）
- 5% 至 95% RH 无凝结（储存）

第二章 硬件安装

2.1. 系统要求

- 标准的个人计算机
- 具备至少 1 个以内网网络适配器（网卡和网线）
- 操作系统：微软 Windows，linux 或 MAC 操作系统
- 具备标准的 WEB 浏览器

2.2 恢复默认

如果想恢复出厂设置，请在路由器通电情况下，用圆珠笔或牙签按压设备面板上的 RESET 键，保持 15 秒，当看到所有网口灯都全部亮一下时，说明设备开始重启自动恢复出厂设置，过一会就可以进去设备重新配置了，设备的默认地址是 192.168.10.1 。

2.3.硬件安装过程

- 给设备接上电源并打开设备上的电源开关，设备上的 PWR 灯会亮起。
- 把连接外网的网线（也称进线）接到 VPN 网关的 WAN 口（或 WAN1 口），连接电脑的网线接到 LAN1-LAN4 任意接口。
- 连接好后，检查 PWR 提示灯及对应插网线的接口（WAN 和 LAN）网口指示灯是否点亮。
-
- 小提示：外网线包括 ADSL Modem(俗称：猫)接出来的网线，或者互联网运营商（电信、联通、移动、长宽等）直接拉进户的网线。

第三章 登入设备

你可以通过基于 WEB 浏览器的配置来管理 VPN 网关。要通过 web 浏览器配置 VPN 网关，至少要一台合理配置的电脑，通过以内网或者无线网络连接到 VPN 网关，**启博 MR 系列 VPN 网关的默认 IP 是 192.168.10.1，子网掩码 255.255.255.0，DHCP 服务器默认是开启的**。在设置 VPN 网关之前，确保电脑的设置是从 VPN 网关自动获取 IP 地址，参照下面的步骤来设置

3.1 Windows XP

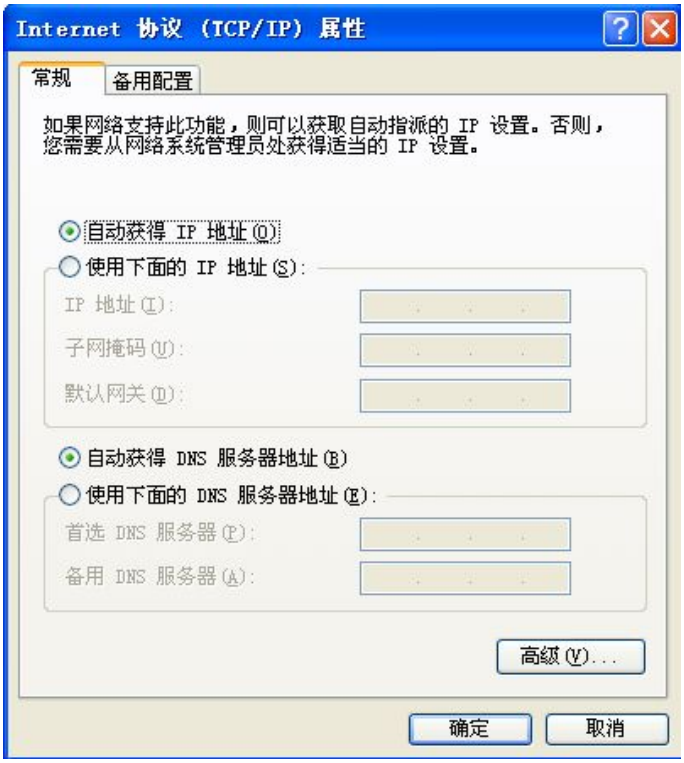
请按照下述步骤来配置你的电脑

3.1.1 在桌面上找到网上邻居图标，鼠标右键点击，选择属性

3.1.2 选择**本地连接**，右键点击**属性**

3.1.3 点击选择 **Internet 协议（TCP/IP）**， 再点击属性按钮

3.1.4 选择自动获得 IP 地址和自动获得 DNS 服务器地址，然后点击确定，关闭 Internet 协议（TCP/IP）属性窗口



3.1.5 点击确定，关闭本地连接属性窗口后生效

3.2 Windows Vista/Windows 7

请按照下述步骤来配置你的电脑

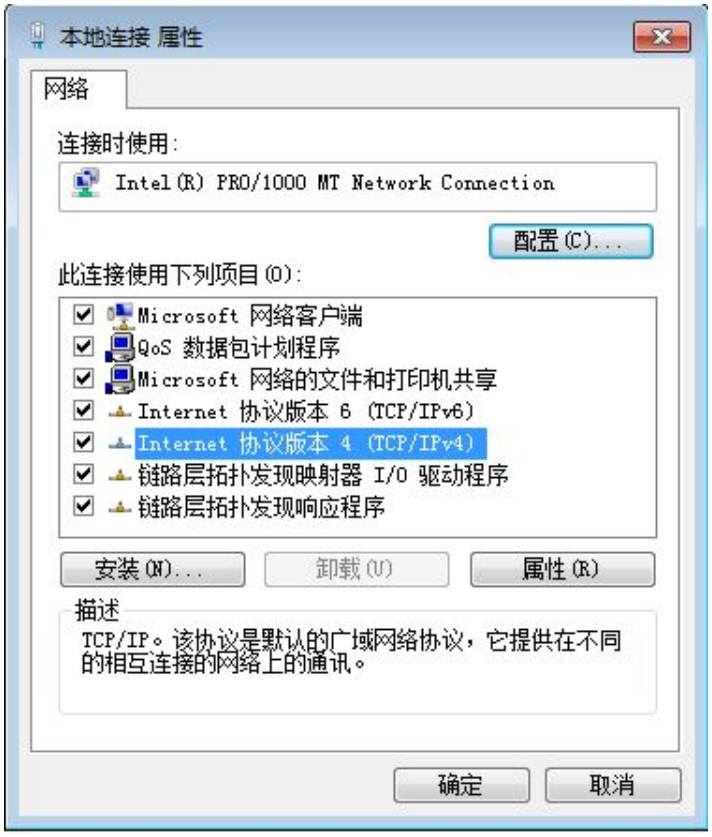
3.2.1 开始---控制面板

3.2.2 点击 查看网络状态和任务

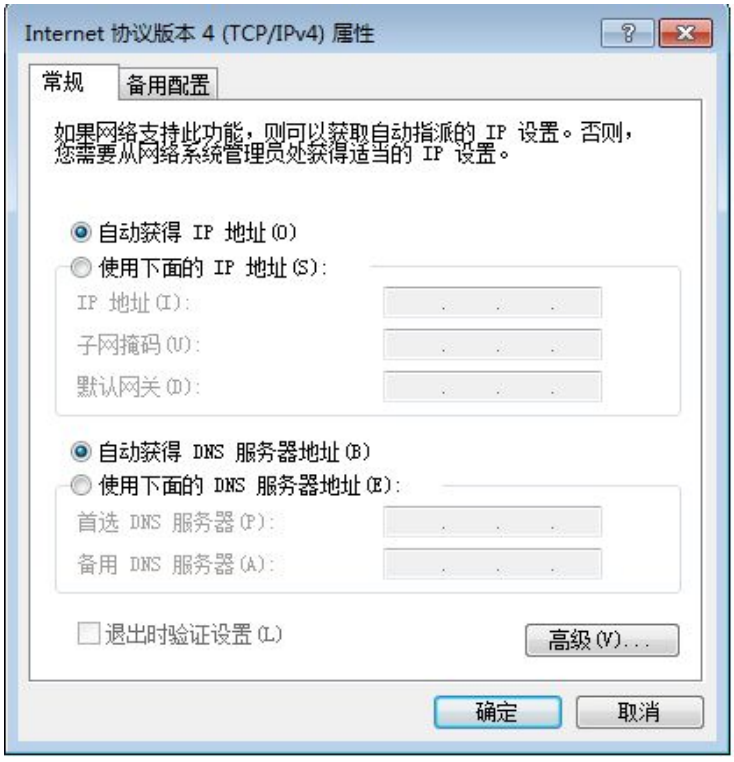
3.2.3 点击窗口最左边的**更改适配器设置**

3.2.4 右键点击 本地连接

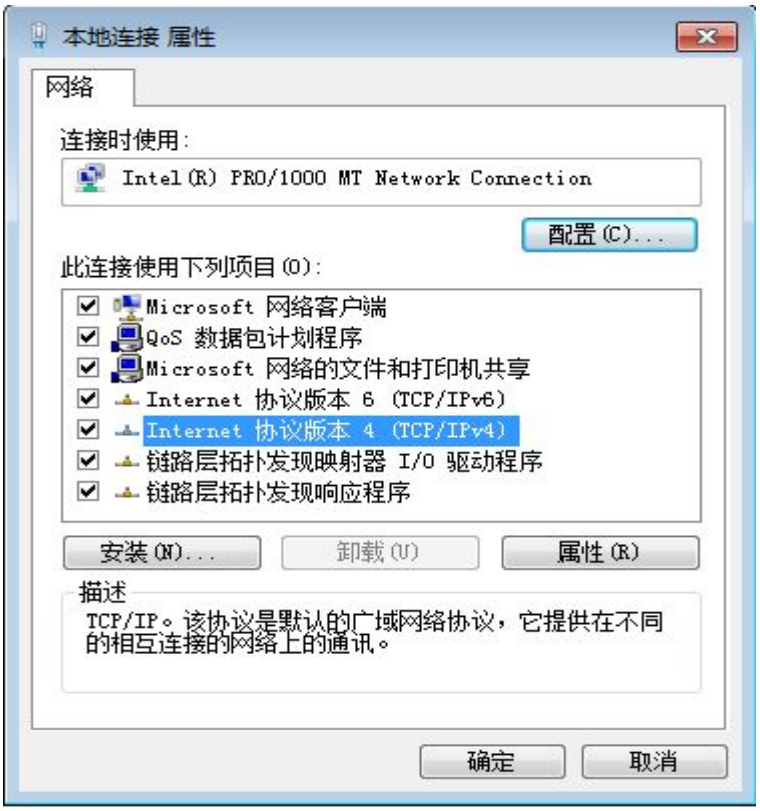
3.2.5 点击 Internet 协议版本 4（TCP/IP）,然后点击属性按钮



3.2.6 选择自动获得 IP 地址和自动获得 DNS 服务器地址，然后点击确定关闭 Internet 协议（TCP/IP）属性窗口



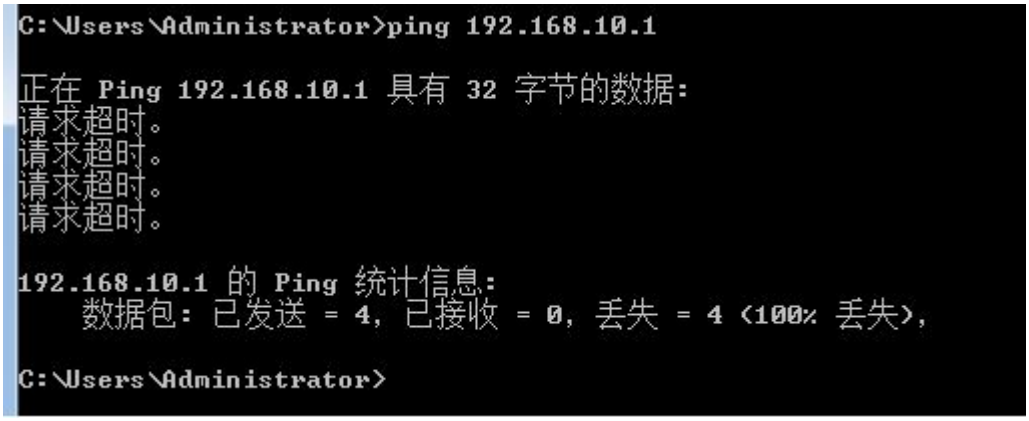
3.2.7 点击 确定 关闭本地连接窗口



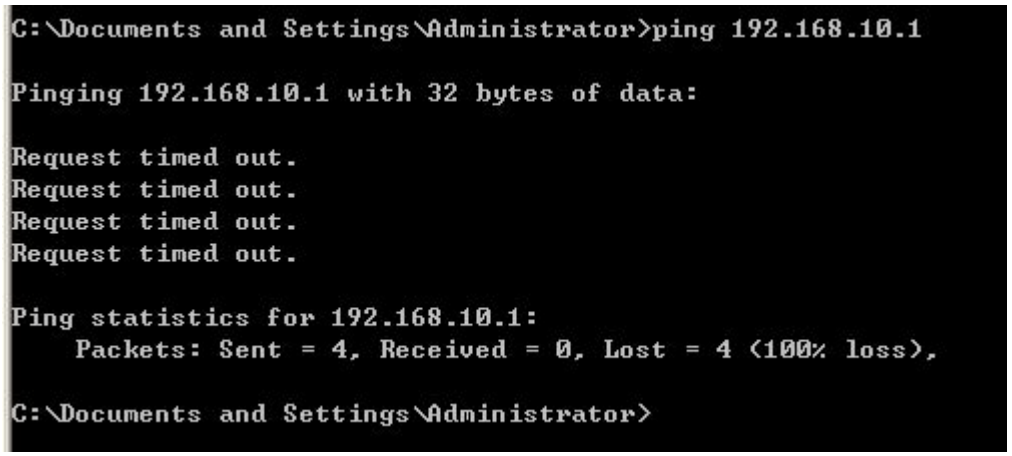
3.3 测试连接

设置完 TCP/IP 协议后，用 Ping 命令来验证电脑是否可以与 VPN 网关通信，要执行 Ping 命令，打开 DOS 窗口，在 DOS 提示里 Ping 启博 VPN 网关的 IP 地址
在桌面左下方，开始--运行，输入 cmd 并回车，在 DOS 提示示，输入下述命令并回车，如果命令窗口返回类似于下面的内容。

那么 VPN 网关与电脑之间的连接就成功的建立了。
如果电脑和 VPN 设备连接有问题或电脑的本地连接设置不正确，将返回下述内容



或者



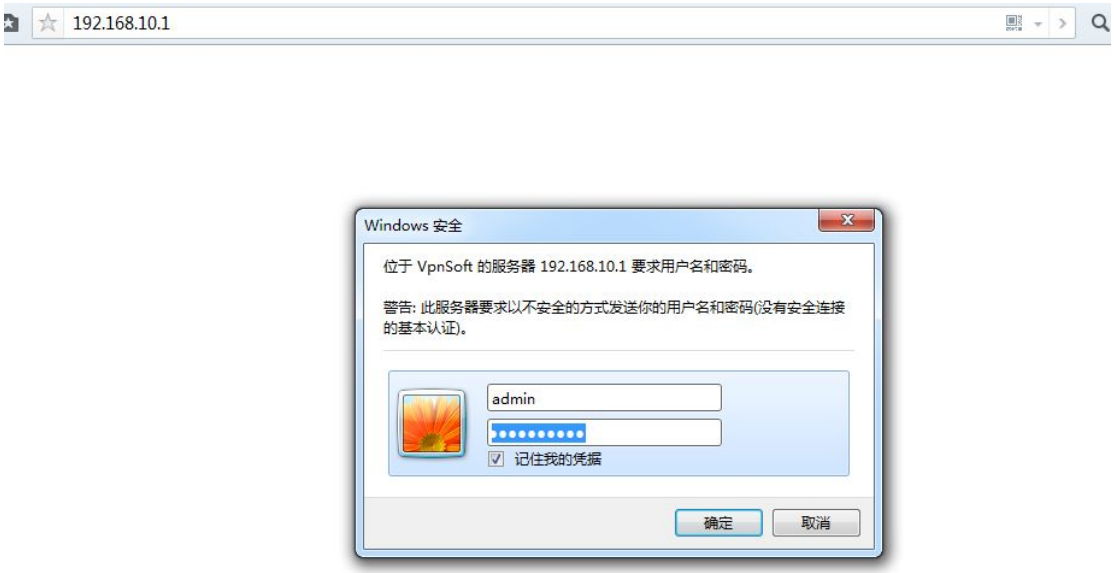
这里要确认你的电脑的网络设置是否正确，并且检查电脑与 VPN 网关之间的线路连接。

3.4 登入

启博 VPN 网关提供基于浏览器（IE、firefox、chrome、腾讯 TT 等）的配置界面，这种配置方案适宜于任何 Windows、Linux(unix)、苹果系统等。

3.4.1 打开桌面上的 Internet Explorer 浏览器或其他浏览器，在地址栏里输入 http://192.168.10.1，点击 回车键

3.4.2 在弹出的窗口中输入用户名：admin 密码：admin 注意都为小写，按下确认键。如果你需要经常配置 VPN 网关，可以勾选记住我的凭据。



进去后就可以看到设备里的基本信息，如下图所示：

包含设备型号、设备编码、固件版本、VPN 授权信息等内容。

第四章 配置设备

4.1 网络

4.1.1 宽带设置

这里是配置 VPN 网关的上网方式，只有这里设置正确后，VPN 网关才能上网，也才能使用 VPN 网关的所有功能。

宽带连接类型分为四种：静态 IP、DHCP、PPPOE 拨号、透明模式

4.1.1.1 静态 IP：这种上网方式，一般是光纤固定 IP 地址或其他指定 IP 地方的上网方式时使用

其中：
IP 地址：是 VPN 网关对广域网的 IP 地址，即 ISP 提供给你的 IP 地址，不清楚可以向 ISP 询问。
子网掩码：是 VPN 网关对广域网的子网掩码，即 ISP 提供给你的子网掩码，不清楚可以向 ISP 询问。
网关：填入 ISP 提供给你的网关，不清楚可以向 ISP 询问。
静态 DNS: 填入 ISP 提供给你的 DNS 服务器，不清楚的可以向 ISP 询问，正常实在不清楚的情况下，输入谷歌提供的 DNS 4.4.4.4 和 8.8.8.8 也是可以的。

4.1.1.2 DHCP：一般小区宽带或 VPN 网关当二级路由器时使用，会使用 DHCP 自动配置方式上网，如下图，DHCP 自动配置情况下，不需要输入任何信息，MTU 值也不需要修改，保存即可上网。

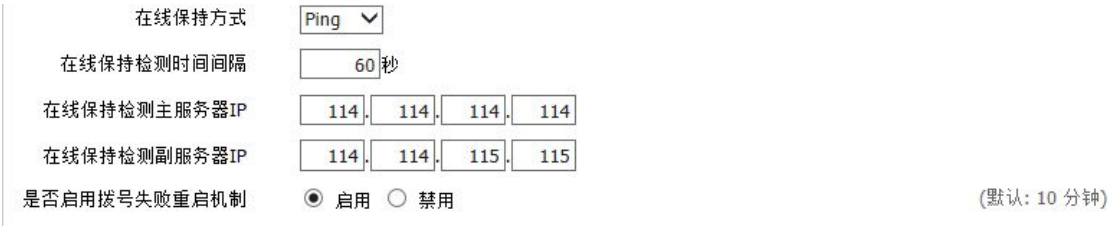
4.1.1.3 PPPOE 拨号：普通的电信或联通的 ADSL 上网方式使用，适用于绝大多数客户，只需要输入用户名和密码，其他选项按默认即可。

其中：
用户名：填入 ISP 为你指定的 ADSL 上网帐号，不清楚可以向 ISP 询问。
密　码：填入 ISP 为你指定的 ADSL 上网密码，不清楚可以向 ISP 询问。
MTU ：MTU 值缺省为 1492，如非特别需要，一般不要更改。
强制重新连接：缺省为禁用，有个别情况下，需要不断变换外网 IP 的客户，可以通过强制重新连接，让 VPN 网关获取不同的外网 IP 地址。

4.1.1.4 透明模式： 透明模式是将 VPN 接在路由器后，不替换客户现有路由器的一种接法，此种配置稍复杂，详见附录

- 双 WAN 配置：某些客户申请了多条宽带，启博 VPN 网关部份产品是支持双 WAN 接入的，下图是常用的两条 ADSL 宽带接入的配置方法。双 WAN 接入时宽带物理线路一定要和对应的帐号和密码完全匹配设备接口，如果是把两条宽带线路的帐号和密码给输颠倒，则两条宽带都无法上网的。

- 在线保持：在线保持是做为一个定时检测机制，确认外网线路是否连通，如果发生断线则会自动启动重新连接的动作，最大程度上保障 VPN 网关与互联网的连通性。



4.1.2 局域网

这里是修改路由器 IP，设备出厂的 IP 地址是 192.168.10.1，客户可以根据自己单位的具体情况进行修改，修改后，保存设备并应用生效。

4.1.3 DDNS

启博 VPN 集成 DDNS 寻址服务功能，客户无需自己申请动态域名或固定 IP，直接用设备本身自带的 DDNS 即可实现 VPN 的寻址。

启博 DDNS 包括三个 DDNS，分别是 DDNS1 和 DDNS2、DDNS3，三个同时工作，保证寻址的稳定可靠。

4.1.4 MAC 地址克隆

有些 ISP 对客户上网的设备进行了 MAC 绑定，只有绑定的 MAC 地址才能拨上号，这里可以修改 LAN 口及线路 1 和线路 2 的 MAC 地址。

4.1.5 多 DHCP

个别企业内部做了多个网段，不同部门使用不同的网段，像酒店里办公网络和客房的网络是相互隔离的，启博 VPN 网关集成多网段功能，实际三层交换机的普通功能。

4.2 转发规则

4.2.1 虚拟服务

虚拟服务是指向外网开放某些资源供第三方远程访问，比如常见的公司内部建一个 OA、FTP 服务器，让公司的同事在外也可以访问到，下面是 sql server 远程访问的例子。

添加规则直接点“添加”，名称可以任意写，协议分为 TCP、UDP 或两者；来源 IP 是指访问者的外网 IP 地址，一般留空，如果填写后，就只有那个 IP 地址的用户才能访问。

4.2.2 DMZ

DMZ 又称为非军事化管理区，在某些特殊情况下，我们需要把内网中的一台计算机完全暴露给互联网，以实现双向通信。

4.2.3 端口触发

某些程序需要多条连接，如网络游戏、视频会议、网络电话等，由于防火墙的存在，这些程序无法在简单的 NAT 路由器下工作，端口触发使得这样的应用程序能够在 NAT 路由器下工作，当一个应用程序在触发端口上发起连接时，在开放端口中的所有端口就会打开，以备后续连接。

4.2.4 UPNP

UPNP 的英文全称是 Universal Plug and Play，即通用即插即用协议,是为了实现电脑与智能的电器设备对等网络连接的体系结构。而内网地址与网络地址的转换就是基于此协议的。

4.3 第三方互联

4.3.1 IPSEC 配置

IPSEC VPN 是标准的网络间互联协议，这里可以和任何一家 VPN 防火墙厂商的，标准的 IPSEC VPN 网关进行对接，

下面实例说明，一边地 192.168.10.0 的网络，另一个地方是 192.168.1.0 的网络，分别在两个不同的地方，我们把 192.168.10.0 的 VPN 配置成服务端，另一方配置为客户端，下图是服务端的配置说明

对方 VPN 客户端的配置如下：

配置完毕，点应用，即可升效，两个网络之间建立隧道连接，并实现双向互访。

4.3.2 L2TP 客户端

设备做为 L2tp VPN 客户端和服务器进行连接，服务器地址可以填服务器端的域名或 IP 地址，用户名和密码是由 L2TP VPN 服务器端分配。

- 服务器地址：L2tp 服务器端的 IP 地址或域名。
- 用户名：管理员分配的连接帐号名称。
- 密　码：密理员分配的连接帐号对应的密码。
- NAT ：启用是可以让 VPN 网关下的设备可以访问 L2tp 服务器端，禁用则只有主机可以和 L2tp 服务器端通信。
- 模式：ISP 模式是指 L2tp 客户端的设备通过 L2tp 服务器端的宽带上网；企业模式：只有访问 L2tp 服务器端的资源时才走 vpn 隧道，一般选企业模式。
- 服务器网段：是指 L2tp 服务器端内网网段。
- 服务器掩码：是指 L2tp 服务器端内网段段的子网掩码。
- IPSEC 封装：不启用是纯 L2tp 模式，启用则是 L2tp+IPsec 隧道模式。
- 预共享密钥：和 L2tp 服务器端保持一致。

4.3.3 L2TP 服务器

L2TP 服务器的客户端可以是 PC 机、安卓、苹果 ISO 等客户端。

- L2TP 服务器地址：这里可以任意设置，但不要和路由器 LAN 口地址相同。
- L2TP 客户端地址池：客户接过来时从这个地址池里动态获取一个 IP。
- IPsec 封装：一般选启用。
- 预共享密钥：是指 L2TP 采用 PSK 认证时，动态认证交换的证书密钥。
- 用户管理：L2tp 客户端接入的帐号和密码管理。

4.3.4 PPTP 客户端

该设备做为 PPTP 客户端与服务器端进行连接。

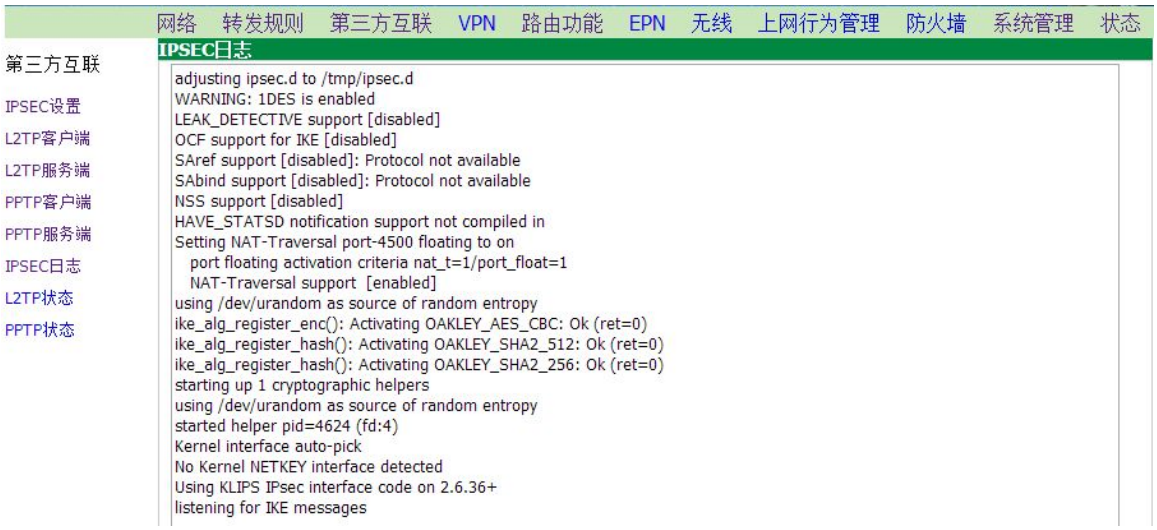
- 启用 PPTP 客户端功能：开启或禁用 PPTP 客户端连接
- 服务器 IP 或域名：可以输入服务器的合法的公网 IP 或动态域名
- 用户名: PPTP 服务器分配

- 密 码：PPTP 服务器分配
- 加 密：VPN 通讯时以明文传送还是加密后再传送
- NAT： 是指该设备下局域网的计算机通过本连接访问 PPTP 服务器端资源。
- 远程子网：PPTP 服务器端内网的网段。
- 远程子网掩码：PPTP 服务器端内网的网段的子网掩码。

4.3.5 PPTP 服务端

- 强制 MPPE 加密是可选项，服务器如果选择了启用，客户端也应启用，只要两部保持一致就行了。
- 服务器 IP：可以任意设置没有具体要求，也可以直接按上图来设置
- 客户端 IP：是指 pptp 客户端拨入后，获取的 IP 地址，这里是设置一个区间，也就是一段 IP 地址，和 pptp 服务器 IP 在相同网段，但不包含服务器 IP。
- 用户管理：添加用户帐号和密码，保存设置并应用后才升效。

4.3.6 Ipsec 日志



这里可以查看 ipsec vpn 连接日志，可以查看到 ipsec vpn 的连接过程，及各种错误信息提示。

4.3.7 L2TP 状态

这里可以要看 L2TP 客户端拨入 L2TP 服务器的情况，也可以显示本设备做为 L2TP 客户端与对端 L2TP 连接的情况，

删除：是可以断开当前接入的客户端，也可以断开本端的客户端与远程的连接。

4.3.8 PPTP 状态

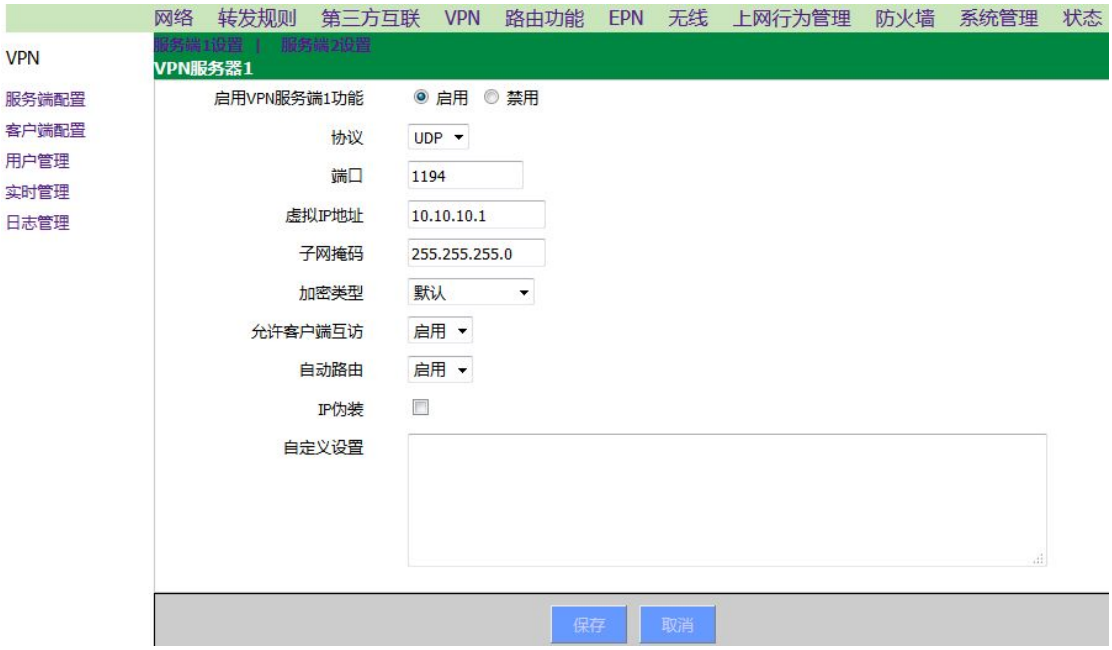
这里可以要看 PPTP 客户端拨入 L2TP 服务器的情况，也可以显示本设备做为 PPTP 客户端与对端 PPTP 连接的情况，

删除：是可以断开当前接入的客户端，也可以断开本端的客户端与远程的连接。

4.4 VPN 配置

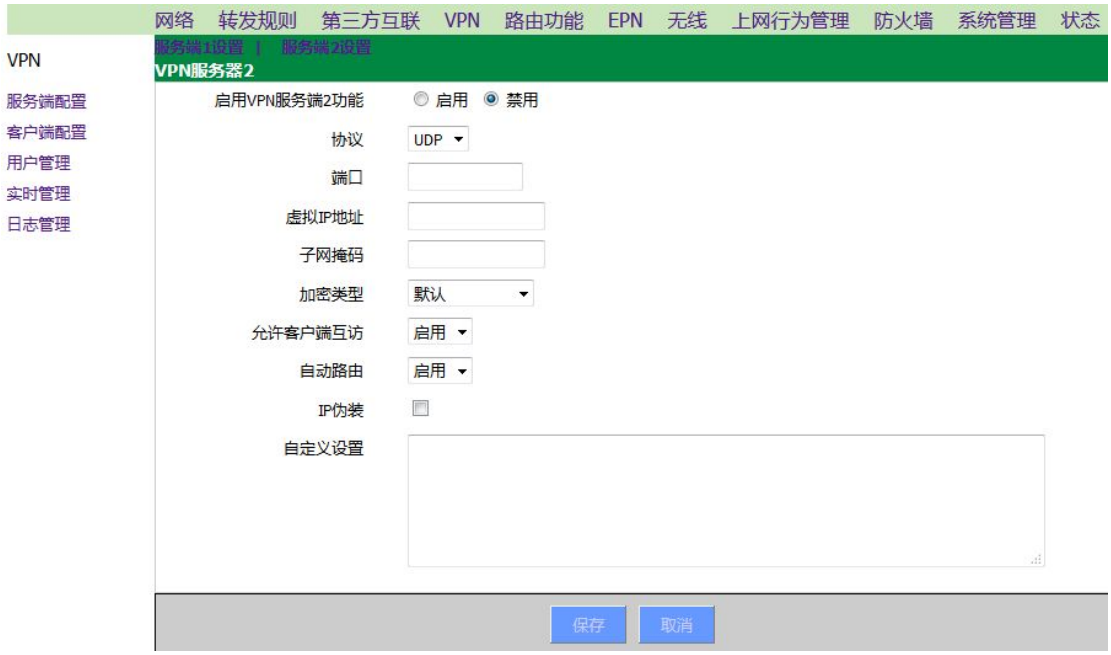
4.4.1 服务器设置

启博 MR 系列的 VPN 防火墙网关，是独特的 VPN 双服务器，两个 VPN 服务器可以同时工作，互不影响，一台设备当作两台设备使用，不同客户端可以接入服务器端 1 也可以接入服务器端 2，使用更方便。



- **协　　议**：UDP、TCP 可选，客户端须与服务器端保持相同。
- **端　　口**：只要是空闲的端口号都可以，客户端须与服务器端保持相同。
- **虚拟 IP 地址**：VPN 服务器虚拟接口的 IP 地址，可以任意设置，比如设为：10.10.10.1
- **子网掩码**：VPN 服务器虚拟接口 IP 的网络网掩码，一般为 255.255.255.0
- **加密类型**：支持默认、AES、BLOWFISH 三种可选，客户端需与服务器端保持一致

- **允许客户端互访**：是指接入同一个 VPN 服务器端的客户端之间能相互通讯。
- **自动路由**：VPN 服务器在客户端接入时，向客户端自动推送本端 LAN 接口路由表，使客户端能访问服务器端内网机器。
- **IP 伪装**：VPN 客户端连接成功后，访问服务器端内网服务器时，VPN 服务器将 VPN 的虚拟 IP 伪装成路由器 LAN 口 IP，躲过防火墙的检查，实现一些特殊的访问。
- **自定义设置**：这里可以输入一些特殊的配置参数，以实现某些特殊的功能需要，普通用户不需要设置。



- VPN 服务器端 2 和 VPN 服务器端 1 配置方法相同，需要注意的是，当 VPN 服务器 1 和 VPN 服务器端 2 同时启用时，服务器端 1 和服务器端 2 的协议和端口，不能同时相同，比如服务器端 1 是用 UDP 协议、1194 端口，服务器 2 就不可以用 UDP 协议、1194 端口，服务器端 2 可以用 TCP 协议、1194 端口，或者 UDP 协议、1195 端口。

- VPN 服务器端 2 和 VPN 服务器端 1 的虚拟 IP 地址一定不能相同。切记!!!

4.4.2 客户端设置

- 启博 VPN 客户端也是有 2 个，分别是客户端 1 和客户端 2，这样一台设备可以同时和两个不同的 VPN 服务器相连，比如一个 VPN 客户端 1 连公司总部，VPN 客户端 2 连接供应商的 VPN 服务器。

- **协　　议**：TCP、UDP 二选一，但必须与 VPN 服务器端保持一致。
- **端　　口**：必须与 VPN 服务器端保持一致。
- **加密类型**：支持默认、AES、BLOWFISH 三种加密方式，但必须与 VPN 服务器保持一致。
- **服务器地址**：是指 VPN 服务器端的地址，可以是 IP 也可以是动态域名
- **备用服务器地址**：是指 VPN 服务器端的备用地址，可以是 IP 也可以是动态域名，这个参数可以为空，也可以填写 VPN 服务器的另外 IP 或域名。
- **用户名**：VPN 服务器端分配的连接帐号
- **密　码**：VPN 服务器端分配的连接帐号对应的密码
- **与服务器端在相同子网**： 两台硬件之间互联时，如果想实现网上邻居功能时，需要启用这个选项。

VPN 客户端 2 与 VPN 客户端 1 配置方法相同，两者可以同时启用，但是不能同时连接同一个 VPN 服务器，否则容易造成路由表混乱。

4.4.3 用户管理

用户管理：用于添加、修改、删除 VPN 接入的帐号

- **用 户 名**：VPN 客户端连接时的帐户名称，只能是英文、数字、标点符号。
- **密　　码**：VPN 客户端连接时的帐户密码，只能是英文、数字、标点符号。
- **IP 地址**：VPN 客户端连接成功后获取的 IP 地址，这个地址必须与 VPN 服务器虚拟 IP 地址在相同网段，IP 地址不能重复。如果是要接入 VPN 服务器端 1，该 VPN 帐号的虚拟 IP 须与 VPN 服务器端 1 的虚拟 IP 地址在相同网段；如果是接入 VPN 服务器端 2，该 VPN 帐号的虚拟 IP 须与 VPN 服务器端 2 的虚拟 IP 地址在相同网段。
- **子网掩码**：VPN 帐号对应虚拟 IP 的子网掩码。
- **备　　注**：是对该帐号进行说明，以方便以后的管理

4.4.4 实时管理

实时管理，这里可以查看和管理 VPN 服务端 1、VPN 服务端 2、客户端 1、客户端 2 运行情况，也可以查看服务器端 1 和服务器端 2 上 VPN 客户端的连接情况。

VPN 服务器的连接状态上显示在线用户及他们连接时公网 IP、连接端口，隧道 IP、备注，一目了然非常直观。

4.4.5 日志管理

日志管理，是显示 VPN 运行时的日志内容，可以用于查看 VPN 运行及连接信息，可帮助管理员查看 VPN 连接过程，以及查看 VPN 连接时出现的问题。

4.5 路由功能

4.5.1 静态路由

- 目的网段：欲访问的主机所属的 IP 网段，如 192.168.2.0 即代表 192.168.2.100 所属网段。
- 网关：数据包被发送时经过的路由器或主机的 IP 地址。
- 子网掩码：是指目的网段的子网掩码，一般为 255.255.255.0。
- Metric :也称为跃点，一般是 1 到 30，可以任意写一个数字，并且可以重复。

- 接口：分为 WAN 接口（线路一、线路 2），LAN，VPN 接口（客户端 1、客户端 2、服务器端 1、服务器端 2），接口一定要根据实际情况选择，否则可能会造成路由不生效。
- 类型：NET 指一个网段的路由；host 是指到一个主机的路由
- 启用：只有选中该项后本条静态路由规则才能生效。

4.5.2 策略路由

- 协议：分为 TCP、UDP、两者三种情况。
- 目的 IP 或网段：这里是指我们通过互联网所要访问的服务器地址。
- 目的端口：指我们要访问的互联网上的服务器的端口号，0 表示全部端口。
- 源 IP: 是指内网中发起访问动作的 PC 机 IP 地址。
- 源端口：是指内网中发起访问动作的 PC 所使用的端口号，0 表示任意端口。
- 线路选择：是指在双线情况下，本条路由规则经过哪条宽带出去互联网。
- 启用：只有选中该项后本条静态路由规则才能生效。

4.6 EPN

EPN 是启博公司推出的新一代 VPN 技术，是一项增值服务，需付费使用。EPN 具有强大的穿透能力，可以穿透多级路由,EPN 能适用包括铁通、广电、长城宽带、歌华、e 家宽等没有公网 IP 的网络。将 VPN 设备设置为不同的网段，EPN 组网后即可让 VPN 设备之间互通。另外启博 EPN 支持 PC 客户端和安卓手机客户端连接，使用非常方便，并大大降低了传统 VPN 的实施复杂度。

4.6.1 基本设置

- EPN 状态：EPN 功能开关，启用 EPN 功能可用，禁用则 EPN 功能失效。
- 本机名称：可以任意输入英文、数字或英文数字组合，不支持中文及特殊符号。
- 本机组网密码：可以是任意的数字及字母，其他设备连接此设备时需要提供给对方，否则对方连接不上。
- 设备子网互通：是指连接到该设备的其他 EPN 设备下设备或 PC 可以互通，类似于客户端互访功能 。

服务状态　是显示当前 EPN 的工作状态，以及 EPN 的序列号情况

- 当前状态：显示该设备是否与 EPN 云服务端是否连接成功，只有成功连接云服务器后，其他设备才能与该设备进行连接。分为已连接和离线两种状态。
- 本机序列号：是指该设备的 EPN 序列号，一台设备有一个唯一的序列号，并且终身有效，无法修改。
- 最大接入数：是指该 EPN 序列号的最多接入许可数，包括 EPN 设备、PC 电脑、手机等的数量总和。
- 服务有效期至：是指该 EPN 序列号的截至有效期，过期 EPN 服务自动停止将无法使用。需付费另行开通 EPN 服务。

4.6.2 组网管理

组网管理是设置需要连接的设备信息，例如我们要连接北京分公司的 EPN 网关，则在这里添加名称：北京分公司，序列号是北京分公司网关的 EPN 序列号和北京的组网密码，MTU 值默任是 1360，其中北京的 EPN 序列号和组网密码需要向北京分公司索取或到北京 EPN 网关上查询。

✧ **注意：如果 A 和 B 两台设备相连，只需要 A 添加 B 或 B 添加 A 即可，不需要互相添加，这一点和传统 VPN 有区别!!!**

- 名称：是对要连接的网关信息的描述，可以为任意字符，支持中文。
- 序列号：是要连接的设备的 EPN 序列号，需向对方索取。
- 组网密码：是要连接的设备上设置的 EPN 组网密码，需向对方索取
- MTU 值：默认值是 1360 ，不建议修改。
- 加密：EPN 连接后数据的传输时是否采用加密，一般选是。

4.6.3 组网状态

组网状态显示和本设备已连接的其他设备及安卓移动端连接情况

- 名称：接入端的设备名称，一般是显示在组网管理中输入的对应 EPN 序列号的名称，对端的 EPN 设备上的组网状态里，名称显示为本端 EPN 设备端设置的本机名称（**见下图**）；对于手机端连接后则显示为 CLIENT。
- 序列号：显示接入的设备的 EPN 序列号，安卓移动端则显示为该安卓设备的硬件标识符。
- 网络：接入的 VPN 设备 LAN 接口 IP 地址及子网掩码、MTU 值信息。
- 当前速率：本端和对端之间当前数据传输的速率，分为接收和分送两种情况。
- 加速：是否使用 EPN 云加速服务器加速，只有个别情况下才会使用，一般不需要。
- 在线时长：EPN 已连接的时间，以秒为单位
- 状态：是接 EPN 设备连接连接的情况，如果正常连接会显示已连接，否则会给出相应的错误提示信息。

4.6.4 客户端帐号

客户端帐号管理是添加或删除 PC 端通过 EPN 连接的用户名和密码，

- 帐号：PC 端 EPN 连接时使用的用户名，可以为字母或数字。
- 密码：PC 端 EPN 连接时使用的密码。可以为字母或数字及英文标点附号。
- IP 地址：是分配给该帐号的 VPN 的虚拟 IP 地址，此帐号不管什么时间连接都会获取相同的 IP 地址。
- 备注：是对该帐号的说明或描述信息，支持中文输入 。

4.6.5 客户端连接

这里显示的是 PC 端 EPN 连接到该设备的情况

可以显示接入的帐号，分配的内部 IP、来源 IP，当前发送速率和当前接收数率，以及连接时长（这里计时以秒为单位）。

4.7 无线设置

4.7.1 基本设置

- 无线网络：无线功能开关，启用无线功能可用，禁用则无效功能失效。
- 无线模式：启博 VPN 的无线模式只有一种 访问点 AP 模式。
- 无线网络模式：无线 B/G/N 网络，可根据需要选择，一般选混合即可。
- 无线网络名（SSID）：其他设备通过无线查找时的 SSID 名称，默认值 qibo_wifi 。
- 无线频道：无线频频道可以任意选择。数值在 1-13 之间，没有优劣之分。
- 频道宽度：分 20MHZ 和 40MHZ 两种，其中 40MHZ 传输速度比 20MHZ 快些，但是穿透能力比 20MHZ 稍差，传输距也近些，一般用 20MHZ 较多。
- 无线 SSID 广播：对外广播 SSID，让别人能搜索到该无线设备。

4.7.2 安全认证

- 安全模式：安全模式可以任选一中即可。
- WPA 算法：一般选 TKIP+AES 兼容性比较好。
- WPA 共享密钥：其他设备通过 WIFI 连接该设备里需要提供的密钥，用户可自行设置。
- 密钥更新时间间隔（秒）：默认值是 3600 。

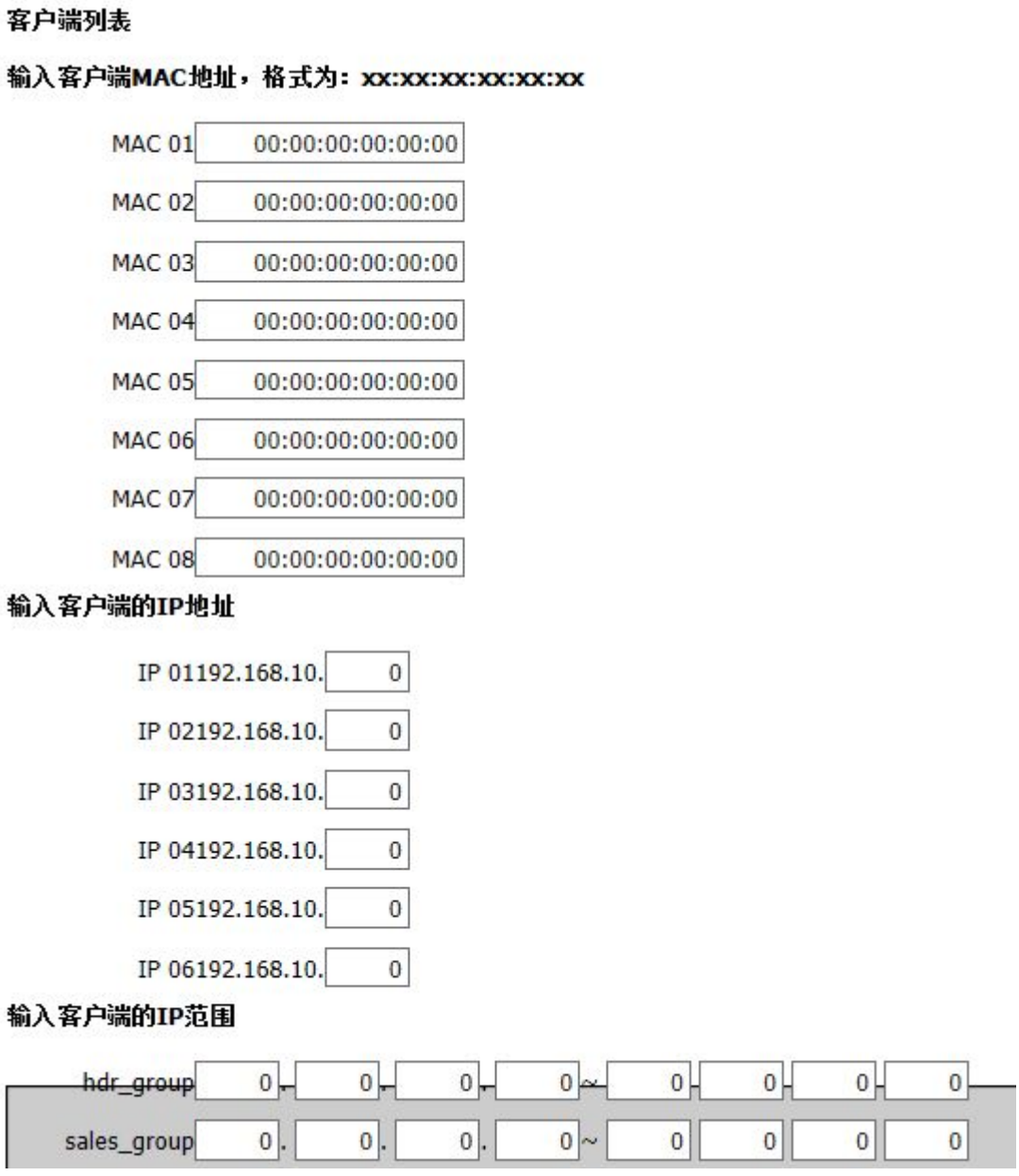
4.8 上网行为管理

4.8.1 基本限制

- 状态：该策略是启用或是禁用情况。
- 策略名称：对该策略的描述，可以为中文。
- PCS: 该规则升效的 IP 地址范围或 MAC 地址，如下图所示。
- 拒绝：直接拒绝，不允许上外网。
- 过滤：允许上外网，但会根据后面的规则设置进行过滤。
- 天：按天为单位进行控制，可以是一周中的某几天或每天。

- 时间：按 24 小时进行控制或者分时间段进行控制。
- 通过 URL 封锁 WEB 站点：根据输入的 URL 进行精确匹配过滤 WEB 站点。
- 通过关键词封锁 WEB 站店：根据输入的 URL 中包含关键词进行过滤 WEB 站点。

编辑客户端列表（PCS）



4.8.2 网址白名单

该功能主要应用于某些情况下，单位只允许访问某个或某些与工作相关的网址，无关网址不允许访问。使用通用的方法很难解决，因为要限制的网址太多了，启博 VPN 特增加了此功能满足客户的个性化需求。

- 功能开关：默认禁用，启用后功能生效。
- URL：可以是完整的 URL 地址，也可以是关键词，即支持模糊匹配。

4.8.3 流量控制---基本配置

- 开启 Qos：流量控制的总开关，启用则功能升效，否则功能关闭。
- 上传总带宽：是指所用宽带的总的上传速度，一般 ADSL 是 512KB/s 。
- 下载总带宽：是指所用宽带的总的下载速度，如 8M 的 ADSL 可以输 8000KB/s 。

4.8.4 IP 带宽控制

- 规则名：指该条规则的描述，可以为任意字符，一般为相应 IP 的设备名或电脑名称。
- LAN IP 地址：该规则应用的 PC 机或设备的 IP 地址

- 上行带宽范围：允许该 IP 地址的最小和最大的上传宽带数值。
- 下行带宽范围：允许该 IP 地址的最小和最大的下载宽带数值。
- 启用：只有选中该项本条目设置的宽带设置才能生效。

4.9 防火墙

4.9.1 过滤器

包过滤功能，

- 启用数据据包过滤：包过滤防火墙的总开关。
- 策略：分为接受和丢弃两种处理方式。
- 协议：分为 TCP、UDP、两种（TCP+UDP）三个选项。
- 源地址：发起方的地址。
- 源端口：发起方所使用的端口。
- 接口：设备接口分为 LAN、WAN、VPN 等几种。
- 目的地址：要连接到的 IP 地址
- 目的端口：要连接到的 IP 地址上端口号。
- 方向：分 LAN 到 WAN、WAN 到 LAN、双向三个选项。
- 启用：启用该包过滤条目。
- 阻止来自 WAN 口匿名请求：是否允许通过 WAN 口 PING 该设备，启用则无法 PING，禁用可以 PING。

4.9.2 MAC 地址绑定

功能描述：

- 没有绑定 MAC 和 IP 机器无法上网。
- 绑定了 MAC 和 IP 地址的机器可以上网，但是如果修改了 IP 或 MAC 就不能上网。
- 只有 IP 和 MAC 地址严格对应了，才可以上网。
- 主机名：可以为英文、数字或中文。

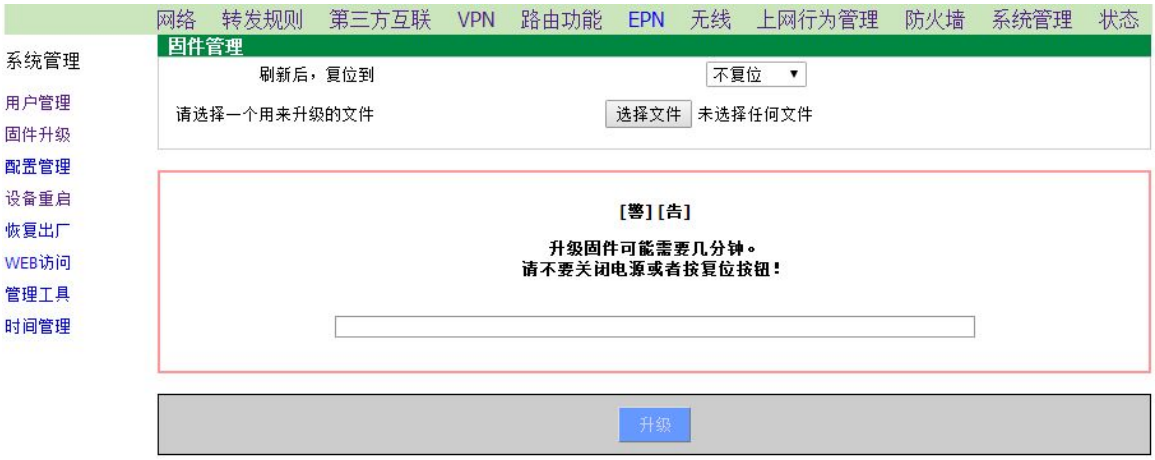
4.9.3 自定义命令工具

4.10 系统管理

4.10.1 用户管理

网络管理员可以通过此页面，修改启博 VPN 网关的登录密码，建议配置好设备一定要修改一下默认密码，避免一些不必要的麻烦。

4.10.2 固件升级



用户可能通过此页面，升级启博 VPN 新发布的固件，从而获取新产品功能。固件可向启博 VPN 官方索取，切莫自行擅自升级，一定要和启博 VPN 技术确认后再升级，以免造成设备的损坏。

4.10.3 配置管理

用户可以将设备的配置导出，以防万一可将此配置重新导入该设备或导入新的设备，达到快速恢复设置的目的。

4.10.4 设备重启

- 定时重启：在设定的时间设备自动重新启动。
- 立即重启：是指手动重启该 VPN 网关。

4.10.5 恢复出厂

恢复出厂默认，是指清空设备里的所有配置信息，将其恢复到出厂状态，重新配置，相当于设备面板上的 reset 键功能。

4.10.6 WEB 访问

本页面设置启博 VPN 网关的 WEB 管理端口和广域网中可以管理的端口，本地 WEB 是指通过 VPN 网关的 LAN 接口访问设备，远程 WEB 是指通过 VPN 网关的 WAN 接口访问设备。

4.10.7 管理工具

该页面是设置允许通过 telnet 和 SSH 两种命令行方式，本地或远程管理启博 VPN 网关，供高级网络工程使用。

4.10.8 时间管理

该页面设置启博 VPN 网关的时间，上面显示的是当前访问该网关的 PC 机的时间。

4.11 运行状态

4.11.1 系统信息

4.11.2 网络状态

4.11.3 实时流量

显示当前网络使用宽带流量最大的前 20 名，分为上传速度、下载速率、总速率。管理员通过此页面很容易找出谁在占用公司的网络。

4.11.4 在线主机

当前在线的活动 PC 机或设备的地址，以及在线时间、IP 地址对应的 MAC 地址。

4.11.5 拨号日志：

拨号日志可以看出设备拨号的情况，以及每次拨号和下线的时间，可以分析出设备拨号的稳定性。

4.11.6 系统日志：

附录一、常见问题解答（FAQ）

1、忘记启博 VPN 网关的登录密码，进不去设备的设置界面怎么办？
答：启博 VPN 网关默认用户名和密码都是小写的 admin ，可以尝试一下默认的用户名和密码能否进去，如果进不去，就只好通过设备面板上的 reset 键来恢复出厂设置了，恢复的方法是通电情况下用牙签等尖状物，顶住 RESET 键 20 秒左右，设备会自动重启并清空里面所有的配置。如果是你感觉里面的配置内容很多，又不想简单清空里面的参数，可以向启博公司寻求帮助试试，电话: 400-618-3858，在线 QQ: 28838513

2、用户收到设备后，第一次如何设置上网？

答：如果你是 ADSL 宽带用户，网络---宽带设置---连接类型 选“PPPoE 拨号上网”，把 ADSL 宽带上网的帐号和密码输入到相应的文本框里，保存即可。（注，有些猫启用了路由拨号功能，请联系客服，改为纯猫模式。）

如果你是光纤固定 IP 方式上网用户，网络----宽带设置---连接类型，选“Static 静态 IP”，把 ISP 运营商分配的 IP 地址、子网掩码、默认网关、DNS 输入保存即可。

如果你是用的小区宽带或天威视讯等小的运营商的网络，网络---宽带设置---连接类型，选“DHCP 自动配置”，保存即可。

3、启博 VPN 需要固定 IP 地址才能用吗？
答：启博 VPN 不需要固定 IP 地址就可以使用，但是对于公司的总部也就是中心端，需要有公网 IP 地址，这个公网 IP 可以是固定的也可以是动态的，中心端不能是私网 IP 的那种网络。
判断中心端的网络是否有公网 IP 地址的方法是，进行路由器，看一下运行状态里，外网那里拨号获取的地址是什么样的，一般以 10 开头或 100 开头的 IP 地址都是私网 IP，如果不确定，可以将这个 IP 地址和打开 www.ip138.com 上面显示的 IP 地址对比，如果是相同的就是合法的公网 IP，否则就是私网 IP。

4、启博 VPN 需要申请动态域名才能用吗？

答：启博 VPN 网关集成启博目录寻址服务和启博 DDNS 服务，用户不需要自己申请动态域名，直接用启博 VPN 网关自带的域名和目录服务就可以了。相比第三方的动态域名，启博 DDNS 是全商用、全封闭的寻址服务，只针对启博 VPN 的用户提供服务，不开放注册使用，不提供给第三方使用。有效的保证启博 DDNS 服务的稳定性和安全性。

5、启博 VPN 网关一定要替换我们现有的路由器吗？

答：启博 VPN 网关可以替换客户现有的路由器，也可以不替换现有路由器，直接放在现有路由器下，把启博 VPN 网关当作一台 PC 机一样使用。

6、启博 VPN 网关当路由器用和放在路由器后有什么区别？

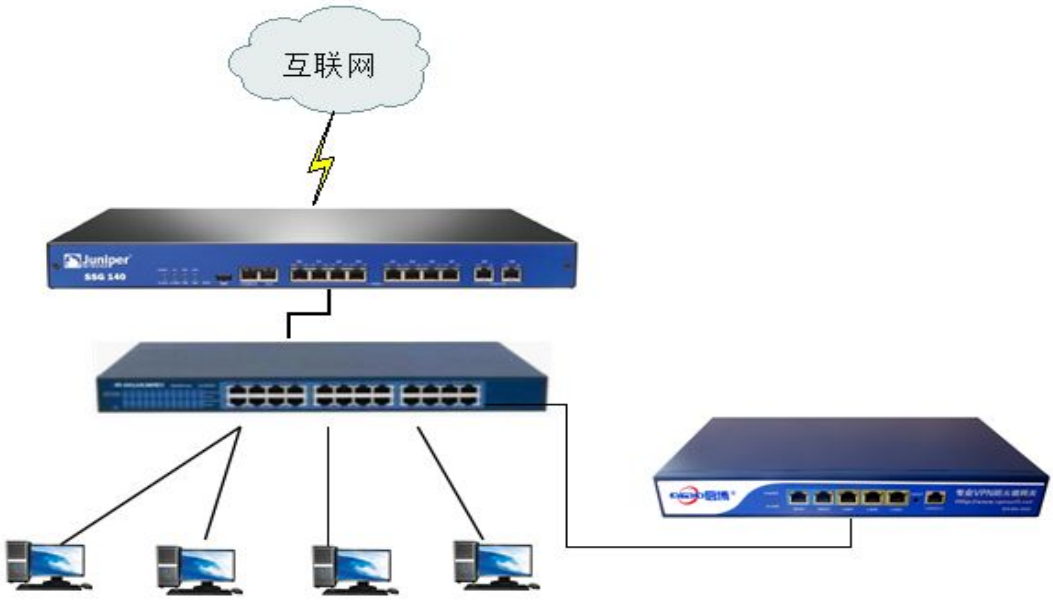
答：启博 VPN 网关当路由器用可以完整使用启博 VPN 所有功能，包括防火墙、VPN 功能、上网行为管理、流量控制等等。启博 VPN 放在路由器后，只用其中的 VPN 功能。
启博 VPN 当路由器比放在现有路由器后寻址稳定性稍好，有些客户网络管理很规范，防火墙、上网行为管理都部署的很好，用启博 VPN 网关放在路由器后也是很方便的，特别的是有固定 IP 地址的网络，使用效果也是不错的。
启博 VPN 当路由器用时需要接两条网线，一条是接外网，一条接内网；启博 VPN 放在路由器后，采用的是启博 VPN 的透明模式，只需要一条网线即可，不区分内网和外网。

7、我们是用的小区宽带，没有公网 IP 能用你们的 VPN 吗？

答：启博 VPN 只要求中心点也就是公司总部有合法的公网 IP 就可以了，如果你是做为 VPN 的分支端或客户端，不管用什么网络都是可以使用启博 VPN 的。如果的确是公司总部的网络没有公网 IP，请采用启博 VPN 双 NAT 版，详情可以登录启博官网进行了解（http://www.vpnsoft.net）。

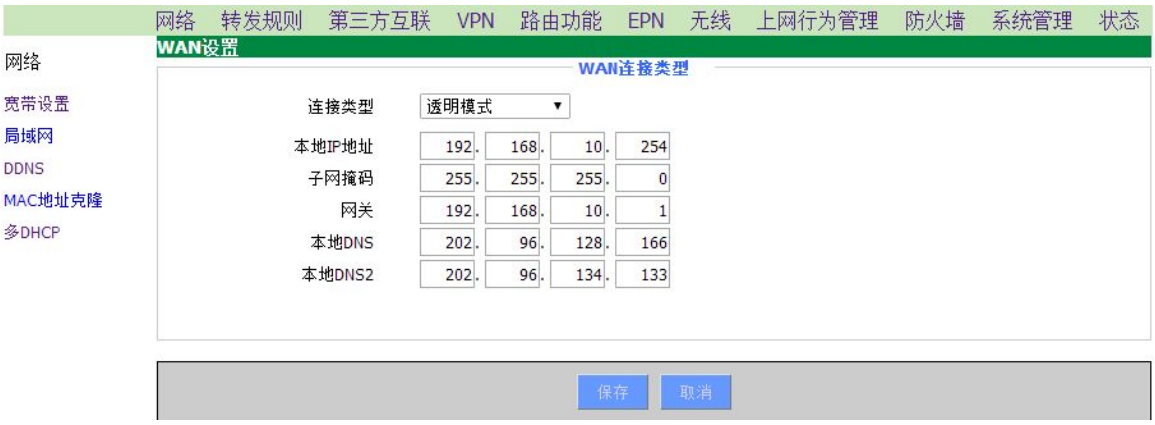
附录二、透明模式接入

有些客户在上 VPN 前，公司网络规划比较好，有专门的防火墙路由器和交换机，网络管理很规范，IT 部门人员也比较熟悉以前设备的维护管理，不太愿意换下以前的防火墙路由器使用 VPN 网关当路由器用，这样可以用启博 VPN 的透明模式的接法。
透明模式接法的优点是无需改变客户的现有网络结构，直接将 VPN 接在网络中的交换机上，网线接在 VPN 设备的 LAN 口上。网络拓朴图如下：



注意：网线一定要接在 VPN 网关的 LAN 口上，WAN 口上不用插线

假设路由器的 LAN 地址为：192.168.10.1，VPN 设备的网络参数配置如下：



注意：VPN 设备的路由 IP 地址，是当前网络中任一空闲 IP 地址均可，不一定是按上图设置；默认网关就是路由器防火墙的地址，静态 DNS 为当地 ISP 的 DNS，如果实在不知道，也可以写成和默认网关相同的内容，DNS 输 1 个或者 2 个都是可以的。

附录三、和第三方 IPSEC 模式互联实例

测试环境，前面放一台路由器，路由器的 IP 地址是 192.168.1.1，第三方网关和启博 VPN 外网用 DHCP 方式上网，第三方网关外网获取的 IP 地址是 192.168.1.138 ，启博 VPN 外网获取的 IP 是 192.168.1.104 ，第三方网关的内网接口 IP 是 192.168.23.1 ，连接电脑的 IP 是 192.168.23.120；启博 VPN 的内网接口 IP 是 192.168.10.1 ，连接电脑的 IP 是 192.168.10.100

一、第三方网关侧配置

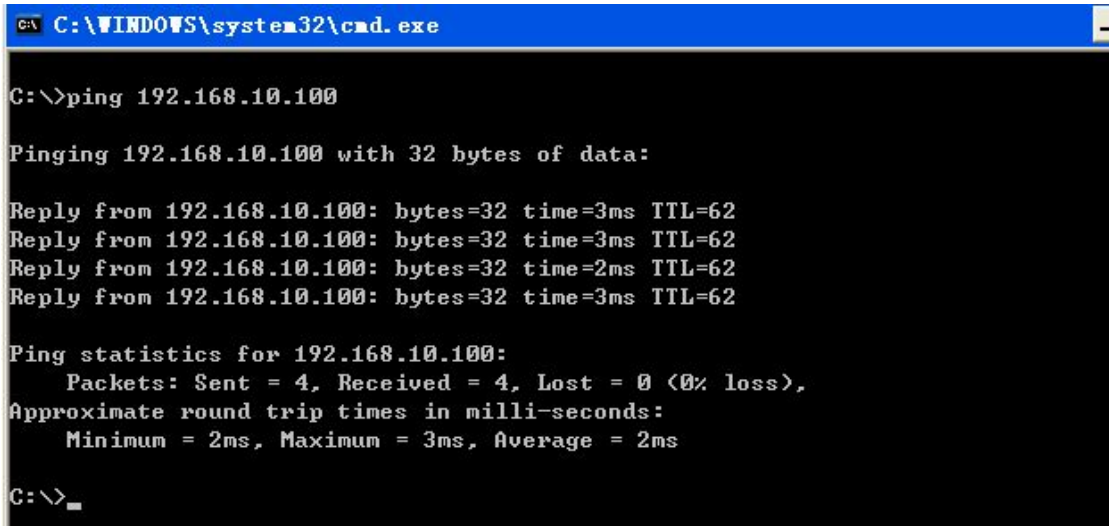
二、启博侧配置

三、连接成功

四、测试

启博 ping 第三方网关下面电脑

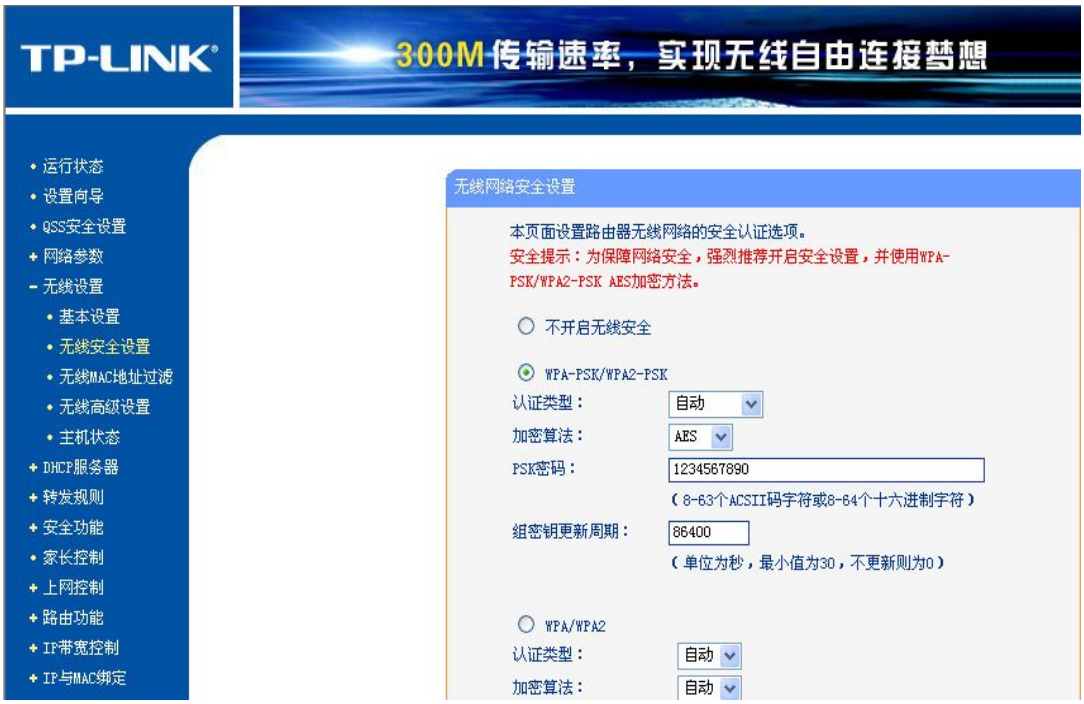
第三方网关 ping 启博下面电脑



附录四、无线路由器连接 VPN 设备的方法

一、首先进入原路由器（例如：TP-LINK），在网络参数---LAN 口设置---IP 地址中改成与 VPN 设备同一网段中的其中一个 IP 地址（例如：VPN 的地址是 192.168.10.1 原路由器就改成 192.168.10.254）

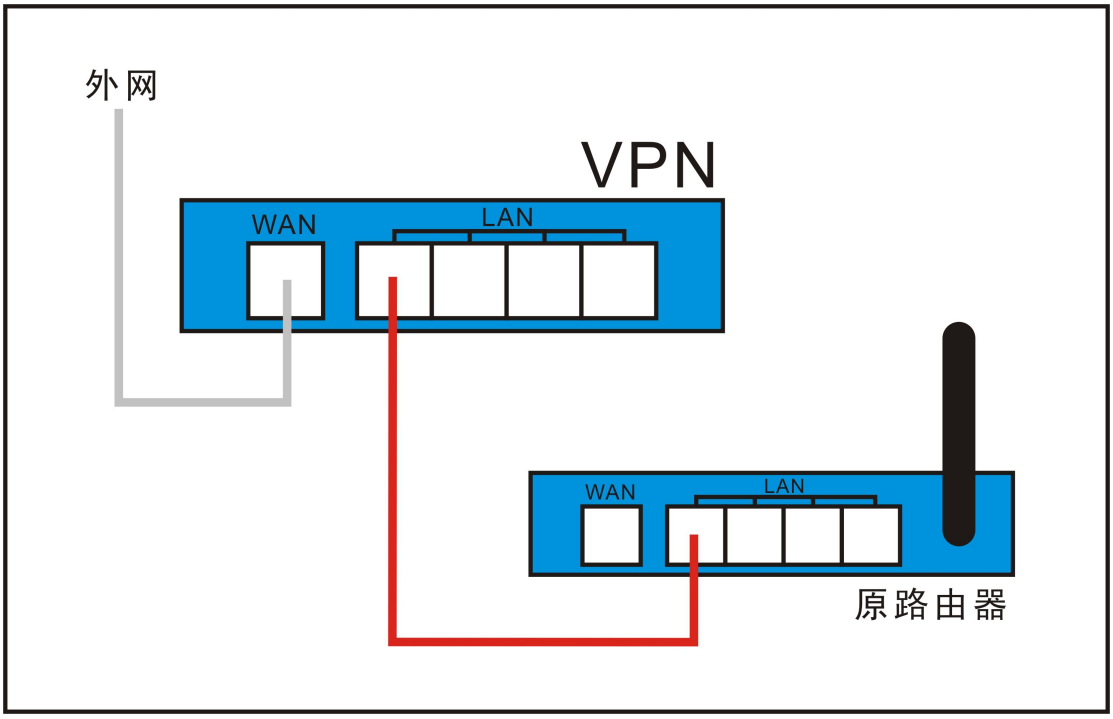
二、设置一下无线，之前设置好的可以直接看下一步。



三、设置 DHCP 服务器。

注：还有一种方式就是直接禁用 DHCP 服务器，有个别路由器的 DHCP 服务无法禁用，就只能按上图的方式设置。

四、设置完后，把 VPN 的 LAN 口跟原路由器的 LAN 口连接上。



附录五、安卓手机/平板连接启博 VPN

1、设备端配置

2、**安卓端配置**，找到“**设定**”---“**更多设置**”---“**VPN**”，点击”**VPN**”，进入下图

点击“**添加**”，进入下图。

- 名称：可以任意输入，这里我们输入“android_qibo”。
- 类型：选择 L2TP/IPSec PSK 。
- 服务器地址：要连的 VPN 设备的域名或 IP 地址。
- L2TP 密钥：不要输入。
- IPSec 识别符：不要输入。
- IPSec 预共享密钥：需要和 VPN 设备端保持相同，我们输入 “123abc”。

最后不要忘记保存，点击“储存”，返回到上级页面，就可以看到我们新建的 VPN 连接，如下图示：

我们点击新建的 VPN 连接，弹出下面对话框，提示输入用户名和密码，我们输入在 VPN 设

备端添加的用户名和密码，如果不想每次连接时都输入用户名和密码，可以打勾“**保存帐户信息**”。

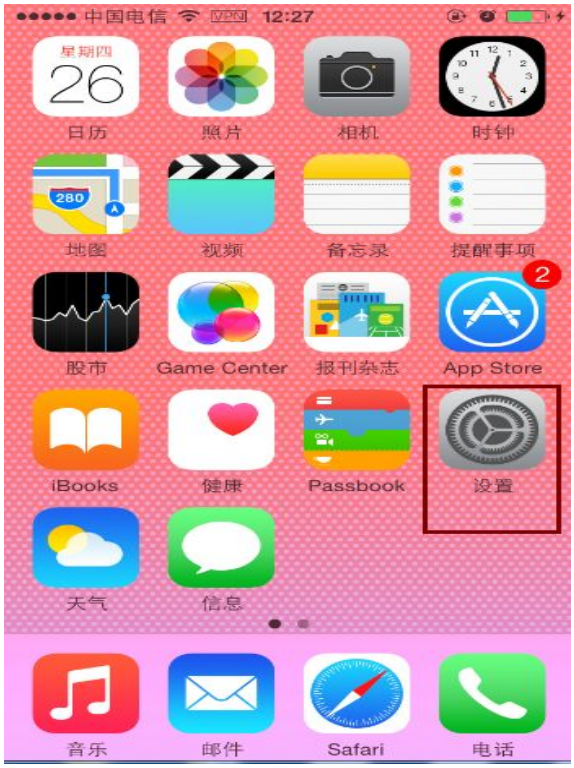
点击“**连接**”，连接成功后，则显示“**已连接**”。

此时，在 VPN 设备端 L2TP 状态里，也可以看到客户端连接进来的信息。

附录六、苹果手机/平板连接启博 VPN

1、VPN 设备端配置

2、苹果手机/平板端设置，先找到 **设置**



点击“**设置**”，进入下一级页面，找到“**通用**”，如下图示

点击“**通用**”，进入下一级页面就会发现“**VPN**”，如下图示：

点击“**VPN**”，进入 VPN 设置内部页面，如下图，点击“**添加 VPN 配置**”

点击“添加 VPN 配置”后，在出现的页面里，里面有 L2TP、PPTP、IPSec 三种 VPN 选项，我们这里选 L2TP。

按下图输入各项内容，其中密码是帐户 lxy 的密码，密钥是设备端配置里的 IPSEC 封装的预共享密钥。RSA SecurID 不需要设置，代理也不用设置，设置完了之后，千万不要忘记“存储”呀。

存储后，返回上级页面，点击 VPN 连接，就可以和 VPN 设备连接了，连接成功后如下图示。

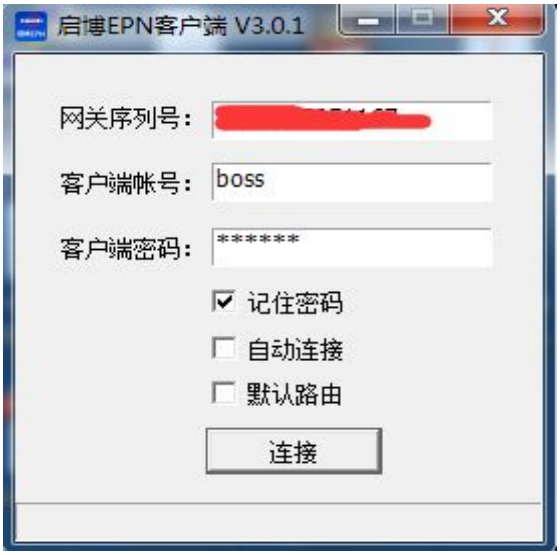
苹果手机/平板连接到 VPN 设备后，在 L2TP 状态里，可以看到客户端在线的信息。

附录七、EPN 客户端使用说明

一、PC 端

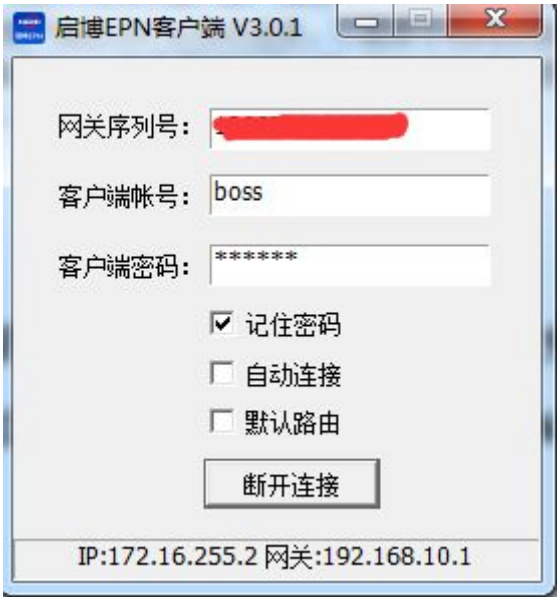
采用默认安装方式安装启博 EPN 客户端，安装成功后会在桌面上出现启博 EPN 的快捷方式，如下图， 

，双击启博 EPN 的快捷方式，显示下列窗口



- 网关序列号：是想要连接的设备的 EPN 序列号，可以在 VPN 设备的管理页面中查询到。
- 客户端帐号：连接到 EPN 网关的帐号，请向单位 IT 管理人员索取。
- 客记端密码：连接到 EPN 网关的密码，请向单位 IT 管理人员索取。
- 记住密码：下次使用时就不用再次输入客户端密码，系统会记住所输密码。
- 自动连接：下次 EPN 客户端启动时会自动连接，不需要手动再点连接按钮。
- 默认路由：EPN 客户端通过 EPN 服务器端代理上网，即实现所谓的借线或 VPN 代理功能。

连接成功后，如下图所示，如果连接失败，会有相应错误提示信息。



二、安卓端

安装文件请联系启博公司索取，按正常安卓文件安装方法安装即可，安装后会在手机屏幕上出现启博 EPN 快捷方式，

点击启博 EPN 快捷方式，

输入需要连接的 EPN 网关序列号和组网密码，点击连接，为了方便下次使用，可勾选 记住密码选项。显示下图表示 EPN 连接成功，如果连接失败会给出相应的提示信息。


63% 09:22
启博EPN
网关序列号：
网关组网密码：
记住密码
自动重连
已连接
断开