**AC\_4.0产品说明书**

**目录**

[一、前言 3](#_Toc19137)

[1.说明书使用约定 3](#_Toc6075)

[二、产品简介 3](#_Toc9771)

[1.主要特性 3](#_Toc27565)

[2.设备管理 4](#_Toc5604)

[三、web管理 4](#_Toc32636)

[四、基本网络设置 6](#_Toc16554)

[1.接口模式 7](#_Toc7982)

[2.接口配置 8](#_Toc2473)

[⑴ LAN口配置 8](#_Toc13199)

[⑵ WAN口配置 8](#_Toc11670)

[⑶ PPTP配置 10](#_Toc20663)

[⑷ VLAN配置 10](#_Toc30162)

[⑸ MACVLAN配置 11](#_Toc28601)

[五、高级网络配置 12](#_Toc18510)

[1.静态路由 12](#_Toc9700)

[2.端口映射 13](#_Toc26770)

[3.网络诊断 14](#_Toc6635)

[4.多WAN负载 15](#_Toc13991)

[⑴ WAN口带宽 16](#_Toc14154)

[⑵ 负载策略 16](#_Toc13645)

[⑶ 高级策略 16](#_Toc28206)

[5.静态IP分配 17](#_Toc21184)

[⑴ 基本配置 17](#_Toc16285)

[⑵ 批量处理 18](#_Toc4284)

[6.防火墙设置 18](#_Toc24555)

[7.UPnP设置 19](#_Toc19881)

[8.DDNS 20](#_Toc18876)

[六、无线配置 20](#_Toc16400)

[1.AP管理 21](#_Toc11804)

[2.Radio状态 24](#_Toc32456)

[3.WLAN配置 24](#_Toc21125)

[4.无线用户 25](#_Toc893)

[5.防终端粘滞 26](#_Toc13244)

[6.无线优化 26](#_Toc17020)

[7.调试功能 27](#_Toc15598)

[七、用户认证 28](#_Toc2549)

[1.认证选项 28](#_Toc7292)

[2.用户管理 29](#_Toc11265)

[3.云端管理 30](#_Toc19537)

[4.四种认证方式 30](#_Toc21046)

[⑴ 自动认证 30](#_Toc20920)

[⑵ web认证 30](#_Toc3732)

[⑶ 微信认证 32](#_Toc6408)

[⑷ 云端认证 34](#_Toc7430)

[八、应用控制 34](#_Toc13225)

[1.控制列表 34](#_Toc8663)

[2.URL控制规则 35](#_Toc8663)

[3.应用控制规则 36](#_Toc13114)

[4.配置案例 37](#_Toc21693)

[5.控制日志 40](#_Toc29404)

[九、审计 3](#_Toc17782)9

[1.免审列表 3](#_Toc26612)9

[2.审计规则 4](#_Toc26612)0

[3.配置案例 43](#_Toc26612)

[4.审计配置 46](#_Toc3589)

[5.上网行为审计 47](#_Toc10251)

[6.用户上下线记录 49](#_Toc23676)

[7.审计统计 50](#_Toc1502)

[十、组设置 51](#_Toc21823)

[1.IP组 51](#_Toc29666)

[2.MAC组 53](#_Toc16613)

[3.URL组 55](#_Toc26573)

[4.时间组 56](#_Toc28466)

[十一、流量控制 57](#_Toc13015)

[1.总出口带宽配置 58](#_Toc12245)

[2.流量策略配置 58](#_Toc8391)

[3.配置案例 60](#_Toc5918)

[十二、VPN管理 63](#_Toc5570)

[1.PPTP服务端 63](#_Toc32078)

[2.PPTP客户端 64](#_Toc17134)

[3.配置案例 65](#_Toc18743)

[十三、系统 68](#_Toc3345)

[1.系统属性 68](#_Toc26837)

[2.网络快速转发 69](#_Toc7486)

[3.系统日志 69](#_Toc5069)

[4.密码修改 69](#_Toc21277)

[5.备份/升级 70](#_Toc22579)

[6.序列号管理 70](#_Toc12756)

[7.重启 71](#_Toc5234)

[十四、设置向导 71](#_Toc24452)

[附录：版本更新说明 73](#_Toc8507)

[新增功能： 73](#_Toc16443)

## 一、前言

感谢您购买我们的产品！阅读此说明书将有助于配置、管理和维护本产品。

### 1.说明书使用约定

说明书中所提到的“AC”、“设备”、“产品”等名词，如无特别说明，均指本网关设备。说明书中涉及到IP地址等数据信息均为举例说明，具体请以实物为准。说明书中涉及的产品图仅供参考，产品的硬件或软件会不定期更新，具体请以实物为准。不同类型产品硬件参数及软件功能存在一定的差异，本文只列出X86的一种类型。

## 二、产品简介

弱行为管理包括x86、7621、7621\_poe、9563+9882、无线9531、有线9531、9531+9887和9531室外共8个系列的产品。将负载均衡、流量控制、用户认证、行为管理等功能集中到一体。既能够满足企业、酒店、学校等大型场所组建高效、安全、易管理网络的需求；又能满足办公室、餐厅、家庭等小型网络稳定、安全、简单上网的功能。

### 1.主要特性

① 提供多个1000Mbps RJ45端口，默认1个广域网WAN口，多个局域网LAN口。

② 网络配置和无线配置功能齐全，可满足绝大多数的使用场景。

③ 支持多 WAN 策略，既方便增加网络带宽又可以让用户自主分配带宽。

④ 支持瘦AP管理功能，AP搭配AC使用，以超高的性价比和简易的管理方式做到大面积的无线网络覆盖。

⑤ 支持无线优化、无线高级配置功能，方便管理员对实际使用场景做出最优的无线解决方案。

⑥ 支持web、微信、短信等多种认证方式，可满足绝大多数的使用场景。

⑦ 支持云端管理功能，用户可远程批量管理设备。

⑧ 支持上网行为控制功能，方便监督以及限制上网用户的行为。

⑨ 支持VPN功能，可搭配DDNS功能，实现远程办公。

### 2.设备管理

设备通电后，指示灯及接口或按钮说明如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 指示灯 | 颜色 | 状态 | 说明 |
| Power | 绿色 | 常亮 | 设备通电正常 |
| 不亮 | 设备通电异常或出现故障 |
| HDD | 红色 | 闪烁 | 设备硬盘在读写数据 |
| 不亮 | 设备硬盘出于待机状态 |

|  |  |
| --- | --- |
| 接口或按钮 | 说明 |
| Reset | 复位按钮，按住6秒以上再松开，可恢复设备的出厂设置 |
| RJ45网口 | 默认1个WAN口，多个LAN口，1000Mbps |
| 电源接口 | 用于连接电源，给设备供电。请使用产品包装盒内的配套电源线进行连接。 |

## 三、web管理

设备默认接口类型为单LAN单WAN，默认的登陆地址为172.16.0.1，用户名admin，密码admin。步骤如下：

步骤1：确保电脑网卡已经连接在设备的LAN口；

步骤2：设置电脑的本地连接为自动获得IP地址；

步骤3：打开电脑上的浏览器，在地址栏输入172.16.0.1后，回车；

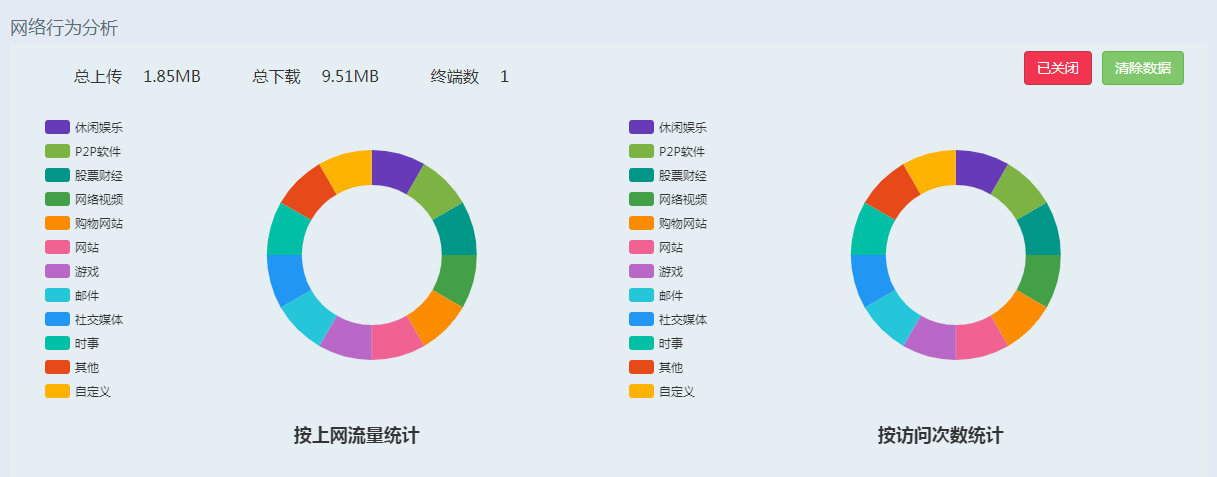
步骤4：进入设备的Web登录页面，如下图所示。



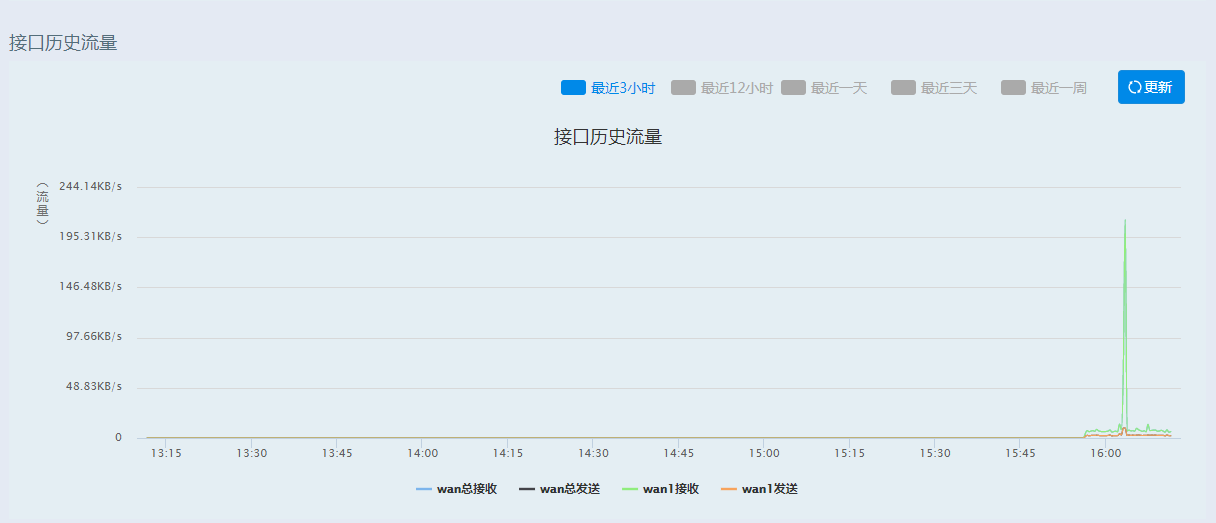
步骤5：输入用户名“admin”，密码“admin”，然后点击“登录”。登录后访问到的是总览页面，页面包含系统状态、接口状态、网络行为分析、接口历史流量、用户实时流量以及连接实时流量，如下图所示。



注：系统状态以及、接口状态流量信息会自动更新，每5秒更新一次。



注：网络行为分析开启后，统计饼状图每小时更新一次。



注：该流量图不会自动更新，需要手动点击又上角的“更新”进行更新。多wan场景下，可以自定义选择wan口展示历史流量。默认提供了5个时间段，用户可以选择不同的时间段展示历史流量，也可以通过拖动鼠标，自定义时间段显示。

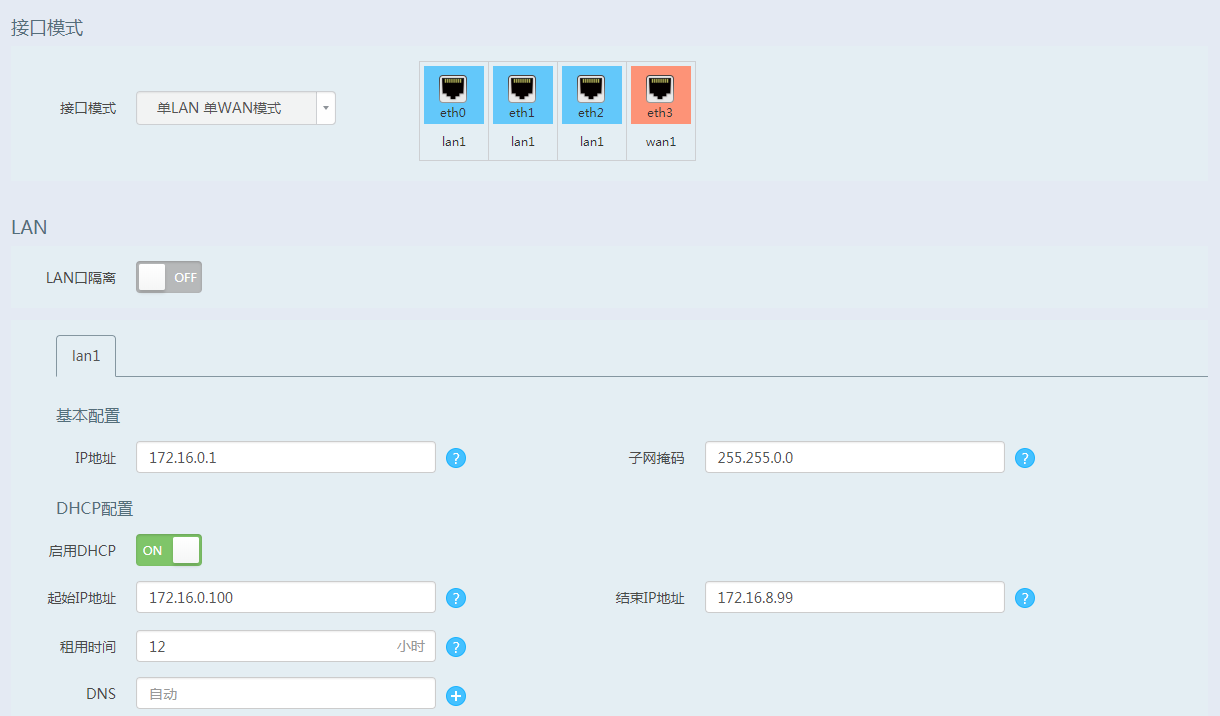


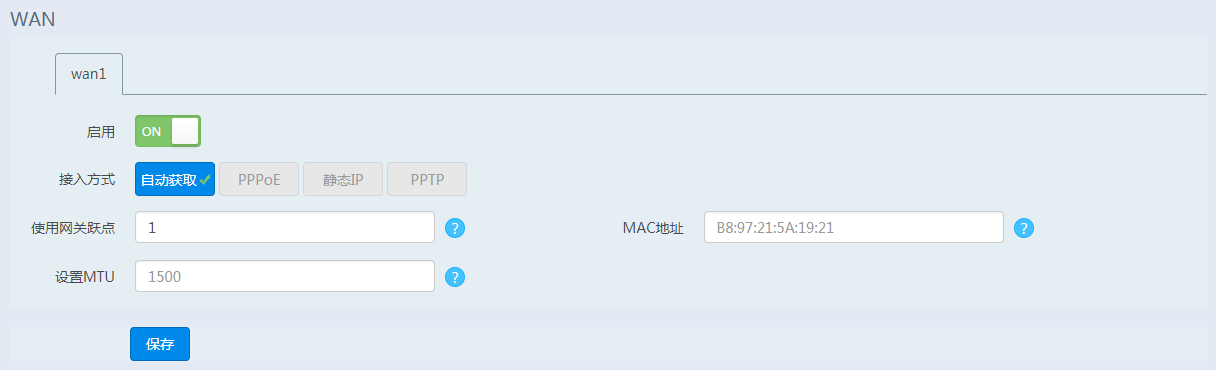
注：连接实时流量的“应用/协议”，在开启网络行为分析之后才会识别。

步骤6：为了网络安全，强烈建议修改路由器的登录密码。具体方法见“密码修改”。

## 四、基本网络设置

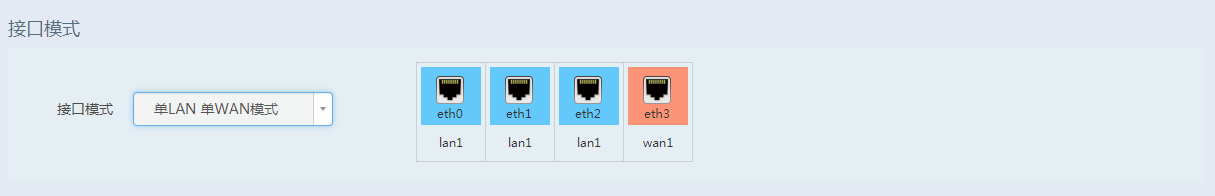
下图显示的为默认的网络配置，即“单LAN单WAN模式”。



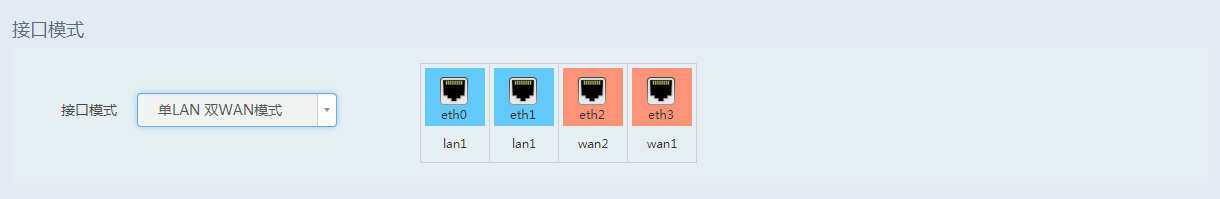


### 1.接口模式

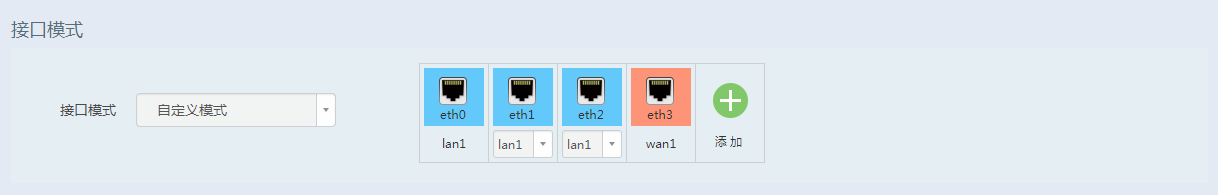
① 单LAN单WAN：一个WAN口，其余的都是LAN口，这5个LAN口等价，如下图所示。



② 单LAN双WAN：两个WAN口，其余的都是LAN口，这4个LAN口等价，如下图所示。



**③ 自定义：除了固定的eth0为lan1口和eth3为wan1口**，其余的2个口可以让用户根据需要自行指定，另外在该模式下可以添加虚拟接口功能，如下图所示。



### 2.接口配置

包括lan口配置、wan口配置、PPTP配置、VLAN配置以及MACVLAN配置。

#### ⑴ LAN口配置

① LAN口默认地址是172.16.0.1/16，若想修改LAN口地址请直接在LAN口的基本配置中修改。

说明：如果您将默认的LAN口地址做了更改，Web登录界面的访问地址也会随之更改

例如：将LAN口地址改为192.168.0.1，那么以后访问Web页面的地址则变为192.168.0.1。

② DHCP服务器配置在LAN口基本配置的下方，默认的地址范围是从172.16.0.100到172.16.8.99，共2048个地址.如果您想要自行设置，请参考以下方法进行。

启用：表示开启DHCP功能，不勾选则表示关闭DHCP功能。

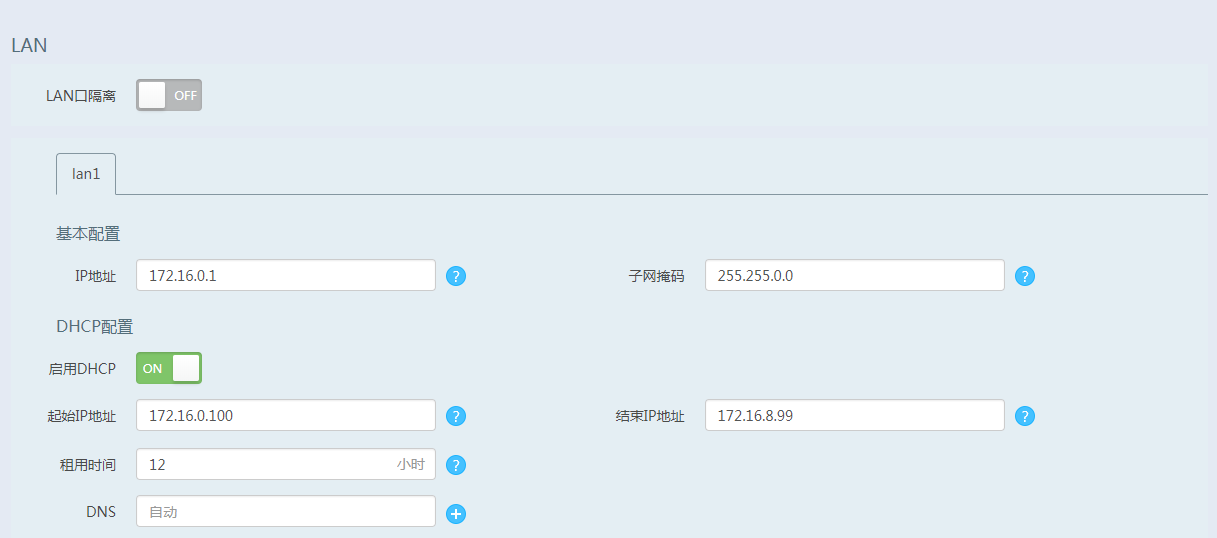
起始IP地址：表示DHCP服务器的起始IP地址。

结束IP地址：表示DHCP服务器的结束IP地址。

租用时间：表示DHCP地址池的租约。

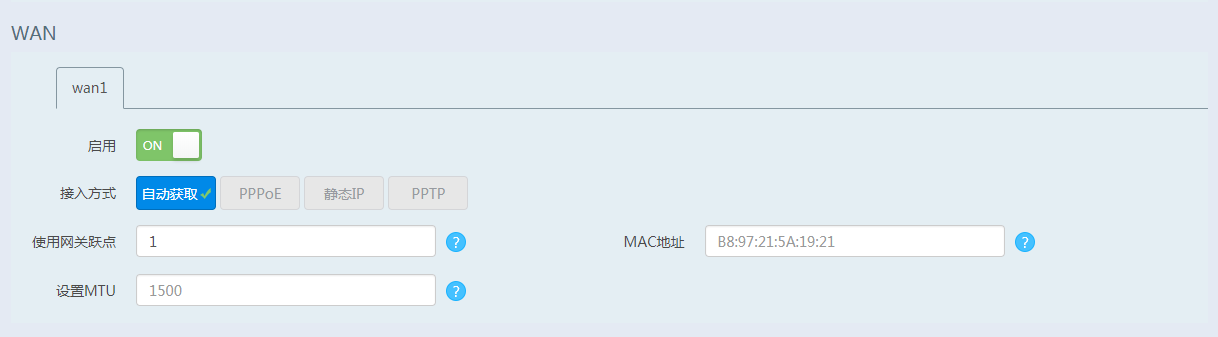
③ lan口隔离：开启后不同lan口之间不能相互通信，可有效实现lan-lan隔离，提高局域网安全性。

④ 具体配置页面如下图所示：



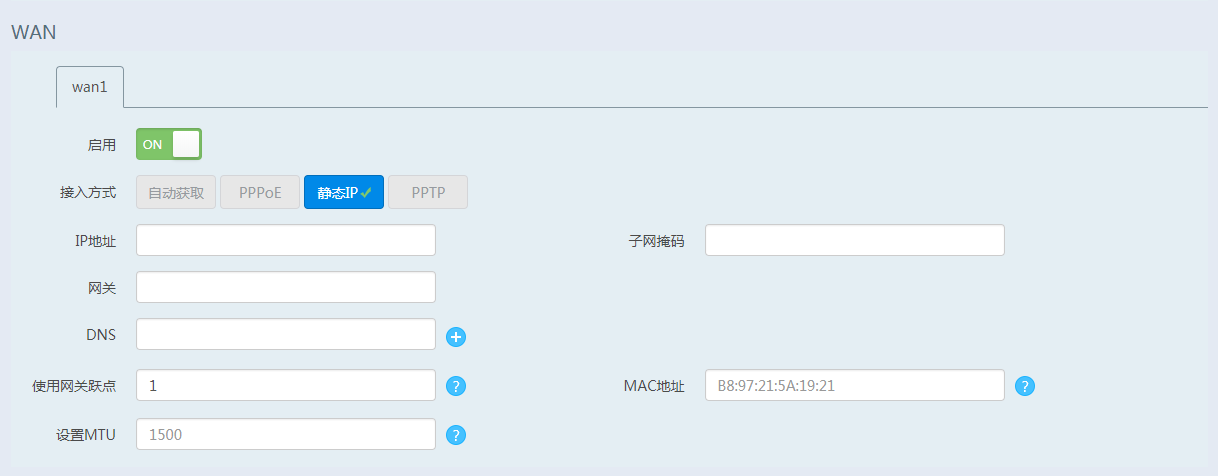
#### ⑵ WAN口配置

① 自动获取：在该模式下可以自动获取上级网关分配的IP地址，如下图所示。

 ② PPPOE配置：即拨号上网，在该模式下需要填写宽带提供商提供的用户名和密码即可自动拨号，如下图所示。



③ 静态IP配置：该模式下，需要您手动配置。具体的内容为：IPV4地址、IPV4子网掩码、IPV4网关、DNS，如下图所示。(您申请宽带服务，并具有固定IP地址时，网络服务商提供给您的一些基本网络参数，请对应填入下框。如您遗忘或不太清楚，请咨询您的网络服务商。)



④ 网关跃点：当使用多个wan口时，需要对多个wan口指定不同的跃点，跃点数越低则优先级越高。

⑤ MAC地址和MTU：用户可以手动修改设备的wan口MAC和MTU值。

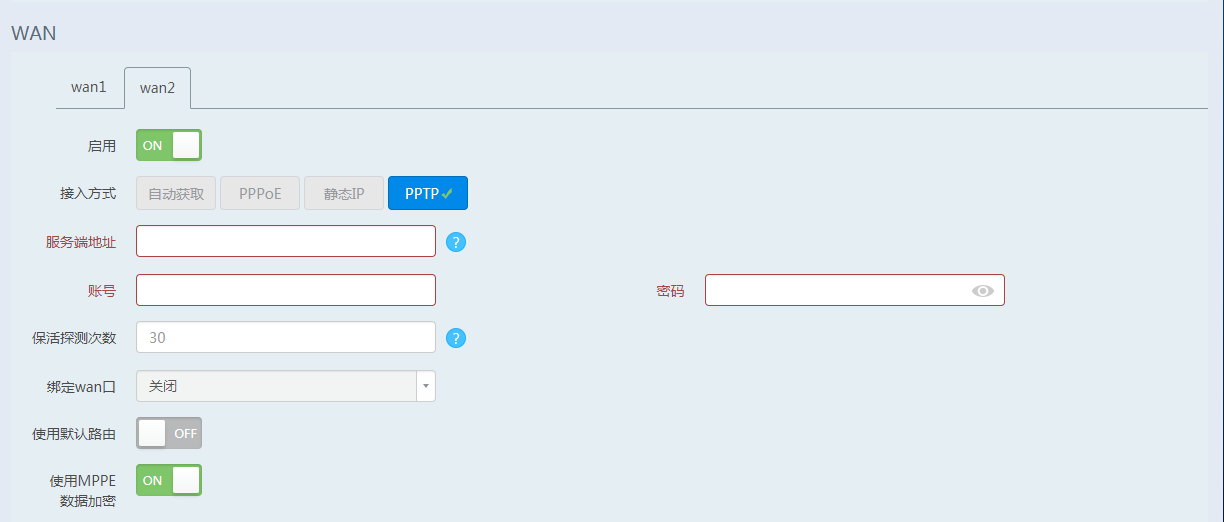
⑥ 启用：控制wan口的开关，用户可以通过此功能启用/禁用wan口，实现手动pppoe重拨。

#### ⑶ PPTP配置

① 添加PPTP：在自定义模式下添加PPTP接口，选择PPTP接口为WAN2，如下图所示。



② PPTP配置：填写好服务端地址、帐号、密码即可自动连接，如下图所示。



③ 保活探测次数：连续探测失败一定次数后，认为连接断开，开始重新连接。每次探测时间间隔为5s，探测次数取值范围1-60，取值越小，灵敏度越高，如无特殊需要，建议不要修改。

④ 绑定wan口：多wan的场景下，用户可以通过指定wan口建立pptp拨号连接，实现最优的VPN线路。

⑤ 使用默认路由：勾选此项将会创建一条指向PPTP服务端的默认路由，优先级最高。

⑥ MPPE数据加密：数据加密功能，要确保和服务端保持一致，否则将会无法连接。

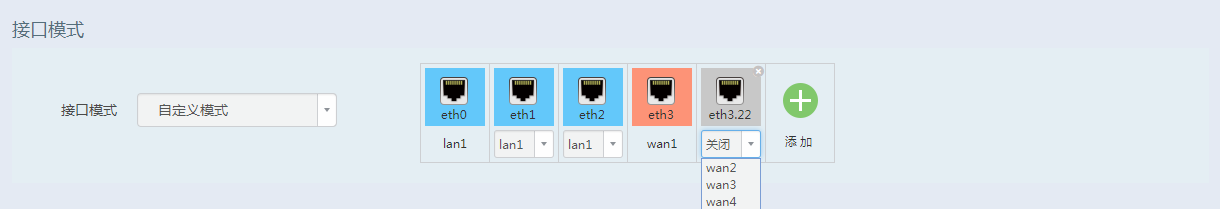
⑦ 启用：控制PPTP客户端的开关。

#### ⑷ VLAN配置

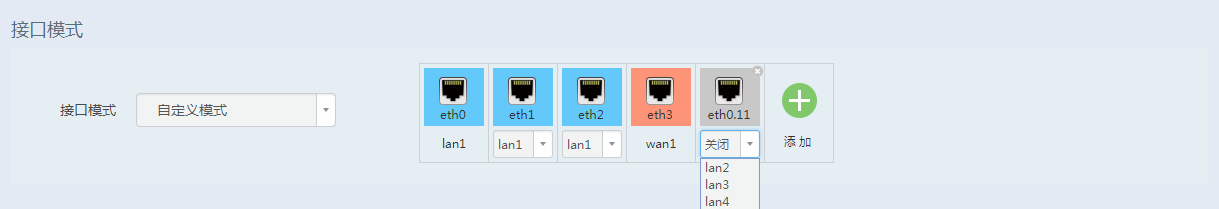
① 添加VLAN：在自定义模式下添加vlan，需要指定网卡和vlan ID，如下图所示。



② 为wan口添加vlan：如果指定的网卡是wan口，则可以设置vlan接口为其它wan口，如下图所示。



③ 为lan口添加vlan：如果指定的网卡是lan口，则可以设置vlan接口为其它lan口，如下图所示。



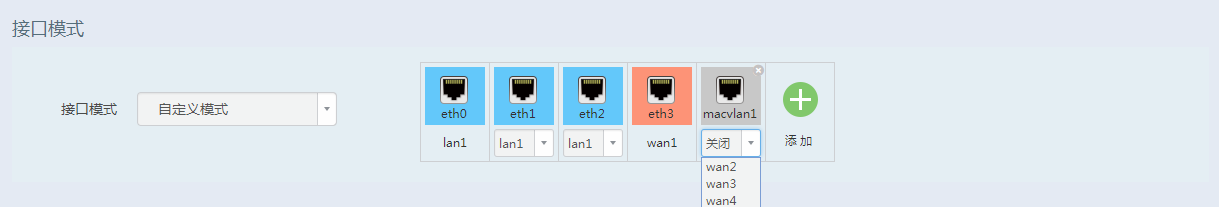
④ 具体的接口配置同lan、wan口配置。

#### ⑸ MACVLAN配置

① 添加VLAN：在自定义模式下添加macvlan，需要指定接口为wan口的网卡，如下图所示。



② 为wan口添加macvlan：添加的macvlan需要设置为逻辑wan口才可以使用。



③ 具体的接口配置同wan口配置，macvlan接口多用于pppoe多播。

## 五、高级网络配置

主要包括下面的8个模块，分别是：静态路由、端口映射、网络诊断、多wan负载、静态IP分配、防火墙设置、UPnP设置、DDNS。

### 1.静态路由

下图显示的为静态路由的默认页面，里面的路由条目不可修改，是设备根据基本网络配置自动创建的，包括网口的直连路由和默认路由。



① 添加静态路由：需要手动依次填写路由的基本信息，包括下一跳接口、目标IP、目标掩码和下一跳地址，如下图所示。



② 跃点数和MTU：可根据需求，手动填写。

### 2.端口映射

端口映射的功能是将局域网内的主机或服务器的端口映射出去，让局域网外的用户可以通过设备的WAN口地址加端口号来访问，配置页面如下图所示。

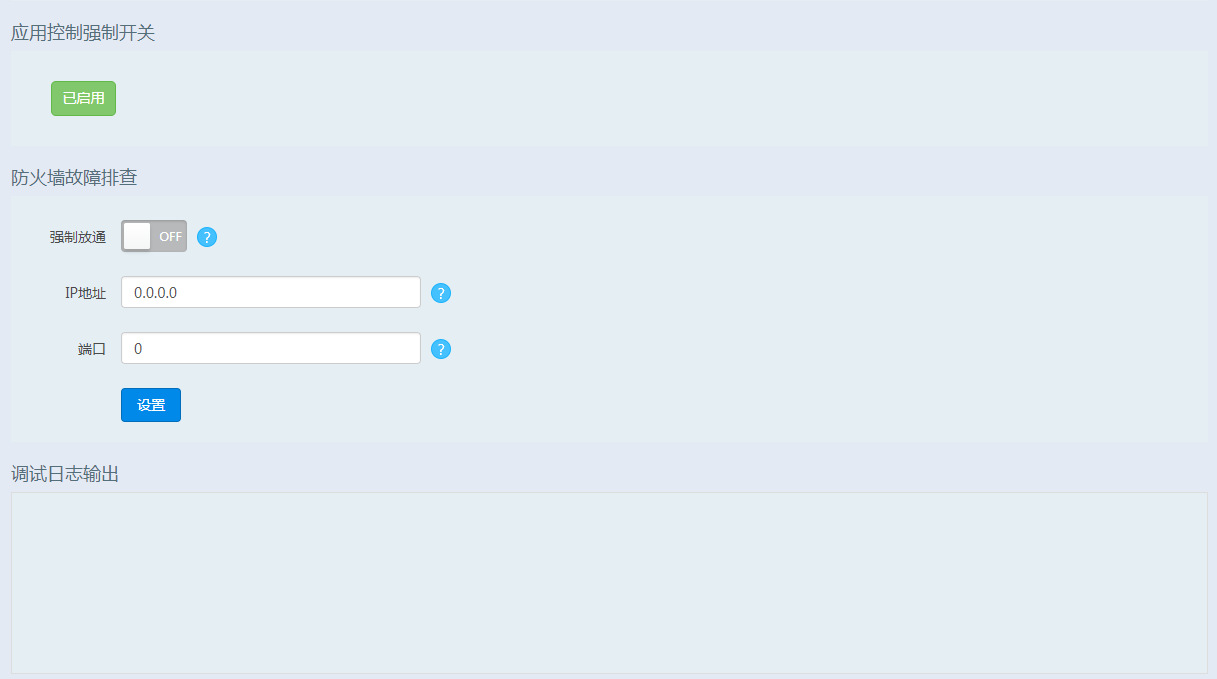


|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| 协议 | 设置端口访问协议的类型，包括TCP协议和UDP协议 |
| 外部端口 | 局域网外的用户用来访问局域网内的服务器的端口号 |
| 内部IP地址 | 设置需要被访问的局域网内的服务器的IP地址 |
| 内部端口 | 局域网内的服务器访问的端口号 |
| 启用回环 | 勾选此选项后，局域网内的用户也可通过WAN口地址加端口号访问局域网内的服务器 |

### 3.网络诊断

下图显示的为网络诊断的默认页面，其中包含了DHCP服务器探测、网络工具、应用控制强制开关和防火墙放通功能，方便管理员诊断网络异常，如下图所示。





① DHCP服务器探测：该功能可以探测到lan区和wan区内的所有DHCP服务器，可有效检测到网络中私接的路由器，消除网络中潜在的风险。

② 网络工具：包含ping、traceroute、nslookup这几个常用的网络诊断工具。

③ 应用控制强制开关：可在需要的情况下，通过此开关，一键“启用/禁用”应用控制。

④ 防火墙放通功能：被放通的IP、端口，可以不受应用控制、流量控制等控制。

### 4.多WAN负载

该策略需要在多wan场景下使用，包括WAN口带宽、负载策略和高级策略三个模块，如下图所示。



下面将通过实际使用场景，来说明负载策略和高级策略的配置。

#### ⑴ WAN口带宽

①多wan场景下，用户可以通过启用/禁用和带宽分配，来决定进行负载的线路，以及在平均分配模式下的负载权重。

② 多wan场景下，用户可以手动配置线路探测的地址，提高多wan稳定性。

#### ⑵ 负载策略

场景描述：某公司接两条宽带，一条电信下行50Mbps，一条联通下行20Mbps，内网全部用户共享两条宽带。

步骤1：网络设置中选择单LAN双WAN模式，配置WAN1和WAN2为PPPOE拨号，WAN1为电信，跃点数配置为1，WAN2为联通，跃点数配置为2。

步骤2：打开多WAN负载页面，启用WAN1口，带宽50M；启用WAN2口，带宽20M。

步骤3：在负载策略中选择策略，平均分配代表两条带宽同时工作，共同负载一定的带宽；线路备份表示选择其中一条为主线路，一条为备份线路，主线路在日常的工作中工作，当主线路发生故障或者说断掉的情况下，备份线路会自行启动工作，保证网络的通畅。

#### ⑶ 高级策略

场景描述：某高校宿舍连接两条带宽，一条电信下行20M，一条校内网下行1M（访问校内资源不限速），同学们需要访问校内资源时，走内网线路，访问其它资源时，走电信线路。

步骤1：网络设置中选择单LAN双WAN模式，配置WAN1和WAN2为PPPOE拨号，WAN1为电信，跃点数配置为1，WAN2为校内网，跃点数配置为2。

步骤2：打开多WAN负载页面，启用WAN1口，带宽20M；启用WAN2口，带宽1M。

步骤3：在负载策略中选择线路备份，主线路为WAN1，备份线路为WAN2。

步骤4：配置高级策略，如下图所示。



### 5.静态IP分配

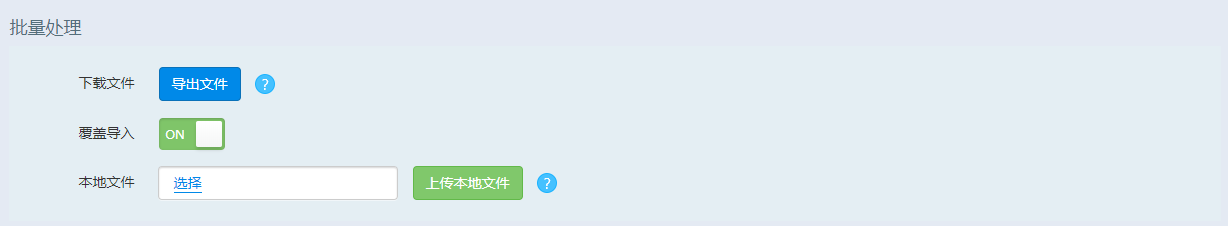
#### ⑴ 基本配置

静态IP分配的功能是给设备下的终端分配一个固定的IP地址，将固定的IP地址和终端的MAC地址绑定，如下图所示。



#### ⑵ 批量处理

对于需要为多台终端进行静态IP分配的场景，可以一键导出，用excel查看。当更换设备时，还可以先导出，再导入；当初次使用此设备时，也可以按照文本格式，在excel表格中添加，之后再导入。该功能避免了繁琐的配置。



### 6.防火墙设置

此功能可以让用户根据IP、MAC、端口和协议进行相应的放通或阻断，如下图所示。



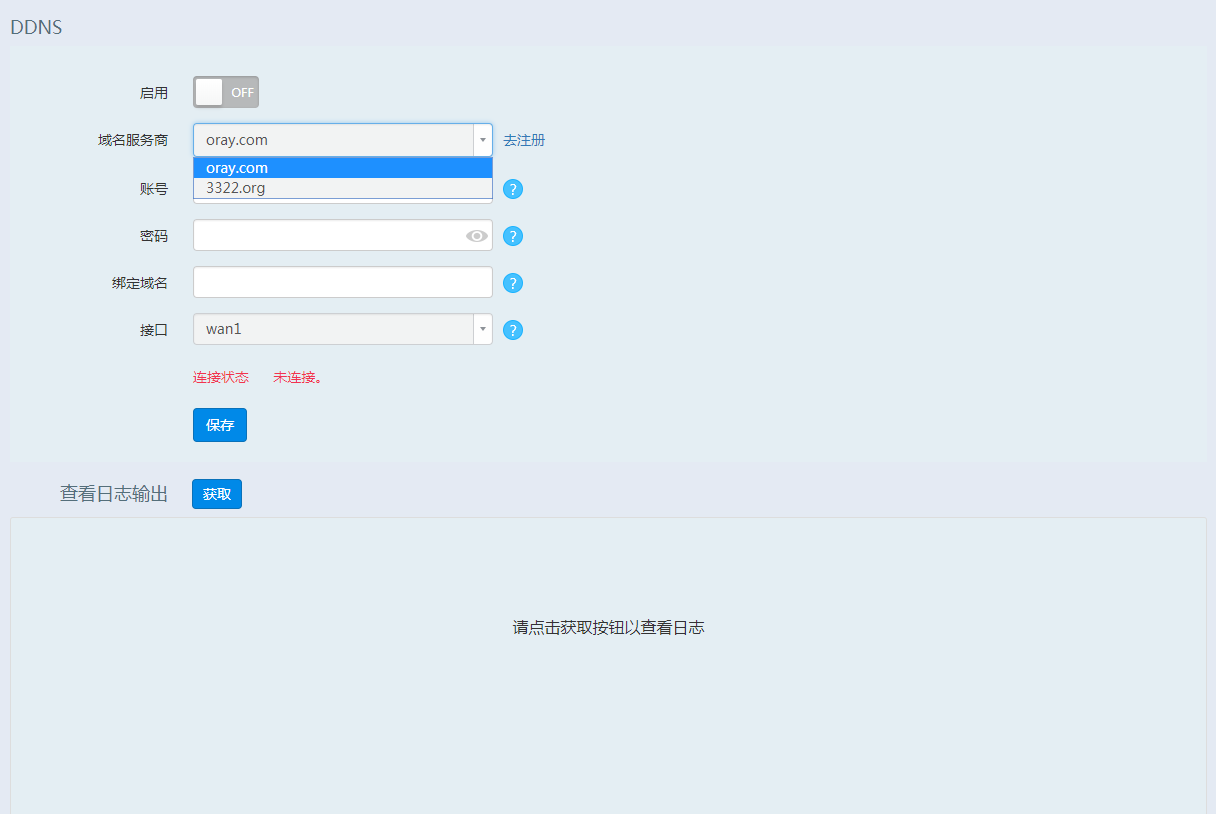
### 7.UPnP设置

开启此功能后，可以自动识别P2P软件（包括迅雷、比特彗星等），将端口映射出去，让外网主动和内网的终端建立连接，增加建立的连接数，进而一定程度上增加了P2P下载速度。



### 8.DDNS

DDNS即动态域名解析，目前版本支持主流的动态域名提供商提供的域名，包括花生壳和3322，如下图所示。



① 选择域名服务商，填写在域名服务商注册的帐号、密码和域名，指定接口后，点击“保存”，可以看到成功与否的连接状态信息。

② 查看日志输出：点击“获取”，可以看到DDNS的日志，方便用户排查问题。

## 六、无线配置

本设备集成了无线控制器的功能，可以自动发现内网中的瘦AP，并进行管理，可同时管理多个2.4G和5G的瘦AP。无线配置主要包括下面的7个模块，分别是：AP管理、Radio状态、无线用户、WLAN配置、防终端粘滞、无线优化、调试功能。

### 1.AP管理

① 首先将瘦AP接入在局域网内，获取到IP地址之后（可在“状态”→“DHCP列表”中找到AP的IP地址），通过浏览器访问这个IP地址，进入AP的web管理页面，将控制器地址设置为设备的LAN口地址，如下图所示。



② 被管理上的AP可以在设备的AP管理页面上显示，如下图所示。



|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| 查找 | 可以通过匹配关键字来查找表格的数据 |
| 批量编辑 | 用于批量编辑已勾选的AP |
| 重启AP | 用于重启已勾选的AP |
| 升级固件 | 把已勾选的AP升级到新版本 |
| 下载AP固件 | 升级AP前，需要先点击按钮，将AP的固件下载下来后再点击升级固件 |
| 恢复出厂配置 | 将已勾选的AP恢复出厂设置 |
| 删除 | 删除已勾选的离线的AP |
| 隐藏/显示列 | 隐藏或者显示表格的列内容 |
| 用户数 | 指当前连接在这个AP上的无线用户数，可点击查看 |
| 邻居AP | 指内网里的同型号的AP |

③ AP参数配置：设备可以对管理上的瘦AP进行配置的下发，找到AP管理列表中的瘦AP，点击修改按钮即可进入AP参数配置下发的页面，如下图所示。





|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| 工作模式 | 指AP的工作模式，包含Normal，Hybrid，Moniter，默认为Normal模式 |
| 控制器地址 | 指AC的lan口地址，可以为AC的任何lan口地址 |
| AP描述名 | 给AP命名，一般描述AP所处的位置，方便管理AP |
| 无线协议 | 即无线的2G/5G协议 |
| 信道带宽 | 即信道带宽20MHz、40MHz、80MHz |
| 工作信道 | 即AP的信道 |
| 功率 | 即AP的无线发射功率 |
| 最大用户数 | 即该AP最大的带机量 |
| 高级配置 | 默认即可，专业人士也可根据使用环境进行一定的优化 |
| 获取日志 | 点击可获取AP的运行日志 |

### 2.Radio状态

为AP下发ssid后，会显示无线的radio状态，如下图所示。



|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| 信道利用率 | 指该AP所处的信道的利用率，利用率越低代表干扰越小 |
| 查找 | 可以通过匹配关键字来查找表格的数据 |
| 所属AP | 指该状态信息属于哪个AP |
| WLAN状态 | 指该AP的SSID，可点击查看当前配置的SSID |
| 隐藏/显示列 | 隐藏或者显示表格的列内容 |
| 相邻WLAN | 指无线覆盖范围内和自己信道有交集的WLAN |
| 用户数 | 指当前连接在这个AP上的无线用户数，可点击查看 |

### 3.WLAN配置

WLAN配置模块用来配置下发给AP的SSID，如下图所示



|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| SSID | AP的无线网络名称 |
| 编码格式 | SSID的编码格式 |
| 隐藏该SSID | 勾选即隐藏该SSID，无线终端搜索不到该无线信号 |
| 加密类型 | 无线密码的加密类型 |
| 无线密码 | 无线网络的无线密码 |
| 频段 | 可以选择该SSID的生效频段，包括2.4G、5G和双频 |
| 启用VLAN | 可为该SSID绑定VLAN |
| VLAN ID | 802.1q VLAN的vlan标识 |
| 生效AP列表 | 对所有AP生效：对被设备管理的所有瘦AP都生效  选择其他：可以选择该无线网络生效的具体AP |

### 4.无线用户

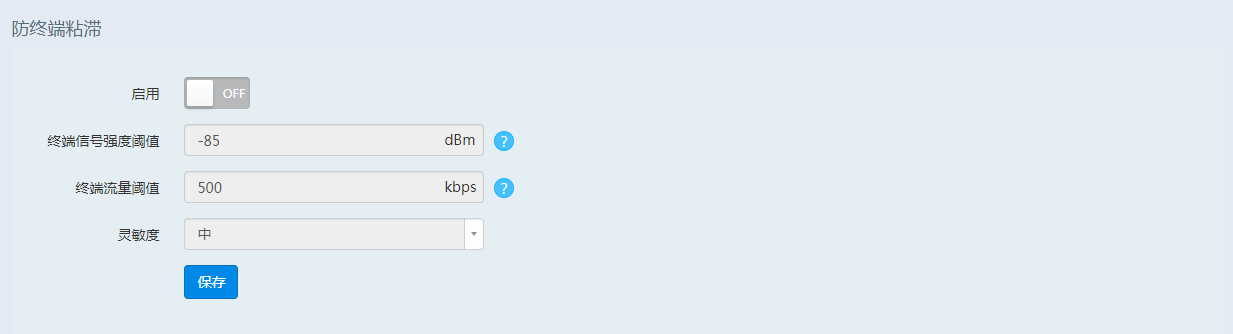
在这里可以查看所有连接无线的终端，如下图所示。



|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| 查找 | 可以通过匹配关键字来查找表格的数据 |
| 所属AP | 该无线用户连接的AP |
| MAC | 指该无线终端的MAC地址 |
| 接入频段 | 指该无线终端使用的无线频段 |
| IP地址 | 该无线终端获取到的IP地址 |
| SSID | 该无线终端所连接的SSID |
| 信号强度 | 该无线终端所连接的SSID的信号强度 |

### 5.防终端粘滞

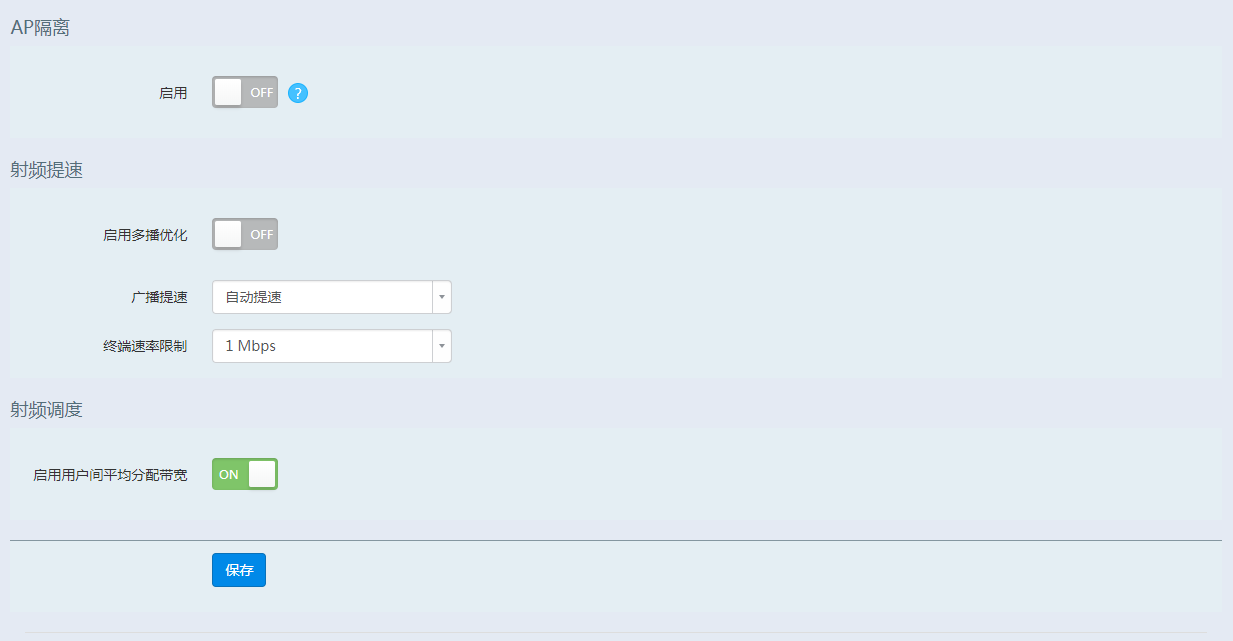
该功能用于做无线漫游，识别到用户的无线达到设置的条件时，主动踢掉用户，漫游到另一个AP上，该功能默认不开启。



|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| 终端信号强度阀值 | 是指AP接收到的无线客户端的信号强度，是AP踢掉无线用户的一个条件，无线用户的信号强度小于该值，则满足条件。 |
| 终端流量阀值 | 指无线用户的实时无线流量速率，低于该值，则满足AP踢掉用户的条件。 |
| 灵敏度 | 是指AP检查到某个无线用户满足以上2个条件的次数，灵敏度越高越容易剔除用户。 |

### 6.无线优化

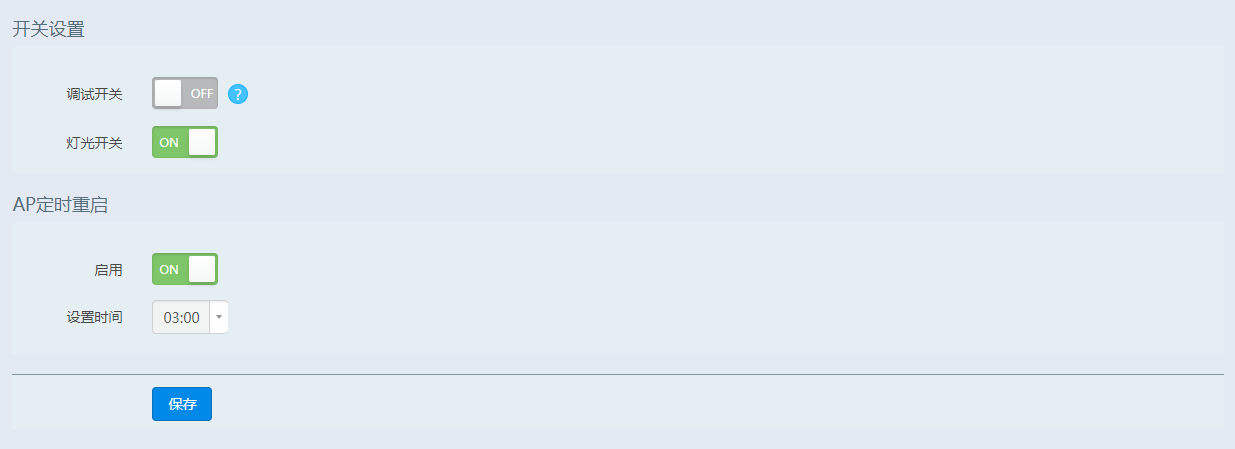
在该配置页面可以对无线进行一定的优化，具体功能如下图所示。



|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| AP隔离 | 同一个AP下面的无线用户之间的隔离 |
| 广播提速 | 经过AP的广播包的提速，建议提速到2Mbps或者5.5Mbps |
| 终端速率限制 | 无线终端接入速率的限制，速率指的是无线网卡跟AP协商的速度，建议使用1Mbps或者2Mbps |
| 启用多播优化 | 对经过AP的多播包进行优化 |
| 启用用户间平均分配带宽 | 指的是无线用户的时间公平机制，有利于提升无线的使用效率 |

### 7.调试功能

在该页面下，可以对瘦AP进行一些调试，具体功能如下图所示。



|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| 调试开关 | 开启后，会不断的检测无线的信道使用率，默认关闭 |
| 灯光开关 | 用来开启或关闭瘦AP灯光的开关 |
| AP重启 | 用来设置AP重启的时间，默认每天凌晨三点重启一次 |

## 七、用户认证

弱行为管理4.1设备支持自动认证、portal认证（包括web认证和微信认证）和云端认证。只有认证成功的用户才能够进行网络访问，否则不能进行网络访问。

### 1.认证选项

新用户认证方式下，有多个认证选项，包括本地认证设置、云端认证设置和全局认证设置，如下图所示。





① 用户认证后，有两种下线方式。一种为无流量超时下线，即用户和设备的连接断开后，超过指定时常下线。一种为超时强制下线，即用户上线超过指定时间后，就会强制下线。

② 放通网站列表：可以指定网站进行放通，被放通的网站，可以被没有认证的终端访问。

③ 临时放通时间：对于非安卓设备，每次触发认证后，可以指定一段时间对终端进行放通，让终端在这期间可以正常上网。

④ 云端认证设置：包括云端放通网站列表和云端白名单MAC列表，该设置不可以在设备上手动修改，需要在云端下发配置到设备。

⑤ 用户认证抢占：当设置web认证时，开启此选项后，同一帐号下，新用户优先登录。

⑥ Https弹认证页面：开启此选项后，终端未认证情况下访问https网站，会重定向到portal页面。

⑦ 认证重定向地址：重定向到认证页面的IP地址，注意不能填写lan口和wan口的IP地址。

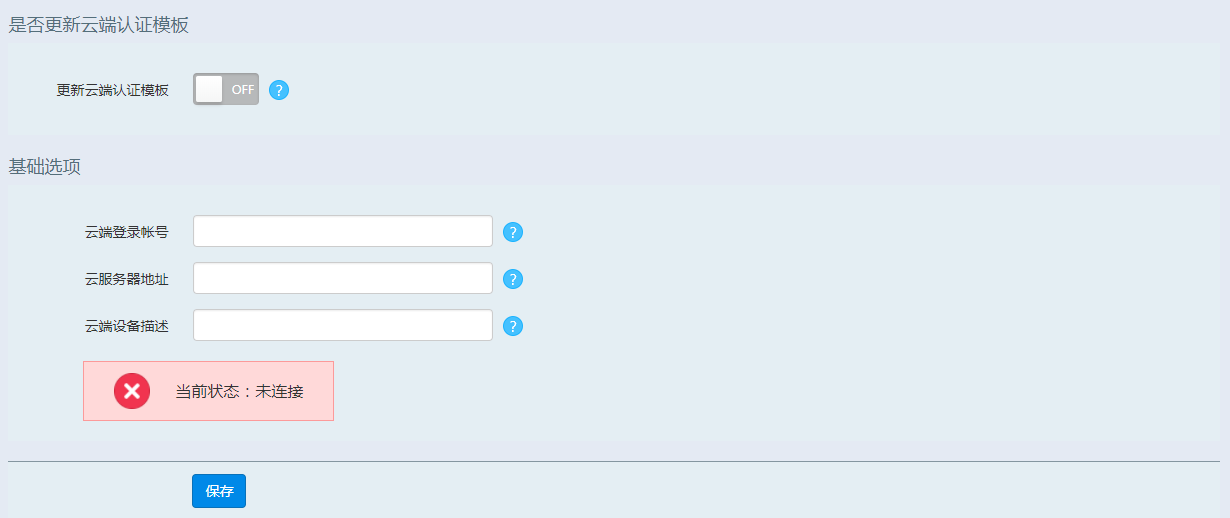
### 2.用户管理

该模块用来配置WEB认证的帐号和密码，如下图所示。



|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| 帐号 | 用于web认证的帐号 |
| 描述 | 帐号的描述信息 |
| 密码 | 用于web认证的密码 |
| MAC绑定 | 表示只允许框中的MAC地址的终端使用此帐号密码 |
| IP绑定 | 表示只允许框中的IP地址的终端使用此帐号密码 |
| 同时勾选MAC绑定和IP绑定 | 表示需要同时满足两个条件的的终端可以使用此账号密码 |
| 允许多用户使用 | 表示允许多个终端同时使用此帐号密码 |
| 过期时间 | 表示此帐号密码的过期时间 |

### 3.云端管理

在这里可以将设备加入云端，方便管理。设备加入云端后，可以使用云端的认证模版，如下图所示。

① 若想使用云端认证，需要勾选“更新云端认证模版”。如果不勾选，云端认证模版无法下载，已下载的认证模版不会更新。

② 设备下载云端认证模版的方式有两种，一种是设备会定时向云端发送请求，自动下载模版，还有一种是管理员控制云端，手动向设备下发模版，比起第一种来说，更具时效性。

### 4.四种认证方式

#### ⑴ 自动认证

默认情况下，路由器接入互联网后，连接到路由器的客户端即可访问互联网。这是因为此时的认证方式为自动认证，接入设备的终端均可自动认证成功。

#### ⑵ web认证

若想对设备下的终端进行web认证，需要添加一条web认证策略，如下图所示。

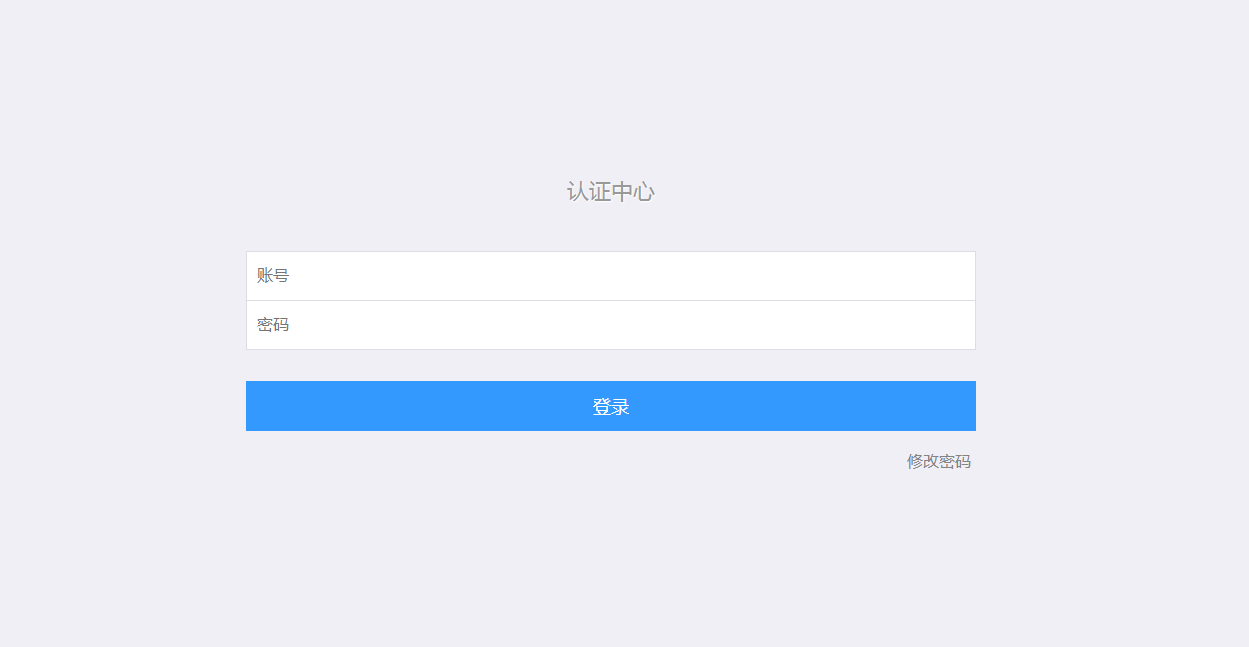


① IP组：选择该认证的使用范围，可以在组设置中自定义设置IP组，默认为“ALL”，表示对所有IP生效。

② 认证成功后重定向地址：认证成功后可重定向的网址，可以填写想要重定向的域名，如不填，认证成功后则会跳转到www.baidu.com。

③ 高级配置：可以设定免认证的IP或MAC，默认为“NONE”，表示没有免认证的IP或MAC。

④ 认证过程：开启web认证后，处于Web认证生效范围的终端打开浏览器，访问任一网页的时候会弹出认证页面，账号和密码即用户管理里面添加的账号和密码，如下图所示。



注：在该页面，终端用户可以点击“修改密码”，修改已知账号的密码。

#### ⑶ 微信认证

若想对设备下的终端进行微信认证，需要添加一条微信认证策略，如下图所示。



① 微信认证的相关配置信息，包括门店名称、Shop Id、Appld和Secrekey，这些信息在微信公众号中提取输入即可。

② 其它配置参数同web认证。

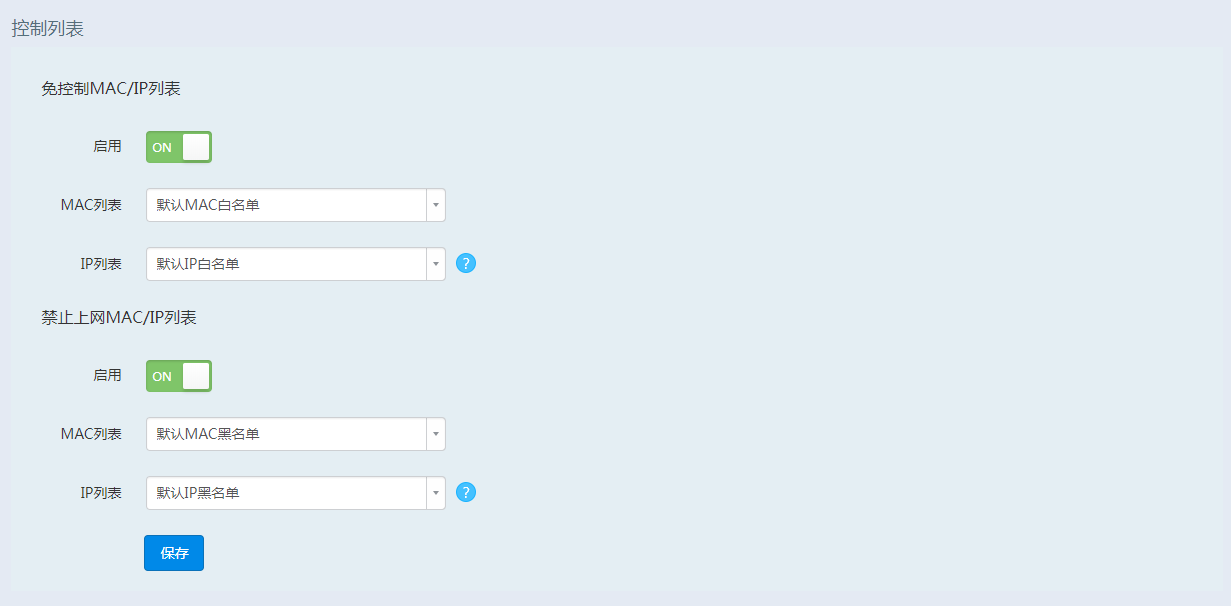
③ 若想同时使用web认证和微信认证，只需在同一条认证规则中同时勾选“web认证”和“微信认证”即可。

#### ⑷ 云端认证

若想对设备下的终端进行云端认证，首先需要从云端下载好认证模版，详见云端管理。下载好云端模版后，需要再添加一条云端认证策略，如下图所示。

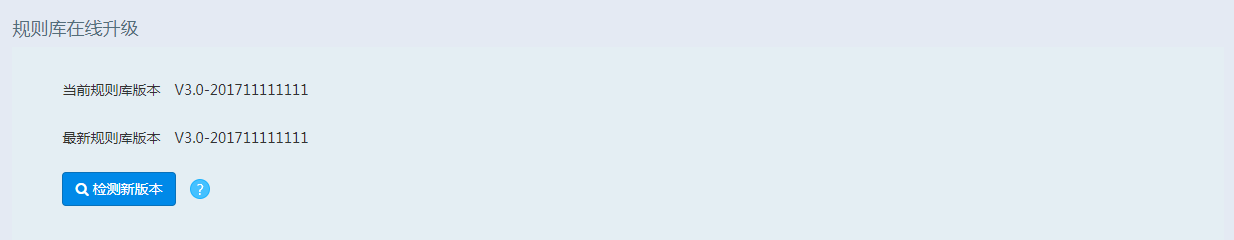
## 八、应用控制

弱行为管理应用控制模块基本功能包括：控制列表、URL控制规则以及应用控制规则。注意：使用应用控制模块的功能，需要将全局禁用启用按钮设置为启用，如图下图所示：









**1.控制列表**

① 免控制MAC/IP列表：勾选启动按钮，说明本列表内的MAC和IP对应的终端不受应用策略的控制。

② 禁止上网MAC/IP列表：勾选启动按钮，说明本列表内的MAC和IP对应的终端不能够进行上网行为。

### 2.URL控制规则

① URL控制协议是要靠用户手动添加的，即在URL组中配置。点击“新增”，弹出URL控制的基本配置选项，如下图所示。



|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| 动作 | 设有允许和阻断规则，表示对相应协议识别后的动作 |
| 时间组 | 表示被控制的时间段（可在时间组内自定义） |
| 源IP组 | 表示被控制的IP组（可在IP组内自定义） |
| 目的IP组 | 表示被控制访问的目的IP（可在IP组内自定义，一般情况下为ALL） |

② URL控制协议的选择：在基本配置选项中，点击“点击更改协议”，弹出URL组的选择页面，从中选择需要被控制访问的URL。

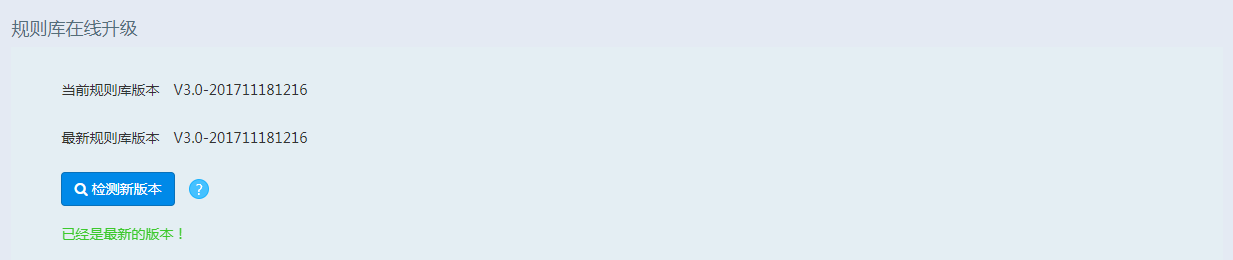
### ****3.应用控制规则****

① 应用控制协议包含多种协议，可根据需要选择用户上网是否需要受到控制，点击“新增”，弹出应用控制的基本配置选项，同URL控制规则一致。

② 应用控制协议的选择：在基本配置选项中，点击“点击更改协议”，弹出协议的选择页面，从中选择需要被控制访问的协议，如下图所示。



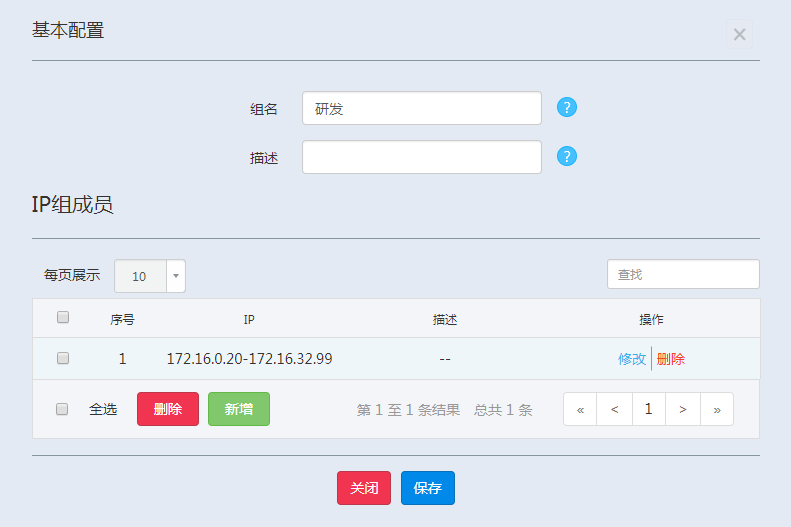
③ 规则库在线升级：弱行为管理的规则库会有不定期的更新，包括新添加的协议和更新的协议，点击“检测新版本”，即可检测规则库是否为最新，如果为最新，显示如下图所示；如果不是最新，会自动弹出在线升级的选项。



### 4.配置案例

场景描述：某公司内部研发部门的IP地址为：172.16.0.20-172.16.32.99，公司决定不允许研发部的电脑在上班的时间：周一至周五 上午8：00-12：00 下午14：00-18：00访问http协议的所有网址。

步骤1：在“IP组”中创建一个172.16.0.20-172.16.32.99网段的IP组，如下图所示。



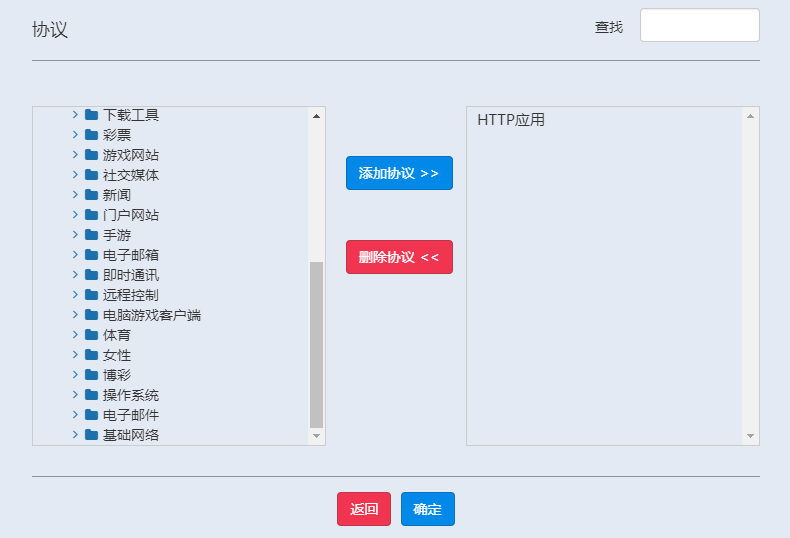
步骤2：在“时间组”中创建一个“周一至周五 上午8：00-12：00 下午14：00-18：00”的上班时间的时间组，如下图所示。



步骤3：点击“应用控制规则”中的“新增”按钮，配置如下图所示。



步骤4：点击“点击更改协议”，在弹出的协议中选择HTTP应用，如下图所示。

 步骤5：点击保存按钮，使用研发部的电脑访问http协议的网站，无法访问。

### 5.控制日志

在该页面可以显示终端上网的受控制记录，如下图所示。



## 九、审计

弱行为管理审计模块基本功能包括：免审列表 、审计规则、审计配置、上网行为审计、用户上下线记录、审计统计6个功能。

### 1.免审列表

① 免审计MAC/IP列表：勾选启用按钮，说明本列表内的MAC和IP对应的终端不受审计规则的控制，如下图所示：



### 2.审计规则

审计规则页面如下图所示：



① 审计控制规则是要靠用户手动添加的，即在审计控制规则列表中。点击“新增”，弹出审计控制的基本配置选项，如下图所示。



|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| 时间组 | 表示被控制的时间段（可在时间组内自定义） |
| 源IP组 | 表示被控制的IP组（可在IP组内自定义） |
| 目的IP组 | 表示被控制访问的目的IP（可在IP组内自定义，一般情况下为ALL） |

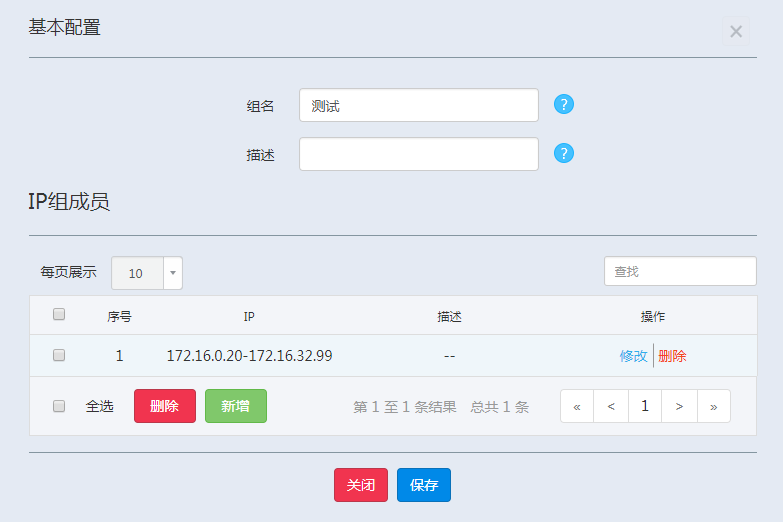
② 审计控制协议的选择：在基本配置选项中，点击“点击更改协议”，弹出协议的选择页面，从中选择需要被审计控制的协议，如下图所示。



### 3.配置案例

场景描述：某公司内部测试部门的IP地址为：172.16.0.20-172.16.32.99，公司要审计测试部的电脑在上班的时间：周一至周五 上午8：00-12：00 下午14：00-18：00的上网行为。

步骤1：在“IP组”中创建一个172.16.0.20-172.16.32.99网段的IP组，如下图所示。



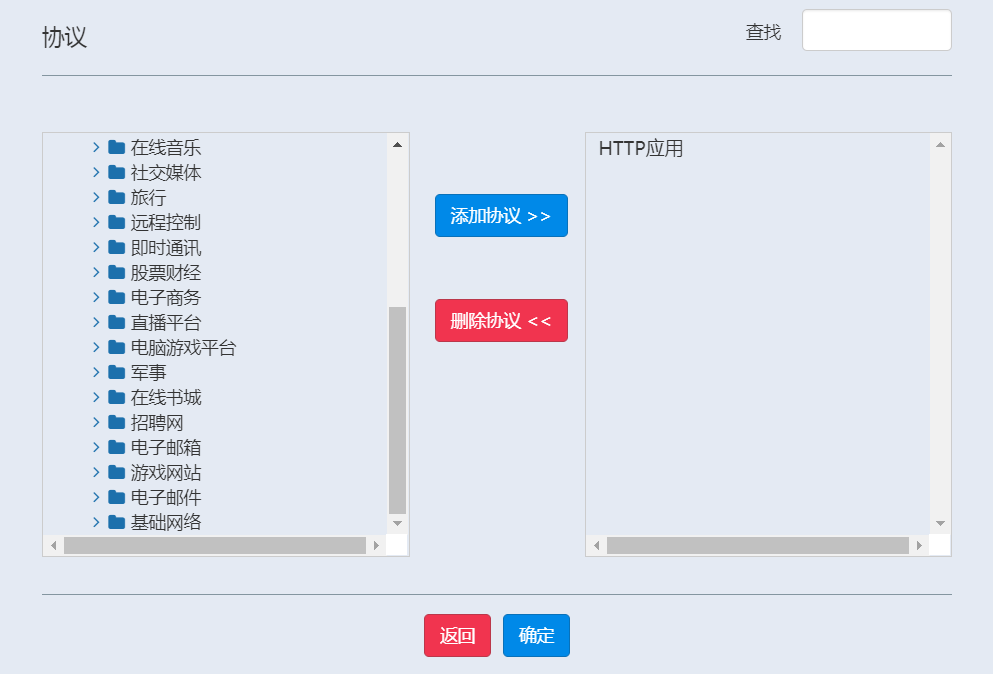
步骤2：在“时间组”中创建一个“周一至周五 上午8：00-12：00 下午14：00-18：00”的上班时间的时间组，如下图所示。



步骤3：点击“审计控制规则”中的“新增”按钮，配置如下图所示。



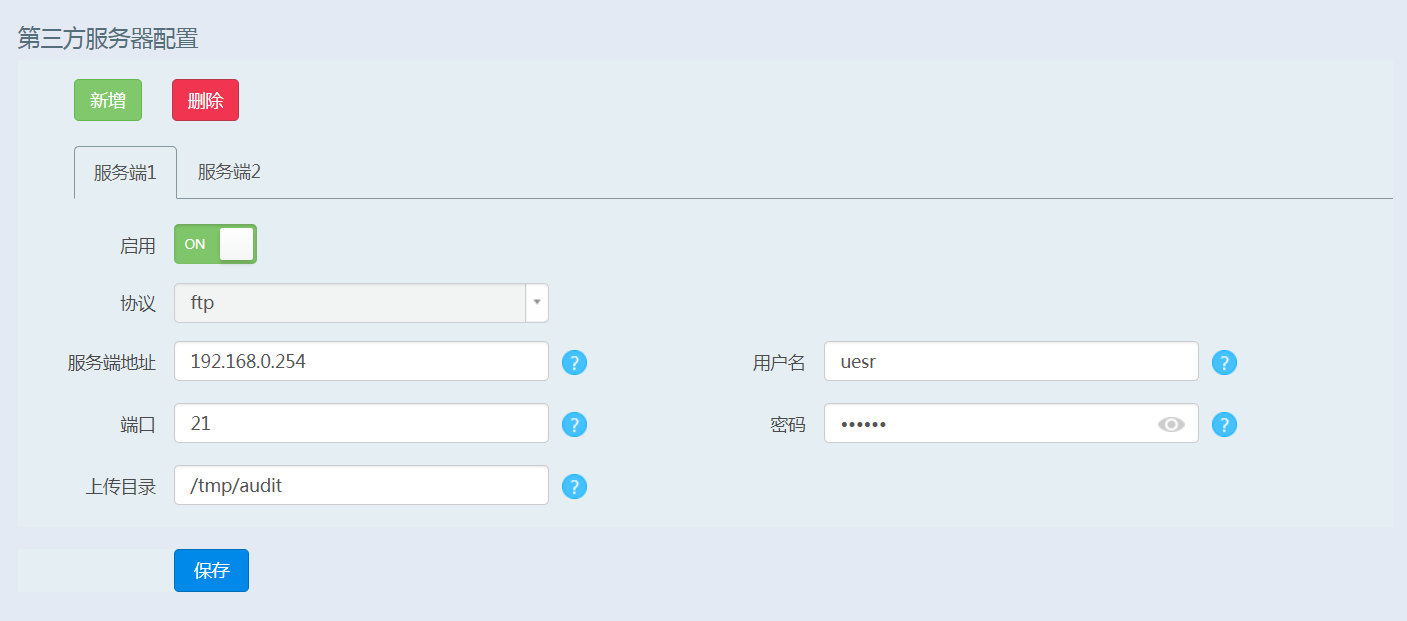
步骤4：点击“点击更改协议”，在弹出的协议中选择HTTP应用，如下图所示。

 步骤5：点击保存按钮，使用测试部的电脑访问网站，在上网行为审计页面只能看到该终端的http应用的上网行为，如下图所示：



### 4.审计配置

在该页面可以配置第三方服务器，在该服务器的目录下就可以查看到第三方服务器的上网行为记录，第三方服务器配置如下图所示：



|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| 增加 | 点击“增加”按钮，可以增加一个服务端 |
| 删除 | 点击“删除”按钮，可以删除一个服务端（没选择服务端时，是从后面开始删除） |
| 启用 | 勾选上“启用”按钮，点击“保存”，配置才生效 |
| 协议 | 可以选择FTP服务器和http服务器 |
| 服务端地址 | 填写该服务器的地址 |
| 用户名 | 填写该服务器的用户名 |
| 端口 | 填写该服务器的端口号 |
| 密码 | 填写该服务器的密码 |
| 上传目录 | 该服务器的上网行为记录的存放目录（该选项不填时，默认是根目录） |

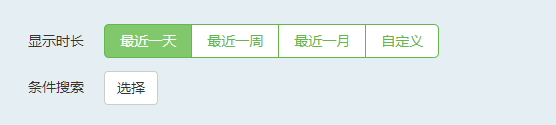
### 注：服务器配置好，记得点击“保存”，过5分钟就能在上传目录下看到该服务器的上网行为记录数据压缩文件。

### 5.上网行为审计

在该页面可以显示终端上网的上网行为记录，如下图所示。



①在上网行为审计页面可以选择显示时长进行搜索，如下图所示：



②在上网行为审计页面可以选择条件进行搜索，点击“选择”按钮，进入搜索条件页面，如下图所示：



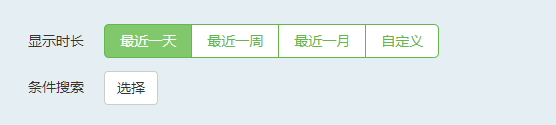
③在上网行为审计页面的下方，点击“导出”按钮，可以导出上网行为数据。

### 6.用户上下线记录

在该页面可以显示用户上下线记录，如下图所示。



①在用户上下线记录页面可以选择显示时长进行搜索，如下图所示：



②在用户上下线记录页面可以选择条件进行搜索，点击“选择”按钮，进入搜索条件页面，如下图所示：



③在用户上下线记录页面的下方，点击“导出”按钮，可以导出用户上下线记录数据。

### 7.审计统计

在该页面可以显示审计的统计数据，如下图所示：



①显示时长、条件搜索、导出功能跟用户上下线记录页面的功能一样。

②网站类型选框：可以选择网站类型进行搜索数据

③展示方式输入框：图表可以选择排名前几的数据进行显示

## 十、组设置

主要包括下面的4个模块，分别是：IP组、MAC组、URL组及时间。

### 1.IP组

下图显示的是IP组的默认页面。如下图所示：



①查找：可以通过匹配关键字来查找列表的数据。

②组名：IP组的名称，方便用户区分添加的IP组。

③成员数：IP组成员数量，点击可查看IP组中IP组成员。如下图所示：



④操作：可对IP组进行修改及删除。

⑤新增：点击新增可以添加IP组及IP组的成员。如下图所示：





### 2.MAC组

下图显示的是MAC组的默认页面。如下图所示：



①查找：可以通过匹配关键字来查找列表的数据。

②组名：MAC组的名称，方便用户区分添加的MAC组。

③成员数：MAC组成员数量，点击可查看MAC组中MAC组成员。如下图所示：



④操作：可对MAC组进行修改及删除。

⑤新增：点击新增可以添加MAC组及MAC组的成员。如下图所示：





### 3.URL组

下图显示的是URL组的默认页面。如下图所示：



①查找：可以通过匹配关键字来查找列表的数据。

②组名：URL组的名称，方便用户区分添加的URL组。

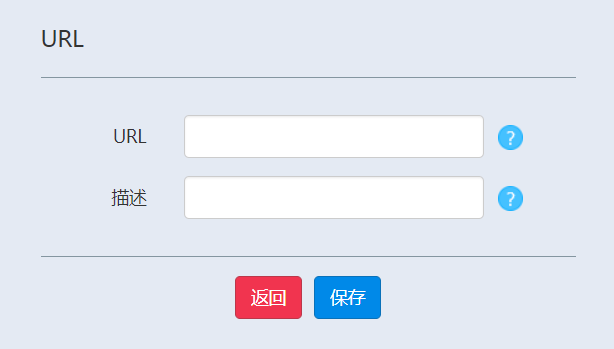
③成员数：URL组成员数量，点击可查看URL组中URL组成员。如下图所示：



④操作：可对URL组进行修改及删除。

⑤新增：点击新增可以添加URL组及URL组的成员。如下图所示：





### 4.时间组

下图显示的是时间组的默认页面。如下图所示：



①查找：可以通过匹配关键字来查找列表的数据。

②组名：时间组的名称，方便用户区分添加的是时间组。

③周期：为期一周（包含周一、周二、周三、周四、周五、周六、周日）。

④生效时间段：指可生效的时间段，精确到1分钟。

⑤操作：可对时间组进行修改及删除。

⑥新增：点击新增可以添加时间组，配置如下图所示：



## 十一、流量控制

该页面可以对终端进行限速配置，如下图所示。



### 1.总出口带宽配置

① 总出口上传配置：表示对wan口的上传速度限制，如果有多个wan口，则表示所有wan口的上传速度之和。

② 总出口下载配置：表示对wan口的下载速度限制，如果有多个wan口，则表示所有wan口的下载速度之和。

### 2.流量策略配置

点击新增，可以看到流量策略的配置页面，如下图所示。



|  |  |
| --- | --- |
| 按钮和参数 | 说明 |
| 地址范围 | 用户的IP在这个范围内时，才进行流量控制 |
| 时间组 | 表示规则生效的时间段（可在时间组内自定义） |
| 共享下载 | 该地址范围内，所有用户最大的下载速度 |
| 共享上传 | 该地址范围内，所有用户最大的上传速度 |
| 单机下载 | 单个用户最大的下载速度 |
| 单机上传 | 单个用户最大的上传速度 |

### 3.配置案例

场景描述：某公司局域网为172.16.0.1/24,现需要对局域网下的客户端设置流量控制，每个客户端都有固定的带宽，IP地址为172.16.0.50-172.16.0.5.250，带宽限制时间段为上班时间：8：00-18：00，周一至周五。

步骤1：进入组设置-时间组，新增一个名为“上班时间”的时间组，并将公司的上班时间添加至该时间组。如下图所示：





步骤2：进入流量控制，点击“新增”，进入流量配置页面。如下图所示：



步骤3：设置名称为“流量控制”，地址范围为“172.16.0.50-172.16.0.5.250”，时间组选择“上班时间”，共享下载设置为“12MBytes”，共享上传设置为“2MBytes”，单机下载设置为“500KBytes”，单机上传设置为“100KBytes”，点击保存。如下图所示：





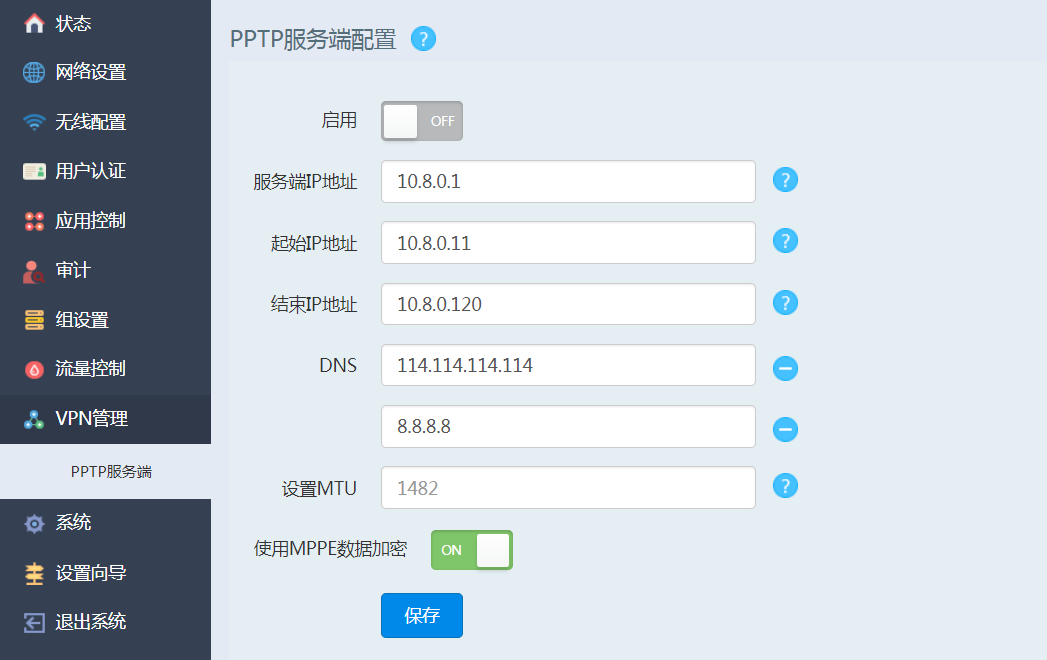
步骤4：IP地址为172.16.0.50-172.16.0.5.250的客户端用户，在上班时间周一至周五，8：00-18：00的时间段内最大下载速率为500KBytes，最大上传速率为100KBytes。

## 十二、VPN管理

当远程客户端通过服务端提供的账号、密码拨号连接上服务端时，便与服务端形成一个私有局域网，客户端可以访问服务端内网共享的信息，达到跨越公网来构建私网的目的。用于远程办公或文件、数据加密传输。

### 1.PPTP服务端

在PPTP服务端，可以设置路由器为PPTP服务端。如下图所示：





①启用：启用后，路由器作为PPTP服务端。可通过“ON/OFF”对PPTP服务端进行禁用、启用。

②服务端IP地址：PPTP服务端的IP地址。

③起始/结束IP地址：PPTP服务端分配给PPTP客户端的地址段。

④DNS：PPTP服务端分配给PPTP客户端的DNS。

⑤MTU：可根据需求，手动填写，MTU默认为1482。

⑥使用MPPE数据加密：是否启用MPPE数据加密。服务端与客户端要设置一致，仅适用于 PPTP。

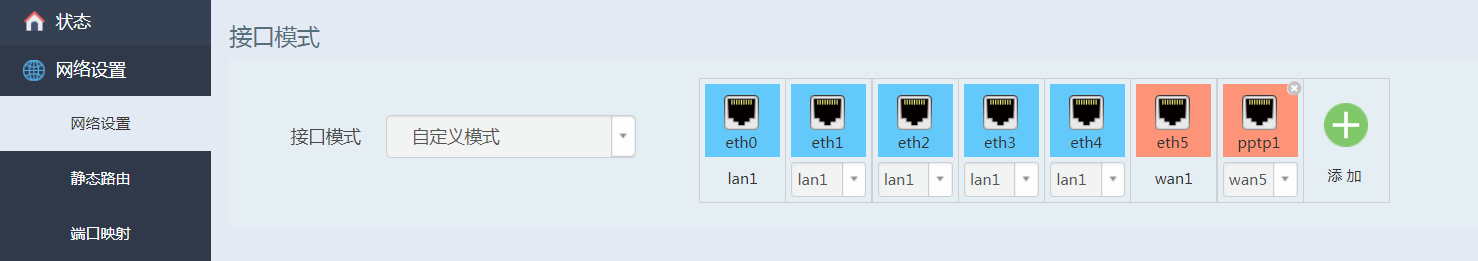
⑦账号信息：设置PPTP客户端连接PPTP服务端时使用的账号和密码。点击“新增”即可添加。如下图所示：



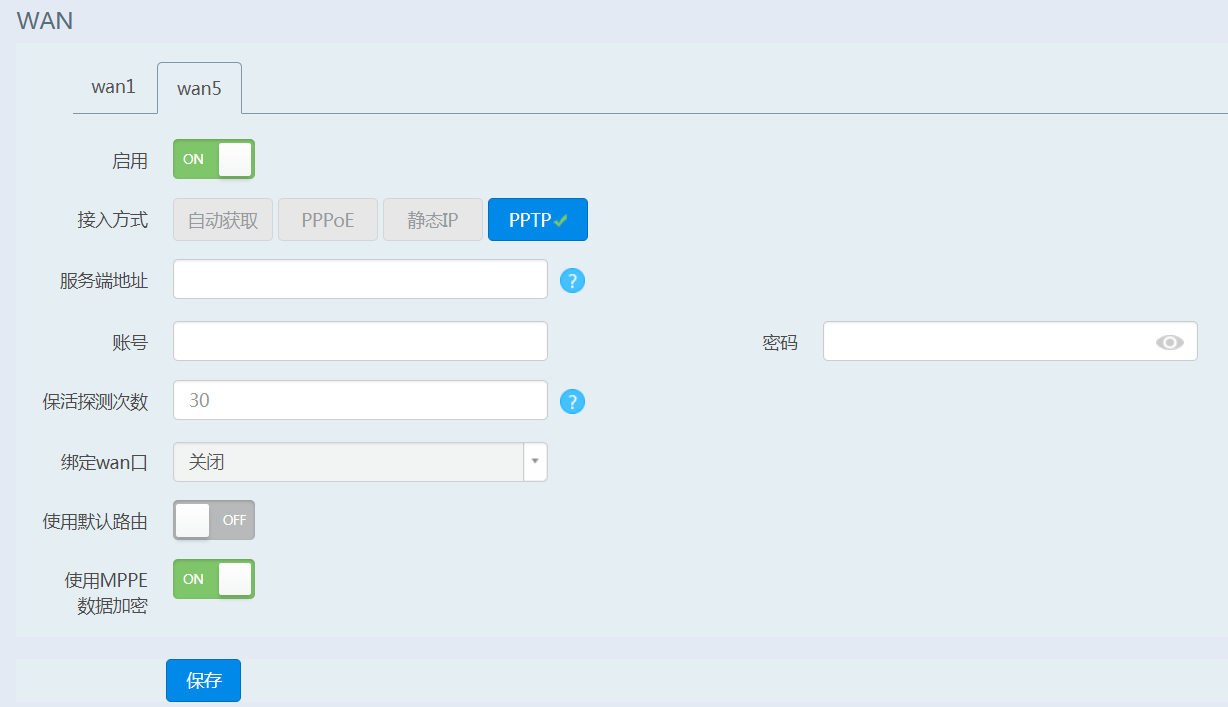
⑧用户信息：页面展示的为PPTP客户端成功连接PPTP服务端的用户名、虚拟接口、PPTP服务端所分配的IP、拨入IP及连接时间。

### 2.PPTP客户端

PPTP客户端需要在网络设置中的接口模式中添加。接口模式选择自定义模式，添加PPTP虚拟接口。如下图所示:



PPTP客户端配置页面，如下图所示：



①启用：启用后，路由器作为PPTP客户端。可通过“ON/OFF”对PPTP客户端进行禁用、启用。

②服务端地址：PPTP服务端的公网IP地址，需填写正确，才能连接PPTP服务端。

③账号及密码：输入PPTP服务端分配给PPTP客户端的账号及密码。

④保活探测次数：连续探测失败一定次数后，认为连接断开，开始重新连接。每次探测时间间隔为5s，默认探测次数为30次。探测次数取值范围1-60，取值越小，灵敏度越高，如无特殊需要，建议不要修改。

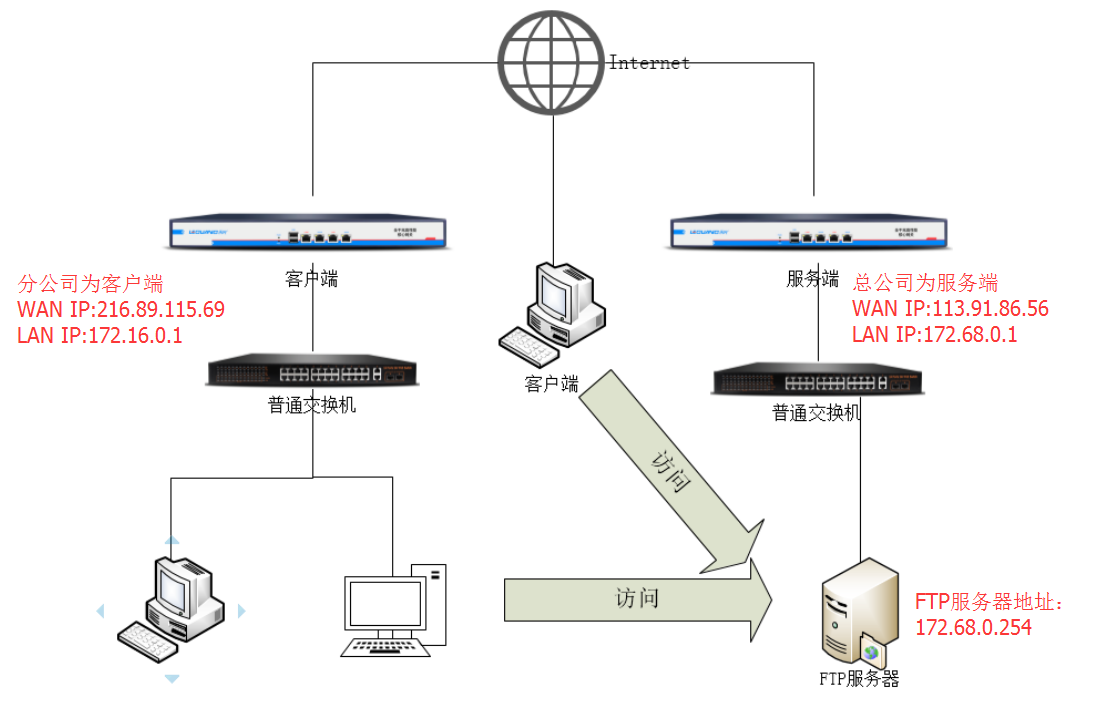
⑤绑定wan口：多wan的场景下，用户可以通过指定wan口建立pptp拨号连接，实现最优的VPN线路。

⑥使用默认路由：启用此项将会创建一条指向PPTP服务端的默认路由，优先级最高。

⑦MPPE数据加密：数据加密功能，要确保和服务端保持一致，否则将会无法连接。

### 3.配置案例

场景描述：某公司总部和分部使用路由器进行网络搭建，分公司员工需要随时经过互联网访问公司总部的资源，这些资源包括：公司的内部资料、项目管理系统、办公OA等。可以在路由器上设置VPN服务，实现公司分部员工访问公司总部服务器。拓扑图如下图所示：



步骤1：设置充当服务器的路由器。

①进入VPN管理-PPTP服务端，点击启用PPTP服务端。

②服务器IP地址、起始/结束IP地址、DNS 及MTU均为默认值。

③启用MPPE数据加密后，点击保存。如下图所示：



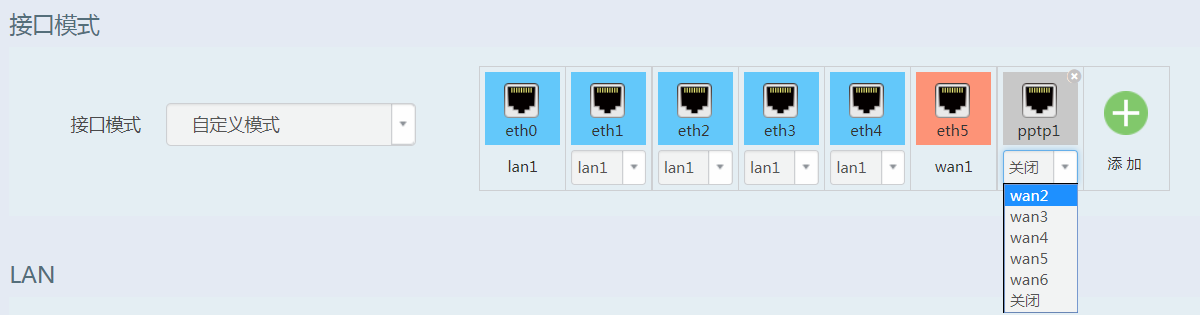
④添加允许接入的账号和密码，点击“新增”。例：添加账号和密码为“zhangsan”，点击保存。如下图所示：



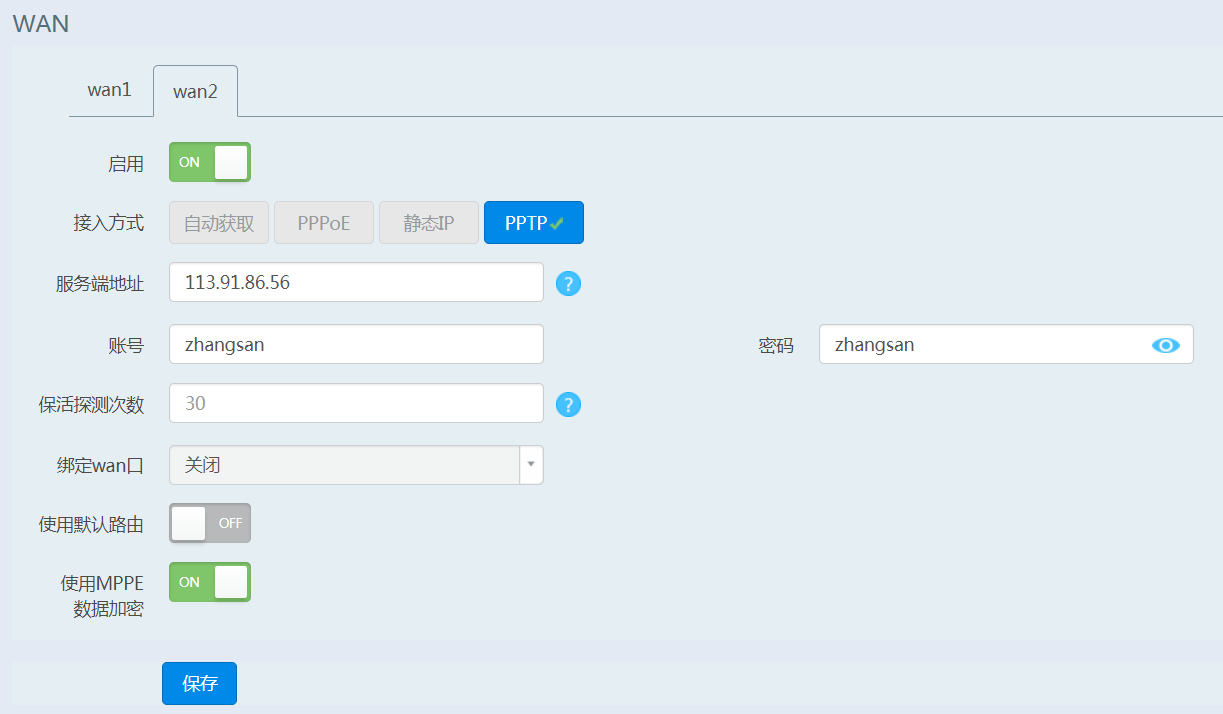


步骤2：设置充当客户端的路由器。

①进入网络设置-在自定义模式下添加PPTP接口，选择PPTP接口为WAN2。如下图所示：



②进入WAN2口配置，服务端地址为服务端公网IP地址、帐号和密码为“zhangsan”、保活探测次数为默认30、绑定wan口为关闭，使用默认路由为禁用，启用MPPE数据加密，点击保存。如下图所示：



步骤3：进入状态-总览页面，查看wan2口接口状态，是否成功连接服务端，成功则如下图所示：

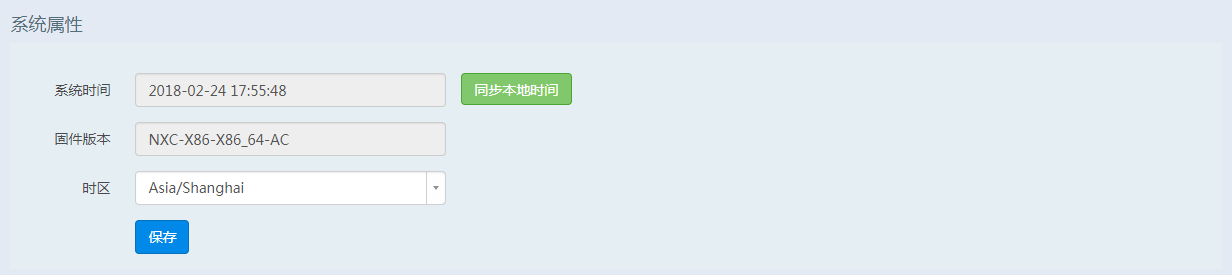


步骤4：VPN 连接成功后，分公司员工可以访问总公司资源。分公司访问总公司 FTP 服务器内容为例。FTP服务器地址：172.68.0.254、端口：21。分公司员工直接在浏览器中输入“FTP://172.68.0.254:21”，即可访问总公司的FTP服务器。

## 十三、系统

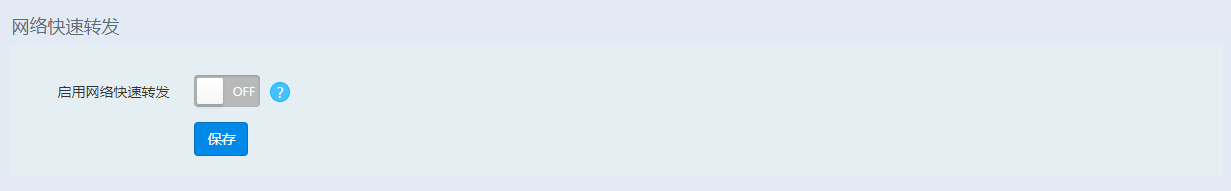
### 1.系统属性

此页面显示系统的基本属性，包括系统时间、固件版本以及时区，通过此页面可以设置时区和同步本地时间，如下图所示。



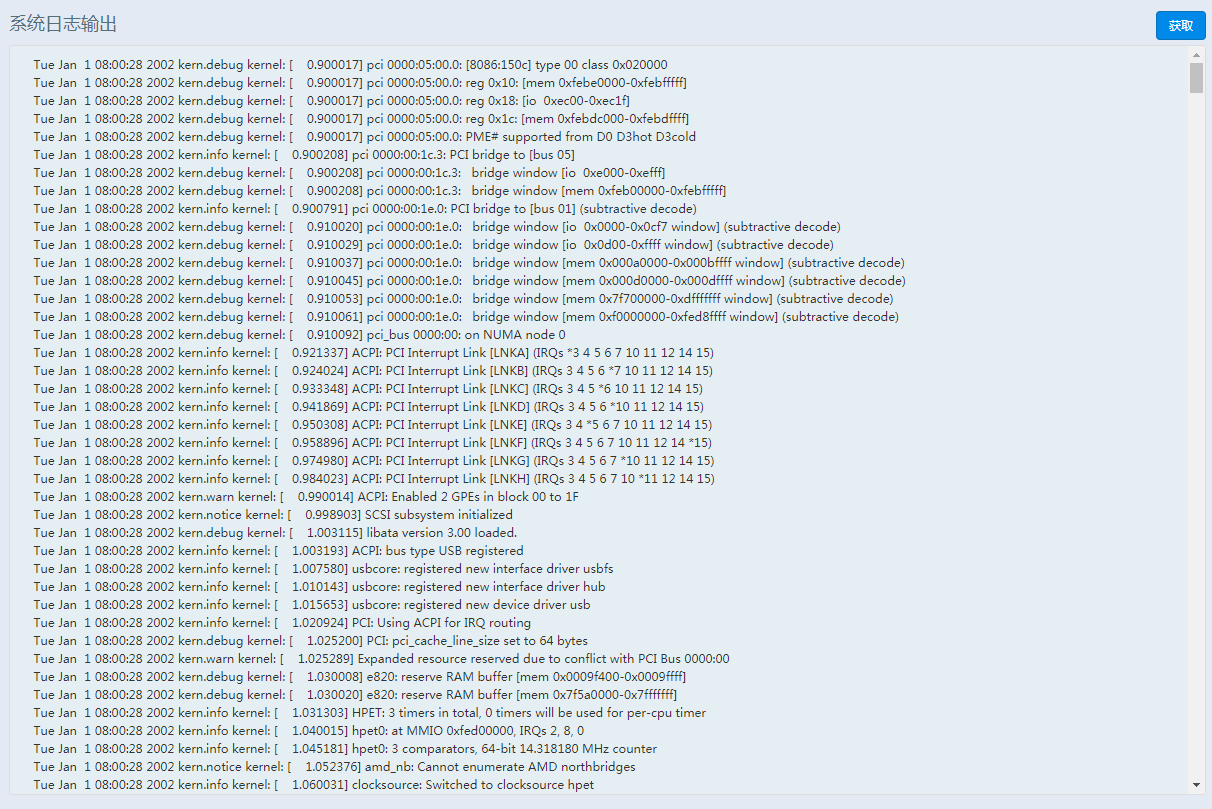
### 2.网络快速转发

开启快速转发后，设备吞吐性能提升近100%，但与其关联的的功能包括“用户认证”、“流量控制”、“应用控制”、“应用识别”以及“流量统计”会停止使用，请酌情开启！



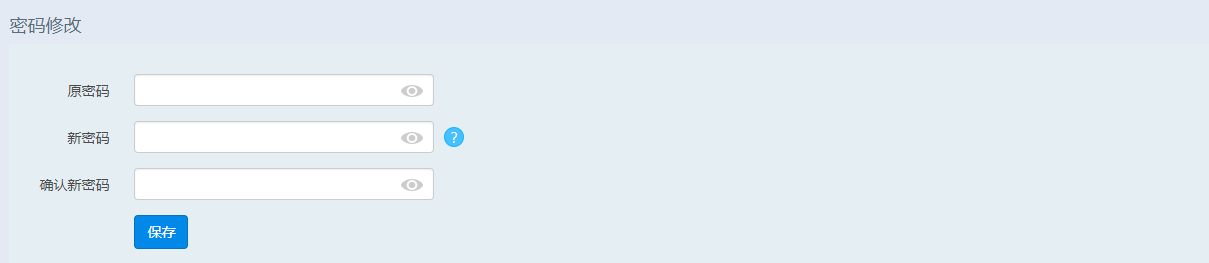
### 3.系统日志

该功能可以查看系统的运行日志，管理员可以据此检查系统异常，例如拨号失败等问题，如下图所示。



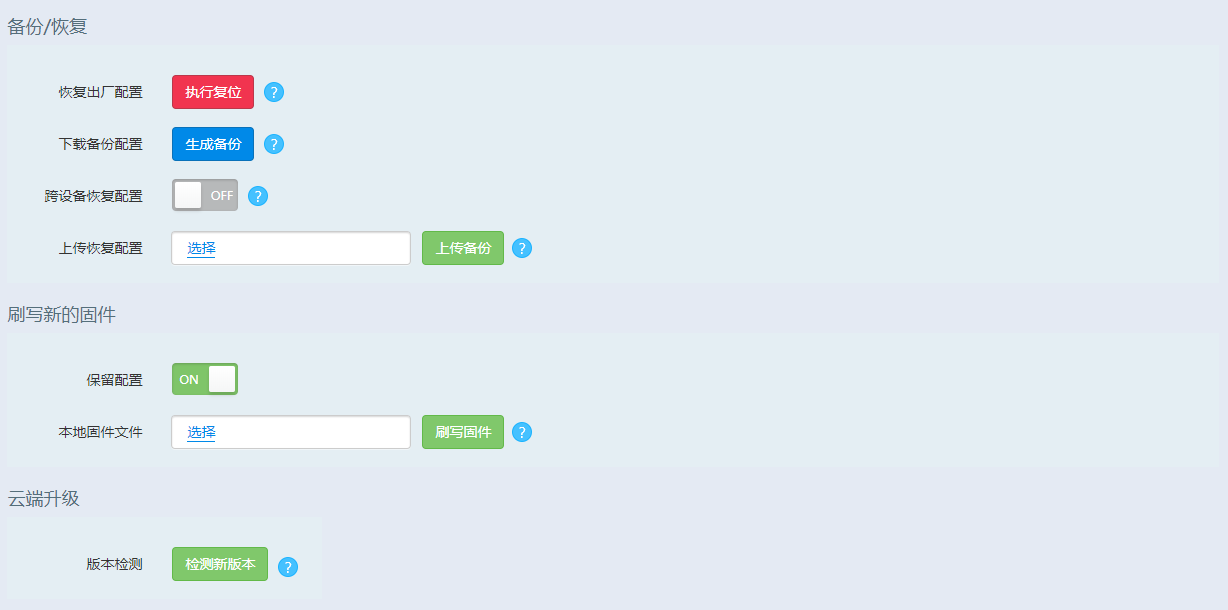
### 4.密码修改

修改系统web管理密码的页面，根据提示即可修改密码，如下图所示。



### 5.备份/升级

在此页面可以进行备份/升级，具体包括执行复位、生成备份、上传备份、刷写固件以及在线云端功能，如下图所示。



① 执行复位：表示重置当前系统配置文件，即恢复出厂配置。

② 生成备份：下载备份当前系统配置文件，可用于恢复配置。

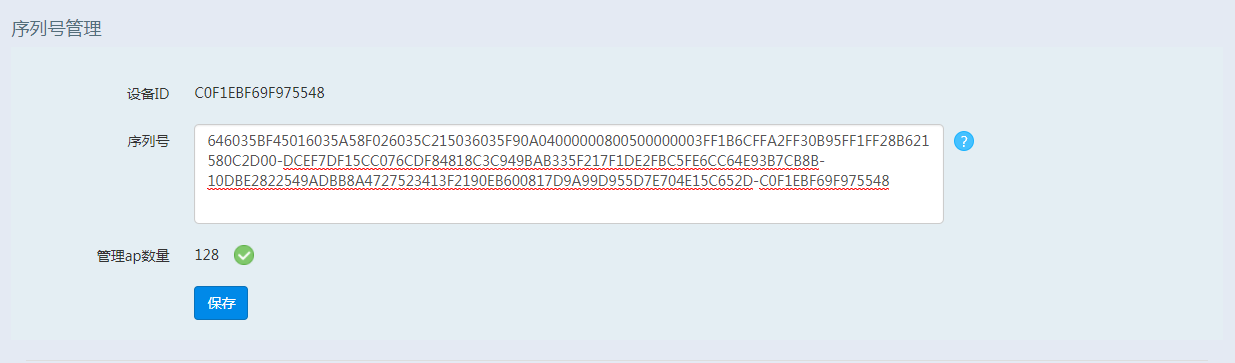
③ 上传备份：将系统的配置文件上传，覆盖现有的配置。

④ 刷写固件：上传固件，进行本地升级。当勾选“保留配置”时，当前的配置不会随着升级而消失；若不勾选“保留配置”，系统升级后，会恢复出厂设置。

⑤ 云端升级：需要结合云端使用，当云端上存在新的固件版本时，可以在线升级。

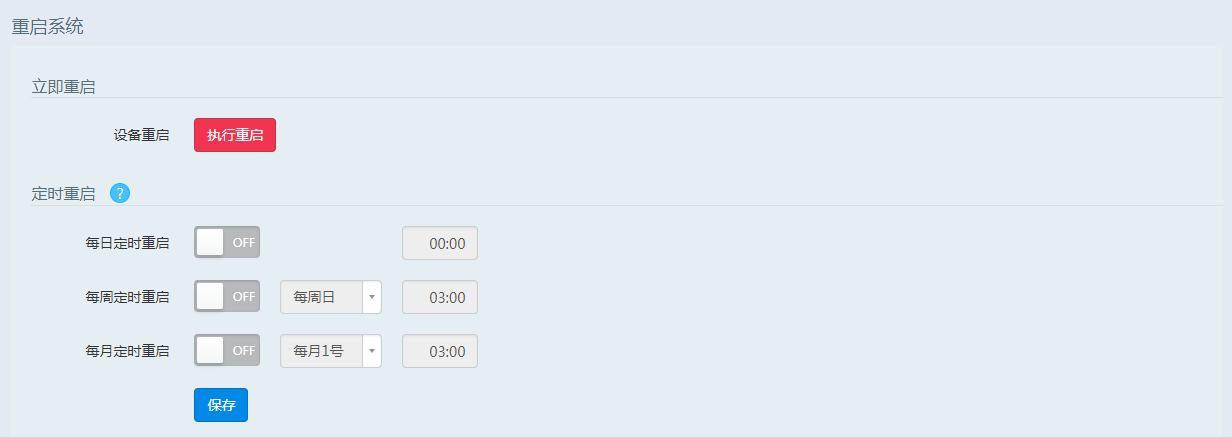
### 6.序列号管理

设备若想管理瘦AP，需联系售后，获得授权，下图显示的是管理128个AP的授权。



### 7.重启

包含立即重启和定时重启功能，用户可自行选择，如下图所示。



## 十四、设置向导

弱行为管理配置了设置向导，方便用户对设备的简单操作，用户首次登录设备的Web页面后会自动弹出设置向导的页面，之后若想进行设置向导需要手动点击“设置向导”，如下图所示。



① 选择“下一步”后，会弹出三种上网配置方式的选择，如下图所示。用户根据自身的情况选择其中一种配置方式，然后点击“下一步”即可。



② 进入下一步配置无线，用户可新建一个SSID，也可在配置方式中选择已经存在的SSID进行修改，如下图所示，配置完成后，点击完成即可简单的接入网络和配置无线了。



## 附录：版本更新说明

### 新增功能：

1. 网络诊断新增“审计开关”功能

2.新增“免审列表”功能：列表内的MAC和IP对应的终端不受审计规则的控制

3.新增“审计规则”功能：制定审计规则。

4.新增“审计配置”功能：可以配置第三方服务器，通过此功能可以查看到第三方服务器的上网行为记录。

5.新增“上网行为审计”功能：可以显示终端上网的上网行为记录。

6.新增“用户上下线记录”功能：可以显示用户上下线记录

7.新增“审计统计”功能：可以显示审计的统计数据