AR7088H ROUTER 使用手册

适用机型：

产品类型	型号	产品名称	产品类型	型号	产品名称
增强型	AR7088H-R	5G WIFI ROUTER	单模双卡型	AR7088H-RS	单模双卡 5G WIFI ROUTER
	AR7088H-A	4G 全网通 WIFI ROUTER		AR7088H-AS	单模双卡 4G 全网通 WIFI ROUTER
	AR7088H-B	TDD/FDD-LTE WIFI ROUTER		AR7088H-BS	单模双卡 TDD/FDD-LTE WIFI ROUTER
	AR7088H-F	FDD-LTE WIFI ROUTER		AR7088H-FS	单模双卡 FDD-LTE WIFI ROUTER
	AR7088H-T	TDD-LTE WIFI ROUTER		AR7088H-TS	单模双卡 TDD-LTE WIFI ROUTER
GPS+增强	AR7088H-RP	GPS+5G WIFI ROUTER	GPS+单模双卡型	AR7088H-RSP	单模双卡 GPS+5G WIFI ROUTER
	AR7088H-AP	GPS+4G 全网通 WIFI ROUTER		AR7088H-ASP	单模双卡 GPS+4G 全网通 WIFI ROUTER
	AR7088H-BP	GPS+TDD/FDD-LTE WIFI ROUTER		AR7088H-BSP	单模双卡 GPS+TDD/FDD-LTE WIFI ROUTER
	AR7088H-FP	GPS+FDD-LTE WIFI ROUTER		AR7088H-FSP	单模双卡 GPS+FDD-LTE WIFI ROUTER
	AR7088H-TP	GPS+TDD-LTE WIFI ROUTER		AR7088H-TSP	单模双卡 GPS+TDD-LTE WIFI ROUTER
标准型	AR7088H-RSTD	5G 标准版 ROUTER	公专一体	AR7088H（公专）	公专一体 WIFI ROUTER
				AR7088H-BSTD（公专）	公专一体标准版 ROUTER
	AR7088H-ASTD	4G 全网通标准版 ROUTER		AR7088H-DSTD	公专一体电力版 ROUTER
				AR7088H-JSDS	公专一体江苏版 ROUTER
	AR7088H-BSTD	TDD/FDD-LTE 标准版 ROUTER	国网加密	AR7088H（加密）	国网加密 WIFI ROUTER
	AR7088H-FSTD	FDD-LTE 标准版 ROUTER		AR7088H-STD（加密）	国网加密标准版 ROUTER
	AR7088H-TSTD	TDD-LTE 标准版 ROUTER	商用型	AR7088H-N	WIFI ROUTER

爱陆通 ALOTCER

厦门爱陆通通信科技有限公司

热线：400-808-5829
电话：0592-6195619
传真：0592-6195620
网址：www.alotcer.com
地址：厦门市集美区杏北二路 146-148 号


PWR APP
SIG NET
GND
RXD
TXD
A B
LAN1
LAN2
LAN3/WAN

目录

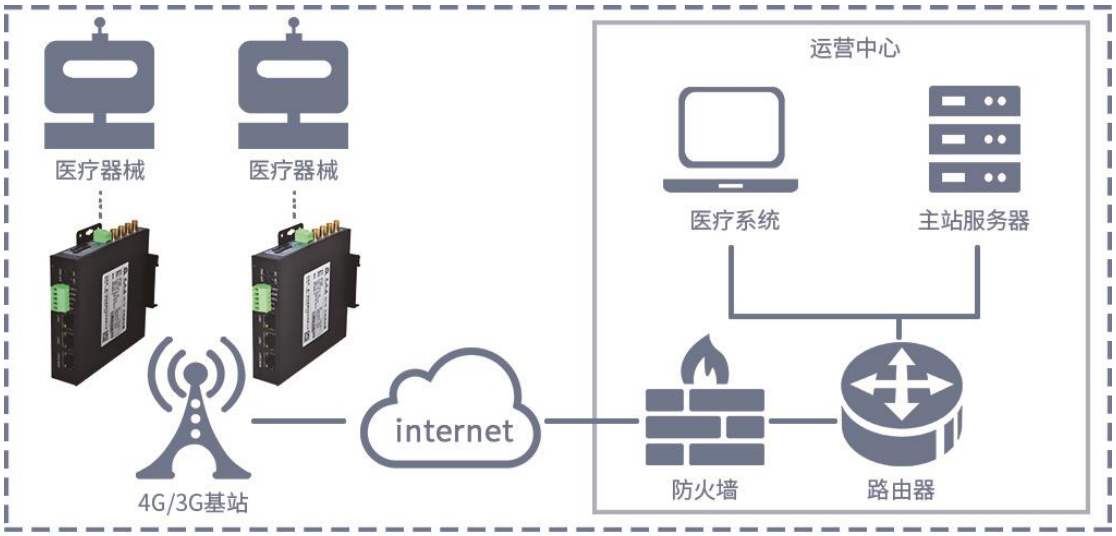
第1章 产品简介

1.1 产品概述

AR7088H ROUTER 是基于 5G/4G/3G/2G、WIFI、虚拟专网等技术开发的无线路由器。产品采用高性能的工业级 32 位通信处理器和工业级无线模块，以嵌入式实时操作系统为软件支撑平台，同时支持 1 个以太网 WAN（可配置为 LAN 口）、2 个以太网 LAN、1 个 RS232/RS485 接口和 1 个 WIFI 接口，能满足工业现场通信的需求。

AR7088H ROUTER 全面支持中国移动、中国联通、中国电信三大运营商的 5G NR SA/NSA、4G（TDD-LTE/FDD-LTE）、3G（WCDMA/HUUPA/HSPA+/CDMA 2000 1x EVDO）2G（GPRS/ CDMA）网络，支持 WIFI 功能，为用户提供全面的无线广域网和无线局域网服务。

该产品已广泛应用于物联网产业链中的 M2M 行业，如电力、交通、邮政、热力、路灯、油田、金融、快递、传媒、POS 自助终端、智能建筑、消防、环境保护、气象、农林、水利、石化等领域。



ROUTER 应用拓扑图

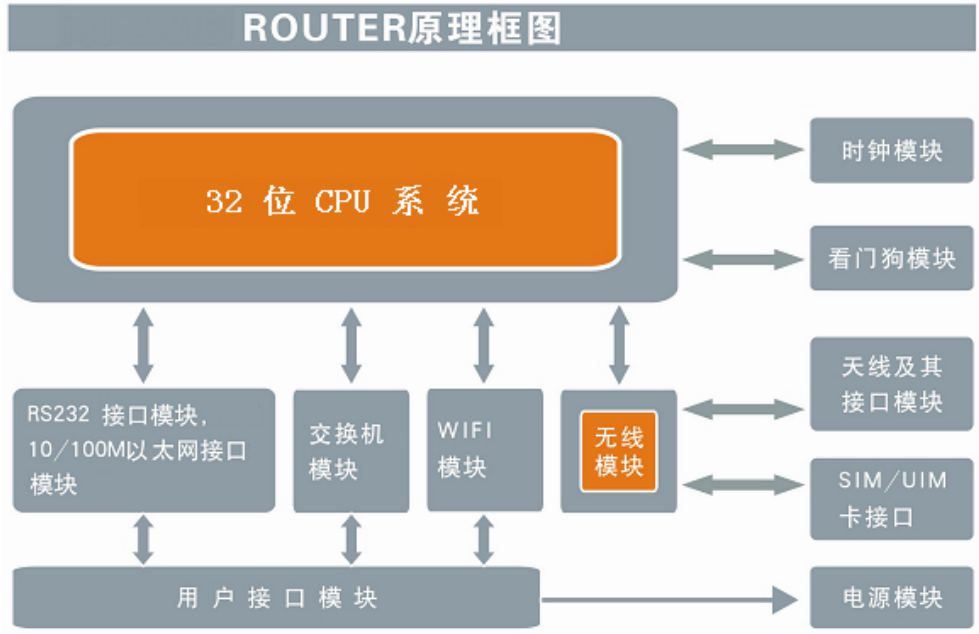
1.2 产品特点

项目	内容
工业化设计	采用高性能工业级无线模块
	采用高性能工业级 32 位通信处理器
	采用金属外壳，保护等级 IP30

	宽电源输入（DC 5~35VDC）
高可靠性设计	WDT 看门狗设计，保证系统稳定
	采用完备的防掉线机制，保证数据终端永远在线
	以太网接口内置 1.5KV 电磁隔离保护
	RS232/RS485 接口内置 15KV ESD 保护
	SIM/UIM 卡接口内置 15KV ESD 保护
	电源接口内置反相保护和过流、过压保护
	天线接口防雷保护（可选）
标准易用	提供标准 RS232（或 RS485）、以太网和 WIFI 接口，可直接连接串口设备、以太网设备和 WIFI 设备
	提供标准有线 WAN 口（支持标准 PPPOE 协议），可直接连接 ADSL 设备
	智能型数据终端，上电即可进入数据传输状态
	使用方便，灵活，多种工作模式选择
	方便的系统配置和维护接口（包括本地和远端 WEB 和 CLI 方式）
	同时支持挂耳式和 35mm Din-rail 式安装
强大安全	支持多种 WAN 连接方式，包括静态 IP，DHCP，PPPOE，2.5G/3G /4G/5G
	支持无线网络和有线 WAN 双链路智能切换备份功能（可选）
	支持 VPN（PPTP，L2TP，IPSEC 和 GRE）（注：仅 VPN 版支持）
	支持远程管理，SYSLOG、SNMP、TELNET、SSHD，HTTPS 等功能
	支持本地和远程在线升级，导入导出配置文件
	支持 NTP，内置 RTC
	支持国内外多种 DDNS
	支持 MAC 地址克隆
	WIFI 支持 802.11b/g/n,支持 WIFI AP、AP Client
	WIFI 支持 WEP,WPA，WPA2 等多种加密方式
	支持多种上下线触发模式，包括短信、电话振铃、串口数据、网络数据触发上/下线模式
	支持 APN/VPDN
	支持多路 DHCP server 及 DHCP client，DHCP 捆绑 MAC 地址，DDNS，防火墙，NAT，DMZ 主机，QoS，流量统计,实时显示数据传输速率等功能
	支持 TCP/IP、UDP、FTP（可选）、HTTP 等多种网络协议
	支持 SPI 防火墙，VPN 穿越，访问控制，URL 过滤，等功能
	支持本地日志存储
	支持 GPS/北斗功能（可选）
	支持双 SIM 卡（可选）
	支持国网硬件加密（可选）
	支持公专一体（可选）

1.3 工作原理框图

ROUTER 原理框图如下：

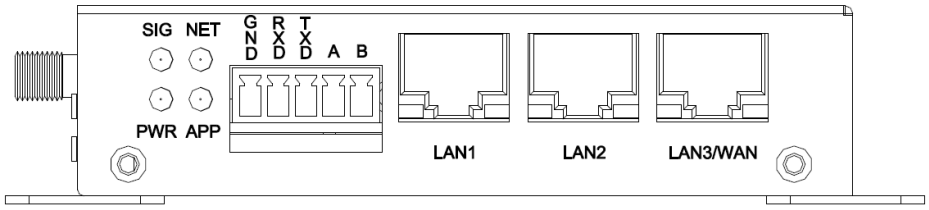


1.4 产品规格

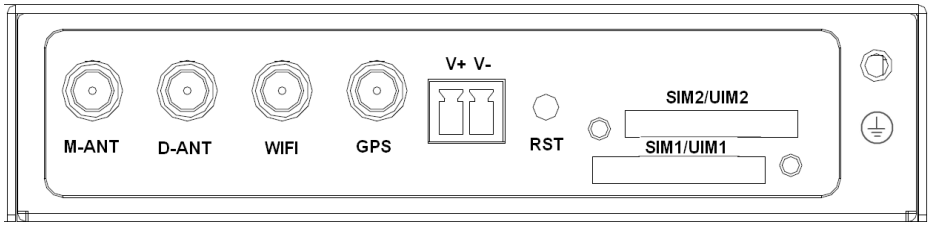
项目		内容
CPU 系统	CPU	工业级 32 位通信处理器
	FLASH	16MB（可扩展至 64MB）
	SDRAM	128MB
接口参数	WAN 接口	1 个 10/100M 以太网口（RJ45 插座），自适应 MDI/MDIX，内置 1.5KV 电磁隔离保护
	LAN 接口	2 个 10/100M 以太网口（RJ45 插座），自适应 MDI/MDIX，内置 1.5KV 电磁隔离保护
	串口	1 个 RS232 /RS485 串口，5 pin 3.5mm 间距端子接口，内置 15KV ESD 保护，串口参数如下： 数据位：5、6、7、8 位 停止位：1、1.5(可选)、2 位 校验：无校验、偶校验、奇校验、SPACE(可选)及 MARK 校验(可选) 串口速率：2400~115200bits/s
	天线接口	蜂窝/GPS/北斗天线：标准 SMA 阴头天线接口，特性阻抗 50 欧 WIFI 天线：标准 SMA 阳头天线接口，特性阻抗 50 欧

	SIM/UIM 卡接口	标准的抽屉式用户卡接口，支持 1.8V/3V SIM/UIM 卡，内置 15KV ESD 保护
	电源接口	2 pin 3.81mm 间距端子接口，内置电源反相保护和过流、过压保护
	Reset 复位按钮	长按此按钮 8S，可将 ROUTER 的配置参数恢复为出厂默认值
	指示灯	具有 “PWR”、“SIG”、“NET”、“APP”、“网口 Link”指示灯

Router 正面接口图：



Router 侧面接口图：



网络参数	无线网络	5G NR SA/NSA：n1/2/3/5/7/8/12/20/28/41/66/ 71/77/78/79 TDD-LTE：B38/39/40/41 和 B61/62（专网） FDD-LTE：B1/2/3/4/5/7/8/13/17/20/25/28 WCDMA：850/900/1900/2100MHz TD-SCDMA：1880-1920/2010-2025MHz(A/F) CDMA2000 1x/ EVDO Rev. A：800/1900MHz GSM/GPRS/EDGE：850/900/1800/1900MHz CDMA：800/1900MHz
	WAN 协议	支持 PPP/PPPOE
	LAN 协议	支持 APR
	网络认证	支持 CHAP/PAP 认证
	网络接入	支持 APN/VPDN
	IP 应用	支持Ping、Trace、DHCPServer 、DHCP Relay、 DHCP Client、DNS relay、DDNS 、Telnet
	IP 路由	支持静态路由
GPS 参数（可选）	接收机类型	50 通道 GPS L1（1575.42MHz）C/A 码 支持 WAAS，EGNOS，MSAS，GAGAN
	最大更新速率	5 Hz
	精确度	定位：2.5m CPE SBAS：2.0m CPE
	捕获	冷启动：32S

		温启动：32S 辅助启动：<1S 热启动：<3S
	灵敏度	跟踪：-160dBm 重新捕获：-160dBm 冷启动：-146dBm
	授时精度	RMS：30ns 99%：<60ns 颗粒度：21ns
	时间脉冲	可以配置，0.1 至 1000Hz
WIFI 参数	标准及频段	支持 IEEE802.11b/g/n 标准
	理论带宽	IEEE802.11b/g：最高速率达 54Mbps EEE802.11n：最高速率达 150Mbps
	安全加密	支持 WEP、WPA、WPA2 等多种加密方式，可选 WPS 功能
供电参数	标准电源	DC 12V/1.5A
	供电范围	DC 5~35V
	通信电流	<500mA (@12VDC，4G 机型) <900mA (@12VDC，5G 机型)
机械参数	外形尺寸	107x98x24mm（不包含配件）
	重量	350g
环境参数	工作温度	-35~+75℃（-31~+167℉）
	储存温度	-40~+85℃（-40~+185℉）
	相对湿度	95%(无凝结)

1.5 订购信息

产品型号	**版本号**		
	网络编号	**功能扩展 1**	**功能扩展 2**
AR7088H	-G：GPRS -C：CDMA -W：WCDMA -E：EVDO -B：TDD/FDD-LTE -T：TDD-LTE -F：FDD-LTE -A：4G 全网通 -R：5G -N：无模块 -WSTD：WCDMA 标准	S：单模双卡功能 P：GPS 功能 B：北斗功能	（公专/加密）

	版 -ESTD：EVDO 标准版 -BSTD： TDD/FDD-LTE 标准版 -TSTD：TDD-LTE 标准版 -FSTD：FDD-LTE 标准版 -ASTD：4G 全网通标准版 -RSTD：5G 全网通标准版		
举例 1	AR7088H-ASP：AR7088H 全网通路由器，全面支持中国移动、中国联通、中国电信的 2G/3G/4G 网络，支持 GPS 功能，支持单模双卡。		
举例 2	AR7088H-R(加密)：AR7088H 国网加密 5G 路由器，全面支持中国移动、中国联通、中国电信的 5G/4G/3G 网络		

第2章 产品安装

2.1 概述

ROUTER 必须正确安装方可达到设计的功能，通常设备的安装必须在本公司认可合格的工程师指导下进行。

注意事项：
请不要带电安装 ROUTER。

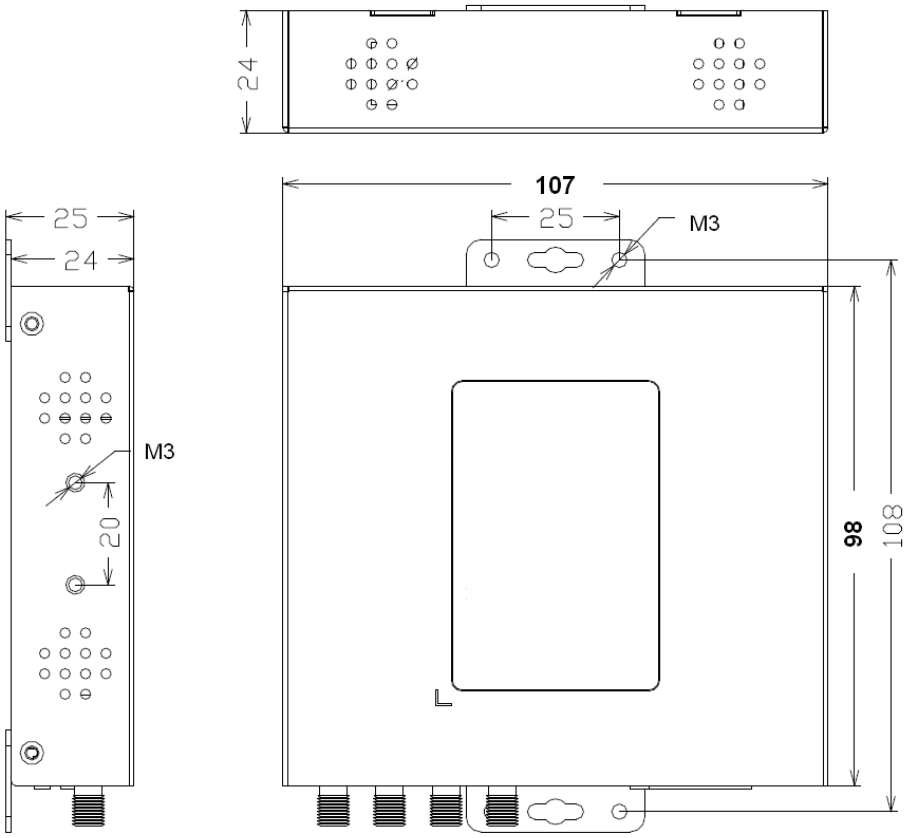
2.2 装箱清单

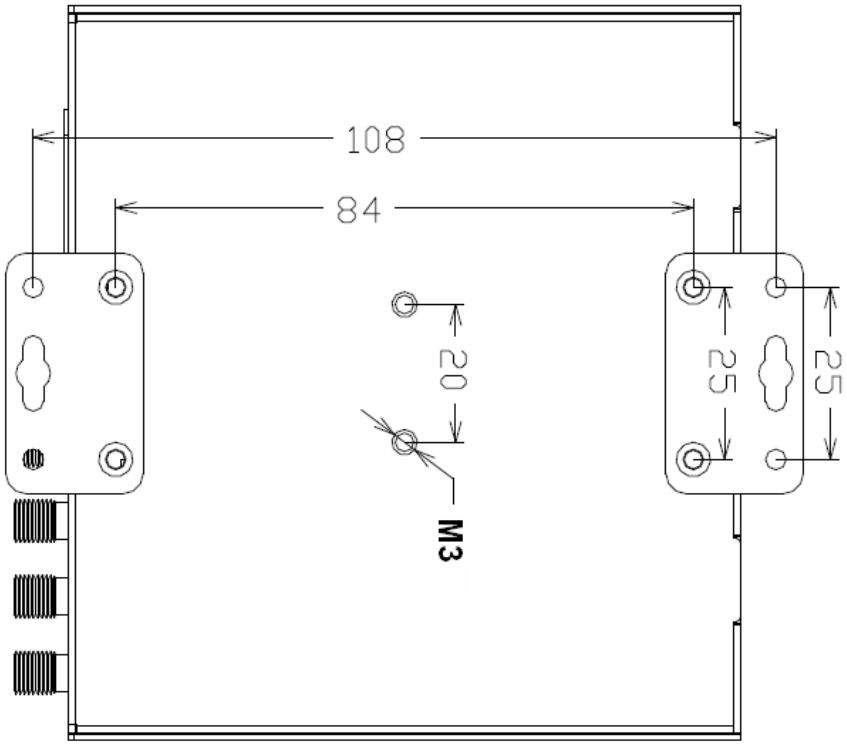
当您开箱时请保管好包装材料，以便日后需要转运时使用。清单如下：

物料类型	数量	备注
ROUTER 主机	1 台	标配
无线蜂窝天线（SMA 阳头）	1 根	标配（部分机型是两根）
WIFI 天线（SMA 阴头）	1 根	标配（部分机型无）
以太网直连线	1 条	标配
产品保修卡	1 份	标配
产品合格证	1 份	标配
配套电源	1 个	选配
RS232 串口线	1 条	选配
RS485 串口线	1 条	选配
GPS/北斗天线	1 根	选配

2.3 安装与电缆连接

AR7088H Router 同时支持挂耳式和 35mm Din-rail 安装，尺寸如下，单位：mm。


24
107
25
25
M3
M3
20
86
108


108
84
20
M3
25
25

天线安装：

蜂窝天线（标配）

WIFI 天线（标配）

无线广域网天线接口为SMA阴头插座(标识为“ANT”,部分机型是两根天线,即“ANT1”、“ANT2”)，将配套的无线蜂窝天线的 SMA 阳头旋到该天线接口上，并确保旋紧，以免影响信号质量。

无线局域网天线接口为 SMA 阳头插座（标识为“WIFI”)，将配套 WIFI 天线的 SMA 阴头旋到该天线接口上，并确保旋紧，以免影响信号质量。

注意：无线蜂窝天线、WIFI 天线不能接反，否则设备无法正常工作。

SIM/UIM 卡安装：

安装或取出 SIM/UIM 卡时，先用尖状物插入 SIM/UIM 卡座旁边的小圆点，SIM/UIM 卡套即可弹出。安装 SIM/UIM 卡时，先将 SIM/UIM 卡放入卡套，并确保 SIM/UIM 卡的金属接触面朝外，再将 SIM/UIM 卡套插入抽屉中，并确保插到位。

安装电缆：

网线（标配）

RS232 串口线（选配）

RS485 串口线（选配）

电源适配器（选配）

将网络直连线的一端插到 ROUTER 的交换机接口上（标识为“LAN1/LAN2/LAN3WAN”)，另一端插到用户设备的以太网接口上。网络直连线信号连接如下：

RJ45-1	RJ45-2
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8

Router 的电源和 RS232/RS485 采用工业级端子接口。建议使用的电源线材和数据线材为 28-16AWG。选配电源和数据线说明如下：

电源（输出 12VDC/1.5A）：

线材颜色	电源极性
黑白相间	正极
黑色	负极

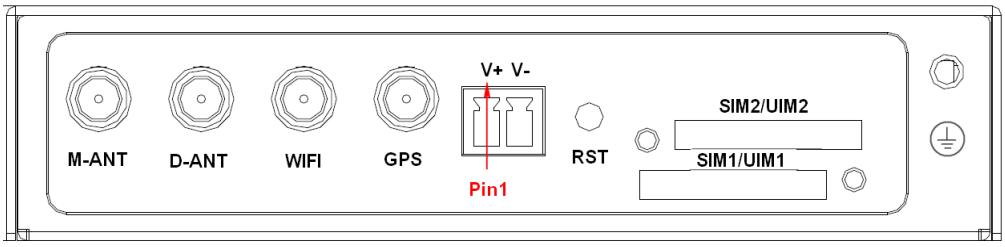
RS232 线（可选，一端为 DB9 母头）：

线材颜色	对应 DB9 母头管脚
蓝色	2
棕色	3
黑色	5

RS485 线（可选）：

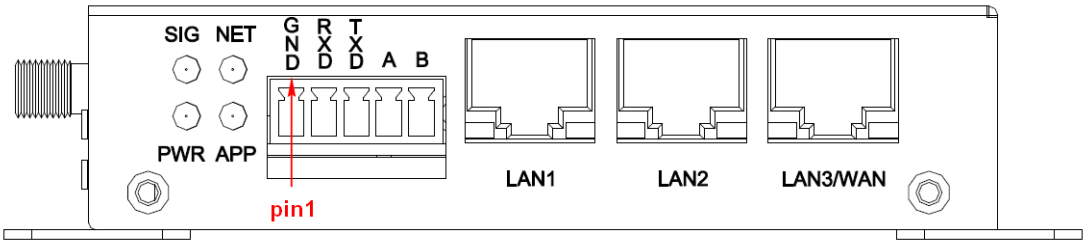
线材颜色	信号定义
红色	RS485 正极（A）
黑色	RS485 负极（B）

电源接口定义：



端子管脚	信号定义	备注	接用户设备
1	V+	电源正极	电源正极
2	V−	电源负极	电源负极

通信接口定义：



通信接口是 5 pin 3. 5mm 间距工业端子，接口定义如下表：

端子管脚	信号定义	备注	接用户设备
1	GND	系统地	系统地
2	RXD	RS232 串口接收	RS232_TXD
3	TXD	RS232 串口发送	RS232_RXD
4	A	RS485+（A）	RS485+（A）
5	B	RS485−（B）	RS485−（B）

2.4 电源说明

电源适配器（标配）

ROUTER 通常应用于复杂的外部环境。为了适应复杂的应用环境，提高系统的工作稳定性，ROUTER 采用了先进的电源技术。用户可采用选配的 12VDC/1.5A 电源适配器给 ROUTER 供电，也可以直接用直流 5~35V 电源给 ROUTER 供电。当用户采用外加电源给 ROUTER 供电时，必须保证电源的稳定性（纹波小于 300mV，并确保瞬间电压不超过 35V），并保证电源功率大于 9W 以上。

推荐使用选配的 12VDC/1.5A 电源。

2.5 指示灯说明

指示灯状态描述：

指示灯	状 态	说 明
Power	灭	设备未上电
	亮	设备电源正常

SIG	灭	无线网络信号强度极差
	闪烁	无线网络信号强度较弱
	长亮	无线网络信号强度较好
NET	灭	未读到 SIM/UIM 卡
	闪烁	读到 SIM/UIM 卡但未拨号
	亮	设备已登录网络
APP	灭	串口应用关闭
	闪烁	串口应用正在连接
	亮	串口应用连接正常
网口 Link（黄色）	灭	WAN/LAN 接口未连接
	亮/闪烁	WAN/LAN 接口已连接/正在数据通信

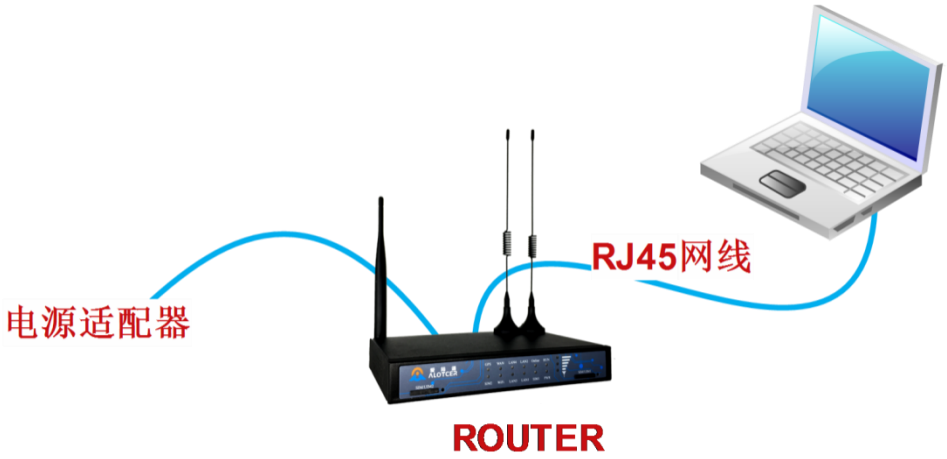
2.6 复位按钮说明

Router 设有一个复位按钮，该按钮的作用是将通讯模块的参数配置恢复为出厂值。方法如下：按下复位按钮 8 秒钟后放开，此时，设备会自动把参数配置恢复为出厂值，并在约 10 秒钟之后，设备自动重启（自动重启现象如下：“电源”指示灯熄灭 10 秒钟左右，然后又正常工作）。

第3章 参数配置

3.1 设备与 PC 连接图

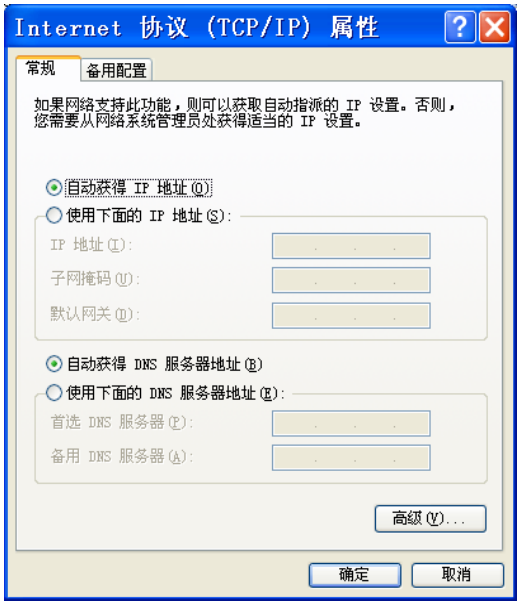
在对路由器进行配置前，需要将路由器和用于配置的 PC 通过出厂配置的网络线或 WIFI 连接起来。用网络线连接时，网络线的一端连接路由器“LAN”以太网接口，另外一端连接到 PC 的以太网口。用 WIFI 连接时，路由器出厂默认的 SSID 为“Alotcer”，无须密码验证。



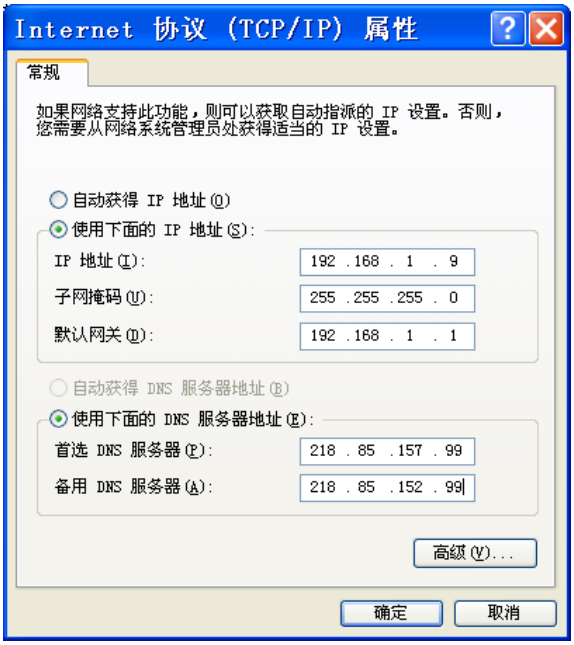
3.2 录到配置页面

3.2.1 PC 机 IP 地址设置（两种方式）

第一种方式：自动获得 IP 地址



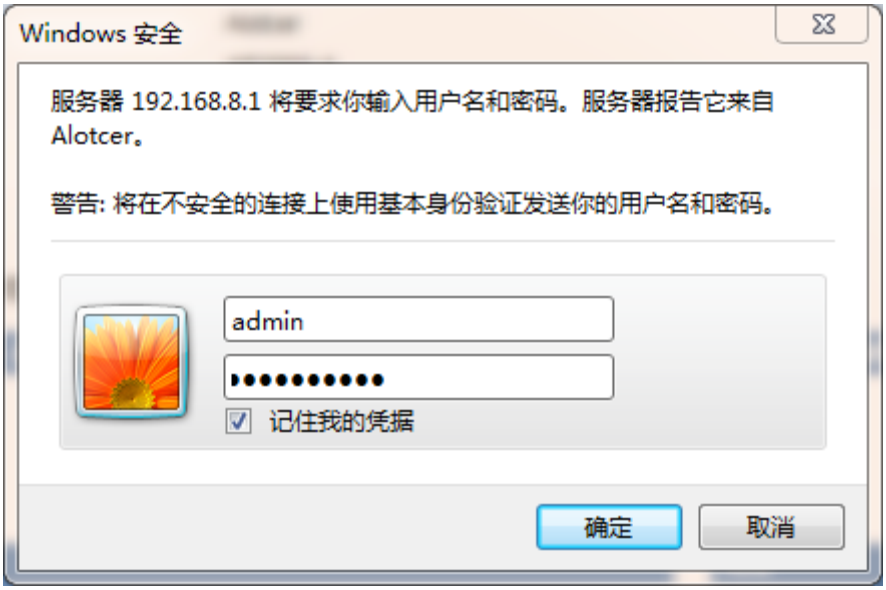
第二种方式：指定 IP 地址。设置 PC 的 IP 地址为 192.168.1.9(或者其他 192.168.1 网段的 IP 地址)，子网掩码设为：255.255.255.0，默认网关设为：192.168.1.1。DNS 设为当地可用的 DNS 服务器。



3.2.2 登录到配置界面

打开浏览器，输入路由器出厂默认的 IP 地址（192.168.1.1）将会出现设备 WEB 界面。点击“继续”按钮进入配置界面。可以根据需要选择语言。

点击“继续”按钮将会出现输入登录密码的提示框。路由器出厂默认的用户名和密码均为“admin”。输入登录密码的提示框。



输入用户名和密码，将会出现配置界面，默认首先显示运行状态，如下图

此界面可以综合的了解设备各模块的运行数据和状态，包括路由基本信息、WAN、LAN、无线、网络、内存等基本信息。

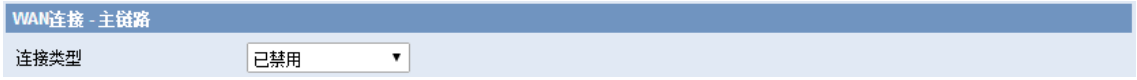
3.3 网络基本

3.3.1 广域网

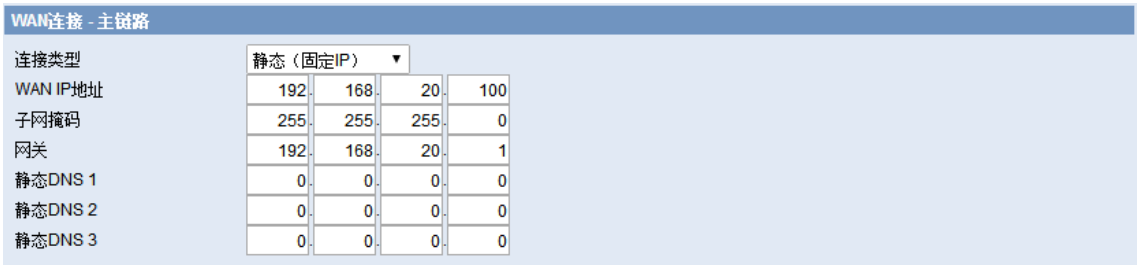
根据不同要求选择适当的广域联网模式，并针对不同的连接模式设置相应的参数。

主备同时在线：主备链路同时保持连接到广域网。在启用情况下，如果主链路可用将自动切换使用主链路通信。

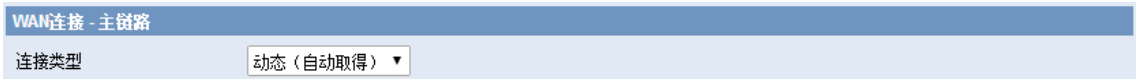
链路异常重启时间：在配置时间内如果广域网链路持续无法连接，设备将重启。



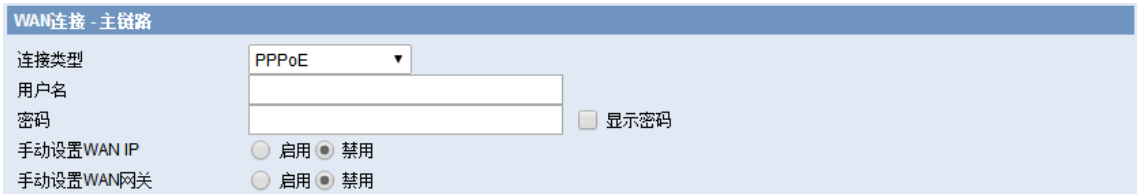
禁用广域网连接



如果广域网络接口需要以固定 IP 地址的接入，选择“静态（固定 IP）”的方式，并正确填入分配的固定 IP，子网掩码，网关，及 DNS 服务器（可选）。

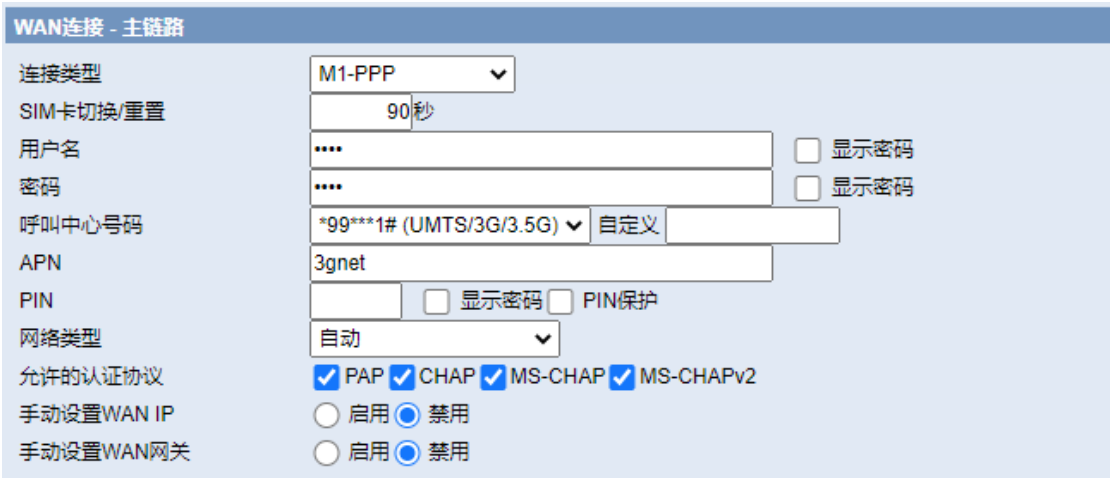


如果广域网络端 IP 地址由广域网络的 DHCP 服务器自动分配。可以选择“动态（自动取得）”的方式，设备将自动从广域网络中发现 DHCP 服务器并自动获得 IP 地址。



如果广域网端连接的是 PPP 服务器，请选择“PPPoE”的方式，并正确填入服务器设置的用户名和密码。

如果想接入 2G/3G/4G/5G 网络，请选择“M1-PPP”模式或者“M1-DHCP”模式。



SIM 卡切换/重置：在配置的时间内，链路持续的无法连接，则重置无线模块，重新识别 SIM 卡。

用户名：无线网络注册用户名。

密码：无线网络注册密码。

呼叫中心号码：启动拨号的呼叫号码。

APN：接入点名称。

PIN：个人识别密码

网络类型：配置注册到无线网络的列表和优先级。

允许的认证协议：拨号时的认证方式有多种。根据运营商要求选择相应正确的方式。

SIM 卡切换/重置：在配置的时间内，链路持续的无法连接，则重置无线模块。

用户名：无线网络注册用户名。

密码：无线网络注册密码。

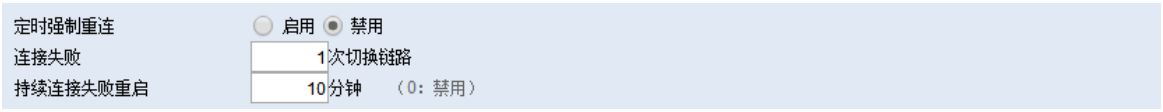
呼叫中心号码：启动拨号的呼叫号码。

APN：接入点名称。

PIN：个人识别密码

网络类型：配置注册到无线网络的列表和优先级。

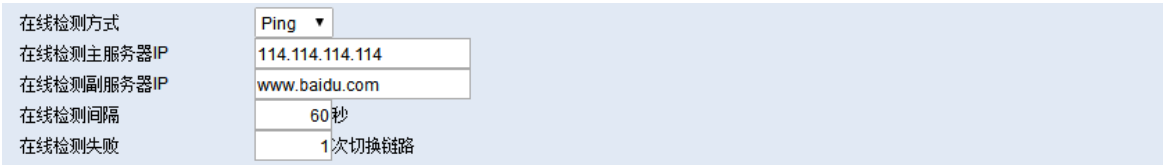
允许的认证协议：拨号时的认证方式有多种。根据运营商要求选择相应正确的方式。



强制重新连接：该功能可以指定路由器在每日指定的时间重新连接 Internet。

连接失败切换链路：如果在配置次数内持续无法拨号成功将切换到另一链路。

连接失败重启：如果在配置时间内持续无法拨号成功将重启设备。



在线检测：这个功能用于检测 ppp 链路是否处于有效状态。如果设置了此项，设备将自动检测链路的连通情况，一旦检测到链路断开或者无效，系统将自动重新建立有效链路。如果网络环境比较差，或者在专网的情况下，建议用 Router 模式。启用该功能将占用一定的流量。在线保持有三种方式：

PING+：串口应用启用时，由串口应用进行链路检查。未启用则使用 PING 方式进行链路检查。

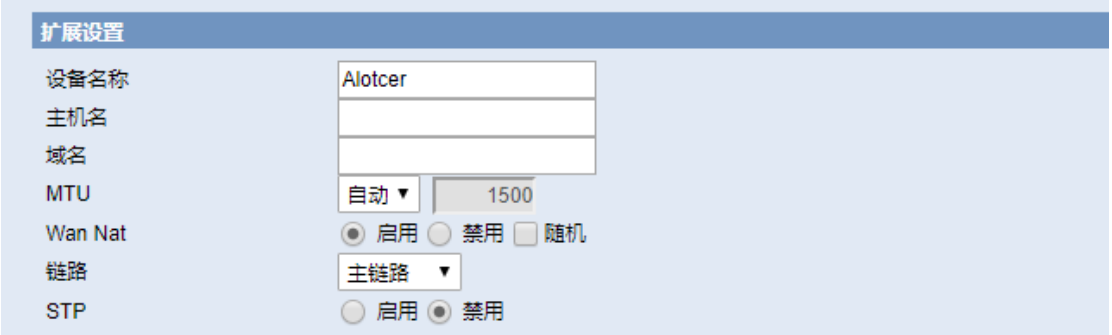
PING：定期发送 PING 数据包，通过检测 PING 包返回情况来检测链路。选择这个方式请正确配置远程主机，并确保远程主机正常接收 PING 数据包。

ROUTE：定期发送计算有效路由跳数的数据包，根据路由返回情况来检测链路，选择这个方式请正确配置远程主机，并确保远程主机链路正常。

PPP：定期发送数据请求，通过接收服务器回应数据包检测路由器与服务器的链路。此方式只能检测与服务器间的链路情况，不能保证与广域网络间的链路。

在线检测间隔：发送测试数据包的时间间隔及失败重连次数。

在线检测失败切换链路：如果在配置次数内在线监测持续失败将切换到另一链路。



设备名称：在这个字段中，您可以输入代表设备的名称。

主机名与域名：可以利用这些选项来提供主机名与域名。一些 ISP（通常是固定网络 ISP）要求提供这些名称作为身份识别。您要与 ISP 确认您的宽带互联网服务中是否配置了主机名与域名。在大多数情况下，保持这些信息空白就可以了。

MTU：MTU 指的是最大传输单元。最大传输单元设置指定互联网传输所允许的最大数据包大小。保持默认设置选择“自动”，设备将选择您的 Internet 连接的最佳 MTU。要指定一个 MTU 大小，请选择“手动”，并输入所需的值（默认为 1500）。你应该设置这个值在 1200 至 1500 的范围内。

Wan Nat：网络地址转换功能。将 LAN 口发送的数据包在转发前，将源地址转换成 WAN 口的地址，避免来自网络外部的攻击，并保护网络内部的计算机。

STP：生成树协议（Spanning Tree Protocol）。该协议可应用于环路网络，通过一定的算法实现路径冗余，同时将环路网络修剪成无环路的树型网络，从而避免报文在环路网络中的增生和无限循环。

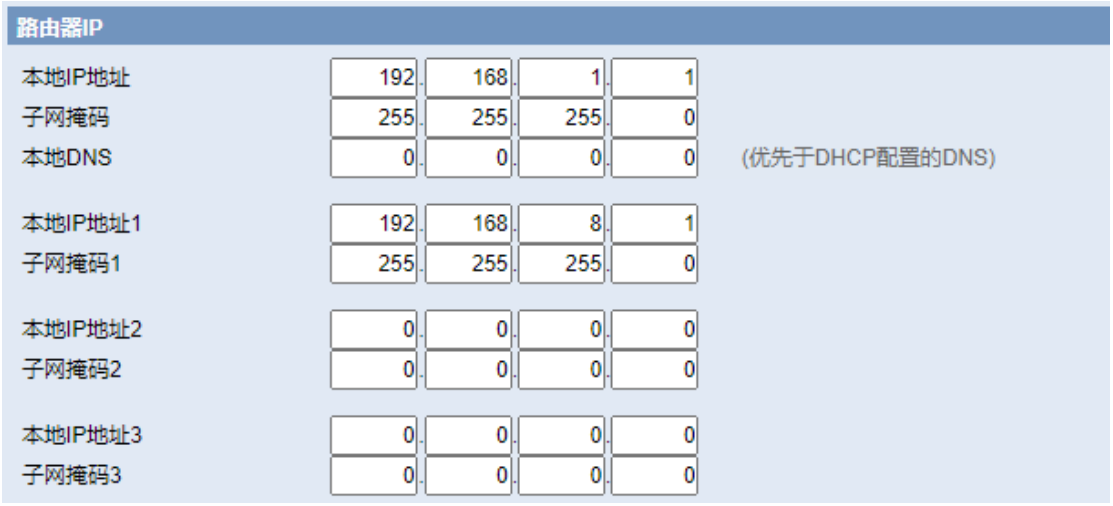
3.3.2 广域网状态

网络控制状态：主动控制广域网链路的链接和断开。

根据不同的连接类型显示具体的连接详细信息，包括模块信息，网络运营商以及连接上的 IP 地址和 DNS 等。

3.3.3 局域网

根据需要配置局域网的网络参数，可以更改路由器 IP 地址以配合实际网络环境的需要。



设置局域网内网接口的 IP 地址及子网掩码。地址不可以与 WAN 口地址在同一网段上。

本地 DNS：DNS 服务器一般由运营商接入服务器自动分配，如果你有自己的 DNS 服务器或者其他稳定可靠的 DNS 服务器，可以选择使用这些可靠的 DNS 服务器。可选配置，若没有则无需设置。

系统除了支持配置基础的内网地址和子网掩码之外，还支持额外三组的内网地址和子网掩码配合。

WAN 口切换为 LAN 口：将 WAN 口配置为 LAN 口使用

DHCP 服务器：在联网用户连接路由器时，从地址池中临时分配一个 IP 地址给连接的客户端。可选择启用或禁用 DHCP 服务器。

起始 IP 地址：服务器分配地址池的起始 IP。

最大 DHCP 用户数：输入您希望 DHCP 服务器能提供分配的最大 IP 地址。默认数值为 50。如果 192.168.1.2 是你的起始 IP 地址，则最大值为 253。

客户端租约时间：客户端从服务器申请到的 IP 地址的租用时间，如果时间到了，客户端需要释放这个 IP 地址，重新申请。客户端比其他主机更优先的更新租约。输入以分钟为单位的时间，动态 IP 地址到期后，如果客户端未进行续约，则此 IP 会自动分配给另外一个客户端。默认设置为 1440 分钟，代表 1 天。可设置范围 0-99999。

静态 DNS：选择给客户端分配 IP 地址的同时，给客户端分配固定的域名解析服务器地址。

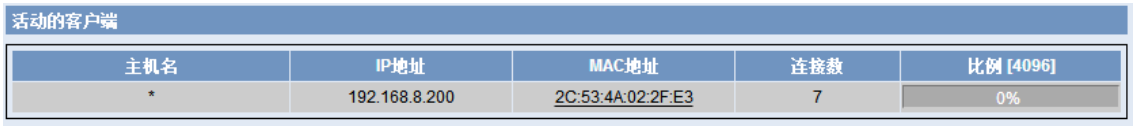
WINS：Windows Internet 命名服务（WINS）管理每一台 PC 与互联网的互动。如果您使用 WINS 服务器，输入该服务器的 IP 地址。否则无需填写。

反域名劫持保护：防止域名劫持攻击。当上级 dns 返回的地址是个私有局域网地址，所以被看作是一次域名劫持，从而丢弃了解析的结果。

DNSMasq 附加选项：可以设置有一些额外的选项，输入你自己的相应配置。例如：dhcp-option=option:acip-code,192.168.8.1 开启 option138 选项，IP 为 AC 的 IP（也可以配置为：dhcp-option=option:138,192.168.8.1）。

3.3.4 局域网状态

局域网口的 MAC、IP 以及 DNS 等信息。



主机名：局域网内活动的客户端的主机名称。

IP 地址：局域网内活动的客户端的 IP 地址。

MAC 地址：局域网内活动的客户端的 MAC 地址。

连接数：局域网内活动的客户端产生的连接数。

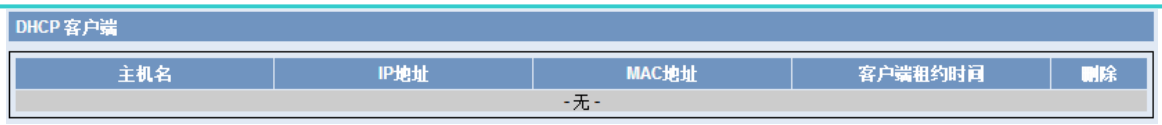
比例：占总连接数的百分比

DHCP 服务器：是否启用 DHCP 服务器。

起始 IP 地址：客户端允许分配的起始 IP 地址。

结束 IP 地址：客户端允许分配的结束 IP 地址。

客户端租约时间：客户端的租约时间。

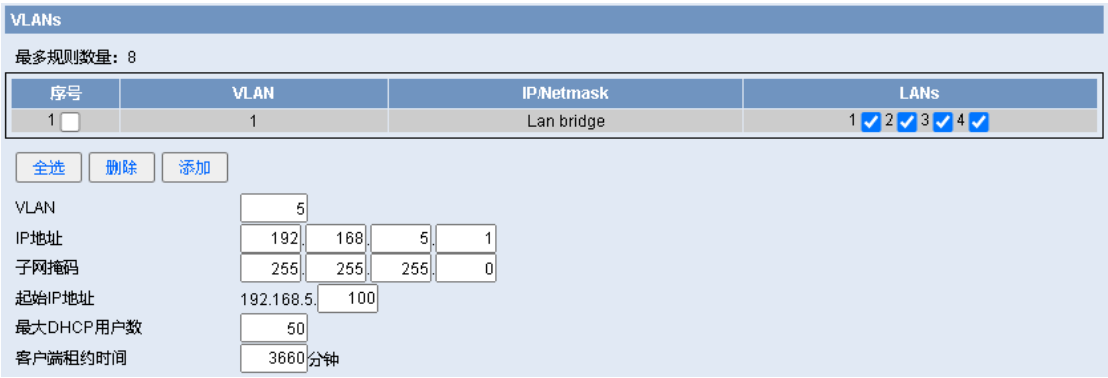


主机名：客户端的主机名称。
IP 地址：客户端的 IP 地址。
MAC 地址：客户端的 MAC 地址。
客户端租约时间：客户端租约这个 IP 地址的时间。
删除：点击可以释放 DHCP 服务器此 IP 的分配。

3.4 网络高级

3.4.1 VLANs

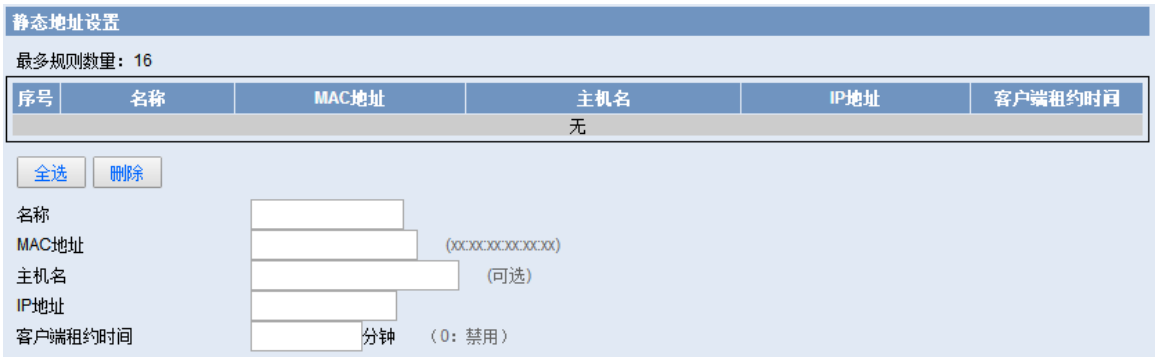
设备根据硬件形态具有不同的 LAN 口个数，每个物理接口都可以支持单独的 VLAN 配置。



VLAN：新建 VLAN ID
IP 地址：VLAN 的接口地址
子网掩码：VLAN 的接口子网掩码
起始 IP 地址：VLAN 接口的 DHCP 服务器的分配起始地址
最大 DHCP 用户数：VLAN 接口的 DHCP 服务器的地址分配数量
客户端租约时间：VLAN 接口的 DHCP 服务器的地址租约时间

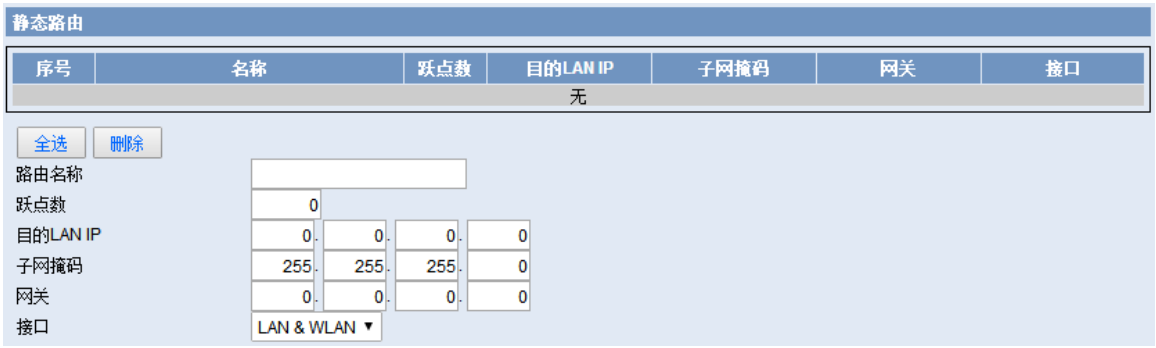
配置每个物理端口上报文的 VLAN TAG 属性，以及端口的 PVID 配置。

3.4.2 静态地址分配



静态地址设置：设置给固定 MAC 地址的客户端分配固定未被分配的 IP 地址。

3.4.3 高级路由



路由名称：路由表项名称定义。

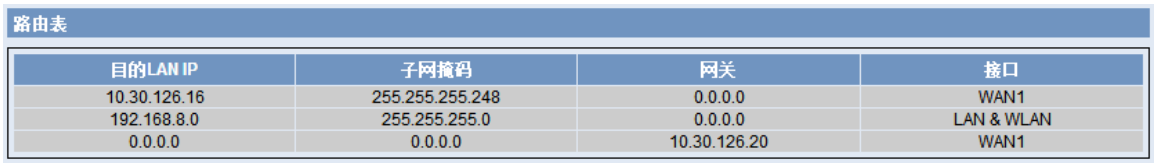
跃点数：网络跳数 0 - 9999。

目的 LAN IP：用户想要分配静态路由的网络或主机的地址。

子网掩码：子网掩码确定 IP 地址的哪个部分是网络部分，哪个部分是主机部分。

网关：网关设备的 IP 地址，允许路由器和网络或主机之间的联系。

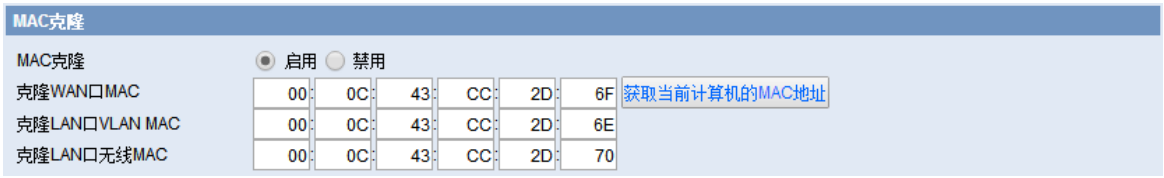
接口：显示用户是否目的 IP 地址在局域网和无线局域网（内部有线和无线网络）、广域网（互联网）。



可在此查看、添加、删除静态路由，也可以查看目前路由器目前活动的路由表

3.4.4 MAC 地址克隆

启动/关闭 MAC 地址克隆功能，更改路由器 WAN 口的 MAC 地址。



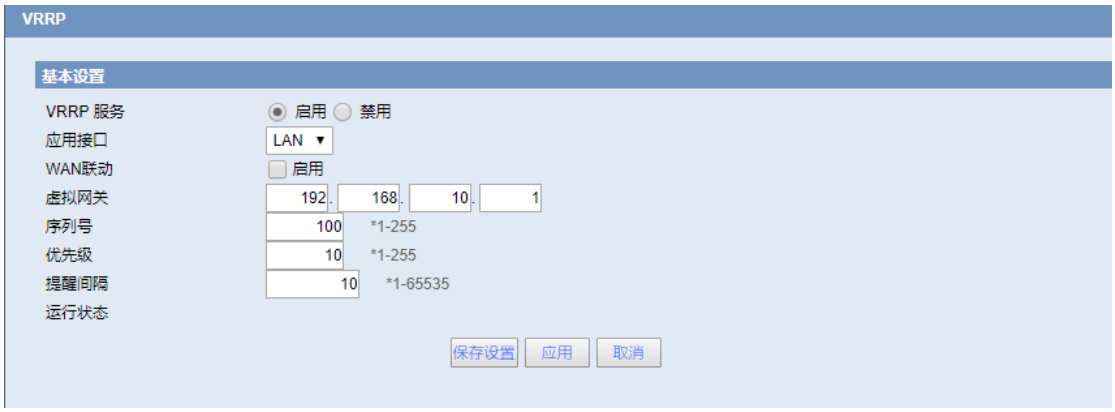
克隆地址：输入需要设定的 WAN 口 MAC 地址值。

获取当前管理 PC 的地址：当前登录 WEB 管理页面的客户端的 MAC 地址，点击按钮，将可以取得当前管理设备的 PC 的 MAC 地址填充到克隆 WAN 口 MAC 地址中去。

3.4.5 静态域名解析

配置网络上的域名解析对应关系。

3.4.6 VRRP



应用接口：绑定的运行接口。

WAN 联动：启用 wan 口联动功，能当 wan 口无法上网时，vrrp 状态值显示 Down，并自动退出 vrrp 备份组，由剩下的 vrrp 路由器中竞选 Master 路由器。

虚拟网关：与外部通讯时候的默认网关地址。

序列号：当前登录 WEB 管理页面的客户端的 MAC 地址，点击按钮，将可以取得当前管理设备的 PC 的 MAC 地址填充到克隆 WAN 口 MAC 地址中去。

优先级：优先级别大的成为 master。

提醒间隔：如果后备机每隔 X 秒没收到主机发来的 advertisement 报文，就会进行新一

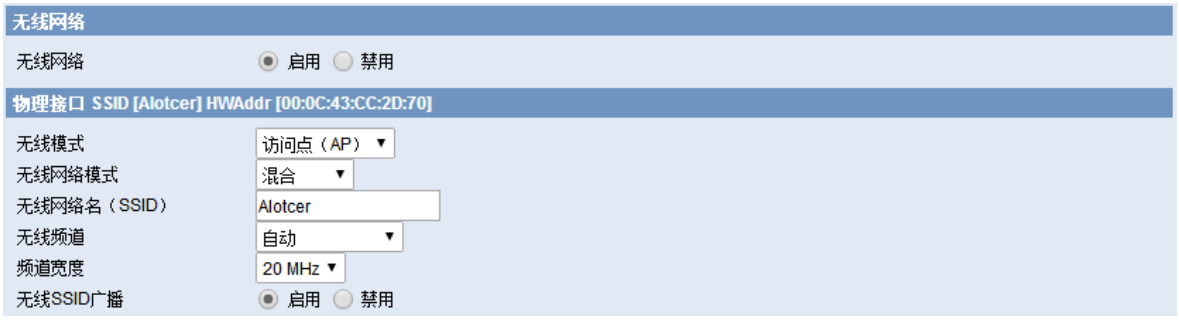
轮的选举。

运行状态：显示当前路由器处于后备状态还是主机状态。

3.5 无线设置

3.5.1 基本设置

设置无线通讯节点的开启关闭状态，并对基本功能进行设置。



无线网络：开启或者关闭无线功能，如果关闭无线功能，则面板上的无线网络指示灯会关闭。

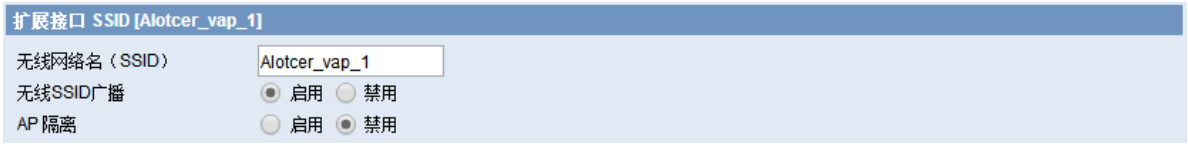
无线网络模式：11b/g mixed mode，同时支持 802.11b 和 802.11g 的无线设备；11b only，只支持 802.11b 的低速无线设备；11g only，只支持 802.11g 的高速设备；11b/g/n mixed mode，同时支持 802.11b、802.11g 和 802.11n 的无线设备；11n only(2.4G)，支持 802.11n 的高速设备。

无线网络名（SSID）：即 Service Set Identification，用于标识无线网络的网络名称。在此输入一个名称，它将显示在无线网卡搜索到的无线网络列表中。

无线频道：以无线信号作为传输媒体的数据信号传送的通道，选择范围从 1 到 13。如果选择自动，则 AP 会自动根据周围的环境选择一个最好的频道。

频道宽度：选择无线信道带宽。通过将两个 20MHz 带宽捆绑在一起组成一个 40MHz 通信带宽，可提升一倍速率。

无线 SSID 广播：该项功能用于将路由器的 SSID 号向周围环境的无线网络内广播，只有开启了 SSID 广播，计算机才能扫描到路由器的无线信号，并可以加入该无线网络。



AP 隔离：选择此项，则同时连上相应 SSID 的客户端之间不可以相互访问。

可以选择“添加”和“删除”按钮来增加或减少扩展的无线 SSID。

3.5.2 无线安全

设置无线网络的安全/加密以防止未被授权的存取与监听。

WEP（有线等效加密）：最基本的无线安全加密措施，采用 64 位或 128 位加密密钥的 RC4 加密算法，保证传输数据不会以明文方式被截获。包括开放模式和共享模式。

开放模式：WEP 加密的一种握手方式，通过 WEP 密钥来进行加密，可以选择默认密钥 1-4，然后分别对 4 个密钥进行定义，4 个密钥都可以满足用户登入无线 AP。

共享模式：WEP 加密的另一种握手方式，通过 WEP 密钥进行加密，加密类型同 OPEN 模式。此模式也可以选择不需 WEP 加密来进行验证。

HEX：十六进制码（0~9，a~f，A~F），WEP 64 bits 为 10 个字符，WEP 128 bits 为 26 个字符。

ASCII：美国标准码（请注意大小写），WEP 64 bits 为 5 个字符，WEP 128 bits 为 13 个字符。

通行短语：用来生成密钥的字母和数字组合，可选。

密钥 1-密钥 4：可以手动填写也可根据输入的通行短语生成。4 个密钥可以只使用其一，也可以多个同时使用。无论哪种情况，客户端网卡上密钥的设置都必须与之一致。

WPA-PSK 或 WPA2-PSK 或 WPA-PSK/WPA2-PSK：WPA-PSK/ WPA2-PSK 安全类型其实是 WPA/WPA2 的一种简化版本，它是基于共享密钥的 WPA 模式，安全性很高，设置也比较简单，适合普通家庭用户和小型企业使用。有 WPA-PSK，WPA2-PSK 两个版本。

WPA 算法：该项用来选择对无线数据进行加密的安全算法，选项有 TKIP、 AES、TKIP+AES。默认选项为 TKIP。

TKIP：使用了 128 位的密钥，变化每个数据包所使用的密钥，具有足够的密码强度，避免了碰撞攻击。

AES：提供了比 TKIP 更加高级的加密技术，采用堆成分组密码体制。

WPA 共享密钥：该项是 WPA-PSK/WPA2-PSK 的初始设置密钥，设置时要求输入 8-63 个 ASCII 字符或 8-64 个十六进制字符。

密钥更新时间间隔：该项设置广播和组播密钥的定时更新周期，以秒为单位，最小值为 30，默认设置为 86400 秒（即 24 小时）。

注: 不是所有的无线适配器都支持 WPA 加密方式，除了硬件支持外，软件也必须支持 WPA 加密方式才可以完全实现 WPA 加密，想了解您所使用的无线适配器是否支持 WPA 加密，请参考其技术文档。WINDOWS XP 和 WINDOWS 2000 在安装 Service Pack 3 的情

况下支持 WPA 加密方式。

企业 WPA-PSK 或企业 WPA2-PSK 或企业 WPA-PSK/WPA2-PSK：相比于普通的 WPA-PSK/WPA2-PSK 使用了服务器来授权访问。

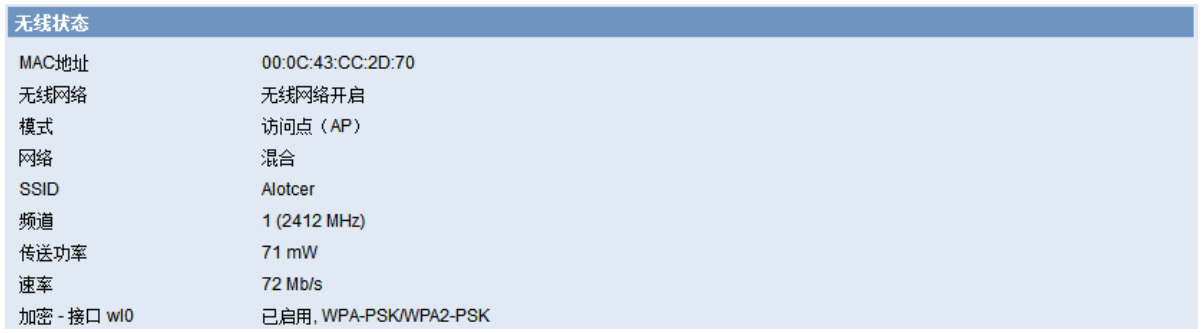
WPA 算法：该项用来选择对无线数据进行加密的安全算法，选项有 TKIP、 AES、TKIP+AES。默认选项为 TKIP。

Radius 鉴权服务器地址，端口：提供授权访问的服务器 IP 地址和端口号。

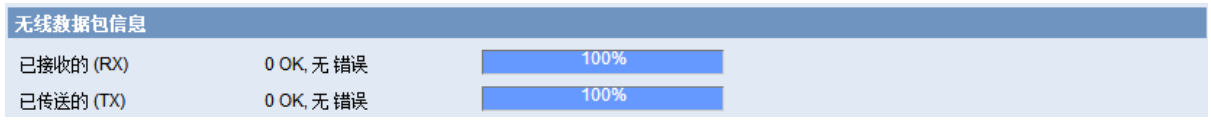
Radius 鉴权共享密钥：该项是企业 WPA-PSK/WPA2-PSK 的初始设置密钥，设置时要求输入 8-63 个 ASCII 字符或 8-64 个十六进制字符。

密钥更新时间间隔：该项设置广播和组播密钥的定时更新周期，以秒为

3.5.3 无线状态



显示无线网络连接的状态信息，可在无线页面进行配置修订。

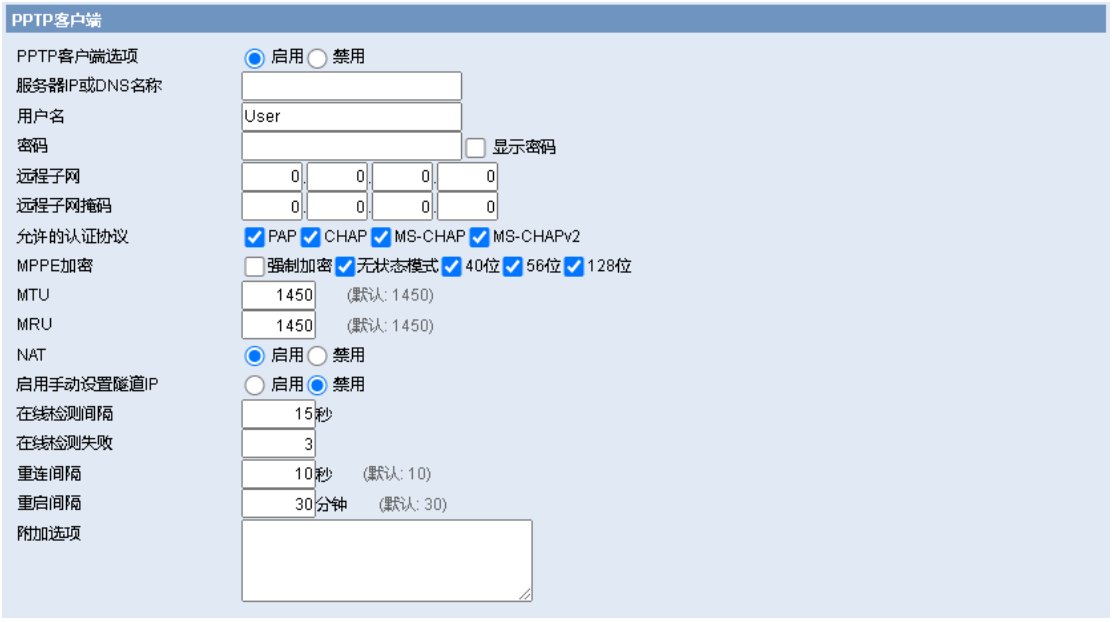


显示无线网络数据收发的状态，接收和发送的报文数以及状态。

显示无线网络所有接入客户端的无线状态信息。

3.6 VPN

3.6.1 PPTP



服务器 IP 或 DNS 名称：PPTP 服务器的 IP 地址或者对应的 DNS 名称

用户名：PPTP 服务器所允许的用户名

密码：PPTP 服务器所允许的用户名对应的密码

远程子网：远程 PPTP 服务器的内网

远程子网掩码：远程 PPTP 服务器的子网掩码

允许的认证协议：*强制认证*-强制对端支持认证；*PAP*-是否拒绝支持 PAP 认证，选择表示不拒绝；*CHAP*-是否强制对方支持 CHAP 认证，选择表示强制对方支持。

MPPE 加密：*强制加密*-强制要求对端支持 MPPE,如果对端不支持则无法连接；*无状态模式*-每个通信报文都单独加密，关闭表示状态保持模式；*40 位/56 位/128 位*-加密位数。

MTU：最大传输单元 0-1500

MRU：最大接收单元 0-1500

NAT：启用或者禁用 NAT 穿越

启用手动设置随地 IP：可手动配置指定的隧道 IP 地址

在线检测间隔：设定定时发送检测报文间隔。

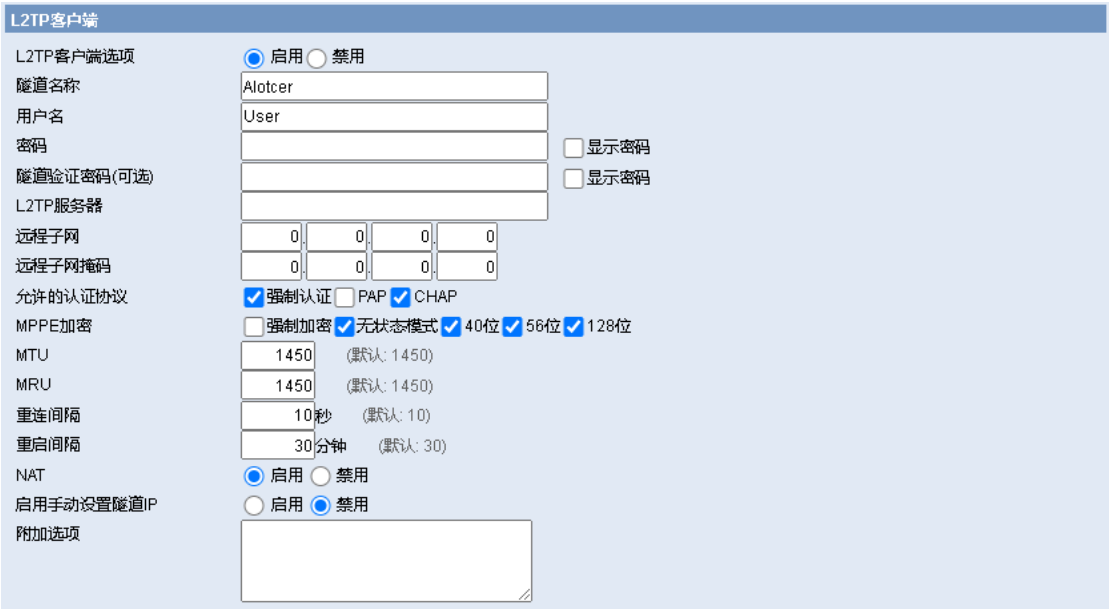
在线检测失败：在达到设定次数后将重新进行连接。

重连间隔：持续设定时间未成功连接服务器，将重新进行连接。

重启间隔：持续设定时间未成功连接服务器，将进行整机重启。

附加选项：其他 PPTP 配置项

3.6.2 L2TP



隧道名称：本地隧道名

用户名：L2TP 服务器所允许的用户名

密码：L2TP 服务器所允许的用户名对应的密码

隧道密码：建立隧道的预设密码

L2TP 服务器：L2TP 服务器的 IP 地址或对应的 DNS 名称

远程子网：L2TP 服务器内网所属的网络

远程子网掩码：L2TP 服务器内网所属的网络掩码

允许的认证协议：*强制认证*-强制对端支持认证；*PAP*-是否拒绝支持 PAP 认证，选择表示不拒绝；*CHAP*-是否强制对方支持 CHAP 认证，选择表示强制对方支持。

MPPE 加密：*强制加密*-强制要求对端支持 MPPE,如果对端不支持则无法连接；*无状态模式*-每个通信报文都单独加密，关闭表示状态保持模式；*40 位/56 位/128 位*-加密位数。

MTU：最大传输单元 0-1500

MRU：最大接收单元 0-1500

重连间隔：持续设定时间未成功连接服务器，将重新进行连接。

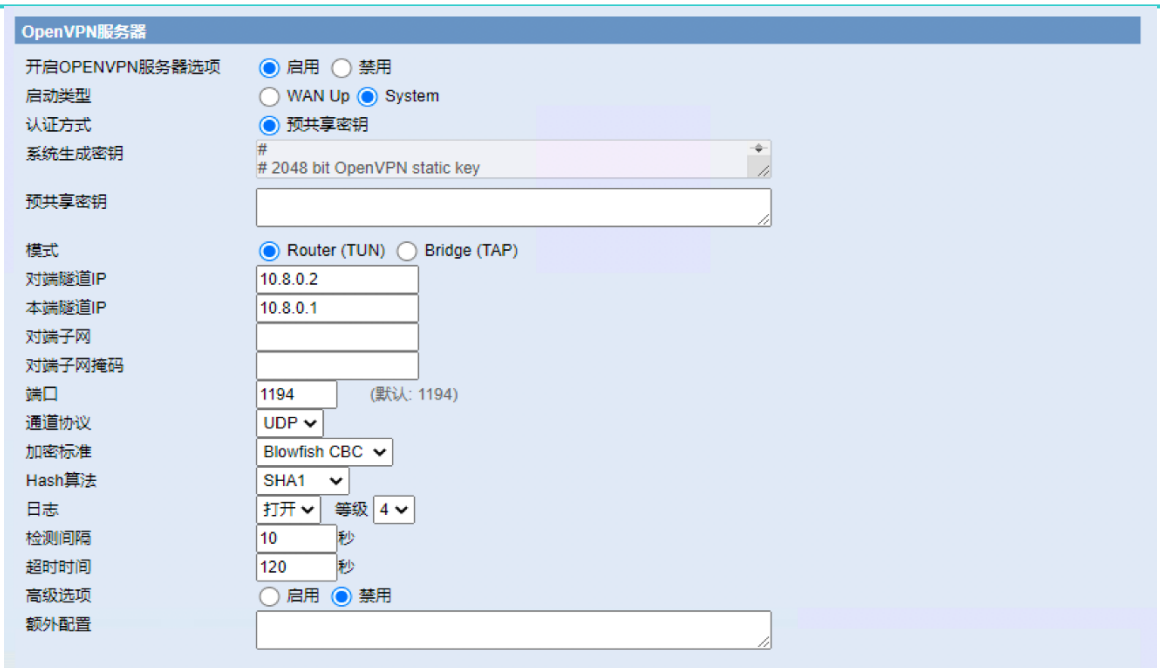
重启间隔：持续设定时间未成功连接服务器，将进行整机重启。

NAT：启用或者禁用 NAT 穿越

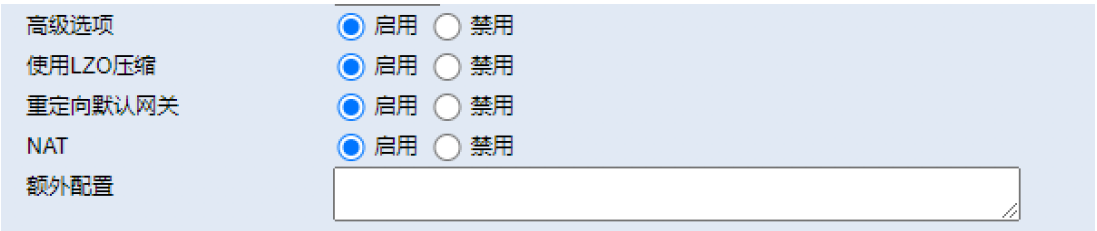
附加选项：其他 L2TP 配置项

3.6.3 OpenVPN

OPENVPN 服务端



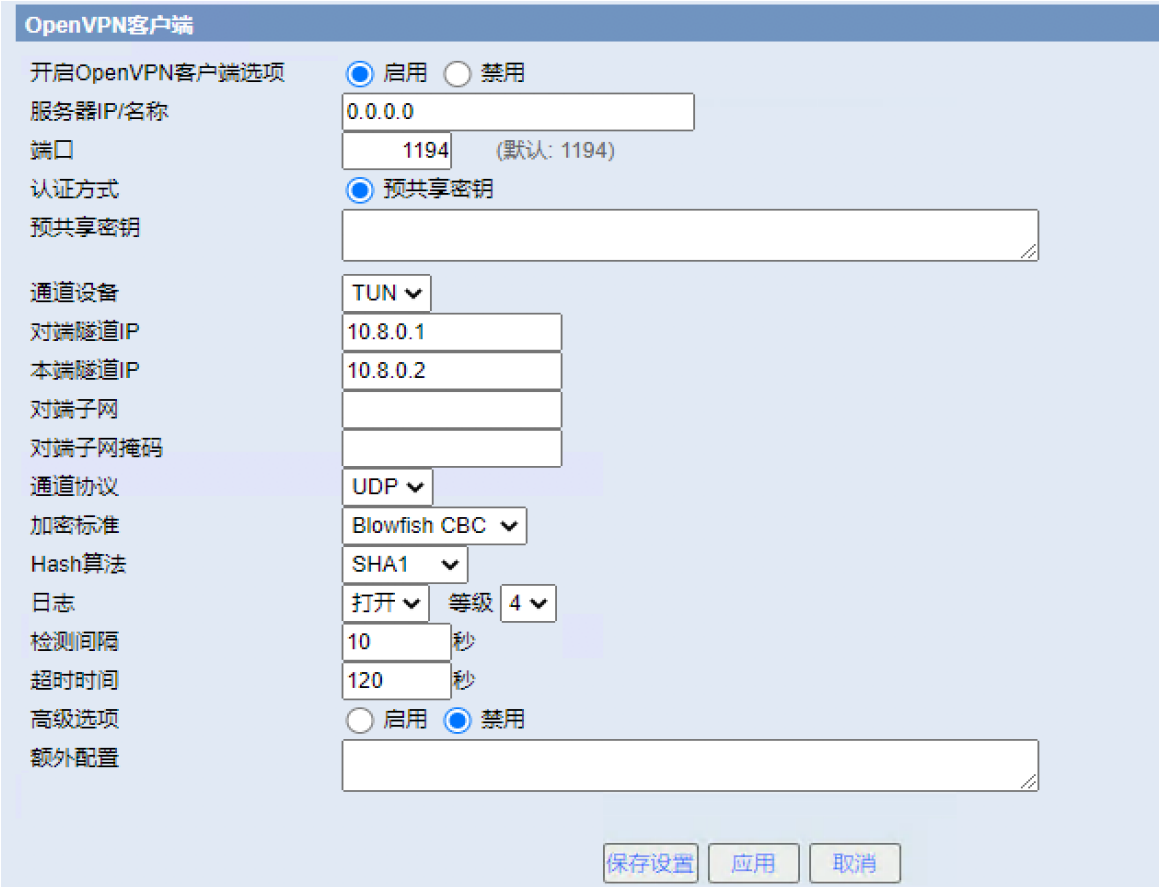
启动类型：WAN Up---上线后启用，System---开机启用
认证方式：支持预共享密钥认证方式
系统生成密钥：由系统随机生成的固定格式的预共享密钥
预共享密钥：用户自定义密钥或者使用系统生成密钥
模式：TUN---路由模式 TAP---网桥模式
对端隧道 IP：OPENVPN 客户端虚拟网卡的 IP 地址
本端隧道 IP：OPENVPN 服务端虚拟网卡的 IP 地址
对端子网：OPENVPN 客户端内网所属的网络
对端子网掩码：OPENVPN 客户端内网所属的网络子网掩码
端口：OPENVPN 服务端监听的端口
通道协议：UDP 和 TCP 协议
加密标准：通道的加密标准包括：Blowfish CBC，AES-128 CBC，AES-192 CBC，AES-256 CBC，AES-512 CBC 五种加密
Hash 算法：Hash 算法提供了一种快速存取数据的方法，包括 SHA1，SHA256，SHA512，MD5 四种算法
日志：日志等级按照日志的严重性分为 4 个等级。
检测间隔：检测 OPENVPN 通道的间隔时间
超时时间：超时没有收到对端响应，认为链路异常
高级选项：



使用 LZO 压缩：启用或禁用传输数据使用 LZO 压缩
重定向默认网关：启用或禁用重定向网关

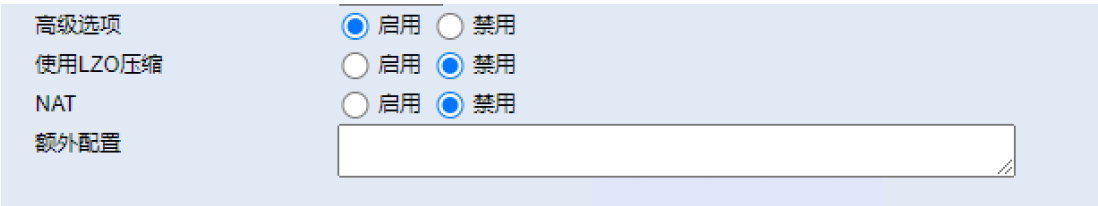
NAT：启用或者禁用 NAT 穿越
额外配置：服务器额外的配置

OPENVPN 客户端



服务器 IP/名称：OPENVPN 服务器的 IP 地址或域名
端口：OPENVPN 服务端监听端口
认证方式：支持预共享密钥认证方式
预共享密钥：用户自定义密钥或者使用系统生成密钥
通道设备：TUN---路由模式 TAP---网桥模式
对端隧道 IP：OPENVPN 服务端虚拟网卡的 IP 地址
本端隧道 IP：OPENVPN 客户端虚拟网卡的 IP 地址
对端子网：OPENVPN 服务端内网所属的网络
对端子网掩码：OPENVPN 服务端内网所属的网络子网掩码
通道协议：UDP 和 TCP 协议
加密标准：通道的加密标准包括：Blowfish CBC，AES-128 CBC，AES-192 CBC，AES-256 CBC，AES-512 CBC 五种加密
Hash 算法：Hash 算法提供了一种快速存取数据的方法，包括 SHA1，SHA256，SHA512，MD5 四种算法
日志：日志等级按照日志的严重性分为 4 个等级。
检测间隔：检测 OPENVPN 通道的间隔时间
超时时间：超时没有收到对端响应，认为链路异常

高级选项：

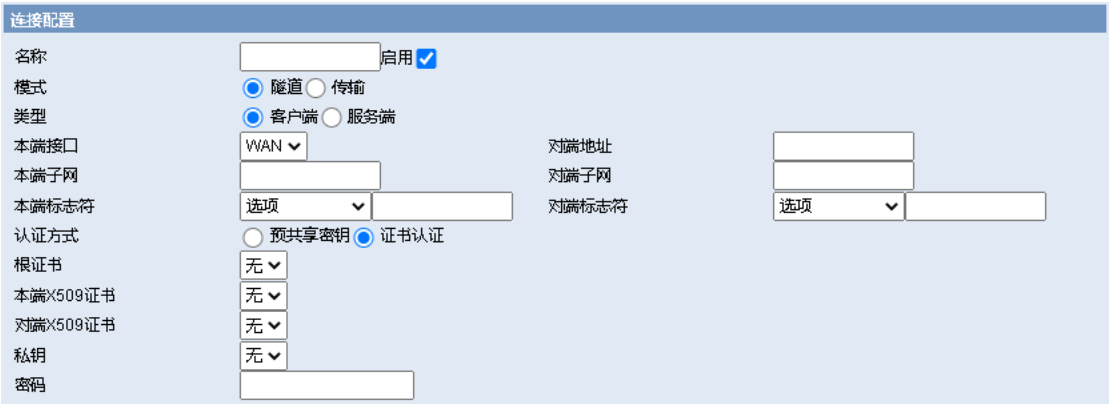


使用 LZO 压缩：启用或禁用传输数据使用 LZO 压缩

NAT：启用或者禁用 NAT 穿越

额外配置：客户端额外的配置

3.6.4 IPSEC



连接配置：该栏目包含了通道的基本地址信息。

名称：用以标示该连接的名称，须唯一；

启用：选择启用，则该条连接在系统起机或者进行重连接操作的时候，将发起通道连接请求；否则不会；

本端接口：通道的本端地址；

对端地址：对端的 IP/域名。如果采用了隧道模式的服务端功能，则该选项不可填；

本端子网：IPSec 本地保护子网及子网掩码，例如：192.168.1.0/24；如果采用传输模式，则该选项不可填写；

对端子网：IPSec 对端保护子网及子网掩码，例如：192.168.7.0/24；如果采用传输模式，则该选项不可填写；

本端标识符：通道本端标识，可以为 IP 及域名；

对端标识符：通道对端标识，可以为 IP 及域名；

预共享密钥：预先设定的共享密码；

根证书：证书认证证书的根证书

本端 X509 证书：本端证书

对端 X509 证书：对端证书

私钥：本端证书私钥

密码：证书密码

高级配置：可以配置第一阶段及第二阶段的信息以及 DPD 检测配置，否则，将根据对端自动协商；

IKE 加密算法：IKE 阶段的加密方式；

IKE 认证算法：IKE 阶段的完整性方案；

IKE DH 小组：DH 交换算法；

IKE 生命周期：设置 IKE 的生命周期，目前以小时为单位，默认为 0；

ESP 加密：ESP 的加密方式；

ESP 完整性：ESP 完整性方案；

ESP 生命周期：设置 ESP 的生命周期，目前以小时为单位，默认为 0；

采用野蛮模式：如果打钩，则协商模式将采用野蛮模式，否则为主模式；

会话密钥向前加密：如果打钩，则启用 PFS，否则不启用；

启用 DPD 检测：是否启用该功能，打钩表示启用；

时间间隔：设置连接检测（DPD）的时间间隔；

超时时间：设置连接检测（DPD）超时时间；

操作：设置连接检测的操作。

链路：选择配置主链路还是备份链路

启动 NAT 穿越：数据包会把 WAN 口 IP 改为 LAN 口 IP。

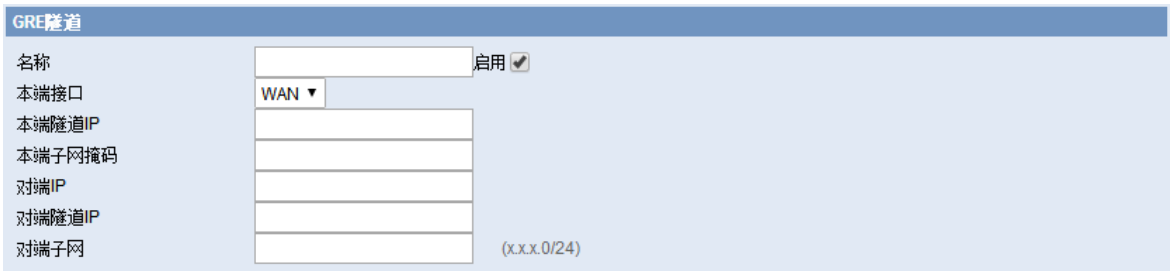
IPSEC 日志：是否开启 IPSEC 日志。

启用链路检测，远程 IP 地址，检测间隔，连续检测失败次数：检测链路配置。

超时重连机制，断线检测时间，断线等待时间，持续连接失败重启:超时重连配置。

3.6.5 GRE

GRE（Generic Routing Encapsulation，通用路由封装）协议是对某些网络层协议（如 IP 和 IPX）的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议（如 IP）中传输。GRE 采用了 Tunnel（隧道）技术，是 VPN（Virtual Private Network）的第三层隧道协议。



名称：隧道的名称最长 30 个字符
启用：是否启用当前配置的 GRE 隧道
本端接口：表示隧道从哪个外网接口建立
本端隧道 IP：本地 GRE 隧道 IP 地址
本端子网掩码：本地子网掩码
对端 IP：输入对端 GRE 的 WAN 口 IP 地址
对端隧道 IP：对端的 GRE 隧道 IP
对端子网：GRE 对端的子网 IP，如：192.168.1.0/24

3.6.6 GRETAP

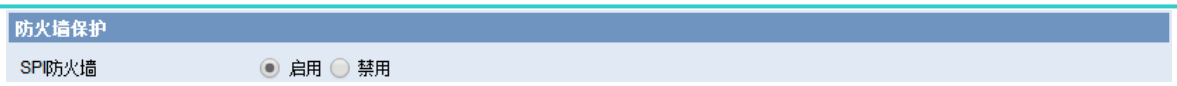
在以太网上承载的 GRE 协议，将在不同位置的网络连接到同一个局域网中。

本端 IP：隧道连接的本端 IP。
远端 IP：隧道连接的对端 IP。
本端隧道 IP：本端 GRETAP 隧道 IP。

3.7 安全

3.7.1 防火墙

您可以启用或禁用防火墙，选择过滤特定的 Internet 数据类型，以及阻止匿名 Internet 请求，通过这些增强网络的安全性。

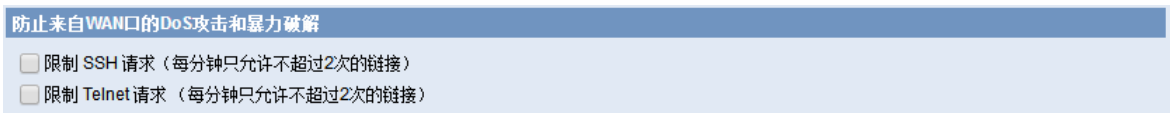


SPI 防火墙： 全状态数据包检测型防火墙对进入网络的数据包进行检查从而判断是否过滤数据包。只有启用了 SPI 防火墙，才能使用其他如过滤代理、阻止 WAN 请求等的防火墙功能。

阻止来自 WAN 口的匿名请求（PING 封包数据）：通过选中“阻止匿名 Internet”请求旁的选项框，启用该功能，从而防止您的网络遭受其他 Internet 用户的 Ping 或者探测，使外部用户更加难以侵入您的网络，这一功能的默认状态为启用，选择禁用可以允许匿名 Internet 请求。

过滤 IDENT(端口 113)：这一功能可以使 113 端口免于被您的本地网络之外的设备进行扫描。

阻止来自 WAN 口的 SNMP 请求：这一功能阻止来自广域网的 SNMP 连接请求。



限制 SSH 请求：该功能限制了来自广域网的 SSH 访问请求，对同一个 IP 每分钟最多接受 2 个 SSH 连接请求。

限制 Telnet 请求：该功能限制了来自广域网的 Telnet 访问请求，对同一个 IP 每分钟最多接受 2 个 Telnet 连接请求。

过滤 Proxy 代理：使用 wan 代理服务器可能降低网关的安全性，过滤代理转发的网页将拒绝任意 wan 代理服务器的访问。

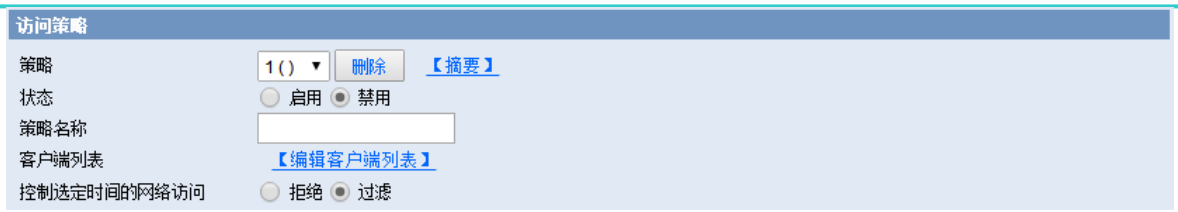
过滤 Cookies：Cookies 是 Web 网站保存在您电脑上的数据，当您和 Internet 站点交互的时候就会使用到 Cookie。

过滤 Java Applets：如果拒绝 Java，则可能无法打开使用 Java 工具编程的网页。

过滤 ActiveX：如果拒绝 ActiveX，则可能无法打开使用 ActiveX 工具编程的网页。

3.7.2 访问限制

使用 Internet 访问页面可以阻止或允许特定类型的 Internet 应用，您可以设置特定 PC 的 Internet 访问策略。



策略：您最多可以定义 10 条访问策略。点击“删除”钮删除一条策略，或者点击摘要按钮察看策略配置情况。

状态：启用或禁用一条策略。

策略名称：您应该为您的策略指定一个名称。

客户端列表：用于编辑客户端列表，策略只对处在该列表中的客户端生效。

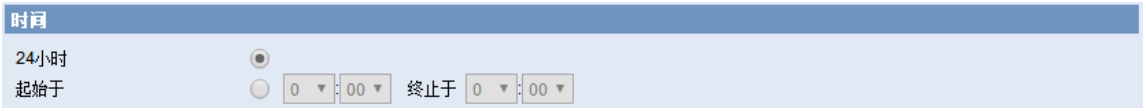
控制选定时间的网络访问：如果你想阻止在指定的日期和时间访问互联网的电脑，则选择拒绝。如果你想在指定的日期和时间过滤互联网的电脑，则单击过滤；您可以设置 10 条 Internet 访问策略过滤特定的 PC 在特定时间段访问的 Internet 服务。

创建 Internet 访问策略：

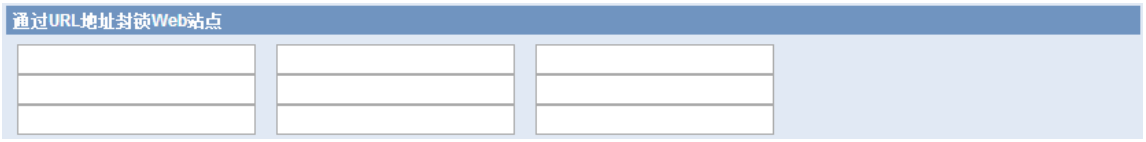
1. 从“Internet 访问策略”下拉菜单中选择一条。

2. 如欲启用这一策略，单击“启用“旁边的单选按钮。
3. 在所提供的字段中输入策略名称。
4. 单击“编辑客户端列表”按钮，出现“客户端列表”页面，输入应用该策略的客户端，可以使用 MAC 地址或者 PC 地址来指定 PC。完成页面修改后，单击“保存设置”，保存所作的修改，或是单击“取消改动”修改，完成修改后关闭这一窗口。
5. 确定这条策略生效的时间。选择这一策略生效的具体日期或是选择“每天”，之后输入这一策略生效的具体时段范围，或选择“24 小时”。
6. 如果拒绝或只允许访问特定 URL 地址的网站，则在“网站 URL 地址”旁边的单独字段内输入每一个 URL 地址。
7. 如果欲拒绝或只允许访问带特定关键字的网站，则在“网站关键字“旁白的单独字段内输入每一个关键字。

天：请选择您希望您的策略被应用的日期。



时间：输入您希望您的策略被应用的时间。



通过 URL 地址封锁 Web 站点：您可以通过输入的 URL 来封锁对部分网站的访问。

通过关键字封锁 Web 站点：您可以通过包含在 Web 页面中的关键字来封锁对其的访问。

3.7.3 DNS 过滤

使用 DNS 相关规则来进行数据过滤

3.7.4 MAC 过滤

使用 MAC 地址或者 PC 地址来进行数据过滤

3.7.5 数据流过滤

此页面可以建立防火墙规则来保护您的网路远离 Internet 网络病毒蠕虫恶意攻击。

数据包过滤：启用或者停用数据包过滤功能。

策略：选择对未符合所设置规则的数据包的动作。

只接受符合以下规则的网址：只允许访问匹配的 URL 地址。

丢弃符合以下规则的网址：只接收符合自定义规则的网络地址，丢弃所有其他的 URL 地址。

添加过滤匹配规则。"源端口"，" 目的端口"，" 源地址"，" 目的地址" 必须至少填写一项。

方向：

进口：数据包从 WAN 口到 LAN 口。

出口：数据包从 LAN 口到 WAN 口。

协议：数据包的协议类型。

源端口：数据包的源端口。

目的端口：数据包的目的端口。

源地址：数据包的源 IP 地址。

目的地址：数据包的目的 IP 地址。

3.8 转发规则

3.8.1 端口转发

端口转发功能允许您在您的网络上设置公共服务，如 Web 服务器，FTP 服务器，电子邮件服务器，或其他需要通过互联网才能运行的应用。当用户通过互联网发送这些类型的请求到您的网络时，路由器会通过端口转发功能将这些请求转发到相应的客户端。

应用程序：在应用程序提供的字段内输入应用程序的名字。

协议：为每一种应用选择 UDP 或者 TCP 协议，两者为同时时选择两种协议。

允许的源 IP 范围：在该栏填入 Internet 用户的 IP 地址。
来源端口：外部客户端服务所使用的外部端口编号。
IP 地址：输入您想让 Internet 用户访问的服务器的内网 IP 地址。
目的端口：服务在内部网络里使用的端口。
启用：选择“启用”框，启用您所定义的多端口转发服务。缺省配置为禁用（未选择）。

3.8.2 端口范围转发

某些应用程序可能要求转发特定的端口范围才能正常运行，当从 Internet 发出对某个端口范围的请求时，路由器会将这些数据发送到指定的计算机。出于安全考虑，可能要将端口转发仅限制在正在使用的那些端口上，如果不再使用该端口转发，建议取消“启用”复选框暂时禁用该端口转发。

转发

删除	编号	应用程序	开始	结束	协议	IP地址	启用
-无-							

应用程序：在应用程序提供的字段内输入应用程序的名字；
开始：内部网络提供给外界使用的开始端口号；
结束：内部网络提供给外界使用的端口范围的结束端口号；
协议：为每一种应用选择 UDP 或者 TCP 协议，两者为同时时选择两种协议；
IP 地址：应用或服务在内部网络上的 IP 地址。
启用：选择“启用”框，启用您所定义的多端口转发服务。缺省配置为禁用（未选择）。

3.8.3 端口触发

当一个应用程序使用特定的端口（称为触发端口）通过路由器向外建立连接时，再产生一定的流量之后,将在路由器上建立端口转发规则。

触发

			已触发端口范围		转发端口范围			
删除	编号	应用程序	开始	结束	协议	开始	结束	启用
-无-								

应用程序：在应用程序提供的字段内输入应用程序的名字；
开始：开始端口号；
结束：结束端口号；
协议：为每一种应用选择 UDP 或者 TCP 协议，两者为同时时选择两种协议；
启用：选择“启用”框，启用您所定义的多端口转发服务。缺省配置为禁用（未选择）。

3.8.4 DMZ 服务

此页面可以建立一个隔离区（DMZ）来区分局域网络与 Internet 网络。来自外网的数据，如果不是对内网数据包的回应或者符合自定义 NAT 条目的数据包，路由器会丢弃这些数据包。如果不想丢弃这些数据包，而是把它们发送到内网的某台计算机上，那么这台计算

机就是 DMZ 主机。

DMZ 主机 IP 地址：内网 DMZ 主机的 IP 地址。

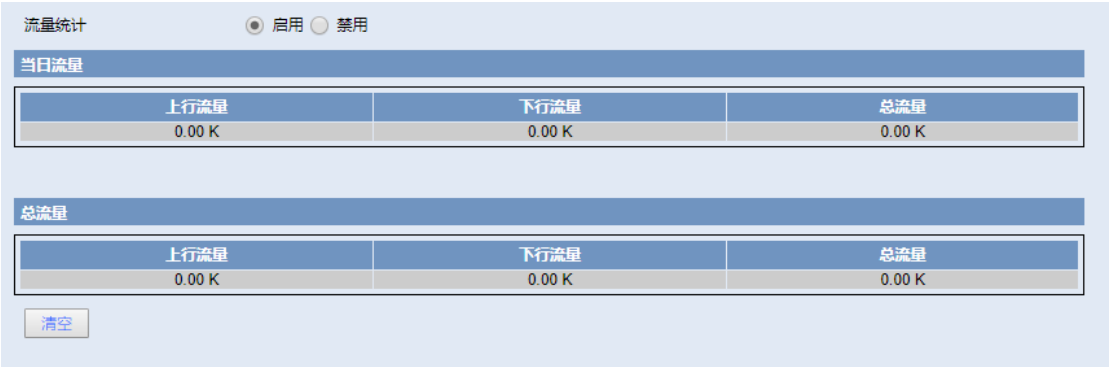
如果计算机未提供任何网络服务请不要设置此选项，因为它将把该计算的所有端口开放到网络上。

3.9 带宽服务

3.9.1 宽带监控

直观显示 WAN、LAN、WIFI 的网速带宽。

3.9.2 流量统计

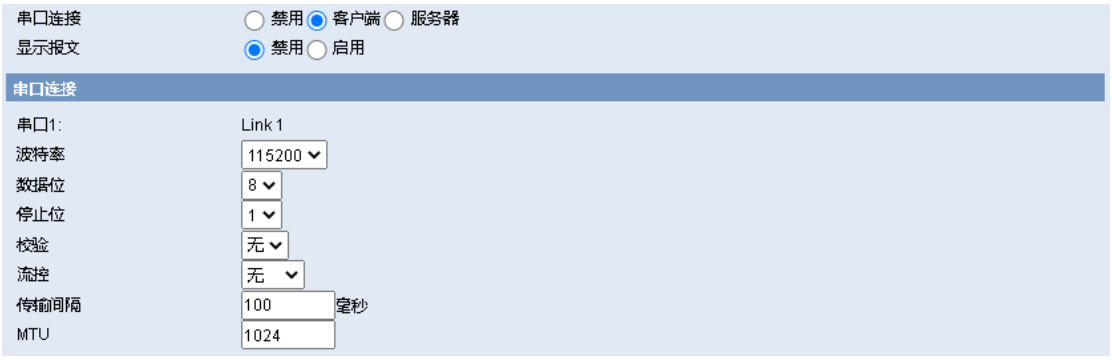


直观显示统计到的上下行，以及总流量。

3.10 物联互通

3.10.1 串口应用

通常情况下路由器拥有一个或者两个串口，同时内置了串口转 TCP/IP 程序。通过配置，路由器的串口作为一个串口协议转换设备，或者完全等同于一台 DTU 设备。



波特率：表示设备每秒传送的字节数。

数据位：数据位的个数可以是 4、5、6、7、8 等，构成一个字符。通常采用 ASCII 码。从最低位开始传送，靠时钟定位。

停止位：它是一个字符数据的结束标志。可以是 1 位、1.5 位、2 位的高电平。

检验：表示一组数据所采用的数据差错校验方式。有奇偶校验两种方式。

流控：包括硬件部分和软件部分两种方式。

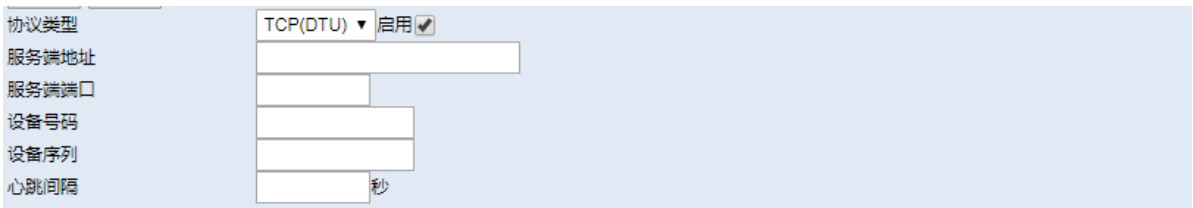
传输间隔：串口报文帧间隔。

MTU：串口报文帧最大长度。

连接模式：多中心为最多 5 个中心同时连接，同时进行数据传输，一份串口数据每个中心都进行发送；主备中心为配置主备两个中心，串口数据只发往其中一条链路。

主备模式：同时在线为主备链路同时连接服务器，但是串口数据只发往其中一条链路；单独在线为同一时间只有一条链路连接到服务器，这条链路断开后将连接另外一条链路。

自动返回主中心：在单独在线模式有效，当前链路为备份链路时，系统将在备份链路传输数据的同时尝试连接主服务器，当主服务器连接上后断开备份链路，使用主链路进行数据传输。



客户端协议类型

UDP(DTU)：串口转 UDP 连接，含自定义应用层协议，完全等同于一台 IP MODEM 的功能。

纯 UDP：标准的串口转 UDP 连接.

TCP(DTU)：串口转 TCP 连接，含自定义应用层协议，完全等同于一台 IP MODEM 的功能。

纯 TCP：标准的串口转 TCP 连接。

HPTCP：标准的串口转 HPTCP 连接。

HPUDP：标准的串口转 HPUDP 连接。

服务器地址：与路由器串口转 TCP 程序进行通信的数据服务中心的 IP 地址或者域名。

服务器端口：数据服务中心程序监听的端口。

设备号码：设备的 ID 号，11 字节的数据字符串。只有当协议类型设置成“UDP(DTU)”或者“TCP(DTU)”的时候这个配置项才有效。

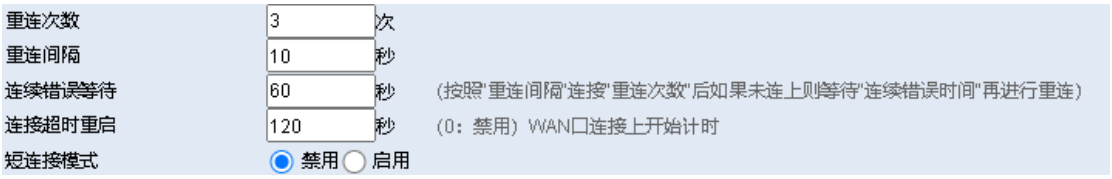
心跳间隔：心跳包的时间间隔。

自定义注册包：用户可以自定义注册包，用于连接时注册。

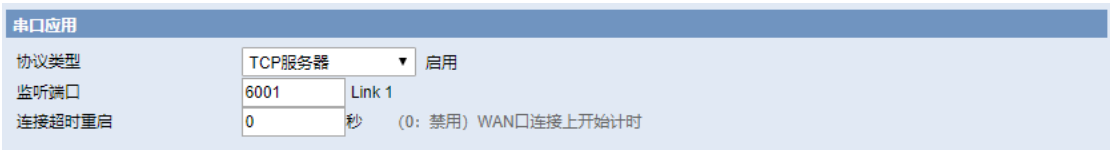
自定义心跳包：用户可以自定义心跳包，用于保持连接。

设备序列：设备序列号。

报文透传：勾选以后，对接收到的报文不做处理，直接转发



配置连接上不 TCP 服务器时执行的操作。

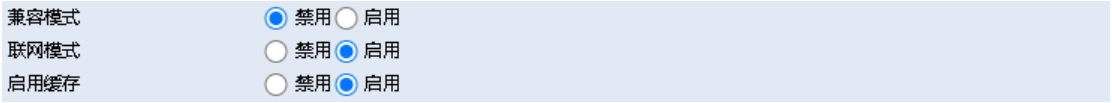


服务器协议类型：

TCP 服务器：透传 TCP 服务器。

Modbus TCP 服务器：设备将 ModbusTCP 报文转换为 ModbusRTU 报文。

监听端口：用于监听建立 TCP 连接的端口号。**连接超时重启**：多久没有客户端连接时重启。

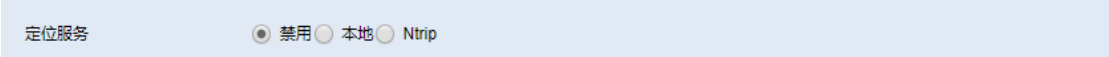


兼容模式：用于查询某些 TAG 值

联网模式：设定串口应用是否在广域网联网情况下才进行服务器连接。

启用缓存：配置是否在未连接服务器时缓存数据

3.10.2 定位服务



配置输出口是输出定位数据还是差分数据。

输出：选择数据输出的方式
网络协议，服务器地址，服务器端口：网络输出配置
信息类型：勾选后，输出的定位的信息会包含相应的类型数据。
设备 ID 号：用户可自定义，用于识别是哪个设备。
信息更新间隔：数据输出的时间间隔。
波特率，数据位，停止位，校验，流控：串口输出配置

3.10.3 短信控制

短信中心号码：用于转发接收到的信息。

名称：该控制动作的名称，自定义。

电话号码：指定接收该手机号控制，为空则接收任何手机号控制。
控制动作：包括连接，断开连接，重启路由器以及正在执行配置路由器的动作命令。
控制内容：接收到该内容的短信，会执行对应的操作。

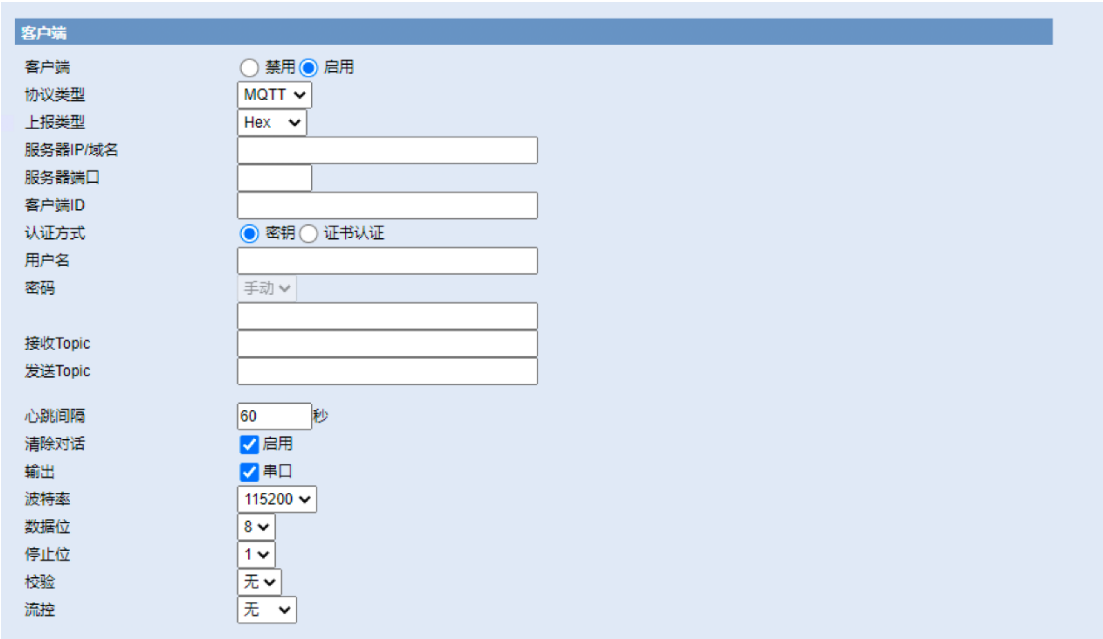
3.10.4 AliIOT

人工智能物联网服务，提供远程连接路由器客户端接口映射。可以提供任意 window 终端通过配置的两个端口连接路由器客户端。

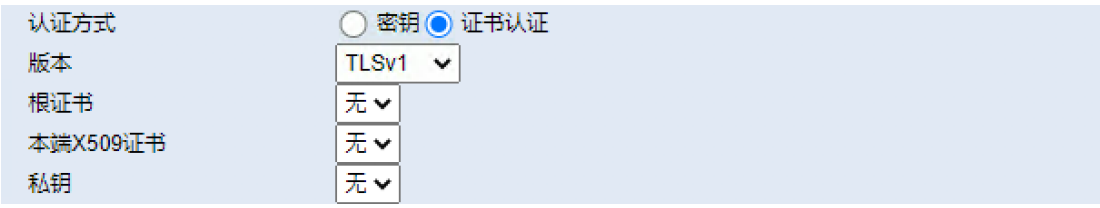
3.10.5 物联平台

物联平台基于 MQTT（Message Queuing Telemetry Transport，消息队列遥测传输协议），是一种基于发布/订阅（publish/subscribe）模式的"轻量级"通讯协议，构建于 TCP/IP 协议上。MQTT 最大优点在于，可以以极少的代码和有限的带宽，为连接远程设备提供实时可靠的消息服务。作为一种低开销、低带宽占用的即时通讯协议，使其在物联网、小型设备、移动应用等方面有较广泛的应用。

物联平台客户端



协议类型：支持通用 MQTT、阿里云、华为云、移动云、电信云五种协议类型
上报类型：支持上报 Hex(16 进制)，String(文本字符串)两种数据类型
服务器 IP/域名：服务器 IP/域名
服务器端口：服务器监听端口
客户端 ID：每个 MQTT 连接都需要唯一的客户端 ID
认证方式：支持自定义密钥跟证书认证两种方式
用户名：认证方式选择密钥认证时，手动填写的用户名
密码：认证方式选择密钥认证时，手动填写的密钥；通用 MQTT 协议下密钥可以自己定义，阿里云、华为云、移动云、电信云支持手动填写密钥或者系统自动生成密钥
接收 Topic：订阅的主题，多个订阅主题用逗号‘,’分隔
发送 Topic：发布的主题
心跳间隔：发送心跳的间隔时间
清除对话：重新连接后不收到断开期间发布的消息
输出：订阅的主题收到消息后，可以将该消息输出到串口
波特率：表示设备每秒传送的字节数
数据位：数据位的个数可以是 4、5、6、7、8 等，构成一个字符。通常采用 ASCII 码。从最低位开始传送，靠时钟定位
停止位：它是一个字符数据的结束标志。可以是 1 位、1.5 位、2 位的高电平
检验：表示一组数据所采用的数据差错校验方式。有奇偶校验两种方式
流控：包括硬件部分和软件部分两种方式
证书认证

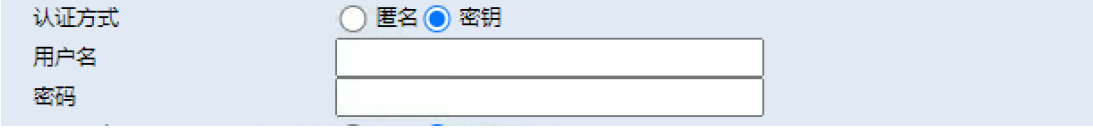


版本：支持 TLSV1、TLSV1.1、TLSV1.2

根证书：在证书系统中生成的根证书
本端 X509 证书：在证书系统中生成的客户端证书
私钥：在证书系统中生成的客户端私钥

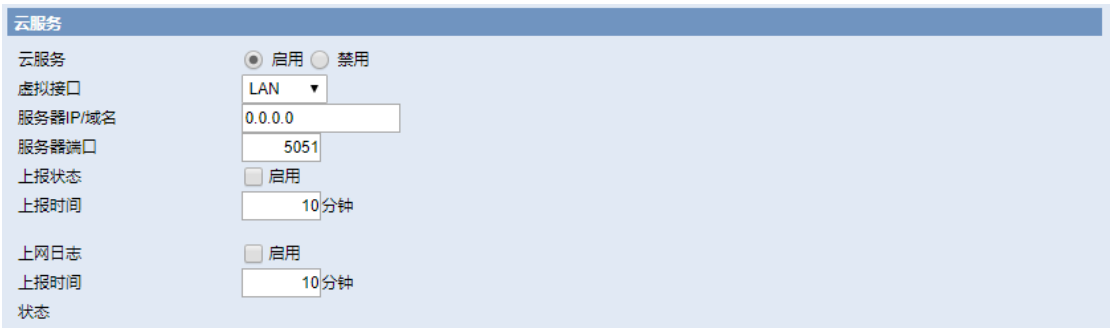
物联平台服务端

监听端口：MQTT 服务器监听的端口号
客户端 ID：填写了客户端 ID 表示只能支持该客户端 ID 的连接，不填写表示不校验
认证方式：支持匿名、密钥认证两种方式
重复消息：是否接收重复消息
日志：日志根据严重性可以输出全部、错误、警告、提醒不同等级的日志
消息重发间隔：对于 QOS1(至少发送一次)跟 QOS2(确保发送一次)两种 QOS 等级下，MQTT 服务器重发消息的间隔
系统主题发布间隔：系统主题$SYS 的发布更新间隔
消息最大并发数：仅针对 Qos 大于 0 的消息有效。表示最大正在处理的消息数，配合消息最大缓存队列可以用于限流和确保 MQTT 的稳定性，但是可能会出现消息丢失现象。
消息最大缓存队列：超过消息最大并发数的消息会被缓存到队列中。
最大连接数：支持的最大客户端同时连接数
额外配置：MQTT 服务器额外的配置
密钥认证



用户名：认证方式选择密钥认证时，需要填写认证的用户名
密码：认证方式选择密钥认证时，手动填写的密钥

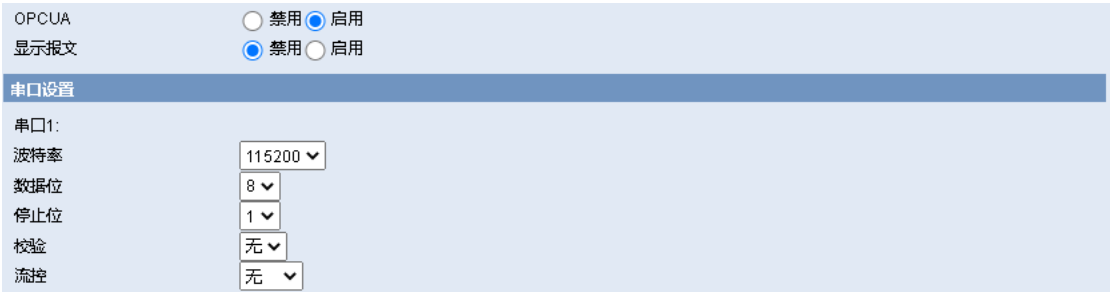
3.10.6 云平台



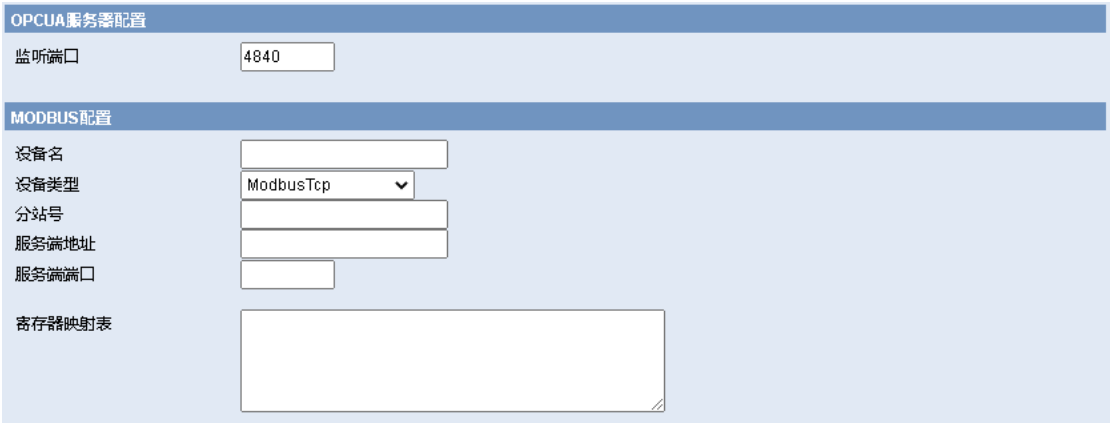
虚拟接口：选择 LAN 会上报 LAN 口的 IP，选择 modem 会上报 WAN 口的 IP
服务器 IP/域名，服务器端口：云服务的 IP 和端口号。
上报状态，时间：配置上报状态。
上报日志，时间：配置上报日志。

3.10.7 OPCUA

提供 OPCUA 设备端转 MODBUS 主机功能



OPCUA：启用关闭功能
串口设置：配置 MODBUS 主机端串口参数。



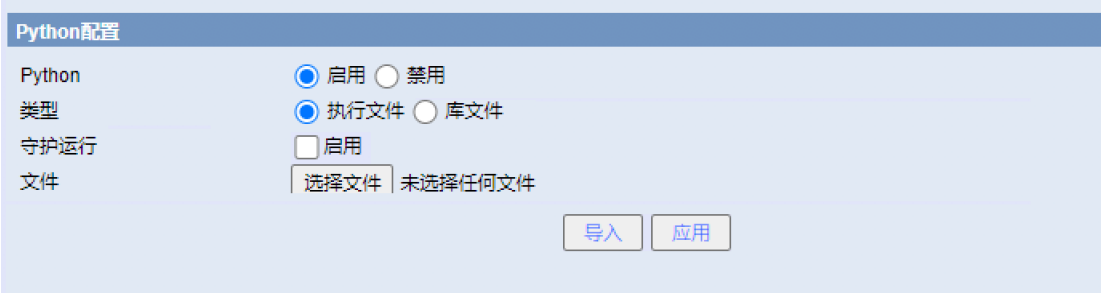
监听端口：OPCUA 设备端 TCP 服务器监听端口
设备名：OPCUA 协议设备名
设备类型：MODBUS 主机协议类型

分站号：OPCUA 设备分站号

寄存器映射表：格式：名字，数据类型，地址，长度；数据类型:SByte|Byte|Int16|UInt16|Int32|UInt32|Int64|UInt64|Float|Double|StringSTRING 类型是字符串长度，其他类型大于 1 会生成数组;eg:reg1,String,1,6;

3.10.8 Python

Python 是一种面向对象的解释型计算机程序设计语言。Python 具有丰富和强大的库，能够把用其他语言制作的各种模块很轻松地链接在一起。Python 功能模块，用户可以通过使用设备提供的 python 库来获取设备的状态(如网络状态，sim 卡信息等)。



类型：导入 python 可执行文件、python 库文件
守护运行：可执行的 python 文件需要长期运行
文件：用户选择需要导入的 python 文件

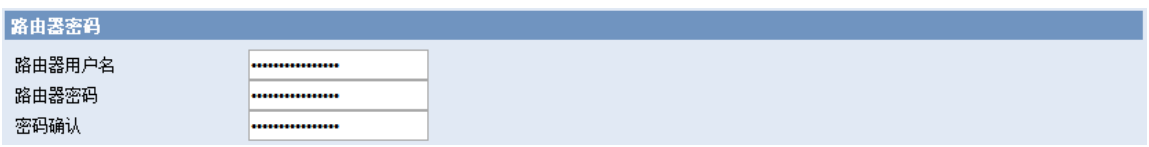
3.11 系统设置

3.11.1 快捷按钮

页面右上角提供设置 WEB 配置页面的显示语言按钮以及重启按钮。

3.11.2 密码管理

设置管理用户名和密码，最大支持 32 个字符的输入。

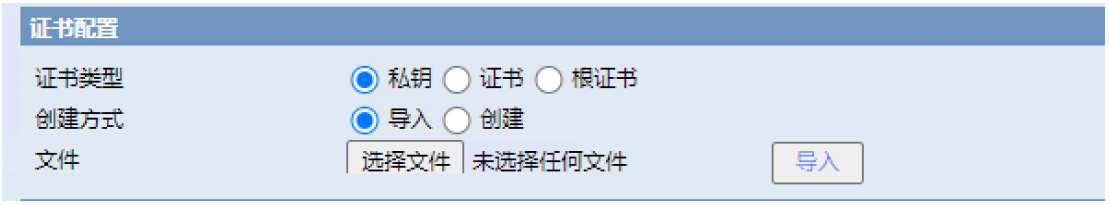


新密码长度不得超过 32 个字符，不得包含任何空格。确认密码应该和你设置的新密码

一致，否则会设置不成功。默认的用户名是：admin。建议您修改出厂的默认密码 admin，这样所有的用户试图访问和修改路由器都应该基于输入正确的路由器密码，才可以访问和使用。

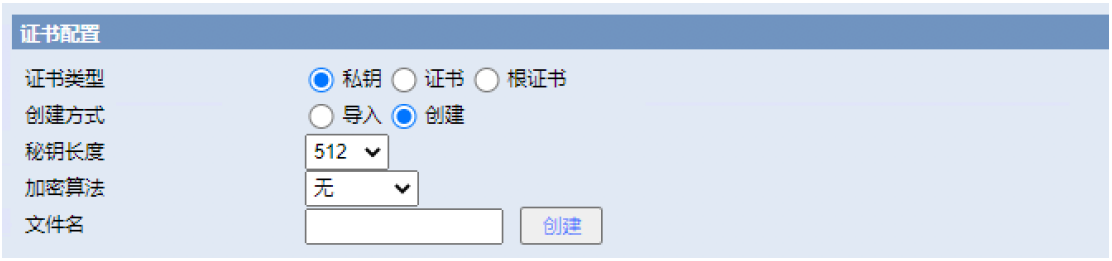
3.11.3 证书管理

证书管理是为了统一管理设备的证书，如 http 证书、mqtt 证书、ipsec 证书、openvpn 证书。



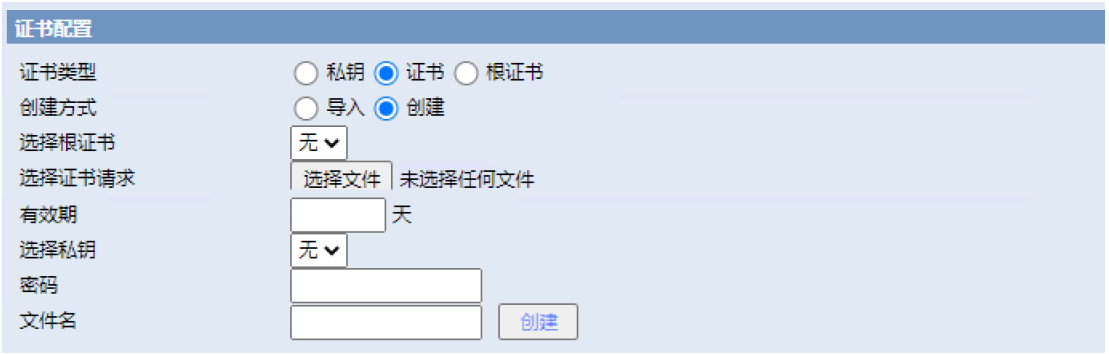
证书类型：分为私钥、证书、根证书三种类型
创建方式：用户可以导入外部创建的证书(PEM 证书文本格式，DER 证书二进制格式)，或者选择设备创建的方式
文件：用户选择将要导入的证书文件

证书配置-私钥



密钥长度：支持 512、1024 两种密钥长度
加密算法：支持 DES、DES3、AES128、AES192、AES256
文件名：将要创建的私钥名称

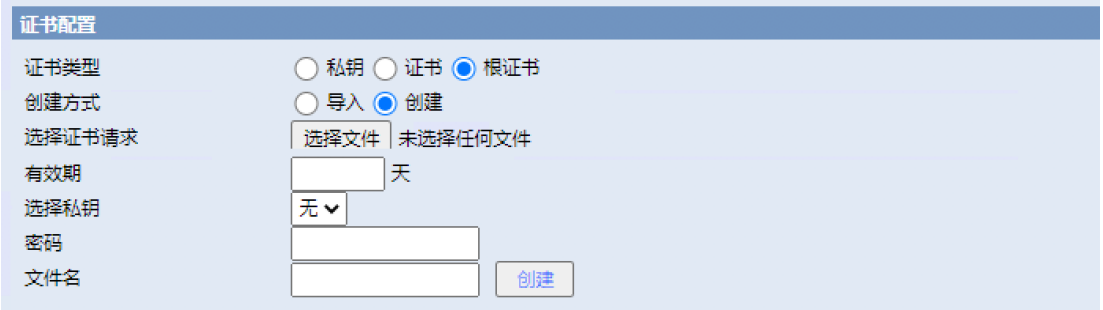
证书配置-证书



选择根证书：选择创建好的根证书文件
选择证书请求：选择创建好的证书请求文件

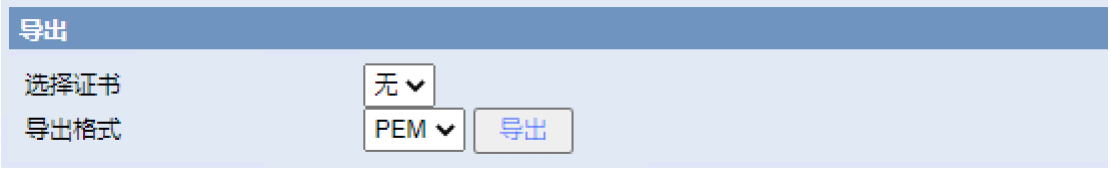
有效期：证书的有效期天数
选择私钥：选择创建好的私钥文件
密码：私钥的密码
文件名：将要创建的证书名称

证书配置-根证书



选择证书请求：选择创建好的证书请求文件
有效期：证书的有效期天数
选择私钥：选择创建好的私钥文件
密码：私钥的密码
文件名：将要创建的根证书名称

导出



选择证书：选择将要导出的证书文件，私钥不支持导出
导出格式：PEM 证书的文本格式，DER 证书的二进制格式

证书请求

选择私钥：选择对应的私钥文件
密码：私钥文件的密码，没有可不填
国家：国家代号

省份：省份代号
城市：城市代号
组织单位：组织单位名称
部门：部门名称
主机名/域名：组织单位的主机名或者域名
导出：导出证书请求文件
一键生成根证书：根据填写的证书请求信息，自动生成根证书

3.11.4 设备管理

配置 WEB 服务器参数。

协议：使用 HTTP 协议或 HTTPS 协议来管理路由器。

本地访问 Web 界面端口：设置 WEB 服务器的访问端口。例如网关地址为 192.168.1.1，设置服务器端口 1010，当访问 WEB 配置界面时要在地址栏中输入 http://192.168.1.1:1010。服务器的默认端口为 80。

选择证书：选择 HTTPS 的证书

选择私钥：选择 HTTPS 的私钥

Telnet：启用或关闭 Telnet 服务器。

SSH 服务：开启或关闭 Secure Shell 功能（SSH2）。

SSH TCP 转发：开启或关闭 SSH TCP 转发功能。

密码登陆：开启或关闭密码登陆。

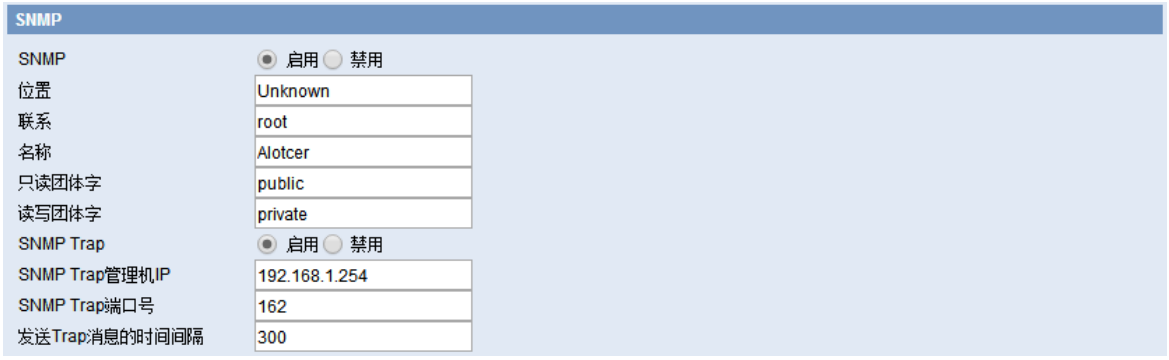
端口：设置 Secure Shell 访问端口。

授权密钥：设置授权密钥。

允许远程通过 Web 访问：此功能允许通过互联网从远程位置管理路由器。

如果你还没有设置密码，您还必须为您自己的路由器设置的默认密码。要远程管理路由器，进入 http://xxx.xxx.xxx.xxx:8088（x 代表的路由器的 Internet IP 地址， 8088 代表指定的端口），在您的网页浏览器地址栏。你会被要求输入路由器的密码。如果您使用 HTTPS，您需要指定 URL 为 https://xxx.xxx.xxx.xxx:8088。

警告：如果远程路由器的访问功能被启用，任何人知道路由器的 Internet IP 地址和密码，将可以改变路由器的设置。



SNMP：根据 SNMP 客户端的配置来配置路由器的 SNMP 选项，各选项需要与客户端都一致才能正常连接。

SNMP Trap：配置设备主动发送 SNMP 通知给对应的 IP 地址。

3.11.5 系统时间

设置系统时间及网络同步时间服务器。

路由器时间：设备的当前时间显示。

PC 系统改时间：当前管理设备的 PC 的系统时间。

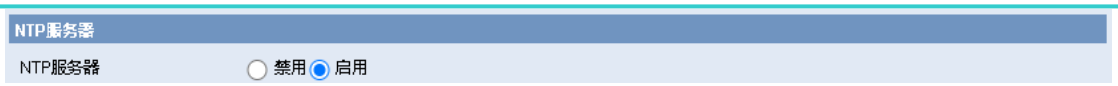
手动设定时间：手动设置设备的系统时间，点击“自动设置”按钮将自动将 PC 系统时间设置到设备上。

时区：选择所在时间的时区。

夏令时(DST)：选择所属的夏令时。

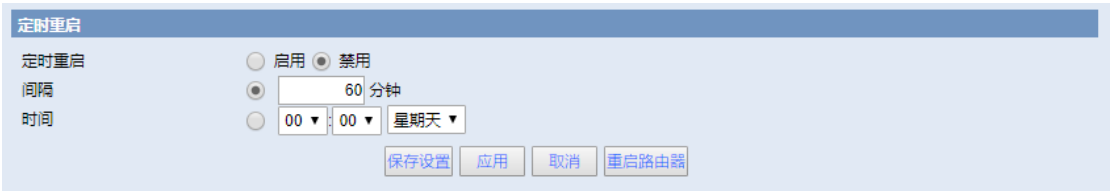
NTP 客户端：启用或禁用时间服务器。

服务器 IP/主机名：输入需要同步的时间服务器。



NTP 服务器：启用或者关闭 NTP 服务器。

3.11.6 重启路由器

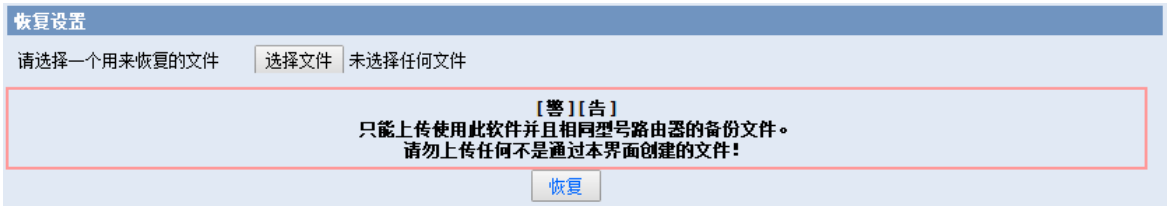


可设置定时重启，也可以立即重启路由器。

3.11.7 配置管理

恢复出厂设置：选择恢复出厂设置点击“应用”按钮，系统将恢复出厂设置。恢复前，请最好先备份系统配置。

备份配置：通过导出配置文件来备份系统的设置或通过导入配置文件来恢复系统设置。

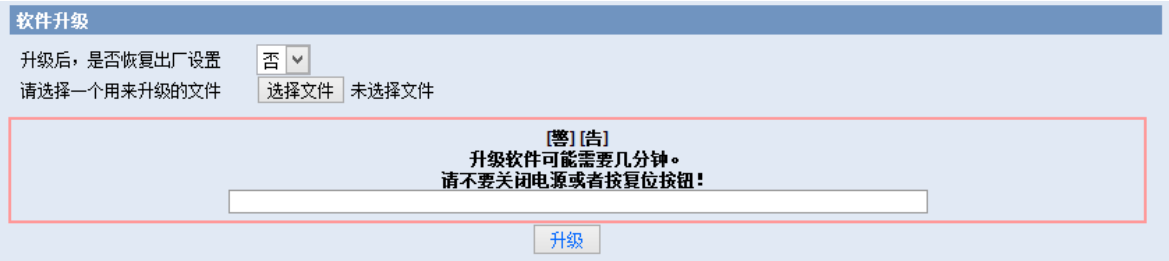


恢复设置：使用导出的配置参数文件来恢复路由器的系统配置。

您可以藉由导出配置文件来保存系统的设置、或藉由导入配置文件来恢复系统设置。

3.11.8 软件升级

更新软件获得新功能。



升级后，是否恢复出厂设置：如果你想在升级后恢复路由器的默认设置，请选择“是”选项。

选择升级文件：升级系统功能程序。

路由器的软件可以通过路由器的 WEB 页面对其进行升级，路由器的升级文件可以从 www.alotcer.com 下载，或者直接向技术人员索取。如果您所得到的升级文件是经过压缩的（.zip 或者.rar），在升级之前请解压压缩文件。

点击“选择文件…”按钮选择用于升级的文件，然后点击“升级”按钮即可开始升级路由器的软件。

上传更新需要大约几分钟的时间请耐心等候。请不要关闭电源或者按复位按钮！警告！不正常的升级文件将中断系统的运作。

3.11.9 DDNS

开启/关闭动态域名解析服务。此服务将更新公网的 IP 地址，请确保想访问的地址处于公网。

动态域名服务：路由 IP 地址将映射到一个固定的域名解析服务上，用户可以通过域名来管理配置路由器。

用户名/密码：从域名解析服务商申请到的用户名及密码。

动态域名：从域名解析服务商申请到的域名。

类型：根据不同的服务器进行配置。

通配符：配置是否支持通配符。

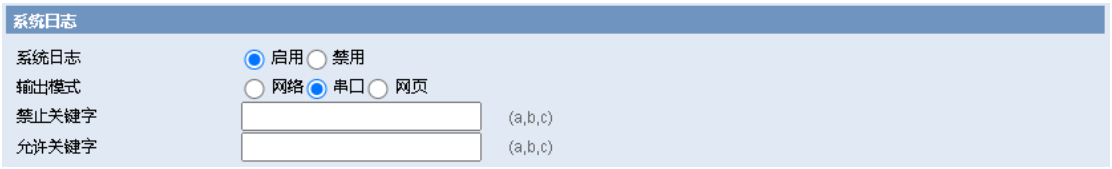
不使用外部 IP 检测：开启或禁用不使用外部 IP 检测。

强制更新间隔：更新动态 DNS 到服务器的间隔。

状态显示目前连接的状态，已经在连接过程中的信息。

3.11.10 系统日志

记录系统的运行日志。



系统日志：是否启用系统日志记录，系统日志以 SYSLOG 格式输出。

输出模式：分为通过网络 SYSLOG、串口、网页进行输出。

网络输出：选择此项则系统日志将发送到所填写的远程主机上，如果远程主机是日志服务器，则可远程查看系统日志。

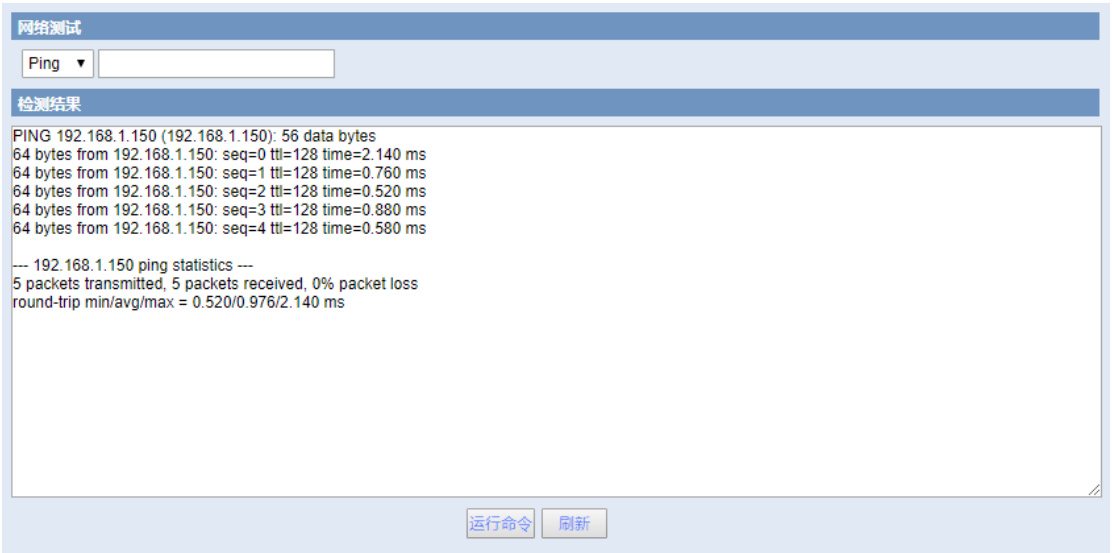
串口输出：日志会从设备的串口输出。

网页输出：日志会直接打印在网页上。

禁止关键字：禁止日志标题中带设定关键字的内容输出。

允许关键字：允许日志标题中带设定关键字的内容输出。

3.11.11 网络测试



测试是否可以连接上其他 IP 或者域名。可以选择使用 PING 或者 TRACE 两种方式