



TG462 系列网关说明书	文档编号	产品版本	密级
		V3.0	低
	产品名称: TG462		共 39 页

TG462 工业级物联网网关用户使用说明书

V3.0

此说明书适用于下列型号产品:

型号	产品类别
TG462-G	GPRS WIFI GateWay
TG462-C	CDMA WIFI GateWay
TG462-W	WCDMA WIFI GateWay
TG462-E	EVDO WIFI GateWay
TG462-LT	LTE/TD-SCDMA WIFI GateWay
TG462-LF	LTE/WCDMA WIFI GateWay
TG462-A	TDD/FDD WIFI GateWay



厦门计讯物联科技有限公司

Xiamen Top-Iot Technology Co., Ltd.





文档修订记录

日期	版本	说明	作者
2018. 10. 15	V1. 0	初始版本	林文浩
2019. 5. 17	V1. 1	改进几个配置描述	詹昌鑫
2020. 11. 23	V3. 0	细节完善	卢惠铃





目录

一	产品简介.....	4
1.1、	产品概述.....	4
1.2、	产品外观尺寸图.....	4
1.3、	物理特性.....	5
二	产品安装.....	5
2.1、	安装前确认.....	5
2.2、	配件的安装.....	5
三	参数配置.....	8
3.1、	查看.....	9
3.2、	设置.....	13
3.3、	安全.....	19
3.4、	VPN.....	23
3.5、	高级.....	29
3.6、	数据采集.....	30
3.7、	管理.....	33



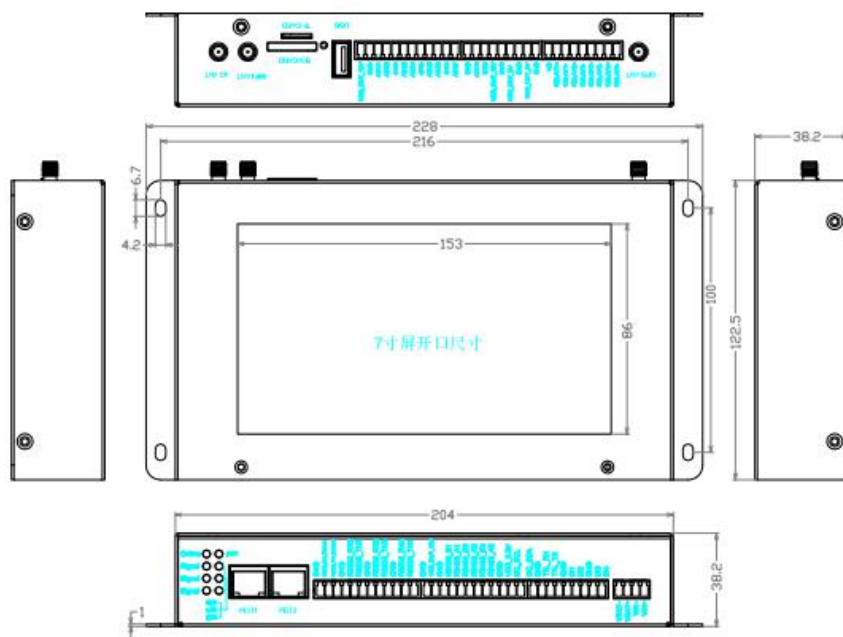
一 产品简介

1.1、产品概述

TG462 系列工业级物联网网关是一款遵循国家环保行业标准设计的专用数据采集网关。设计完全满足工业级标准和环保行业需求，采用高性能的工业级高端处理器，软件多级检测和硬件多重保护机制来提高设备稳定性。该产品广泛应用大气扬尘监测、污染源监测、污水处理、废弃监测、噪声扬尘等环境监测领域



1.2、产品外观尺寸图





1.3、物理特性

项 目	内 容
外壳	金属外壳，保护等级 IP30。外壳和系统安全隔离，特别适合工控现场应用
外形尺寸	228mm X 122.5mm X 38.2mm

二 产品安装

2.1、安装前确认

设备的包装包括以下：

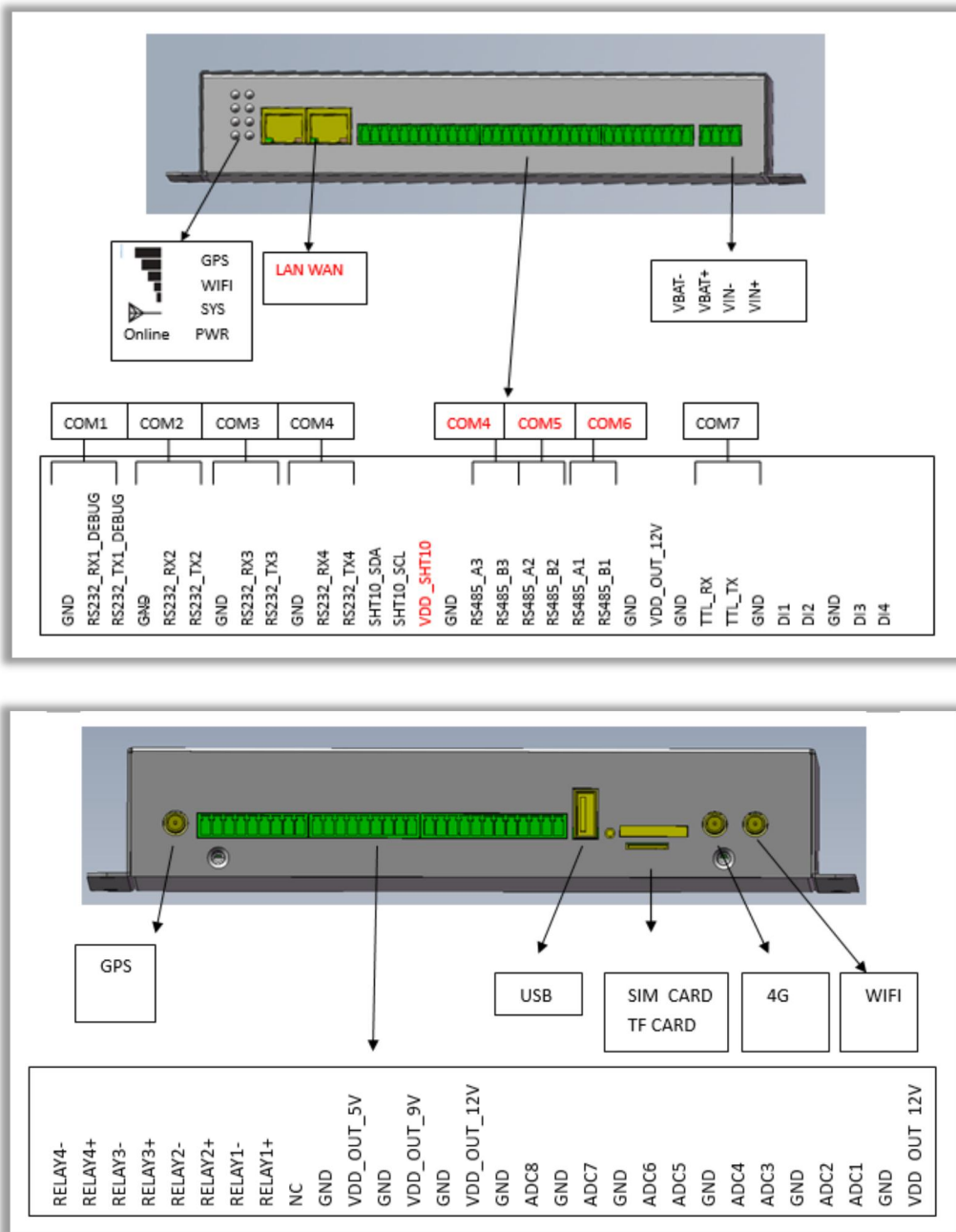
- 一台 TG462
- 一个电源
- 一根 4G 天线
- 一根 WiFi 天线
- 一根串口线
- 一根以太网线
- 一个 4PIN 绿色接线端子
- 三个 9PIN 绿色接线端子
- 三个 12PIN 绿色接线端子

如果有缺失，请联系销售人员

2.2、配件的安装

配件接线如下图：





■ SIM 卡安装:

SIM/UIM 卡是无线拨号上网的必要辅件，所以 SIM/UIM 卡必须被正确安装才能达到无线稳定快速上网的效果。

现今运营商办理在 SIM/UIM 卡有多种标准，本设备使用的是大卡，若办理的是小卡，则需要带着相应卡套方能在本设备上使用。

安装时先用尖状物插入 SIM/UIM 卡座旁边小黄点，卡槽弹出。SIM/UIM 金属芯片朝外放置于 SIM/UIM 卡槽中，插入抽屉，并确保插到位。



注意：SIM 卡请勿在设备上电的情况下插拔，会导致 SIM 卡损坏

■ 接口连接：

TG462 自带一个 RS232（com1）串口作为日志输出，此串口可用于系统日志查看、调试功能等应用。

TG462 带有 4 个 RS232 接口（其中 1 路做 DEBUG、1 路和 RS485 复用）、3 个 RS485 接口（其中 1 路和 RS232 复用）、1 个 I2C 接口、1 个 TTL 电平串口、4 路开关量输入接口、8 路模拟量输入接口（12 位 AD、支持 4-20mA 电流或 0-5V 电压信号）、4 路继电器输出、5 路电源输出（外设供电）。

可扩展 USB、TF 卡接口、TFT 显示屏、GPS 等其他功能。

线材颜色	对应 DB9 母头管脚	对应设备
蓝色	2 (RX)	(TX)
棕色	3 (TX)	(RX)
黑色	5 (GND)	(GND)

线材颜色	对应网关
红	(A)
黑	(B)

■ 电源安装：

可使用标配 1.5A/12VDC 电源，也可以直接采用 5-35VDC 电源给设备供电，当用户采用外加电源给设备供电时，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）。

■ 天线安装：

天线为设备增强信号的必要配件，必须正确安装方能达到最优的上网体验。

设备天线接口为 SMA 阴头插座。将配套天线的 SMA 阳头旋到 ANT 天线接口上，并确保旋紧，以免影响信号质量。

■ 指示灯说明：

指示灯是设备运行状态的最直观显示，从指示灯的状态可以方便、快速、较准确地判断设备的运行状态。

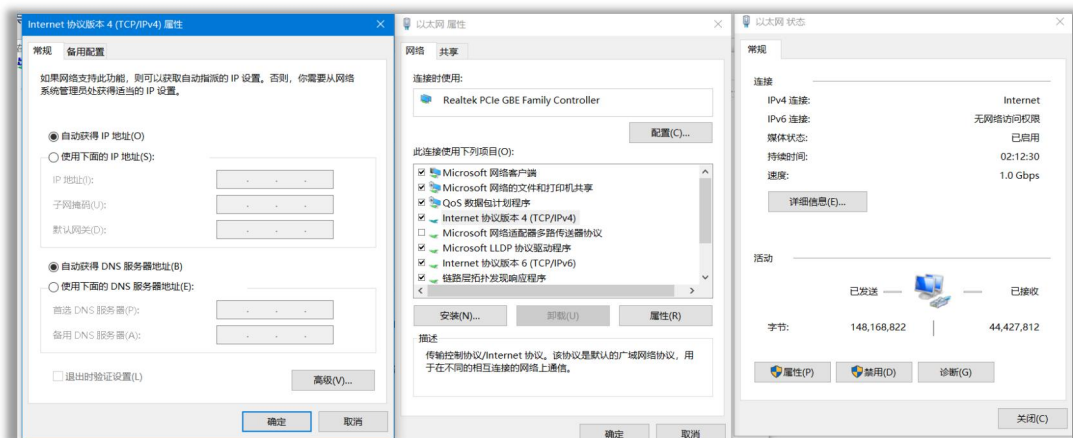


指示灯	状 态	说 明
PWR	亮	设备电源正常
	灭	设备未上电
信号强度指示灯	亮一个灯	信号强度较弱
	亮两个灯	信号强度中等
	亮三个灯	信号强度极好
System	闪烁	系统正常运行
	灭	系统不正常
GPS	亮	GPS 获取到位置
	灭	GPS 没有获取到位置
Online	亮	设备已登录网络
	灭	设备未登录网络
WIFI	灭	WIFI 未启用
	亮	WIFI 已启用
WAN	灭	WAN 网线未连接
	亮	WAN 网线已连接
LAN	LAN 闪烁	LAN 口连接正常
	灭	LAN 口未连接

三 参数配置

用一根网线将设备的 LAN 口和电脑的网口连接。

或使用笔记本电脑或手机等移动终端连接设备的默认 WIFI 热点



网卡配置自动获取或者设置 IP 为 192.168.1.xxx（和 TG462 同个网段），如：192.168.1.212



网络连接详细信息	
网络连接详细信息(D):	
属性	值
连接特定的 DNS 后缀	lan
描述	ASIX AX88772C USB2.0 to Fast Ethernet
物理地址	00-0E-C6-AA-EF-1E
已启用 DHCP	是
IPv4 地址	192.168.1.149
IPv4 子网掩码	255.255.255.0
获得租约的时间	2019年5月16日 13:42:58
租约过期的时间	2019年5月17日 1:42:59
IPv4 默认网关	192.168.1.1
IPv4 DHCP 服务器	192.168.1.1
IPv4 DNS 服务器	192.168.1.1

Router

← → ↻ ⓘ 不安全 | 192.168.1.1/cgi-bin/luci

需要授权
请输入用户名和密码。

用户名

密码

打开浏览器，输入默认登入 192.168.1.1，进入登入页面

输入默认用户名 admin，默认密码 admin，进入配置页面

3.1、查看

查看菜单用来查看系统相关信息



3.1.1、系统

显示与系统相关的信息

状态	
系统	
主机名	router
主机型号	tg462
SN	20190516051
固件版本	1.0.16_256m
发布时间	2019-05-08 15:22:17
本地时间	2019-05-16 16:44:05 Thursday
运行时间	0h 12m 50s
平均负载	0.05, 0.05, 0.05
内存	
可用数	225112 kB / 248220 kB (90%)
空闲数	218412 kB / 248220 kB (87%)
已缓存	6700 kB / 248220 kB (2%)
已缓冲	0 kB / 248220 kB (0%)



3.1.2、网络

显示网络信息

状态

网络

IPv4 WAN状态

usb0

类型: lte
地址: 10.207.37.90
子网掩码: 255.255.255.252
网关: 10.207.37.89
MAC地址: 22:7b:87:30:cd:72
DNS 1: 218.85.152.99
DNS 2: 218.85.157.99
已连接: 0h 0m 57s
信号: 31 dBm
网络: LTE
SIM卡状态: ON
IMEI: 867732038557856
连接状态: 已连接

在线状态

在线

活动连接

43 / 16384 (0%)

LAN状态

IP地址

192.168.1.1

子网掩码

255.255.255.0

DHCP服务器

启用

MAC地址

fe:e9:fd:9b:2c:f0

无线状态

无线

禁用

DHCP分配

主机名	IPv4-地址	MAC-地址	剩余租期
DESKTOP-IBPGIDR	192.168.1.149	00:0e:c6:aa:ef:1e	11h 58m 43s

3.1.3、路由表

显示路由表

ARP

IPv4-地址	MAC-地址	接口
192.168.1.100	08:57:00:e5:88:93	br-lan

活动的IPv4-链路

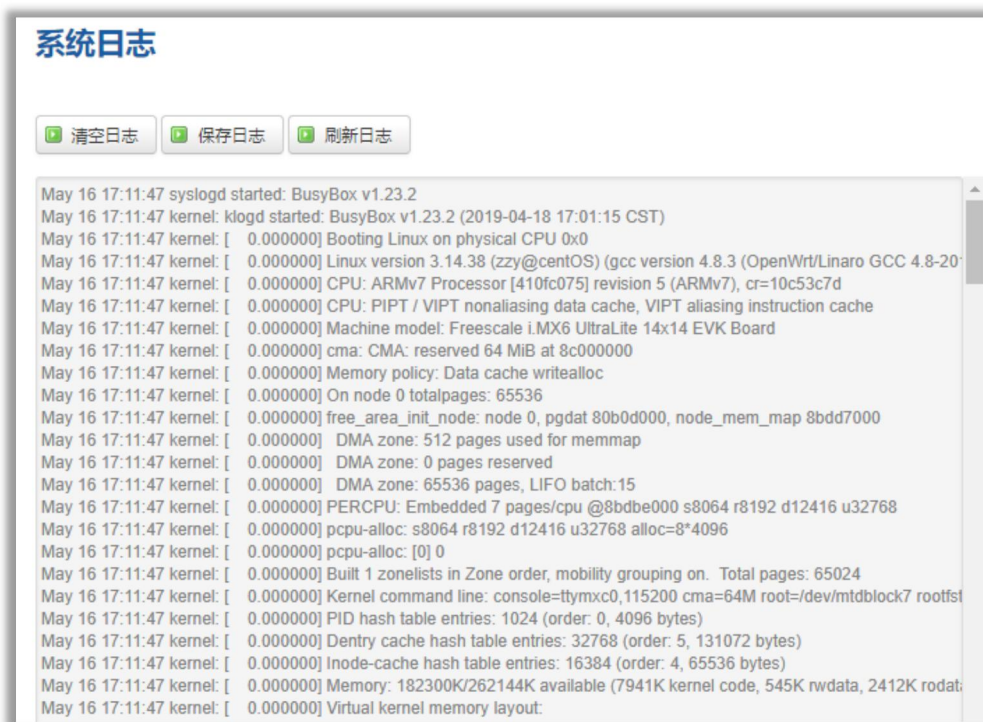
网络	目标	IPv4-网关	跃点数
wan	172.28.120.22	0.0.0.0	0
lan	192.168.1.0/24	0.0.0.0	0
wan	0.0.0.0/0	172.28.120.22	0

活动的IPv6-链路

网络	目标	IPv6-网关	跃点数
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF
loopback	0:0:0:0:0:0:0:1	0:0:0:0:0:0:0:0/0	00000000
lan	FF02:0:0:0:0:0:1:2	0:0:0:0:0:0:0:0/0	00000000
(eth2)	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
lan	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
(ra0)	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF

3.1.4、系统日志

显示系统日志



默认日志保存 64KB，重启后清空。可在管理-日志设置 调整日志存储大小最高 2048KB。

点击保存日志可以导出当前日志

3.1.5 、VPN 状态

显示 VPN 的状态

VPN		
VPN状态	类型:	l2tp
	IP地址:	192.168.18.2
	子网掩码:	255.255.255.255
	网关:	192.168.18.1
	已连接时间:	3s

3.2、设置

设置主菜单下面包括了需要设置的对象有：WAN（外网），LAN（内网），WIFI 设置，在线探测等子菜单项。



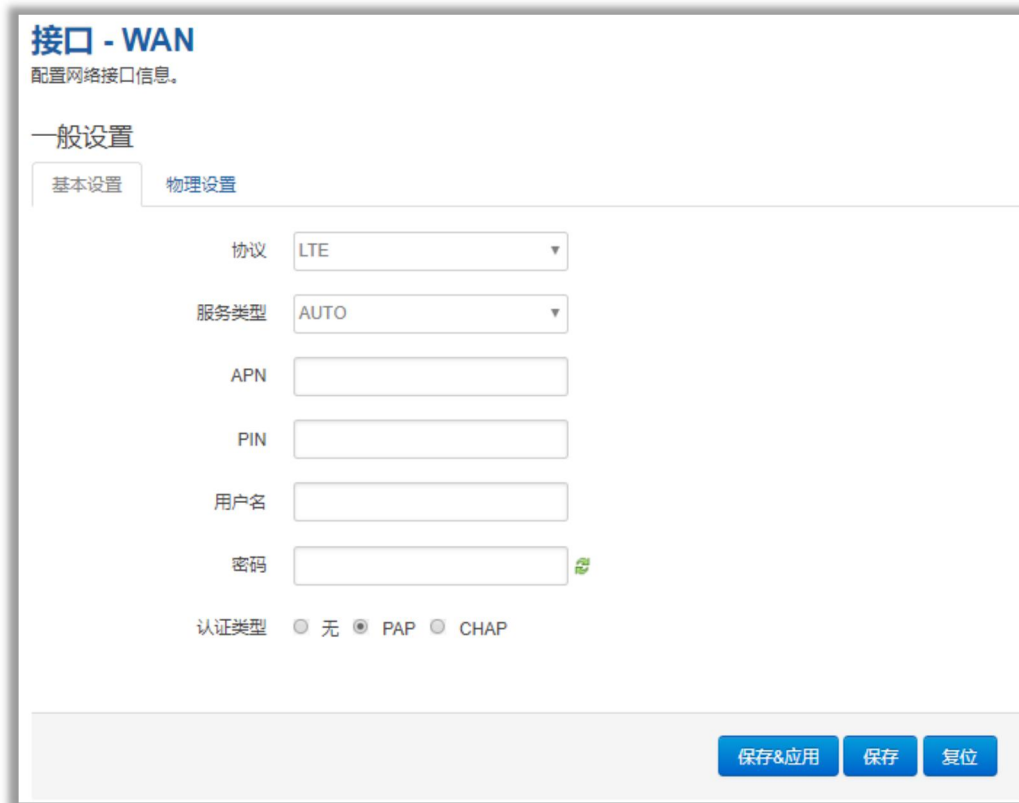


主要是用来设置网络相关参数。

3.2.1、WAN 口

WAN 口菜单项支持 DHCP/静态 IP/PPPoE/3G/LTE 等连接模式。

选择你需要的模式，点击切换 “切换协议”，再配置相关的参数，就可以实现连接。



服务类型：指的是网络类型，默认是自动的，如果对网络类型不熟悉，请保持默认值

APN：运营商的 apn，不同的运营商有不同的 apn。

中国移动是 cmnet，中国联通是 3gnet，中国电信是 ctnet。

专网卡也会有一个专门的 apn，在办卡时，由运营商提供；具体的 apn 参数可以咨询运营商
对于普通的数据卡，这个值可以为空。

通常情况下，保留默认参数即可，设备将自动启用最合适的 apn。

若运营商有要求特定的 APN 参数，则按照运营商给的 APN 参数配置。

PIN：SIM 卡的 PIN 码, 请慎重使用，以避免卡被锁住

PAP/CHAP 用户名：专网卡时需要输入用户名，其它卡时可以为空

PAP/CHAP 密码：专网卡时需要输入密码，其它卡时可以为空

当使用的是非专网卡





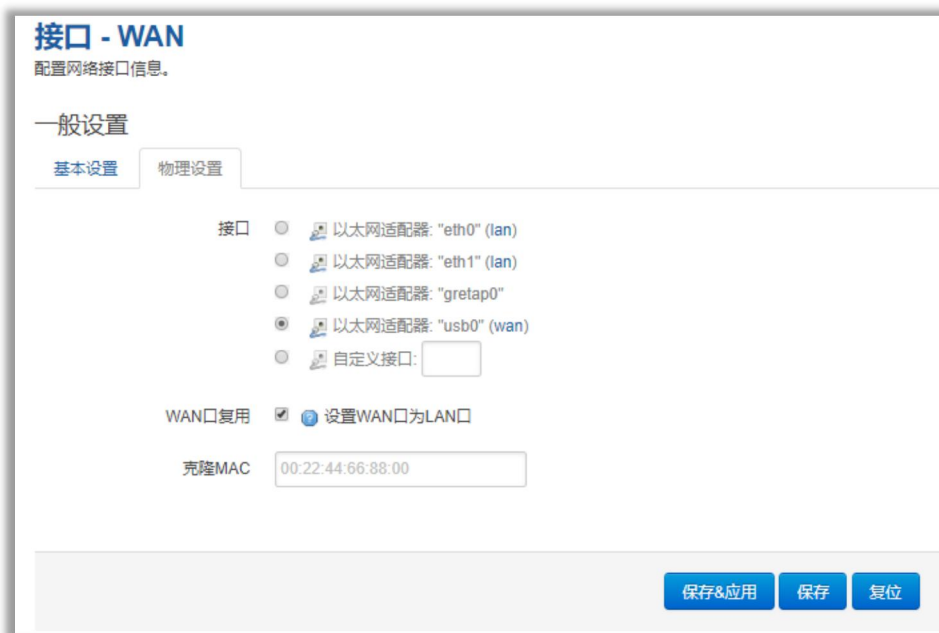
拨号号码：不同的网络类型对应不同的拨号号码

认证类型：如果有用户名，密码，需要指定认证类型。

PAP 是明文认证，CHAP 是握手认证。

要根据运营商的网络来选择认证类型，否则拨号会失败

WAN 口复用：当连接模式 3G 或者 LTE 时，可以利用 WAN 口为 LAN 口



3.2.2、LAN 口

LAN 口菜单项主要用来配置设备的 IP，DHCP 服务器的启用，以及分配的 IP 地址的范围。

参数的含义如下：






IPv4 地址：要配置 LAN 口的地址

IPv4 子网掩码：LAN 口地址的掩码

IPv4 网关：指明下一跳路由网关



DHCP服务器

基本设置

关闭DHCP ☐ ② 禁用本接口的DHCP。

开始 ② 网络地址的起始分配地址。

客户数 ② 最大地址分配数量。

租用时间 ② 地址租期，最小2分钟(2m)。

保存&应用 保存 复位

关闭 DHCP：点击关闭 DHCP 服务器

开始：分配的 dhcp 服务器的起始地址，比如 100，代表从 192.168.1.100 开始分配

客户数：可分配的 IP 地址数，确保开始数加客户数不能超过 250

租用时间：分配的 IP 的时间长短。

3.2.3、无线

无线菜单项主要用来设置无线的 SSID，工作模式，密码等参数，不同的环境可能需要不同的配置参数。



无线设置

在本页面，我们可以配置无线的基本与高级参数

接口配置

基本设置

WiFi 2.4G ☒ 启用 ☐ 禁用

网络名(SSID)

信道

模式

密码

保存&应用 保存 复位





WiFi 2.4G: 点击”开启“，启用 WiFi 功能

网络名 (SSID)：无线网络名

信道：支持 1~13 信道，默认是自动，信道可以自动变化。

模式：目前支持 802.11b, 802.11g, 802.11n 802.11b 速率只能达到 11Mbps, 802.11g 可以达到 54Mbps

密码：预共享密码，用户需要输入这个密码，才能连上；密码最短 8 个字节。

3.2.4、在线探测

在一些恶劣的环境，很容易出现网络连接断开的情况。在线探测会定时去检测网络连接状况，如果出现异常，就会重新连接；在尝试了一段时间后，如果还是无法连上，就会重启设备，以达到网络上线的目的。各个参数的含义如下：



The image shows a web interface titled "在线探测" (Online Detection). It contains several configuration options:

- 在线探测** (Online Detection): A toggle switch set to "启用" (Enabled).
- 探测类型** (Detection Type): A dropdown menu set to "Ping".
- 主探测服务器** (Primary Detection Server): A text input field containing "114.114.114.114".
- 次探测服务器** (Secondary Detection Server): A text input field containing "202.96.199.133".
- 重试次数** (Retry Count): A text input field containing "3".
- 重试间隔** (Retry Interval): A text input field containing "60", followed by a unit selector set to "秒" (Seconds).
- 启用重启** (Enable Restart): A toggle switch set to "启用" (Enabled).
- 探测失败重启时间** (Restart Time after Detection Failure): A text input field containing "10", followed by a unit selector set to "分钟" (Minutes).

At the bottom right, there are three buttons: "保存&应用" (Save & Apply), "保存" (Save), and "复位" (Reset).

探测类型：目前支持 ping/traceroute/DNS 三种探测方式。

Ping: ping 会去 ping 一个 IP 或者域名，ping 通否认为在线

Traceroute: traceroute 会去跟踪路由路径，如果可以到达目的地址，则认为在线

DNS: DNS 会解析一个域名，如果可以解析，则认为在线

默认使用 ping，使用 traceroute 相对会比较耗流，DNS 解析较快，但因为 DNS 有缓存，导致离线后，还在线的情况。相对使用 ping 是最合理的。

主探测服务器：优先检测的服务器，可以是 IP，也可以是域名

次探测服务器：如果探测主服务器失败，则可以选择次探测服务器。





重试次数：如果探测失败，可以指定重试的次数

重试间隔：两次探测之间的时间间隔

启用重启：如果一直不在线，点击“开启“，会在指定的时间后重启

探测失败重启时间：指定多长时间不在线，重启设备

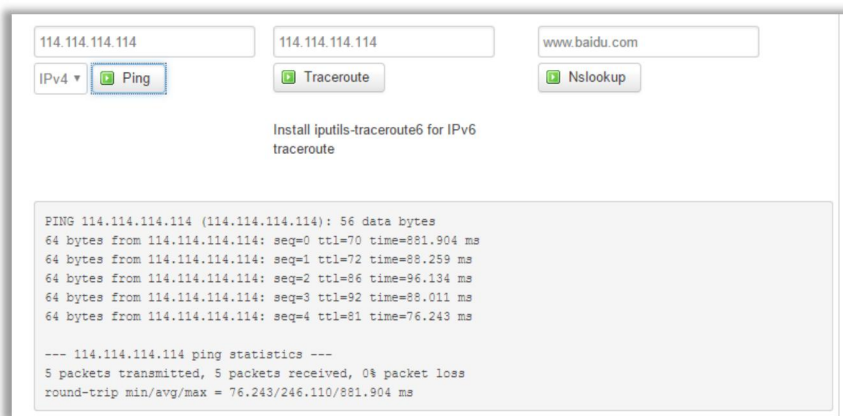
3.2.5、网络诊断

支持 ping/traceroute/dnslookup 这三种方式的网络诊断；

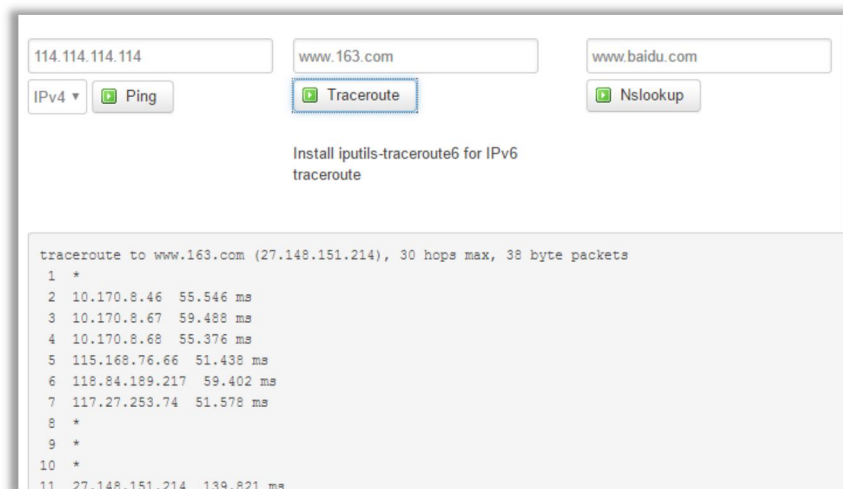
ping/traceroute 参数可以是一个域名，或者是一个 IP，是用来诊断网络是否在线。

Dnslookup 用来解析一个域名。

点击 ping，就可以诊断一个地址是否有响应，如下：

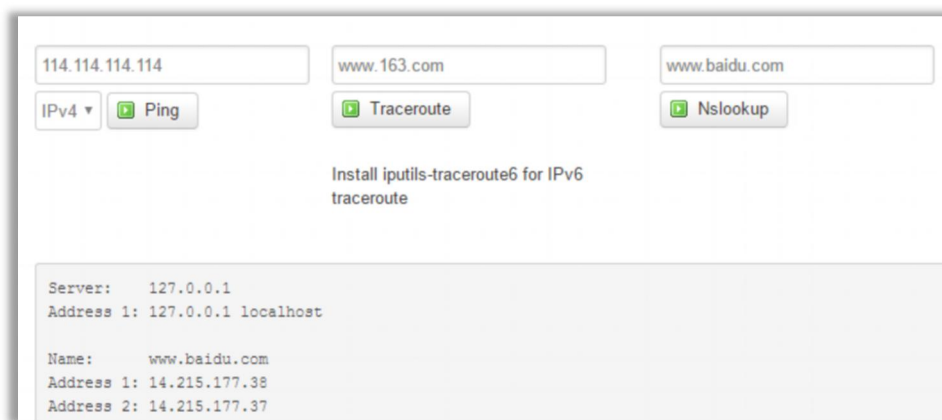


点击 traceroute





点击 nslookup:



3.3、安全

安全菜单主要是为了配置防火墙;目前所有从WAN口进来的TCP/UDP连接都会被过滤掉,但是从WAN口出去的包则会放过。如果需要对特定的IP,特定的端口放行的话,则需要配置子菜单项中的某一项。

3.3.1、DMZ 主机

DMZ 功能可以把WAN口地址映射成LAN端的某一台主机;所有到WAN地址的包都会被转到指定的LAN端主机。



DMZ: 选择开启的时候,启用DMZ功能

DMZ 主机: 指定要映射的LAN端某一台主机的IP地址





3.3.2、端口转发

相比 DMZ，端口转发是更精细化控制，可以把发往某一端口的数据包转发到 LAN 端的某一台主机，可以实现把不同的端口转到不同的主机



名字：指定这条规则的名字，可以起一个有意义的名字

协议：指定要转发的协议，可以是 TCP，UDP，或者 TCP/UDP

外部端口：端口转发前的目的端口

内部 IP 地址：要转发的主机 IP 地址

内部端口：端口转发后的目的端口，一般外部端口与内部端口是一样的，也可以不一样。

配置完后，点击“添加”按钮，新增一条转发规则。点击“保存&应用”按钮，使规则生效。





3.3.3、通信规则

通信规则可以用来打开一些设备端口，比如需要远程访问设备的配置页面，可以打开 80 端口，远程 ssh 连接， 可以打开 22 端口。

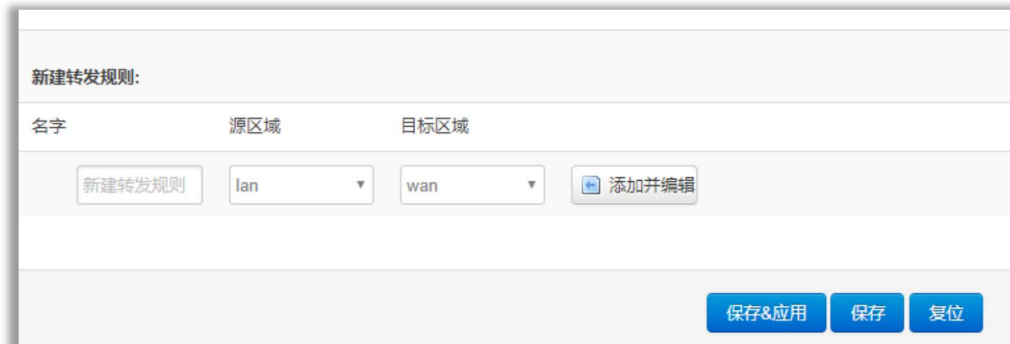


名字：指定这条规则的名字，可以起一个有意义的名字

协议：指定要转发的协议，可以是 TCP，UDP，或者 TCP/UDP

外部端口：指定设备要打开的端口号。

通信规则还可以用来新建一些访问控制规则，可以从 LAN 到 WAN，也可以从 LAN 到 LAN。



名字：指定这条规则的名字，可以起一个有意义的名字

源区域：指定数据包从哪里开始

目标区域：指定数据包要转到哪里。

点击“添加并编辑”按钮，可以看到更详细的匹配条件。



Rule is enabled ☒ 禁用

名字

限制地址 IPv4 和 IPv6

协议 TCP+UDP

匹配ICMP类型 any

源区域

☐ 任意区域

☒ lan: lan: 

☐ wan: wan: 

源MAC地址 所有

源地址 所有

源端口 所有

目标区域

☐ 设备 (输入)

☐ 任意区域 (转发)

☐ lan: lan: 

☒ wan: wan: 

目标地址 所有

目标端口 所有

动作 接受

附加参数 传递到iptables的额外参数。小心使用！

限制地址：可以指定限制 IPv4, IPv6, 或者 IPv4/IPv6 地址。

协议：指定要访问控制的协议，可以是 TCP, UDP, 或者 TCP/UDP

源 MAC 地址：指定数据包的源 MAC

源地址：指定数据包的源 IP

源端口：指定数据包的源端口

目标地址：指定数据包的目标 IP

目标端口：指定数据包的目标端口

动作：如果匹配上面的条件，执行相应的动作。

目前支持的动作有：

接受（允许数据包通过）



丢弃（丢掉数据包）

拒绝（丢掉数据包，并返回一个不可达数据包）

无动作（不做任何处理）

3.4、VPN

VPN 用来创建一条虚拟专用通道，在这条通道上，数据是加密的，以保证数据的安全传输。

可创建 VPN 的软件有 PPTP，L2TP，OpenVPN，IPSec。

PPTP/L2TP 是二层 VPN。OpenVPN 是基于 SSL VPN。IPSec 是三层 VPN。

PPTP/L2TP 使用相对方便，OpenVPN，IPSec 需要复杂的证书管理，所以会比较难用，但是提供更安全的数据加密。

3.4.1、PPTP

PPTP 可配置为客户端或者服务端，注意要么服务端生效，要么客户端生效，否会引起一些不可预测的问题`

PPTP 客户端：点击“开启”，则启用 PPTP 客户端功能



PPTP设置
设置PPTP

PPTP客户端 ☒ 启用 ☐ 禁用

服务器地址

用户名

密码

对端子网 eg: 192.168.10.0

对端子网掩码 eg: 255.255.255.0

NAT ☒

启用MPPE加密 ☒

启用静态IP地址 ☐

默认网关 ☐ ☒ 所有流量会通过VPN上网

服务器地址：指定 PPTP 服务端的地址，可以是 IP 地址，也可以是域名

用户名：服务器提供的用户名

密码：服务器提供的密码





对端子网：对端的子网，比如 PPTP 服务端的 LAN 端是 192.168.2.1 那么对端子网就是 192.168.2.0

对端子网掩码：子网的掩码，一般是 255.255.255.0

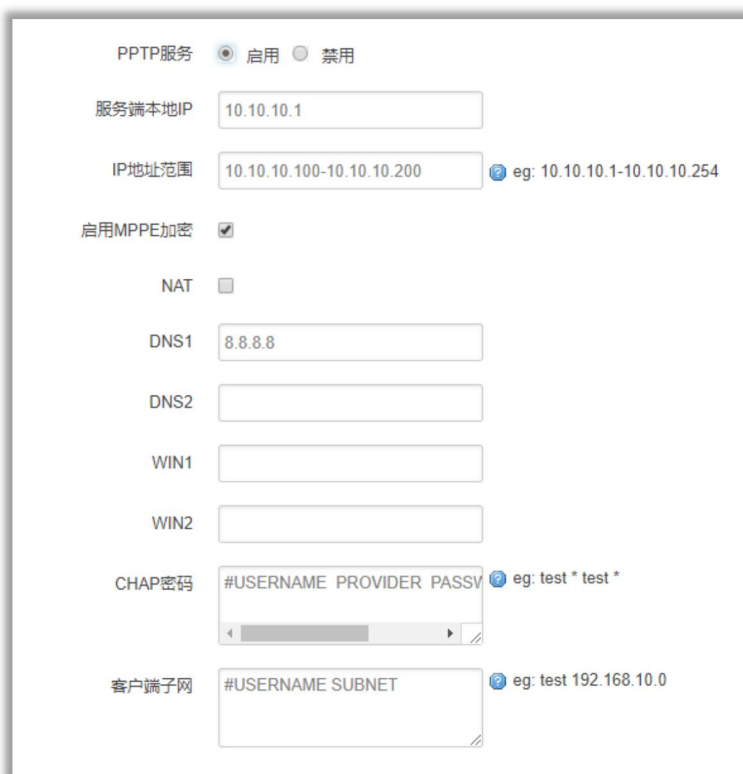
NAT：所以从 ppp0 接口出去的包，包的源 IP 都会替换成 ppp0 的 IP

启用 MPPE 加密：打勾选择 MPPE 加密

启用静态 IP 地址：可以设置 VPN 的静态 IP

默认网关：打勾，则会以 ppp0 创建一条默认路由，所有的数据都会走这条路由

PPTP 服务：点击开启，启用 PPTP 服务端功能



The image shows a configuration interface for PPTP service. It includes fields for 'PPTP服务' (PPTP Service) with radio buttons for '启用' (Enable) and '禁用' (Disable). Below are input fields for '服务端本地IP' (Server Local IP) set to '10.10.10.1', 'IP地址范围' (IP Address Range) set to '10.10.10.100-10.10.10.200' with an example 'eg: 10.10.10.1-10.10.10.254', '启用MPPE加密' (Enable MPPE Encryption) checked, 'NAT' unchecked, 'DNS1' set to '8.8.8.8', 'DNS2' empty, 'WIN1' empty, 'WIN2' empty, 'CHAP密码' (CHAP Password) with a placeholder '#USERNAME PROVIDER PASSW' and example 'eg: test * test *', and '客户端子网' (Client Subnet) with a placeholder '#USERNAME SUBNET' and example 'eg: test 192.168.10.0'.

服务端本地 IP：指定服务端的 IP 地址

IP 地址范围：指定要分配的 IP 地址范围

启用 MPPE 加密：打勾选择 MPPE 加密

DNS1/DNS2：指定要分配的 DNS 地址

WIN1/WIN2：指定 WIN 的地址

CHAP 密码：用来创建客户账号，一条记录对应一个用户。

格式如下：





用户名<空格> * <空格> 密码<空格> *,

比如增加一个账号: test 密码: test,

则这条记录如: test * test *

3.4.2、L2TP

L2TP 可配置为客户端或者服务端, 注意要么服务端生效, 要么客户端生效, 否会引起一些不可预测的问题

L2TP 客户端: 点击“开启”, 则启用 L2TP 客户端功能

L2TP设置

设置L2TP

L2TP客户端

☒ 启用
☐ 禁用

服务器地址

119.28.134.146

用户名

zhancx01

密码

使用IPsec

☒

预共享密钥

对端ID

对端子网

eg: 192.168.10.0

对端子网掩码

eg: 255.255.255.0

NAT

☒

启用MPPE加密

☒

MTU

1350

600~1450

启用静态IP地址

☐

默认网关

☐

所有流量会通过VPN上网

启用Ping

☐

Ping失败重连

服务器地址: 指定 PPTP 服务端的地址, 可以是 IP 地址, 也可以是域名

用户名: 服务器提供的用户名





密码：服务器提供的密码

使用 Ipsec：勾选使用密钥

预共享密钥：服务器提供的密钥

对端子网：对端的子网，比如 L2TP 服务端的 LAN 端是 192.168.2.1 那么对端子网就是 192.168.2.0

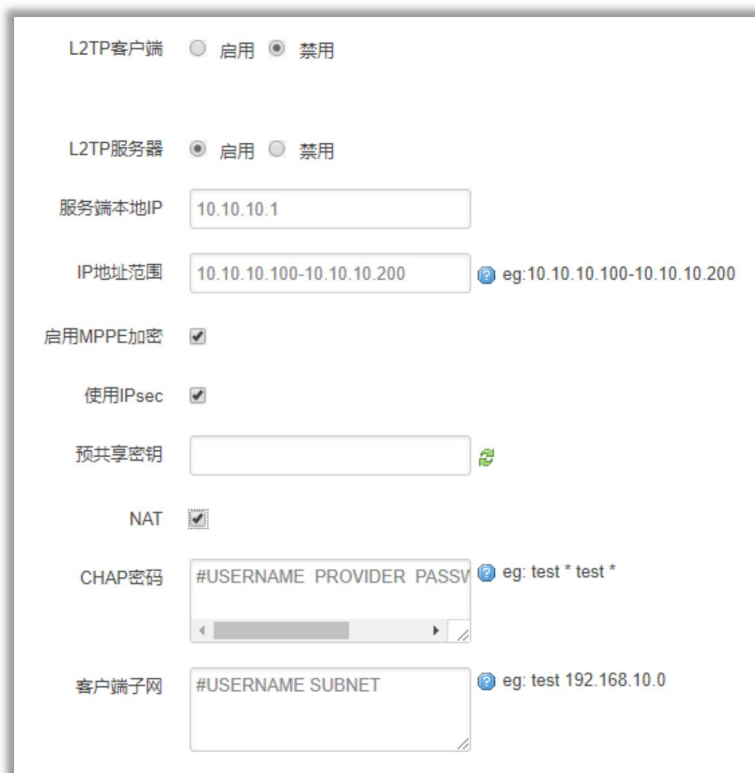
对端子网掩码：子网的掩码，一般是 255.255.255.0

NAT：所以从 ppp0 接口出去的包，包的源 IP 都会替换成 ppp0 的 IP

启用 MPPE 加密：打勾选择 MPPE 加密

默认网关：打勾，则会以 ppp0 创建一条默认路由，所有的数据都会走这条路由

L2TP 服务器：点击开启，启用 L2TP 服务端功能



L2TP客户端 ☐ 启用 ☒ 禁用

L2TP服务器 ☒ 启用 ☐ 禁用

服务端本地IP

IP地址范围 eg: 10.10.10.100-10.10.10.200

启用MPPE加密 ☒

使用IPsec ☒

预共享密钥

NAT ☒

CHAP密码 eg: test * test *

客户端子网 eg: test 192.168.10.0

服务端本地 IP：指定服务端的 IP 地址

IP 地址范围：指定要分配的 IP 地址范围

启用 MPPE 加密：打勾选择 MPPE 加密

使用 Ipsec：设置密钥

CHAP 密码：用来创建客户账号，一条记录对应一个用户。



格式如下：

用户名<空格> * <空格> 密码<空格> *，

比如增加一个账号：test，密码：test，

则这条记录如：test * test *

3.4.3、OpenVPN



OpenVPN ☒ 开启 ☐ 禁用

拓扑

角色

协议

端口

设备类型

OpenVPN服务端

认证类型

CA 未选择任何文件

公开证书 未选择任何文件

私钥 未选择任何文件

DH 未选择任何文件

对端子网地址

对端子网掩码

启用NAT ☐

启用LZO压缩

加密算法

MTU

OpenVPN：点击“开启”开始 OpenVPN 服务

拓扑：指定 OpenVPN 组网的拓扑结构，可以是点到点，也可以是子网

点对点：两个设备之间建立一条隧道

子网：多个设备连到一个服务器



角色：当拓扑结构是子网的时候，需要指定设备的角色是客户端还是服务端

协议：指定连接是基于 UDP，还是 TCP，默认是 UDP

端口：指定 OpenVPN 使用哪一端口连接，默认端口是 1194

设备类型：设备的类型有 tun，tap，tun 是在三层数据封装，tap 是二层数据封装

OpenVPN 服务端：你角色是客户端的时候，需要指定服务端的地址，可以是 IP，或是域名

认证类型：拓扑结构是子网，认证方式为证书，是点对点，可以无密码，证书或者静态密码

TLS Role：当认证类型是证书认证，需要指定 TLS 的角色是客户端还是服务端

3.4.4、IPSec

在 IPSEC 页面，会显示当前设备具有的 IPSEC 连接及其状态。



The screenshot shows the IPsec configuration interface. At the top, there is a toggle for 'IPSec' with '开启' (Enable) selected and '禁用' (Disable) unselected. Below this are several configuration fields:

- 对端地址 (Peer Address): %any
- 协商方法 (Negotiation Method): 主模式 (Main Mode)
- 隧道类型 (Tunnel Type): 子网到子网 (Subnet to Subnet)
- 本地子网 (Local Subnet): 192.168.4.0/24
- 对端子网 (Peer Subnet): 192.168.5.0/24
- IKE加密算法 (IKE Encryption Algorithm): AES-128
- IKE校验算法 (IKE Hash Algorithm): SHA-1
- Diffie-Hellman组 (Diffie-Hellman Group): Group14(2048bits)
- IKE生存时间 (IKE Lifetime): 28800
- 认证类型 (Authentication Type): 预置密钥 (Pre-shared Key)
- 预置密钥 (Pre-shared Key): 123456abc

Below these fields, there are two more sections for additional configuration:

- 本地识别码 (Local ID): [Empty field]
- 对端识别码 (Peer ID): [Empty field]
- ESP加密算法 (ESP Encryption Algorithm): AES-128
- ESP校验算法 (ESP Hash Algorithm): SHA-1
- DPD超时 (DPD Timeout): 60s
- DPD检测周期 (DPD Detection Cycle): 150
- DPD Action (DPD Action): 重启 (Restart)

对端地址：对端的 IP 地址或域名。如果采用了服务端功能，则该选项不可填；

协商方法：可选择“主模式”和“积极模式”





隧道类型: 可选择“子网到子网”、“子网到主机”、“主机到子网”、“主机到主机”等

本端子网: 本地子网及子网掩码, 例如: 192.168.10.0/24;

对端子网: 对端子网及子网掩码, 例如: 192.168.20.0/24;

IKE 加密算法: IKE 阶段的加密方式;

IKE 生存时间: 设置 IKE 的生命周期;

本端识别码: 通道本端标识, 可以为 IP 及域名;

对端识别码: 通道对端标识, 可以为 IP 及域名。

ESP 加密: ESP 的加密方式;

3.5、高级

高级菜单中包含了一些高级功能, 一般是不常用的功能。

3.5.1、静态路由

静态路由用来添加路由表项

接口	目标	IPv4-子网掩码	IPv4-网关	跃点数	
主机IP或网络 如果对象是一个网络					
lan		255.255.255.255		0	删除

接口: 指定要在哪一个接口增加路由

目标: 可以是主机 IP, 也可以是子网

IPv4 子网掩码: 目标的子网掩码, 如果目标是主机, 子网掩码应该是 255.255.255.255

IPv4 网关: 下一跳网关地址, 注意, 这个地址应该是可达的, 否则会添加失败

3.5.2、花生壳

花生壳这个功能实现了内网 IP 与域名绑定的功能。

服务提供商:	花生壳
状态:	在线
SN:	TOPS4890fc48bc30e8cc
登录管理 重置	





点击“登陆管理”，开始配置

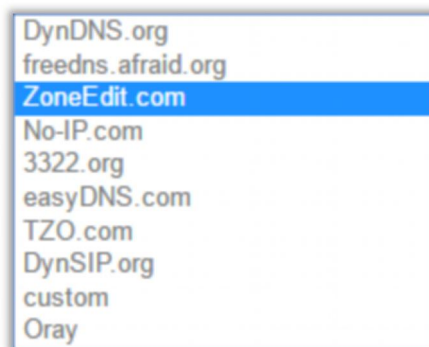
点击“重置”会清空以前的配置

3.5.3、动态 DNS

动态 DNS 用来绑定 WAN 口的公网 IP 跟一个域名。不管 WAN 口的 IP 怎么变，域名总会跟 WAN 口 IP 一一对应。



服务类型：目前支持的动态 DNS 有以下几中类型



用户名：你在服务提供商注册的用户名

用户密码：你在服务提供商注册时设定的密码

主机名：要绑定的域名

3.6、数据采集

Modbus 采集，212 协议上报





3.6.1、采集配置

时间设置

实时数据间隔
秒

分钟数据间隔
分钟

实时数据间隔：212 报文实时数据的上报时间

分钟数据间隔：212 报文分钟数据的上报时间

通讯口配置

COM2 (RS232)
COM3 (RS232)
COM4 (RS232/485)
COM5 (RS485)
COM6 (RS485)
COM7 (TTL)

启用
☒ 启用
☐ 禁用

波特率

数据位

停止位

奇偶校验

波特率：目前支持的波特率有：

4800
9600
19200
38400
57600
115200
230400

默认是 115200

数据位：数据位有 8 位，7 位两个选择，默认是 8 位

停止位：停止位有 2 位，1 位两个选择，默认是 1 位

奇偶校验：校验有无校验，奇校验，偶校验，默认是无校验

流控制：流控制有无控制，硬件控制，软件控制三种选择，默认是无控制



启用Modbus0 ☒

设备名

设备ID 1~255

功能码 1~255

寄存器地址 0~65535

寄存器个数 1~255

数据类型 16Bits AB 1~255

运算符 无 +,-,*,/

运算数

变量名 多个变量以分号连接

小数点个数 0 0~6

设备名： 可用来备注当前的设备名称，可为空

设备 ID： 设备的从设备地址

功能码： 如 03 （读保持寄存器）

寄存器地址： 数据存储的首地址

寄存器长度： 读取数据的长度，单位字节

目前支持的寄存器数据类型有：

- 16Bits AB
- 16Bits BA
- 32Bits ABCD
- 32Bits CDAB
- 32Bits DCBA
- Float ABCD
- Float CDAB
- Float DCBA

运算符： 对数据进行加减乘除，默认不操作

运算数： 与操作符配合使用

变量名： 数据前面的变量名称，用于区分数据

小数点个数： 数据的小数点个数，默认为整数



3.6.2、服务端配置

服务端配置

服务端1配置

服务端2配置

服务端3配置

服务端4配置

服务端5配置

启用 ☒ 启用 ☐ 禁用

协议

HJ212

服务器地址

192.168.1.10

服务器端口

9001

MN

201903140000000000000001

ST

31

2字节长

密码

123456

6字节长

连接状态

已连接

协议（HJ212）：是由国家环保行业制定的数据传输标准协议

服务器地址：指定连接服务端的地址

服务器端口：服务端开启的端口

MN：MN 号根据对应的不同设备下发该设备的 MN 号(必填)

ST：ST 设备和服务端一致(必填)

密码：6 字节长的密码(必填)

3.7、管理

管理菜单主要是用来管理设备，配置一些与管理相关的参数。

3.7.1、系统

系统设置用来系统的主机名，时区，是否允许 telnet，ssh 连接等参数。






主机名: router

时区: (GMT+08:00)北京,重庆,香港,马尼拉

语言: 中文

开启telnet访问: ☒ 开启 ☐ 禁用

开启SSH访问: ☐ 开启 ☒ 禁用

主机名: 指定设备的主机名，默认是 router

时区: 配置系统的时区，默认是 GMT8

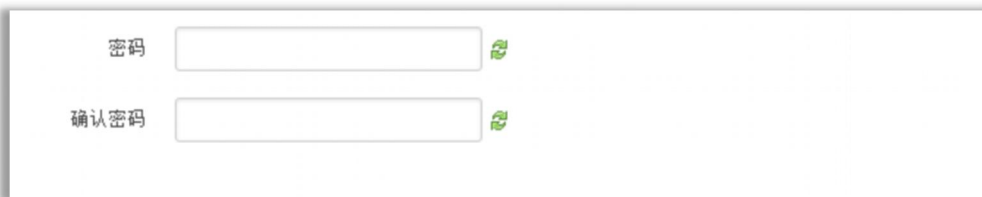
语言: 指定配置界面的语言，默认是中文

开启 telnet 访问: 点击 “开启”，启用 telnet 服务端，默认是开启

开启 SSH 访问: 点击 “开启”，启用 SSH 服务端，默认是禁用

3.7.2、密码

主要用来修改设备的密码



密码:

确认密码:

密码: 指定你要修改的密码

确认密码: 确认你要修改的密码

如果密码与确认密码不一致，则修改密码会失败。

如果一致，则修改成功，页面会重新跳到登陆页面，让你重新输入用户名与密码

3.7.3、日志设置

日志设置主要用来配置系统的日志输出参数。





输出到设备	/var/log/
日志大小	64 KB
日志服务器	0.0.0.0
日志服务器端口	514
输出级别	调试

输出到设备： 指定日志要输出到哪里，可以输出到串口，也可以输出到用户指定的文件路径，如果有外接存储设备，还可以存储到外接设备，默认路径：/var/log/

日志大小： 指定日志文件的大小，默认是 64KB

日志服务器： 指定日志服务器的 IP 地址

日志服务器端口： 指定日志服务器的端口，默认是 514

输出级别： 目前支持的输出级别有“调试”，“信息”，“注意”，“警告”，“错误”，级别依次递增，级别越高，输出的日志越少

3.7.4、备份与恢复

用户可以备份设备的当前配置，也可以恢复到出厂设置。

备份/恢复当前系统配置文件或重置OpenWrt(仅squashfs固件有效)。	
下载备份:	生成备份
恢复到出厂设置:	执行复位

下载备份： 点击“生成备份”，会生成一个“backup-router-2016-**-**.tar.gz”配置文件

恢复到出厂设置： 点击“执行复位”，会弹出一个“确认放弃所有修改”的确认框，点击“确定”开始恢复出厂设置。

恢复完出厂设置后，也可以把保存的配置导入到设备，恢复到以前的配置。

上传备份存档以恢复配置。	
恢复配置:	选择文件 未选择任何文件 上传备份...

恢复配置： 点击“选择文件”，选择你的备份配置文件，点击上传备份。会弹出一个“真的





要恢复”的确认框，选择“确定”，开始恢复系统配置。

3.7.5、固件升级

升级设备之前，务必确认下要升级的固件，是针对你手上的设备。



固件文件：点击“选择文件”，选择你的固件文件。点击”刷写固件”，会上传固件文件到设备。



校验值：固件的 MD5 检测值

大小：固件文件的大小

点击“执行”，开始固件升级

3.7.6、远程配置

在这个菜单项中可以指定远程服务器的地址与端口，本设备的设备号等信息。



远程配置

远程配置 ☒ 启用 ☐ 禁用

服务器地址

服务器端口

心跳包间隔

设备号

连接状态 CONNECTING Login Server

远程管理：选择“开启”，启用远程管理，选择“禁用”，禁用远程管理

服务器地址：指定登陆服务器的地址，可以是 IP 地址，也可以是一个域名

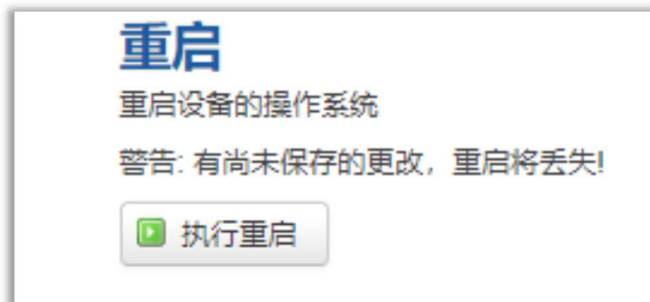
服务器端口：指定登陆服务器的端口

心跳包间隔：指定发送心跳包的时间间隔，单位是秒

设备号：指定设备的设备 ID

3.7.7、手动重启

这个菜单项主要用来重启设备。



点击“执行重启”，会弹出一个“真的要重启的确认框”，选择“确定”开始重启

3.7.8、定时重启

定时重启

启用定时重启 ☒ 启用 ☐ 禁用

定时类型 ☒ 按周期 ☐ 按时间

周期间隔 分，最小5分钟

保存&应用
保存
复位

定时重启有两种方式

- 1、周期重启，设置 5 分钟，每 5 分钟就会重启一次。
2. 时间重启：在特定的时间重启，可以设置周一至周天的其中一天，也可以每天。

定时重启

启用定时重启 ☒ 启用 ☐ 禁用

定时类型 ☐ 按周期 ☒ 按时间

小时

分钟

星期

保存&应用
保存
复位



Tel: 0592-6211770

Web: www.top-iot.com

Mail: service@top-iot.com

Add: 厦门市集美区软件园三期 A1 栋 15 层

