R105 工业路由器

用户手册

版本：1.2

版本记录：

编号	软件版本	说明	日期
V1.0	V200R003	首次发布	2023 年 1 月 2 日
V1.1	V200R003	1. 根据页面布局变更，删除防火墙区域相关描述； 2. 添加白名单和黑名单说明。	2023 年 4 月 4 日
V1.2	V200R004	1. 更新**概览**页面说明； 2. 删除快速联网说明； 3. 更新自动路由章节； 4. 修改 4G/LTE 页面描述； 5. 增加网络诊断功能说明； 6. 增加 IPSec 设置说明	2023 年 7 月 11 日

目录

前言

感谢购买 R105 工业路由器（“路由器”或“产品”）。本手册旨在就产品的设置、操作及维护提供必要的指导和帮助。请仔细阅读本手册，并确保您在使用产品前已理解产品的结构和功能。

目标用户

本手册旨在提供给：

- 网络架构师
- 网络管理员
- 技术支持工程师
- 其他用户

版权说明

免责声明

尽管已对本手册包含的所有信息进行了仔细检查，以确保其技术细节和印刷的准确性，但万创对本手册的任何错误或特性，或由于本手册或软件的不当使用造成的后果不承担任何责任。

产品额定功率或者特性发生变化时，或者发生重大结构变更时，我们会更换配件编号。产品规格如有变更，我们或不会另行通知。

技术支持与帮助

如您遇到本手册未曾提及的情况，请联系您的销售代表了解相关解决方案。请在来函中附上以下信息：

- 产品名称和订单编号；
- 关于相关问题的描述；
- 收到的报错信息，如有。

美国：Vantron Technology, Inc.
地址：440 Boulder Court, Suite 300 Pleasanton, CA 94566
电话：916-202-7042
邮箱: sales@vantrontech.com

中国：成都万创科技股份有限公司
地址：四川省成都市武侯区武科东三路9号1号楼6楼 610045
电话：86-28-8512-3930/3931, 86-28-8515-7572/6320
邮箱：sales@vantrontech.com.cn

法规信息

产品符合：

- FCC 第 15B 部分
- IC
- PTCRB

请查阅**附录**的合规声明

符号约定

本手册使用以下符号，提醒用户注意相关信息。

⚠	提醒可能会造成潜在的系统损坏或人员伤害。
▷	提示重要信息或法规。

一般安全说明

产品应当由合格熟练的技术人员按照当地及/或国际电气规范和法规进行安装。为保证人身安全并防止产品及其所连接设备发生损坏，请于产品安装和运行前，仔细阅读并遵守以下安全说明。请保留本手册，以供将来查阅。

- 请勿拆卸或以其他方式改装产品。此类行为可能造成发热、起火或人身伤害等其他损害，且导致产品保修失效。
- 保持产品远离加热器、散热器、发动机机壳等热源。
- 请勿将任何物品塞入产品，否则可能导致产品故障或烧坏。
- 为确保产品正常运行，防止产品过热，请勿阻挡产品通风口。
- 请使用提供或推荐的安装工具并遵守安装说明。
- 作业工具的使用或放置应当遵守此类工具的实施规程，避免产品短路。
- 检查产品前，请切断电源，避免出现人身伤害或产品损坏。

电缆和配件安全说明

⚠ 仅使用满足条件的电源。确保使用符合手册规定范围的供电电压。产品使用 9-36V 直流电源供电。上电前，请确认产品接入了直流电。

⚠ 请确保合理放置电缆，避免受到挤压。

⚠ 仅使用授权的天线。未经授权的天线可能产生无效或过量的射频传输功率，从而违反联邦通信委员会规定的限度。

⚠ 清洁说明：

- 清洁前请关闭产品电源
- 请勿使用喷雾清洁剂
- 使用湿布进行清洁
- 除非使用除尘器，否则请勿清洁裸露的电子组件

⚠ 出现以下故障时，请关闭电源并联系万创技术支持工程师：

- 产品损坏
- 温度过高
- 根据手册检修后，故障仍然无法解决

⚠ 请勿在易燃易爆环境中使用：

- 远离易燃易爆环境
- 远离通电电路
- 未经授权，不得拆开产品外壳
- 拔掉电源之前，请勿更换零件
- 某些情况下，拔掉电源后，产品仍有余电。因此，更换零件前，必须停止充电并等待产品完成放电。

第 1 章 硬件说明

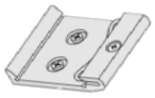
1.1 产品概述

万创 R105 工业路由器提供各种通信连接方式，集双卡 4G、Wi-Fi、有线网络及虚拟专用网络等功能于一体，满足工业物联网领域不同组网需求。产品支持全网通中高速率 CAT 4 蜂窝网络，同时配备 5 个网口，其中一个 LAN 口提供 PoE 选配功能，支持最大 30W 供电。R105 不仅支持 Wi-Fi IEEE 802.11 b/g/n/ac 标准，还支持选配 IEEE 802.11ax (Wi-Fi 6), 满足用户更高的通讯要求。

R105 工业路由器支持多通道故障切换，保障网络访问的安全和稳定。BlueSphere GWM 作为万创路由器和网关集中管理云平台门户，可以为用户提供 R105 远程配置和管理解决方案。R105 非常适用于工业自动化、智能家居、智慧城市等领域。

1.2 开箱

本产品包装细致，质量严格把关。但是，若您发现任何损坏或遗失，请立即联系您的销售代表。

标准配件		可选配件	
	1 x R105 路由器		1 x 12V 电源适配器和电源线
	2 x Wi-Fi 天线		1 x 电源转接线
	1 x 4G LTE 天线（胶棒）		1 x 4G LTE 天线（吸盘）
	1 x 导轨安装支架（已安装到设备上）	/	/

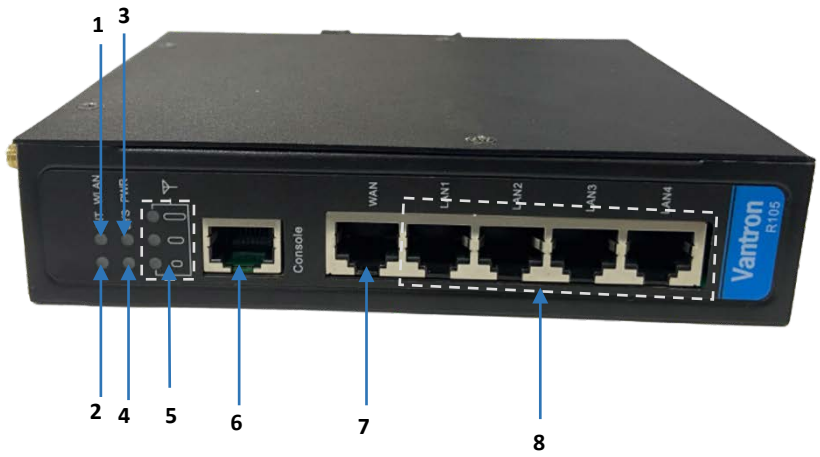
以上配件取决于用户的选配规格，实际情况可能略有不同。

1.3 规格

R105			
通信	以太网	5 x RJ45, 10/100/1000Mbps (1 x WAN & 4 x LAN, 可选 PoE, 30W 输出)	
	Wi-Fi	2.4GHz & 5GHz, IEEE 802.11 b/g/n/ac, AP & Client 可选: Wi-Fi 6, IEEE 802.11 b/g/n/ac/ax	
	4G LTE	1 x Mini PCIe 连接蜂窝模块 (CAT 4，支持全网通)	
	WAN 协议	PPP、DHCP	
输入/输出	Console	1 x Console 接口，用于本地配置	
	串口	1 x RS485，带隔离	1 x RS232，带隔离
	SIM 卡槽	2 x SIM 卡槽	
	天线 (SMA 接头)	1 x LTE 天线	2 x Wi-Fi 天线
	接地方式	设备机壳接地 & PCB 板接地	
	电源接入	1 x 3.81mm 凤凰端子	
系统控制	复位键	1 x 针孔式复位键	
	LED 指示灯	3 x 蜂窝信号强度指示灯 1 x 电源指示灯 1 x 系统指示灯	1 x 网络指示灯 1 x WLAN 指示灯
机械	尺寸	150mm x 120mm x 35mm	
	壳体	钣金	
	安装方式	面板安装/导轨安装/壁挂安装	
	IP 防护等级	IP30	
	跌落测试	6 英尺	
	散热方式	无风扇散热	
电源	输入	9-36V DC，支持过流保护、防接反保护	
软件	操作系统	VantronOS	
	网络管理	SNMP v2c/v3	
	联网协议	IPV4, HTTPS, TCP & UPD, NTP client and server, ARP, TLS	
	VLAN	支持	
	设备管理平台	万创 BlueSphere GWM	
	链路在线检测	发送心跳包检测，断线自动连接	
	设备日志	可检索	
	网络可靠性	多通道故障切换，支持有线、Wi-Fi、4G 通讯互为备份	
	双卡切换	支持双卡链路互为备份，自动切换	
	IP 应用	Ping、Traceroute、DHCP Server/Client、DDNS	
	IP 路由	静态路由、动态路由	
	网络地址转换	支持	
安全	防火墙	支持状态防火墙	
	访问控制列表	MAC 地址、IP 地址	
	数据安全	PPTP、L2TP、GRE、IPSec、OpenVPN	
	Wi-Fi 安全	64/128 位 WEP、TKIP、WPA、WPA2、WPA3、AES、WPS	
环境条件	温度	工作温度：-20℃~+60℃	存储温度：-40℃~+70℃
	湿度	存储湿度：相对湿度 5%-95%（无凝露）	
	认证	FCC、IC、PTCRB	

1.4 接口定义

1.4.1 前视图



指示灯/接口	说明
1	Wi-Fi 状态指示灯
2	网络连接指示灯
3	电源指示灯
4	系统状态指示灯
5	4G LTE 信号强度指示灯
6	Console 接口，用于设备调试（波特率：57600）
7	WAN 口，在 VantronOS 中为 **eth0.2**，默认在 WAN 区工作
8	4 x LAN 口，在 VantronOS 中为 **eth0.1**，默认在 LAN 区工作

LED 指示灯说明

1. Wi-Fi 状态指示灯

Wi-Fi 状态	说明
Wi-Fi 模块开启	指示灯绿色长亮
存在 Wi-Fi 通信	指示灯闪烁
Wi-Fi 模块关闭	指示灯熄灭

2. 网络连接指示灯

路由器网络连接情况	说明
路由器所有线路均无法连接到互联网	指示灯熄灭
路由器任意线路连接到互联网	指示灯以 1 秒的间隔闪烁

3. 电源指示灯

路由器接通电源后，电源指示灯长亮。

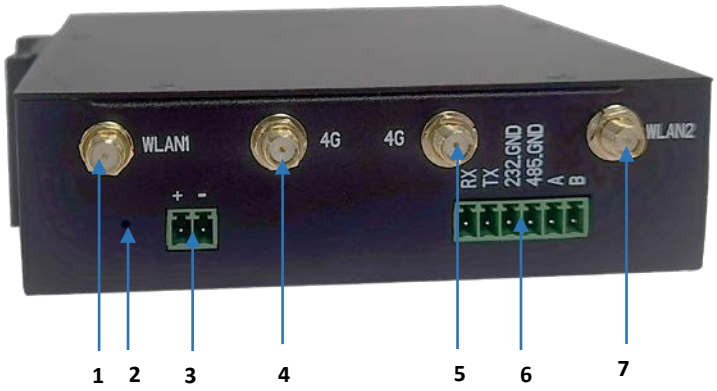
4. 系统指示灯

系统动作	说明
系统启动过程中	指示灯熄灭
系统正常运转	指示灯以 1 秒的间隔闪烁
系统重启、升级或恢复出厂设置	指示灯以 0.3 秒的间隔快速闪烁

5. 4G LTE 信号强度指示灯

信号强度	说明
>67%	三个指示灯绿色常亮
38% 至 67%	下方两个指示灯绿色常亮
<38%	底部指示灯闪烁

1.4.2 左视图



接口	说明
1	Wi-Fi 天线接头 1
2	针孔复位键
3	电源端子 (9V-36V DC)
4	4G LTE 从天线接头
5	4G LTE 主天线接头
6	RS232 & RS485 串口
7	Wi-Fi 天线接头 2

复位键说明

1. 短按该键 0~2 秒，可以重启路由器。
2. 长按该键 3~6 秒，可以将路由器恢复出厂设置。
3. 长按该键 6~10 秒，可以将路由器恢复出厂设置并清除所有用户数据。

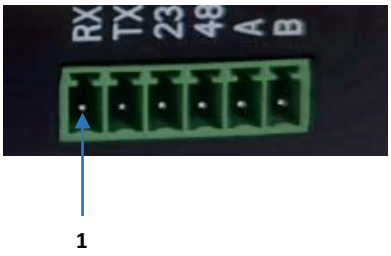
1.4.3 右视图

接口	说明
1	Micro SIM 卡槽 1
2	Micro SIM 卡槽 2
3	接地螺丝

1.4.4 后视图

接口	说明
1	DIN 导轨支架

1.5 串口说明



1

绿色端子包含一个 RS232 串口和一个 RS485 串口，其引脚定义如下：

编号	信号	设备名称	接口	类型	说明
1	RX	/dev/ttyS1	COM1	I	RS232 接收信号
2	TX			O	RS232 发送信号
3	232. GND			NC	RS232 隔离接地
4	485. GND	/dev/ttyS2	COM2	NC	RS485 隔离接地
5	A			I/O	RS485 A 信号
6	B			I/O	RS485 B 信号

RS232 串口连接：RX-TX, TX-RX, GND-GND

RS485 串口连接：A-A, B-B, GND-GND

使用串口通信程序（如 microcom）输入以下命令打开串口设备：

COM1:

```
~# microcom /dev/ttyS1 -s 115200
```

COM2:

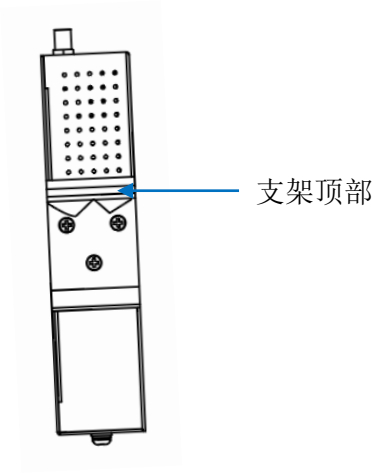
```
~# microcom /dev/ttyS2 -s 115200
```

第 2 章 快速开始

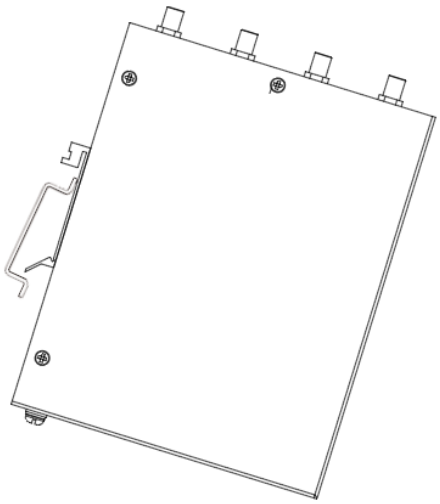
2.1 设置路由器

配置路由器前，需执行以下步骤完成产品硬件连接。

1. 竖直方向握住路由器；

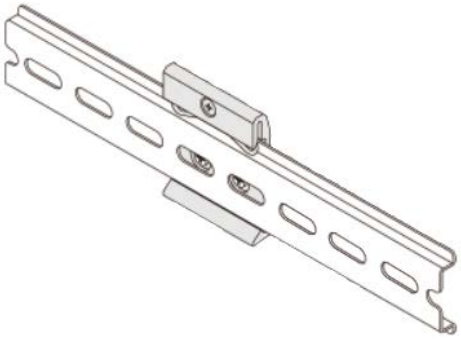


2. 将路由器倾斜放置在 DIN 导轨上；
3. 将 DIN 导轨一侧对准安装支架顶部的卡扣，放置于三角形固定件后侧；

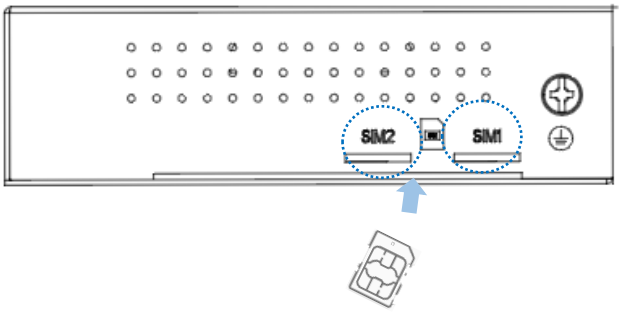


4. 向下推动路由器，压缩支架；

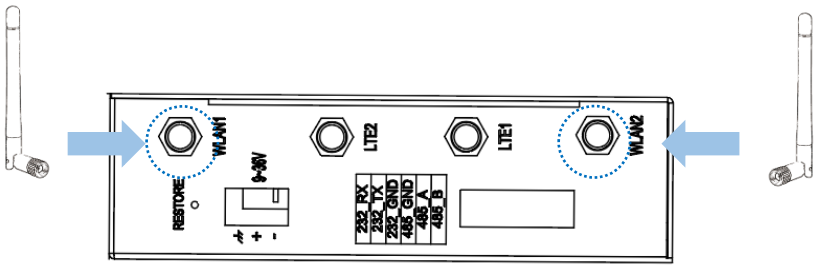
5. 待支架下部有足够空间卡入导轨另一侧时松开路由器；



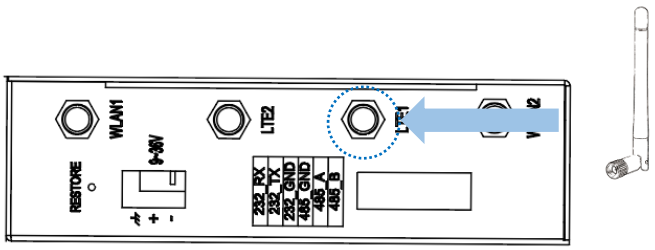
6. 轻轻晃动路由器，确保已将其固定在导轨上；
7. 金属芯片朝上，将已激活的 Micro SIM 卡插入任意一个 SIM 卡槽，保持 SIM 卡剪切边朝内；



8. 向内推动 Micro SIM 卡，使其固定；
9. 将 Wi-Fi 天线（胶棒）安装到 WLAN 天线接头；

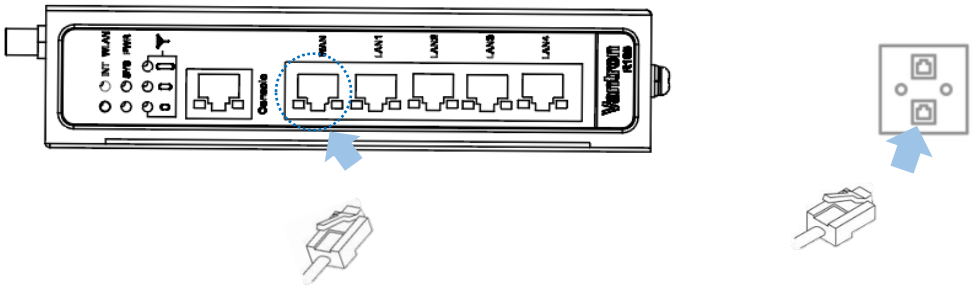


10. 将 LTE 天线（胶棒/吸盘）安装到 LTE 天线接头；



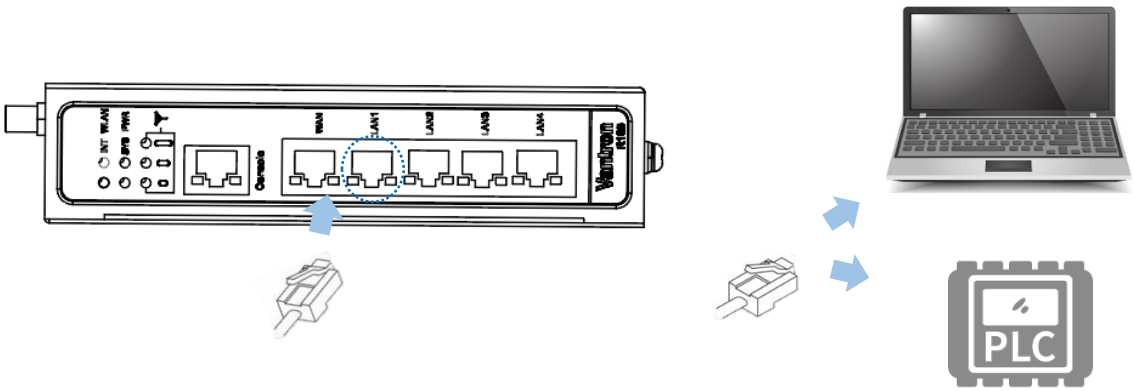
11. 紧固天线接头，将天线固定在合适的位置；

12. 取一条网线，将网线的一端连接到路由器 WAN 口，另一端连接至外网接口；

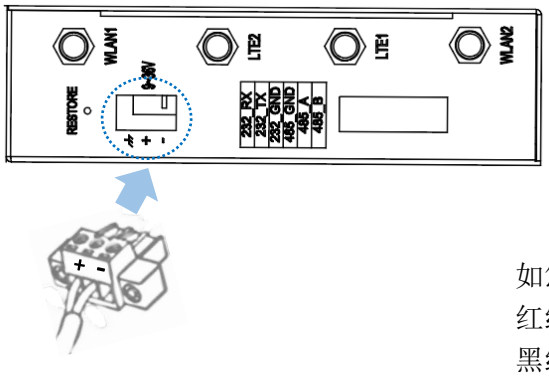


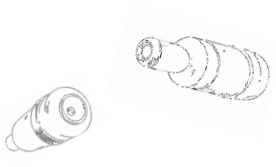
如果选择无线网络连接，则跳过此步。

13. 另取一条网线，将网线的一端连接至路由器 LAN 口，另一端根据当前的用途，连接至主控电脑或客户端设备；



14. 将电源转接线的端子头插入路由器的电源端子座，另一端与电源线连接；





如您使用万创提供的电源转接线：
红线: 电源 (+)
黑线: 接地 (-)

15. 将适配器插入符合路由器工作电压要求（9V-36V）的直流电源插座，使路由器通电；

16. 接通电源后，电源指示灯将变为绿色常亮。

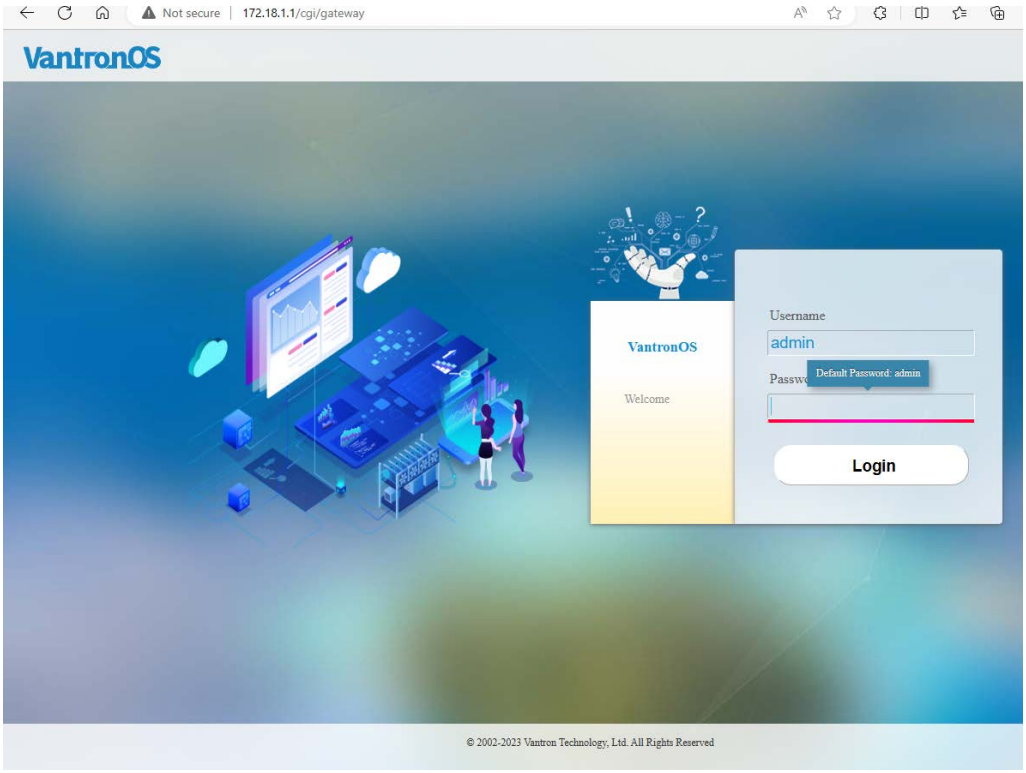
实际提供的天线可能与图示不同。如您在安装天线的过程中遇到问题，请联系销售代表解决。

2.2 登录 VantronOS 系统

此路由器设计为通过最简单的配置即可实现网络连接。即便如此，用户也可以通过 VantronOS 界面更改路由器的网络设置，进行个性化配置。

1. 在浏览器中输入路由器 LAN 口的 IP 地址登录 VantronOS 网页界面（默认地址：http://172.18.1.1/）.

   - 默认用户名：**admin** / 超级用户：**root**
   - 默认密码：**admin** / 超级用户密码：**rootpassword**



2. 如需 SSH 登录，使用 LAN 口 IP 地址（默认地址：http://172.18.1.1/）。

   - 端口： **22**
   - 账号：**root**
   - 密码：**rootpassword**

网页登录地址与路由器 LAN 口的 IP 地址一致，因此，如果用户重置了此 IP 地址，则需要更改登录地址。

SSH 登录默认禁用，请参考 3.13.3 了解具体设置步骤。

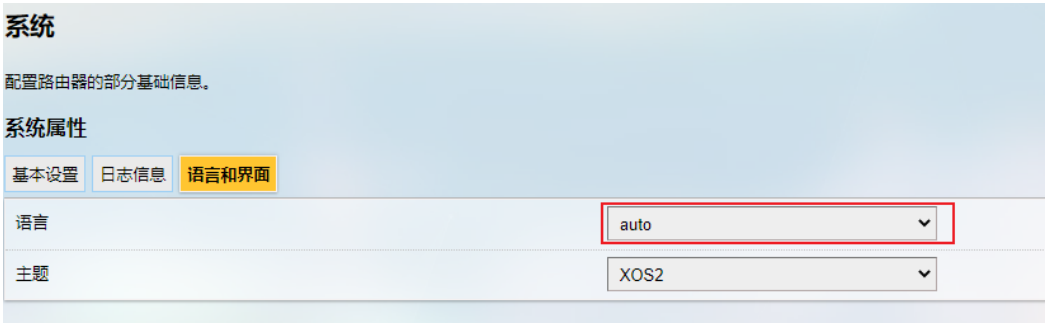
2.3 修改密码

登录 VantronOS 之后，用户可以自行决定是否更改登录密码。如需更改密码，请执行以下步骤。

1. 导航至**系统 > 管理权**;
2. 输入当前用户的原始密码；
3. 输入新的密码并确认改密码；
4. 保存设置并应用；
5. 系统将自动退出登录；
6. 使用新密码登录即可。

2.4 修改语言

目前，系统支持中文和英语，系统语言默认自动跟随浏览器语言。用户可以导航至**系统 > 系统 > 语言和界面**，手动更新系统语言。



Auto: 系统语言跟随浏览器语言（默认）

English：英文界面

简体中文：中文界面

2.5 连接万创网关管理平台

BlueSphere GWM (“GWM”) 是万创网关管理云平台，可帮助企业无缝配置、监控和管理万创的网关、路由器和 DTU 等物联网通信设备。利用 BlueSphere GWM，企业可以简化设备的设置过程，确保设备状况实时可见，并轻松管理设备配置，有助于提高运营效率、提高企业决策。

如需使用 BlueSphere GWM 网关管理平台实现设备远程管理，请确保设备符合以下条件：

- 已获得 BlueSphere GWM 登录许可
- 设备上已安装用于对接 BlueSphere GWM 的 DMP agent
- DMP agent 配置页面为“启用”状态（配置说明请参考 3.10.4 DMP Agent）
- 已将设备的序列号添加至 BlueSphere GWM

第 3 章 VantronOS 页面配置路由器

3.1 VantronOS 简介

VantronOS 是万创团队共同协作，在 Linux 系统的基础上，利用嵌入式硬件，实现系统和功能独立自主开发的智能操作系统。系统采用模块化和插件扩展的设计理念，使用 Linux 内核配合防火墙功能，保障设备连接安全，不受攻击。

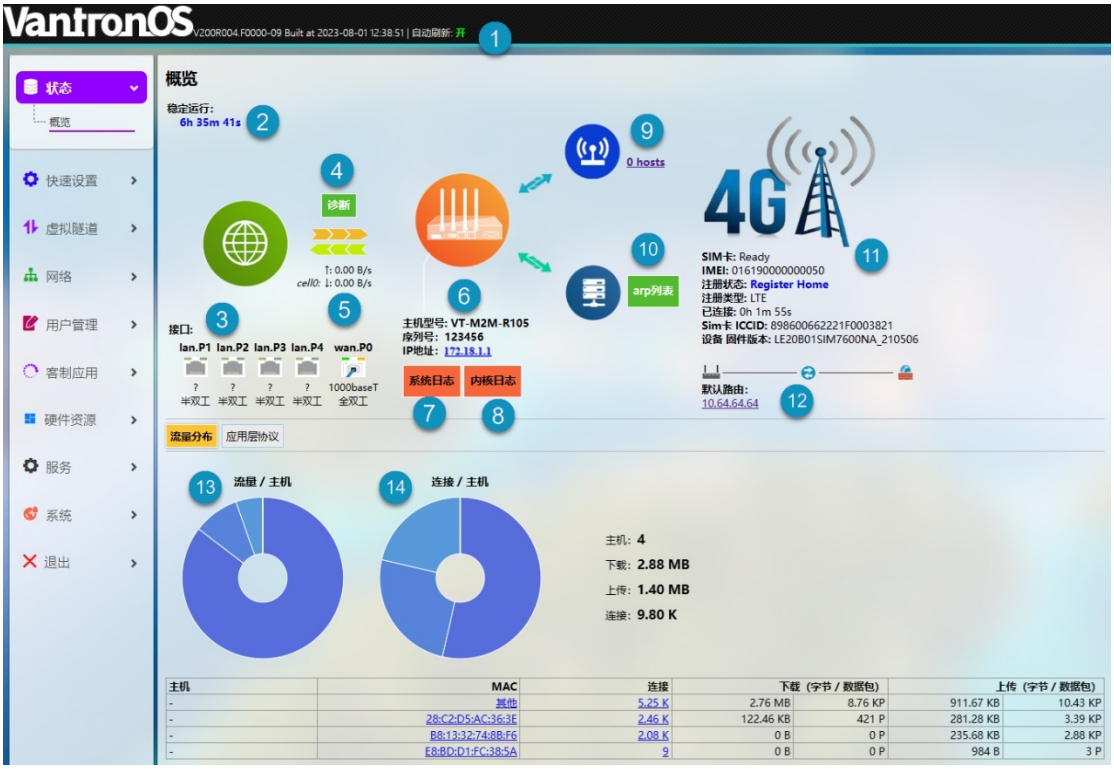
基于 MVC 框架开发的 UI 界面支持简单高效的设置入口。VantronOS 可以与万创自主研发的 BlueSphere GWM 管理平台、Azure、阿里云、华为云、树根云等云系统对接，实现云端对工业物联设备的监控、操作和诊断，以及用户与工业物联网设备之间的互联互动，提高了设备管理的整体效率和便利程度。

后文中，如您发现使用“admin”账号登录 VantronOS 界面后，未出现描述的功能或特性，请切换至“root”账号。

退出前，确保保存所有设置和变更，使之生效。

3.2 状态

状态页面呈现了路由器的整体信息，包括稳定运行时间、通过无线或有线连接接入路由器的设备数量、默认路由、硬件信息、流量统计信息等。



编号说明

1. 固件版本和自动刷新打开/关闭（可以点击切换模式）
2. 联网后路由器的稳定运行时间
3. 当前网口的工作状态

   （本例中，WAN 口已连接）

4. 网络诊断工具集 （详情请查看 3.7）
5. 即时默认出口流量
6. 当前所使用路由器的型号、序列号、网关管理地址
7. 系统日志信息
8. 内核日志信息
9. 通过 Wi-Fi 接入的子设备数量

点击该数字即可进入 Wi-Fi 设置。

10. 通过有线网络端口连接到路由器的设备信息

IPv4 地址	MAC 地址
172.18.1.174	18:c0:4d:43:ad:8b

11. 路由器接入口详情

根据路由器通信模块的不同，图示会有所不同。

12. 路由器当前使用的默认路由
13. 接入的子设备按 MAC 地址统计的流量分布信息

点击页面底部表格中的每一个 MAC 地址将得到子设备的详细流量信息。

14. 应用层协议

HTTPS、HTTP、QUIC 是数据下载和上传的前三大协议。
HTTPS、HTTP、DNS 是设备连接的前三大协议。

3.3 快速联网— 自动线路

自动线路用于保证当前设备在多链路场景下，可以正常访问网络。它实现了网络自动链路探测以及线路切换与恢复功能。

默认的线路探测以及数据转发优先级规则为：有线线路 > Wi-Fi > LTE > 其它线路。

编号说明

1. 启用/禁用路由跟踪
2. 自动线路运行模式（见后文）
3. 自动线路探测策略（见后文）
4. 指定接口启用/禁用探测功能

   截图中，wan 指有线连接，cell0 指蜂窝数据连接，wwan0 指 Wi-Fi 连接。
5. 启用/禁用探测网关功能
6. 探测自定义 IP 地址
7. 编辑特定网口的自动线路规则（见后文）
8. 接口连接状态
9. 接口探测日志和服务运行日志

自动线路运行模式

模式	说明
静态模式 （默认）	1. 接口按照用户指定的网络接口优先级调度； 2. 如果用户没有指定优先级，则以默认的优先级规则为准。
动态模式	1. 整个路由策略由默认的优先级规则接管； 2. 用户指定的链路优先级规则被禁用。 如果路由器上安装了依赖于指定的线路优先级的特殊应用，则不建议使用此模式。

自动线路探测策略

策略	说明
探测自定义 IP 地址 （默认）	1. 用户可以为特定的网络接口设置 IP 地址。如果该地址可以接收和发送数据，则该接口为活跃接口，被设置为“在线”状态； 2. 如果路由器所在位置无法连接到外网，请将探测策略修改为“探测网关”或者添加一些路由器可以探测到的 IP 地址。
探测网关	此策略在于识别当前网络的网关 IP 地址。 P2P/PPP 连接场景不建议使用探测网关策略，这种情况下，可以探测公网 IP 地址（比如 8.8.8.8）。

注意：

1. 请根据设备网络位置以及接口所使用的入网协议，选择适当的探测策略。
2. 如果同时选择了“探测自定义 IP 地址”和“探测网关”的策略，“探测网关”策略优先。
3. 如果选择了“探测自定义 IP 地址”却没有提供任何 IP 地址，系统将自动切换到探测网关。
4. 请参考下页路由规则的编辑说明，了解更多详细信息。

点击**修改**按钮，进入如下规则修改页面。

编号说明

1. 启用/禁用该接口的路由跟踪
2. 网关跃点设置（数值越小，优先级越高）
3. 探测超时的情况下总共发送的探测报文数（默认为 3）
4. 单次跟踪的超时时间（默认为 5 秒）
5. 跟踪间隔，为一次跟踪完成至下一次跟踪开始之间的时间（默认为 10 秒）
6. 启用/禁用网关探测
7. 选择 IP 探测的默认 IP 地址（‘工厂默认值’）或者自定义 IP 地址（‘自定义’）
8. 保存 & 应用上述设置
9. 回到自动线路页面

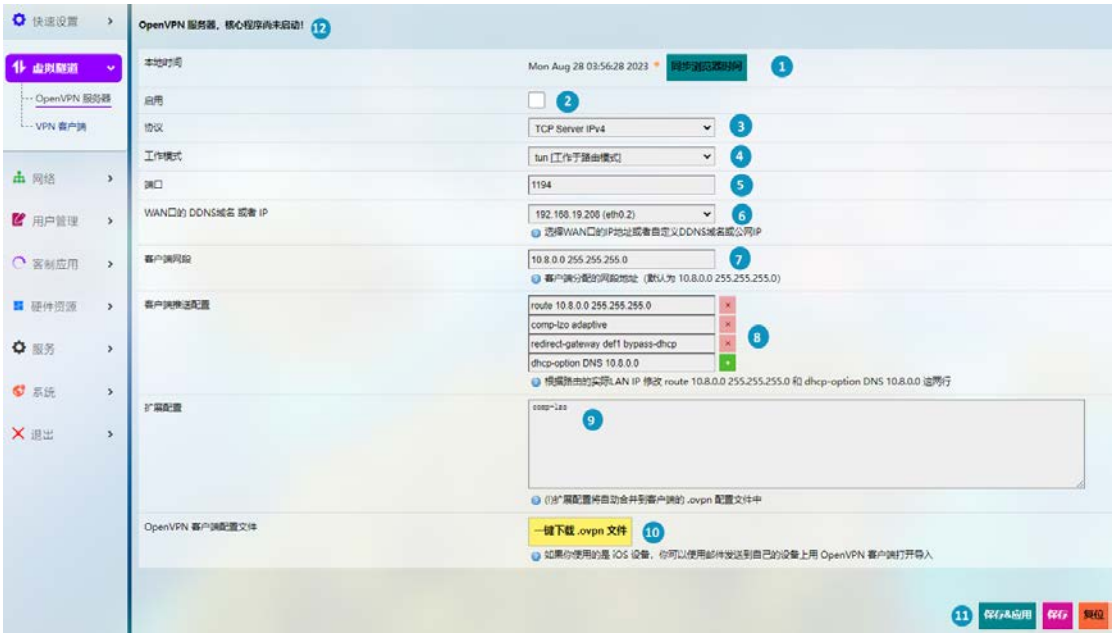
3.4 虚拟隧道

互联网用户可以通过虚拟专用网络（VPN）远程安全访问网络。路由器支持 PPTP、L2TP、GRE、IPSec、OpenVPN 等 VPN 协议，保证数据隐私且不受干扰。

用户可以根据需要，将路由器配置为 OpenVPN 服务器或者 OpenVPN 客户端。

3.4.1 OpenVPN 服务器

此页面提供基于 SSL 连接和传输的虚拟专用网络线路，配置简单灵活。OpenVPN 服务器的基本和高级设置均可以在此页面完成。



按照以下步骤搭建 OpenVPN 服务器：

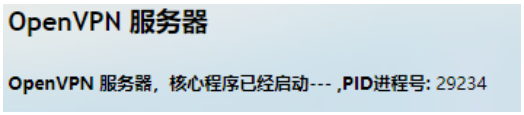
1. 同步网关时间与浏览器（本地）时间；
2. 创建后是否启用服务器；
3. 选择协议（默认选择 TCP）；

TCP 提供从用户到服务器的有序数据传递（反之亦然），UDP 不专门用于端到端的通信，也不检查接收端的准备情况。

4. 选择 **tap** 或 **tun** 工作模式（默认选择 tun）；

> ***Tap*** *可以桥接不同位置的两个以太网段，所以如果您需要连接到远程网络（远程桌面、PLC、控制器等），就使用* ***tap****。如果你只需要网络连接，那么就使用* ***tun****。*

5. 配置服务器监听的**端口号**；
6. 从下拉菜单中选择服务器监听的 WAN 口 IP 或 DDNS 域名或公网 IP；
7. 配置为客户端分配的虚拟**网段**；
8. 设置推送给客户端的基础配置（tap 工作模式下不适用）；
9. 输入向客户端推送的**扩展配置**；
10. 下载**服务器配置文件**用于客户端连接（设置服务器时，无需下载配置文件）；
11. 保存并应用上述设置；
12. 配置完成后，运行状态将如下图所示。



用户可以在**高级选项**页面设置权鉴方式、证书权鉴选项，并且更新系统证书。

运行日志显示服务器设置后的详细信息。

3.4.2 VPN 客户端

如需将路由器用作客户端，连接某个 VPN 服务器，请导航至 **虚拟隧道 > VPN 客户端**进行设置。

编号说明

1. 同步 VPN 时间与浏览器（本地）时间
2. 选择虚拟线路的出口协议（**OPENVPN** 和 **PPTP 两种协议可选**）
3. 点击按钮切换至该协议
4. 勾选或取消勾选以启用或禁用该协议

只有启用协议时，才会展示后面的相关选项。展示的选项与所选的 VPN 协议相关。

5. 如果选择 OpenVPN 协议，则需要上传.ovpn 文件完成配置

如果选择 PPTP 协议，则需要填写 PPTP 服务器地址、账号和密码。

6. 选择本地.ovpn 文件进行配置
7. 上传配置文件
8. 选择使用证书还是用户名及密码的方式作为鉴权方式

权鉴模式自动更新，请保留默认设置。

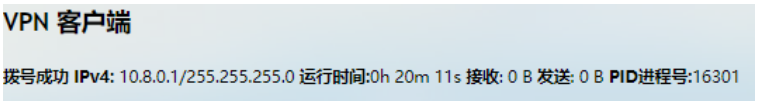
9. MTU 设置
10. 跃点数设置（1 至 255 之间）

跃点数值越小，优先级越高。

11. 禁用/启用对端/心跳检测

*选择**自定义**并输入心跳检测的 IP 地址，可启动该机制。*

12. 输入自定义的 DNS 服务器
13. **保存 & 应用**上述设置
14. 设置完成后 VPN 客户端的状态



3.5 IPSec 连接

3.5.1 前提条件

- 一台 R105 工业路由器（简称‘G1’）
- 一台运行 VantronOS 且支持 IPSec 的网关/路由器（简称‘G2’）
- G1 和 G2 的权鉴证书：

1. 假设 G1 和 G2 的 IP 地址如下：

   G1— LAN IP：172.18.2.1，WAN IP：192.168.9.78

   G2— LAN IP：172.18.3.1，WAN IP：192.168.9.82

2. 两台设备的证书:

   G1—

   X509 根证书: rootca.cert

   X509 证书: 78.cert

   私钥: 78.priv.key

   公钥: 78.pub.key

   G2—

   X509 根证书: rootca.cert

   X509 证书: 82.cert

   私钥: 82.priv.key

   公钥: 82.pub.key

3.5.2 证书配置

- 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 证书管理**上传证书（如上传 G1 的证书）：

根据以下步骤上传证书：

1. 选择 X509 根证书；
2. 选择 X509 证书；
3. 选择私钥文件；
4. 选择公钥文件；
5. 点击**确认**上传 G1 的证书。

以上截图仅就如何上传 G1 的证书进行说明，请使用同样的方法上传 G2 的证书。

您可以使用页面底部的工具生成一对公钥和私钥，但此处生成的公钥和私钥只能用于公钥认证。

编号说明：

1. 输入秘钥名称
2. 点击**生成**按钮
3. 新生成的私钥
4. 新生成的公钥

3.5.3 密码配置

此配置仅适用于预共享秘钥（PSK）作为认证方式的情况。

- 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 密码管理配置**设置本地密码（以 G1 的配置为例）：

根据以下步骤设置本地密码：

1. 设置密码名称；
2. 从下拉菜单选择**启用**，开启密码；
3. 选择 PSK 预共享秘钥作为密码类型；
4. 输入 PSK ID: 192.168.9.78 (G1 的 WAN IP);
5. 输入密码；
6. 点击**确认**保存密码。

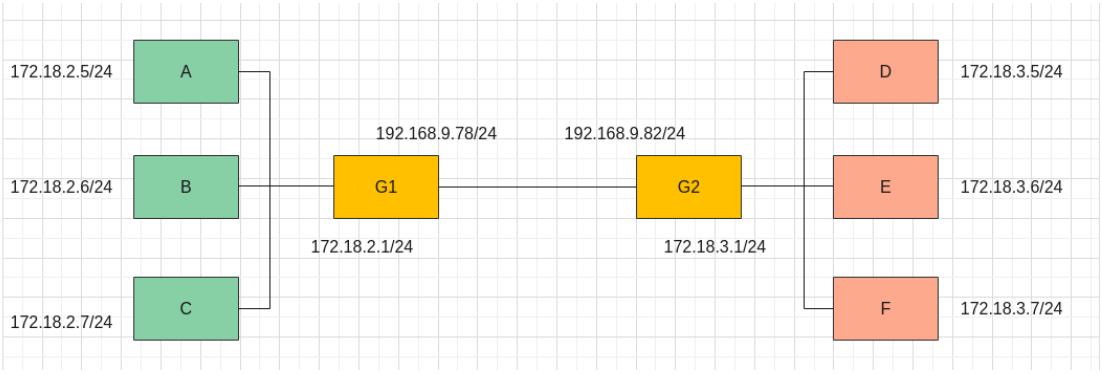
- 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 密码管理配置**设置远端密码（以 G1 的配置为例）：

根据以下步骤设置远端密码：

1. 设置密码名称；
2. 从下拉菜单选择**启用**，开启密码；
3. 选择 PSK 预共享秘钥作为密码类型；
4. 输入 PSK ID: 192.168.9.82 (G2 的 WAN IP);
5. 输入密码；
6. 点击**确认**保存密码。

注意：G1 的本地密码为 G2 的远端密码，而 G1 的远端密码为 G2 的本地密码。

3.5.4 IPSec 连接设置



上图场景介绍：

- 场景 1：主机到主机，G1 与 G2 建立 IPSec 连接，子网互不通
- 场景 2：现场到现场，G1 与 G2 建立 IPSEC 连接，子网互通
- 场景 3：远程访问（服务器），D 通过 IPSEC 连接到 G1，可以访问到 G1 的子网
- 场景 4：远程访问（客户端），A 通过 IPSEC 连接到 G2，可以访问到 G2 的子网

第一步：启用 IPSec

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IPSEC 配置**
2. 框选启用 IPSec 配置
3. 点击**确认**保存设置

加载设置后，IPSec 的运行状态将变更为“运行中”，如下图所示。

第二步：IKE 策略配置

场景 1 和场景 2 的配置：

设置 G1

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IKE 策略配置**
2. 设置策略名称
3. 从下拉菜单中选择**启用**，启用该策略
4. 输入本地地址：192.168.9.78
5. 输入对端地址：192.168.9.82
6. 点击**确认**，保存设置

设置 G2

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IKE 策略配置**
2. 设置策略名称
3. 从下拉菜单中选择**启用**，启用该策略
4. 输入本地地址：192.168.9.82
5. 输入对端地址：192.168.9.78
6. 点击**确认**，保存设置

场景 3 的配置（G1 和 G2 的配置互换即为场景 4 的配置）：

设置 G1

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IKE 策略配置**
2. 设置策略名称（to_82）
3. 从下拉菜单中选择**启用**，启用该策略
4. 输入本地地址：192.168.9.78
5. 输入对端地址：192.168.9.82
6. 点击**进阶设置**，展开高级设置页面
7. 点击**虚拟 IP 池**
8. 选择**作为连接响应端**作为 G1 的角色
9. 双击可选的‘to_82’，选中此 IP
10. 点击**确认**，保存设置

设置 G2

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IKE 策略配置**
2. 设置策略名称（to_78）
3. 从下拉菜单中选择**启用**，启用该策略
4. 输入本地地址：192.168.9.82
5. 输入对端地址：192.168.9.78
6. 点击**进阶设置**，展开高级设置页面
7. 点击**虚拟 IP 池**
8. 选择**作为连接发起端**作为 G2 的角色
9. 输入虚拟 IP（0.0.0.0）
10. 点击**确认**，保存设置

第三步：IPSec 策略配置

场景 1 的配置：

设置 G1

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IPSEC 策略**
2. 设置策略名称（to_82）
3. 从下拉菜单中选择**启用**，启用该策略
4. 选择**隧道**作为传输模式
5. 输入本地地址：192.168.9.78
6. 输入对端地址：192.168.9.82
7. 点击**确认**，保存设置

设置 G2

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IPSEC 策略**
2. 设置策略名称（to_78）
3. 从下拉菜单中选择**启用**，启用该策略
4. 选择**隧道**作为传输模式
5. 输入本地地址：192.168.9.82
6. 输入对端地址：192.168.9.78
7. 点击**确认**，保存设置

场景 2 的配置：

设置 G1

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IPSEC 策略**
2. 设置策略名称（to_82_site）
3. 从下拉菜单中选择**启用**，启用该策略
4. 选择**隧道**作为传输模式
5. 输入本地地址：172.18.2.1/24 (G1 的 LAN IP)
6. 输入对端地址：172.18.3.1/24 (G2 的 LAN IP)
7. 点击**确认**，保存设置

设置 G2

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IPSEC 策略**
2. 设置策略名称（to_78_site）
3. 从下拉菜单中选择**启用**，启用该策略
4. 选择**隧道**作为传输模式
5. 输入本地地址：172.18.3.1/24 (G2 的 LAN IP)
6. 输入对端地址：172.18.2.1/24 (G1 的 LAN IP)
7. 点击**确认**，保存设置

场景 3 的配置（G1 和 G2 的配置互换即为场景 4 的配置）：

设置 G1 虚拟 IP

编号说明：

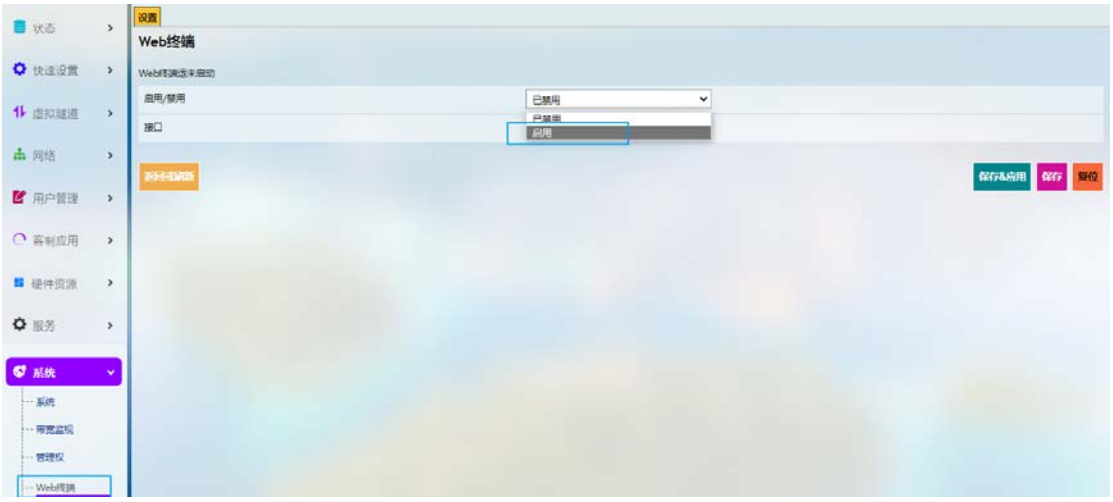
1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IPSEC 虚拟 IP 池配置**
2. 设置策略名称（to_82）
3. 从下拉菜单中选择**启用**，启用该策略
4. 输入虚拟地址：10.10.7.0/24
5. 点击**确认**，保存设置

设置 G1 IPSec 策略

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IPSEC 策略**
2. 设置策略名称（to_82_server）
3. 从下拉菜单中选择**启用**，启用该策略
4. 选择**隧道**作为传输模式
5. 输入本地地址：10.10.7.0/24
6. 点击**确认**，保存设置

导航至**系统 > Web 终端 > 设置**，启用系统终端。



登录 root 用户（默认密码：rootpassword），然后输入以下命令，将 IP 地址添加到 G1。

```
ip address add 10.10.7.2/24 dev eth0
```

设置 G2 IPSec 策略

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IPSEC 策略**
2. 设置策略名称（to_78_client）
3. 从下拉菜单中选择**启用**，启用该策略
4. 选择**隧道**作为传输模式
5. 输入对端地址：10.10.7.0/24
6. 点击**确认**，保存设置

第四步：认证管理

认证方式有三种：证书认证、PSK 预共享秘钥认证、公钥认证。从中选择一种即可。

证书认证

G1 本地认证设置

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 认证管理**
2. 设置认证名称（local_cert）
3. 该认证默认被启用
4. 证书认证为默认的认证方式
5. 双击可选的‘78.cert’，选中此证书
6. 点击**确认**，保存设置

G1 远端认证设置

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 认证管理**
2. 设置认证名称（remote_cert）
3. 该认证默认被启用
4. 证书认证为默认的认证方式
5. 双击可选的‘78.cert’，选中此证书
6. 点击**确认**，保存设置

G2 本地认证设置

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 认证管理**
2. 设置认证名称（local_cert）
3. 该认证默认被启用
4. **证书认证**为默认的认证方式
5. 双击可选的‘82.cert’，选中此证书
6. 点击**确认**，保存设置

G2 远端认证设置

编号说明：

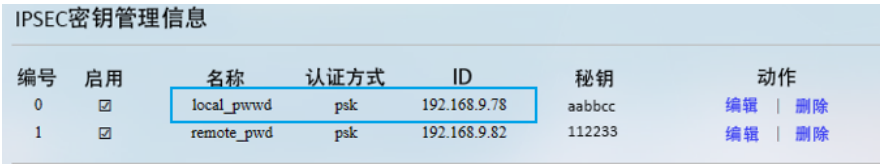
1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 认证管理**
2. 设置认证名称（remote_cert）
3. 该认证默认被启用
4. **证书认证**为默认的认证方式
5. 双击可选的‘82.cert’，选中此证书
6. 点击**确认**，保存设置

PSK 预共享秘钥认证

G1 本地认证设置

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 认证管理**
2. 设置认证名称（local_cert）
3. 该认证默认被启用
4. 输入**密码配置**步骤中所设置的相同的 ID（192.168.9.78）

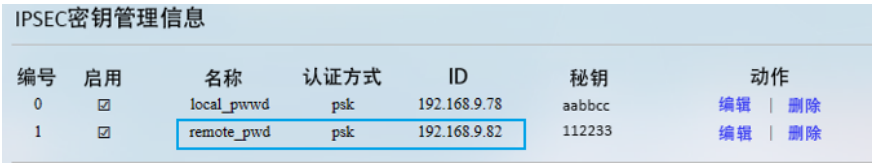


5. 从下拉菜单中选择 **PSK 预共享秘钥**作为认证方式
6. 点击**确认**，保存设置

G1 远端认证设置

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 认证管理**
2. 设置认证名称（remote_cert）
3. 该认证默认被启用
4. 输入**密码配置**步骤中所设置的相同的 ID（192.168.9.82）



5. 从下拉菜单中选择 **PSK 预共享秘钥**作为认证方式
6. 点击**确认**，保存设置

G2 本地认证设置

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 认证管理**
2. 设置认证名称（local_cert）
3. 该认证默认被启用
4. 输入**密码配置**步骤中所设置的相同的 ID（192.168.9.82）
5. 从下拉菜单中选择 **PSK 预共享秘钥**作为认证方式
6. 点击**确认**，保存设置

G2 远端认证设置

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 认证管理**
2. 设置认证名称（remote_cert）
3. 该认证默认被启用
4. 输入**密码配置**步骤中所设置的相同的 ID（192.168.9.78）
5. 从下拉菜单中选择 **PSK 预共享秘钥**作为认证方式
6. 点击**确认**，保存设置

公钥认证

公钥认证需将 G1 的公钥（78.pub.key）上传至 G2，将 G2 的公钥（82.pub.key）上传至 G1。

G1 本地认证设置

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 认证管理**
2. 设置认证名称（local_cert）
3. 该认证默认被启用
4. 从下拉菜单中选择**公钥**作为认证方式
5. 双击可选的‘78.pub.key’，选中此证书
6. 点击**确认**，保存设置

G1 远端认证设置

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 认证管理**
2. 设置认证名称（remote_cert）
3. 该认证默认被启用
4. 从下拉菜单中选择**公钥**作为认证方式
5. 双击可选的‘82.pub.key’，选中此证书
6. 点击**确认**，保存设置

G2 本地认证设置

编号说明：

7. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 认证管理**
8. 设置认证名称（local_cert）
9. 该认证默认被启用
10. 从下拉菜单中选择**公钥**作为认证方式
11. 双击可选的‘82.pub.key’，选中此证书
12. 点击**确认**，保存设置

G2 远端认证设置

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > 认证管理**
2. 设置认证名称（remote_cert）
3. 该认证默认被启用
4. 从下拉菜单中选择**公钥**作为认证方式
5. 双击可选的‘78.pub.key’，选中此证书
6. 点击**确认**，保存设置

第五步：IPSec 连接配置

设置 G1

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IPSEC 连接信息**
2. 设置连接名称（to_82）
3. 该认证默认被启用
4. 从下拉菜单中选择一个之前创建的 IKE 策略（本例中使用‘to_82’）
5. 双击之前创建的本地认证策略（本例中使用‘local_cert’），选定该策略
6. 双击之前创建的远端认证策略（本例中使用‘remote_cert’），选定该策略
7. 双击之前创建建的 IPSec 策略（本例中使用‘to_82’），选定该策略
8. 点击**确认**，保存设置

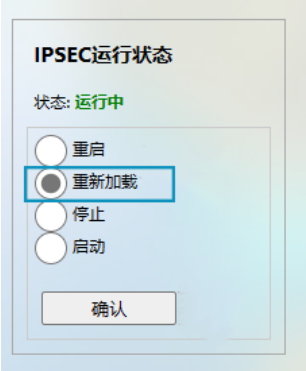
设置 G2

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 配置 > IPSEC 连接信息**
2. 设置连接名称（to_78）
3. 该认证默认被启用
4. 从下拉菜单中选择一个之前创建的 IKE 策略（本例中使用‘to_78’）
5. 双击之前创建的本地认证策略（本例中使用‘local_cert’），选定该策略
6. 双击之前创建的远端认证策略（本例中使用‘remote_cert’），选定该策略
7. 双击之前创建建的 IPSec 策略（本例中使用‘to_78’），选定该策略
8. 点击**确认**，保存设置

第六步：重新加载 IPSec 程序

点击**重新加载**前的按钮并**确认**，重新加载 IPSec 程序。



第七步： IPSec 连接

编号说明：

1. 导航至**虚拟隧道 > IPSEC > IPSEC 状态 > 连接列表**
2. 选择连接设置并点击**连接**

当所选连接添加到 IPSEC IKE SAS 后，即成功建立连接。

3.6 网络

用户可以在**网络**页面查看当前可访问的网络接口，并根据需要相应地编辑网络接口。

3.6.1 接口

当前可访问且可以配置的所有接口都在**网络 > 接口**页面显示。

编号说明

1. 接口总览
2. 接口流量详情
3. 手动重启接口
4. 编辑接口设置
5. 删除接口（仅在使用 root 账号登录时出现）
6. 接口即时流量
7. 添加新的接口（仅在使用 root 账号登录时出现）

由于某些接口是否展示取决于用户之前的配置以及设备上安装的通信模块，因此实际接口展示或与上图有所差异。

下文主要说明如何修改路由器的 LAN 口和 WAN 口设置。

3.6.1.1 LAN

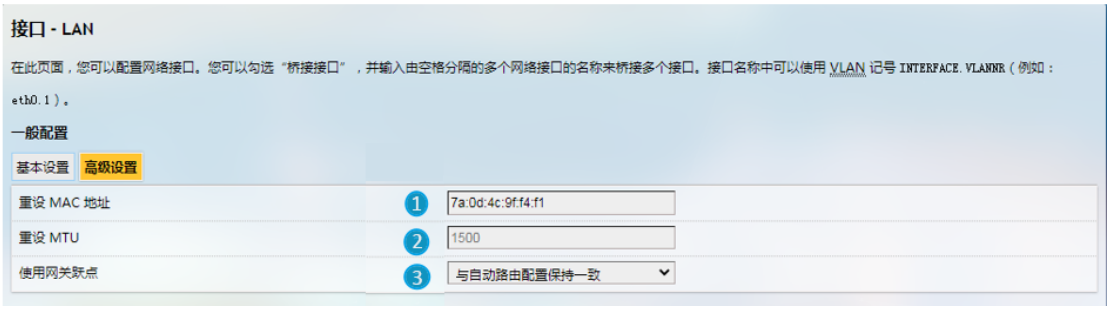
- **一般配置**

点击 **LAN** 口后面的**修改**按钮可进入该接口的配置页面，页面默认展示**基本设置**信息。

编号说明

1. 接口状态
2. 输入 LAN 口的 IP 地址
3. 选择 LAN 口子网掩码

在一般配置区域，选择**高级设置**可进一步编辑接口信息：



编号说明

1. MAC 地址克隆
2. 设置 MTU （保持默认设置）
3. 设置网关跃点

退出页面前，请保存设置。

如果以 root 用户登录 VantronOS，则**高级设置**按钮旁会有一个**物理设置**按钮，用于 LAN 口的桥接设置。

编号说明

1. 启用网桥接口
2. 启用 STP 协议
3. 选择桥接的接口

退出页面前，请保存设置。

- **DHCP 服务器**

在 DHCP 服务器的**基本设置**页面下，用户可以配置 LAN 口的 DHCP 服务：

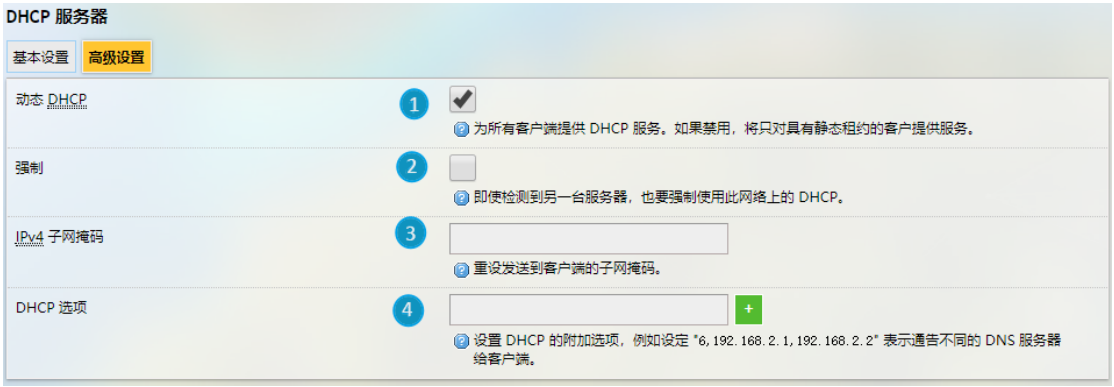
编号说明

1. 禁用 DHCP 服务

如果禁用LAN 口的DHCP 服务，则不会为连接至路由器的设备提供DHCP 服务。

2. DHCP 起始分配基址
3. 地址分配最大数量（最高可设置 150 个）
4. 租用地址的失效时间（最短 2 分钟）

DHCP 服务**高级设置**：



编号说明

1. 为所有客户端提供动态地址分配
2. 强制使用此网络上的 DHCP 服务（忽略其他服务器）
3. 重设发送到客户端的子网掩码

一般从接受服务的子网开始计算。

4. 为客户端添加不同的 DNS 服务器

*退出页面前，请保存设置。点击**返回或刷新**即返回网络接口的设置页面。*

3.6.1.2 WAN

- **DHCP 基本配置**

点击 **WAN** 口后面的**修改**按钮可进入该接口的配置页面，页面默认展示**基本设置**信息。

编号说明

1. WAN 口状态
2. 选择 DHCP 客户端作为 WAN 口协议
3. 请求 DHCP 时发送的主机名

退出页面前，请保存设置。

- **DHCP 高级设置**

如果选择 DHCP 客户端协议，如前述步骤所述完成基本的配置后，用户还可以进行高级设置。

编号说明

1. 勾选此选项后，路由器启动时即开启该接口
2. 勾选此选项后，链路更换不会触发 hotplug 事件处理
3. 启用**使用默认网关**
4. 启用**使用对端通告的 DNS 服务器**

如果此选项禁用，则需要指定 DNS 服务器。

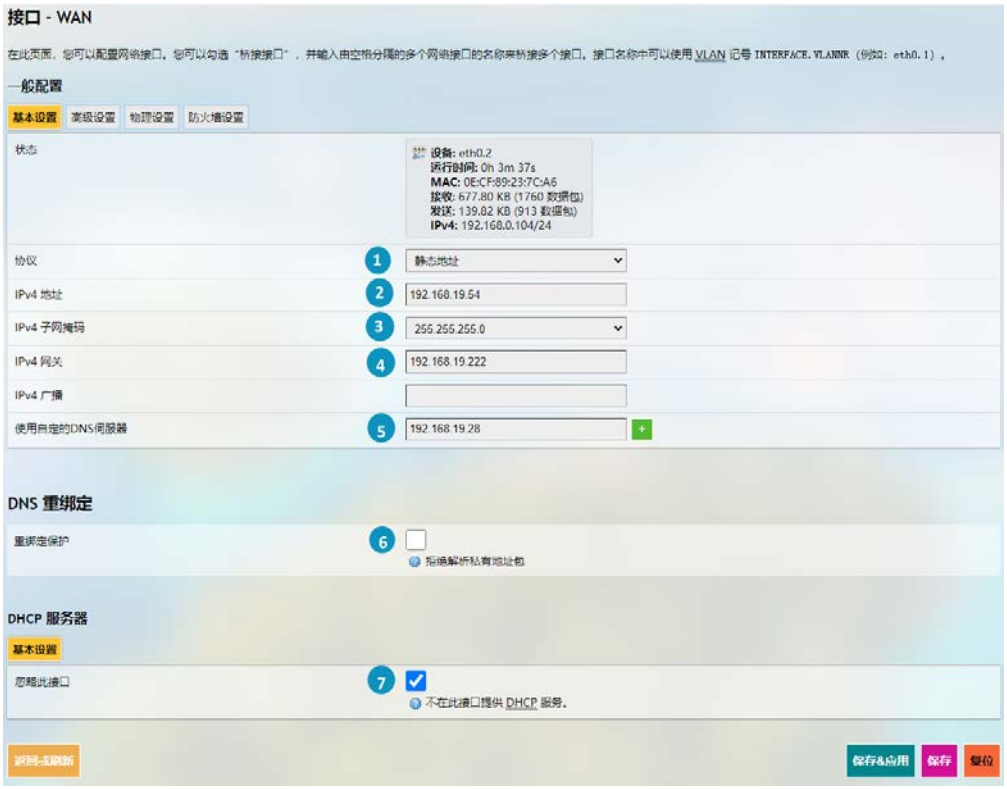
5. 设置网关跃点
6. MAC 地址克隆
7. 设置网络 MTU

退出页面前，请保存设置。

- **静态地址基本设置**

如需启用静态地址协议，在 WAN 口**基本设置**的协议下拉列表中选择**静态地址**，并点击**切换协议**按钮。

点击**切换协议**后，需要输入 IPv4 地址、子网掩码、IPv4 网关，以及 IPv4 广播。



编号说明

1. 当前协议
2. 输入 IPv4 地址
3. 输入 IPv4 子网掩码
4. 输入 IPv4 网关
5. 设置自定义 DNS 服务器（可以由运营商提供或者自定义）
6. DNS 重新绑定保护（如果启用，则拒绝解析私有地址包）

7. 禁用 DHCP 服务（保留默认设置）
8. 保存 & 应用上述设置

如果不适用，请保留字段的默认设置。

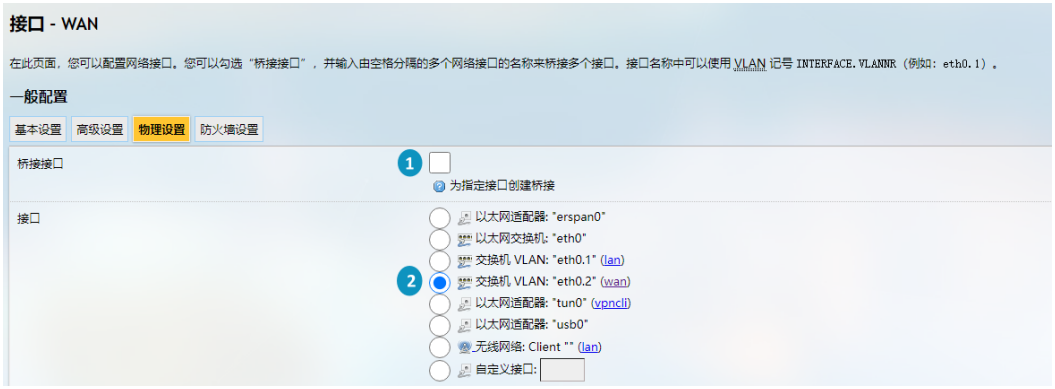
选择静态地址协议后，将自动禁用 DHCP 服务器。

高级设置与 DHCP 协议的高级设置选项基本相同。

退出页面前，请保存设置。

其他 WAN 口协议还包括 PPPoE、GRE tunnel over IPv4，以及中继桥。具体设置取决于相关协议。点击**返回或刷新**即返回接口设置页面。

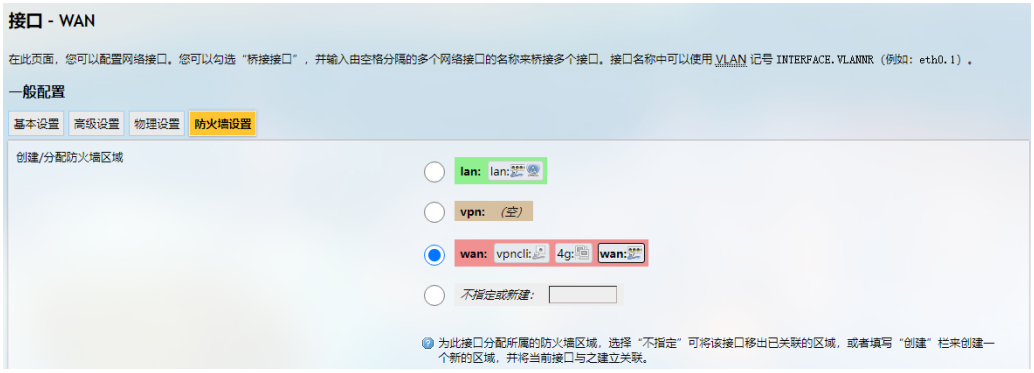
如果以 root 用户登录 VantronOS，则**高级设置**按钮旁会有一个**物理设置**按钮，用于 WAN 口的桥接设置。



编号说明

1. 启用网桥接口
2. 选择桥接的接口

如果以 root 用户登录 VantronOS，则物理设置按钮旁会有一个**防火墙设置**按钮，用户可以创建或指定防火墙区域。



如果选择“不指定或新建”，可以从相关的防火墙区域移除该接口或者创建一个新的防火墙区域。

3.6.2 无线（WIFI）

无线连接提供接入点（AP）和客户端（Client）两种模式，用户可以根据需要进行切换。 将网关用作 AP 时，请确保网关已联网。

3.6.2.1 Wi-Fi - AP 模式（基本设置）

编号说明

1. 设置路由器的无线连接名称（SSID）

名称中不能含有$、`、\等特殊符号。

2. 选择 Wi-Fi 信道
3. 选择加密方式（加密方式不同，后续配置选项也会有所不同）
4. 选择加密算法
5. 设置 Wi-Fi 密码（不少于 8 个字符）
6. 当前连接设备的明细

退出页面前，请保存设置。

3.6.2.2 Wi-Fi - AP 模式（高级选项）

编号说明

1. 打开/关闭 Wi-Fi
2. 设置 Wi-Fi 频段（由硬件决定）
3. 点击按钮切换频段
4. Wi-Fi 所属网络接口

选项 2 的修改对 Wi-Fi 的信道有影响，故单击切换后页面会自动跳转回基本设置页面。

退出页面前，请保存设置。

3.6.2.3 Wi-Fi – 客户端模式

当路由器被设置为某个无线网络的客户端时，通过下文页面可以变更网络设置。

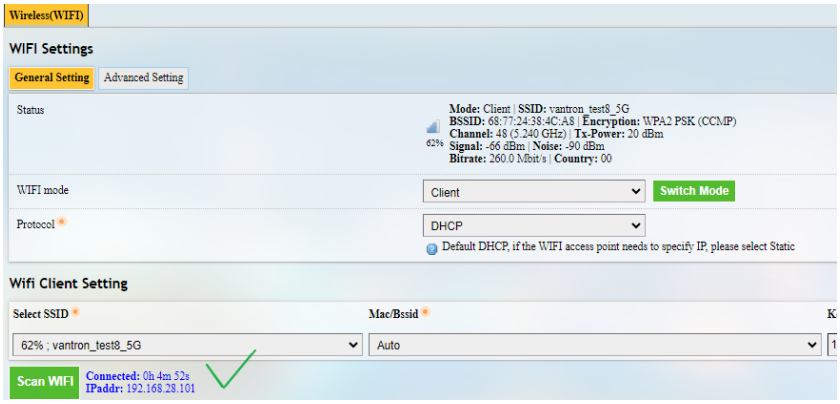
*如果将 Wi-Fi 配置为客户端模式，将自动添加 wwan0 网络接口（显示于**接口**页面）。*

编号说明

1. 切换至**客户端模式**
2. 选择 DHCP 协议自动获取 IP 地址，或者选择静态地址协议并为路由器指定 IP 地址
3. 选择待接入的无线网络
4. 选择待连接 Wi-Fi 的 MAC 地址，如果不清楚则保持“Auto”选项
5. 输入 Wi-Fi 的密码
6. 如果未识别到目标 Wi-Fi，点击**重新扫描周边 WIFI 信号**按钮，刷新 Wi-Fi 列表

退出页面前，请保存设置。

当路由器作为客户端成功连接后，**重新扫描周边 WIFI 信号**按钮旁边将显示所连接的网络信息。



3.6.2.4 Wi-Fi – AP + 客户端模式

AP + 客户端模式允许用户在客户端模式下将路由器连接外部 Wi-Fi 后，再将其作为接入点为其他设备提供网络连接服务。

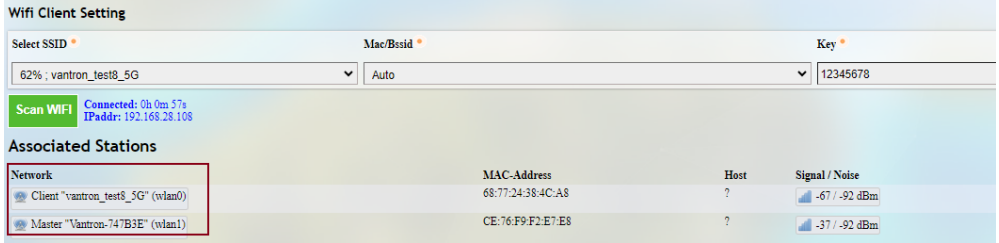
编号说明

1. 切换至 **AP + 客户端模式**
2. 设置路由器作为接入点时的 SSID
3. 选择 Wi-Fi 信道
4. 选择加密方式
5. 选择加密算法
6. 设置 Wi-Fi 密码（不少于 8 个字符）
7. 选择待接入的无线网络
8. 选择待连接 Wi-Fi 的 MAC 地址，如果不清楚则保持“Auto”选项
9. 输入接入点 Wi-Fi 的密码

如果未识别到目标 Wi-Fi，点击重新扫描周边 WIFI 信号，刷新列表。

退出页面前，请保存设置。

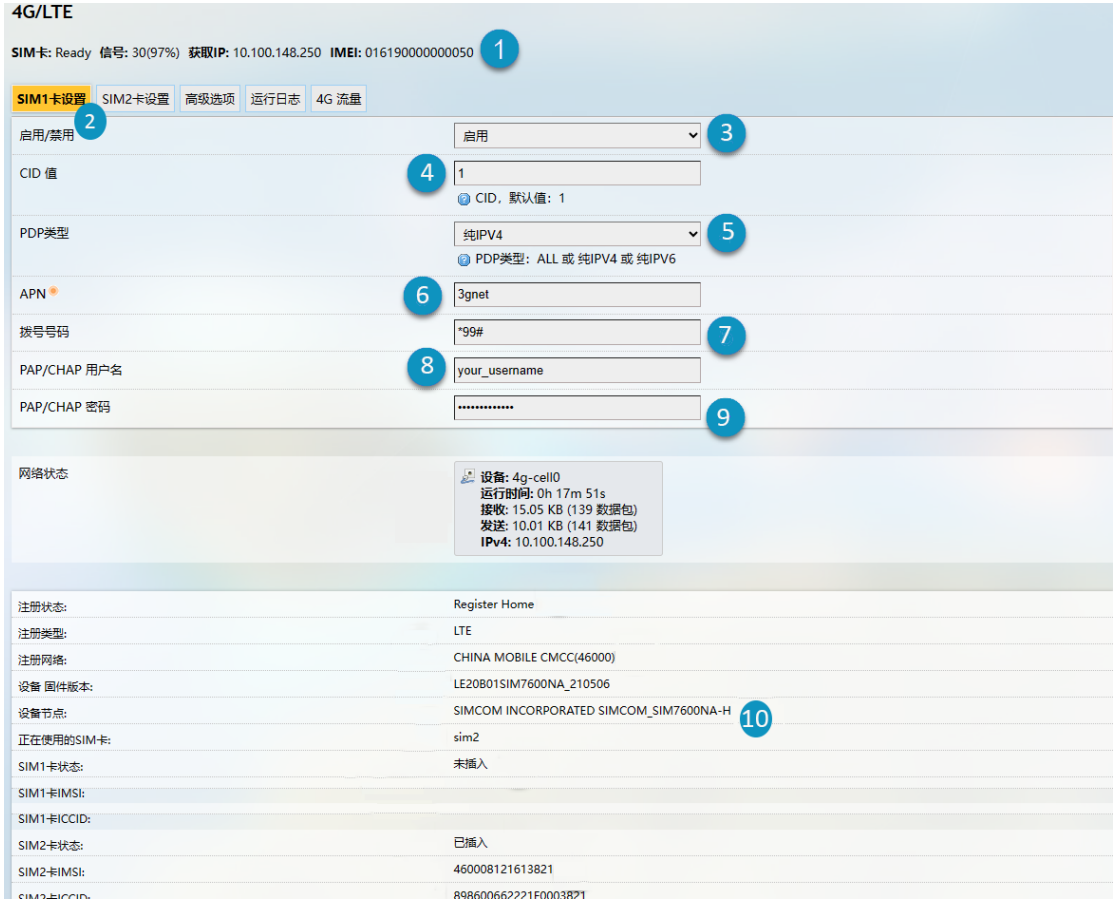
设置生效后，连接状态如下图所示。



3.6.3 4G/LTE

在进行 4G/LTE 配置前，请确保已根据 2.1 中的说明，将激活的 SIM 卡插入了卡槽并安装了 LTE 天线。插入已激活的 SIM 卡之后，页面顶端会显示 SIM 卡的信号强度、IP 和 IMEI 等信息。而 SIM 卡的注册状态、设备节点、SIM 卡 ICCID 等基本信息将展示于**详细信息**下方。

安装后，路由器上的 4G 信号指示灯会点亮，用于提示信号强度。用户可以导航至**网络 > 4G/LTE** 完成更多设置。



编号说明

1. 连接状态信息（包括 SIM 卡状态、信号强度、IP、IMEI）
2. 设置 SIM 卡 1/2
3. 启用/禁用 SIM 卡
4. 设置 CID 值
5. 选择 PDP 类型
6. 输入供应商提供的 APN
7. 输入拨号号码
8. 输入运营商提供的用于 PAP/CHAP 鉴权的用户名
9. 输入运营商提供的用于 PAP/CHAP 鉴权的密码
10. 当前网络接口状态
11. SIM 卡详细信息

如果不适用或不确定，请保留字段原样。

如果运营商设置了 APN 用户名和密码，则需要指定 PAP/CHAP 用户名和密码。

如果在 SIM 卡槽 2 插入了 SIM 卡，请点击 SIM2 卡按钮进行设置。

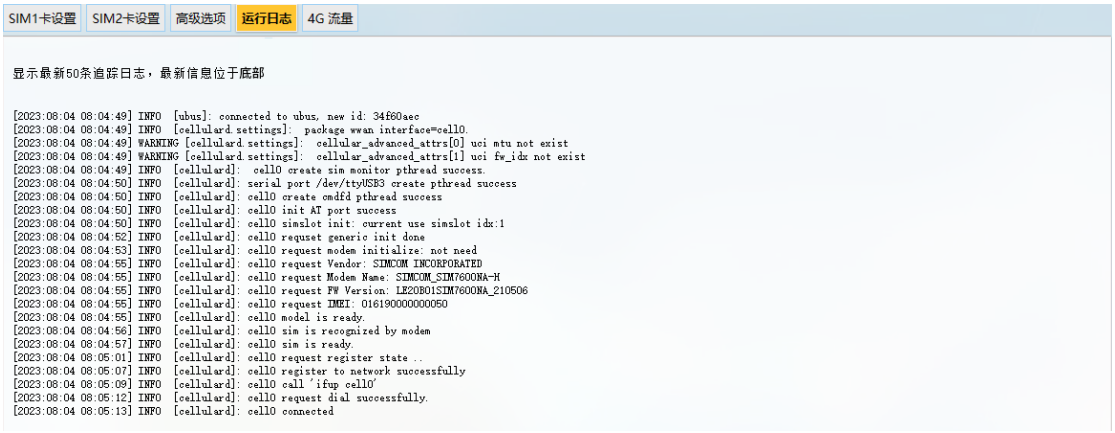
在**高级选项**页面，用户还可以进一步配置移动网络。

编号说明

1. 点击重新启动 4G 模块
2. 4G 模块断网后自动重启的时间
3. 蜂窝信息自动刷新的时间间隔

退出页面前，请保存设置。

高级设置按钮旁的**运行日志**展示模块最近的 50 条追踪日志。



4G 流量页面可以查询 SIM 卡的实时流量和每日/每月流量，也可以设置内存中的临时数据库提交到持久性数据库目录的间隔时间。

编号说明

1. 实时流量
2. 当月使用的数据流量
3. 当天使用的数据流量
4. 将临时数据库提交到持久性数据库目录的间隔时间

退出页面前，请保存设置。

3.6.4 静态路由

静态路由作为一个高级功能，允许用户为路由访问指定接口规则。

例：

要求：当路由器有 4G 和 WAN 网络接口时，内部网络（192.168.0.0 - 192.168.255.254）由内部服务器通过 WAN 口访问，其他数据访问通过 4G 接口实现。

点击**添加**，选择一个要配置的接口。

编号说明

1. 选择配置路由的接口
2. 输入主机 IP 地址
3. 输入子网掩码（默认为 255.255.255.255）
4. 输入 IPv4 网关地址
5. 设置网关跃点（数值越小，优先级越高）
6. 设置 MTU
7. 选择路由类型（参见下一页的说明）

退出页面前，请保存设置。

路由类型说明：

类型	说明
Unicast	该类型路由描述由路由前缀覆盖的目的地址的真实路径。
Local	目的地址被分配给本机，数据包通过回环被投递到本地。
Broadcast	目的地址是广播地址，数据包作为链路广播发送。
Multicast	单次传输中，将 IP 数据报发送至一组目标接收器。在普通的路由表中，这种路由并不存在。
Unreachable	目的路由无法到达。丢弃数据包并生成 ICMP 消息主机不可访问，本地发件人收到 EHOSTUNREACH 错误本地发件人收到 EHOSTUNREACH 错误。
Prohibit	目的路由无法到达。数据包将被丢弃，并生成管理上禁止的 ICMP 消息通信。本地发件人收到 EACCES 错误。
Blackhole	目的路由无法到达。数据包被悄悄丢弃，本地发件人收到 EINVAL 错误。
Anycast	未分配给此主机的路由地址，它们主要等效于本地，但有一个区别：这些地址用作任何数据包的源地址时都是无效的。

3.6.5 防火墙

- **黑名单和白名单**

黑白名单功能允许用户启用/禁用特定地址的转发。

白名单策略：除了添加到访问控制规则的 IP 地址外，所有地址均能访问

黑名单策略：除了访问控制规则放行的 IP 地址外，所有地址均被阻止

场景 1：阻止 172.18.4.199 上网

编号说明

1. 选择**白名单策略**并点击该策略后的按钮切换至该策略
2. 选择 IP 协议
3. 输入源 IP
4. 选择“丢弃”动作
5. 点击**添加**，将该地址加入访问控制清单

退出页面前，请保存设置。

场景 2：阻止 172.18.4.199 通过 80 端口与外网进行 TCP 通信

编号说明

1. 选择**白名单策略**并点击该策略后的按钮切换至该策略
2. 选择 TCP 协议
3. 输入源 IP
4. 输入目的端口
5. 选择“丢弃”动作
6. 点击**添加**，将该地址加入访问控制清单

退出页面前，请保存设置。

场景 3：允许 172.18.4.199 上网

编号说明

1. 选择**黑名单策略**并点击该策略后的按钮切换至该策略
2. 选择 IP 协议
3. 输入源 IP
4. 选择“接受”动作
5. 点击**添加**，将该地址从访问控制清单中释放出来

退出页面前，请保存设置。

场景 4：允许 172.18.4.199 通过 80 端口与外网进行 TCP 通信

编号说明

1. 选择**黑名单策略**并点击该策略后的按钮切换至该策略
2. 选择 TCP 协议
3. 输入源 IP
4. 输入目的端口
5. 选择“接受”动作
6. 点击**添加**，将该地址从访问控制清单中释放出来

退出页面前，请保存设置。

- **端口转发**

端口转发控制着区域之间的流量，并可以启用 MSS 钳制特定方向。转发规则仅覆盖一个方向。为了允许两个区域之间的双向流量流动，需要两个转发，每个区域中的 src 和 dest 端口都反向。

端口转发设置示例（WAN 口 3222 端口到 LAN 网络 172.18.1.174 端口 22 的访问转发）：

编号说明

1. 规则名称
2. 协议（支持 TCP/UDP/TCP + UDP）
3. 外部区域：WAN
4. 外部端口： 3222
5. 内部区域：选择 LAN 口
6. LAN 主机：172.18.1.174
7. 内部区域的目标主机端口号：22
8. 添加规则（强制）

- **自定义规则**

自定义规则允许用户执行不属于防火墙框架的任意 iptables 命令。每次重启防火墙时，在默认的规则运行后这些命令将立即执行。

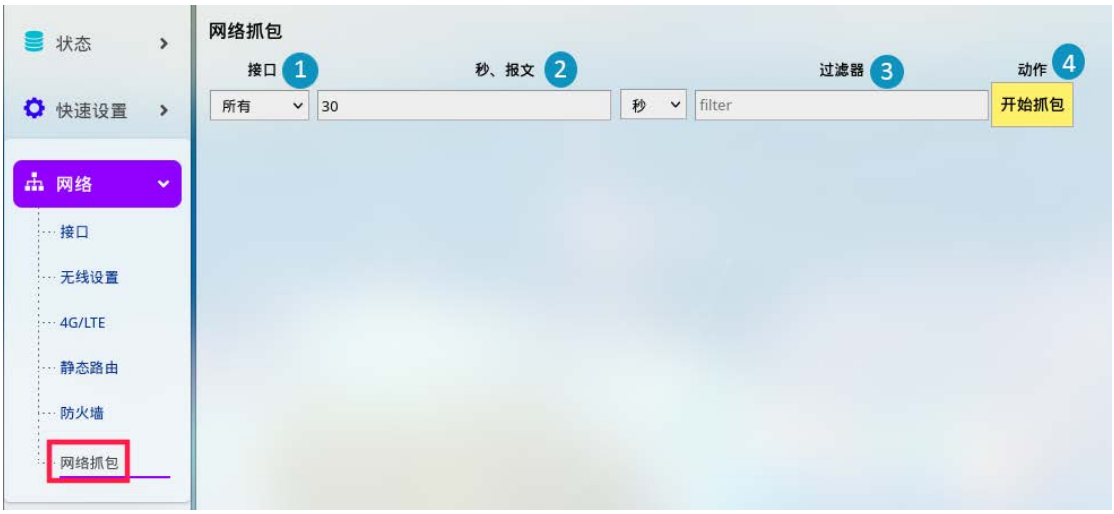
3.7 网络诊断

设备提供的网络诊断工具及其作用如下：

工具	说明
Ping	测试路由器与互联网外部 IP 地址之间的连接性并测量响应时间
Traceroute	获取网络流量路径信息，包括跃点数量和每个跃点的响应时间
Nslookup	查询域名系统 (DNS)，获取有关域名、IP 地址和 DNS 记录的信息

3.8 网络抓包

网络抓包功能方便用户灵活进行网络问题跟踪与验证。抓到的报文可以通过软件 wireshark 打开并查看里面的内容。



编号说明

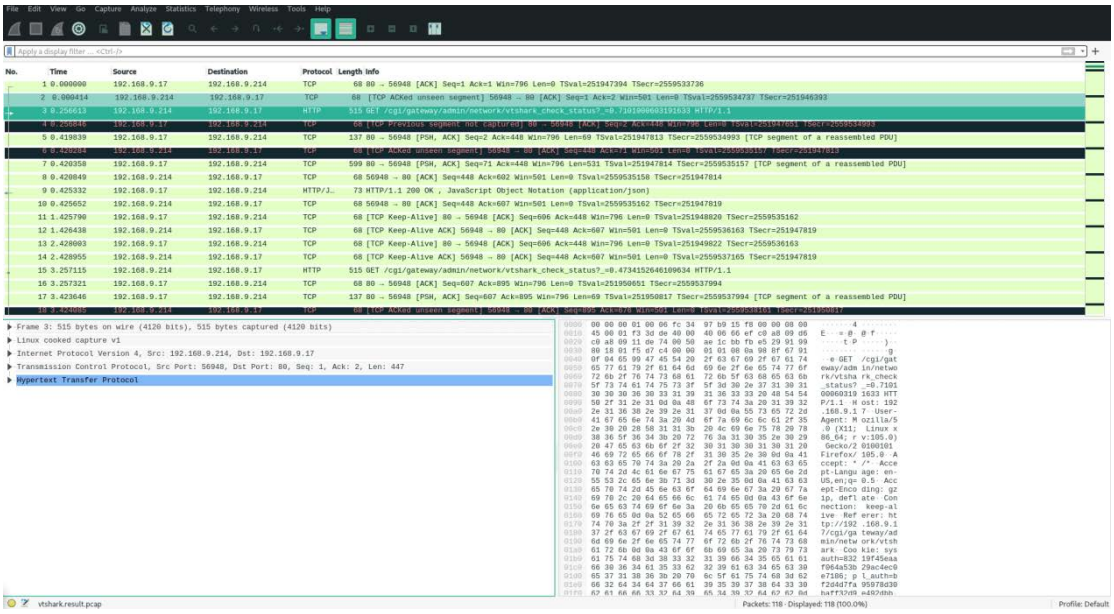
1. 选择抓包的接口，默认抓取所有接口的报文
2. 选择抓包方式（按秒或报文数目抓取数据，具体区别见后文）
3. 设置过滤器，用于抓取指定数据包的报文（更多过滤设置可查看：https://www.tcpdump.org/manpages/pcap-filter.7.html）
4. 开始抓取数据

按秒和按报文数目抓取报文的区别：

方式	说明
按秒	指定抓包时长 例，可以设置抓包时长为 '10/20/30...'，表示 10/20/30 秒后，抓包结束。
	以时间为准的抓包，系统支持的最大报文数为 500,000 个。这就意味着，超出该数目后，系统将停止抓包，即使尚未达到设定的抓包时长。
按报文数目	指定抓包数目 例，可以设置抓包数目为'100/200/500...'，表示抓包数目达到 100/200/500 后，抓包结束。
	以抓包数量为准的抓包，系统支持的最大抓包时长为 1 分钟（600 秒）。这就意味着，超出该时长后，系统将停止抓包，即使尚未达到设定的抓包数目。

以下场景中，系统抓取所有接口来自 TCP 80 端口的 http 报文，抓包时长 30 秒。

抓包完成后，点击结果下方的链接可以将抓包结果下载到本地。之后，用户可以使用 wireshark 打开并查看结果。

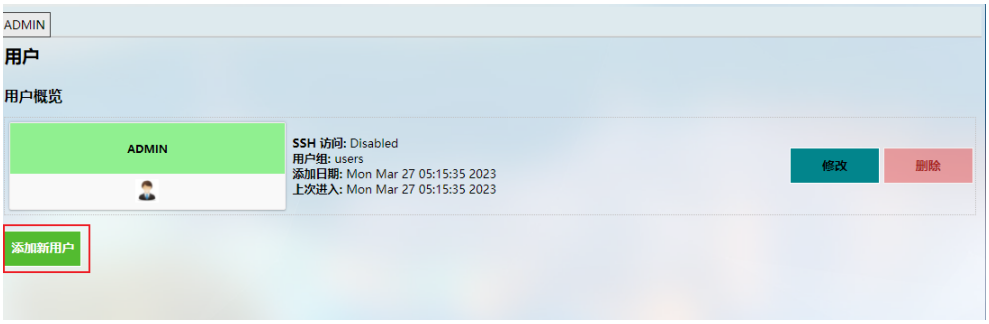


3.9 用户管理

此功能会更改系统设置，因此需要使用 **root** 账号登录（账号、密码见 2.2），然后启用该功能。

在**修改用户**页面，您可以添加新用户或者修改现有用户的权限，实现根据角色设置不同的权限。

如需添加用户，请点击当前用户信息下面的**添加新用户**按钮。



在打开的页面，您可以创建用户并为用户指定相应的功能。

编号说明

1. 输入用户名称
2. 选择新用户的用户分组
3. 选择是否为新用户启用 **SSH 登录**选项
4. 为新用户指定相应功能

退出页面前，请保存设置。

创建用户后，该用户会被添加到用户列表。通过单个用户后面的**修改**和**删除**按钮，您可以启用/禁用该用户的某些功能，或者删除该用户。

3.10 客制应用

该菜单下部分功能会更改系统设置，因此需使用 **root** 账号登录（账号、密码见 2.2），然后启用该功能。

3.10.1 客制程序

客制程序功能允许用户将自己的脚本或程序（sh/bin）上载到路由器，并设置为在启动时运行。

编号说明

1. 选择要上传到路由器的脚本
2. 上传脚本至路由器
3. 当脚本成功上传后，页面将显示文件名和文件目录
4. 启用该脚本，则该脚本将在下次启动路由器时自动运行
5. 如果上传多个脚本，用户可以上下移动任意脚本，重新排列脚本顺序，并编辑/删除脚本
6. 查看脚本日志
7. **保存 & 应用**上述设置

3.10.2 IPK 安装器

该页面允许客户将自己开发和编译的 IPK 软件包安装到路由器。工业协议安装包也在该页面上传。

编号说明

1. 从本地选择待上传的.ipk 文件包
2. 点击**上传**按钮，将安装包上传到设备
3. 之后用户可以删除或安装.ipk 软件包
4. 安装.ipk 文件并等待，会出现显示文件安装状态的信息
5. 您也可以输入相关文件在设备上的路径，将文件下载到本地

3.10.3 厂商信息定制

如需自定义厂商信息，请导航至**客制应用>厂商信息定制**，并在厂商信息模式下拉菜单中选择**定制模式**。

编号说明

1. 选择定制模式
2. 下载示例包到本地，并根据需要将示例包内的相关文件替换为自定义的文件
3. 从本地选择目标文件
4. 将文件上传至路由器
5. 文件的保存路径将被记录
6. 选择下一次启动设备时，是否应用自定义文件
7. 选择文件类型
8. **保存 & 应用**上述设置

三种厂商信息模式解释如下，用户可以根据自身需求选择其一：

模式	说明
万创模式	VantronOS 中显示的所有信息均为万创相关
中性模式	VantronOS 中部分字段将默认显示“网关”，其余信息如版权等，将显示空白。
定制模式	所有展示信息都是用户自定义

3.10.4 DMP Agent

网关/路由器通过 DMP Agent 与 BlueSphere GWM 平台通讯。用户可以在**客制应用 > DMP Agent** 页面更改相关设置。

编号说明

1. DMP Agent 运行状态
2. 修改配置前，点击该按钮，清空 Agent

> *如果其他条件满足（请参考2.5 连接万创网关管理平台），并且已启用 DMP agent，那么联网后，DMP Agent 将自动运行。此按钮将禁用 Agent、杀死后台进程，并在原始安装路径下删除程序包。*

3. 启用/禁用 Agent
4. 用户可以自定义 Agent 的安装路径（默认安装路径为“/usr/vtmdm_agent_c/”）
5. 设置 Agent 服务器的下载地址（建议不做更改）
6. 公域请选择互联网服务器，私域工作选择下载地址服务器

> *如果路由器恢复出厂设置，设备在 BlueSphere GWM 平台的状态将变为离线模式。如需使其重新上线，请在 VantronOS 页面点击**清空 Agent**，然后选择**启用** Agent，等待一会儿后，设备将重新在 BlueSphere GWM 平台上线。*

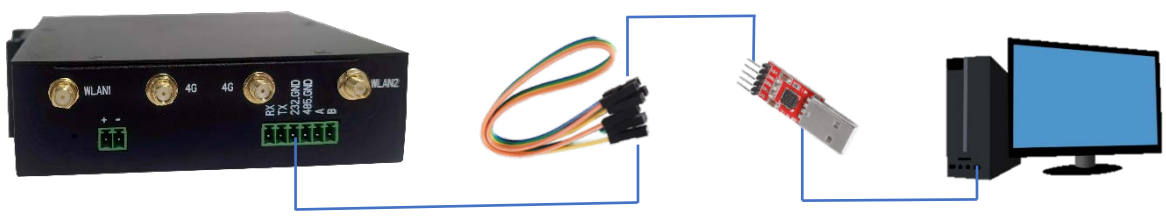
3.11 硬件

3.11.1 串口转 TCP

串口转 TCP 是将本地串口数据转换成以太网数据与远端设备双向通信的工具，每条转换规则可独立配置为服务器端或客户端模式。用户也可以添加、编辑或删除该页面的转换规则。

3.11.2 Ser2net 环境搭建与验证

- 环境准备：
  - 一台 R105 路由器
  - 一台 Linux 主机（此处以 Ubuntu 为例）
  - USB 转 TTL 串口适配器
  - 杜邦线
  - 如下图所示，连接路由器串口和主机（接口的连接请参考 1.5，此处以 RS232 模式进行说明）



- 客户端模式：

(1) VantronOS 页面的配置

编号说明

1. 点击**添加**，新增一条转换规则
2. 选择**启用**该规则
3. 设置波特率为 115200
4. 保存设置
5. 点击**修改**，进入高级设置页面

编号说明

1. 选择启用该规则
2. 选择**客户端**模式
3. 输入服务器的 IP 地址和端口号（Ubuntu 主机为服务器，端口号由用户设置）
4. 点击下拉框，选择串口设备（如 1.5 所述，RS232 串口点位为/dev/ttyS1）
5. 选择波特率为 115200（默认为添加规则时设置的数值）
6. 输入超时时间
7. 选择数据位“8 bits”
8. 选择奇偶校验“无”
9. 选择停止位“1”

*设置完成后，**保存 & 应用**上述设置。*

(2) Ser2net 运行进程如下：

```
uart2net -c -d 192.168.93.1 -p 8888 -t /dev/ttyS1 -b 115200 -a 8 -r none -s 1 -o 20
```

(3) Ubuntu 主机端设置

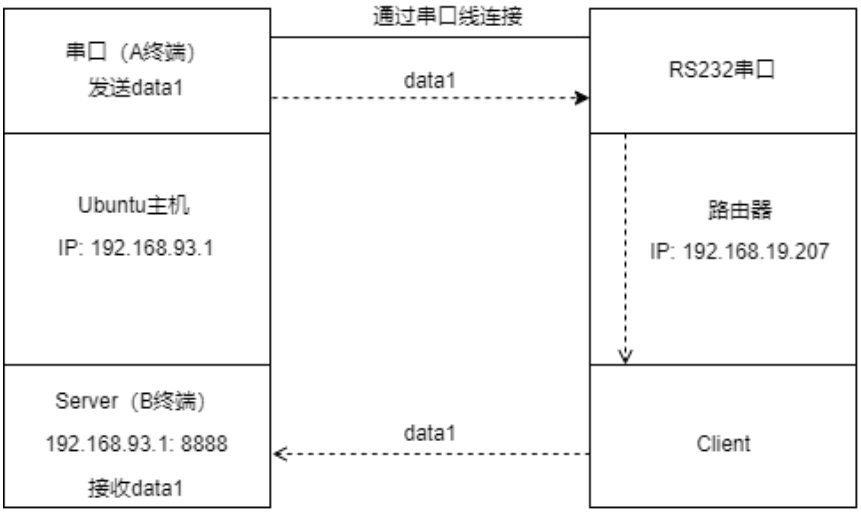
- 在 A 终端使用 microcom 工具命令打开串口（假设识别出 USB 转 TTL 串口适配器的设备名为/dev/ttyUSB1）

```
sudo microcom -p /dev/ttyUSB1 -s 115200
```

- 在 B 终端监听端口（前述步骤设置为 8888）

```
tcpudp_test tcp server:tcpudp_test -p 8888
```

- 此时在 A 终端输入数据后，可在 B 终端接收，拓扑图如下



- 服务器模式：

(1) VantronOS 页面的配置

编号说明

1. 点击**添加**，新增一条转换规则
2. 选择**启用**该规则
3. 设置波特率为 115200
4. 保存设置
5. 点击**修改**，进入高级设置页面

编号说明

1. 选择启用该规则
2. 选择**服务器**模式
3. 输入端口号（端口号由用户设置）
4. 点击下拉框，选择协议（以 Telnet 为例，协议区别见 3.11.3）
5. 选择串口设备（如 1.5 所述，RS232 串口的软件点位为/dev/ttyS1）
6. 选择波特率为 115200（默认为添加规则时设置的数值）
7. 输入超时时间
8. 选择数据位“8 bits”
9. 选择奇偶校验“无”
10. 选择停止位“1”

退出页面前，请保存设置。

(2) Ser2net 运行进程如下：

```
/usr/sbin/ser2net -n -c /tmp/ser2net.conf
```

(3) Ubuntu 主机端设置

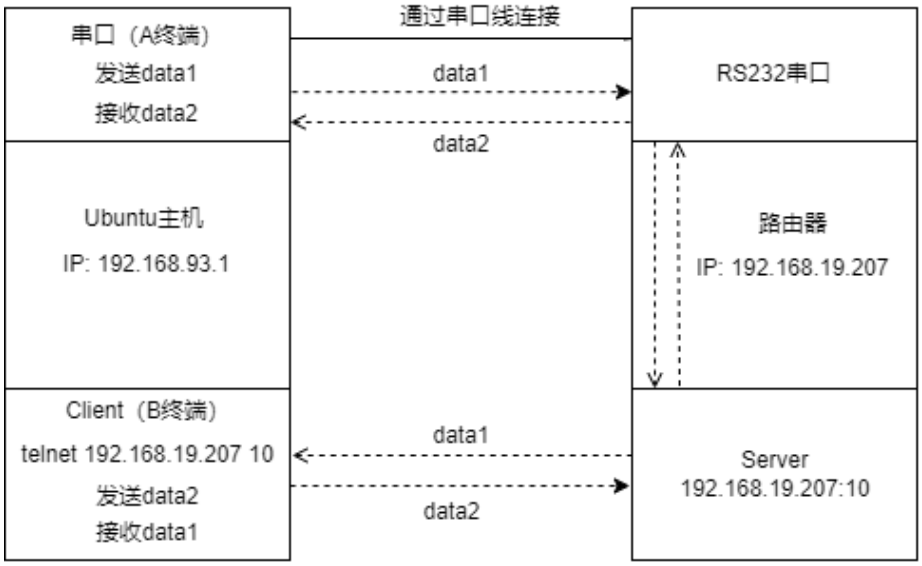
- 在 A 终端使用 microcom 工具命令打开串口（假设识别出 USB 转 TTL 串口适配器的设备名为/dev/ttyUSB1）

```
sudo microcom -p /dev/ttyUSB1 -s 115200
```

- 在 B 终端使用 Telnet 协议监听端口（前述步骤设置为 10）

```
telnet 192.168.19.207 10
```

- 此时 A/B 两个终端可以互相发送和接收信息，拓扑图如下



3.11.3 协议对比

在**服务器模式**下，存在两种协议，区别如下：

1) Raw：启用端口，在端口和长整数之间按照原样传输所有数据。

2) Telnet：启用端口，并在端口允许 Telnet 协议，以设置 Telnet 参数（较少使用）。

3.12 服务

3.12.1 动态域名系统（DDNS）

动态域名系统（DDNS）是域名系统（DNS）中的一种自动更新名称服务器（Name server）内容的技术。通常，主机、地址等信息会进行主动配置。

输入子域名或根域名的名称，然后点击**添加**按钮，进入 DDNS 设置页面。之后即可根据需要编辑动态域名服务。

3.12.2 PLC 远程连接

如需通过 OpenVPN 协议远程访问和控制 PLC 设备，用户需使用位于同一网络环境下的两台 R105 路由器和一台 Windows 控制主机，其中一台路由器设备（R1）用于搭建 OpenVPN 服务器，另一台路由器设备（R2）则用于连接 R1 搭建的 OpenVPN 服务器。

前提条件：

1. 根据上述说明，准备 R1、R2、Windows 主机、PLC 设备
2. 将 R1 和 R2 通过无线 Wi-Fi 或以太网连接到同一网络
3. 在 Windows 主机上安装 OpenVPN 客户端程序（如，OpenVPN-2.5.2-I601-amd64.msi）和 PLC 编程软件（如 STEP7，取决于 PLC 设备）
4. 参考 3.4.1 OpenVPN 服务器中所述，在 R1 上搭建 OpenVPN 服务器（**Tap** 工作模式），并下载.ovpn 文件
5. 通过 OpenVPN 客户端程序将 Windows 主机连接到 R1 搭建的 OpenVPN 服务器
6. 将 R2 连接到 R1 搭建的 OpenVPN 服务器（见下文）
7. 将 PLC 设备连接到 R2 其中一个 LAN 口，并将 PLC 设备的 IP 地址设置为静态地址（见下文）
8. 通过以太网将 PLC 设备连接到 Windows 主机，并通过 PLC 编程软件（STEP7）控制 PLC 设备

用户可以通过 VantronOS 连接 R2 和 R1 并配置 PLC 设备和 R2。关于其他设置，请下载相关软件程序，进行配置。

编号说明

1. 下载并保存 R1 配置 OpenVPN 服务器所生成的.ovpn 文件，然后点该击按钮打开文件目录；
2. 点击**连接**，等待 R2 连接 R1 配置的 OpenVPN 服务器；
3. 连接成功后，将出现 OpenVPN 服务器分配的 IP 地址；
4. 输入 PLC 的 IP 地址（与 R2 的 LAN 口在同一网段）；
5. 输入虚拟 IP 地址（需与第 3 步中 OpenVPN 服务器分配的 IP 地址在同一网段，且未被占用）；

完成设置后，请保存页面并应用。

3.13 系统

3.13.1 系统

用户除了可以根据前述章节更改路由器设置，还可以在此处修改主机名称、时区、密码等信息。

编号说明

1. 同步路由器时间与浏览器（本地）时间
2. 更改主机名称
3. 选择时区
4. 启用 NTP 在线时间调整
5. 启动 NTP 服务器（路由器作为 NTP 时间服务器）
6. NTP 在线时间服务器

日志相关的设置，请点击**基本设置**页面旁边的**日志信息**。

编号说明

1. 系统日志缓冲区的大小
2. 日志服务器地址
3. 日志服务器端口
4. 日志服务器使用的协议
5. 系统日志的文件路径
6. 调试串口日志的打印等级
7. Cron 日志等级

3.13.2 带宽监视

基本设置

编号说明

1. 设置监控活动的数据统计周期
2. 指定每月某一天为下一轮监控的起点

1 中选择“每月的某一天”时适用

3. 统计接口
4. 本地子网

在**高级设置**页面，用户可以进一步设置监控行为。

编号说明

1. 选择数据库中存储的最大条目数量（‘0’表示无限制）
2. 勾选此项，预分配一个数据库（常用于设备内存空间不足的情况）
3. 勾选此项，压缩数据库
4. 保留的最大统计周期数（‘0’表示无限制）
5. 将临时数据库提交到永久数据库的时间间隔
6. 从 netlink 信息中刷新流量计数器的时间间隔
7. 数据库目录

协议映射用于区分每个主机的流量类型。每个映射占用一行，第一个值为 IP 协议，第二个值为端口号，第三个值为映射协议的名称。

3.13.3 管理权

用户可以在该页面重设路由器访问密码。

SSH 访问

由于此功能可能影响网络安全性，用户需要使用 root 账户登录页面。

第 1 步：点击左下角的**退出**，退出当前页面；

第 2 步：使用 root 账号（**root**）和密码（**rootpassword**）登录网关；

第 3 步：导航至**系统 > 管理权**，并启用 Dropbear。

编号说明

1. 选择访问接口（默认 LAN 口）

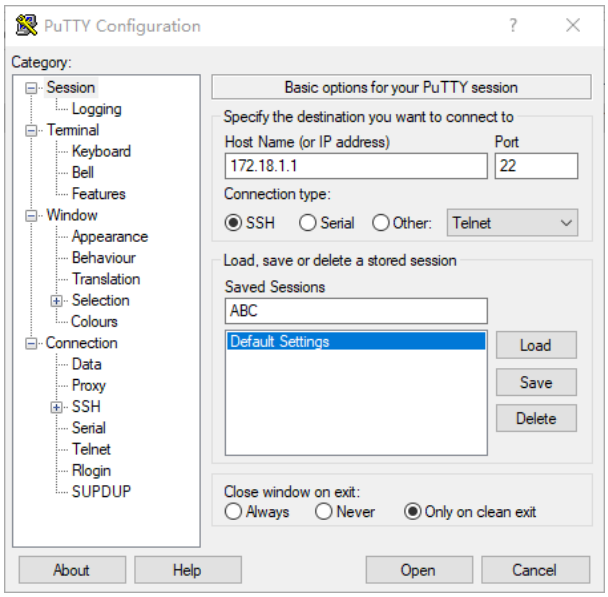
如果选择"未指定"，则所有接口都将被监听。

2. 指定监听端口（默认为端口 22）
3. 允许 SSH 密码验证
4. 添加 SSH 密钥进行公钥认证

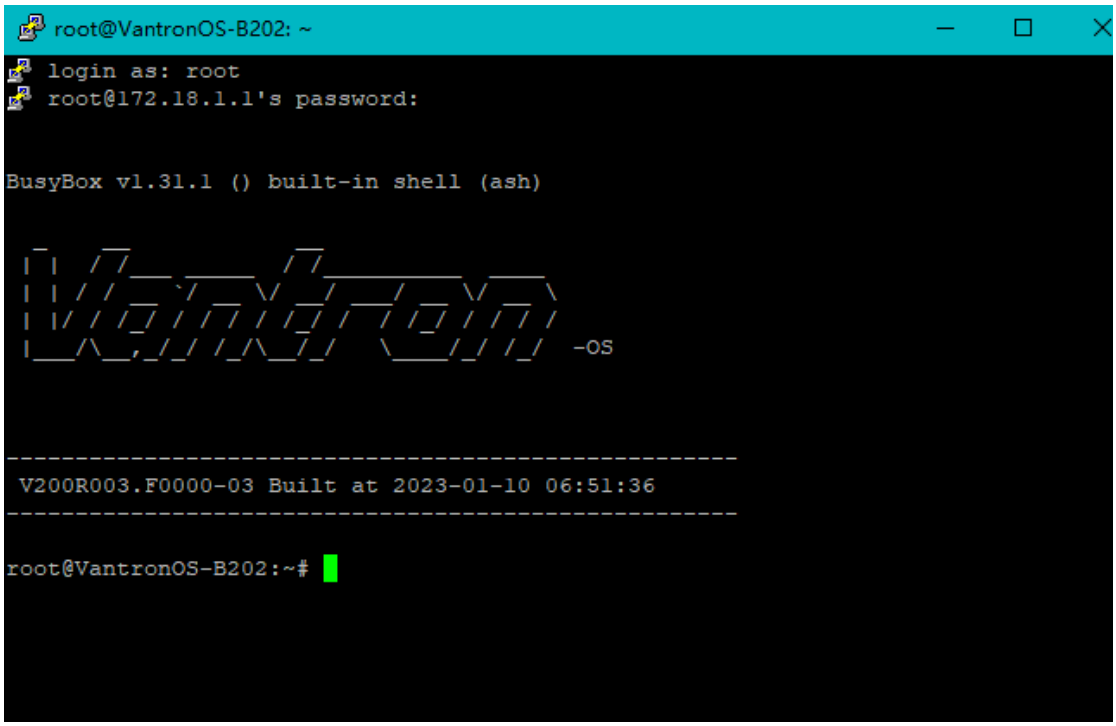
第 4 步：在 Windows 主机打开 SSH 客户端工具（推荐 PuTTY 或 MobaXterm）；

第 5 步：输入主机名或 IP 地址（默认为 LAN 口 IP 地址 172.18.1.1），保持默认端口（22）不变，并选择 **SSH** 连接方式；

第 6 步：设置会话名称并点击**保存**，其余设置保持不变，然后点击**打开**；

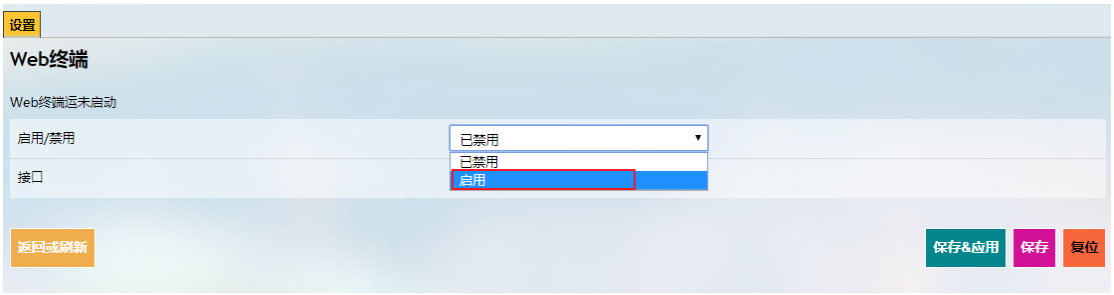


第 7 步：登录 root 账号（同前述步骤中路由器登录密码一致），并开启 SSH 远程会话。



3.13.4 Web 终端

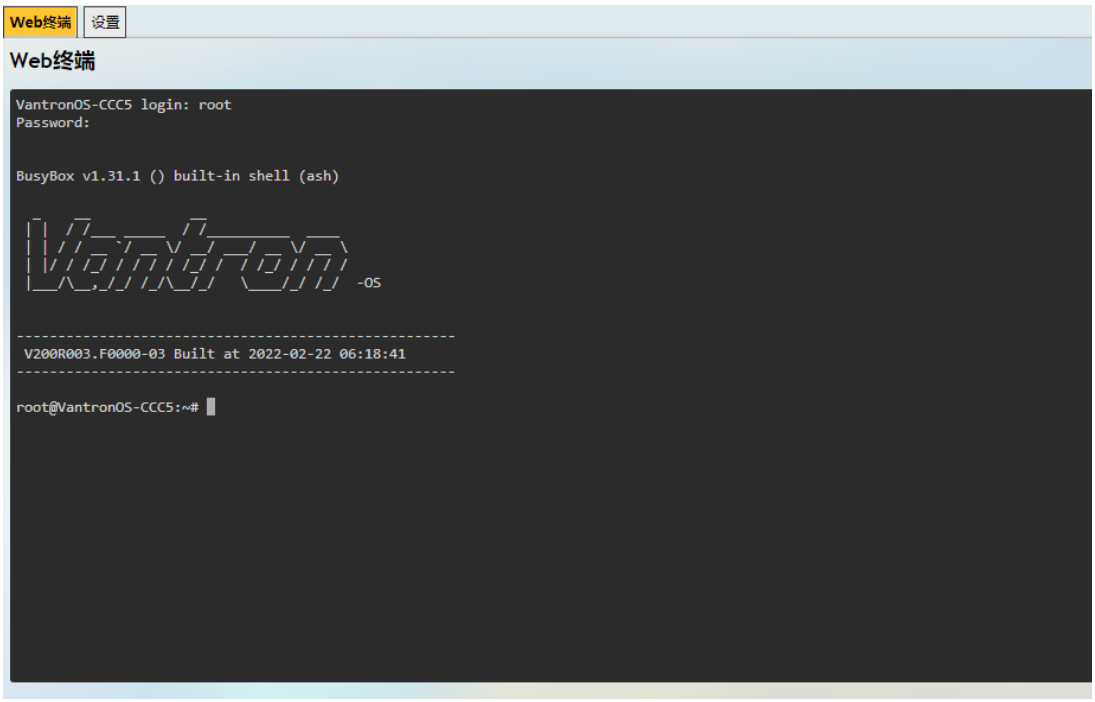
在 Web 终端页面**设置**项下点击**启用** Web 终端并保存&应用后，用户可以登录并输入命令行调试路由器。



启用 Web 终端后，在**设置**页面旁会出现 **web 终端**页面选项：

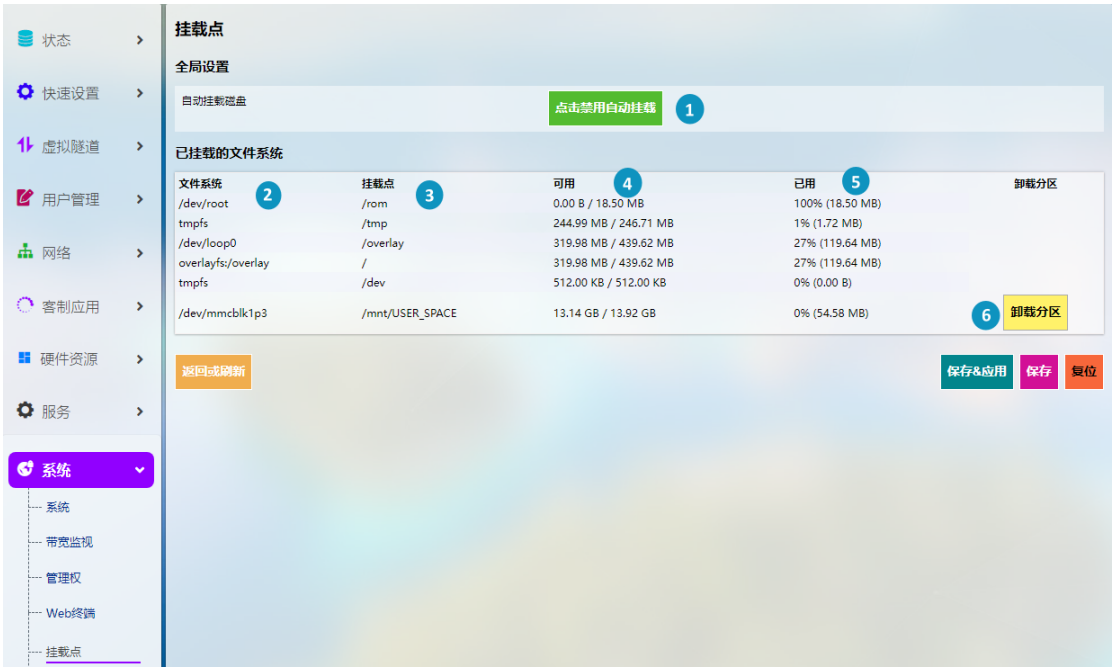
登录名：**root**

登录密码：**rootpassword**（输入时不可见）



3.13.5 挂载点

用户可以在此启用/禁用自动挂载并查看挂载信息。



编号说明

1. 禁用/启用自动挂载
2. 设备上的文件路径
3. 挂载点
4. 挂载点的可用空间
5. 已使用空间（百分比）
6. 如果之前在设备上挂载了文件，可以在此处手动取消挂载

如需手动挂载文件，请先**禁用自动挂载**，然后继续进行设置。

编号说明

1. 检查可挂载点
2. 点击**添加**，可添加挂载点

添加挂载点后，点击该挂载点后的**修改**按钮，进入设置页面。

3. 点击启用该挂载点
4. 选择设备的 UUID
5. 选择挂载点

之后点击**高级设置**按钮，进入高级设置。

6. 选择用于格式化存储器的文件系统
7. 输入挂载选项
8. 保存设置，然后点击**返回或刷新**按钮，回到基本设置页面。

新建的挂载点如上图所示。

3.13.6 备份/升级

用户可以在此备份/恢复参数、恢复出厂设置（清除用户设置）并从本地或通过 OTA 升级固件。

OTA 升级

编号说明

1. 将云端版本号刷新至最新版本（需联网）
2. 升级路由器时重置配置
3. 升级路由器时保留现有设置

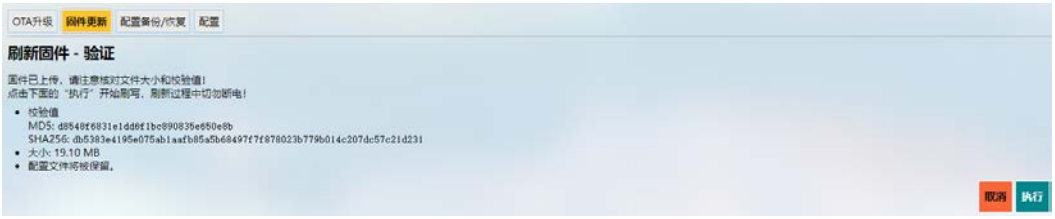
如果云端版本号显示 Failure，则该路由器未在云端激活，请联系销售代表解决该问题。

固件升级

编号说明

1. 勾选此项后，设备更新过程中将保留用户设置（不推荐）
2. 从本地路径选择相关固件
3. 点击按钮，上传固件
4. 固件包上传进度

当固件信息出现时，验证固件是否正确，然后点击**执行**，开始更新固件。



固件升级需要一定时间，在此过程中，请勿断电。

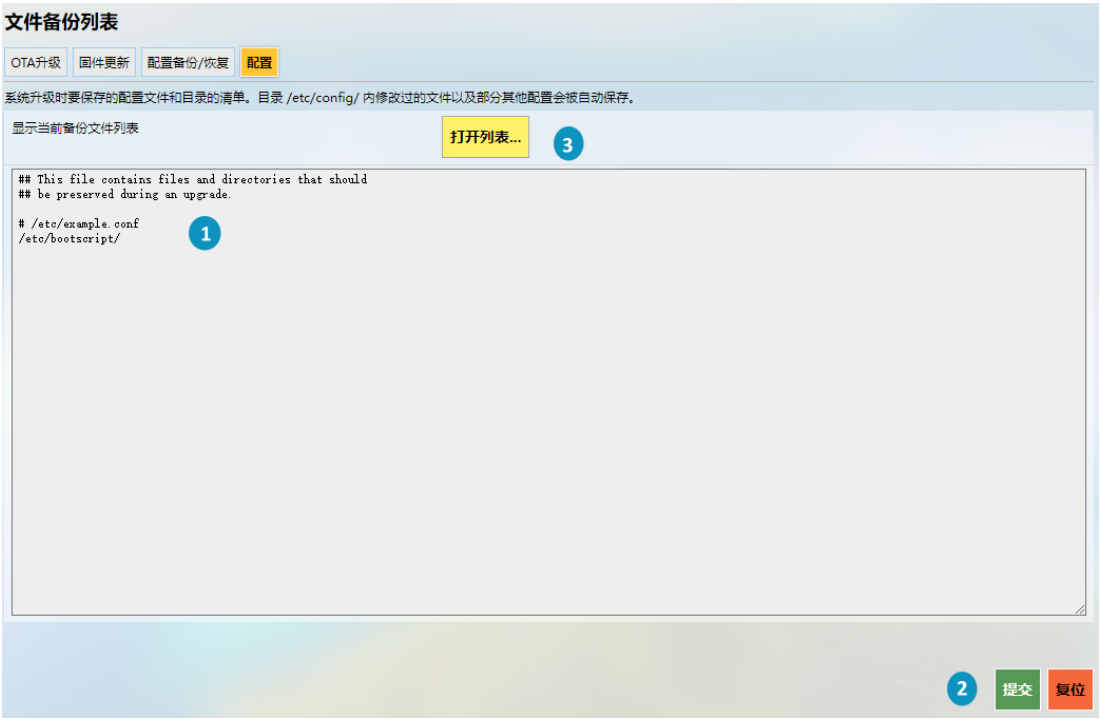
升级完成后，登录页面将被刷新。用户可以登录并在主页查看固件版本信息。

在**配置备份/恢复**页面，用户可以下载配置文件和预设文件夹等参数的备份文件包、将路由器恢复出厂设置，并上传以前保存的备份文件包。

编号说明

1. 点击此按钮备份系统配置（仅包含配置文件和预设文件，不包含客户端文件或程序）
2. 将设备恢复出厂设置（用户配置将被清除）
3. 从本地选择备份文件，恢复备份设置
4. 上传备份文件

在**配置**页面，用户可以设置系统升级时要保留的配置文件或目录。



编号说明

1. 输入升级时要保留的配置文件或目录
2. 点击**提交**，确认设置
3. 显示保留配置的文件列表

3.13.7 重启

重启路由器前，请确保没有开启任何进程。

3.14 退出

点击**退出**后，用户将退出 VantronOS 网页界面。如需再次登录页面，请使用默认密码：**admin**。退出前请确保已保存更改。

第 4 章 废弃处理与产品质保

4.1 废弃处理

当设备到了使用期限，为了环境和安全，建议您适当地处理设备。

处理设备前，请备份您的数据并将其从设备中删除。

建议在处理前拆解设备，以符合当地法规。请确保废弃的电池已按照当地关于废物处理的规定进行处理。电池具有爆炸性，请勿将其扔进火中或放入普通垃圾桶中。标有 "爆炸性"标志的产品或产品包装不应该按照家庭垃圾处理，应当该送到专门的电气和电子垃圾回收/处理中心。

妥善处理这类废物有助于避免对周围环境和人们的健康造成伤害和不利影响。请联系当地机构或回收/处理中心，了解更多相关产品的回收/处理方法。

4.2 质保

产品质保

万创向客户保证，万创或万创分包商制造的产品从万创发运时将严格符合双方商定的规格，不存在工艺和材料上的缺陷（由客户提供的除外）。万创的质保义务限于产品的更换或维修（由其自行决定）。如果出现质量问题，产品发货后，客户应当自开具发票之日起 **24 个月**内，自付运费将产品返回万创工厂。经检查后，万创合理确认产品具有缺陷的，由万创承担质保责任。之后，由万创承担将产品发运给客户的运输费用。

保修期外的维修

万创将按照当时的服务费率为已过保修期的产品提供维修服务。只要市场有售，万创将根据客户要求向客户提供非保修期内的维修部件，但客户需提前下达采购订单。维修部件有 3 个月的延长保修期。

产品退回

任何根据上述条款被认定为有缺陷并在保修期内的产品，只有在客户收到并参照万创提供的退货授权（RMA）号码后，才能退回万创。万创应在客户提出要求后的 3（三）个工作日内提供 RMA。万创应在向客户发出退货产品后，向客户提供新的发票。在客户因拒收或保修期内的缺陷而退回任何产品之前，应向万创提供在客户所在地检查该产品的机会。除非拒收或缺陷的原因被确定为万创的责任，否则经检查的产品不得退回万创。万创应在收到产品后的 14（十四）个工作日内，向客户发回维修后的产品。如果万创由于其无法控制的原因而不能提供上述服务，万创应记录这种情况并立即通知客户。

附录 A　合规声明

FCC 声明

此设备经检测，符合 FCC 规则第 15 部分中关于 B 级数字设备的限制规定。这些限制的目的是为了在居住区中安装此设备时，可以提供合理的保护以防止有害干扰。此设备会产生、使用和辐射射频能量，如果未遵照制造商的使用手册安装和使用，可能会对无线电通信产生有害干扰。但是，这并不能确保在某些特定安装中绝不会产生干扰。如果此设备确实对无线电或电视机接收信号造成有害干扰,而这一点可以通过关闭和打开设备来确定,那么建议用户尝试使用以下一种或多种措施来消除干扰:

- 调整接收天线的方向或重新放置。
- 扩大设备与接收器之间的距离。
- 将设备连接至与接收器不同的电路。
- 请与代理商或有经验的无线电/电视技术人员联系获得帮助。

此设备符合 FCC 规则的第 15 部分。操作应符合以下两个条件：（1）该设备不会产生有害干扰，以及（2）本设备必须承受收到的任何干扰，包括可能导致意外操作的干扰。

注意：制造商对未经授权改装本设备而造成的任何无线电或电视干扰不承担任何责任。改装后，用户或将无权操作本设备。