G335 边缘计算网关

用户手册

版本：1.5

版本记录：

编号	软件版本	说明	日期
V1.0	V200R003	首次发布	2020/05/25
V1.1	V200R003	修改网关配置	2020/06/30
V1.2	V200R005	1. 增加串口、CAN、GPS、ZigBee、系统启动等相关信息 2. 修改 3.5.3 4G/LTE 的描述 3. 增加 SSH 登录说明 4. 增加工业协议配置章节	2022/06/01
V1.3	V200R005	更新联系地址和电话	2022/06/15
V1.4	V200R003	更新接口说明和网关设置说明(Gen 7)	2022/11/21
V1.5	V200R003	更新协议门户登录和配置说明	2023/02/27

目录

前言

感谢购买 G335 工业网关（“网关”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/程序员
- 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排版的准确性，但万创对因本手册的任何错误或特性造成的，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：48434 Milmont Drive, Fremont, CA 94538

电话：(650) 422-3128

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
- PTCRB

请查阅**附录 A** 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。
ℹ	提示重要信息或法规。

一般安全说明

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 6-36V 直流电源供电。上电前，请确认产品接入了直流电。

⚠ 产品有一块锂离子纽扣电池，可以在临时掉电的情况下，向实时时钟供电。避免产品从高空掉落或将产品置于高温环境，此类情况可能导致电池短路并导致爆炸。

⚠ 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(FCC)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。

第一章

硬件说明

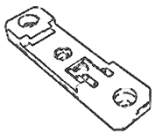
1.1 产品概述

万创 G335 边缘计算网关是成都万创科技股份有限公司为应对不同工业场景中机器对机器交流（M2M）和工业物联网应用的需求而推出的旗舰网关产品。产品支持多种工业协议，可接入现场工业设备如 PLC、控制器及传感器等。同时支持边缘计算，在物联网边缘节点实现数据优化，减少现场与中心端的数据量。支持标准 MQTT 协议，可接入广泛的工业数据平台，助力工厂数字化转型。

产品采用工业化设计，保证其质量和可靠性，是理想的物联网应用解决方案。支持各种无线通信网络，包括 3G/4G/LTE 数据通信、WLAN、GPS、ZigBee、LoRa、蓝牙。而且可接入万创自研的 BlueSphere 云平台，实现统一管理。通过实时监测和追踪、OTA 升级、远程维护、任务分配与跟踪等功能，用户足不出户，在中心端即可运筹帷幄。

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 G335 网关		1 x 电源适配器
	1 x Wi-Fi 天线		1 x 电源转接线
	1 x 导轨安装支架		1 x 4G LTE 天线
/	/		1 x ZigBee 天线
/	/		1 x GPS 天线

以上配件取决于用户的选配规格，实际情况可能略有不同。

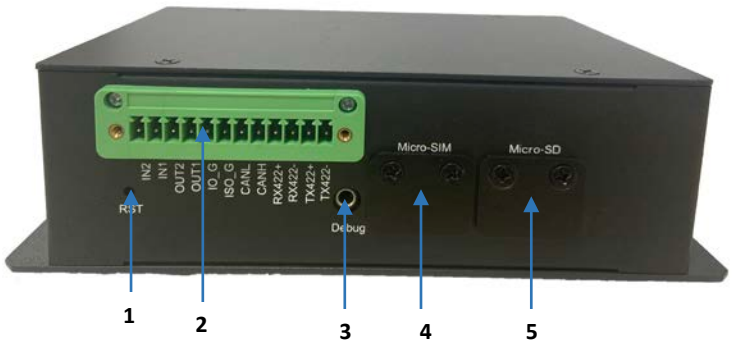
1.3 规格

G335		
系统	CPU	TI, AM335x, ARM Cortex-A8, 32‑Bit, 1GHz
	内存	512MB
	存储	8GB 1 x Micro SD 卡
通信	以太网	2 x 千兆以太网口（其中一个网口可支持 PoE）
	4G/LTE	1 x PCIe 插槽用于 4G 模块，支持 CAT 1 和 CAT 4
	Wi-Fi 及蓝牙	Wi-Fi 802.11 a/b/g/n/ac + 蓝牙 5.0
	射频模块	ZigBee 模块（可选）
	GPS	GPS 模块（可选）
输入/输出	串口	1 x RS232，用于调试 1 x RS232/RS485（DB9） 1 x RS232/RS485/RS422（接线端子预留）
	USB	1 x USB Type-C
	GPIO	2 x 输入，2 x 输出，带隔离（可选）
	报警器	1 x 蜂鸣器（可选）
	RTC	支持
	CAN	1 x CAN 2.0b（接线端子预留）
系统控制	按键	1 x 重置键 1 x 更新键
	LED	1 x 电源指示灯 1 x 状态指示灯
机械	尺寸	155mm x 105mm x 50mm（壳体） 177mm x 105mm x 50mm（带安装支架）
	壳体	金属
	安装方式	导轨安装
	IP 防护等级	IP30
	散热方式	无风扇散热
电源	输入	6-36V DC，支持过流保护，防接反保护
	电源端子	3 芯 3.81mm 凤凰端子
	功耗	平均 1.8W（不考虑无线模块功耗）
软件	操作系统	VantronOS
	软件开发包	支持
	网络管理	SNMP v1/v2c/v3
	设备管理平台	万创 BlueSphere 平台
	第三方平台	MQTT
	IPK 导入	支持
	界面语言	中文和英文（默认） 其他语言（可选）
	NTP	支持
	日志	支持

安全	防火墙	支持
	数据安全	OpenVPN、L2TP、PPTP、IPSec
	配置模式	本地、远程
	升级	本地升级、OTA 升级
	配网指引	LTE、Wi-Fi 和以太网一键配置
	流量统计	每月/每周/每天
	IP 应用	Ping、Traceroute、Nslookup
	IP 路由	静态路由
	网络地址转换	支持
	链路在线检测	发送心跳包检测，断线自动连接
	网络可靠性	支持故障切换，有线、Wi-Fi、4G/LTE 通讯互为备份
	多级权限	支持
工业协议	工业协议	Modbus TCP、Modbus RTU、EtherNet/IP、ISO-on-TCP、CC-link 等
边缘计算	边缘计算	JavaScript, MicroPython
用户可编程项目	开发语言	C/C++/Python/Node-Red/Node JS
环境条件	温度	工作温度：-20℃ ~ +70℃ （可选：-40℃ ~ +85℃） 存储温度：-40℃ ~ +85℃
	湿度	相对湿度 5%-95%（无凝露）
	认证	UL、CE、FCC、PTCRB

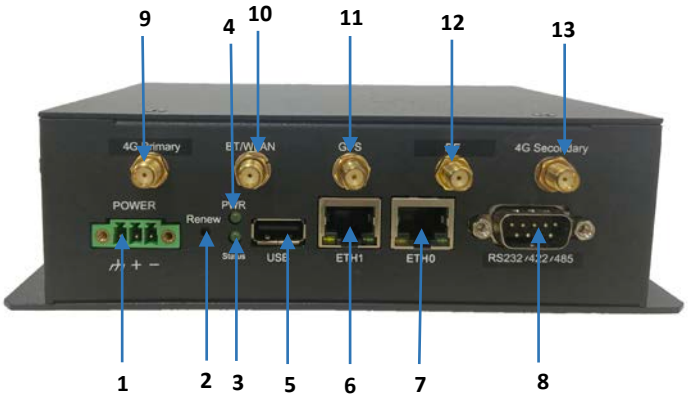
1.4 接口定义

1.4.1 前视图



编号	名称	说明
1	复位键	短按此键可以重置网关并重启
2	接线端子	接线端子引脚说明详见 1.5 串口说明
3	调试接口	
4	Micro SIM 卡槽	
5	Micro SD 卡槽	

1.4.2 后视图

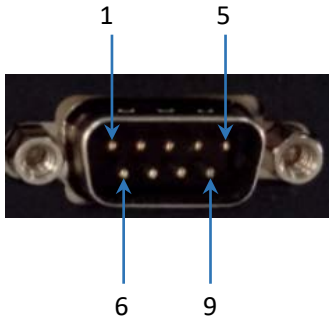


编号	名称	说明
1	电源端子	12V DC 电源端子
2	更新键	1.如果将系统升级驱动插入 SD 卡槽或 USB 接口中，按下此键约 2 秒，系统将会升级，同时蜂鸣器会触发 3 秒。 2.按下此键 3-10 秒，网关将恢复出厂设置，所有的用户数据和自定义配置都清除，同时蜂鸣器会触发 1 秒。 3.按下此键超过 10 秒，将格式化用户分区并清除用户分区数据，蜂鸣器会以 200 毫秒的间隔在 4 秒内发出蜂鸣音。
3	状态指示灯	1.网关启动时，指示灯闪烁。 2.启动完成后，指示灯变为绿色常亮。 3.升级系统或清除配置时，指示灯闪烁。
4	电源指示灯	网关通电后，指示灯常亮。
5	USB 2.0 Type-C	
6	ETH 1	在 VantronOS 中显示为 ETH1,且默认在 WAN 区工作
7	ETH 0	在 VantronOS 中显示为 ETH0,且默认在 LAN 区工作
8	串口	RS232/RS485 (DB9 连接器)
9	4G 主天线	
10	蓝牙/WLAN 天线	
11	GPS 天线	
12	ZigBee 天线	
13	4G 分集天线	

1.5 串口说明

1.5.1 DB9 连接器

DB9 串口连接器可以复用为 RS232 或 RS485。



引脚说明：

引脚编号	信号	节点	接口	类型	说明
1	RS485-A	/dev/ttyO4	UART1		RS485 A 信号
2	RS485-B / RS232RXD			I	RS485 B 信号 / RS232 接收信号
3	RS232TXD			O	RS232 发送信号
4	NC				
5	GND			P	GND
6	NC				
7	NC				
8	NC				
9	NC				

开启串口 RS232 模式并通过串口通信工具（如 microcom）打开串口：

```
~# gpio set uart1 rs232 save
或者
~# gpio set uart1 rs232
~# gpio get uart1
rs232

~# microcom /dev/ttyO4 -s 115200
```

开启串口 RS485 模式并通过串口通信工具（如 microcom）打开串口：

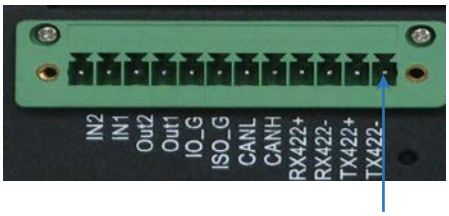
```
~# gpio set uart1 rs485 save

~# microcom /dev/ttyO4 -s 115200
```

上述命令行中的“**save**”为可选项。将该配置设置为默认值时，重启设备后依然有效。

1.5.2 接线端子

接线端子上部分引脚复用为 RS232、RS485 和 RS422。



引脚说明：

引脚编号	信号	节点	接口	类型	说明
1	TX422-	/dev/ttyO1	UART0		
2	TX422+				
3	RX422- / RS485_2_B / SRXD3			跳线帽配置	
4	RX422+ / RS485_2_A / STXD3			跳线帽配置	
5	CANH				
6	CANL				
7	ISO_GND			P	GND
8	IO_GND			P	GND
9	GPIO_OUT1			IO	
10	GPIO_OUT2			IO	
11	GPIO_IN1			IO	
12	GPIO_IN2			IO	

不同的串口模式可能具有不同的跳线连接方式。

如需开启 RS232 模式，请拆开顶盖，取出 JP2、JP3 和 JP4 跳线帽，然后通过串口通信工具（如 microcom）打开串口：

```
~# gpio set uart0 rs232 save
或者
~# gpio set uart0 rs232

~# gpio get uart0
rs232

~# microcom /dev/ttyO1 -s 115200
```

如需开启 RS485 模式，请拆开顶盖，取出 JP2 跳线帽并保留 JP3 和 JP4。然后输入以下命令启用 RS485 功能并通过 microcom 调试串口：

```
~# gpio set uart0 rs485 save

~# microcom /dev/ttyO1 -s 115200
```

如需开启 RS422 模式，请拆开顶盖，取出 JP2、JP3 和 JP4 跳线帽。然后输入以下命令启用 RS422 功能并通过 microcom 调试串口：

```
~# gpio set uart0 rs422 save

~# microcom /dev/ttyO1 -s 115200
```

上述命令行中的“**save**”为可选项。将该配置设置为默认值时，重启设备后依然有效。

1.6 CAN（可选）

根据接线端子的引脚说明，接线端子可以配置 CAN 总线接口。两台 G335 网关之间通过 CAN 协议进行通信的方法如下文所述。若您持有定制的 CAN 终端设备且支持特定的数据协议，需要万创在此基础上进行定制，请联系您的销售代表。

1. 准备两台 G335 网关，其物理连接应为：

网关 A		网关 B
CANH	<->	CANH
CANL	<->	CANL
发送数据	->	接收数据

2. 在网关 B 上运行“candump”命令并将波特率设置为 100000 (100kbps)至 1000000 (1000kbps)；

```
# ip link set can0 type can bitrate 100000
# ifconfig can0 up
# candump can0
```

3. 网关 A 发送数据；

```
# ifconfig can0 up
# cansend can0 5A1#11.2233.44556677.88
```

4. 数据将打印在网关 B 上。

1.7 GPIO（可选）

接线端子可以配置 GPIO 接口。请参考以下说明，启用 GPIO 接口。

名称	引脚编号
"gpio_in1" (gpio0_22)	22
"gpio_in2" (gpio0_26)	26
"gpio_out1" (gpio0_28)	60
"gpio_out2" (gpio0_8)	104

1. 向“/sys/class/gpio/export”写入 GPIO 的引脚编号，将该引脚导出。例如引脚 22：

```
~# echo 22 > /sys/class/gpio/export
```

2. 定义引脚方向为输入或输出（in 为输入，out 为输出）：

```
~# echo out > /sys/class/gpio/gpio22/direction
```

3. 如果在前述步骤中将方向设置为输出，则可以将 value（端口数值）设置为 0 或 1（对应“低”或“高”）：

```
~# echo 0 > /sys/class/gpio/gpio22/value
```
[设置为低]，或者

```
~# echo 1 > /sys/class/gpio/gpio22/value
```
[设置为高]

4. 读取 GPIO 值；

```
~# cat /sys/class/gpio/gpio22/value
```

5. 引脚使用完成后，取消导出。将引脚编号写入导出文件：

```
~# echo 22 > /sys/class/gpio/unexport
```

1.8 蓝牙

1. 打开并初始化 HCI 设备；

```
~# hciconfig hci0 up
```

2. 搜索或发现蓝牙设备（已发现蓝牙设备的 MAC 地址将显示在命令行下面）；

```
~# hcitool scan
```

3. 浏览目标蓝牙设备上的所有可用服务，并获取服务“OBEX Object Push”的通道值；

   例如，蓝牙设备“3C:CD:5D:36:9F:A6”上的所有服务如下所示，“OBEX Object Push”服务的通道值为 12。

```
# sdptool browse 3C:CD:5D:36:9F:A6
Browsing 3C:CD:5D:36:9F:A6 ...
Service RecHandle: 0x10000
Service Class ID List:
  "Generic Attribute" (0x1801)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 31
……
……
Browsing 3C:CD:5D:36:9F:A6 ...
Service Name: OBEX Phonebook Access Server
Service RecHandle: 0x1000a
Service Class ID List:
  "Phonebook Access - PSE" (0x112f)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 19
  "OBEX" (0x0008)
Profile Descriptor List:
  "Phonebook Access" (0x1130)
    Version: 0x0101



Service Name: OBEX Object Push
Service RecHandle: 0x1000b
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
```

```
   "L2CAP" (0x0100)
   "RFCOMM" (0x0003)
      Channel: 12
   "OBEX" (0x0008)
Profile Descriptor List:
   "OBEX Object Push" (0x1105)
      Version: 0x0102
……
……
```

如果网关不支持“OBEX Object Push”服务，请输入以下命令行：

```
~# sdptool add --channel = 12 OPUSH
```

4. 使用“obex_test”命令将测试文件发送到蓝牙设备：obex_test -b <蓝牙设备 MAC 地址> <通道>;

   例如，将测试文件发送至前述蓝牙设备：

```
# obex_test -b 3C:CD:5D:36:9F:A6 12
> c
[注：与蓝牙设备建立连接]

……
Connect OK!
【注：蓝牙设备已连接至网关。】

Version: 0x10. Flags: 0x00
> p /etc/usb-mode.json
【注：“p”后面的参数是待发送的测试文件的路径】

PUT file (local)> name=send.txt, size=9
PUT remote filename (default: send.txt)>
Going to send 9 bytes
……
PUT successful!
【注：测试文档已发送至蓝牙设备】

> q
【注：退出 obex_test】
```

5. 退出“obex_test”，启用页面和查询扫描，使目标蓝牙设备可以被发现；

```
~# hciconfig hci0 piscan
```

6. 启用 obexd 服务以接收文件:obexd -a -n -r <文件保存路径>；

   例如，测试文件的保存路径为“ /tmp”：

```
~# export
DBUS_SESSION_BUS_ADDRESS="unix:path=/var/run/dbus/system_bus_socket"
~# obexd -a -n -r /tmp/
```

7. 文件传输完成后，禁用页面和查询扫描，该蓝牙设备将不会再被发现。

```
~# hciconfig hci0 noscan
```

如果顺利完成上述步骤，则测试完成。

如需关闭 HCI 设备，输入以下命令行：

```
~# hciconfig hci0 down
```

如需将 HCI 设备重新命名（如“Bluez 5.21 test”），输入以下命令行：

```
~# hciconfig hci0 name “Bluez 5.21 test”
~# hciconfig hci0 down
~# hciconfig hci0 up
```

1.9 GPS（可选）

网关可以配置 GPS 模块。

1. GPS 模块上电：

```
~# gpio set gps on
```

2. 获取 GPS 数据：

```
# gps 9600 /dev/ttyS0
GPRMC,,V,,,,,,,,,,N*53
GPVTG,,,,,,,,,N*30
GPGGA,,,,,,0,00,99.99,,,,,,*48
GPGSA,A,1,,,,,,,,,,,,,99.99,99.99,99.99*30
GPGLL,,,,,,V,N*64
GPRMC,,V,,,,,,,,,,N*53
GPVTG,,,,,,,,,N*30
GPGGA,,,,,,0,00,99.99,,,,,,*48
GPGSA,A,1,,,,,,,,,,,,,99.99,99.99,99.99*30
GPGLL,,,,,,V,N*64
GPRMC,,V,,,,,,,,,,N*53
GPVTG,,,,,,,,,N*30
GPGGA,,,,,,0,00,99.99,,,,,,*48
GPGSA,A,1,,,,,,,,,,,,,99.99,99.99,99.99*30
GPGLL,,,,,,V,N*64
GPRMC,,V,,,,,,,,,,N*53
GPVTG,,,,,,,,,N*30
GPGGA,,,,,,0,00,99.99,,,,,,*48
GPGSA,A,1,,,,,,,,,,,,,99.99,99.99,99.99*30
GPGLL,,,,,,V,N*64
GPRMC,,V,,,,,,,,,,N*53
GPVTG,,,,,,,,,N*30
```

3. 关闭 GPS 模块：

```
~# gpio set gps off
```

1.10 ZigBee（可选）

1.10.1 ZigBee MGM12P 模块

1. ZigBee 模块上电：

```
~# gpio set zigbee3 on
```

2. 由于网关可选择两个模块版本，运行应用程序的命令行根据版本不同而不同，模块 V2.6 的指令为 **Z3GatewayHost -p /dev/ttyO3 -f x -b 115200**，模块 Silabe3.0 ZigBee（YEM001R077）的指令为 **Z3Gateway610 -p /dev/ttyO3 -f x -b 115200**。带有模块 V2.6 的网关序列号如下：PO110221-04-001, PO110221-04-002, PO110221-04-003, PO081321-23-MA-001, PO081321-23-MA-002, V5106-202110010-001。因此，序列号不在上述范围内的网关运行应用程序的指令如下：

```
~# Z3Gateway610 -p /dev/ttyO3 -f x -b 115200
Reset info: 11 (SOFTWARE)
ezspSetupSerialPort: bps:115200 stopBits:1 rtsCts:0
ezspSetupSerialPort: bps match 115200(8)<->115200
ezspSetupSerialPort: serialPort:/dev/ttyO3
ezspSetupSerialPort:SUCCESS
ezsp ver 0x08 stack type 0x02 stack ver. [6.10.3 GA build 297]
Ezsp Config: set address table size to 0x0002:Success: set
Ezsp Config: set TC addr cache to 0x0002:Success: set
Ezsp Config: set MAC indirect TX timeout to 0x1E00:Success: set
Ezsp Config: set max hops to 0x001E:Success: set
Ezsp Config: set tx power mode to 0x8000:Success: set
Ezsp Config: set supported networks to 0x0001:Success: set
Ezsp Config: set stack profile to 0x0002:Success: set
Ezsp Config: set security level to 0x0005:Success: set
Ezsp Value : set end device keep alive support mode to 0x00000003:Success: set
Ezsp Policy: set binding modify to "allow for valid endpoints & clusters only":Success: set
Ezsp Policy: set message content in msgSent to "return":Success: set
Ezsp Value : set maximum incoming transfer size to 0x00000052:Success: set
Ezsp Value : set maximum outgoing transfer size to 0x00000052:Success: set
Ezsp Config: set binding table size to 0x0010:Success: set
Ezsp Config: set key table size to 0x0004:Success: set
Ezsp Config: set max end device children to 0x0020:Success: set
Ezsp Config: set aps unicast message count to 0x000A:Success: set
Ezsp Config: set broadcast table size to 0x000F:Success: set
Ezsp Config: set neighbor table size to 0x0010:Success: set
NCP supports maxing out packet buffers
Ezsp Config: set packet buffers to 72
```

```
Ezsp Config: set end device poll timeout to 0x0008:Success: set
Ezsp Config: set zll group addresses to 0x0000:Success: set
Ezsp Config: set zll rssi threshold to 0xFFD8:Success: set
Ezsp Config: set transient key timeout to 0x00B4:Success: set
Ezsp Endpoint 1 added, profile 0x0104, in clusters: 8, out clusters 19
Ezsp Endpoint 242 added, profile 0xA1E0, in clusters: 0, out clusters 1
HA Gateweay EUI64 = BC33ACFFFE71A457
MQTT Client Init
MQTT Client ID = gwBC33ACFFFE71A457
Found 0 files

MQTT not connected, message not sent: gw/BC33ACFFFE71A457/settings - {"ncpStackVersion":"6.10.3-297","networkUp":false}
MQTT not connected, message not sent: gw/BC33ACFFFE71A457/relays - {"relays":[]}
MQTT not connected, message not sent: gw/BC33ACFFFE71A457/devices - {"devices":[]}
Attempting to reconnect to broker
Z3Gateway610>MQTT connected to broker
MQTT connected, starting gateway heartbeat and command processing
Subscribing to topic "gw/BC33ACFFFE71A457/commands" using QoS2
Subscribing to topic "gw/BC33ACFFFE71A457/publishstate" using QoS2
Subscribing to topic "gw/BC33ACFFFE71A457/updatesettings" using QoS2

Z3Gateway610>
Z3Gateway610> network leave
# 命令说明：清除所有网络
Z3Gateway610> plugin network-creator start 1
# 命令说明：创建网络
Z3Gateway610> plugin network-creator-security open-network
# 命令说明：允许设备加入网络
Z3Gateway610> network change-channel 25
# 命令说明：将通道值设置为 25
Z3Gateway610> info
# 命令说明：查看当前通道的设置
```

3. 关闭 ZigBee 模块：

```
~# gpio set zigbee3 off
```

1.10.2 ZigBee Digi XB24C（XBee）模块

完成通信需要两个网关。XBee 模块可以自动设置 ZigBee 网络并相应地分配网络地址。

1. 模块上电：

```
~# gpio set zigbee on
```

2. 将模块连接到"/dev/ttyO3"，将 AT 命令写入 tty 设备中（关于 AT 命令的详情，请参考 Digi XBee S2C 的数据手册）。

3. 设置其中一台网关设备作为协调器（默认为路由模式），并输入字符串 "Hello world"：

```
~# at 9600 /dev/ttyO3
+++OK
atce 1
atnd
…….（显示路由信息；如果无法加入网络，则显示错误信息）
atdh 0
OK
atdl ffff
OK
atcn
OK
Hello world!
```

4. 另一台网关为路由模式，该网关将显示"Hello world"字符串：

```
~# at 9600 /dev/ttyO3
+++OK
atnd
…….（显示路由信息；如果无法加入网络，则显示错误信息）
atdh 0
OK
atdl ffff
OK
atcn
OK
Hello world!
```

上述示例中使用的 ZigBee AT 命令：

AT 命令	说明
+++	切换至 AT 命令模式
atmy	响应网络地址
atce 1	设置为协调器（1 为协调器，0 为路由）
atdh 0	设置高地址为 0x00000000
atdl ffff	设置低地址为 0x0000ffff
atnd	响应路由表
atcn	退出 AT 命令模式

5. 关闭 ZigBee 模块：

```
~# gpio set zigbee off
```

1.11 3.5mm 调试接口

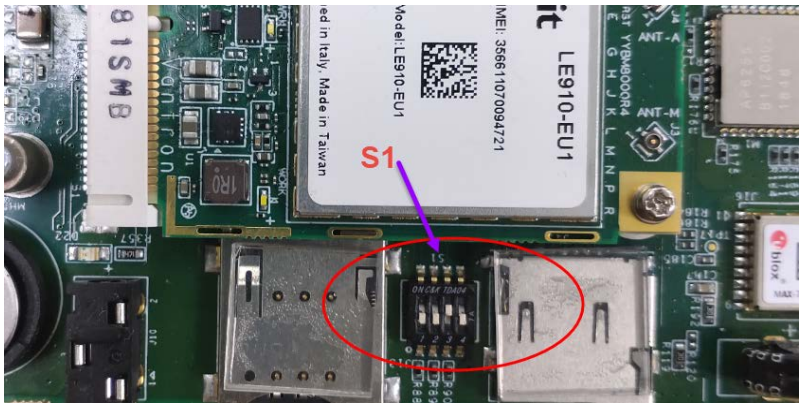
引脚编号	说明
引脚1	GND
引脚2	TXD (RS232)
引脚3	RXD (RS232)

1.12 系统启动

系统默认从 eMMC 启动。

1.12.1 从 SD 卡启动系统并刷新 eMMC

1. 打开网关盒子；
2. 将 DIP 开关 S1 设置为关:关:开:关，如下图所示；



3. 制作 SD 卡/U 盘启动盘；
   1) 将 SD 卡/U 盘插入 Linux 主机，使用 dmesg 命令获得 SD 卡/U 盘的设备路径（例如：/dev/sdb）；
   2) 输入以下命令行将万创发送的镜像文件包解压：

      unzip XOS_sd2mmc_VT-M2M-G335S_“version number”.zip

   3) 用户解压后将获得如下文档：

      ├── build.date //镜像创建日期

      ├── sd2emmc.sh //SD 卡启动制作脚本

      ├── XOS_sd2mmc_VT-M2M-G335_V200R001.F0000-03.img //启动镜像

      ├── XOS_sd2mmc&sdAutoUpgrade_VT-M2M-G335_V200R003.F0000-03.sha256sum //sha256sum 文件

      └── XOS_sdAutoUpgrade_VT-M2M-G335S_V200R003.F0000-03.img.gz//升级镜像

   4) 以 root 用户运行以下命令，制作 SD 卡启动盘：

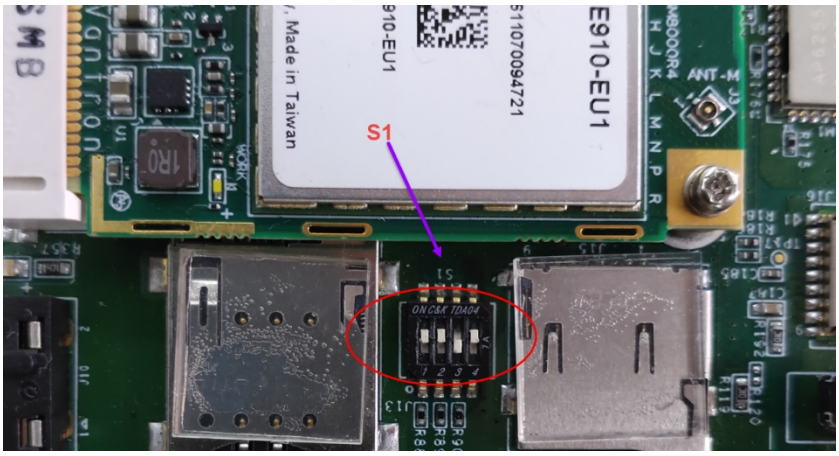
      sudo ./sd2emmc.sh /dev/sdb

- 使用正确的 SD 卡路径替换 **/dev/sdb**。
- 制作程序完成的消息弹出前拔出 SD 卡会导致制作失败。
- 若制作过程中提示失败，则可拔下 SD 并重新执行上述命令。

4. 将 SD 卡插入卡槽；
5. 网关上电。系统启动完成后，蜂鸣器将以 200 毫秒的间隔持续鸣响 10 秒，eMMC 刷机完成。

1.12.2 从 eMMC 闪存启动系统

1. 打开网关盒子；
2. 如下图所示，将 DIP 开关 S1 设置为开:开:关:开；



3. 网关上电。系统从 eMMC 启动后，蜂鸣器会鸣响 1 秒。

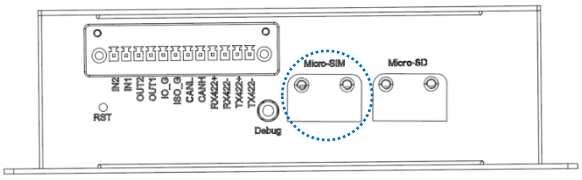
第二章

快速开始

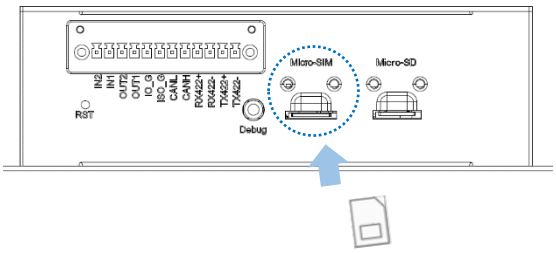
2.1 设置网关

配置网关前，需执行以下步骤完成产品硬件连接。

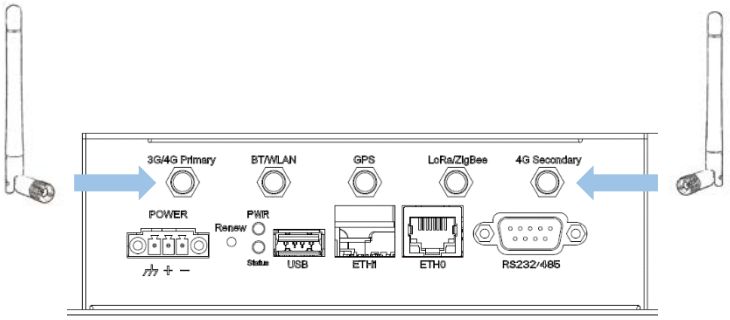
1. 使用提供的安装支架和螺丝将网关安装在安全处；
2. 松开网关侧面 SIM 卡盖板上的螺丝；



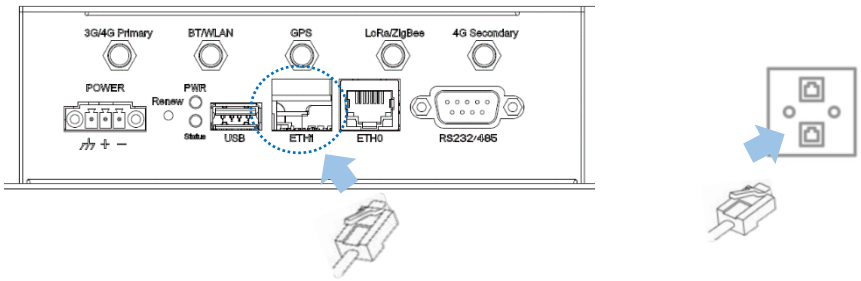
3. 金属芯片朝下，将激活的 Micro SIM 卡插入卡槽；



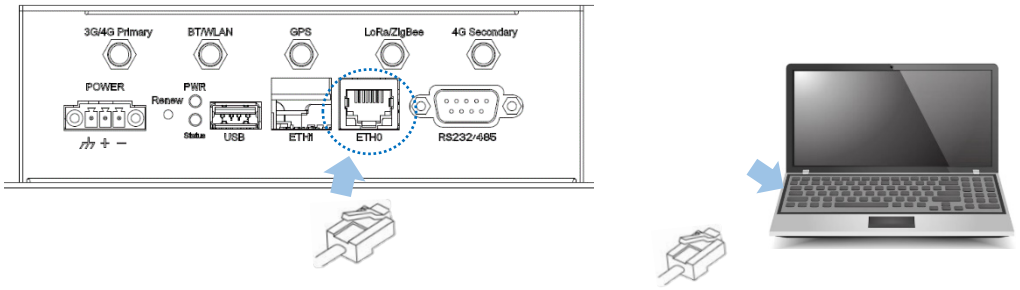
4. 推动 Micro SIM 卡将其固定；
5. 放回 SIM 卡盖板，使用螺丝刀紧固卡板；
6. 按照安装 Micro SIM 卡的步骤松开 SD 卡盖板；
7. 金属排针朝下，将 Micro SD 卡插入卡槽，然后按照前述步骤放回 SD 卡盖板并紧固卡板；
8. 将天线与天线接头相连接，并紧固接头；



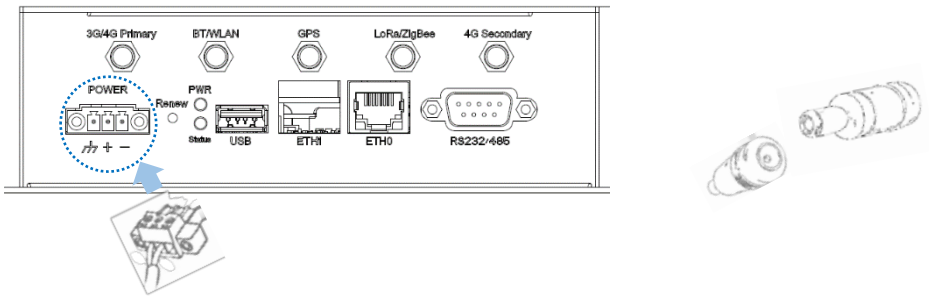
9. 将网线的一端连接至网关 ETH1（WAN）口，另一端连接至外网接口；



10. 将另一条网线的一端连接至网关 ETH0（LAN）口，另一端连接至个人电脑。某些情况下，网关上的网口丝印为 ETH1 和 ETH2，其功能分别对应上述的 ETH1 和 ETH0；



11. 将电源转接线的端子头接入网关的电源端子座，圆头的一端与电源适配器连接；



12. 将适配器插入符合网关工作电压要求（6V-36V）的直流电源插座，使网关通电；

13. 通电后，网关会发出“哔”声，电源指示灯和状态指示灯将显示为绿色常亮。

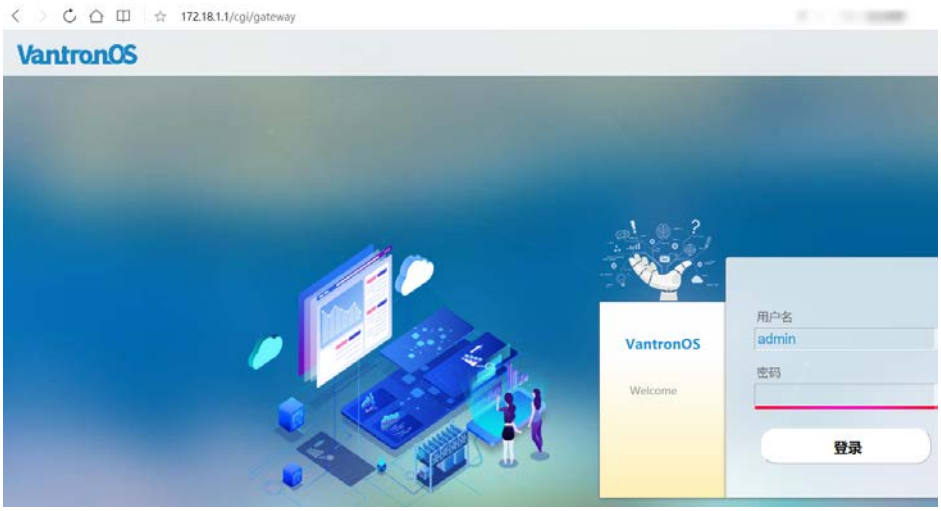
如果采用无线网络连接方式，则略过第 9、10 步。

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 登录网关

此网关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 界面完成网络设置，也可以进行个性化配置。

1. 在浏览器中输入以下默认地址登录 Vantron OS 网页界面 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. 进入 VantronOS 网页界面后，用户可以在该界面配置和变更网关设置。
3. 如需 SSH 登录，使用以下 IP 地址：172.18.1.1（默认）。
   - 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 登录功能默认关闭，如需开启，请根据 3.10.3 进行配置。

推荐使用最新的 Google Chrome 或火狐浏览器。

2.3 连接万创网关管理平台

BlueSphere GWM 是万创网关管理云平台，作为一个控制平台，该平台可以对多台网关/路由器进行分组管理，提供目标设备相关信息。如果网关/路由器支持数据采集/上传工业协议，用户还可以在该平台设置网关/路由器的数据采集任务、采集变量、上传规则等参数。

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
- 网关/路由器上已安装用于对接 BlueSphere GWM 的 DMP agent
- VantronOS 中 DMP agent 配置页面为“启用”状态（配置说明请参考 3.7.4 DMP Agent）
- 已将网关/路由器的序列号添加至 BlueSphere GWM

2.4 网络连接

当网关连接网络时，状态页将显示如下。

2.4.1 以太网连接

用户无需额外配置，使用默认的 WAN 设置即可将网关接入目标以太网。

网关默认使用 DHCP 协议下发 IP 地址、子网掩码、默认网关地址和域名（DNS）服务器地址。如果将 DCHP 协议切换为静态协议，则需要手动设置上述所有 IP 地址。

2.4.2 Wi-Fi 连接

网关可以设置为客户端（client）模式和接入点（AP）模式。

无线网络的高级设置请参考 3.5.2 无线(WIFI)。

2.4.3 移动网络连接

若客户使用 SIM 卡为网关提供网络连接，可以通过**网络**标签下的 4G/LTE 功能更改移动网络的设置。配置 4G/LTE 网络前，请确保 SIM 卡已激活且正确安装在网关上。

移动网络的高级设置请参考 3.5.3 4G/LTE。

2.5 自定义设置

由于万创提供软件开发工具包(SDK)，用户可以将脚本或程序上传至网关，设置为开机运行。也可以开发和编译 IPK 工具包，并上传至网关。

定制套件和程序的高级设置请参考 3.7 客制应用。

第三章

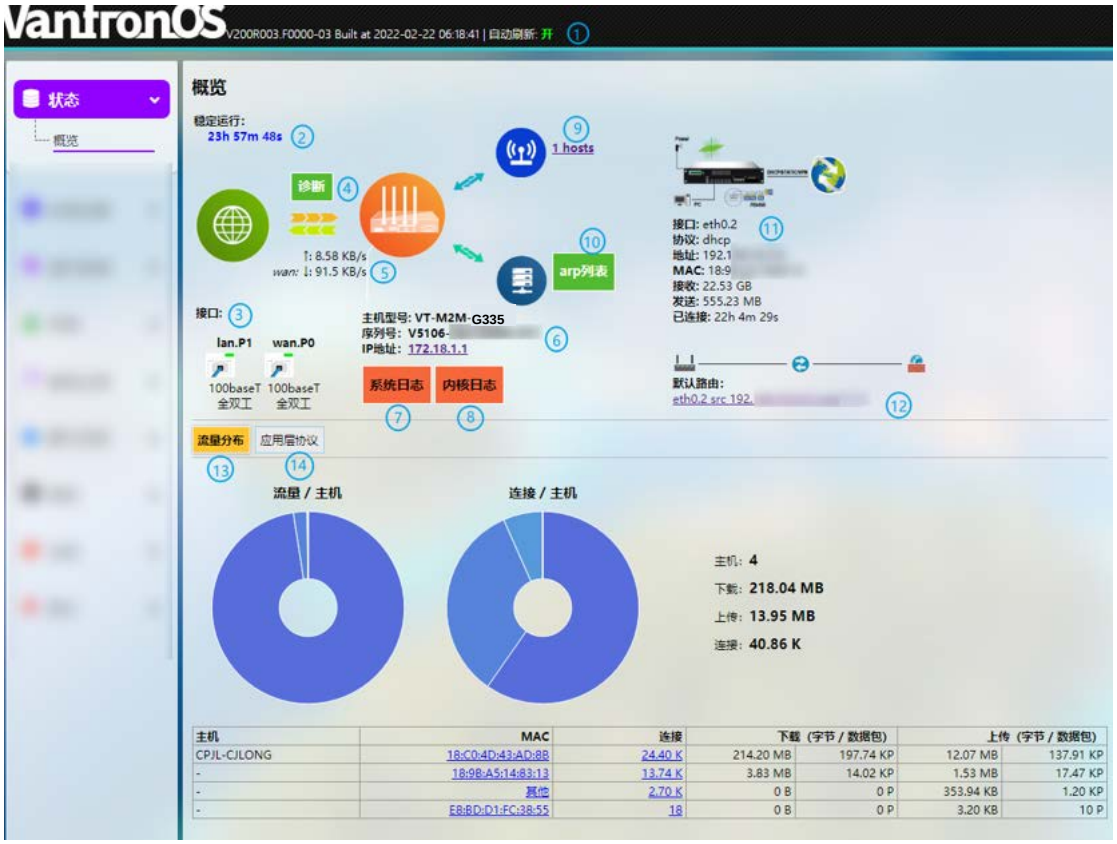
VantronOS 页面配置网关

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 网关管理平台、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。

3.2 状态

该页面呈现了网关的整体信息，包括稳定运行时间、通过无线或有线连接接入网关的设备数量、默认路由、硬件信息、流量统计等。



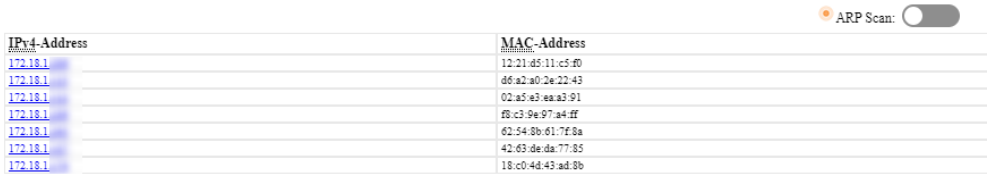
编号说明

1. 固件版本和自动刷新打开/关闭
2. 联网后网关的稳定运行时间
3. 当前网口的工作状态
4. 网络诊断工具集
5. 即时默认出口流量
6. 当前所使用网关的型号、序列号、IP 地址
7. 系统日志信息
8. 内核日志信息
9. 通过 WiFi 连接网关的子设备数量

> 点击该数字即可进入 Wi-Fi 设置。

10. 连接至网关的子设备地址信息

> 默认禁用 ARP 扫描。可以点击 **arplist** 图标并在弹窗中切换至 ARP 扫描来启用该功能。



11. 接入口详情

> 当网关连接移动数据时，图片展示将有所不同。

12. 网关当前使用的默认路由

13. 连接网关的子设备按 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、POP3S 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 快速设置

3.3.1 快速联网

该页面简要说明了网关快速配网以及网口状态和接口逻辑图的展示。高级设置请参考 3.5.1 接口。

使用网络安装向导将清除自定义的配置参数。

关于接口的说明，请参考 1.4 接口定义。

3.3.2 WAN 设置– 自动获取 DHCP

DHCP 动态 IP：**ETH0** 和 **WLAN0**（AP 模式下）绑定网桥（br-lan）。**ETH1** 为 WAN 口，连接上层网络。

自动获取 DHCP 设置流程：

第 1 步：选择 **DHCP** 作为 **WAN 协议**；

第 2 步：点击按钮将协议切换为 **DHCP**；

第 3 步：点击保存 & 应用。

切换 WAN 协议会将网络接口拓扑和网络参数重置为默认值。

3.3.3 WAN 设置 – 客户端 Client

客户端 **Client**：**ETH0** 和 **ETH1** 绑定网桥（br-lan）。**WLAN0**（client 模式下）作为 WAN 口。

客户端 Client 设置流程：

第 1 步：选择**客户端 Client** 作为 **WAN 协议**；

第 2 步：点击按钮将协议切换为**客户端 Client**；

第 3 步：选择网关需要连接的 Wi-Fi 网络；

第 4 步：如果未识别到目标 Wi-Fi，点击**重新扫描周边 Wi-Fi 信号**，刷新 Wi-Fi 列表；

第 5 步：选择待连接 AP 的 MAC 地址（如果不确定，保留“Auto”）；

第 6 步：输入目标 Wi-Fi 的密码；

第 7 步：确认 Wi-Fi 网络是否可以连接。如果不行，选择 **No**;

第 8 步：选择 IP 寻址协议（默认为 DHCP 协议）；

第 9 步：点击保存 & 应用。

3.3.4 WAN 设置– 4G/LTE

在进行 4G/LTE 配置前，请确保已将激活的 SIM 卡插入了卡槽，并且已安装 LTE 天线。高级设置请参考 3.5.3 4G/LTE。

4G/LTE: ETH0、ETH1 和 WLAN0（**AP** 模式下）绑定网桥（br-lan）。一般情况下，如果网关使用普通 4G 模块，协议下显示的 4G/LTE 通讯设备名称为“3g-4g”，作为 WAN 口。使用万创提供的运营商预认证 4G 模块时，协议下显示的 4G/LTE 通讯设备名称为“eth2”，作为 WAN 口。

4G/LTE 设置流程：

第 1 步：选择 **4G/LTE** 作为 **WAN 协议**；

第 2 步：点击按钮将协议切换为 **4G/LTE**；

第 3 步：输入运营商提供的 SIM 卡 ICCID；

第 4 步：输入运营商提供的 **APN**，便于通过蜂窝数据连接网络；

第 5 步：输入运营商提供的用户名，用于 PAP/CHAP 验证；

第 6 步：输入运营商提供的密码，用于 PAP/CHAP 验证；

第 7 步：点击**保存 & 应用**。

若不适用，请保留字段原样。

仅当运营商使用用户名和密码设置 APN 时，才需要指定 PAP/CHAP 用户名和密码。

3.3.5 WAN 设置 – 宽带拨号 PPPOE

PPPOE：ETH0 和 WLAN0 绑定网桥（br-lan）。**ETH1** 为 WAN 口，连接上层网络。

宽带拨号 PPPOE 设置流程：

第 1 步：选择**宽带拨号 PPPOE** 作为 **WAN 协议**；

第 2 步：点击按钮将协议切换为宽带拨号 PPPOE；

第 3 步：输入用户名，用于 PAP/CHAP 验证；

第 4 步：输入密码，用于 PAP/CHAP 验证；

第 5 步：点击保存 & 应用。

3.3.6 WAN 设置 – 静态地址 Static

静态地址 Static：ETH0 和 WLAN0 绑定网桥（br-lan）。**ETH1** 为 WAN 口，连接上层网络。

静态地址 Static 设置流程：

第 1 步：选择**静态地址 Static** 作为 **WAN 协议**；

第 2 步：点击按钮将协议切换为**静态地址 Static**；

第 3 步：指定 IPv4 地址；

第 4 步：指定子网掩码；

第 5 步：指定 IPv4 网关；

第 6 步：指定 IPv4 广播；

第 7 步：设置 DNS 服务器；

第 8 步：点击**保存 & 应用**。

若不适用，请保留字段原样。

3.3.7 自动线路

自动线路的特征如下：

- 连接单个 4G 网口时，启动心跳检测；
- 设备有多个 WAN 口时，用户可以根据网关跃点优先级指定数据接口。其中一个接口掉线时，可以通过自动路由切换至其他可用的接口。掉线的接口恢复并重新上线时，可以自动重新连接互联网；
- 插入/拔下网口时，启动自动识别并自动添加检测到的网口。

编号说明

1. 路由跟踪的相关接口
2. 启用/禁用路由跟踪
3. 网关跃点设置（数值越小，优先级越高）
4. 检查间隔，为一次跟踪完成至下一次跟踪开始之间的时间
5. 可追踪的 IP（心跳服务器）

> 使用空格键隔离多个 IP 地址。如果没有网络连接或者没有专用网络，可以将检测 IP 设置为上层网关的 IP 地址。

6. 修改规则
7. 删除规则
8. 所跟踪接口的状态信息

9. 接口跟踪日志，最新信息位于底部

10. 保存 & 应用所做更改

点击接口后面的**修改**按钮，进入规则修改页面。

编号说明

1. 启用/禁用路由跟踪
2. 选择路由跟踪的接口
3. 网关跃点设置（数值越小，优先级越高）
4. 单次跟踪失败允许的最大尝试次数
5. 单次跟踪失败允许的最长尝试时间
6. 在线接口的数量

> 如果跟踪成功，接口则视为在线。

7. 离线接口的数量

> 如果跟踪失败且确认数量达到/超过预设值，该接口将视为离线。

8. 检查间隔，为一次跟踪完成至下一次跟踪开始之间的时间
9. 可追踪的 IP（心跳服务器）

> 使用空格键隔离多个 IP 地址。如果没有网络连接或者没有专用网络，可以将检测 IP 设置为上层网关的 IP 地址。

10. 保存 & 应用上述设置

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。网关支持 OpenVPN、L2TP、PPTP、IPSec 等 VPN 协议，保证数据隐私且不受干扰。

用户可以根据需要，将网关配置为 OpenVPN 服务器或者客户端。

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. 启动服务器；
3. 选择协议；

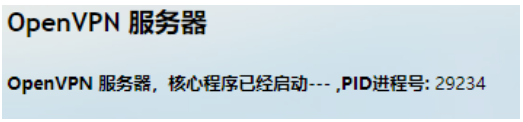
TCP 提供从用户到服务器的有序数据传递（反之亦然），UDP 不专门用于端到端的通信，也不检查接收端的准备情况。

4. 选择 **tap** 或 **tun** 工作模式；

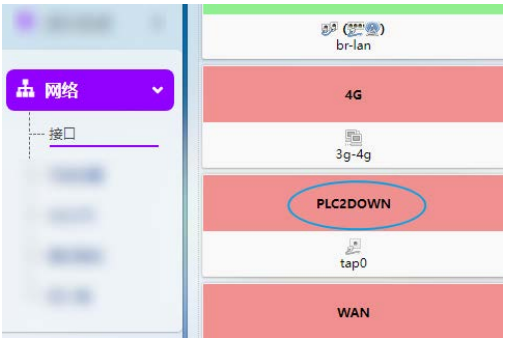
Tap 可以桥接不同位置的两个以太网段，所以如果您需要连接到远程网络（远程桌面、PLC、控制器等），请使用 **tap**。如果你只需要网络连接，则使用 **tun**。

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. 输入向客户端推送的**扩展配置**；
9. 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）；
10. 保存并应用上述设置；
11. 配置完成后，运行状态将如下图所示。



服务器设置完成后，会自动添加 PLC2DOWN 接口，用户可以做进一步配置和编辑。



3.4.2 VPN 客户端

如需将网关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。

启用 VPN 客户端之前，请将客户端时间与浏览器时间校准并同步。

编号说明

1. VPN 运行状态
2. 同步 VPN 时间与浏览器（本地）时间
3. 选择虚拟线路的出口协议（**OPENVPN** 和 **PPTP 两种协议可选**）
4. 点击按钮切换至该协议
5. 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。

6. 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。

7. 选择本地.ovpn 文件进行配置
8. 上传本地配置文件
9. 选择使用证书还是用户名及密码的方式作为鉴权方式
10. MTU 设置
11. 跃点数设置

> 跃点数值越小，优先级越高

12. 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，启动该机制

13. 输入自定义的 DNS 服务器
14. 保存 & 应用上述设置

3.5 网络

快速设置页面下的**快速联网**提供了网络快速设置通道，用户还可以在**网络**页面查看网配置详情并相应做出变更。

> 无论用户通过哪个界面改变网络设置，保存并应用当前设置后，之前的设置将被覆写。

3.5.1 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）

由于某些设备配置/未配置相关模块实现相应的接口功能，实际接口展示或与上图略有差异。

后文将对上述接口进行详细说明。

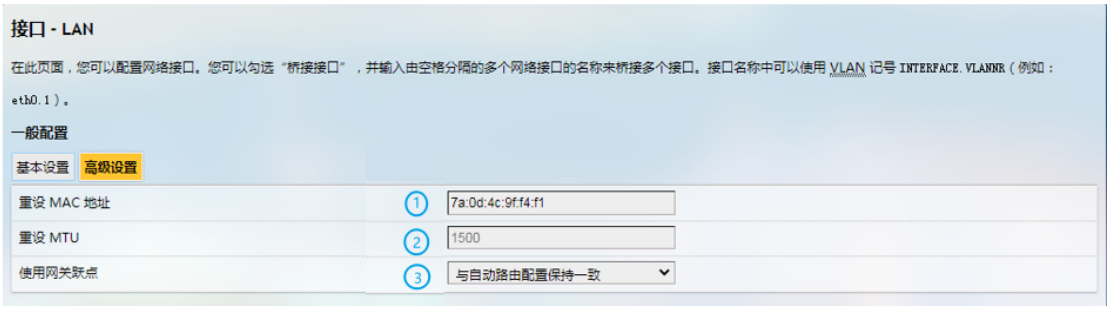
LAN

点击 **LAN** 后面的**修改**按钮，进入**一般配置**页面，然后点击**基本设置**。

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**：



编号说明

1. MAC 地址克隆
2. MTU 设置
3. 将网关跃点设置为与自动路由配置保持一致或者进行自定义设置

退出页面前，请保存设置。

如果以 root 用户登录 VantronOS（**密码：rootpassword**），则**高级设置**按钮旁会有一个**物理设置**按钮，用于桥接设置。

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

LAN – DHCP 服务器

一般配置页面下，通过 LAN 口的**基本配置**选项可以详细配置 DHCP 服务器：

编号说明

1. 禁用 DHCP 服务

   如果禁用 LAN 口 DHCP 服务，则不会为连接至网关的设备提供 DHCP 服务。

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

DHCP 服务器**高级设置**：

编号说明

1. 为所有客户端提供动态地址分配

如果禁用，将只对具有静态租约的客户提供服务。

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

一般根据所服务的子网计算

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**即返回接口设置页面。

4G

点击 4G 后面的**修改**按钮将转入 4G/LTE 配置页面。详情请参考 3.5.3 4G/LTE。

WAN

WAN 口的基本和高级设置均在此页面完成。

WAN – DHCP 客户端

WAN 口 DHCP 协议的基本设置如下。

编号说明

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

WAN 口 DHCP 协议的高级设置如下。

编号说明

1. 启用**使用默认网关**
2. 启用**使用对端通告的 DNS 服务器**
3. 使用网关跃点
4. MAC 地址克隆
5. 网络 MTU

退出页面前，请保存设置。

WAN – 静态地址

如需启用静态地址协议，在**基本设置**的下拉列表中选择**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。还需要添加自定义的 DNS 服务器。

- 若不适用，请保留字段原样。
- 选择静态地址协议后，DHCP 服务器将被自动禁用。
- 静态地址协议的高级设置与 DHCP 协议高级设置基本一致。

WAN – PPPoE

WAN 口的 PPPoE 协议基本设置和高级设置与上述协议的设置基本一致。点击**返回或刷新**即返回接口设置页面。

3.5.2 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。

Wi-Fi - AP 模式（基本设置）

编号说明

1. 设置网关的无线连接名称（SSID）

名称中不能含有$、`、\等符号。

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. 当前连接设备明细

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. 设置 Wi-Fi 国家代码
5. 点击切换国家

> 选项 2 和 4 的修改均对 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。

6. Wi-Fi 所属的网络接口

Wi-Fi – 客户端模式

当网关被设置为某个无线网络上的客户端时，通过下文页面可以变更网络设置。

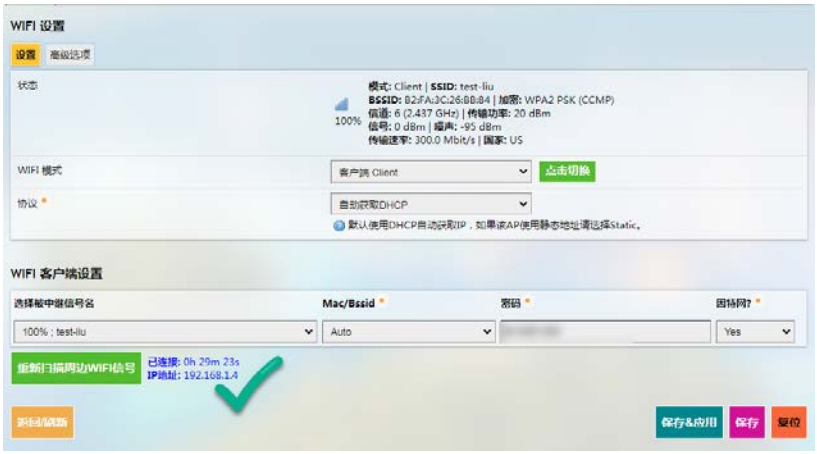
如果用户修改 3.3.3 WAN 设置 – 客户端 Client 下的设置，此页面的参数将被覆写。

如果将 Wi-Fi 配置为客户端模式，将自动添加 wwan0 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为网关指定 IP 地址
3. 选择待接入的无线网络（默认展示连接过的网络名称）
4. 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
5. 选择待连接 Wi-Fi 的 MAC 地址（如果不确定，保留“Auto”）；
6. 输入待连接 Wi-Fi 的密码
7. 确认待连接 Wi-Fi 有网络

当网关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。



3.5.3 4G/LTE

在进行 4G LTE 配置前，请确保已将激活的 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。

在**设置**项下，用户可以启用/禁用移动网络，并输入 APN 和用于 PAP/CHAP 鉴权的用户名和密码（如果运营商已预先设置）。

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. 当前 SIM 卡拨号失败的最大允许次数（仅适用于双 SIM 卡设备，最好保留字段原样）
2. 点击重新启动 4G 模块
3. 4G 模块断网后自动重启的时间
4. 选择 PDP 类型（保留字段原样）
5. 设置 CID 值
6. 默认 MTU 值（1500）

高级选项旁边的**运行日志**显示 4G 模块最近 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，并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。

3.5.4 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：当网关有 4G 和 WAN 网络接口时，内部服务器通过 WAN 口访问内部网络（192.168.0.0 - 192.168.255.254）。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。

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。数据包被丢弃，并生成主机不可访问的 ICMP 消息，本地发件人收到 EHOSTUNREACH 错误。
Prohibit	目的路由无法到达。数据包被丢弃，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。数据包被静默丢弃，本地发件人收到 EINVAL 错误。
Anycast	目的路由是分配给该主机的任何强制转换地址，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。

3.5.5 防火墙

防火墙 – 基本设置

以下是防火墙可以定义的配置项目。最低防火墙配置通常包含一个基本设置项、至少两个区域（LAN 和 WAN）和一个转发服务，以允许数据包从 LAN 口转发到 WAN 口。

基本设置定义不依赖于特定区域的防火墙全局设置。以下选项可以进行定义：

名称	类型	是否强制	默认值	说明
入站数据	字符串	否	接受	输入链默认策略（接受、拒绝、删除）
出站数据	字符串	否	接受	输出链默认策略（接受、拒绝、删除）
转发	字符串	否	拒绝	转发链默认策略（接受、拒绝、删除）

防火墙 – 区域设置

一个区域部分将多个接口和服务器分组，并充当转发、规则和重定向的源或目的地。出站流量的伪装（NAT）按区域进行控制。

编号说明

1. 唯一的区域名称

区域名字下至少应显示 LAN 口和 WAN 口。

2. 区域转发模型说明
3. 用于传入区域流量的默认策略（接受、拒绝、删除）
4. 用于传出区域流量的默认策略（接受、拒绝、删除）
5. 转发区域流量的默认策略（接受、拒绝、删除）
6. IP 动态伪装（NAT）
7. MSS 钳制
8. 修改区

点击接口后面的**修改**按钮将进入区域设置页面，在此可以进行基本设置、高级设置和转发规则的设置。

防火墙 – 端口转发

转发部分控制区域之间的流量，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，每个区域中的目的端口都反向。

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）

防火墙 - 自定义规则

自定义规则允许执行任意 Iptables 命令，而防火墙框架没有涵盖这些命令。在每次重新启动防火墙之后，即在加载默认规则设置之后，立即执行命令。

3.6 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。

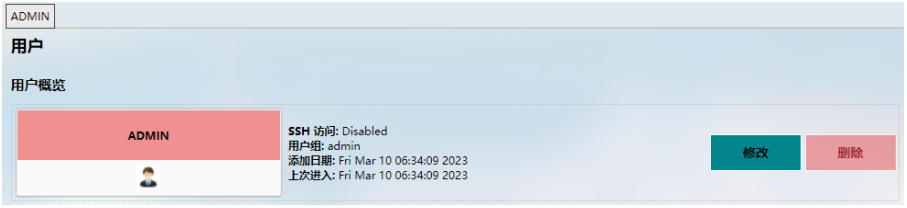
如需添加用户，请点击当前用户信息下面的添加按钮：

编号说明

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

退出页面前，请保存设置。

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。



3.7 客制应用

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

3.7.1 客制程序

客制程序允许用户将自己的脚本或程序（sh/bin）上载到网关，并设置为在启动时运行。

编号说明

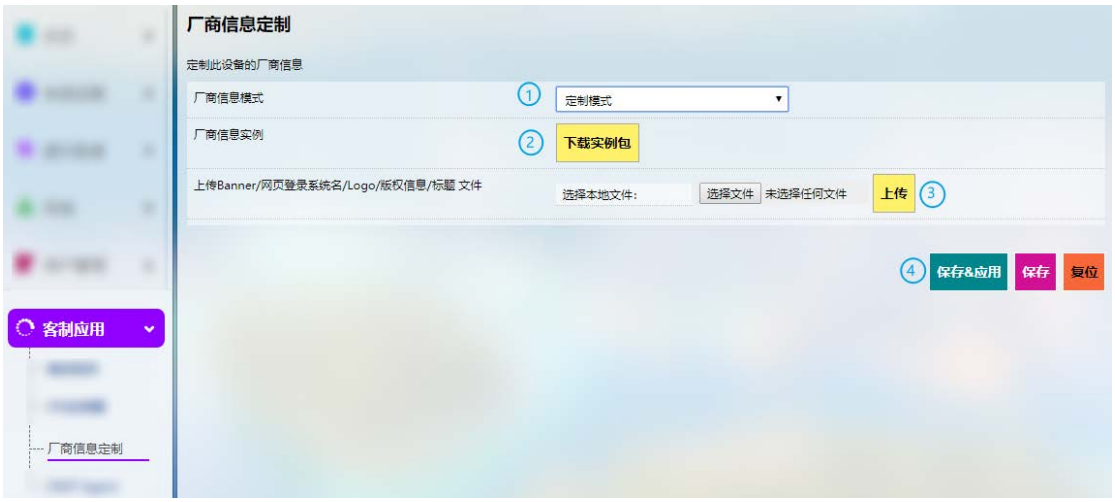
1. 选择要上传到网关的脚本
2. 上传脚本至网关
3. 保存 & 应用上述设置
4. 当脚本成功上传后，将显示文件名和文件目录
5. 启用该脚本，则该脚本将在下次启动网关时运行
6. 如果上传多个脚本，用户可以上下移动任意脚本，重新排列脚本顺序，并编辑/删除脚本

3.7.2 IPK 安装器

该页面允许客户将自己开发和编译的 IPK 软件包安装到网关。万创工业协议安装包也在该页面上传。关于工业协议的详细信息，请参考 4.2 协议配置与应用。

3.7.3 厂商信息定制

如需定制厂商信息，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
3. 根据需要修改示例包内的文件并逐个上传
4. 保存 & 应用上述设置

三种厂商信息模式解释如下：

万创模式：文件中所有信息都将展示万创相关信息。

中性模式：文件中的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：所有展示信息都是定制化信息。

3.7.4 DMP Agent

网关/路由器通过 DMP Agent 与 BlueSphere GWM 平台通讯。请参考以下说明，了解如何启用 DMP，从而实现网关/路由器的远程管理。

编号说明

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

如果其他条件满足(请参考 2.3 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. 用户可以在此自定义 Agent 的安装路径（默认安装路径为“/usr”）
5. 设置 Agent 服务器的下载地址（建议不做更改）
6. 检测服务器

如果网关恢复出厂设置，网关在 BlueSphere GWM 平台的状态将变为离线模式。如需重新激活网关，请在 VantronOS 页面点击**清空 Agent**，然后选择**启用** agent，等待一会儿后，网关将重新上线。

3.8 硬件

3.8.1 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。

3.8.2 Ser2net 环境搭建与验证

- 环境准备：
  - 一台 G335 网关
  - 一台运行 Ubuntu 系统的主机
  - 双母头 DB9 串口线
  - RS232 转 USB 串口线
  - 如下图所示，连接网关串口（DB9 为例）和主机

- 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， DB9 串口的点位为/dev/ttyO4）
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/ttyO4 -b 115200 -a 8 -r none -s 1 -o 20
```

(3) Ubuntu 主机端设置

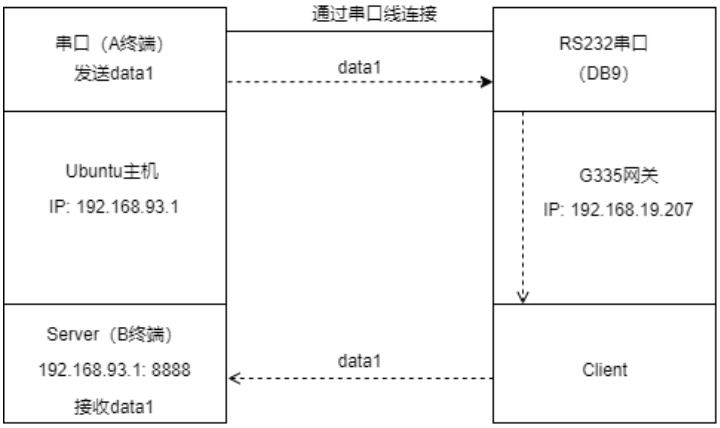
- 在 A 终端使用 microcom 工具命令打开串口（假设识别出 RS232 转串口适配器名为/dev/ttyUSB1）

```
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 Telnet 协议（协议区别见 3.8.3）
5. 选择串口设备（如 1.5 所述， DB9 串口的点位为/dev/ttyO4）
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”

设置完成后，**保存 & 应用**上述设置。

(2) Ser2net 运行进程如下：

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

(3) Ubuntu 主机端设置

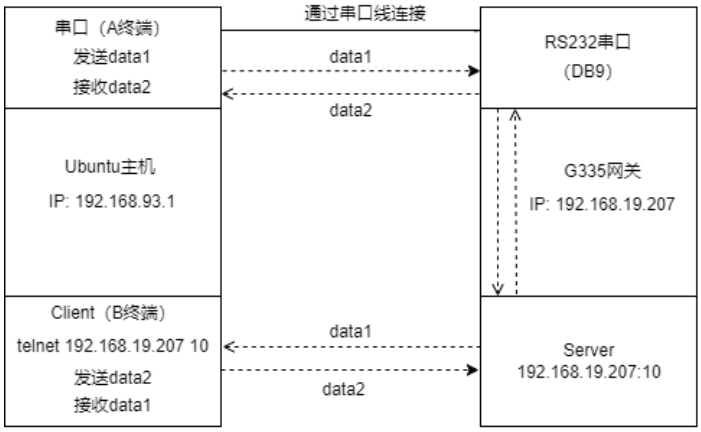
- 在 A 终端使用 microcom 工具命令打开串口（假设识别出 RS232 转串口适配器的设备名为/dev/ttyUSB1）

```
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



3.8.3 协议对比

在**服务器模式**下，存在三种协议，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) Rawlp：启用端口，并将所有输入数据传输给未进行任何 Termios 设置的网关，允许使用连接的/dev/lpx 设备和打印机。

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

3.9 服务

3.9.1 PLC 远程连接

如需通过 OpenVPN 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网关设备和一台控制主机，其中一台网关设备（G1）用于搭建 OpenVPN 服务器（设置参见 3.4.1 OpenVPN 服务器），另一台网关设备（G2）通过 VantronOS 中的 PLC 远程连接页面进行设置，连接 G1 配置的 OpenVPN 服务器（设置如下）。

编号说明

1. 下载并保存 G1 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 G2 连接 G1 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 G2 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。

此外，如需远程控制 PLC 设备，用户还需：

- 使用网线将 PLC 设备连接至 G2 的 LAN 口
- 在控制主机上安装 OpenVPN 客户端，连接 G1 配置的 OpenVPN 服务器；安装 PLC 控制程序，管理 PLC 的 IP 等设置

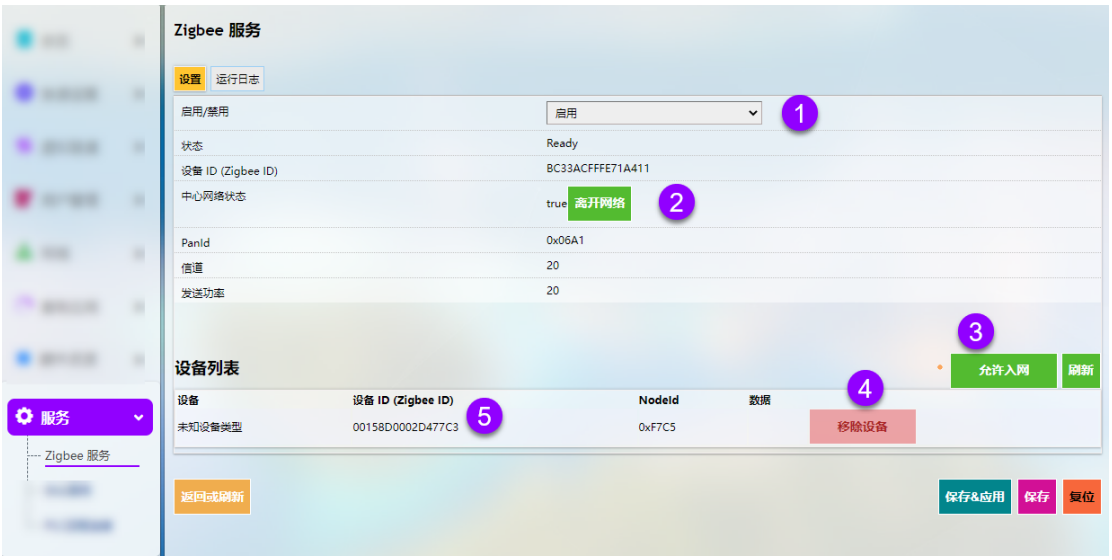
3.9.2 协议服务

若安装了工业协议相关.ipk 文件，以 root 账号登录后，可在 VantronOS 页面查看协议相关服务，其信息展示与万创工业协议端口页面展示一致。

请参考第四章内容了解工业协议的配置及应用。

3.9.3 ZigBee 服务

若网关配置了 ZigBee 模块，以 root 账号登录后，可在 VantronOS 页面创建 ZigBee 网络。



ZigBee 网络配置步骤：

1. 点击下拉选框，选择**启用** ZigBee 服务，并点击**保存&应用**；
2. 已添加 ZigBee 网络的情况下，页面显示如上图；如果未添加 ZigBee 网络，则点击**创建网络**；
3. 创建网络后，点击**允许入网**，开启入网通道，设备入网或者无设备入网达 180 秒，则将关闭入网通道；
4. 点击**移除设备**，可将入网设备移出 ZigBee 网络；
5. 连接 ZigBee 网络的设备信息。

3.10 系统

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

3.10.1 系统

编号说明

1. 同步网关时间与浏览器（本地）时间
2. 设置主机名称
3. 选择时区
4. 启用 NTP 在线时间调整
5. 启动 NTP 服务器（网关用作 NTP 时间服务器）
6. NTP 在线时间服务器

针对日志相关设置，请点击**基本设置**标签后面的**日志信息**。如需更改界面语言，请点击后面的**语言和界面**标签。

3.10.2 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

选项 1 选择“每月的某一天”时适用

3. 统计接口
4. 本地子网

高级设置页面中，每一个设置项均有详细解释，因此用户可以清楚如何进行相应设置。

协议映射可用于区分每台主机的流量类型。每条映射占据一行，第一个值指定 IP 协议类型，第二个值是端口号，第三个值是映射的协议名称。

3.10.3 管理权

在**主机密码**部分，用户可以重置网关访问密码。

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 账号和密码登录网关：

账号：**root**

密码：**rootpassword**

第 3 步：导航至**系统>管理权**，并启用 Dropbear；

编号说明

1. 选择访问端口（默认 LAN 口）

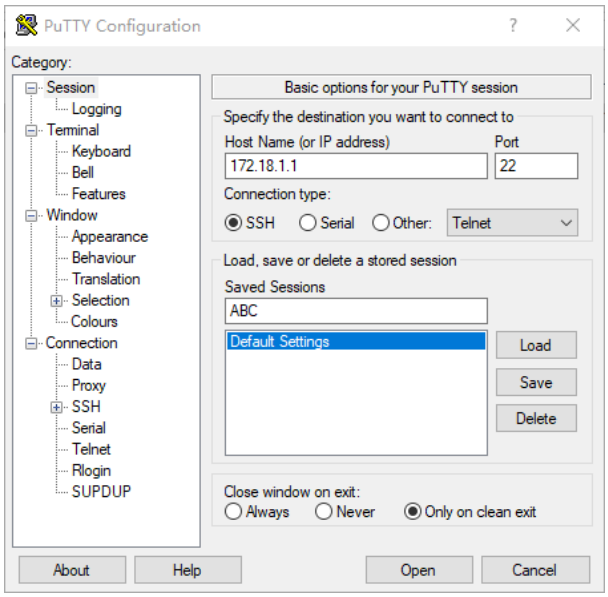
如果选择“未指定”，则所有端口都将被监视。

2. 指定监视端口（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

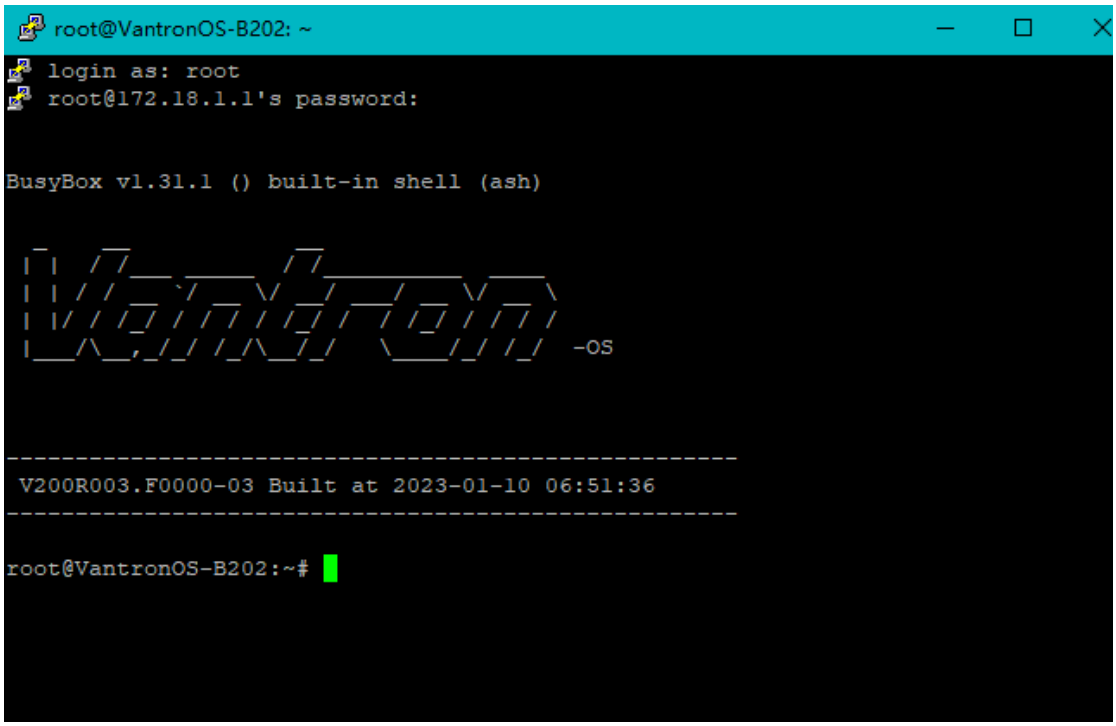
第 4 步：在 Windows 主机打开 SSH 客户端工具（推荐 PuTTY 或 MobaXterm）；

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**；

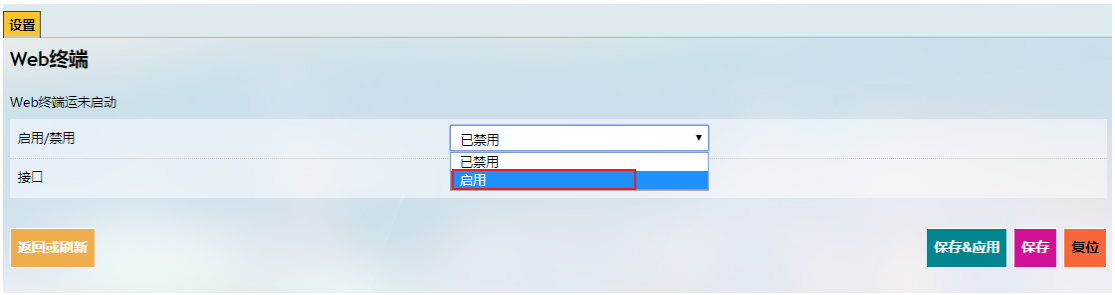


第 7 步：登录 root 账号（同前述步骤中网关登录密码一致），并开启 SSH 远程会话。



3.10.4 Web 终端

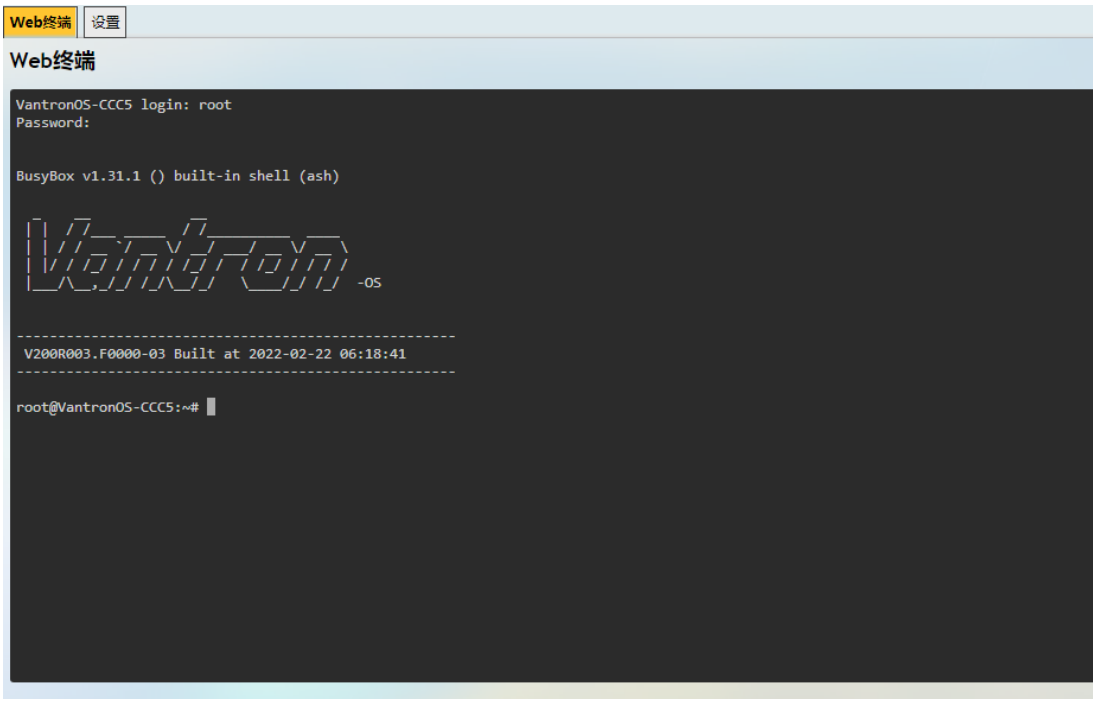
在 Web 终端页面**设置**项下点击**启用** Web 终端并保存&应用后，用户可以登录并输入命令行。



启用 Web 终端后，在**设置**标签旁会出现 **web 终端**标签：

登录名：**root**

登录密码：**rootpassword**（输入时不可见）



3.10.5 挂载点

用户可以在此启用/禁用自动挂载并查看挂载信息。

3.10.6 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。

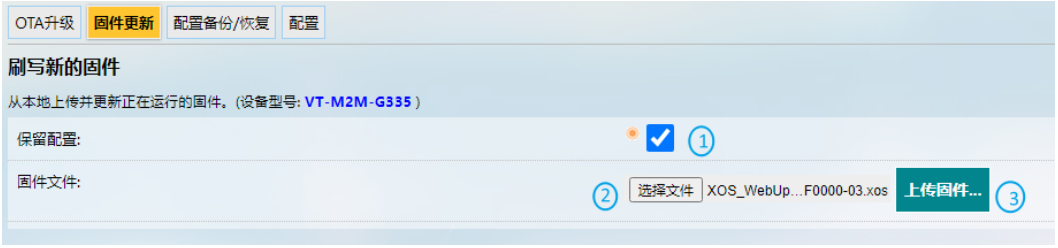
OTA 升级

编号说明

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

如果云端版本号显示 Failure，则该网关未在云端激活，请联系销售代表解决该问题。

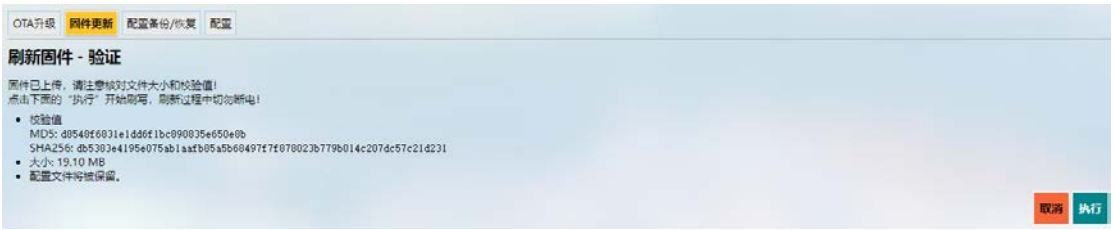
固件更新



编号说明

1. 选择是否保留原来的用户配置（建议不保留）
2. 从本地选择固件版本
3. 点击按钮，上传固件

当固件信息出现时，验证信息，然后点击**执行**并等待更新完成。固件升级过程中，请勿断电。升级完成后，登录页面将被刷新。



在**配置备份/恢复**标签下，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、将网关恢复出厂设置，并上传以前保存的备份文件包。

在**配置**标签下，用户可以设置系统升级时要保存的配置文件和目录。

3.10.7 重启

重启网关前，请确保没有开启任何进程。

3.11 退出

点击**退出**标签后，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。

第四章

工业协议配置

4.1 工业协议软件安装

在 VantronOS 网页界面，导航至**客制应用>IPK 安装器**，选择并上传.ipk 文件进行工业协议配置。

编号说明

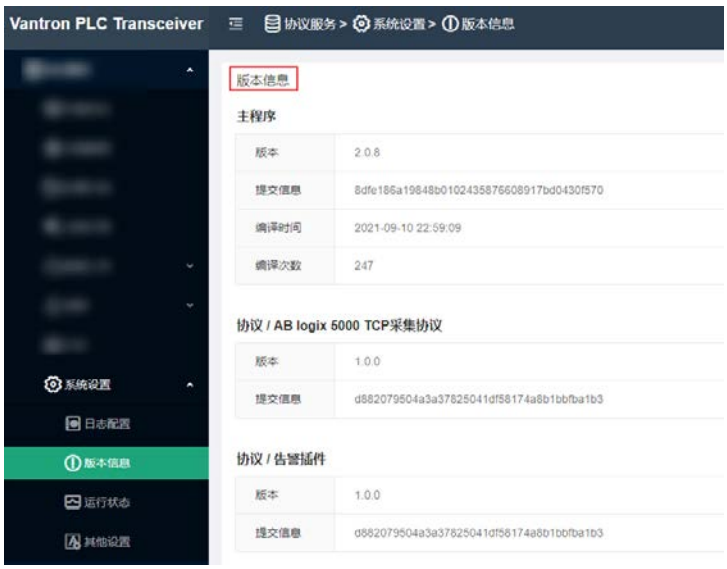
1. 上传.ipk 文件包后，会显示文件保存路径
2. 之后用户可以删除或安装.ipk 软件包

安装.ipk 文件后，将出现显示文件安装状态的信息。

之后在网关 LAN 口 IP 地址后，输入端口号（8081），如：172.18.1.1:8081，进入协议登录页面，然后输入用户名和密码登录（与网关用户名和密码一致）。

- 账号：**admin / root**
- 密码：**admin / rootpassword**

用户可以在**系统设置**页面查看该协议包的版本信息。

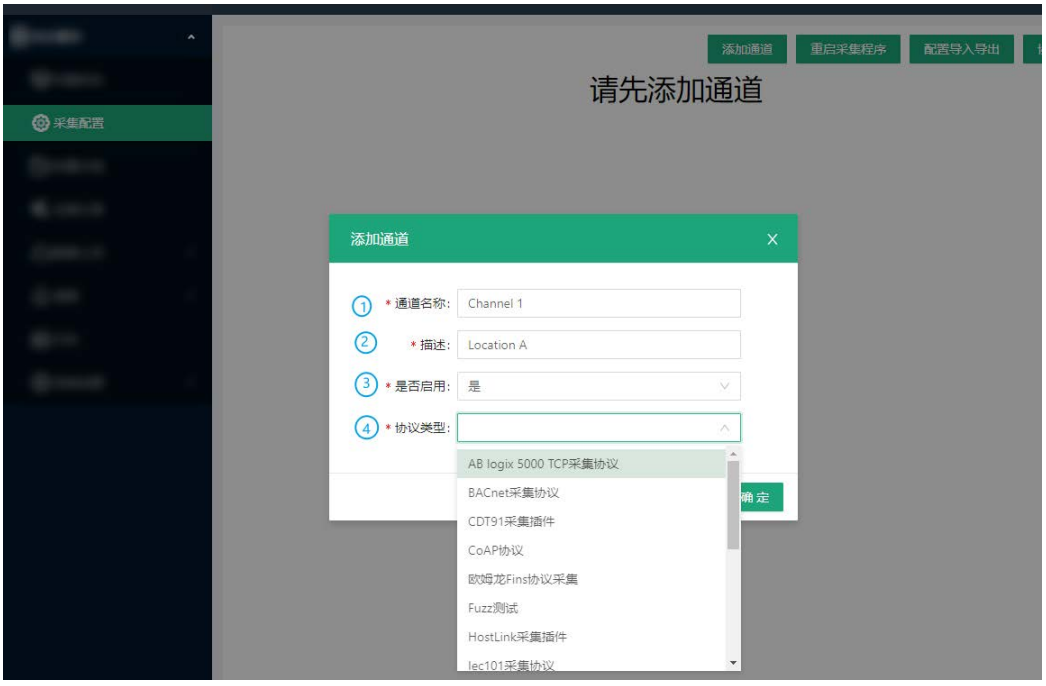


4.2 协议配置与应用

配置协议进行数据采集和边缘计算之前，请确认采集数据所使用的设备型号，并进行相应配置。

4.2.1 配置数据采集协议

点击左侧导航栏上的**采集配置**，添加通道后进行数据采集。



编号说明

1. 输入通道名称，该名称不能与已有的通道名称重复
2. 对协议通道进行描述
3. 选择是否启用该通道（默认启用）
4. 根据数据采集设备的型号，在下拉菜单中选择一项协议（协议类型由所安装的.ipk 文件支持）

对于某些协议类型，还需要继续配置其通信方式及协议模式等参数。下文以 Modbus RTU 采集协议为例，说明该协议的配置。

编号说明

4. 在协议类型下拉菜单中选择 Modbus 采集协议
5. 选择串口通讯作为通信方式（也可选择 TCP 通讯）
6. 传输模式可以选择 Modbus RTU，也可以选择 Modbus ASCII（此处以 Modbus RTU 为例）
7. 根据设备管理器识别到的设备，选择相关串口
8. 确定串口模式（网关型号不同，串口选项也不同）
9. 选择波特率
10. 通信中实际数据位的参数（RTU 通信参数默认是 8 位）
11. 校验位有三种：无校验（N）、奇校验（O）、偶校验（E）
12. 停止位表示单个包的最后一位，典型的值为 1、1.5 和 2 位
13. 选择是否开启请求发送（RTS）协议

协议通道配置完成后，该协议即展示在页面上。稍后用户可以删除或者修改通道。

编号说明

1. 删除通道或进入通道详情页并进行相应更改，如禁用通道。
2. 通道默认每 5 秒自动刷新一次，用户也可以设置 1-99 之间的任意数字。
3. 添加设备（如 PLC）用于数据采集

4.2.2 配置设备

如需在协议页面配置数据采集设备（下文以 PLC 指代，便于说明）的采集和上传任务，首先需将 PLC 与网关相连接，然后在采集配置页面添加该设备。

点击**新增**按钮并在弹窗内输入设备信息。

待填入的设备信息取决于所添加的通信协议。

例如西门子 S7-200 Smart PLC，如果用户采用以太网通信，则需确保.ipk 软件包中包含 **S7 协议**，并且已为该协议创建了通道。之后，用户可以在该通道下继续完成 PLC 设置。

编号说明

1. 输入设备名称
2. 输入从站地址
3. 选择是否启用该设备
4. 设置数据采集间隔
5. 设置寄存器起始位置
6. 选择下发的数据源（已采集数据）

4.2.3 添加设备变量

PLC 设备配置完成后，在右侧变量列表处点击**新增**，根据弹窗的指引，可以为已添加的设备设置点位变量。

编号说明

1. 设置该 PLC 所采集的变量名称
2. 添加标题对变量进行说明
3. 设置变量的读写权限
4. 选择功能码
5. 采集的数据类型默认为布尔值
6. 输入或上下调整寄存器地址（范围在 1 至 65535 之间）
7. 设置数据计算方式
8. 用户也可以跳过上述字段，直接上传 csv 文件，批量设置变量
9. 首次批量添加变量时，可以下载 csv 模板，查看必填字段（若已创建变量，则可以导出该设备的所有变量）

数据类型（5）由网关连接的数据采集设备决定。

变量添加完成后，可以点击导航栏左侧的**变量分组**标签，添加变量分组。

数据采集设备及变量配置完成后，可以在采集配置页面将配置导出备份到本地，反之，也可以导入之前备份好的配置。

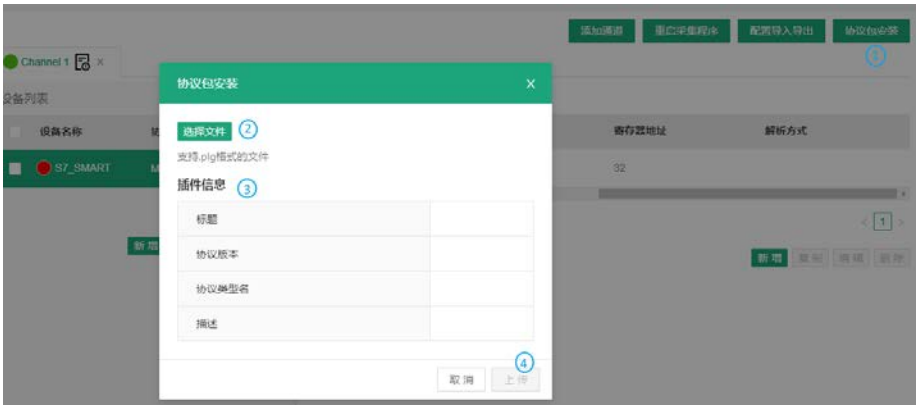
编号说明

1. 点击**配置导入导出**进入操作页面
2. 导出通道配置到本地
3. 从本地导入之前备份的配置文件

导出配置的操作会将采集配置页面所有通道的配置备份到本地。

点击**重启采集程序**按钮，将重启设备通道及采集任务。

点击**协议包安装**按钮，可以在此处上传协议安装包插件。

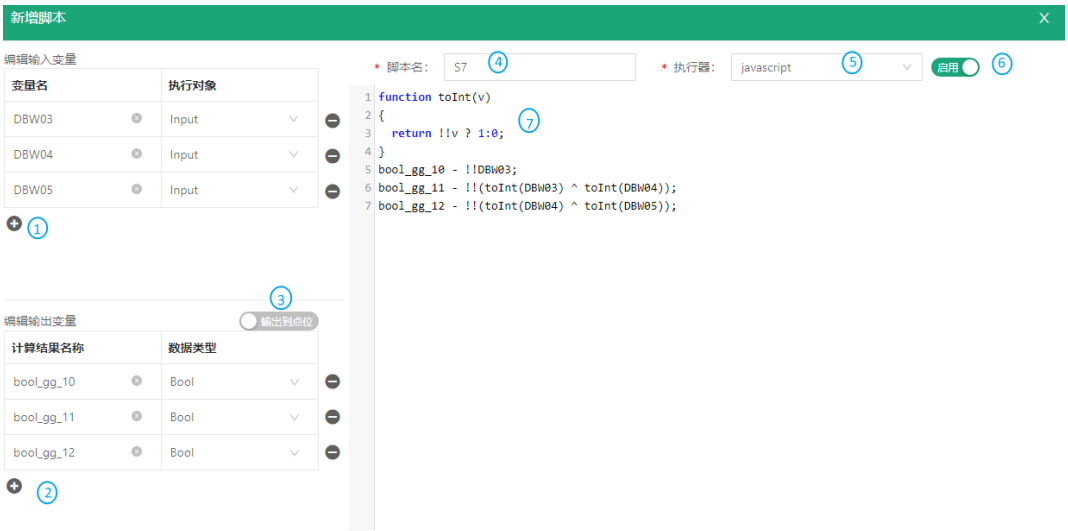


编号说明

1. 点击**协议包安装**按钮进入操作页面
2. 从本地选择插件文件（支持.plg 格式）
3. 导入插件后，会展示插件的详细信息
4. 上传插件

4.2.4 设置边缘计算脚本

如需添加边缘计算脚本，点击左侧导航栏的**边缘计算**标签，在页面上点击**新增脚本**，然后在弹窗内输入脚本信息。



编号说明

1. 编辑输入变量：添加变量名称和脚本所执行的变量对象（可添加多个变量）
2. 编辑输出变量：添加计算结果名称和数据类型
3. 通过切换按钮，选择将计算结果输出到边缘点位或变量
4. 输入脚本名称
5. 选择脚本格式（支持 JavaScript、Lua 和 Python）
6. 选择是否启用该脚本
7. 在窗口中编译脚本

完成编译后，点击**确定**退出。

在**边缘计算脚本列表**页面，用户可以执行多项操作。

编号说明

1. 边缘计算脚本列表
2. 刷新脚本
3. 新增脚本
4. 批量导入脚本/导出已设置的脚本
5. 脚本执行策略（可以批量设置多个脚本的执行策略）

执行策略分为自动触发和定时执行。

自动触发：当脚本执行对象出现异常时，自动触发脚本的执行。

定时执行：系统默认每隔 1000ms 即自动执行一次脚本，执行间隔可以调整。

执行间隔为所选脚本的执行时间间隔（默认为 1000ms）

执行环境复用可以设置脚本的重启机制。

6. 启用/暂停、复制、编辑和删除脚本（点击**编辑**可以访问单个脚本信息和执行日志）

4.2.5 采集状态

上述参数设置完成后，用户可以点击左侧导航栏的**采集状态**，在该页面查看设备和变量信息。

编号说明

1. 设备列表
2. 变量列表
3. 使用筛选工具筛选所需信息
4. 选择变量分组
5. 自动刷新间隔
6. 手动点击刷新
7. 变量详情
8. 数据下发设置

4.2.6 数据上传和封装

采集好的数据经边缘计算处理后，通过相关协议上传至云平台。以 MQTT 协议为例，配置过程如下：

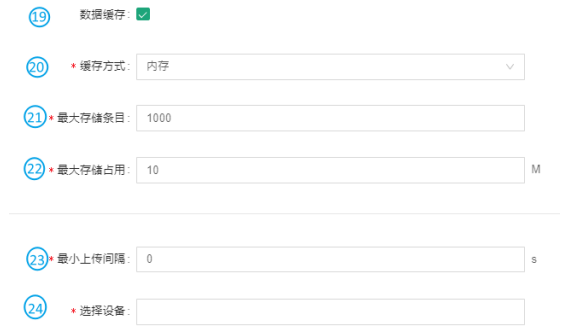
- 展开**数据上传**标签，点击**上传配置**；
- 点击右上角的**新建数据上传**，在弹窗中添加数据上传服务，然后确定。

- 其后，在 MQTT 客户端页面进行详细配置。

编号说明

1. 选择配置完成后是否启用数据上传，若启用，则采集的数据将自动上传至云平台
2. 选择数据封装格式，默认无格式要求
3. 中心平台自动填写且不可更改
4. 填写 MQTT 服务器的 IP 地址
5. MQTT 服务器端口自动填充为 1883
6. 客户端会在一个心跳间隔内发送一条消息给服务端，如果服务端未收到消息，则会断开客户端的网络连接，默认间隔时间为 90 秒
7. MQTT 客户端 ID：客户端唯一标识，不可重复
8. 设置 QoS（服务质量）
   - QoS 0：消息最多传递一次，如果当时客户端不可用，则丢失该消息。
   - QoS 1：消息至少传递一次。
   - QoS 2：消息仅传递一次。
9. 数据上传主题：MQTT 发布消息用到的主题名，用于识别有效载荷数据应该被发布到哪一个信息通道
10. MQTT 订阅消息用到的主题名，订阅后服务器可以向客户端发布消息实现控制

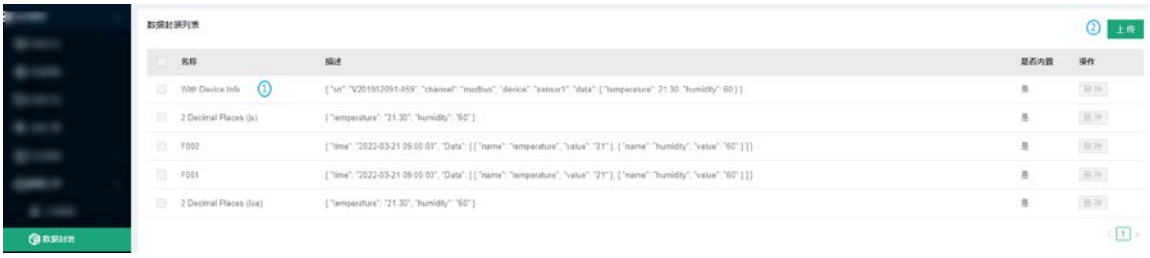
11. 填写用户名（非必须）
12. 填写密码（非必须）
13. 选择是否启用 SSL 认证（若启用，可选择普通 SSL 或国密 SSL）
14. 如果启用普通 SSL，需要选择服务器认证方式
15. 选择是否启用客户端认证
16. 如果启用客户端认证，需要上传客户端证书
17. 如果启用客户端认证，还需要上传客户端私钥
18. 填写客户端秘钥密码（非必须）



19. 选择是否缓存数据
20. 如果选择缓存，则需选择缓存方式（内存或磁盘），默认缓存至内存
21. 输入最大存储条目为
22. 输入最大存储占用空间
23. 输入最小上传间隔
24. 选择上传数据的来源设备

点击右侧**提交**后，上传配置完成。用户即可以在 MQTT 云平台浏览网关上传的数据，实现数据展现、统计、运维分析等功能。

在数据封装页面，用户可以上传封装数据或配置数据封装格式。

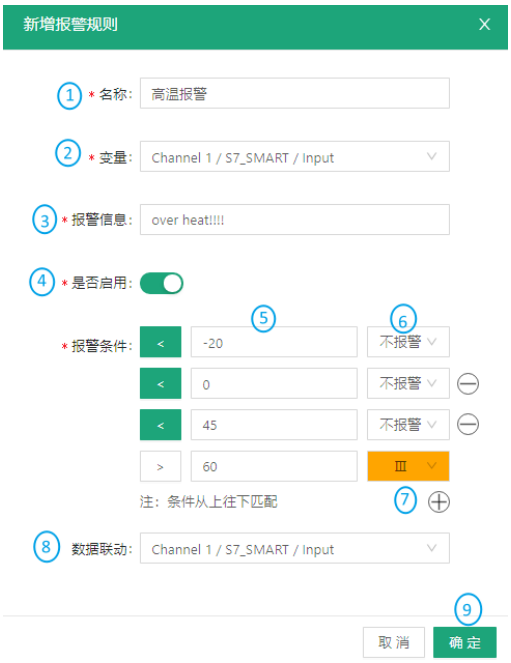


编号说明

1. 内置的数据封装格式说明
2. 上传.json 数据进行封装

4.2.7 报警

在**报警>报警配置**页面，允许用户设置报警触发条件，当点位状态满足条件时触发报警，当点位状态转变为不满足条件时，报警解除。



编号说明

1. 设置报警名称
2. 选择对应的变量
3. 设置报警显示信息
4. 选择是否启用该警报
5. 设置报警条件（条件从上至下匹配）
6. 选择警报等级（如果选择不报警，条件触发后将不会发出警报）
7. 点击“+”添加条件，点击“-”删除条件
8. 选择联动数据
9. 设置完成后，点击**确定**，保存报警规则

添加报警规则后，用户可以在**报警>报警推送**页面设置报警推送规则。

编号说明

1. 设置报警间隔时间，默认为 120 秒
2. 设置报警记录最大存储值，默认为 1024M
3. 选择是否启用结果输出
4. 选择报警输出到报警记录或者报警记录+邮件

若选择输出到报警记录+邮件，则需对邮件相关信息进行设置。

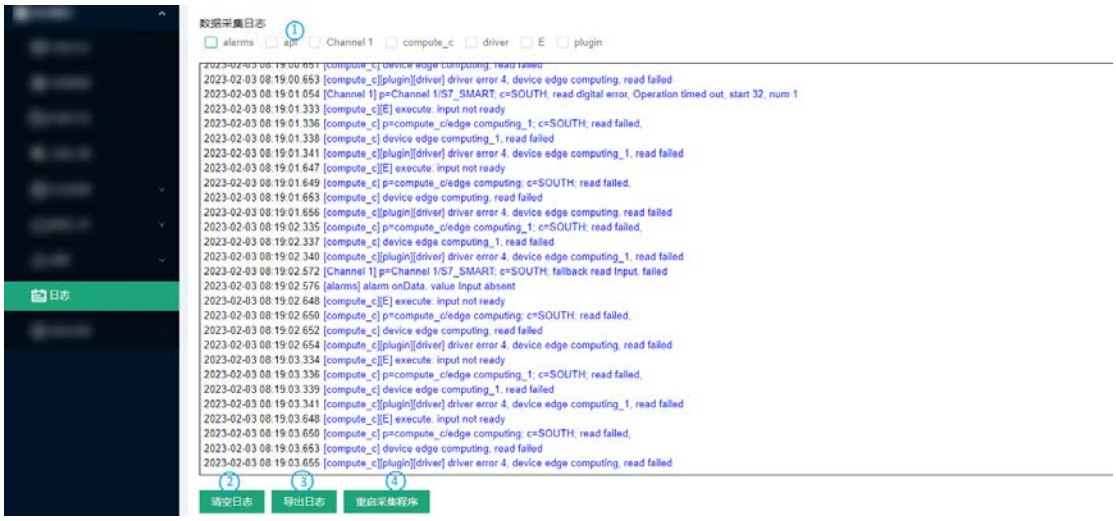
5. 填写接收推送的邮箱地址
6. 填写发件服务器 IP 地址（可查看所使用的邮件服务器设置）
7. 如果服务器支持，可选择加密传输
8. 设置报警推送的用户名
9. 选择是否打开服务器身份验证
10. 如果开启服务器身份验证，则需要输入密码

完成设置后，用户可以点击**发送测试邮件**，验证设置是否正确，最后提交设置。

报警>报警记录页面显示事件触发后的报警记录，用户可以查看报送状态、出发时间等详细信息。

4.2.8 日志

日志页面显示数据采集日志和云服务日志，用户可以做相应变更。



编号说明

1. 点击相关标签，筛选日志
2. 清空日志
3. 导出日志
4. 重启采集程序

4.2.9 系统设置

在**系统设置**页面，用户可以配置系统参数，并查看相关系统信息。

- **日志配置**

编号说明

1. 选择各类日志级别（根据紧急程度，分为 NONE、FATAL、ERROR、WARNING、INFO、DEBUG、TRACE）
2. 设置单个日志文件大小（默认为 1024K）
3. 点击**确定**，保存配置

日志配置后需回到**日志>重启采集程序**页面，重启采集程序后，设置才能生效。

- 日志存储

  在**日志配置>日志存储**页面，用户可以删除或下载单条/全部日志。

- 运行状态

  运行状态页面显示系统时间以及程序运行开始时间和运行时长。

- 其他设置

  在**其他设置**页面，可以更改页面语言。

- GSD 文件管理

  用户可以在 GSD 文件管理页面上传通用站点描述（GSD）文件，用于 PROFIBUS DP 或者 PROFINET IO 通讯。

第五章

废弃处理与质保

5.1 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。

5.2 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。

附录 B 缩写

缩写	说明
RXD	接收数据
TXD	发送数据
GND	接地
ISO-GND	隔离接地
NC	无连接