

C335 系列

工业边缘计算网关



用户手册

版本：1.4

© 成都万创科技股份有限公司 版权所有

版本记录

编号	软件版本	说明	日期
V1.0	V200R002	首次发布	2020年7月19日
V1.1	V200R003	添加串口端子说明	2021年8月18日
V1.2	V200R003	更新联系地址与电话	2022年6月15日
V1.3	V200R003	更新 C335L 接口说明	2022年11月23日
V1.4	V200R003	更新协议门户登录和配置说明	2023年3月24日

目录

前言	1
第一章 硬件说明	5
1.1 产品概述	6
1.2 开箱	7
1.3 规格	8
1.4 接口定义 (C335L)	10
1.4.1 前视图	10
1.4.2 左视图	11
1.4.3 串口	12
1.5 接口定义 (C335)	13
1.5.1 前视图	13
1.5.2 右视图	14
1.5.3 串口	14
1.6 接口定义 (C335S)	16
1.6.1 前视图	16
1.6.2 右视图	17
1.6.3 串口	17
1.7 可选功能	19
1.7.1 蓝牙 (C335L)	19
1.7.2 CAN (C335)	21
1.7.3 GPIO (C335)	22
1.8 系统启动	23
1.8.1 从 SD 卡启动系统并刷新 eMMC	23
1.8.2 从 eMMC 闪存启动系统	24
第二章 快速开始	25
2.1 设置网关	26
2.2 登陆网关	32
2.3 连接万创网关管理平台	33
2.4 网络连接	33
2.4.1 以太网连接	33
2.4.2 Wi-Fi 连接	34
2.4.3 移动网络连接	34
2.5 自定义设置	34
第三章 VantronOS 页面配置网关	35
3.1 VantronOS 简介	36
3.2 状态	37
3.3 快速设置	39
3.3.1 快速联网	39
3.3.2 WAN 设置 - 自动获取 DHCP	39
3.3.3 WAN 设置 - 客户端 Client	40
3.3.4 WAN 设置 - 4G/LTE	41
3.3.5 WAN 设置 - 宽带拨号 PPPOE	42
3.3.6 WAN 设置 - 静态地址 Static	43
3.3.7 自动线路	44

3.4	虚拟隧道.....	46
3.4.1	OpenVPN 服务器.....	46
3.4.2	VPN 客户端.....	47
3.5	网络.....	48
3.5.1	接口.....	49
	LAN 口.....	50
	4G.....	52
	WAN 口.....	53
3.5.2	无线（WIFI）.....	54
	Wi-Fi - AP 模式（基本设置）.....	55
	Wi-Fi - AP 模式（高级选项）.....	56
	Wi-Fi - 客户端模式.....	57
3.5.3	4G/LTE.....	58
3.5.4	静态路由.....	59
3.5.5	防火墙.....	60
3.6	用户管理.....	63
3.7	客制应用.....	64
3.7.1	客制程序.....	64
3.7.2	IPK 安装器.....	65
3.7.3	厂商信息定制.....	65
3.7.4	DMP Agent.....	66
3.7.5	SNMP 服务.....	67
3.8	硬件.....	68
3.8.1	AIDI 采集.....	68
3.8.2	串口转 TCP.....	69
3.8.3	Ser2net 环境搭建与验证.....	69
3.8.4	协议对比.....	75
3.9	服务.....	76
3.9.1	PLC 远程连接.....	76
3.9.2	协议服务.....	77
3.10	系统.....	77
3.10.1	系统.....	77
3.10.2	带宽监视.....	78
3.10.3	管理权.....	79
	SSH 访问.....	79
3.10.4	终端.....	81
3.10.5	挂载点.....	81
3.10.6	备份/升级.....	82
3.10.7	重启.....	83
3.11	退出.....	83
第四章	工业协议配置.....	84
4.1	工业协议软件安装.....	85
4.2	协议配置与应用.....	86
4.2.1	配置数据采集协议.....	86
4.2.2	配置设备.....	88
4.2.3	添加设备变量.....	89

4.2.4	设置边缘计算脚本.....	92
4.2.5	采集状态.....	94
4.2.6	数据上传和封装.....	94
4.2.7	报警.....	97
4.2.8	日志.....	99
4.2.9	系统设置.....	99
第五章	废弃处理与质保.....	101
5.1	废弃处理.....	102
5.2	质保.....	103
附录	合规声明.....	104

前言

感谢购买万创工业边缘计算网关（“网关”或“产品”）。C335 系列网关包含三款网关产品：C335L、C335、C335S，因此，针对已购网关，请查阅本手册对应部分的说明。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

成都万创科技股份有限公司（“万创”）保留本手册的所有权利，包括随时更改内容、形式、产品功能和规格的权利，恕不事先另行书面通知。您可访问 www.vantrontech.com.cn 获取本手册最新版本。

本手册中的商标和注册商标均为其各自所有者的财产。本手册的任何部分均不得复制、翻印、翻译或出售。未经万创事先书面同意，不得对本手册进行任何更改或将其用于其他用途。万创保留对本手册所有公开发布副本的权利。

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。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（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

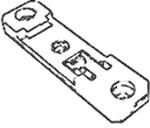
1.1 产品概述

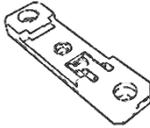
万创 C335 系列边缘计算网关是成都万创科技股份有限公司为应对不同工业场景中工业物联网应用的需求而推出的边缘计算网关产品家族。该系列产品采用高性能低功耗工业级 ARM 处理器，提供大容量的存储、丰富的工业接口，搭载万创自主开发的操作系统 Vantron OS，支持多种工业协议，可接入现场工业设备如 PLC、HMI 及传感器等。同时支持边缘计算，在物联网边缘节点实现数据优化，减少现场与中心端的数据量。支持标准 MQTT 协议，可接入广泛的工业数据平台，助力工厂数字化转型。

C335 系列产品采用工业化设计，保证其质量和可靠性，是工业物联网应用解决方案的理想选择。产品可接入万创自研的 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 (C335S & C335L)		可选配件 (C335S & C335L)	
	1 x C335S/C335L 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

标准配件 (C335)		可选配件 (C335)	
	1 x C335 网关		1 x 电源适配器
	1 x 导轨安装支架		1 x 电源转接线
\	\		1 x 4G LTE 天线 或 1 x Wi-Fi 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。

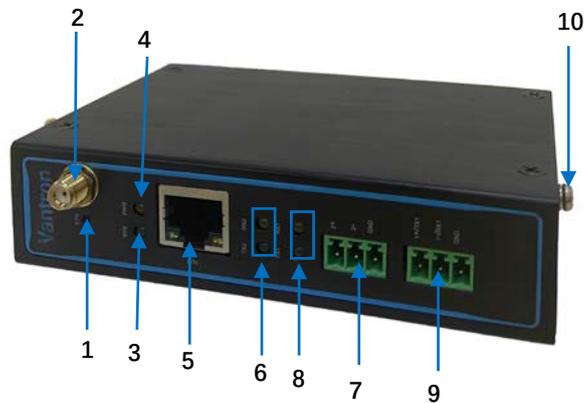
1.3 规格

型号		C335L	C335	C335S
系统	CPU	TI, AM335x, ARM Cortex-A8, 600MHz	TI, AM335x, ARM Cortex-A8, 600MHz	TI, AM335x, ARM Cortex-A8, 1GHz
	内存	512MB	1GB	1GB
	存储	8GB (最大 64GB) 1 x Micro SD 卡	8GB (最大 64GB) 1 x Micro SD 卡	8GB (最大 64GB) 1 x Micro SD 卡
通信	以太网	1 x RJ45, 10/100Mbps	2 x RJ45, 10/100Mbps	6 x RJ45 (其中一个用于调试), 10/100Mbps
	LTE & Wi-Fi 及蓝牙	Mini PCIe 用于 CAT 1/CAT 4 板载 Wi-Fi 802.11 a/b/g/n/ac & 5.0	Mini PCIe 用于 CAT 1/CAT 4 或 Wi-Fi 802.11 a/b/g/n/ac & BT 5.0	Mini PCIe 用于 CAT 1/CAT 4 板载 Wi-Fi 802.11 a/b/g/n/ac & 5.0
	网口协议		PPP、PPPoE、DHCP、ARP	
输入/输出	串口	1 x RS485 1 x RS232/RS485	3 x RS485 1 x RS232/RS485	3 x RS485 1 x RS232/RS485
	数字输入	无	无	4 x 数字输入
	模拟输入	无	无	2 x 模拟输入
	SIM 卡槽		1 x 抽屉式 SIM 卡槽	
	接地		设备机壳接地&PCB 接地	
	RTC	独立的 RTC 芯片, 纽扣电池供电	独立的 RTC 芯片, 纽扣电池供电	独立的 RTC 芯片, 系统或纽扣电池供电
	GPIO	4 x GPIO (可选)	4 x GPIO (可选)	4 x GPIO
系统控制	按键	1 x 重置键	1 x 重置键 1 x 更新键	1 x 重置键 1 x 恢复设置键
	LED 指示灯	1 x 电源指示灯 1 x 系统状态指示灯 4 x 串口状态指示灯	1 x 电源指示灯 1 x 系统状态指示灯 8 x 串口状态指示灯	1 x 电源指示灯 1 x 系统状态指示灯 4 x 串口状态指示灯
	尺寸	113.5mm x 82mm x 28.5mm	125mm x 110mm x 30mm	132mm x 124mm x 40mm
机械	壳体		金属	
	安装方式		导轨安装/墙挂安装/面板安装	
	IP 防护等级		IP30	
	散热方式		无风扇散热	
电源	输入	9-36V 直流电, 支持过流保护, 防接反保护	12-48V 直流电, 支持过流保护, 防接反保护	12-48V DC, 支持过流保护, 防接反保护
	电源端子	3 芯 3.81mm 凤凰端子	3 芯 3.81mm 凤凰端子	3 芯 3.81mm 凤凰端子
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	
	IoT 协议		MQTT/HTTPS	
	IPK 导入		支持	

型号		C335L	C335	C335S
	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	SYN 泛洪保护、端口转发、自定义规则		
	数据安全	OpenVPN、L2TP、PPTP、IPSec		
	链路在线检测	发送心跳包检测，断线自动连接		
	网络可靠性	故障切换，支持有线、Wi-Fi、4G 通讯互为备份		
	多级权限	支持		
功能应用	配置模式	本地、远程		
	升级	本地升级、OTA 升级	本地升级、OTA 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		
工业协议	M2M 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/ Lua/ Node.js/Java/ Node-Red（可选）		
环境条件	温度	工作温度：-20°C ~ +70°C 存储温度：-30°C ~ +85°C	工作温度：-20°C ~ +70°C 存储温度：-30°C ~ +85°C	工作温度：-20°C ~ +70°C （可选：-20°C ~ +85°C） 存储温度：-40°C ~ +85°C
	湿度	相对湿度 5%-95%（无凝露）		
	认证	CE、FCC、PTCRB		

1.4 接口定义（C335L）

1.4.1 前视图



项目编号	说明
1	BTN 按键（见后文描述）
2	4G 主天线
3	系统状态指示灯
	系统启动时闪烁
	系统启动后，切换为绿色常亮
	系统升级或清除配置时闪烁
4	电源指示灯
5	以太网端口：在 VantronOS 中显示为 ETH0，默认在 LAN 区工作
6	R2 串口的状态指示灯（传输数据时闪烁）
7	R2 串口（RS485）
8	R1 串口的状态指示灯（传输数据时闪烁）
9	R1 串口（RS485/RS232）
10	接地螺丝

▶ BTN 按键说明

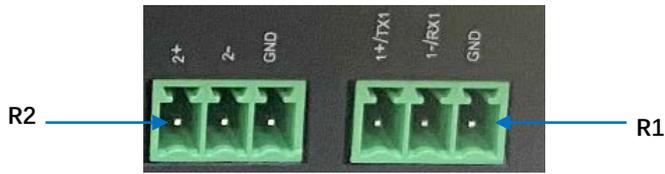
- 当系统升级盘插入 SD 卡槽或 USB 端口中时，短按该按键 2 秒，则状态指示灯闪烁，表明系统正在升级。升级完成后，系统将重启（从 eMMC 闪存启动）。
- 按下该按键 3-10 秒，将清除用户配置和自定义参数，网关恢复出厂设置。操作完成后，系统将重启。
- 按下该按键 10 秒以上，将格式化用户分区并清除用户分区的数据。

1.4.2 左视图



接口	说明
1	4G 分集天线
2	调试接口
3	Micro SIM 卡槽
4	Micro SD 卡槽
5	Wi-Fi & BT 天线
6	9V-36V DC 电源端子
7	4G 主天线

1.4.3 串口



引脚说明：

串口	节点	串口模式	对应的指示灯
R1（右）	/dev/ttyO2	RS232 或 RS485	TX1/RX1
R2（左）	/dev/ttyO4	RS485	TX2/RX2

R1 端子可以复用为 RS232 或 RS485 模式（默认），R2 端子为 RS485 模式。

1. 输入以下命令，在 R1 串口启用 RS232 模式，并使用串口通信程序（如 microcom）打开串口：

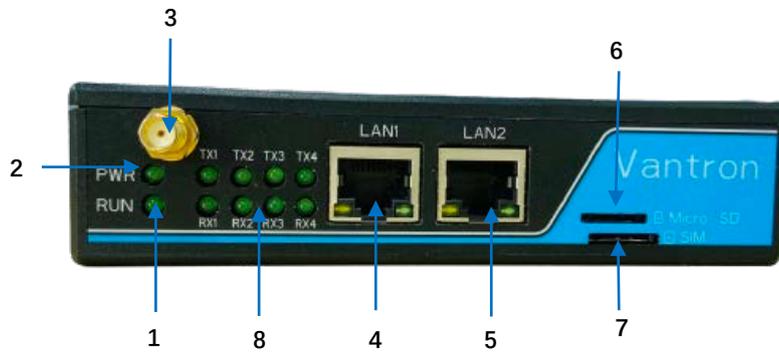
```
~# gpio set uart0 rs232 save  
或者  
~# gpio set uart0 rs232  
  
~# gpio get uart0  
rs232  
  
~# microcom /dev/ttyO2 -s 115200
```

2. 输入以下命令，在 R1 串口启用 RS485 模式，并开始通信：

```
~# gpio set uart0 rs485 save  
或者  
~# gpio set uart0 rs485  
  
~# gpio get uart0  
rs485  
  
~# microcom /dev/ttyO2 -s 115200
```

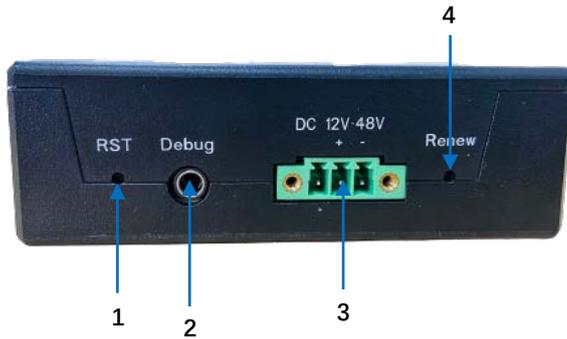
1.5 接口定义（C335）

1.5.1 前视图



项目编号	说明
1	系统启动时闪烁
	系统状态指示灯 系统启动后，切换为绿色常亮
	系统升级或清除配置时闪烁
2	电源指示灯
3	天线接头（4G/LTE 或 Wi-Fi）
4	LAN1：在 VantronOS 中显示为 ETH0，且默认在 LAN 区工作
5	LAN2：在 VantronOS 中显示为 ETH1，且默认在 WAN 区工作
6	Micro SD 卡槽
7	Micro SIM 卡槽
8	8 x 串口状态指示灯（数据传输时闪烁）

1.5.2 右视图

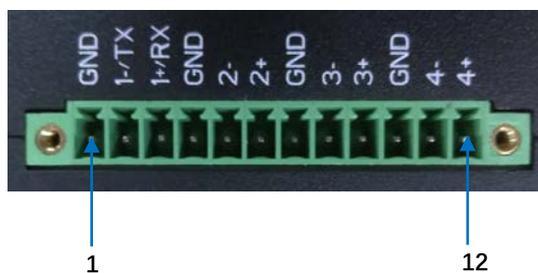


项目编号	说明
1	重置键
2	调试接口
3	12-48V DC 电源端子
4	更新键（描述见下文）

更新键说明

- 当系统升级盘插入 SD 卡槽或 USB 端口中时，短按该按键 2 秒，则状态指示灯闪烁，表明系统正在升级。升级完成后，系统将重启（从 eMMC 闪存启动）。
- 按下该按键 3-10 秒，将清除用户配置和自定义参数，网关恢复出厂设置。操作完成后，系统将重启。
- 按下该按键 10 秒以上，将格式化用户分区并清除用户分区的数据。

1.5.3 串口



串口引脚定义：

编号	信号	节点	接口名称	串口模式	指示灯
1	GND1	/dev/ttyO2	COM2	RS232 或 RS485（默认）	TX1/RX1
2	RS485_1_B/STXD2				
3	RS485_1_A/SRXD3				
4	GND2	/dev/ttyO3	COM3	RS485	TX2/RX2
5	RS485_2_B				
6	RS485_2_A				
7	GND3	/dev/ttyO4	COM4	RS485	RX4/RX4
8	RS485_3_B				
9	RS485_3_A				
10	GND4	/dev/ttyO5	COM5	RS485	RX3/RX3
11	RS485_4_B				
12	RS485_4_A				

COM2 的引脚可以复用为 **RS232** 或 **RS485**。

输入以下命令，在 **COM2** 串口启用 **RS232** 模式，并使用串口通信程序（如 **microcom**）打开串口：

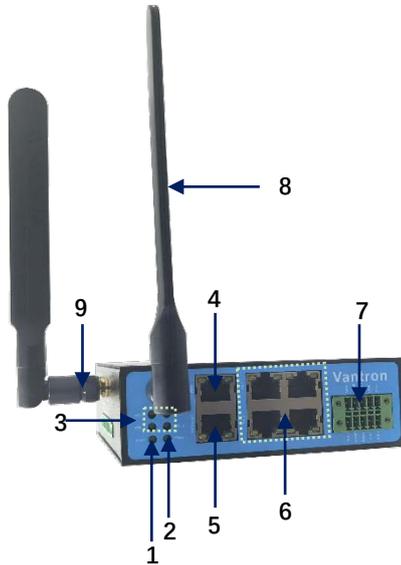
```
~# gpio set uart0 rs232 save  
或者  
~# gpio set uart0 rs232  
  
~# gpio get uart0  
rs232  
~# microcom /dev/ttyO2 -s 115200
```

输入以下命令，在 **COM2** 串口启用 **RS485** 模式，并使用串口通信程序（如 **microcom**）打开串口：

```
~# gpio set uart0 rs485 save  
或者  
~# gpio set uart0 rs485  
  
~# gpio get uart0  
rs485  
~# microcom /dev/ttyO2 -s 115200
```

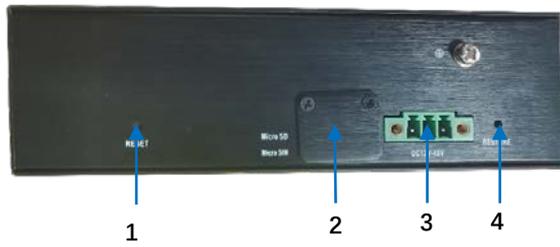
1.6 接口定义（C335S）

1.6.1 前视图



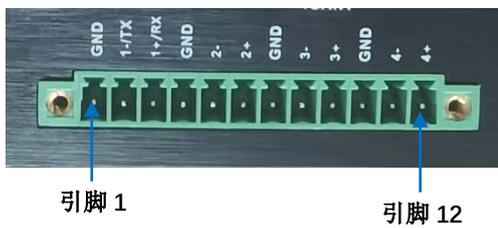
项目编号	说明	
1	系统状态指示灯	系统启动时闪烁
		系统启动后，切换为绿色常亮
		系统升级或清除配置时闪烁
2	电源指示灯	
3	4 x 串口状态指示灯（数据传输时闪烁）	
4	WAN 口：在 VantronOS 中显示为 ETH1，且默认在 WAN 区工作	
5	RJ45 转 DB9 调试口，用于串口调试	
6	4 x LAN 口：在 VantronOS 中显示为 ETH0，且默认在 LAN 区工作	
7	模拟输入（AI）/数字输入（DI）接口	
8	4G 天线 1	
9	4G 天线 2	

1.6.2 右视图



项目编号	说明
1	重置键
2	Micro SD & Micro SIM 卡槽
3	12V-48V DC 电源端子
4	恢复设置键

1.6.3 串口



串口引脚定义：

编号	信号	节点	接口名称	串口模式	指示灯
1	GND1	/dev/ttyO1	COM 1	RS232 或 RS485 (默认)	485_1
2	RS232_TX / RS485_1_B				
3	RS232_RX / RS485_1_A				
4	GND2	/dev/ttyO2	COM2	RS485	485_2
5	RS485_2_B				
6	RS485_2_A				
7	GND3	/dev/ttyO3	COM3	RS485	485_3
8	RS485_3_B				
9	RS485_3_A				
10	GND4	/dev/ttyO4	COM4	RS485	485_4
11	RS485_4_B				
12	RS485_4_A				

COM1 可以复用为 RS232 或 RS485（默认）。

输入以下命令，在 COM1 串口启用 **RS232** 模式，并使用串口通信程序（如 microcom）打开串口：

```
~# gpio set uart0 rs232 save  
或者  
~# gpio set uart0 rs232  
  
~# gpio get uart0  
rs232  
  
~# microcom /dev/ttyO2 -s 115200
```

输入以下命令，在 COM1 串口启用 **RS485** 模式，并使用串口通信程序（如 microcom）打开串口：

```
~# gpio set uart0 rs485 save  
或者  
~# gpio set uart0 rs485  
  
~# gpio get uart0  
rs485  
  
~# microcom /dev/ttyO2 -s 115200
```

1.7 可选功能

1.7.1 蓝牙（C335L）

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：蓝牙设备成功连接网关]

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：测试文件成功发送至蓝牙设备]

> 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
```

如需重新命名 HCI 设备，输入以下命令行：

```
~# hciconfig hci0 name "Bluez 5.21 test"
~# hciconfig hci0 down
~# hciconfig hci0 up
```

1.7.2 CAN (C335)

两台 C335 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网关定制，请联系您的销售代表。

1. 准备两台 C335 网关，其 CAN 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。

1.7.3 GPIO (C335)

GPIO 接头上的引脚说明如下：

名称	引脚编号
"gpio_in1" (gpio0_22)	22
"gpio_in2" (gpio0_23)	23
"gpio_out1" (gpio0_26)	26
"gpio_out2" (gpio0_27)	27

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 或者 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：

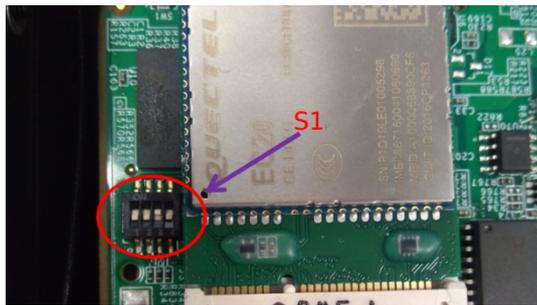
```
~# echo 22 > /sys/class/gpio/unexport
```

1.8 系统启动

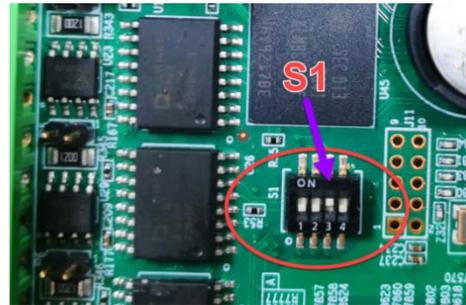
系统默认从 eMMC 启动。

1.8.1 从 SD 卡启动系统并刷新 eMMC

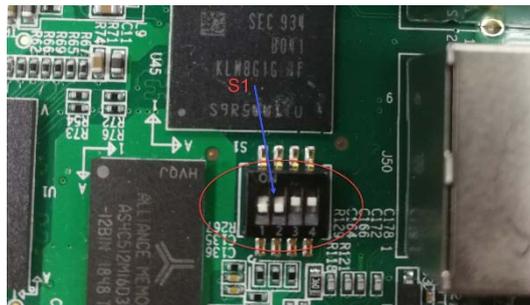
1. 打开网关盒子；
2. 将 DIP 开关 S1 设置为 **off:off:on:off** (C335L & C335S) 或 **off:off:on:on** (C335)，如下图所示；



C335L



C335S



C335

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提供的发布包解压（以 C335S 为例）：

```
~# unzip XOS_sd2mmc_VT-M2M-C335S "version number".zip
```
 - 3) 解压后的文档说明如下：

```
└── build.date //镜像编译日期
└── sd2emmc.sh //SD 卡启动制作脚本
└── XOS_sd2mmc_VT-M2M-C335S_Vxxxxxxx.Fxxxxxxx.img //启动镜像
└── XOS_sd2mmc&sdAutoUpgrade_VT-M2M-C335S_Vxxxxxxx.Fxxxxxxx.sha256sum //sha256sum 文件
└── XOS_sdAutoUpgrade_VT-M2M-C335S_Vxxxxxxx.Fxxxxxxx.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
```

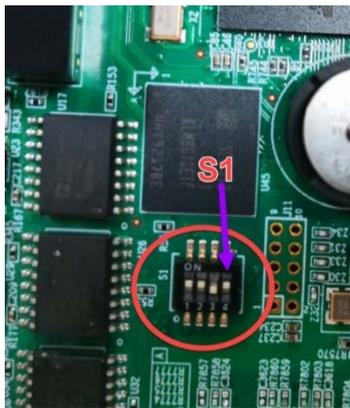
- ▶ 使用正确的 SD 卡路径替换 /dev/sdb。
- ▶ 制作程序完成的消息弹出前拔出 SD 卡会导致制作失败。
- ▶ 若制作过程中提示失败，则可拔下 SD 并重新执行上述命令。

4. 将 SD 卡插入卡槽；

5. 网关上电。系统启动后，状态指示灯将变为绿色常亮，且 eMMC 刷新完成。

1.8.2 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 on:on:off:on；



图为 C335S

3. 网关上电。系统从 eMMC 启动后，状态指示灯将变为绿色常亮。

第二章

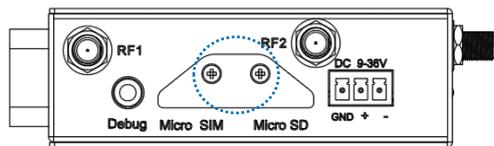
快速开始

2.1 设置网关

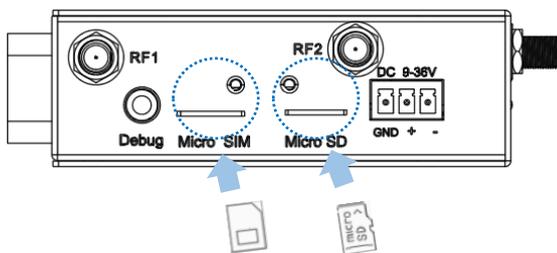
配置网关前，需执行以下步骤完成产品硬件连接。

C335L 网关

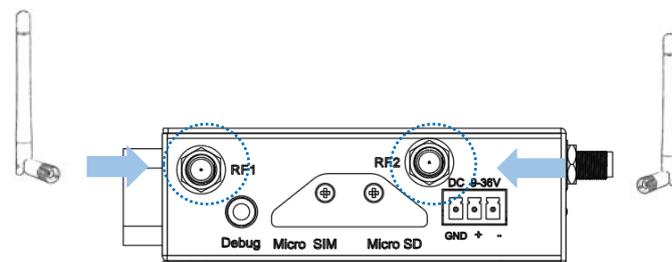
1. 使用安装支架和螺钉将网关安装在安全处；
2. 松开网关左侧 SIM 卡和 SD 卡盖板上的螺丝；



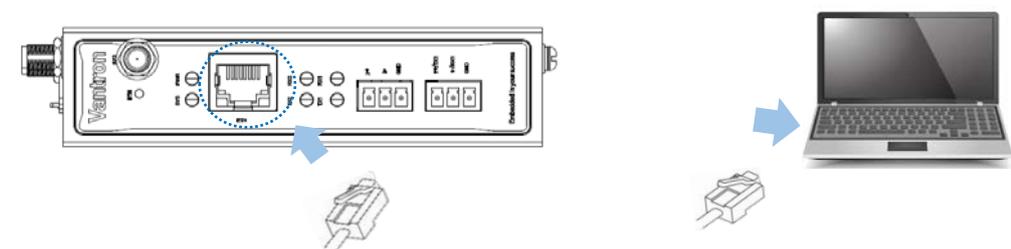
3. 金属芯片/引脚朝下，将激活的 SIM 卡和 SD 卡分别插入对应的卡槽；



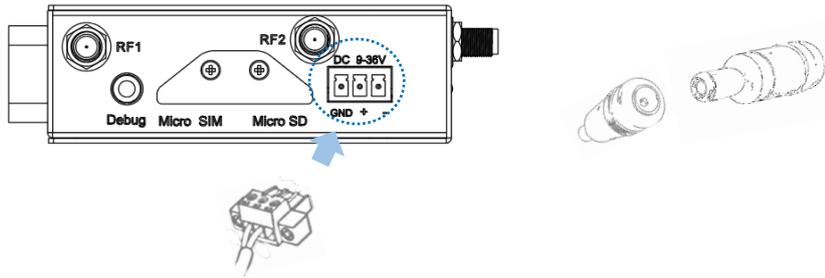
4. 推动 SIM 卡和 SD 卡将其固定；
5. 将盖板装回卡槽处，并拧紧螺丝；
6. 将天线安装到天线接头上，并紧固接头；



7. 将网线的一端连接至网关以太网口，另一端连接至个人电脑（C335L 的网口默认为 LAN 口）；



- 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；

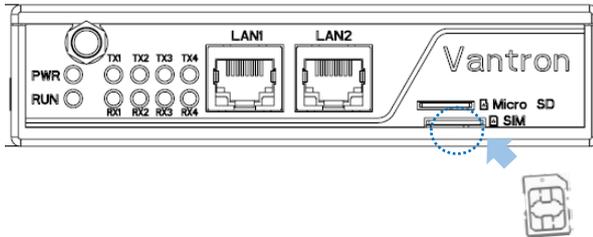


- 将适配器插入符合网关工作电压要求(9V-36V)的直流电源插座，使网关通电；
- 通电后，电源和状态指示灯将转为绿色常亮。

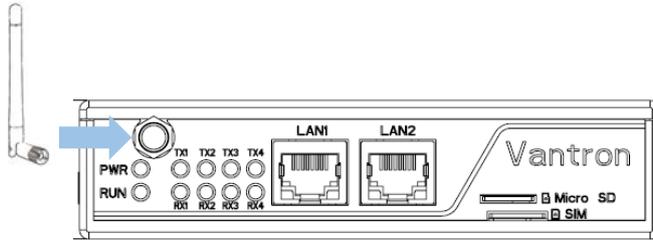
▶ 实际提供的天线可能与图示不同。如您在安装天线的过程中遇到问题，请联系销售代表解决

C335 网关

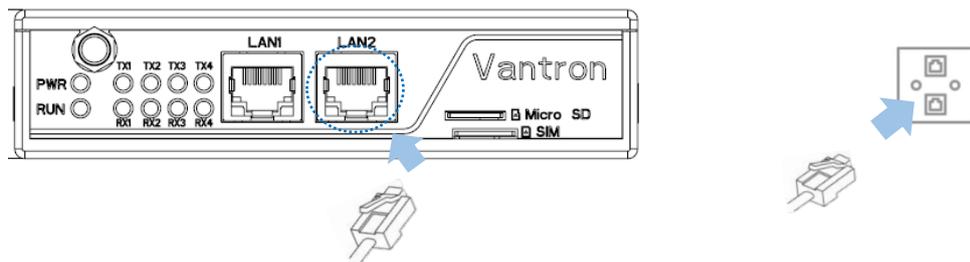
1. 使用安装支架和螺丝将网关安装在安全处；
2. 金属芯片朝上，将激活的 SIM 卡插入 SIM 卡槽；



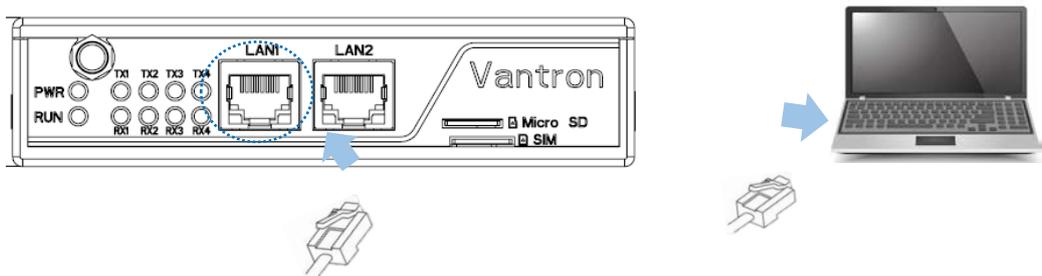
3. 推动 SIM 卡将其固定；
4. 按照上述步骤安装 Micro SD 卡，并保证金属排针朝下；
5. 将天线（具体功能取决于用户配置）安装到天线接头上，并紧固接头。



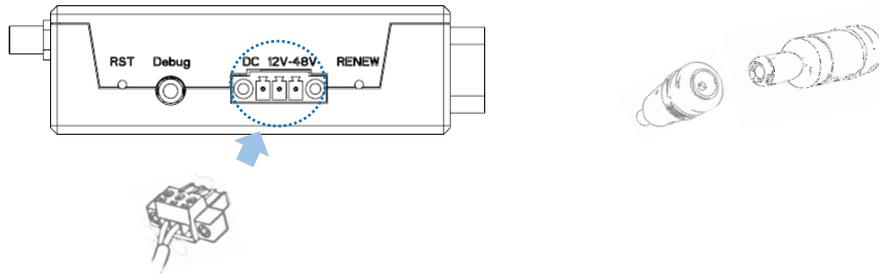
6. 将网线的一端连接至网关 LAN2（WAN 口），另一端连接至外网接口。



7. 将另一条网线的一端连接至网关 LAN1（LAN 口），另一端连接至个人电脑。



- 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。

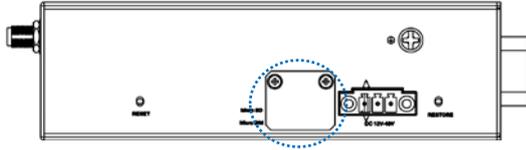


- 将适配器插入符合网关工作电压要求(12V-48V)的直流电源插座，使网关通电；
- 通电后，电源和状态指示灯将转为绿色常亮。

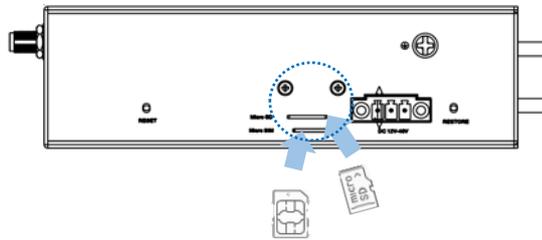
- ▶ 如果选择无线网络连接，则跳过第 6、7 步。
- ▶ 实际提供的天线可能与图示不同。如您在安装天线的过程中遇到问题，请联系销售代表解决。
- ▶ C335 的 mini-PCIe 插槽用于连接 4G/LTE 或者 Wi-Fi 及蓝牙模块，因此天线功能取决于用户选择何种通信模块。

C335S 网关

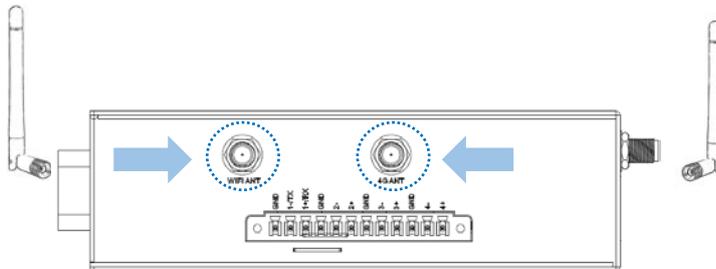
1. 使用安装支架和螺丝将网关安装在安全处；
2. 松开网关右侧 SIM 卡和 SD 卡盖板上的螺丝；



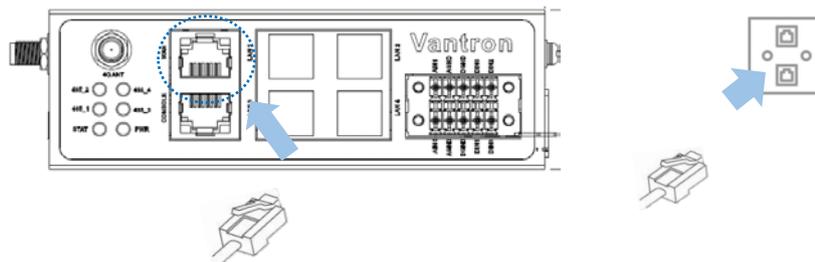
3. 金属芯片朝上，将激活的 SIM 卡插入对应的卡槽，同时金属引脚朝下，将 SD 卡插入对应的卡槽；



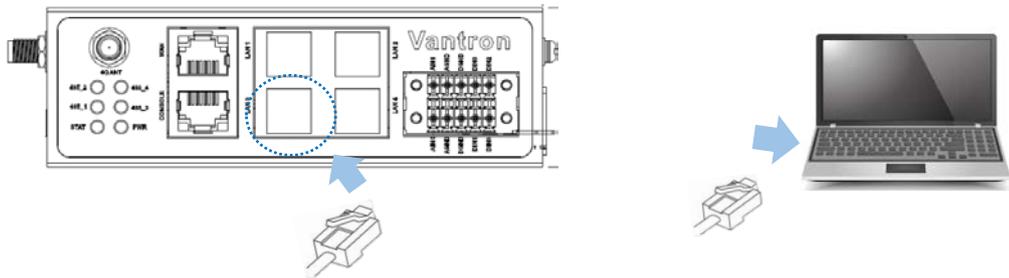
4. 推动 SIM 卡和 SD 卡将其固定；
5. 将盖板装回卡槽处，并拧紧螺丝；
6. 将天线安装到天线接头上，并紧固接头；



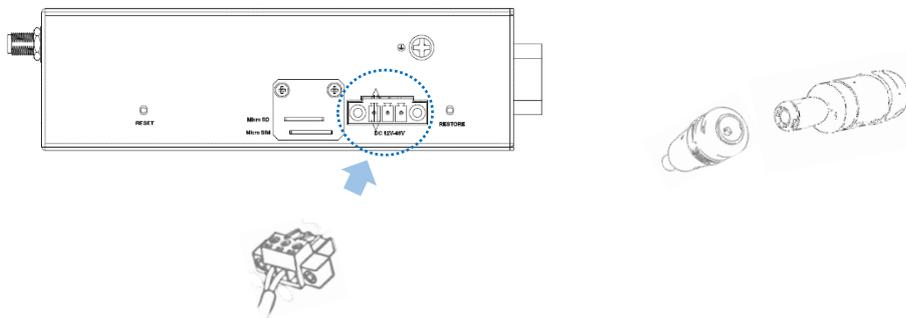
7. 将网线的一端连接至网关 WAN 口，另一端连接至外网接口；



8. 将另一条网线的一端连接至网关任意 LAN 口，另一端连接至个人电脑；



9. 将电源线的母头接入网关的电源端子座，圆头的一端与电源适配器连接；



10. 将适配器插入符合网关工作电压要求(12V-48V)的直流电源插座，使网关通电；

11. 通电后，电源和状态指示灯将转为绿色常亮。

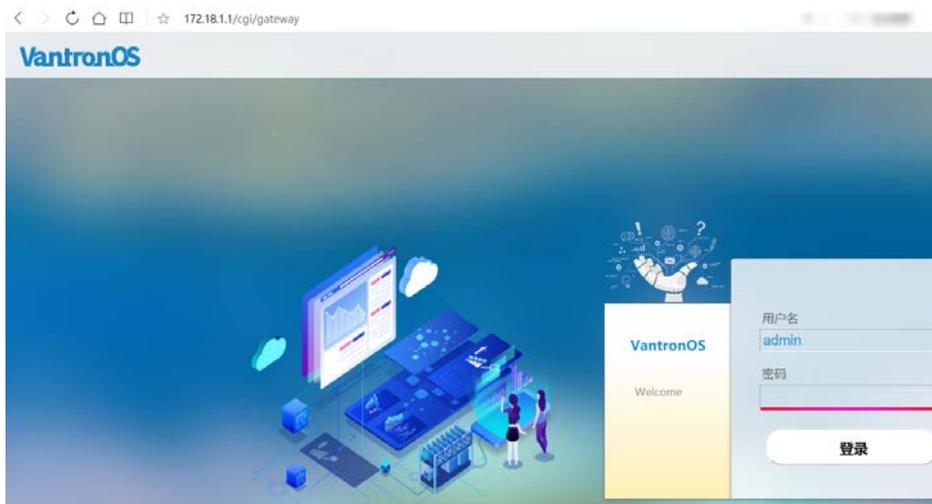
▶ 如果选择无线网络连接，则跳过第 7、8 步。

▶ 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 登陆网关

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 界面进行网关的网络设置和一些个性化配置。

1. 在浏览器中输入以下默认地址登录 VantronOS 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，用户可以通过该界面进行网关配置和变更。
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 [3.9.3](#) 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 DHCP 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。

因 C335 网关的 Wi-Fi 和 4G/LTE 功能为二选一。因此，如果用户选择 Wi-Fi 无线连接技术，则不能使用 4G/LTE 功能，反之亦然。

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 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或 IPK 软件包上传至网关，设置为开机运行或支持某些协议的应用。

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

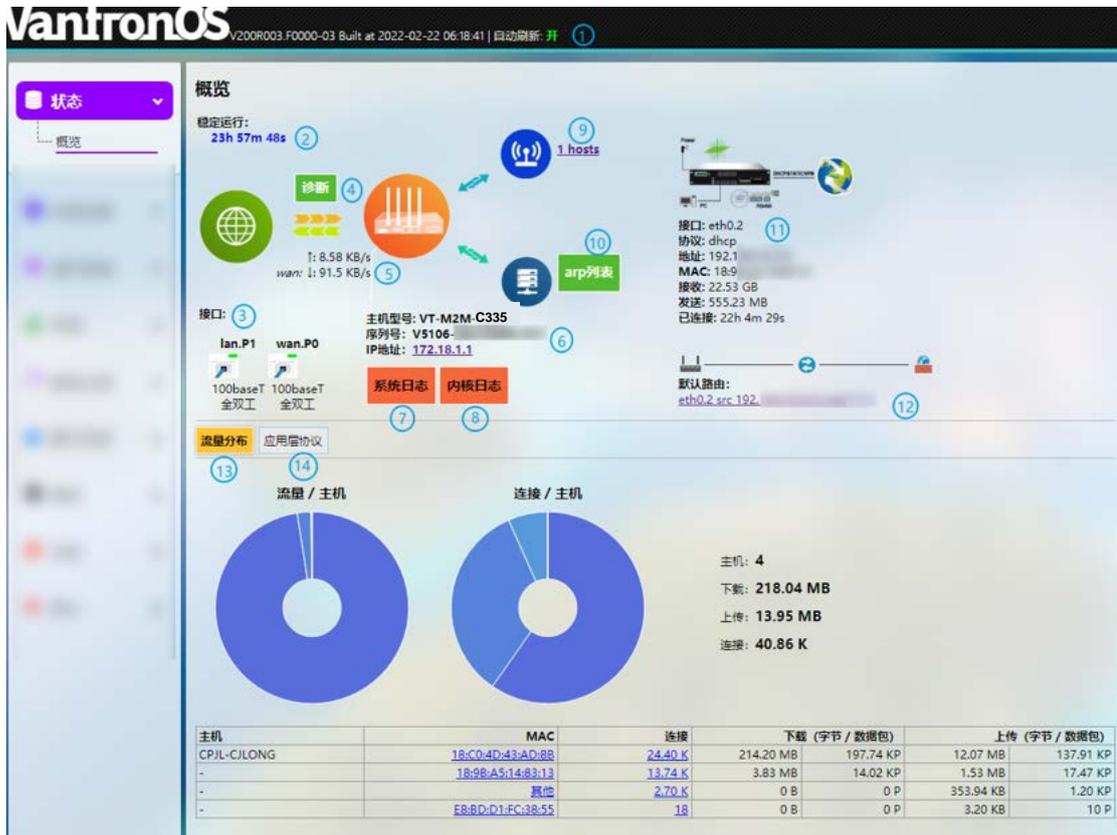
VantronOS 是万创团队共同协作，在 Linux 系统的基础上，利用嵌入式硬件，实现系统和功能独立自主开发的智能操作系统。系统采用模块化和插件扩展的设计理念，使用 Linux 内核配合防火墙功能，保障设备连接安全，不受攻击。基于 MVC 框架开发的 UI 界面支持简单高效的设置入口。VantronOS 可以与万创自主研发的 BlueSphere GWM 管理平台、Azure、阿里云、华为云、树根云等云系统对接，实现云端对工业物联网设备的监控、操作和诊断，以及用户与工业物联网设备之间的互联互通。

后文将就整个 C335 系列网关的配置和功能进行介绍，因此，用户实际网关页面的显示内容或跟此处介绍有所不同。

用户可以使用文件的导航窗格查看特定的配置或功能。

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。

IPv4-Address	MAC-Address
172.18.1	12:21:85:11:c5:d0
172.18.1	d6:a2:a0:2e:22:43
172.18.1	02:a5:e3:ea:a3:91
172.18.1	f8:c3:9e:97:a4:ff
172.18.1	02:54:3b:61:7f:8a
172.18.1	42:63:de:da:77:85
172.18.1	18:c0:4d:43:ad:8b

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的快速配网并展示了网口状态和接口逻辑图。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。
- ▶ 因 C335L 只有一个网口，默认工作于 LAN 区，所以 WAN 设置不适用该型号。但其网口也可以设置为 WAN 口，这种情况下，在 PPPOE/DHCP/静态地址等模式中，WiFi AP 连接网桥（br-lan），ETH0 连接上层网络。
- ▶ 由于 C335 的配置为 Wi-Fi 和 4G/LTE 通信模式二选一，因此，如果用户选择 4G/LTE 用于无线连接，则此处的 WiFi AP/client 连接不适用。
- ▶ 关于接口的说明，请参考 [1.4/1.5/1.6 接口定义](#)。

3.3.2 WAN 设置 – 自动获取 DHCP

自动获取 DHCP：ETH0 和 WiFi AP 绑定网桥(br-lan)。ETH1 为 WAN 口，连接上层网络。4G/LTE 接口在该模式下不工作。



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)。WiFi Client 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“自动”);
- 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, 则选择 **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 卡插入了卡槽并安装了 LTE 天线。
高级设置请参考 [3.5.3 4G/LTE](#)。

4G/LTE: ETH0、ETH1 和 WiFi AP 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 WiFi AP 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 WiFi AP 绑定网桥(br-lan)。ETH1 为 WAN 口，连接上层网络。

快速设置

快速网络配置工具，使用此工具能快速完成互联网配置

Wan口设置

出口协议 ① 静态地址Static 切换协议 ②

状态

设备: eth0.2
运行时间: 22h 19m 51s
MAC: 18:9B:A5:14:83:13
接收: 22.54 GB (12817982 数据包)
发送: 555.93 MB (8059355 数据包)
IPv4: 192.168.19.212/24

接口逻辑图

PPPoE/DHCP/Static
ETH1

br-lan
ETH0
WiFi AP

IPv4 地址 ③

IPv4 子网掩码 ④ 255.255.255.0

IPv4 网关 ⑤

IPv4 广播 ⑥

使用自定义的DNS服务器 ⑦

8.8.8.8 ×
114.114.114.114 +

返回或刷新

⑧ 保存&应用 保存 复位

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. 检测 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私有网络，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**修改**按钮，进入规则修改页面。

高级选项	
启用/禁用	① 启用
网络	② wan ③ 接口
Metric	③ 51 ④ 网关跃点取值范围: 1-255
超时计数	④ 2 ⑤ 次
检测超时	⑤ 8 ⑥ 秒
在线	⑥ 2 ⑦ 次
离线	⑦ 4 ⑧ 次
检查间隔	⑧ 10 ⑨ 秒
检测IP(心跳服务器)	⑨ 工厂默认值 ⑩ 多IP用空格隔开

返回或刷新

⑩ 保存&应用 保存 复位

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
- ① 如果跟踪成功，接口则视为在线。
7. 离线接口的数量
- ① 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. 检测 IP（心跳服务器）
- ① 使用空格键隔离多个 IP 地址。如果没有网络连接或者没有私有网络，可以将检测 IP 设置为上层设备的 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

如需在网关配置 VPN 客户端，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
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

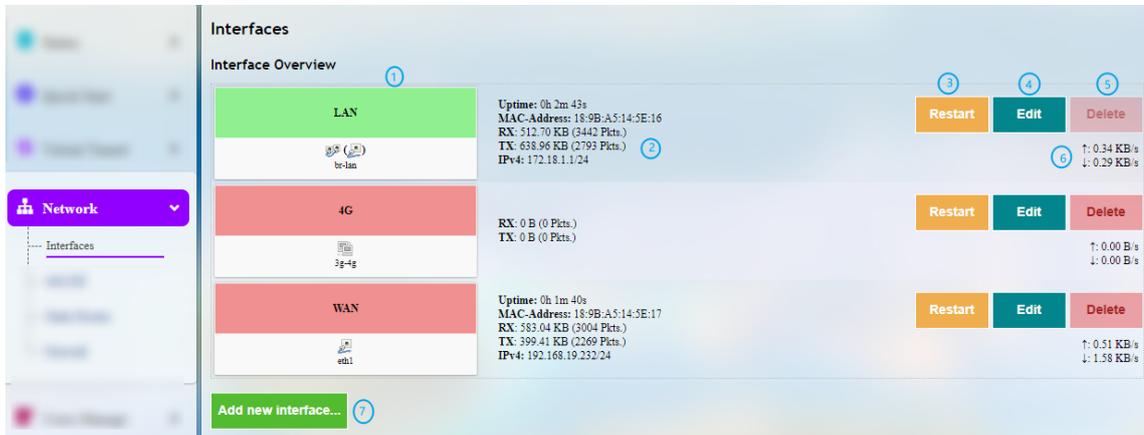
3.5 网络

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）

▶ 由于某些型号配置/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 口

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**。

接口 - LAN	
在此页面，您可以配置网络接口。您可以勾选“桥接接口”，并输入由空格分隔的多个网络接口的名称来桥接多个接口。接口名称中可以使用 VLAN 记号 INTERFACE.VLANNR（例如：eth0.1）。	
一般配置	
基本设置 高级设置	
状态	设备: br-lan 运行时间: 0h 9m 50s MAC: 18:9B:A5:14:83:13 接收: 393.37 KB (3887 数据包) 发送: 474.07 KB (3141 数据包) IPv4: 172.18.1.1/24
协议	静态地址
IPv4 地址	172.18.1.1
IPv4 子网掩码	255.255.255.0

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**。

接口 - LAN	
在此页面，您可以配置网络接口。您可以勾选“桥接接口”，并输入由空格分隔的多个网络接口的名称来桥接多个接口。接口名称中可以使用 VLAN 记号 INTERFACE.VLANNR（例如：eth0.1）。	
一般配置	
基本设置 高级设置	
重置 MAC 地址	7a:0d:4c:9f:f4:f1
重置 MTU	1500
使用网关跃点	与自动路由配置保持一致

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**标签旁会有一个**物理设置**标签，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:

DHCP 服务器	
基本设置	高级设置
动态 DHCP	<input checked="" type="checkbox"/> ① 为所有客户端提供 DHCP 服务。如果禁用，将只对具有静态租约的客户提供服务。
强制	<input type="checkbox"/> ② 即使检测到另一台服务器，也要强制使用此网络上的 DHCP。
IPv4 子网掩码	<input type="text"/> ③ 重设发送到客户端的子网掩码。
DHCP 选项	<input type="text"/> + ④ 设置 DHCP 的附加选项，例如设定 "6, 192. 168. 2. 1, 192. 168. 2. 2" 表示通告不同的 DNS 服务器给客户端。

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 口

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。

接口 - WAN

在此页面，您可以配置网络接口。您可以勾选“桥接接口”，并输入由空格分隔的多个网络接口的名称来桥接多个接口。接口名称中可以使用 VLAN 记号 INTERFACE.VLANNR（例如：eth0.1）。

一般配置

基本设置 高级设置

状态	①  设备: eth0.2 运行时间: 0h 16m 45s MAC: 18:9B:A5:14:83:13 接收: 672.31 KB (6320 数据包) 发送: 11.68 KB (278 数据包)
协议	② DHCP 客户端
请求 DHCP 时发送的主机名	③ VantronOS-CCC5

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：

接口 - WAN

在此页面，您可以配置网络接口。您可以勾选“桥接接口”，并输入由空格分隔的多个网络接口的名称来桥接多个接口。接口名称中可以使用 VLAN 记号 INTERFACE.VLANNR（例如：eth0.1）。

一般配置

基本设置 **高级设置**

使用默认网关	① <input checked="" type="checkbox"/>  留空则不配置默认路由
使用对端通告的 DNS 服务器	② <input checked="" type="checkbox"/>  留空则忽略所通告的 DNS 服务器地址
使用网关跃点	③ 与自动路由配置保持一致
重设 MAC 地址	④ 18:9B:A5:14:83:13
重设 MTU	⑤ 1500

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**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。再次强调，如果 C335 网关配置选择了 4G/LTE，则该功能不适用。

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。

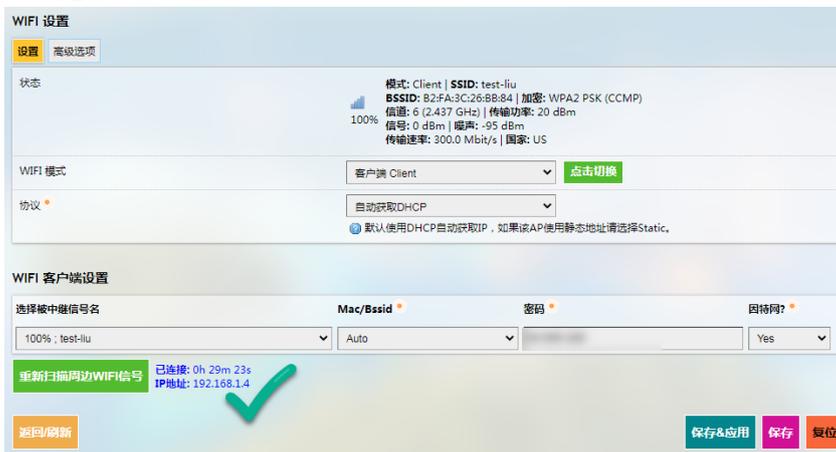
▶ 如果将 Wi-Fi 配置为客户端模式，将自动添加 `wwan0` 接口。



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
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

如果 C335 网关配置选择了 Wi-Fi，则此页面不会展示。

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。



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
进站数据	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

点击区域后面的**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）：

名字	匹配规则	转发到	启用
尚无任何配置			

名字	协议	外部区域	外部端口	内部区域	内部 IP 地址	内部端口	
3222to22	TCP+UDP	wan	3222	lan	172.18.1.174 (CPJL-CJLONG.lan)	22	添加

编号说明

1. 规则名称
2. 协议（支持 TCP/UDP/TCP + UDP）
3. 外部区域：选择 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：

添加新用户

用户配置

用户名 ①

用户组 ②

SSH 访问 ③

开启网络菜单

接口 无线设置 4G/LTE 路由表 防火墙 Anti_DDoS

开启虚拟隧道菜单

VPN 客户端 OpenVPN 服务器

开启定制应用菜单 ④

厂商信息定制 定制程序 DMP Agent IPK安装器

开启服务菜单

动态DDNS PLC远程连接

开启硬件资源菜单

串口转TCP

开启系统菜单

系统 管理权 挂载点 备份/升级 重启 带宽监视 Web终端

开启快速设置菜单

自动线路 快速联网

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。

ADMIN

用户

用户概览

ADMIN

SSH 访问: Disabled
用户名: admin
添加日期: Fri Mar 10 06:34:09 2023
上次进入: Fri Mar 10 06:34:09 2023

修改 删除

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）上传到网关，并设置为在启动时运行。



编号说明

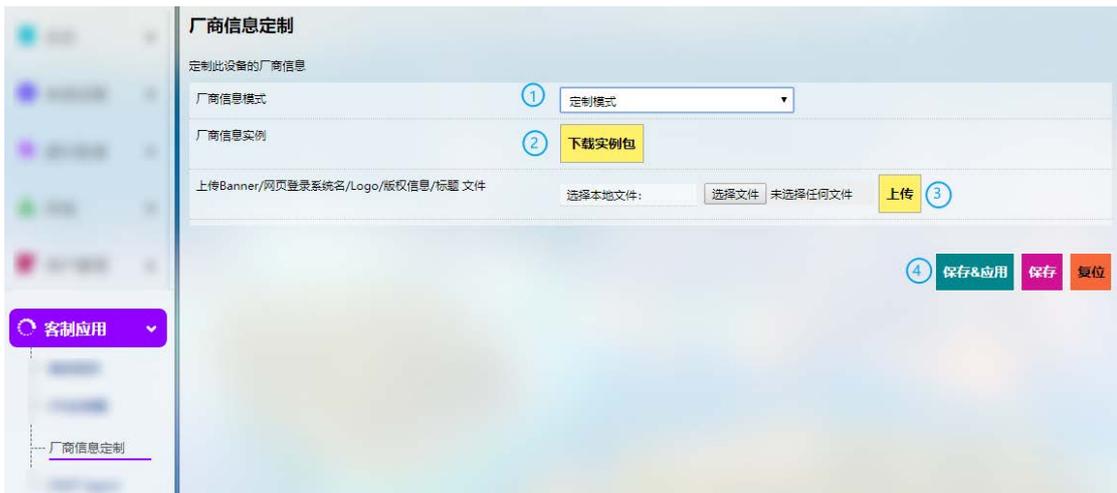
1. 选择要上传到网关的脚本
2. 上传脚本至网关
3. **保存 & 应用** 上述设置
4. 当脚本成功上传后，将显示文件名和文件目录
5. 启用该脚本，则该脚本将在下次启动网关时运行
6. 如果上传多个脚本，用户可以上下移动任意脚本，重新排列脚本顺序，并编辑/删除脚本

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。

3.7.5 SNMP 服务

SNMP 基本组件包含：

网络管理系统（NMS）—用于监控和管理网络的所有硬件（设备）和软件（SNMP 管理器）合集。SNMP 管理器负责采集被管理设备的相关信息，包括网络连接、活动、事件等。

被管理设备—被管理设备是一个网络中被 NMS 管理的任意设备，也叫网络元素。典型的被管理设备有路由器和开关等。

SNMP 代理—SNMP 代理响应 SNMP 管理器关于信息与行动等请求。SNMP 代理同时还控制其管理信息数据库（MIB）的访问，MIB 主要由 SNMP 管理器可以查看或修改的各种对象构成。MIB 包含名称、数据类型和对象标识符(OID)。OID 使用数字地址来检查网络设备组成部件（如 CPU、内存、电源、网络流量等）的状态。



编号说明

1. 启用/禁用 SNMP 服务
2. SNMP 代理默认使用 UDP 161 端口听取管理器发出的 SNMP GET 等请求
3. 用户自定义 SNMP 指令名称
4. 指令内容
5. 命令参数
6. OID（每一个数值都代表相应的信息）
7. 删除现有指令
8. 添加新指令

9. 保存 & 应用上述设置

10. 高级配置

▶ 若不适用，请保留字段原样。

一个 SNMP 代理即一个自动化 SNMP engine。仅 SNMPv3 实体使用 Engine ID 进行唯一的识别。在高级配置项下，用户可以编辑服务器和 engine ID 的信息。

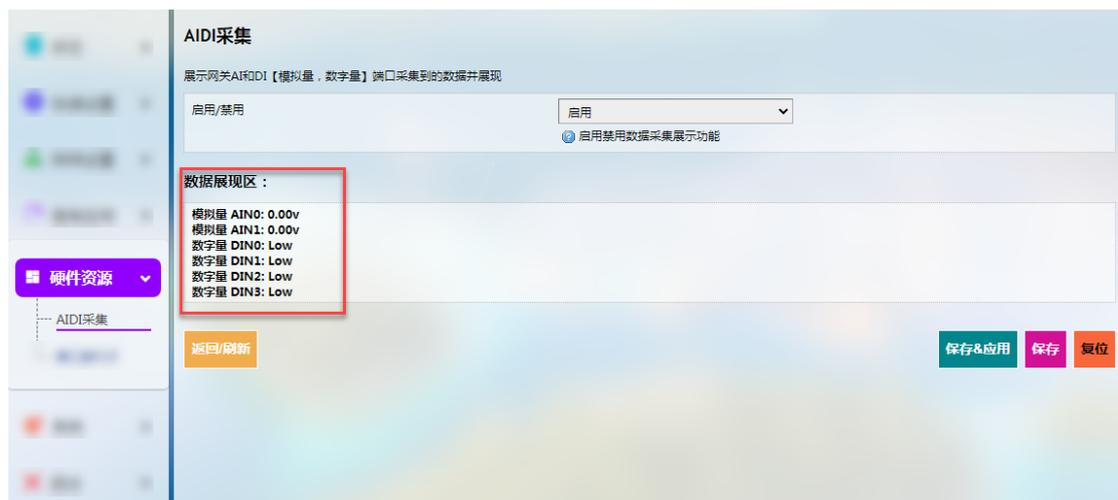
3.8 硬件

3.8.1 AIDI 采集

C335S 配备了 2 个模拟输入接口（AIN0 & AIN1）和 4 个数字输入接口（DIN0, DIN1, DIN2, DIN3）。



用户可以在该页面启用数据采集显示，并读取接口数据。



▶ 模拟输入电压范围：0-8V。

▶ 数字输入电压范围：0-3.3V。

3.8.2 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。

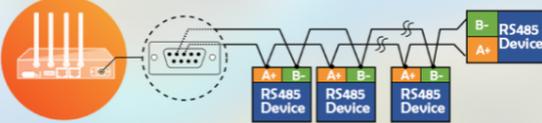
串口转TCP

这是一个将串口转化成TCP协议的工具

设备	启用/禁用	波特率 此设备的波特率	修改	删除
/dev/ttyDemo	禁用	115200	修改	删除
/dev/ttyUSB0	禁用	115200	修改	删除
/dev/ttyUSB1	禁用	9600	修改	删除

添加

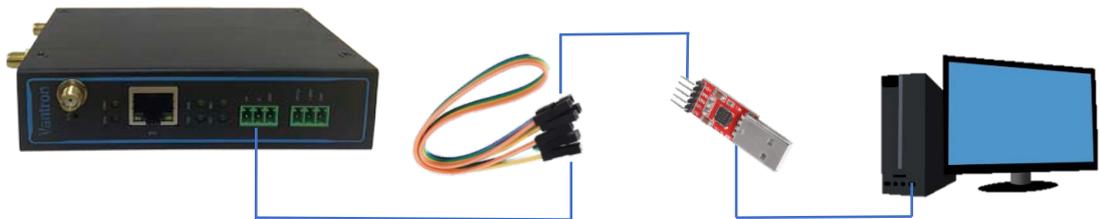
串口列表及详情



串口号	波特率	状态	被调用进程PID	进程名
/dev/ttyO0	115200	using	1262	/sbin/askfirst
/dev/ttyO1	115200	idle	null	null
/dev/ttyO2	3000000	using	3657	brcm_tool
/dev/ttyO3	115200	idle	null	null
/dev/ttyO4	9600	idle	null	null
/dev/ttyS0	9600	using	2845	/usr/bin/vt_datacapture

3.8.3 Ser2net 环境搭建与验证

- 环境准备：
 - 一台 C335 系列网关（C335L 为例）
 - 一台运行 Ubuntu 系统的主机
 - USB 转 TTL 串口适配器
 - 杜邦线
 - 如下图所示，连接 C335L 网关串口和主机（以左边的 RS485 串口(R2)为例）



- 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

高级设置	
启用/禁用	启用 ①
工作模式	客户端模式 ②
服务器与端口	192.168.93.1:8888 ③ <small>例如：177.6.6.6:678</small>
设备	/dev/ttyO4 ④
波特率	115200 ⑤ <small>此设备的波特率</small>
检测超时	20 ⑥ <small>单位：秒</small>
数据位	8 bits ⑦
奇偶校验	无 ⑧
停止位	1 ⑨

返回或刷新 保存&应用 保存 复位

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 [1.4.3](#) 所述，左边(R2) RS485 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

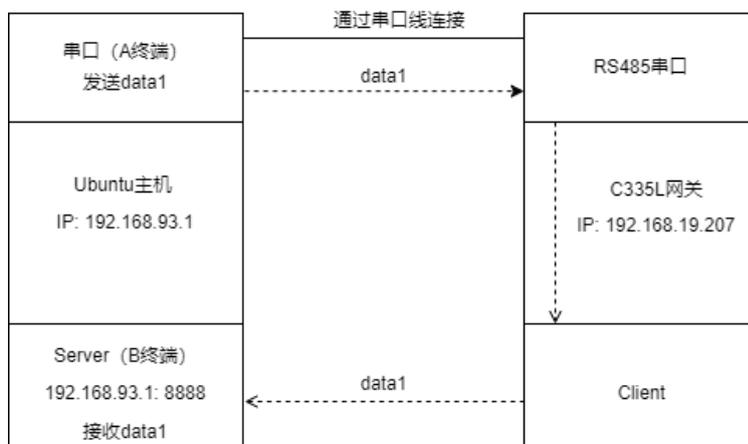
- 在 A 终端使用 `microcom` 工具命令打开串口（假设识别出 USB 转 TTL 串口适配器的设备名为 `/dev/ttyUSB1`）

```
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

串口转TCP

这是一个将串口转化成TCP协议的工具

设备	启用/禁用	波特率 此设备的波特率	修改	删除
/dev/ttyDemo	禁用	115200	修改	删除
/dev/ttyUSB0	禁用	115200	修改	删除
/dev/ttyUSB1	禁用	9600	修改	删除
	启用	115200	修改	删除

添加

串口列表及详情

串口号	波特率	状态	被调用进程PID	进程名
/dev/ttyO0	115200	using	1312	/sbin/askfirst
/dev/ttyO1	115200	idle	null	null
/dev/ttyO2	3000000	using	3530	brcm_tool
/dev/ttyO3	9600	idle	null	null
/dev/ttyO4	115200	using	4991	/usr/plc_protocol/plugin_loader
/dev/ttyS0	9600	idle	null	null
/dev/ttyUSB0	9600	idle	null	null
/dev/ttyUSB1	9600	idle	null	null
/dev/ttyUSB2	9600	idle	null	null
/dev/ttyUSB3	9600	idle	null	null

返回或刷新 **保存&应用** **保存** **复位**

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

高级设置	
启用/禁用	启用 ①
工作模式	服务器模式 ②
端口	10 ③ 0~65535
协议	Telnet ④
设备	/dev/ttyO4 ⑤
波特率	115200 ⑥ 此设备的波特率
检测超时	20 ⑦ 单位: 秒
数据位	8 bits ⑧
奇偶校验	无 ⑨
停止位	1 ⑩

返回或刷新 保存&应用 保存 复位

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 [3.8.4](#)）
5. 选择串口设备（如 [1.4.3](#) 所述，左边(R2) RS485 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

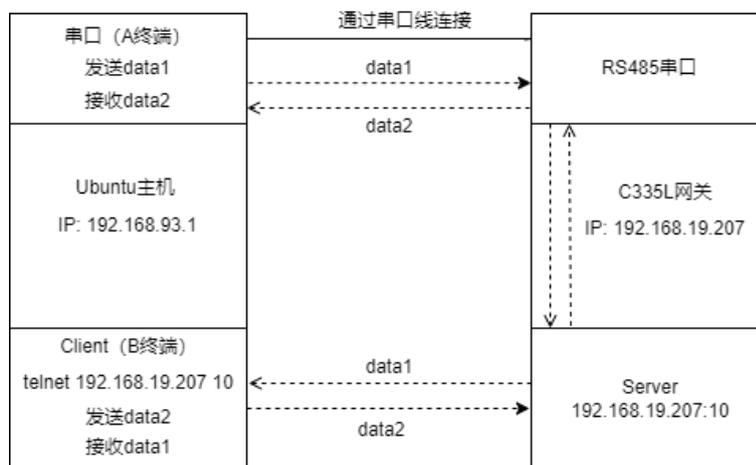
- 在 A 终端使用 `microcom` 工具命令打开串口（假设识别出 USB 转 TTL 串口适配器的设备名为 `/dev/ttyUSB1`）

```
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



3.8.4 协议对比

在服务器模式下，存在三种协议，区别如下：

- Raw:** 启用端口，在端口和长整数之间按照原样传输所有数据。
- 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。
- 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）。

PLC远程连接

第一步：上传key

设置 运行日志

上传Key文件 选择文件 未选择任何文件 连接

重启核心进程 已连接, IP地址: 10.8.0.2

第二步：配置IP映射关系

状态	PLC IP地址	虚拟IP	标记
Not Ready	172.18.1.132	10.8.0.6	

添加 删除

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

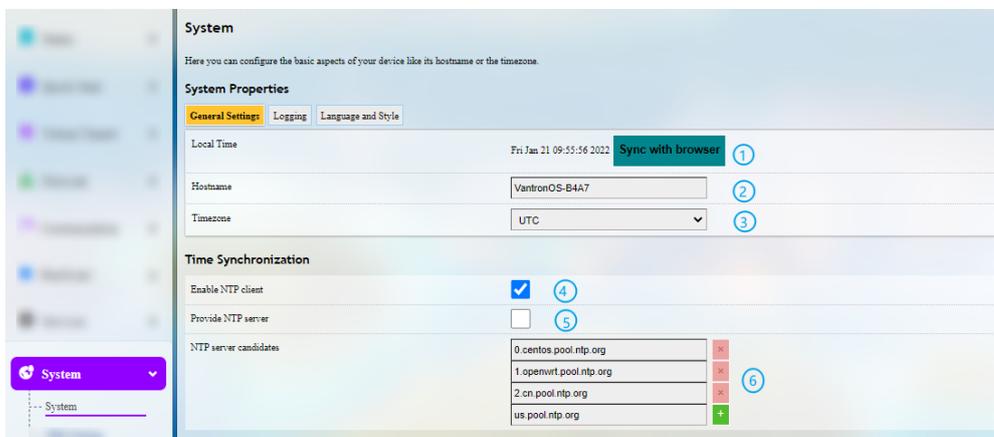
若安装了工业协议相关.ipk 文件，以 root 账号登录后，可在 VantronOS 页面查看协议相关服务，其信息展示与万创工业协议端口页面展示一致。

请参考第四章内容了解工业协议的配置及应用。

3.10 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

网络带宽监视器 (nlbwmon) 是一个轻量、高效的流量统计程序，可以统计每个主机和协议的带宽使用情况。

基本设置 | 高级设置 | 协议映射

统计周期 ① 每月的某一天
② 选择“每月的某一天”来设置统计周期的重启时间，例如：每个月的第 3 天。选择“固定周期”来设置从给定日期开始每 N 天重启统计周期。

重置日期 ② 1 - 每月的第一天重新开始
② 每个月重启统计周期的日期。使用负数表示从月底开始计算，例如：“-5”可以表示 7 月份的 27 号或者 2 月份的 24 号。

本地接口 ③
 4g
 lan
 plc2down
 vpn
 wan
③ 仅统计来自或目标为这些网络接口的连接流量。

本地子网 ④
192.168.0.0/16
172.16.0.0/12
10.0.0.0/8
④ 仅统计来自或目标为这些子网的连接流量。

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

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。



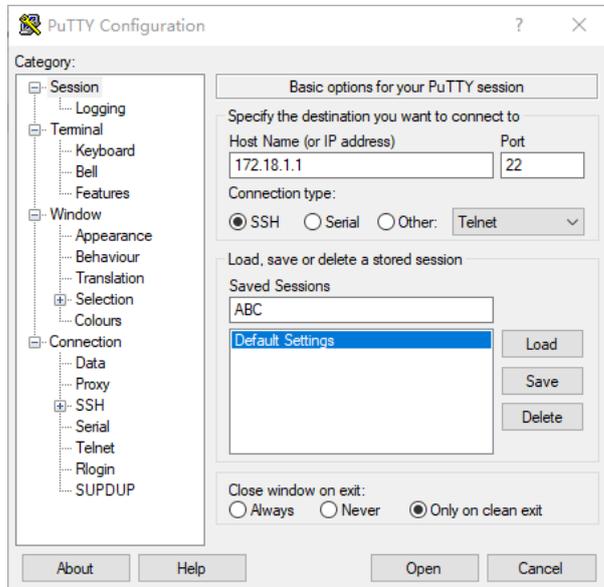
编号说明

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

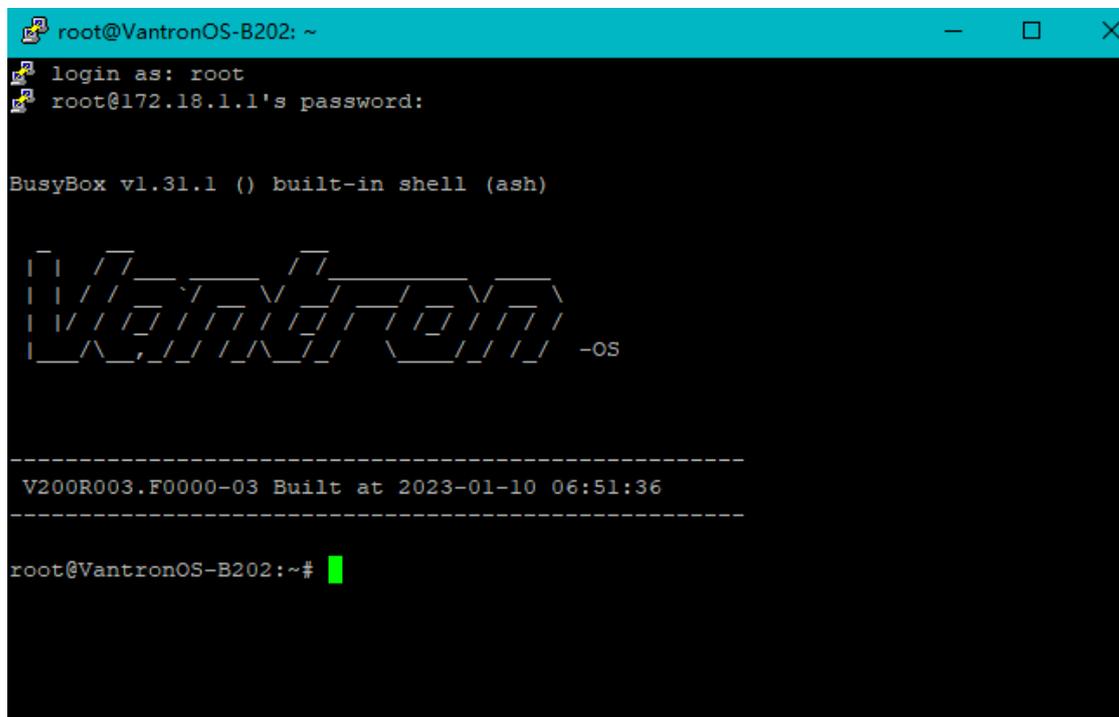
第 4 步：在 Windows 主机打开 SSH 客户端工具（推荐 PuTTY 或 MobaXterm）；

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（同网关登录密码一致），并开启 SSH 远程会话。



3.10.4 终端

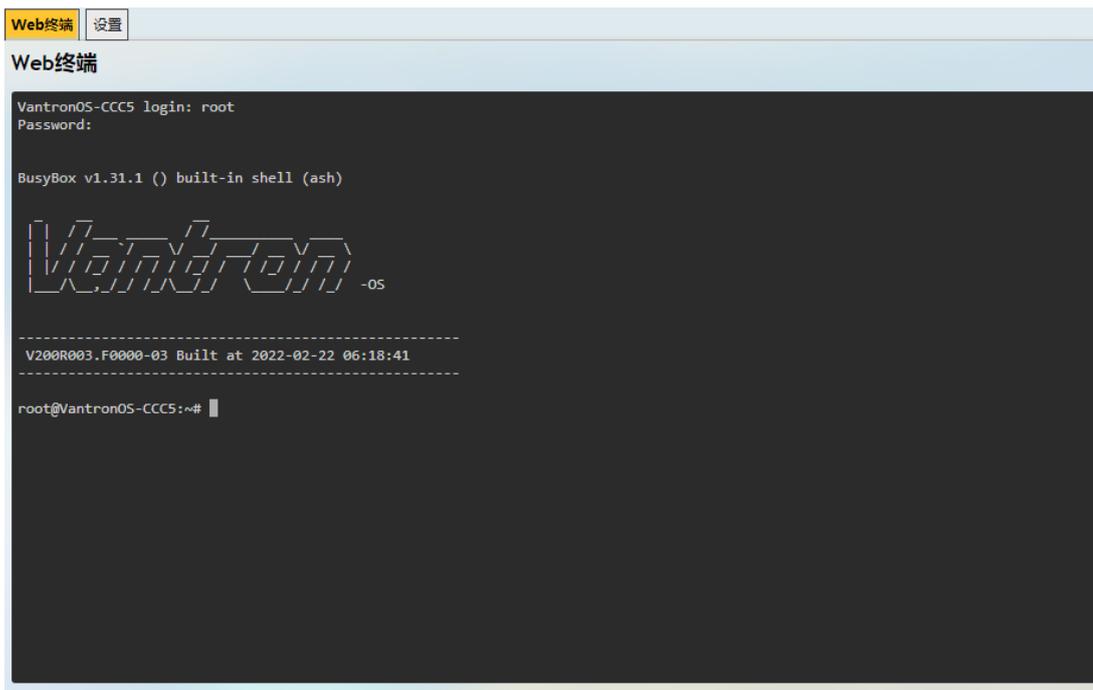
在 Web 终端页面**设置**项下点击**启用** Web 终端并保存&应用后，用户可以登录并输入命令行。



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



3.10.5 挂载点

用户可以在此启用/禁用自动挂载并查看挂在信息。

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 升级固件应用件。

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。

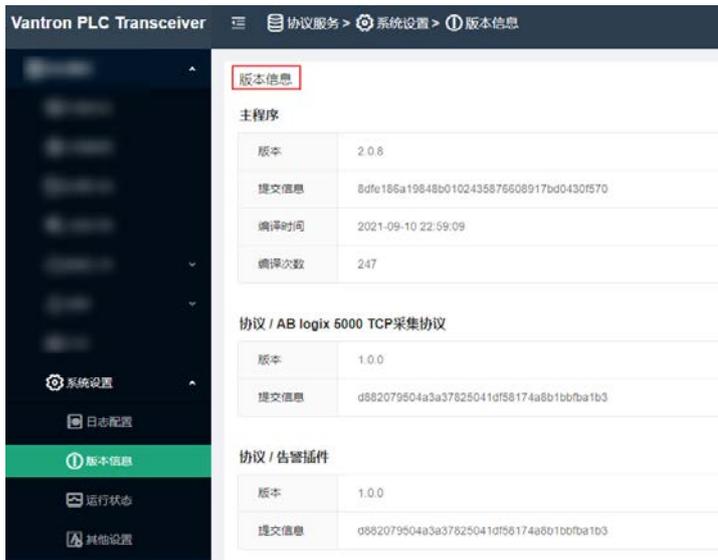


之后在网关 IP 地址后，输入端口号（8081），如：172.18.1.1:8081，进入协议登录页面，然后输入用户名和密码登录（与网关用户名和密码一致）。

- 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。

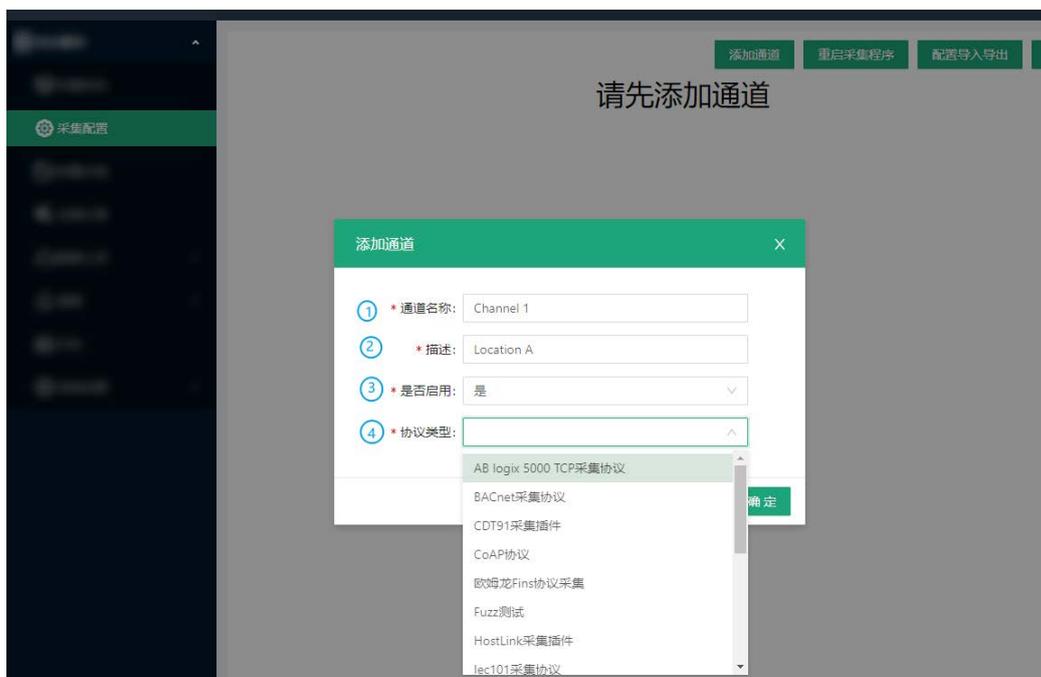


4.2 协议配置与应用

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。

添加通道

- 1 * 通道名称: Channel 1
- 2 * 描述: Modbus
- 3 * 是否启用: 是
- 4 * 协议类型: Modbus采集协议
- 5 * 通信方式: Modbus 串口通讯
- 6 * 协议模式: Modbus RTU
- 7 * 串口: COM3
- 8 * 串口模式: RS485
- 9 * 波特率: 9600
- 10 * 数据位: 8
- 11 * 校验位: N
- 12 * 停止位: 1
- 13 * RTS: 无

取消 确定

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. 选择对应的网关串口
8. 确定串口类型（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。



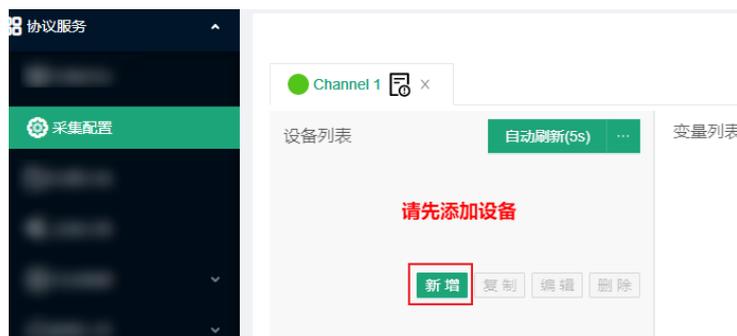
编号说明

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。



新增

① * 设备名称: RS232通讯一个通道只能创建一个设备

② * 从站地址: 从站地址0~255

③ * 是否启用: 是

④ * 采集周期(毫秒): 1000

⑤ * 寄存器起始位: 0

⑥ 数据下发: 选择数据源

取消 确定

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。



新增变量到设备57_200 smart×

① * 变量名:

② * 标题:

③ * 权限:

④ * 功能码:

⑤ * 数据类型:

⑥ * 寄存器地址:

⑦ * 数值运算:

⑧ 通过CSV上传⑨ 下载模板

取消确定

编号说明

1. 输入该 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）

通过CSV上传导出变量

取消确定

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。



数据采集设备及其点位的变量配置完成后，可以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。



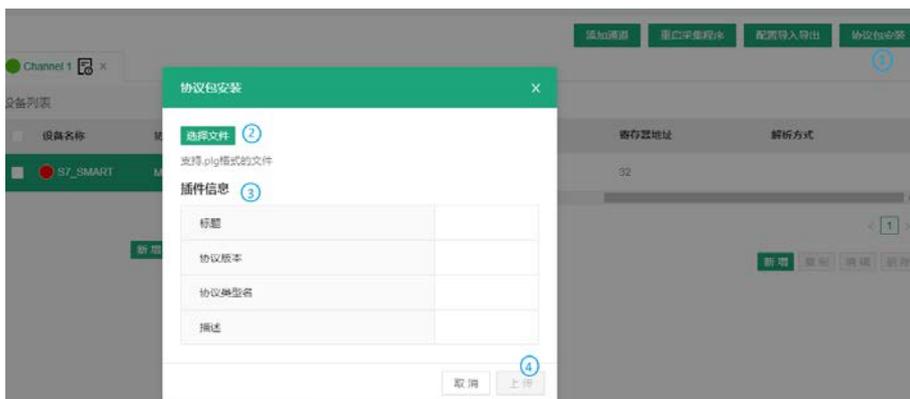
编号说明

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。

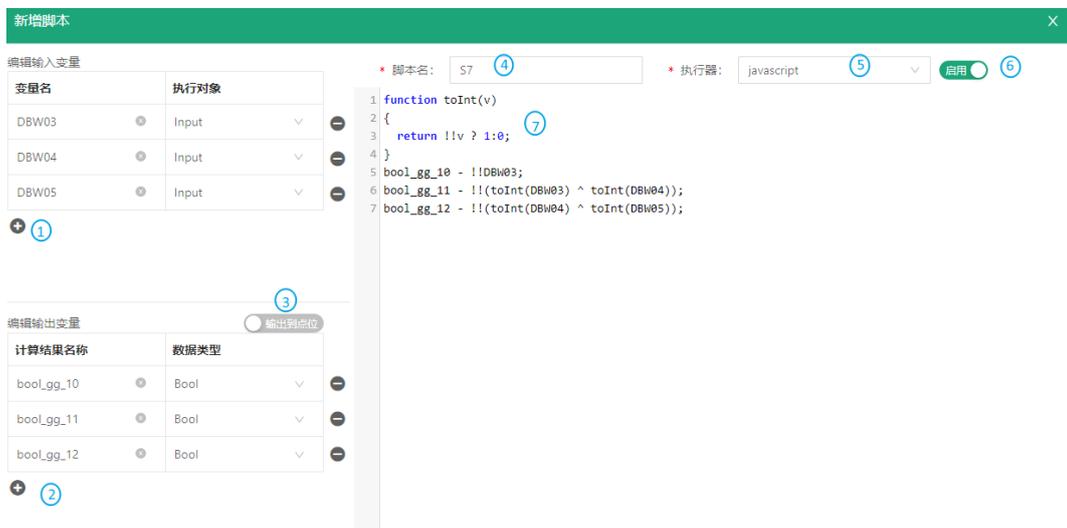


编号说明

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。

脚本名称	执行对象	执行策略	最后一次执行状态	执行次数	操作
<input type="checkbox"/> S7	[DBW03,DBW04,DBW05]	定时执行	失败	628	<input type="checkbox"/> 暂停 复制 编辑 删除
<input type="checkbox"/> edge computing	[DBW03,DBW04,DBW05]	定时执行	失败	628	暂停 复制 编辑 删除

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）

脚本名称	当前策略	执行间隔	执行环境复用机制
<input type="checkbox"/> S7	定时执行	1000	执行100次后重启
<input checked="" type="checkbox"/> edge computing	定时执行	1000	执行100次后重启
<input checked="" type="checkbox"/> edge computing_1	定时执行	1000	执行100次后重启

2个脚本被选中

* 执行方式: 定时执行

* 执行间隔: 定时执行 ms

* 执行环境复用: 自动触发

取消 确定

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。

设备列表 (5)	变量列表 (5)	所有分组 (4)	自动刷新(2s)	刷新	
变量名称	变量值	所属设备 (3)	通道 (5)	读写模式 (6)	操作 (6)
<input type="checkbox"/>	Switch_on	S7_200 smart	Channel 1	只读	
<input type="checkbox"/>	Switch_off	S7_200 smart	Channel 1	只读	
<input type="checkbox"/>	result	S7_200 smart A	边缘计算		
<input type="checkbox"/>	bool_gg_10	S7_200 smart B	边缘计算		
<input type="checkbox"/>	bool_gg_11	S7_200 smart B	边缘计算		

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. 自动刷新闻隔
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。

新建数据上传服务

* 通道名称: channel 1

* 协议类型: MQTT协议

* 云平台: MQTT客户端

取消 确定

- 其后，在 MQTT 客户端页面进行详细配置。

The image shows a configuration form for an MQTT client. It consists of ten numbered steps, each with a corresponding field or control:

1. 启用: A checkbox that is checked.
2. 数据封装: A dropdown menu with '无' selected.
3. 中心平台: A dropdown menu with 'MQTT客户端' selected.
4. 地址: A text input field containing '192.168.16.229'.
5. 端口号: A text input field containing '1883'.
6. MQTT心跳间隔: A text input field containing '90'.
7. MQTT客户端ID: A text input field containing '12345678'.
8. qos: A dropdown menu with '1' selected.
9. 数据上传主题: A text input field containing 'dryer'.
10. 订阅主题: An empty text input field.

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

The screenshot shows a configuration interface with the following elements:

- 11. 用户名: [Text input field]
- 12. 密码: [Text input field with eye icon]
- 13. 启用SSL: [Dropdown menu with '普通SSL' selected]
- 14. 服务器认证方式: [Dropdown menu with '内置根证书校验' selected]
- 15. 客户端认证: [Checked checkbox]
- 16. 客户端证书: [Text area containing a certificate block starting with '-----BEGIN CERTIFICATE-----']
- 17. 客户端私钥: [Text area containing a private key block starting with '-----BEGIN PRIVATE KEY-----']
- 18. 客户端私钥密码: [Text input field with eye icon]

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. 填写客户端私钥密码（非必须）

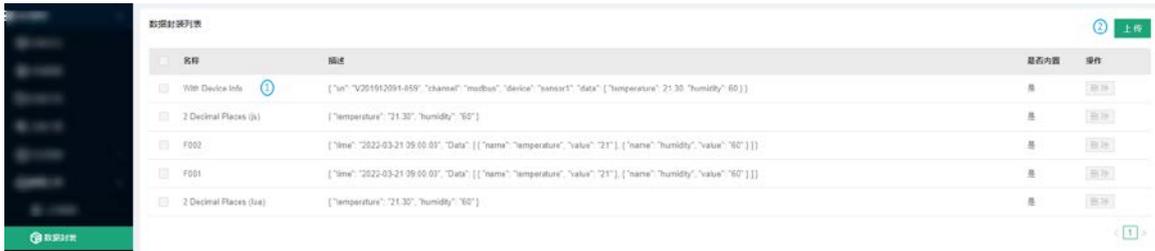
The screenshot shows a configuration interface with the following elements:

- 19. 数据缓存: [Checked checkbox]
- 20. 缓存方式: [Dropdown menu with '内存' selected]
- 21. 最大存储条目: [Text input field with value '1000']
- 22. 最大存储占用: [Text input field with value '10' and unit 'M']
- 23. 最小上传间隔: [Text input field with value '0' and unit 's']
- 24. 选择设备: [Dropdown menu]

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. 内置的数据封装列表（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。

新增报警规则

1 * 名称: 高温报警

2 * 变量: Channel 1 / S7_SMART / Input

3 * 报警信息: over heat!!!!

4 * 是否启用:

* 报警条件:

- < -20 不报警
- < 0 不报警
- < 45 不报警
- > 60 III

注: 条件从上往下匹配

8 数据联动: Channel 1 / S7_SMART / Input

9 取消 确定

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。

报警推送

① * 报警间隔: 秒

② * 报警记录最大存储: 兆

③ * 启用结果输出:

④ * 报警输出到:

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。

④ * 报警输出到:

⑤ 报警接收地址:

⑥ * 发件服务器: SSL 端口:

⑦ * 加密传输: 如果服务器支持，就使用加密传输

⑧ * 用户名:

⑨ 服务器身份验证: 开

⑩ * 密码:

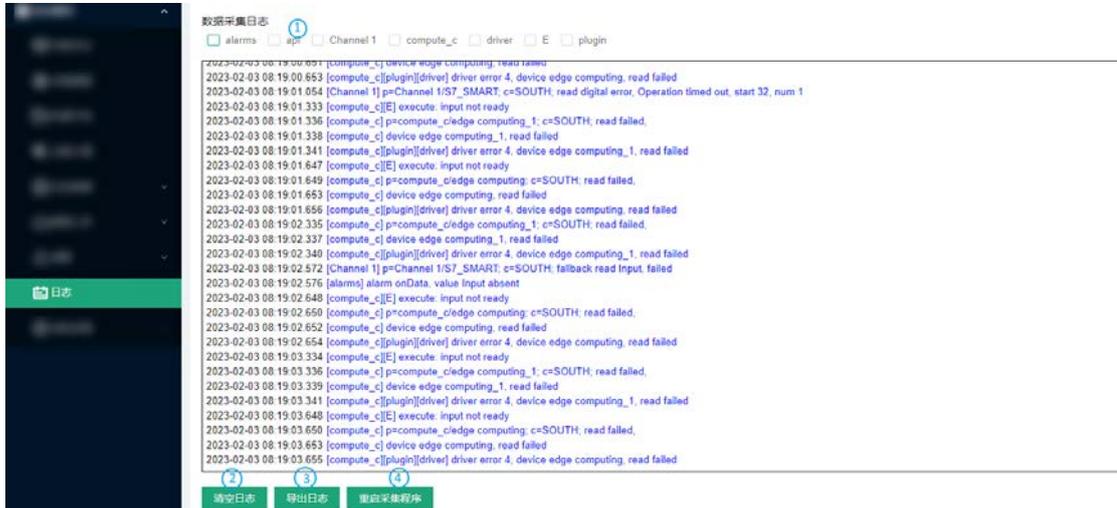
5. 填写接收推送的邮箱地址
6. 填写发件服务器 IP 地址（可查看所使用的邮件服务器设置）
7. 如果服务器支持，可选择加密传输
8. 设置报警推送的用户名
9. 选择是否打开服务器身份验证
10. 如果开启服务器身份验证，则需要输入密码

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

日志配置

* 控制台日志级别: INFO

① * Web日志级别: INFO

* 文件日志级别: WARNING

② * 单个日志文件大小: 1024 K

注: 日志配置后需要重启采集程序才能生效

取消 确定 ③

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 and 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，才能退回给万创。万创应在客户要求后的 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 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。