Modbus 网关通讯协议

1、产品简介

卓岚带 Modbus 协议网关的产品可以将网络 Modbus tcp 协议和串口 Modbus rtu 协议进行互转，并且还有多主机功能。

设置为 Modus 网关时，可以让多个主机查询，设备会分别应答，实现多主机查询；在非 Modbus 网关模式下，只要勾选更多高级选项的“多主机”支持同样也可以实现多主机查询的调度。

卓岚多主机技术是为多机同时监控一台设备而开发的技术。在普通设备中，当有 A、B 两台监控计算机时，A 和 B 都可以将数据发向设备，但是设备从串口收到的数据会同时发送给 A、B。也就是说当 A 和设备通信时，B 会收到不想要的数据，这样会干扰 B 的通信，很多软件协议将无法适应这种情况，可能无法运转。

卓岚多主机技术能够实现 A、B 计算机之间的通信调度，当 A 与设备通信时，设备的回复数据只发给 A；当 B 需要通信时又可以快速切换给 B。

2、Modbus 协议简单介绍

Modbus 协议定义了总线上主站（Master）与从站（Slave）之间的通讯格式。MODBUS 协议包含 ASCII 和 RTU 两种格式，两种格式的通讯字段含义是相同的，差别在于字段的传输方法不同、帧开始与结束的判断条件不同、数据校验的方法不同。目前 GUTTA PLC 支持 RTU 通讯格式（虽然在 CPU-EC20 系统功能块中保留了 7 位 ASCII 模式的配置，但并未实现。）

完整的 Modbus RTU 帧应该是下面的格式（不论是主站发起还是从站应答）：

空闲	地址	功能码	数据	CRC 校验	空闲
	1 个字节	1 个字节	N 个字节	2 个字节	

站地址用来指示哪个从设备来应答主站的通讯报文。在总线上，每个从设备必须指定一个唯一的站地址，只有当通讯报文中地址与该从设备地址相同时，该从设备才能应答主站的通讯报文。从设备应答的通讯报文也必须包含该地址，以告知主站，这个通讯报文是哪个从设备应答的。

完整的 Modbus TCP 帧应该是下面的格式：

MBPA 报头文				功能码	数据区
传输标志	协议标志	长度	地址	功能码	数据
2 个字节	2 个字节	2 个字节	1 个字节	1 个字节	N 个字节

MBAP 报文头格式

域	长度	描述	客户端	服务器端
传输标志	2 字节	标志某个 Modbus 询问/应答的传输	由客户端生成	应答时复制该值
协议标志	2 字节	0=Modbus 协议 1=UNI-TE 协议	由客户端生成	应答时复制该值
长度	2 字节	后续字节计数	由客户端生成	应答时由服务器端重新生成
单元标志	1 字节	定义连接于目的节点的其它设备	由客户端生成	应答时复制该值

Modbus TCP 转 RTU 详细分析

Modbus rtu 数据：02 06 01 00 01 02 08 54

由 modbus rtu 帧格式可知：

1 字节：从设备站地址

2 字节：功能码

3～4 字节：起始地址

5～6 字节：数量

7～8 字节：CRC 效验码

Moebus tcp 数据：00 01 00 00 00 06 02 06 01 00 01 02

由 Modbus TCP 帧格式可知：

1～2 字节：00 01 是传输标志

3～4 字节：00 00 是协议标志

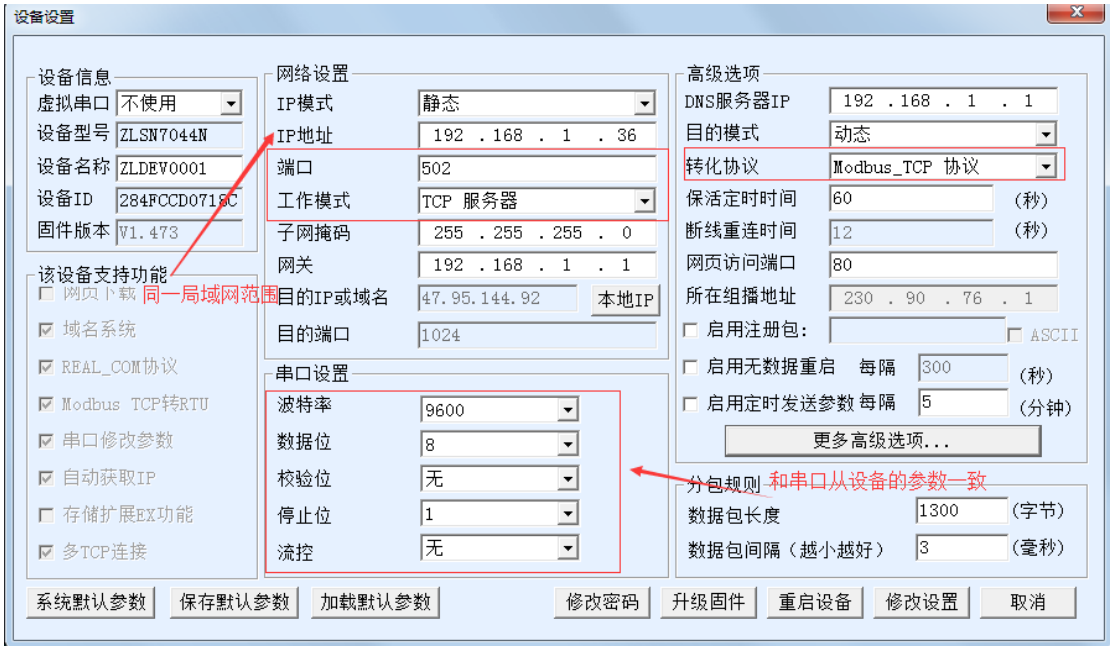
5～6 字节：00 06 是后续字节数的标志

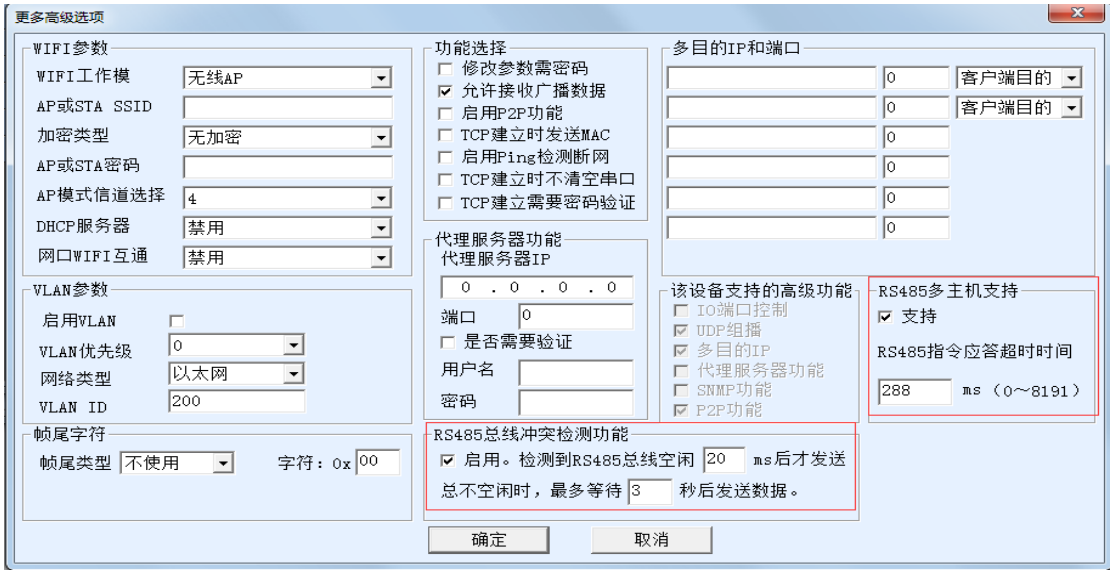
后续字节：RTU 数据去除末尾 CRC 校验的部分。

3、常见使用案例

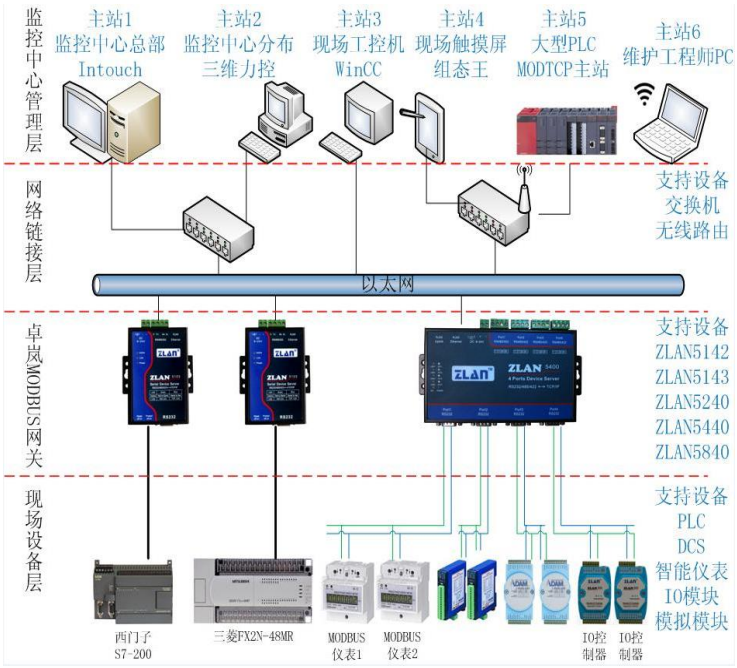
3.1 单设备 modbus 协议网关的使用

客户大部分的使用场景是：网络终端做主站去访问串口从设备的数据。则我们设备配置如下：



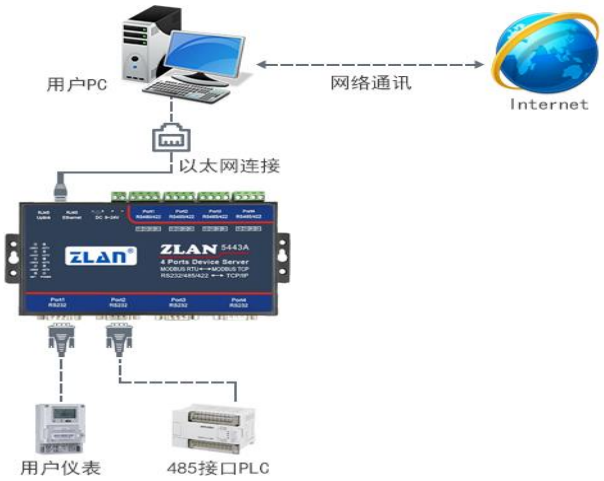


一般带 modbus 协议网关的产品串口 485 可以手拉手最多挂载 32 个，带隔离型 modbus 协议网关的产品手拉手最多挂载 256 个，前提还是挂载在一起的串口设备的串口参数须一致，接线示例图如下：



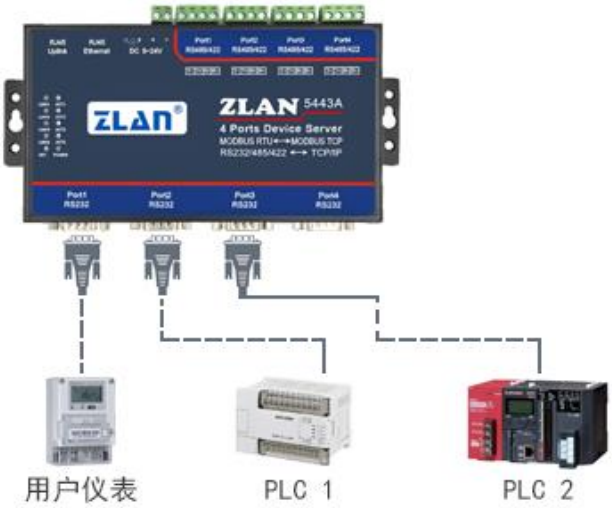
3.2 多串口设备带 modbus 协议的使用

1.网络做主站，串口做从站，同时访问一个串口从站,如下图 PLC 和用户电脑同时做主站，监控采集从站仪表的数据可以将 port1 设置



为 TCP 服务器模式，勾选多主机 port2 设置为 TCP 客户端模式，目的 IP 和目的端口填写 port1 的 IP 和端口转化协议都勾选 modbus tcp 协议。

2.多串口做主站访问一个串口从设备，如下图 PLC1 和 PLC2 同时做主站，读取从站仪表的数据可以将 port1 设置为 TCP 服务器模式，



勾选多主机 port2 和 port3 设置为 TCP 客户端模式，目的 IP 和目的端口都填写 port1 的 IP 和端口转化协议都勾选无。

4、常见问题

1.发送数据没有返回，检查 TCP 是否建立，串口参数是否一致，指令报文及其格式是否正确。

2.存在丢包，检查采集频率是否太快，建议设备 485 总线空闲等待时间为数据包间隔的 2 倍多，指令应答超时时间设置大一点，一般 300ms。