Modbus TCP 介绍

Modbus=MBAP(报文头)+PDU（帧结构）

Modbus TCP 使用 TCP 协议传输数据，传输的数据是 Modbus 格式。

客户端传输数据时是以十六进制发送，每次发送两位；服务器接收数据时也是以十六进制的形式接收，每次接收两位。 如：0X00，两位十六进制数是 8 位二进制数。

MBAP

事务标识符	协议标识	长度	单元标识符
2 字节	2 字节	2 字节	1 字节
00 00	00 00	00 00	01

- 事务标识符：可以解释为报文的序列号，例如测试使用的 Modbus Poll 客户端一直发送数据，所以每发送一次数据标识符就加一。服务器接收时会把这个数据原封返回。
- 协议表示：00 00 代表 TCP 协议。
- 长度：表示从单元标识符开始后面数据的长度。如：00 06 表示后面有 0X06 个字节长度的数据。
- 单元标识符：相当于设备的地址。一般为 01。

PDU

PDU=功能码+数据

功能码	数据
1 字节	视功能而定

功能码：

Modbus 的操作对象有四种：线圈、离散输入、输入寄存器、保持寄存器。

- 线圈：相当于开关，在 Modbus 中可读可写，数据只有 00 和 01。
- 离散量：输入位，开关量，在 Modbus 中只读。
- 输入寄存器：只能从模拟量输入端改变的寄存器，在 Modbus 中只读。
- 保持寄存器：用于输出模拟量信号的寄存器，在 Modbus 中可读可写。

根据对象的不同，Modbus 的功能码有：

- 0x01：读线圈
- 0x05：写单个线圈
- 0x0F：写多个线圈
- 0x02：读离散量输入
- 0x04：读输入寄存器
- 0x03：读保持寄存器
- 0x06：写单个保持寄存器
- 0x10：写多个保持寄存器

报文的详细解读

这里只以读保持寄存器内容为例，以下数据全部为 16 进制数据。

请求：00 01 00 00 00 06 01 03 00 02 00 04（客户端）

- 00 01：事务标识符
- 00 00：Modbus TCP 协议
- 00 06：后面有 00 06 个字节数据
- 01：单元标识符
- 03：功能码（读保持寄存器）
- 00 02：开始读的数据的地址。从 00 02 开始读数据。
- 00 04：注意这里不是读到 00 04，而是从开始位置读 00 04 个寄存器数据。

回应：00 01 00 00 00 09 01 03 08 00 00 00 37 00 00 00 00（服务器）

- 00 01：事务标识符
- 00 00：Modbus TCP 协议
- 00 09：后面有 00 09 个字节数据
- 01：单元标识符
- 03：功能码
- 08：后面有 08 个字节的数据，后面的数据每两字节表示一个寄存器数据。
- 00 00：第一个寄存器数据
- 00 37：第二个寄存器数据
- 00 00：第三个寄存器数据
- 00 00：第四个寄存器数据