

I0 模块网口 Modbus TCP/IP 通讯协议说明书



www.rockmong.com

上海岩獾科技有限公司
V1.0

目录

I0 模块网口 Modbus TCP/IP 通讯协议说明书.....	1
一. 术语和定义.....	3
1.1 线圈.....	3
1.2 离散输入.....	3
二. 通讯硬件接口.....	3
三. MODBUS 协议格式.....	3
3.1 概述.....	3
3.2 Modbus TCP 模式的通用通讯帧格式	3
3.3 功能码.....	4
3.4 读线圈（0x01）	5
3.5 写单个线圈（0x05）	5
3.6 写多个线圈（0x0F）	6

一. 术语和定义

1.1 线圈

在 Modbus 通信协议中，“线圈”通常指的是数字输出线圈（Coils）。这些线圈用于控制外部设备，如继电器或开关。每个线圈都对应一个二进制状态，可以是打开（1）或关闭（0）。在 Modbus 通信中，可以使用读取和写入操作来读取线圈的状态或改变它们的状态。

1.2 离散输入

在 Modbus 通信协议中，“离散输入”通常指的是数字输入（Discrete Inputs），也称为离散输入状态。这些离散输入用于表示外部设备的状态，例如传感器的开关状态或其他数字输入状态。每个离散输入都对应一个二进制状态，可以是打开（1）或关闭（0）。

二. 通讯硬件接口

RJ45 网口通讯	
默认 IP 地址 (可使用工具修改)	192.168.1.123
端口	502

三. MODBUS 协议格式

3.1 概述

由于 Modbus 协议完全开放、应用广泛，而且协议简单、调试手段丰富，在多机通讯的场合很容易提高开发速度，还可以很方便地与市场上已有支持 Modbus 协议的设备连接，实现数据通讯，从而成为一种事实上的工业通讯标准。Modbus 通讯协议有两种传输模式，分为 RTU 模式和 ASCII 模式。本产品接口采用 Modbus RTU 通讯模式。

3.2 Modbus TCP 模式的通用通讯帧格式

ModbusTCP 的数据帧可分为两部分：MBAP+PDU。

报文头 MBAP

MBAP 为报文头，长度为 7 字节，组成如下：

事务处理标识	协议标识	长度	单元标识符
2字节	2字节	2字节	1字节

内容	解释
事务处理标识	可以理解为报文的序列号，一般每次通信之后就要加1以区别不同的通信数据报文。
协议标识符	00 00表示ModbusTCP协议。
长度	表示接下来的数据长度，单位为字节。
单元标识符	可以理解为设备地址。

帧结构 PDU

PDU 由功能码+数据组成。功能码为 1 字节，数据长度不定，由具体功能决定。

功能码

Modbus 的操作对象有四种：线圈、离散输入、保持寄存器、输入寄存器

对象	含义
线圈	PLC的输出位，开关量，在Modbus中可读可写
离散量	PLC的输入位，开关量，在Modbus中只读
输入寄存器	PLC中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	PLC中用于输出模拟量信号的寄存器，在Modbus中可读可写

3.3 功能码

功能码主要是对离散量输入、线圈、输入寄存器、保持寄存器进行读写。本产品这里只需要用到线圈和离散输入。

名称	功能码	对应本产品实际功能
读线圈	0x01	读输出端的状态
写单个线圈	0x05	写/控制单个输出端的状态
写多个线圈	0x0F	写/控制多个输出端的状态
读离散输入	0x02	读输入端的状态

表 2 功能码

3.4 读线圈（0x01）

发送

报文头 MBAP				帧结构 PDU		
事务处理标识	协议标识	长度	单元标识符 (设备地址)	功能码	起始地址	数量
00 00	00 00	00 06	01	01	XX XX	XX XX

起始地址：D00 (或 P0) 的地址为 0，D01 (或 P1) 的地址为 1，依此类推...

数量：要读取线圈的数量。

接收

报文头 MBAP				帧结构 PDU		
事务处理标识	协议标识	长度	单元标识符 (设备地址)	功能码	字节计数	状态
00 00	00 00	00 XX	01	01	XX	XX

字节计数，读取到的线圈状态的字节数。

状态：要读取线圈的状态。每个 bit 是一个线圈，相应 bit 为 0 或 1 即是相应线圈 0 或 1。

举例：读取 D00~D07 (或 P0~P7) 共 8 路输出端状态

发送：

报文头 MBAP				帧结构 PDU		
事务处理标识	协议标识	长度	单元标识符 (设备地址)	功能码	起始地址	数量
00 00	00 00	00 06	01	01	00 00	00 08

接收：

报文头 MBAP				帧结构 PDU		
事务处理标识	协议标识	长度	单元标识符 (设备地址)	功能码	字节计数	状态
00 00	00 00	00 04	01	01	01	FF

3.5 写单个线圈（0x05）

发送：

报文头 MBAP				帧结构 PDU		
事务处理标识	协议标识	长度	单元标识符	功能码	起始地址	状态

			(设备地址)			
00 00	00 00	00 06	01	05	00 XX	XX 00

起始地址：P0(或 D00)的地址为 0，P1(或 D01)的地址为 1，依此类推...

状态：要写入线圈的状态。写 00 00 即写 0，写 FF 00 即写 1。不能写入其他数据，否则会返回错误。

接收：

同发送。不同则代表发生错误。

举例：写入 D01（或 P1）为高电平

发送：

报文头 MBAP				帧结构 PDU		
事务处理标识	协议标识	长度	单元标识符 (设备地址)	功能码	起始地址	状态
00 00	00 00	00 06	01	05	00 01	FF 00

接收：

同发送。不同则代表发生错误。

举例：写入 D01（或 P1）为低电平

发送：

报文头 MBAP				帧结构 PDU		
事务处理标识	协议标识	长度	单元标识符 (设备地址)	功能码	起始地址	状态
00 00	00 00	00 06	01	05	00 01	00 00

接收：

同发送。不同则代表发生错误。

3.6 写多个线圈（0x0F）

发送：

报文头 MBAP				帧结构 PDU				
事务处理标识	协议标识	长度	单元标识符 (设备地址)	功能码	起始地址	数量	字节计数	状态
00 00	00 00	00 XX	01	0F	00 XX	00 XX	XX	XX XX...

起始地址：D00(或 P0)的地址为 0，D01(或 P1)的地址为 1，依此类推...

数量：要控制线圈的数量。

字节计数：写入线圈状态的字节数

状态：要写入线圈的状态。每个 bit 写 0 或 1，多少个线圈写多少个 bit。如果不足一个字
节则按一个字节算。

接收：

报文头 MBAP				帧结构 PDU		
事务处 理标识	协议 标识	长度	单元标识符 (设备地址)	功能 码	起始地址	数量
00 00	00 00	00 06	01	0F	00 XX	00 XX

举例：D00~D07（或 P0~P7）共 8 路输出端同时输出高电平

发送：

报文头 MBAP				帧结构 PDU				
事务处 理标识	协议 标识	长度	单元标识符 (设备地址)	功能码	起始地址	数量	字节 计数	状态
00 00	00 00	00 08	01	0F	00 00	00 08	01	FF

接收：

报文头 MBAP				帧结构 PDU		
事务处 理标识	协议 标识	长度	单元标识符 (设备地址)	功能码	起始地址	数量
00 00	00 00	00 06	01	0F	00 00	00 08

举例：D00~D07（或 P0~P7）共 8 路输出端同时输出低电平

发送：

报文头 MBAP				帧结构 PDU				
事务处 理标识	协议 标识	长度	单元标识符 (设备地址)	功能码	起始地址	数量	字节 计数	状态
00 00	00 00	00 08	01	0F	00 00	00 08	01	00

接收：

报文头 MBAP				帧结构 PDU		
事务处 理标识	协议 标识	长度	单元标识符 (设备地址)	功能码	起始地址	数量
00 00	00 00	00 06	01	0F	00 00	00 08

3.7 读离散输入（0x02）

发送

报文头 MBAP				帧结构 PDU		
事务处 理标识	协议 标识	长度	单元标识符 (设备地址)	功能码	起始地址	数量
00 00	00 00	00 06	01	02	00 XX	00 XX

起始地址：DI0(或 P0)的地址为 0，DI1(或 P1)的地址为 1，依此类推...

数量：要读取离散输入的数量。

接收

报文头 MBAP				帧结构 PDU		
事务处理标识	协议标识	长度	单元标识符(设备地址)	功能码	字节计数	状态
00 00	00 00	00 06	01	02	XX	XX ...

字节计数，读取到的离散输入状态的字节数。

状态：要读取离散输入的状态。每个 bit 是一个离散输入，相应 bit 为 0 或 1 即是相应离散输入 0 或 1。

举例：读取 DI0~DI7(或 P0~P7) 共 8 路输入端状态

发送：

报文头 MBAP				帧结构 PDU		
事务处理标识	协议标识	长度	单元标识符(设备地址)	功能码	起始地址	数量
00 00	00 00	00 06	01	02	00 00	00 08

接收：

报文头 MBAP				帧结构 PDU		
事务处理标识	协议标识	长度	单元标识符(设备地址)	功能码	字节计数	状态
00 00	00 00	00 04	01	02	01	FF