

物联网网关 通讯协议



北京昆仑海岸传感技术有限公司

目录

1、网关支持的 Modbus TCP 协议的功能码.....	1
1.1 Modbus TCP 报文格式.....	1
1.2 0x03 功能码：读取保持寄存器.....	1
1.3 0x01 功能码：读取设备在线状态.....	2
2、网关地址规范.....	3
2.1 网关内部参数地址规范.....	3
2.2 功能码：读线圈 0x01.....	4
2.3 功能码：读保持寄存器 0x03.....	5
2.4 读取通道值解析.....	7
2.5 通道值解析实例.....	11
3、接口编程指南.....	12
3.1 网关做服务器.....	12
3.2 网关做客户端.....	13
3.3 编程实例.....	14

1、网关支持的 Modbus TCP 协议的功能码

1.1 Modbus TCP 报文格式

Modbus TCP 报文包格式								
MBAP 报文头						功能码	数据	
事务元标识符		协议标识符		长度		单元标识符		
2 字节		2 字节		2 字节		1 字节	1 字节	
15	01	00	00					

1.2 0x03 功能码：读取保持寄存器

请求包格式：

Modbus TCP 0x03 功能码请求包													
MBAP 报文头								功能码		起始地址		寄存器数量	
事务元标识符		协议标识符		长度		单元标识符							
2 字节		2 字节		2 字节		1 字节		1 字节		2 字节		2 字节	
15	01	00	00			设备地址		0x03					

响应包格式：

Modbus TCP 0x03 功能码响应包										
MBAP 报文头						功能码	字节数	寄存器值		
事务元标识符	协议标识符	长度		单元标识符						
2 字节	2 字节	2 字节		1 字节	1 字节	1 字节	字节数	字节数		
15	01	00	00		设备地址	0x03				

错误包格式：

Modbus TCP 0x03 功能码响应包										
MBAP 报文头						差错码	异常码			
事务元标识符	协议标识符	长度		单元标识符						
2 字节	2 字节	2 字节		1 字节	1 字节	1 字节	1 字节			
15	01	00	00	00	03	设备地址	0x83	0x01/0x02/0x03/0x0C/0x0D/0x0E		

注：异常码的含义：

- 1) 0x01 功能码错误
- 2) 0x02 起始地址错误

- 3) 0x03 寄存器数量错误
- 4) 0x0C 协议标识符错误
- 5) 0x0D 请求包长度错误
- 6) 0x0E 设备地址错误

1.3 0x01 功能码：读取设备在线状态

请求包格式：

Modbus TCP 0x01 功能码请求包									
MBAP 报文头						功能码	起始地址	传感器节点数量	
事务元标识符		协议标识符		长度		单元标识符			
2 字节		2 字节		2 字节		1 字节	1 字节	2 字节	2 字节
15	01	00	00			设备地址	0x01		

响应包格式：

Modbus TCP 0x01 功能码响应包									
MBAP 报文头						功能码	字节数	传感器节点状态	
事务元标识符		协议标识符		长度		单元标识符			
2 字节		2 字节		2 字节		1 字节	1 字节	1 字节	字节数个字节
15	01	00	00			设备地址	0x01		

错误包格式：

Modbus TCP 0x01 功能码响应包									
MBAP 报文头						差错码	异常码		
事务元标识符		协议标识符		长度		单元标识符			
2 字节		2 字节		2 字节		1 字节	1 字节	1 字节	
15	01	00	00	00	03	设备地址	0x81	0x01/0x02/0x03/0x0C/0x0D/0x0E	

注：异常码的含义：

- 1) 0x01 功能码错误
- 2) 0x02 起始地址错误
- 3) 0x03 寄存器数量错误
- 4) 0x0C 协议标识符错误
- 5) 0x0D 请求包长度错误
- 6) 0x0E 设备地址错误

2、网关地址规范

2.1 网关内部参数地址规范

网关的设备地址为 0xFF(255)

0x03 功能码			
网关参数	起始地址(2bytes)	寄存器个数 (2bytes)	存储格式
网关 IP 地址 (r)	0x0000	0x0008	字符格式: “192.168.0.222”
子网掩码 (r)	0x0008	0x0008	字符格式: “255.255.255.0”
网关 IP(r)	0x0010	0x0008	字符格式: “192.168.0.1”
网关 DNS(r)	0x0018	0x0008	字符格式: “192.168.0.1”
MAC 地址 (r)	0x0020	0x0009	字符格式: “AA:CD:EF:12:34:03”
网关序列号 (r)	0x0029	0x0008	字符格式: “1111222233334444”
0x01 功能码			
网关参数	起始地址(2bytes)	线圈个数 (2bytes)	存储格式
节点状态 (r)	0x5555	0x00F7	1=在线, 0=不在线

示例

读取网关 IP 地址, 网关地址为 192.168.0.111

查询命令

15 01 00 00 00 06 FF 03 00 00 00 08

第 字节	1-2	3-4	5-6	7	8	9-10	11-12
内容	15 01	00 00	00 06	FF	03	00 00	00 08
名称	事物元 标识符	协议标 识符	长度	单元标识 符 (设备 地址)	功能码	读线圈 起始地址	读取8个保 持寄存器

返回数据

15 01 00 00 00 13 FF 03 10 31 39 32 2E 31 36 38 2E 30 2E 31 31 31 0D 00 00

第 字节	1-2	3-4	5-6	7	8	9	10
内容	15 01	00 00	00 13	FF	03	10	31
名称	事物元 标识符	协议标 识符	从第七字 节之后所 有数据的 字节数	单元标 识符 (设 备地址)	功能码	读取所 有通道 的字节 数	ASSIC码表 示为 “1”

第 字 节	11	12	13	14	15	16	17
内容	39	32	2E	31	36	38	2E
名称	ASSIC码 表示为 “9”	ASSIC码 表示为 “2”	ASSIC码 表示为 “.”	ASSIC码 表示为 “1”	ASSIC码 表示为 “6”	ASSIC码 表示为 “8”	ASSIC码 表示为 “.”

第 字节	19	20	21	22	23	24	25	26
内容	30	2E	31	31	31	0D	00	00
名称	ASSIC码 表示为 “0”	ASSIC码 表示为 “.”	ASSIC码 表示为 “1”	ASSIC码 表示为 “1”	ASSIC码 表示为 “1”	ASSIC码 表示回车 符	多 余 位 数 补 零	多 余 位 数 补 零

由示例可看出,IP 地址 192.168.0.111,在返回数据中表示为十六进制 ASSIC 码,当读取全部 IP 地址后,以一个回车符结束,如果后面还有空位,则补零。如果 IP 地址为 192.168.200.111,在返回数据中占 15 位,加回车符,占满 16 位,则后面不用补零。

2.2 功能码：读线圈 0x01

网关地址为 0xFF,读线圈功能码: 0x01,可以读取网关下挂 247 个节点在线状态。

查询命令

15 01 00 00 00 06 FF 01 55 55 00 F7

第 字节	1-2	3-4	5-6	7	8	9-10	11-12
内容	15 01	00 00	00 06	FF	01	55 55	00 F7
名称	事物元 标识符	协议标 识符	长度	单元标识 符（设备 地址）	功能码	读线圈起 始地址	线圈数量, 247个线 圈, 247个 节点在线 状态

返回数据

15 01 00 00 00 22 FF 01 1F FF 7F FF FF FF FF FF FF FF FF FF FF FF FF
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

第 字节	1-2	3-4	5-6	7	8	9	10
内容	15 01	00 00	00 22	FF	01	1F	FF
名称	事物元标识符	协议标识符	从第七字节之后所有数据的字节数	单元标识符（设备地址）	功能码	读取所有通道的字节数	第1-8个节点在线状态，按照从低位到高位顺序排列

第 字节	11	12	13		38	39	40
内容	7F	FF	FF		00	00	00
名称	第9-16个节点在线状态，按照从低位到高位顺序排列	第17-24个节点在线状态，按照从低位到高位顺序排列	第25-32个节点在线状态，按照从低位到高位顺序排列		第225-232个节点在线状态，按照从低位到高位顺序排列	第233-240个节点在线状态，按照从低位到高位顺序排列	第241-247个节点在线状态，按照从低位到高位顺序排列

注：节点在线状态是按位表示的，1 代表在线，0 代表不在线。

Modbus TCP 错误响应包：15 01 00 00 00 03 FF 81 01（02/03/0C/0D/0E）

注：0x01 功能码，详细可参照标准 Modbus TCP 通讯协议。

2.3 功能码：读保持寄存器 0x03

网关最大可与 247 个节点进行组网（通过用户配置的节点的设备地址进行区分），每个节点支持 32 个通道，每个通道占 2 个寄存器（4 个字节）。

节点设备地址	通道	起始地址	寄存器个数
用户配置的节点的设备地址（0x01~0xF7）	第 1 个通道	0x0000	0x02
	第 2 个通道	0x0002	0x02
	第 3 个通道	0x0004	0x02
			
	第 32 个通道	0x003e	0x02

示例：

(1) 读取设备地址为 0x40 的节点的所有 32 个通道的值

设备地址=0x40, 起始地址=0x0000, 寄存器个数=0x40(每个节点有 32 个通道, 每个通道 4 个字节, 所以每个节点的通道值共 128 个字节, 64 个寄存器)

查询命令

15 01 00 00 00 06 40 03 00 00 00 40

第 字节	1-2	3-4	5-6	7	8	9-10	11-12
内容	15 01	00 00	00 06	40	03	00 00	00 40
名称	事物元标识符	协议标识符	长度	单元标识符（设备地址）	功能码	保持寄存器起始地址	保持寄存器数量

返回数据

[illegible]

第 字节	1-2	3-4	5-6	7	8	9	10-13
内容	15 01	00 00	00 83	40	03	80	01 81 00 BA
名称	事物元标识符	协议标识符	从第七字节之后所有数据的字节数	单元标识符（设备地址）	功能码	读取所有通道的字节数	第1通道的标识符和通道数值，前两字节为标识符，后两字节为通道值

第 字 节	14-17	18-21	22-25	26-29	……	134-137
内容	02 01 00 F3	F2 01 00 22	00 00 00 00	00 00 00 00	……	00 00 00 00
名称	第2通道的标识符和通道数值，前两字节为标识符，后两字节为通道值	第3通道的标识符和通道数值，前两字节为标识符，后两字节为通道值	第4通道的标识符和通道数值，前两字节为标识符，后两字节为通道值	第5通道的标识符和通道数值	……	第32通道的标识符和通道数值

Modbus TCP 错误响应包：15 01 00 00 00 03 40 83 01 (02/03/0C/0D/0E)

(2) 读取第 7 个节点的第 3 个通道值

设备地址=0x07，起始地址=0x0004，寄存器个数=2

查询命令

15 01 00 00 00 06 07 03 0004 0002

第 字节	1-2	3-4	5-6	7	8	9-10	11-12
内容	15 01	00 00	00 06	07	03	00 04	00 02
名称	事物元标识符	协议标识符	长度	单元标识符（设备地址）	功能码	保持寄存器起始地址	保持寄存器数量

返回数据

15 01 00 00 00 07 07 03 04 F2 01 00 22

第 字节	1-2	3-4	5-6	7	8	9	10-13
内容	15 01	00 00	00 07	07	03	04	F2 01 00 22
名称	事物元标识符	协议标识符	从第七字节之后所有数据的字节数	单元标识符（设备地址）	功能码	读取所有通道的字节数	第3通道的标识符和通道数值，前两字节为标识符，后两字节为通道值

Modbus TCP 错误响应包：15 01 00 00 00 03 07 83 01 (02/03/0C/0D/0E)

2.4 读取通道值解析

从网关读取的通道值如 F2 01 00 22、01 81 00 BA 的解析遵循昆仑海岸物联网无线通讯协议。

数据组名称及格式 (2 个字节)		数据组数值 (2 个字节)	
名称	格式	高位	低位
1-255 0-无效	XX	XX	XX

数据名称及格式：数据名称，1 个字节，每个数值的名称代码，详细名称见表一。

数据格式：1 个字节，根据该格式，可以将无符号整型数转化为具体的实际值。定义数值的正负特性，数值量或开关量，是否为长整型数的一部分，此数据转换为小数的小数位，格式如下：

位地址	Bit7	Bit 6	Bit 5	Bit 4
含义	0: 无符号数 1: 有符号数	数值类型 0 数值 1 开关量	长整型数值标识 0 双字节 1 四字节	四字节数字标识 0 低 2 字节 1 高 2 字节

位地址	Bit3	Bit2	Bit1	Bit0
含义	保留	小数点位置: 0-7 0 无小数 1 一位小数 2 两位小数		

举例

帧	01 81 FF68	02 01 0118	03 00 0258	04 81 00BD	05 03 01FA	F2 02 014A
含义	01: 温度; 81: 有符号, 1 位小数; FF68 转化十进制数-152; 温度: -15.2℃ (4 字节)	02: 湿度; 01: 无符号, 1 位小数; 0118 转化十进制数 280; 湿度: 28.0%RH (4 字节)	03: 照度; 00: 无符号, 无小数 0258 转化十进制数 600 照度: 600lux (4 字节)	04: 土壤温度 81: 有符号, 1 位小数; 00BD 转化十进制数 189; 温度: 18.9℃ (4 字节)	05: 土壤水分 03: 无符号, 3 位小数 01FA 转化十进制数 506 土壤水分: 0.506V 注: 查土壤水分含量表可知 (4 字节)	F2: 电量; 02: 无符号, 2 位小数 014A 转化十进制数 330 电量: 3.30V (4 字节)

帧	01 81 00FA	02 01 0115	F2 02 014A
含义	01 温度; 81 有符号, 1 位小数; 00FA 转化十进制数 250; 温度: 25.0℃ (4 字节)	02 湿度; 01 无符号, 1 位小数; 0115 转化十进制数 277; 湿度: 27.7%RH (4 字节)	F2: 电量; 02: 无符号 2 位小数 014A 转化十进制数 330 电量: 3.30V (4 字节)

帧	A140FFFF	A2400000	A340FFFF	A4400000
含义	A1: 开关量 1 40: 开关量 FFFF 启动 0000 停止	A2: 开关量 2 40: 开关量 FFFF 启动 0000 停止	A3: 开关量 3 40: 开关量 FFFF 启动 0000 停止	A4: 开关量 4 40: 开关量 FFFF 启动 0000 停止

表一

数据代码	数据名称	
01	温度	
02	湿度	
03	照度	
04	土壤温度	
05	土壤水分	
06	大气压力	
07	压力/液位	
08	流量	
09	超声波	
0A	雷达	
0B	单界面	
0C	双界面	
0D	浸水	
0E	感烟器	
0F	明火探测器	
10	红外探测器	
11	射频物位开关	
12	浮球开关	
13	音叉物位开关	
14	CO2	
15	粉尘	
16	空气质量等级	
17	CO	
18	H2	
19	H2S	
1A	O2	
1B	SO2	
1C	CL2	
1D	NH3	
1E	CH3OH	
1F	CH3CH2OH	
20	CH4	
21	露点	
...	...	
30	风速	
31	风向	
32	雨量	
...	...	
80	压力液位 Pa	
81	压力液位 kPa	
82	压力液位 MPa	

数据代码	数据名称	
83	压力液位 Bar	
84	压力液位 m	
85	压力液位（预留）	
...	...	
A1	开关量 1（输出）	
A2	开关量 2（输出）	
A3	开关量 3（输出）	
A4	开关量 4（输出）	
A5	开关量 5（输出）	
A6	开关量 6（输出）	
A7	开关量 7（输出）	
A8	开关量 8（输出）	
...	...	
B1	开关量 1（输入）	
B2	开关量 2（输入）	
B3	开关量 3（输入）	
B4	开关量 4（输入）	
...	...	
C0	模拟量 1（mA）	
C1	模拟量 2（mA）	
C2	模拟量 3（mA）	
C3	模拟量 4（mA）	
...	...	
C8	模拟量 1（V）	
C9	模拟量 2（V）	
CA	模拟量 3（V）	
CB	模拟量 4（V）	
...	...	
...	...	
E0	数据传输	
F0	设备名称	
F1	设备版本	前两位硬件版本 后两位软件版本
F2	设备电量	
FF	路由心跳	注：路由心跳数据为 0

2.5 通道值解析实例

示例：

读取设备地址为 0x07 的温湿度传感器的前三个通道的值。

设备地址=0x07，起始地址=0x0000，寄存器个数=6

查询命令

15 01 00 00 00 06 07 03 00 00 00 06

第 字节	1-2	3-4	5-6	7	8	9-10	11-12
内容	15 01	00 00	00 06	07	03	00 00	00 06
名称	事物元标识符	协议标识符	长度	单元标识符（设备地址）	功能码	保持寄存器起始地址	保持寄存器数量

返回数据

15 01 00 00 00 0F 07 03 0C 01 81 FF 68 02 01 00 FD F2 01 00 1E

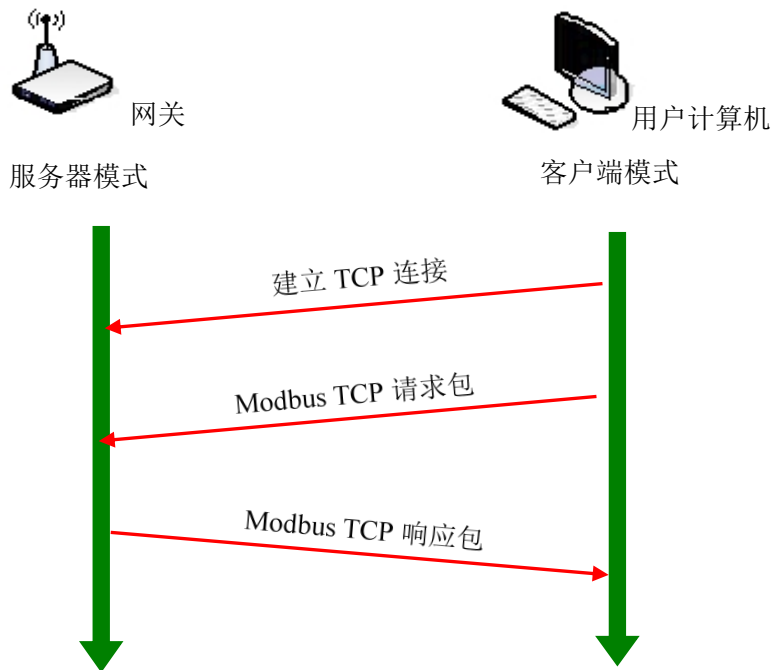
第 字节	1-2	3-4	5-6	7	8	9
内容	15 01	00 00	00 0F	07	03	0C
名称	事物元标识符	协议标识符	从第七字节之后所有数据的字节数	单元标识符（设备地址）	功能码	读取所有通道的字节数

10-13	14-17	18-21
01 81 FF 68	02 01 00 FD	F2 01 00 1E
第一通道：01代表温度；81代表有符号，一位小数；FF68为温度值，转化成十进制是-152； 温度：-15.2℃（4字节）	第二通道：02代表湿度；01代表无符号，一位小数；00FD为湿度值，转化成十进制是253； 湿度：25.3%RH（4字节）	第三通道：F2代表电量；01代表无符号，一位小数；001E为电量值，转化成十进制是30； 电量：3.0V（4字节）

Modbus TCP 错误响应包：15 01 00 00 00 03 07 83 01（02/03/0C/0D/0E）

3、接口编程指南

3.1 网关做服务器

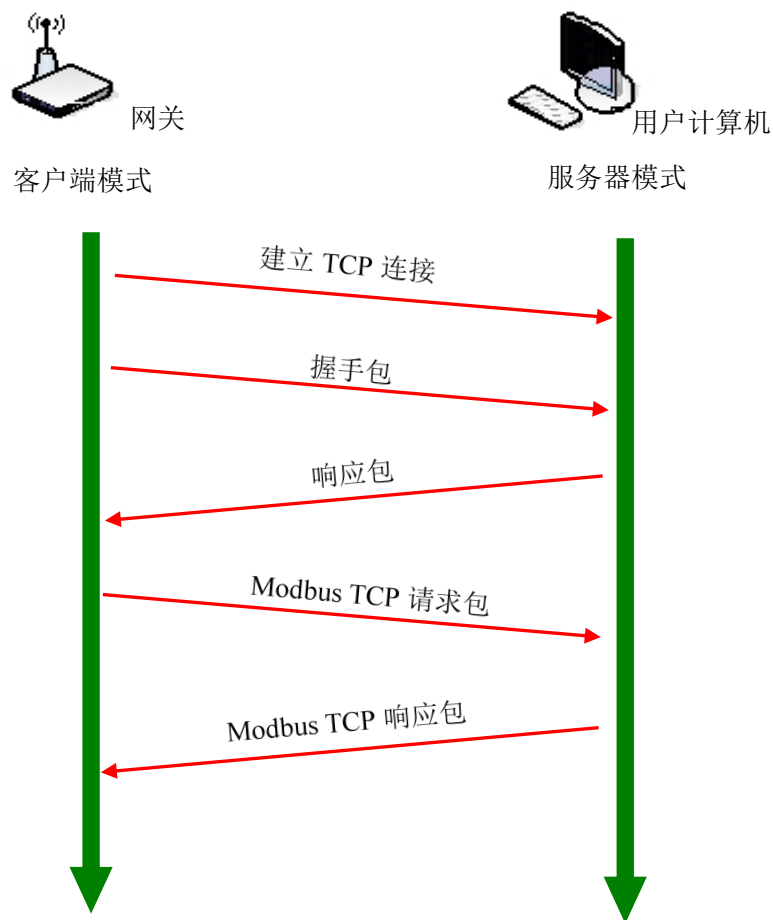


注：按照功能分，Modbus Tcp 的请求包分 2 种：

- (1) 读取网关采集节点的通道值
- (2) 读取网关采集节点的状态值

网关工作于服务器模式，客户计算机作为客户端，主动向网关建立 TCP 连接，建立成功之后，发送 Modbus Tcp 请求包，请求相关数据，网关返回相应的响应包。需要注意的是，如果客户和网关服务器建立连接后 30 分钟没有数据请求，则网关自动断开此连接

3.2 网关做客户端



握手包: 15 01 22 22 00 10 +网关序列号“2222333344445555”

响应包: 15 01 22 22 00 01 80

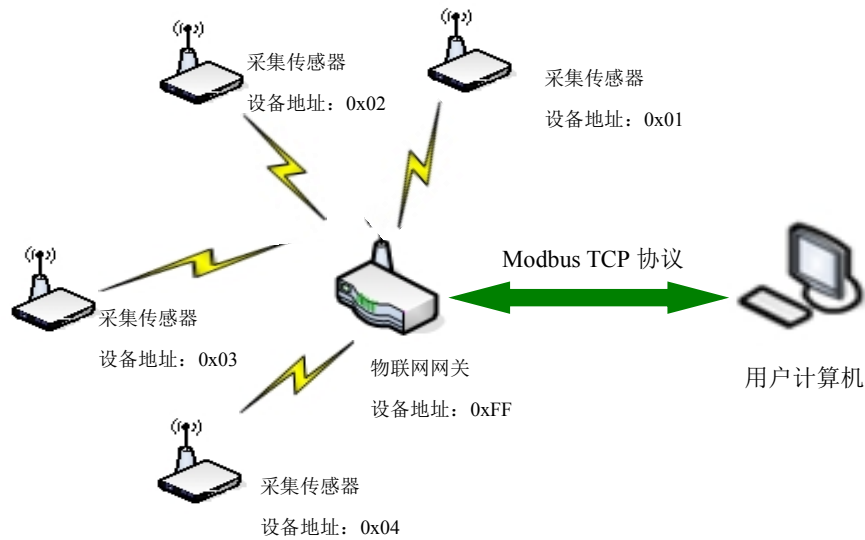
错误包: 15 01 22 22 00 01 01

注: 按照功能分, Modbus TCP 的请求包分 2 种:

- (1) 读取网关采集节点的通道值
- (2) 读取网关采集节点的状态值

网关工作于客户端模式, 主动向客户端服务器发起 TCP 连接, 建立 TCP 连接成功后, 网关发送握手包, 服务器收到握手包之后返回响应包, 之后握手过程结束, 然后服务器向网关发送 Modbus TCP 请求包, 网关给予相关响应。其中, 握手过程中如果服务器没有返回握手响应包或者返回错误包, 客户端断掉本连接, 重新建立新的连接。通讯过程中, 出现任何异常, 客户端不会退出, 始终在尝试进行与服务器的重连, 如服务器因为异常退出后, 网关客户端启动重连机制, 一直在尝试重连, 直到服务器恢复正常。

3.3 编程实例



RFID 网络组织结构

示例：

1、读取网关下挂传感器节点的在线状态

Modbus Tcp 请求包: 15 01 00 00 00 06 FF 01 55 55 00 F7

[illegible]

Modbus Tcp 错误响应包: 15 01 00 00 00 06 FF 80 01 (02/03/0C/0D/0E)

2、读取设备地址为 0xf4 的传感器节点的通道信息

Modbus Tcp 请求包: 15 01 00 00 00 06 F4 03 00 00 00 40

[illegible]

Modbus Tcp 错误响应包: 15 01 00 00 00 03 F4 83 01 (02/03/0C/0D/0E)