物联网网关
通讯协议
V1.6

北京昆仑海岸传感技术有限公司

目 录

1、网关支持 Modbus TCP 查询应答式的通讯协议

1.1 网关支持的 Modbus TCP 协议的功能码

1.1.1 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					

1.1.2 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	0x01/0x02/0x03/0x04/0x0C/0x0D/0x0E/0x0F

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）0x04 从站设备故障（如设备不在线）
5）0x0C 协议标识符错误
6）0x0D 请求包长度错误
7）0x0E 设备地址错误
8）0x0F 请求包的寄存器内容错误

1.1.3 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	字节数个字节
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
15	01	00	00	00	03	设备地址	0x83	0x01/0x02/0x03/0x04/ 0x0C/0x0D/0x0E/0x0F

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）0x04 从站设备故障（如设备不在线）
5）0x0C 协议标识符错误
6）0x0D 请求包长度错误
7）0x0E 设备地址错误
8）0x0F 请求包的寄存器内容错误

1.1.4 0x10 功能码：写保持寄存器

请求包格式：

ModbusTcp 0x10 功能码请求包											
MBAP 报文头						功能码	起始地址	寄存器数量	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	2 字节	2 字节	1 个字节	字节数个字节
15	01	00	00			设备地址	0x10				

响应包格式：

ModbusTcp 0x10 功能码响应包									
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	0x10		

错误包格式：

ModbusTcp 0x10 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		设备地址	0x90	0x01/0x02/0x03/0x04/ 0x0C/0x0D/0x0E/0x0F	

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）0x04 从站设备故障（如设备不在线）
5）0x0C 协议标识符错误
6）0x0D 请求包长度错误
7）0x0E 设备地址错误
8）0x0F 请求包的寄存器内容错误

1.2 网关地址规范

1.2.1 网关内部参数地址规范（只读）

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	0x0040	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，网关设备地址=0xFF，功能码=0x03，起始地址=0x0000，寄存器数量=0x0008。

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。

1.2.2 功能码：读线圈 0x01

网关地址为 0xFF，读线圈功能码：0x01，可读取网关下挂 64 个节点在线状态。

查询命令

15 01 00 00 00 06 FF 01 55 55 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	FF	01	55 55	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	读线圈起始地址	线圈数量，64个线圈，64个节点在线状态

返回数据

15 01 00 00 00 0B FF 01 08 FF 7F FF FF FF FF FF FF

第 字节	1-2	3-4	5-6	7	8	9	10
内容	15 01	00 00	00 0B	FF	01	08	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	14	15	16	17
内容	7F	FF	FF	FF	FF	FF	FF
名称	第9-16个节点在线状态，按照从低位到高位的顺序排列	第17-24个节点在线状态，按照从低位到高位的顺序排列	第25-32个节点在线状态，按照从低位到高位的顺序排列	第33-40个节点在线状态，按照从低位到高位的顺序排列	第41-48个节点在线状态，按照从低位到高位的顺序排列	第49-56个节点在线状态，按照从低位到高位的顺序排列	第57-64个节点在线状态，按照从低位到高位的顺序排列

注：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（02/03/04/0C/0D/0E/0F）
注：0x01 功能码，详细可参照标准 Modbus TCP 通讯协议。

1.2.3 功能码：读保持寄存器 0x03

网关最大可与 64 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（0x01~0x40）	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
15 01 00 00 00 83 40 03 80 A1 40 00 00 A2 40 00 00 A3 40 00 00 A4 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 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	10-13
内容	15 01	00 00	00 83	40	03	80	A1 40 00 00
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	32-35	…	38-41
内容	A2 40 00 00	A3 40 00 00	A4 40 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6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（02/03/04/0C/0D/0E/0F）

（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 A3 40 FF FF

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	A1 40 FF 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（02/03/04/0C/0D/0E/0F）

1.2.4 功能码：写保持寄存器 0x10

本指令控制开关量的输出只针对昆仑海岸传感技术有限公司的 JZH-2 控制系列产品使用。

JZH-2 控制系列产品的每路控制量占一个通道，4 路开关量控制即占 4 个通道，通道值为 0xFFFF 表示开，0x0000 表示关。

节点设备地址	通道	起始地址	寄 存 器 个数	寄存器值
用户配置的节点的设备地址（0x01~0x40）	第 1 路	0x0000	0x02	开：A140 FFFF 关：A140 0000
	第 2 路	0x0002	0x02	开：A240 FFFF 关：A240 0000
	第 3 路	0x0004	0x02	开：A340 FFFF 关：A340 0000
	……	……	…..	……
	第 N 路	0x003E	0x02	开：AN40 FFFF 关：AN40 0000

示例：

（1）对设备地址为 0x02 的 4 路开关量控制节点下发控制指令，打开第一路开关

设备地址=0x02，起始地址=0x0000，寄存器个数=2

控制指令15 01 00 00 00 0B 02 10 00 00 00 02 04 A1 40 FF FF

第 字节	1-2	3-4	5-6	7	8	9-10	11-12
内容	15 01	00 00	00 0B	02	10	00 00	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

第 字节	13	14-17
内容	04	A1 40 FF FF
名称	字节数	写入数据

正确返回：15 01 00 00 00 04 02 10 00 02

第 字节	1-2	3-4	5-6	7	8	9-10
内容	15 01	00 00	00 04	02	10	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	寄存器个数

Modbus TCP 错误响应包：15 01 00 00 00 03 02 90 01（02/03/04/0C/0D/0E/0F）

（2）对设备地址为 0x02 的 4 路开关量控制节点下发控制指令，关闭第二路开关

设备地址=0x02，起始地址=0x0002，寄存器个数=2

控制指令 15 01 00 00 00 0B 02 10 00 02 00 02 04 A2 40 00 00

第 字节	1-2	3-4	5-6	7	8	9-10	11-12
内容	15 01	00 00	00 0B	02	10	00 02	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

第 字节	13	14-17
内容	04	A2 40 00 00
名称	字节数	写入数据

正确返回: 15 01 00 00 00 04 02 10 00 02

第 字节	1-2	3-4	5-6	7	8	9-10
内容	15 01	00 00	00 04	02	10	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	寄存器个数

Modbus TCP 错误响应包：15 01 00 00 00 03 02 90 01（02/03/04/0C/0D/0E/0F）

1.2.5 读取通道值解析

以下数据解析的内容的详细资料参见昆仑海岸物联网无线通讯协议
http://www.klha.cn/upload/file/1468480490.pdf

网关读取了通道值，如 A1 40 FF FF、01 81 01 18，通道值的解析遵循昆仑海岸物联网无线通讯协议。

数据组 0 名称及格式 (2 个字节)		数据组 0 数值 (2 个字节)		…	数据组 M 名称及格式 (2 个字节)	
名称	格式	高位	低位		名称	格式
1-255 0-无效	XX	XX	XX	…	1-255 0-无效	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数，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	四字节数字节标识 0 低 2 字节 1 高 2 字节

位地址	3	2	1	0
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℃ (8 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℃(8 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	数据代码	数据名称
01	温度	2A	温度 6
02	湿度	…	…
03	照度	30	风速
04	土壤温度	31	风向
05	土壤水分	32	雨量
06	大气压力	…	…
07	压力/液位	80	压力液位 Pa
08	流量	81	压力液位 kPa
09	超声波	82	压力液位 MPa
0A	雷达	83	压力液位 Bar
0B	单界面	84	压力液位 m
0C	双界面	85	压力液位（预留）
0D	浸水	…	…
0E	感烟器	A1	开关量 1（输出）
0F	明火探测器	A2	开关量 2（输出）
10	红外探测器	A3	开关量 3（输出）
11	射频物位开关	A4	开关量 4（输出）
12	浮球开关	A5	开关量 5（输出）
13	音叉物位开关	A6	开关量 6（输出）
14	CO2	A7	开关量 7（输出）
15	粉尘	A8	开关量 8（输出）
16	空气质量等级	…	…
17	CO	B1	开关量 1（输入）
18	H2	B2	开关量 2（输入）
19	H2S	B3	开关量 3（输入）

1A	O2	B4	开关量 4（输入）
1B	SO2	B5	开关量 5（输入）
1C	CL2	B6	开关量 6（输入）
1D	NH3	B7	开关量 7（输入）
1E	CH3OH	B8	开关量 8（输入）
1F	CH3CH2OH	…	…
20	CH4	C0	模拟量 1（mA）
21	露点	C1	模拟量 2（mA）
22	水浸报警状态	C2	模拟量 3（mA）
23	水浸报警数据	C3	模拟量 4（mA）
24	EC 值（dS/m）	C4	模拟量 5（mA）
25	温度 1	C5	模拟量 6（mA）
26	温度 2	C6	模拟量 7（mA）
27	温度 3	C7	模拟量 8（mA）
28	温度 4	C8	模拟量 1（V）
29	温度 5	C9	模拟量 2（V）
CA	模拟量 3（V）		
CB	模拟量 4（V）		
CC	模拟量 5（V）		
CD	模拟量 6（V）		
CE	模拟量 7（V）		
CF	模拟量 8（V）		
…	…		
E0	数据传输		
E1	传感器 1 ID 号		
E2	传感器 2 ID 号		
E3	传感器 3 ID 号		
F0	设备名称		
F1	设备版本		
F2	设备电量		
F3	时间（年、月）		
F4	时间（日、时）		
F5	时间（分、秒）		
F6	主动上报时间		
FD	传感器工作作态		
FE	网关工作状态		
FF	路由心跳		

1.3 通道值解析实例

实例背景：

KL-H1100 物联网网关下挂载着三只传感器，分别为节点型温度传感器 JZH-001-D（设备地址=01）；路由型温湿照度传感器 JZH-010-12（设备地址=02）；JZH-201 无线控制模块（设备地址=03）。

1.3.1 读取传感器的在线状态

查询命令：15 01 00 00 00 06 FF 01 55 55 00 08

指令解析：

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 08
名称	事物元标识符	协议标识符	长度	网关设备地址	功能码	读传感器状态起始地址	读取传感器

返回指令： 15 01 00 00 00 0B FF 01 01 07

第 字节	1-2	3-4	5-6	7	8	9	10
内容	15 01	00 00	00 03	FF	01	01	07
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	网关设备地址	功能码	读取所有通道的字节数	第1-8个节点在线状态，按照从低位到高位的顺序排列，0x07转换成二进制为00000111，可知节点1、2、3全部在线

1.3.2 读取传感器值

1.读取节点型温湿度传感器的值。

由背景可知，节点型温湿度传感器设备地址为 0x01，可读取三个物理量：温度、湿度、设备电量。功能码=0x03，起始地址=0x0000，寄存器数量=0x06。

查询命令：15 01 00 00 00 06 01 03 00 00 00 06

指令解析：

第 字节	1-2	3-4	5-6	7	8	9-10	11-12
内容	15 01	00 00	00 06	01	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

返回指令： 15 01 00 00 00 0F 01 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	01	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

第 字节	10-13	14-17	18-21
内容	01 81 FF 68	02 01 00 FD	F2 01 00 1E
名称	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−152；温度：−15.2℃（4 字节）	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）	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）

说明：由上表可得，JZH-001-D 传感器的的当前温度是-15.2℃，湿度是 25.3%RH，设备电量是 3.0V。

2.读取路由型温度湿度照度传感器的值

由背景可知，路由型传感器的设备地址为 0x02，含有温度湿度和照度三个物理量。功能码=0x03，寄存器起始地址=0x0000，寄存器数量=0x0006。

查询命令：15 01 00 00 00 06 02 03 00 00 00 06
指令解析：

第 字节	1-2	3-4	5-6	7	8	9-10	11-12
内容	15 01	00 00	00 06	01	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 1：15 01 00 00 00 0F 01 03 0C 01 81 01 02 02 01 00 F9 03 00 00 80

第 字节	1-2	3-4	5-6	7	8	9
内容	15 01	00 00	00 0F	01	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

第 字节	10-13	14-17	18-21
内容	01 81 01 02	02 01 00 F9	03 00 00 80
名称	01 代表温度；81 代表有符号，一位小数；0x0102 为温度值，转化成十进制是 258； 温度：25.8℃（4 字节）	02 代表湿度；01 代表无符号，一位小数；0x00F9 为湿度值，转化成十进制是 249； 湿度：24.9%RH（4 字节）	03 代表照度；00 代表无符号，一位小数；0x0080 为照度值，转化成十进制是 128； 照度：128Lx（4 字节）

说明：由上表可得，JZH-010-12 传感器的当前温度值为 25.8℃，湿度值为 24.9%RH，照度值为 128Lx。

※在有的环境下，照度值有时会超过 0xFFFF，即 65535Lx，此时 2 个寄存器已不能满足数值要求，例如 123456Lx，这时就需要用 4 个寄存器保存。

返回数据 2：15 01 00 00 00 10 01 81 01 02 02 01 00 F9 03 20 E2 40 03 30 00 01

照度值解析		
数据	**03 20 E2 40**	**03 30 00 01**
解析	03 代表照度；20 代表四字节，低 2 字节；0xE240 是照度值的低 4 位	03 代表照度；30 代表四字节，高 2 字节；0x0001 是照度值的高 4 位
	照度值：0x0001E240 转换成十进制为 123456Lx	

说明：根据 1.2.5 读取通道值解析可知，按位解析数据组 03 20 E2 40，其中代表数据格式的“20”转换成二进制是 00100000，第 5 位为“1”，代表此数据是四字节，第 4 位为“0”，代表此数据组中 E240 是照度值的低 2 字节；按位解析数据组 03 30 00 01，其中“30”转换成二进制是 00110000，第 5 为的“1”代表此数据是四字节，第 4 位的“1”表示此数据族中 0001 是照度值的高 2 字节，所以两个数据组的数据值组合起来就是 0x0001E240，转换成十进制就是当前的照度值 123456Lx。

1.3.3 控制开关量输出

控制 JZH-201 无线控制模块的开关量输出，打开第一路和第二路通道，关闭第三路和第四路通道。

控制模块设备地址=0x03，功能码=0x10，起始地址=0x0000，寄存器个数=0x08。

控制指令：15 01 00 00 00 17 03 10 00 00 00 08 10 A1 40 FF FF A2 40 FF FF A3 40 00 00 A4 40 00 00

指令解析：

第 字节	1-2	3-4	5-6	7	8	9-10	11-12
内容	15 01	00 00	00 17	03	10	00 00	00 08
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	寄存器起始地址	保持寄存器个数

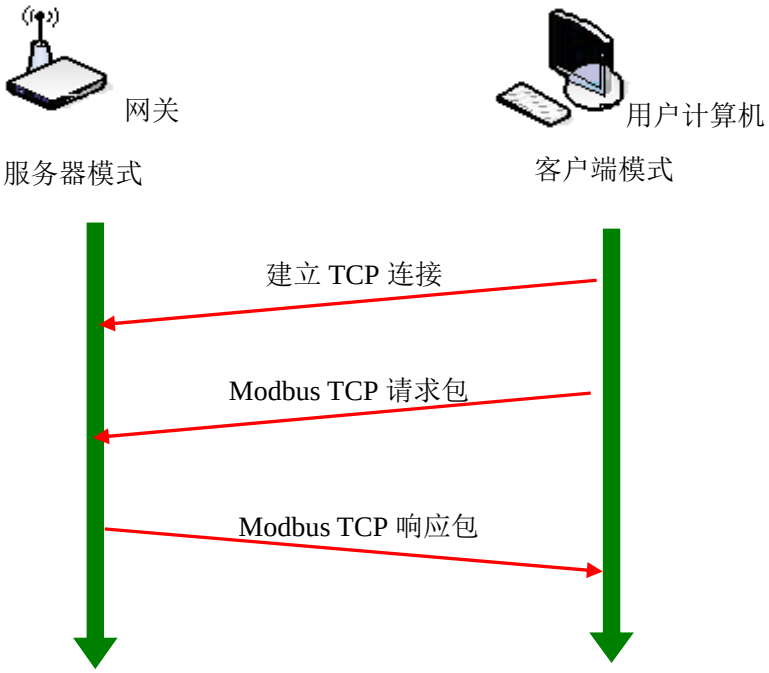
第 字节	13	14-17	18-21	22-25	26-29
内容	10	A1 40 FF FF	A2 40 FF FF	A3 40 00 00	A4 40 00 00
名称	数据长度	A1：开关量 1 40：开关量 FFFF：开	A2：开关量 2 40：开关量 FFFF： 开	A3：开关量 3 40：开关量 0000： 关	A4：开关量 4 40：开关量 0000： 关

返回数据：15 01 00 00 00 04 03 10 00 08
数据解析：

第 字节	1-2	3-4	5-6	7	8	9-10
内容	15 01	00 00	00 04	03	10	00 08
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	保持寄存器个数

1.4 接口编程指南

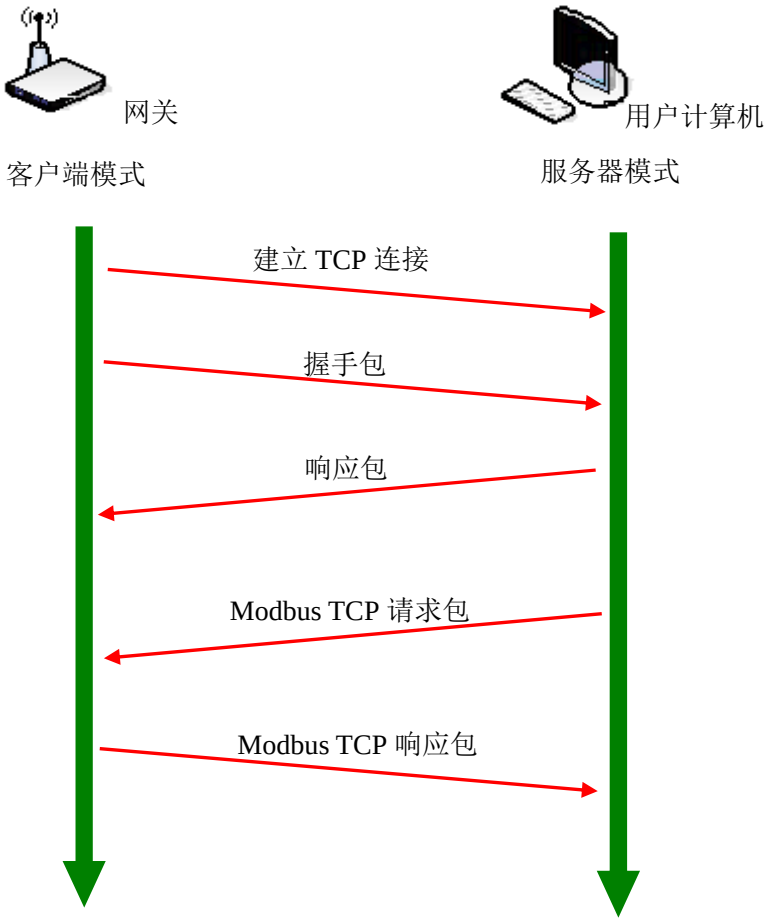
1.4.1 网关做服务器



注：按照功能分，Modbus Tcp 的请求包分 3 种：
（1）读取网关采集节点的通道值包
（2）读取网关采集节点和控制节点的状态值包
（3）对控制节点下发控制指令包

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

1.4.2 网关做客户端



握手包：15 01 22 22 00 10 +网关序列号“2222333444445555”
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 3 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
（3）对控制节点下发控制指令包

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。

2、网关支持 ModbusRtu 查询应答式的通讯协议

2.1 通讯接口定义

数据传输格式：ModbusRtu 格式，CRC 校验；
通讯格式：8 个数据位，无校验，1 个停止位(默认)；
通讯波特率：9600bps，19200bps，38400bps，115200bps(默认)；
数据接口：RS232 或者 RS485 接口。

2.2 寄存器地址分配

2.2.1 读取传感器的值

0x03 功能码，每个传感器占 64 个寄存器，一个网关最多挂载 64 个传感器。

功能码：0x03（读多个）		
寄存器地址	**寄存器个数**	**功能描述**
0x0000~0x003F	0x40	第 1 路传感器采集值
0x0040~0x007F	0x40	第 2 路传感器采集值
0x0080~0x00BF	0x40	第 3 路传感器采集值
……	……	……
0x0FC0~0x0FFF	0x40	第 64 路传感器采集值

2.2.2 读取传感器的节点序列号

0x03 功能码，每个传感器的节点序列号占 4 个寄存器。

功能码：0x03（读多个）		
寄存器地址	**寄存器个数**	**功能描述**
0x1000~0x1003	0x04	第 1 路传感器节点序列号
0x1004~0x1007	0x04	第 2 路传感器节点序列号
0x1008~0x100B		第 3 路传感器节点序列号
……	……	……
0x10FC~0x10FF	0x04	第 64 路传感器节点序列号

2.2.3 读取传感器的在线状态

0x01 功能码，读取 1 至 64 个传感器的在线离线状态，从 0 开始寻址，因此寻址传感器 1-64 为 0-63。指令响应报文中的数据域的每个比特表示一个传感器的状态，一个字节为 8 个比特，表示 8 个传感器的状态，1 为在线，0 为离线。如果返回的输出数量不是 8 的倍数（即不够一个字节），将用 0 填充最后数据字节中的剩余比特。

功能码：0x01（读多个）		
寄存器地址	**功能描述**	**备注**
0x0001	01 节点传感器的在线状态	1 代表在线，0 代表不在线
0x0001	02 节点传感器的在线状态	1 代表在线，0 代表不在线
0x0002	03 节点传感器的在线状态	1 代表在线，0 代表不在线

……	……	……
0x003F	64 节点传感器的在线状态	1 代表在线，0 代表不在线

2.3 Modbus RTU 通讯协议解析

2.3.1 03 功能码：读取传感器的值和序列号

1、读取网关下挂的第一个传感器的值

查询指令(Hex)：01 03 00 00 00 40 44 3A

指令格式解析						
指令	01	03	00 00	00 40	44	3A
内容	设备地址	功能码	起始地址	寄存器个数	CRC 校验	

返回数据(Hex):01 03 80 01 81 FF 68 02 01 00 FD F2 01 00 1E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2A A0

返回数据解析						
数据	01	03	80	01 81 FF 68	02 01 00 FD	F2 01 00 1E
内容	设备地址	功能码	128 个字节	第 1 通道采集值，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-152；温度：-15.2℃（4 字节）	第 2 通道采集值，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 3 通道采集值，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）

数据	00 00 00 00	……	00 00 00 00	4C 7C
内容	第 4 通道采集值，因该传感器共包含 3 种采集值，故其余通道全为 0。	……	同第 4 通道	CRC 校验

以上数据解析的内容的详细资料参见昆仑海岸物联网无线通讯协议

http://www.klha.cn/upload/file/1468480490.pdf

2、读取网关下挂的第一个传感器的序列号

查询指令(Hex)：01 03 10 00 00 04 40 C9

指令格式解析						
指令	01	03	10 00	00 04	40	C9
内容	设备地址	功能码	起始地址	寄存器个数	CRC 校验	

返回数据(Hex)：01 03 08 01 1F 01 01 19 24 00 32 40 49

返回数据解析					
数据	01	03	08	01 1F 01 01 19 24 00 32	40 49
内容	设备地址	功能码	32 个字节	传感器序列号	校验码

2.3.2 01 功能码：读取传感器状态

读取网关下挂的 1-64 个传感器的状态

查询指令(Hex)：01 01 00 00 00 40 3D FA

指令格式解析						
指令	01	01	00 00	00 40	3D	FA
内容	设备地址	功能码	起始地址	输入寄存器个数	CRC 校验	

返回数据(Hex)：01 01 08 00 01 00 00 00 00 00 00 24 DD

返回数据解析								
数据	01	01	08	00	01	……	00	24 DD
内容	设备地址	功能码	32 个字节	第 1~8 个节点在线状态	第 9~16 个节点在线状态，9 在低位，16 在高位，及第 9 节点为在线状态，其余为离线状态。	……	第 57~64 个节点在线状态	CRC 校验