物联网网关
通讯协议
V1.2

北京昆仑海岸传感技术有限公司

目录

KL-H1200 系列网关共分 4 个标准型号，如图所示：

产品型号	4～20mA 电流信号采集路数	0~5V 电压信号采集路数	开关量信号采集路数	继电器输出控制路数
KL-H1200-A	4	------	4	2
KL-H1200-B	------	4	4	2
KL-H1200-C	8	------	------	2
KL-H1200-D	------	8	------	2

带串口扩展可以在标准型号后面添加串口后缀，
如扩展 2 路 RS232 串口，KL-H1200-A/B/C/D-232
扩展 2 路 RS485 串口，KL-H1200-A/B/C/D-485
扩展 1 路 RS232，一路 RS485，KL-H1200-A/B/C/D-232-485
以 KL-H1200-A 为例，网关在使用 ModbusTcp 通讯是，在系统内部将虚拟出两个设备，一个设备为 4 路电流 4-20mA 采集，4 路开关量采集，令一个设备为 2 路的控制设备，采集设备固定的设备地址为 0x01，控制设备固定的设备地址为 0x02，用户无法更改。使用 ModbusRtu 通讯除外。

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	协议	长度	单元			

标识符		标识符				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

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

1.3 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	0x01/0x02/0x03/0x04

1.4 0x10 功能码：下发控制命令

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

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

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	0x0002	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	协议	从第七字	单元标	功能码	读取所	ASSIC码表

	标识符	标识符	节之后所有数据的字节数	识符（设备地址）		有通道的字节数	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

网关设备地址为 0xFF, 读线圈功能码：0x01，读取网关内 2 个虚拟节点在线状态。

查询命令

15 01 00 00 00 06 FF 01 55 55 00 02

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 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	读线圈起始地址	线圈数量，2个线圈，2个节点在线状态

返回数据

15 01 00 00 00 06 FF 01 01 01

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

2.3 功能码：读保持寄存器 0x03

网关内部虚拟了 2 个节点设备，一个 8 路采集节点，一个 2 路控制节点，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
虚拟节点的设备地址 采集节点：0x01 控制节点：0x02	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）读取采集节点的所有 32 个通道的值

设备地址=0x01，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 01 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	01	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 01 03 80 C0 03 0F A0 C1 03 0F A0 C2 03 0F A0 C3

03 0F A0 B1 40 FF FF B2 40 FF FF B3 40 FF FF B4 40 FF FF 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	01	03	80	C0 03 0F A0
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	…	38-41
内容	C1 03 0F A0	C2 03 0F A0	C3 03 0F A0	B1 40 FF FF	…	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 01 83 01（02/03/04/0C/0D/0E/0F）

（2）读取采集节点的第 3 个通道值
设备地址=0x01，起始地址=0x0004，寄存器个数=2
查询命令
15 01 00 00 00 06 01 03 00 04 00 02

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 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 01 03 04 C2 03 0F A0

第 字节	1-2	3-4	5-6	7	8	9	10-13
内容	15 01	00 00	00 07	01	03	04	C2 03 0F A0
名称	事物元标	协议	从第七字	单元标识	功能	读取所	第1通道的标识符

	识符	标识符	节之后所有数据的字节数	符（设备地址）	码	有通道的字节数	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 01 83 01（02/03/04/0C/0D/0E/0F）

2.4 功能码：写保持寄存器 0x10

本控制指令需配合 KL-H1000 控制模块使用，控制模块带 2 路继电器输出控制，每路控制量占一个通道，2 路开关量控制即占 2 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
控制节点的设备地址 0x02	第 1 路	0x0000	0x02	开：A140 FFFF 关：A140 0000
	第 2 路	0x0002	0x02	开：A240 FFFF 关：A240 0000

示例：

（1）打开控制节点的第一路继电器输出

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 01 90 01（02/03/04/0C/0D/0E/0F）

（2）关闭控制节点的第二路继电器输出

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 01 90 01（02/03/04/0C/0D/0E/0F）

2.5 读取通道值解析

从网关读取的通道值如 A1 40 FF FF、C0 03 0F A0 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	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℃ （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	
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）	
C4	模拟量 5（mA）	
C5	模拟量 6（mA）	
C6	模拟量 7（mA）	
C7	模拟量 8（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）	
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	
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

2.6 通道值解析实例

以 KL-H1200-A 为例。
示例 1：读取采集节点的 8 路通道值（4 路模拟量和 4 路开关量）。
设备地址=0x01，起始地址=0x0000，寄存器数量=0x10
查询命令
15 01 00 00 00 06 01 03 00 00 00 10

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 10
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 23 01 03 20 C0 03 0F A0 C1 03 0F A0 C2 03 0F A0 C3 03 0F A0 B1 40 FF FF B2 40 FF FF B3 40 00 00 B4 40 FF FF

第 字节	1-2	3-4	5-6	7	8	9
内容	15 01	00 00	00 23	01	03	20
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	22-25
C0 03 0F A0	C1 03 0F A0	C2 03 0F A0	C3 03 0F A0
C0：第1路电流输入；03：无符号3位小数 0FA0：电流值，转换成十进制为4000；电流值：4.000mA	C1：第2路电流输入；03：无符号3位小数 0FA0：电流值，转换成十进制为4000；电流值：4.000mA	C2：第3路电流输入；03：无符号3位小数 0FA0：电流值，转换成十进制为4000；电流值：4.000mA	C3：第4路电流输入；03：无符号3位小数 0FA0：电流值，转换成十进制为4000；电流值：4.000mA

26-29	30-33	34-37	38-41
B1 40 FF FF	B2 40 FF FF	B3 40 00 00	B4 40 FF FF
B1：第1路开关量输入 40：开关量 FF FF：开启	B2：第2路开关量输入 40：开关量 FF FF：开启	B3：第3路开关量输入 40：开关量 00 00：关闭	B4：第4路开关量输入 40：开关量 FF FF：开启

注：具体解析详见 2.5 节。

示例 2：读取控制节点的 2 路通道值。
设备地址=0x02，起始地址=0x0000，寄存器数量=0x04
查询命令
15 01 00 00 00 06 02 03 00 00 00 04

第 字节	1-2	3-4	5-6	7	8	9-10	11-12
内容	15 01	00 00	00 06	02	03	00 00	00 04
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 0B 02 03 08 A1 40 FF FF A2 40 FF FF

第 字节	1-2	3-4	5-6	7	8	9
内容	15 01	00 00	00 0B	02	03	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	读取所有通道的字节数

10-13	14-17
A1 40 FF FF	A2 40 00 00
A1：第1路开关量输出 40：开关量 FF FF：开启	A2：第2路开关量输出 40：开关量 00 00: 关闭

注：具体解析详见 2.5 节。

示例 3：关闭第一路控制，打开第二路控制。
设备地址=0x02，起始地址=0x0000，寄存器数量=0x04，寄存器值=A1 40 00 00 A2 40 FF FF
写指令
15 01 00 00 00 0F 02 10 00 00 00 04 08 A1 40 00 00 A2 40 FF FF

第 字节	1-2	3-4	5-6	7	8	9-10
内容	15 01	00 00	00 0F	02	10	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	保持寄存器起始地址

11-12	13	14-17	18-21
00 04	08	A1 40 FF FF	A2 40 FF FF

保持寄存器数量	读取所有通道的字节数	A1：第1路开关量输出 40：开关量 00 00：关闭	A2：第2路开关量输出 40：开关量 FF FF：开启

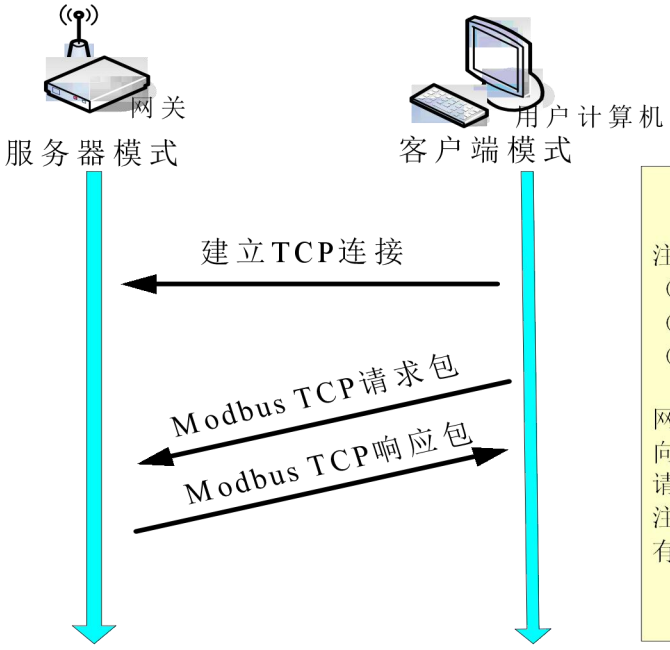
返回数据

15 01 00 00 00 04 02 10 00 04

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

3、接口编程指南

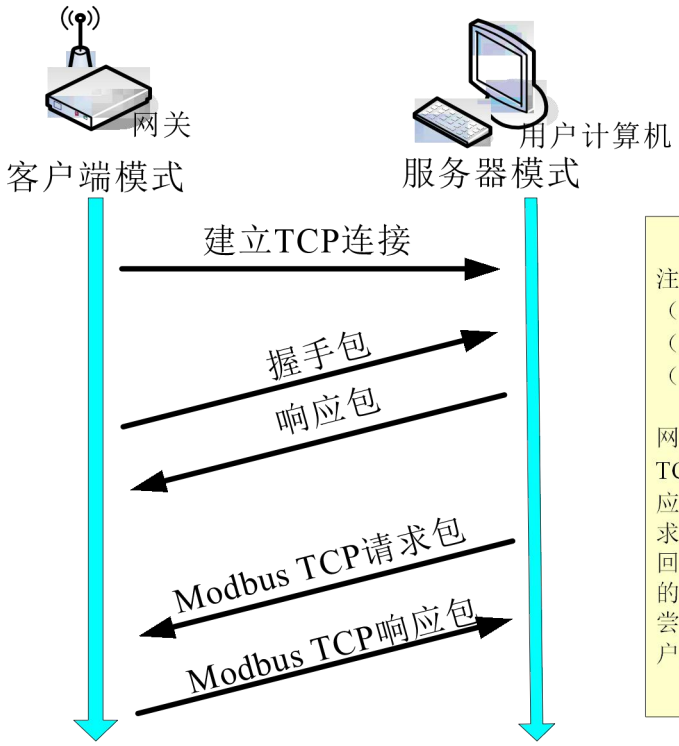
3.1 网关做服务器



注：按照功能分，ModbusTcp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



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，服务器收到我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，网关内客户端启动重连机制，一直在尝试重连，直到服务器端恢复正常。

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

4、网关支持的 Modbus RTU 协议的功能码

4.1 通讯接口定义

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

4.2 寄存器地址分配

1. 模拟量和开关量输入寄存器

功能码：0x03（读多个）		
寄存器地址	**功能描述**	**备注**
0x0000H	第 1 路模拟量采集值	模拟量：无符号 16 位整型数
0x0002H	第 2 路模拟量采集值	模拟量：无符号 16 位整型数
0x0004H	第 3 路模拟量采集值	模拟量：无符号 16 位整型数
0x0006H	第 4 路模拟量采集值	模拟量：无符号 16 位整型数
0x0008H	第 5 路模拟量采集值或 第 1 路开关量输入状态	模拟量：无符号 16 位整型数 开关量：00 00 代表关，FF FF 代表开
0x000AH	第 6 路模拟量采集值或 第 2 路开关量输入状态	模拟量：无符号 16 位整型数 开关量：00 00 代表关，FF FF 代表开
0x000CH	第 7 路模拟量采集值或 第 3 路开关量输入状态	模拟量：无符号 16 位整型数 开关量：00 00 代表关，FF FF 代表开
0x000EH	第 8 路模拟量采集值或 第 4 路开关量输入状态	模拟量：无符号 16 位整型数 开关量：00 00 代表关，FF FF 代表开

2. 继电器输出寄存器

功能码：0x03（读多个） 0x05（写单个）		
寄存器地址	**功能描述**	**备注**
0x0011H	第 1 路继电器控制输出值	00 00 代表断开；FF FF 代表导通
0x0013H	第 2 路继电器控制输出值	00 00 代表断开；FF FF 代表导通

4.3 Modbus RTU 通讯协议解析

4.3.1 03 功能码：读取模拟量和开关量采集值

1、读模拟量和开关量采集值

查询指令(Hex)：01 03 00 00 00 10 44 06

指令格式解析						
指令	01	03	00 00	00 10	44	06
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 20 C0 03 2E E0 C1 03 0F A0 C2 03 0F A0 C3 03 0F A0 B1 40 00 00 B2 40 00 00 B3 40 FF FF B4 40 FF FF 4C 7C

返回数据解析							
数据	01	03	20	C0 03 2E E0	C1 03 0F A0	C2 03 0F A0	C3 03 0F A0
内容	设备地址	功能码	32 个字节	第 1 路电流值 C0：数据代码 03：无符号 3 位小数 2E E0:电流值，十进制 4000，即电流值为 12.000mA	第 2 路电流值 C1：数据代码 03：无符号 3 位小数 0F A0:电流值，十进制 4000，即电流值为 4.000mA	第 3 路电流值 C2：数据代码 03:无符号 3 位小数 0F A0:电流值，十进制 4000，即电流值为 4.000mA	第 4 路电流值 C3：数据代码 03：无符号 3 位小数 0F A0:电流值，十进制 4000，即电流值为 4.000mA

数据	B1 40 00 00	B2 40 00 00	B3 40 FF FF	B4 40 FF FF	4C 7C
内容	第 1 路开关量值 B1：开关量输入 40：开关量 00 00 ：关	第 2 路开关量值 B2：开关量输入 40：开关量 00 00 ：关	第 2 路开关量值 B3：开关量输入 40：开关量 FF FF：开	第 2 路开关量值 B4：开关量输入 40：开关量 FF FF ：开	CRC 校验

2、读取继电器控制输出值

查询指令(Hex)：01 03 00 11 00 04 14 0C

指令格式解析						
指令	01	03	00 11	00 04	14	0C
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 A1 40 FF FF A2 40 00 00 3D D0

返回数据解析						
数据	01	03	08	A1 40 FF FF	A2 40 00 00	3D D0
内容	设备地址	功能码	32 个字节	A1：第 1 路继电器输出状态 40：开关量 FF FF：继电器导通	A2：第 2 路继电器输出状态 40：开关量 00 00：继电器断开	校验码

4.3.2 05 功能码：写单个继电器状态

1、控制第一路继电器打开

控制指令：01 05 00 11 **FF 00** DC 3F

指令格式解析						
指令	01	05	00 11	FF 00	DC	3F
内容	设备地址	功能码	起始地址	寄存器值	CRC 校验	

寄存器值：FF 00：代表继电器导通

00 00：代表继电器断开

返回数据：01 05 00 11 **FF 00** DC 3F

返回数据解析						
数据	01	05	00 11	FF 00	DC	3F
解析	设备地址	功能码	起始地址	寄存器值	CRC 校验	

2、控制第二路继电器关闭

控制指令：01 05 00 13 **00 00** 3C 0F

指令格式解析						
指令	01	05	00 13	00 00	3C	0F
内容	设备地址	功能码	起始地址	寄存器值	CRC 校验	

寄存器值：FF 00：代表继电器导通

00 00：代表继电器断开

返回数据：01 05 00 13 **00 00** 3C 0F

返回数据解析						
数据	01	05	00 11	FF 00	3C	0F
解析	设备地址	功能码	起始地址	寄存器值	CRC 校验	