

# MBUS 远传通讯协议

## 一、通讯数据格式

字节	0	1	2	3	4	5	6	7	8	9	10	…… n	n + 1	n + 2
Code	68	T	A0	A1	A2	A3	A4	A5	A6	C	L	DATA	CS	16
说明	起始帧	表类型	表地址							控制码	数据长度	数据	校验码	结束帧

### 1、表类型 T:

表 3 仪表类型及其代码

仪表类型	代码(T)	仪 表
10 H~19 H:水表	10 H	冷水水表
	11 H	生活热水水表
	12 H	直饮水水表
	13 H	中水水表
20 H~29 H:热量表	20 H	热量表(计热量)
	21 H	热量表(计冷量)
30 H~39 H:燃气表	30 H	燃气表
40 H~49 H:其他仪表	40 H	如:电度表

根据 CJ-T188-2004 规约，设定表计类型及其代码，设定**水表为 10H**，**电表为 40H**。

### 2、表地址

表地址由 A0~A6 共 7 个字节表示，字节形式为 16 进制形式，其结构见下表

表地址						
A0	A1	A2	A3	A4	A5	A6
地址码			表类型		厂商代码	

厂商代码：同卡结构内块 7 厂商代码，用于区分不同厂家。对每个厂家，该代码唯一不变。

表 类 型：用于区分该表类型，其划分同表类型 T，方便对统一厂家内不同类型表进行区别编号。

地 址 码：厂商内该表型唯一编号，编号在出厂时设定，一般不做修改。

注：地址 AA AA AA AA AA AA AAH 为总线广播地址，所有地址的表均应该对该广播指令接收机处理。

广播指令一般用于表计设置、参数、地址读取等，且使用时应点对点通讯，防止总线被堵塞。

### 3、控制码

控制码是控制指令的类型。控制码各位说明见 188 规约。

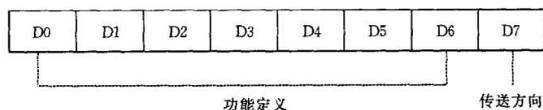


图 2 控制码格式

- D7:0——由主站发出的控制帧；
- 1——由从站发出的应答帧。
- D6:0——通讯正常；
- 1——通讯异常。
- D5~D0: 000000:保留；
- 000001:读数据；
- 000100:写数据；
- 001001:读密钥版本号；
- 000011:读地址(表号)；
- 010101:写地址(表号)；
- 010110:写机电同步数(置表底数)；
- 1XXXXX:厂商自定义。

控制码与控制指令和操作对象关系见下表。

指令类型	控制码	应答码	数据标识	数据类型	备注
读数据	01H	81H	901FH	读累计流量	累计流量+表状态字
读地址	03H	83H	810AH	读表地址	
			81AAH	读用户参数	读系统号, 用户号, 表号
写数据	04H	84H	A013H	写购买金额	
			A017H	写阀门状态	开: 55H; 关: 99H
			A021H	初始化表状态	0xC3 可清厂商代码, 0x5A 可清单位代码, 其它同普通清零卡
			A027H	写用户参数	写系统号, 用户号, 表号
写地址	15H	95H	A018H	写新地址	写 A0~A6, 以新地址号返回

### 4、数据长度

为数据域的字节数。

### 5、数据域

数据域为写入表端、或表端返回的参数、数据。其包含的内容如下。

数据域						
D10	DI1	SER	1	2	.....	n
数据标识		序列号 00H	数据内容			

## 6、校验值

为从帧起始符 68H（开始的）所有字节十六进制累加和。单独为 1 个字节。

## 二、通讯指令

### 1、读表数据

表示读取地址为 A0~A6 表端的累计使用量及设备状态。

采集器——>表 端：

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	01H	03H	90H	1FH	00H	CS	16H
说明	起始帧	表类型	表地址（广播或指定）						控制码	数据长度	数据标识	序列号	校验码	结束帧		

表 端——>采集器：

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	81H	12H	90H	1FH	00H	高	中	中	低	高	中	中	低	高	中	中	低	xxH	S0	S1	CS	16H
说明	起始帧	表类型	表地址（本机）						控制码	数据长度	数据标识	序列号	累计使用量			剩余量			总购买量			次数	状态字	校验码	结束帧						

状态字说明：

S1：保留

S0：见下表

表 14 状态 ST 第一字节定义表

	D0	D1	D2	D3	D4	D5	D6	D7
定义	阀门状态		电池电压	—	—			
说明	00:开 01:关 11:异常		0:正常 1:欠压	保留	保留	厂商定义	厂商定义	厂商定义

### 2、读表地址

采集器——>表 端：

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Code	68H	T	AA	AA	AA	AA	AA	AA	AA	03H	03H	81H	0AH	00H	CS	16H
说明	起始帧	表类	表地址（广播）						控制码	数据长度	数据标识	序列	校验	结束帧		

	帧	型													号	码	
--	---	---	--	--	--	--	--	--	--	--	--	--	--	--	---	---	--

表端——>采集器:

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	83H	03H	81H	0AH	00H	CS	16H
说明	起始帧	表类型	表地址（本机）						控制码	数据长度	数据标识	序列号	校验码	结束帧		

### 3、写购买数据

采集器——>表端:

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	04H	08H	A0H	13H	00H	xxH	高	中	中	低	CS	16H
说明	起始帧	表类型	表地址（广播或指定）						控制码	数据长度	数据标识	序列号	次数	当前购买量	校验码	结束帧					

购买次数、本次购买量、总购买量等均是十六进制数据。

购买次数 > 表内次数+1: 次数错误, 返回表内次数+末次购买量

购买次数 = 表内次数+1: 正常购买, 返回购买后表内次数+末次购买量

购买次数 < 表内次数+1: 次数错误, 返回表内次数+末次购买量

表端——>采集器:

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	84H	08H	A0H	13H	00H	xxH	高	中	中	低	CS	16H
说明	起始帧	表类型	表地址（本机）						控制码	数据长度	数据标识	序列号	次数	末次成功购买量	校验码	结束帧					

#### 购买次数说明

	实际次数	系统中（指令）次数 （销售前）	系统中（指令）次数 （销售后）	表端次数 （销售前）	表端次数 （销售后）
第 1 次销售	1	0	1	0	1
2	2	1	2	1	2
3	3	2	3	2	3
...	...	...	...	...	...
255	255	254	255	254	255
256	256	255	256	255	0
257	257	256	257	0	1

数据域（购买次数+购买量）内容加密传输，上行下行传输均使用相同加密算法。

加密方式:

- ①计算 A0、A1、A2、A3、A4、A5、A6 单字节累加和为 x，次数与 x 异或值为 y；
- ②计算购买量 4 字节内容与 x 按字节异或值 z；
- ③z 值一起循环左移 y 位。

例：表地址 A0-A6： 12H 23H 34H 45H 10H 67H 78H

购买次数：05H

购买量：00H 00H 03H 45H

→ x = 9DH

→ y = 98H

→ z = 9DH 9DH 9EH D8H

→ 次数：98H

购买量：D8H 9DH 9DH 9EH

注：校验码为加密后的数据域数据与其他位置数据的单字节累加和。

## 4、写阀门状态

采集器——>表端：

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	04H	04H	A0H	17H	00H	55H/99H	CS	16H
说明	起始帧	表类型	表地址（广播或指定）						控制码	数据长度	数据标识	序号	开/关	校验码	结束帧		

表端——>采集器：

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	84H	05H	A0H	17H	00H	S0	S1	CS	16H
说明	起始帧	表类型	表地址（本机）						控制码	数据长度	数据标识	序号	状态码	校验码	结束帧			

## 5、写地址

采集器——>表端：

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	15H	0AH	A0H	18H	00H	A0	A1	A2	A3	A4	A5	A6	CS	16H
说明	起始帧	表类型	表地址（广播或指定）						控制码	数据长度	数据标识	序号	新地址						校验码	结束帧			

表端——>采集器：

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	95H	03H	A0H	18H	00H	CS	16H
说明	起始帧	表类型	新表地址（本机）						控制码	数据长度	数据标识	序号	校验码	结束帧		

## 6、写用户参数

采集器——>表端：

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	04H	0AH	A0H	27H	00H	00H	63H	00H	01H	01H	0	0	CS	16H
说明	起始帧	表类型	表地址（广播或指定）						控制码	数据长度	数据标识	序列号	单位代码	用户号	表号	空	校验码	结束帧					

表端——>采集器：

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	84H	0AH	A0H	27H	00H	00H	63H	00H	01H	01H	0	0	CS	16H
说明	起始帧	表类型	表地址（本机）						控制码	数据长度	数据标识	序列号	单位代码	用户号	表号	空	校验码	结束帧					

## 7、读用户参数

采集器——>表端：

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Code	68H	T	AA	AA	AA	AA	AA	AA	AA	03H	03H	81H	AAH	00H	CS	16H
说明	起始帧	表类型	表地址（广播）						控制码	数据长度	数据标识	序列号	校验码	结束帧		

表端——>采集器：

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	83H	0AH	81H	AAH	00H	00H	63H	00H	01H	01H	0	0	CS	16H
说明	起始帧	表类型	表地址（本机）						控制码	数据长度	数据标识	序列号	单位代码	用户号	表号	空	校验码	结束帧					

## 8、清零初始化

采集器——>表端：

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	04H	04H	A0H	21H	00H	C3H/ 其它	CS	16H
说明	起始帧	表类型	表地址（广播或指定）						控制码	数据长度	数据标识	序列号	清零类型	校验码	结束帧		

表端——>采集器:

字节	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Code	68H	T	A0	A1	A2	A3	A4	A5	A6	84H	03H	A0H	21H	00H	CS	16H
说明	起始帧	表类型	新表地址（本机）						控制码	数据长度	数据标识		序列号	校验码	结束帧	