

台区精益化管理系统 通信协议

密 级： 机密

编 写 人： 程建刚

文档版本： 2.38

更新日期： 20210513



北京恒启达科技有限公司
Beijing HunchTek Co., Ltd.

2021 年 1 月 10 日

目 录

- 1、概述
- 2、上行数据包
 - 2.1 上行数据包结构
 - 2.2 报文：心跳包（所有终端）
 - 2.3 报文：时钟查询命令包（所有终端）
 - 2.4 报文：状态查询应答包（所有终端）
 - 2.5 报文：定期采集数据包（台变监测终端）
 - 2.6 报文：定期采集数据包（总表监测终端）
 - 2.7 报文：定期采集数据包（分支监测终端）
 - 2.8 报文：定期采集数据包（表箱监测终端）
 - 2.9 报文：设置心跳周期应答包（所有终端）
 - 2.10 报文：设置采集周期应答包（所有终端）
 - 2.11 报文：设置通信信道应答包（所有终端）
 - 2.12 报文：电表召测应答包（表箱监测终端）
- 3、下行数据包
 - 3.1 下行数据包结构
 - 3.2 报文：状态查询命令包（所有终端）
 - 3.3 报文：时钟查询应答包（所有终端）
 - 3.4 报文：设置心跳周期命令包（所有终端）
 - 3.5 报文：设置采集周期命令包（所有终端）
 - 3.6 报文：设置通信信道命令包（所有终端）
 - 3.7 报文：电表召测命令包（表箱监测终端）

1、概述

在精益化台区管理系统中，当前包含 4 类终端设备：台变监测终端、总表监测终端、分支监测终端、表箱监测终端。这些设备通过 4G 无线网络与服务器通信。

终端与服务器之间的通信包括以下几类：

- (1) 在终端上电后，终端按照指定的 IP、端口号，与服务器建立 TCP 连接。
- (2) 终端以固定的周期（例如 5 分钟），向服务器发送“定期采集数据包”，这是最主要的通信内容。此通信不要求可靠，服务器也不返回应答。
- (3) 终端发送的心跳包。
- (4) 服务器或终端发送的命令包、应答包。

数据格式说明：

- (1) 本文中的数值，未特别注明的均为十进制，加"0x"前缀的为十六进制。
- (2) 数据字节序为小端模式，即：先发送或先存储的是低位字节。
- (3) unixstamp 时间格式：以 32 位无符号整数来记录时刻，遵循 UNIX 时间戳，其值等于自 1970-01-01 0:0:0 开始，到某个时刻的累计秒数。
- (4) 本文中所说的 CRC8 校验，其使用的多项式是 $X^8+X^5+X^4+1$ ，算法的 C 语言描述如下：

```
unsigned char CRC8Cal(unsigned char *ptr, unsigned int len)
{
    unsigned char i;
    unsigned char crc = 0; //初始 crc 值=0

    if (len > 65536) return 0;
    while (len-->0)
    {
        crc ^= *ptr; //每次先与需要计算的数据异或,计算完指向下一数据
        ptr++;
        for (i=8; i>0; --i) //计算一个字节的 crc
        {
            if (crc & 0x80) crc = ((crc << 1) ^ 0x31);
            else crc <<= 1;
        }
    }
    return crc;
}
```

其它：

- (1) 对于组合有功电能、瞬间功率、温度，服务器接收到数据，并换算为实际值时，其值允许为负值。
- (2) 终端的采集时刻，总是对齐到整数分钟，因此秒值总是 0。
- (3) 每个分支监测终端内含 8 个监测单元，每个单元均具有独立的终端地址，因此，服务器软件可以将每个监测单元看作一个独立设备。但由于这 8 个监测单元使用的是同一个通信硬件，因此软件上也是同一个 socket 连接。设置分支监测终端的参数时，只需设置某一个监测单元即可。
- (4) 当前版本，对于终端身份认证、通信数据加密等问题，暂不考虑，留待后续升级。

2、上行数据包

2.1 上行数据包结构

终端向服务器发送的数据包，结构如下。

长度 (字节)	数据类型	项目	描述
4	uint8	帧头	固定为：0xFF、0xFF、0xFF、0x5A
1	uint8	数据包长度	数据包的全部数据的长度，含帧头、CRC 校验码、帧尾。合法值=[17,249]
1	uint8	终端类型	合法值如下： 0：台变监测终端 1：总表监测终端 2：分支监测终端 3：表箱监测终端
1	uint8	报文类型	合法值如下： 0：终端心跳包 1：时钟查询命令包 2：状态查询应答包 3：定期采集数据包 4：设置心跳周期应答包 5：设置采集周期应答包 6：设置通信信道应答包 7：电表召测应答包
1	uint8	报文格式版本	合法值范围=[0,250]，当前均为 0
4	uint32	终端通信地址	合法值范围=[1,999999999]，例如：123456789。 在终端外壳上印刷的终端地址，长度总是 9 位数字。
0-232		报文内容	详见后文（其中，心跳包报文内容为空、长度=0）
1	uint8	CRC8 校验码	对本字节之前的所有字节（包括帧头），执行 CRC8 运算的结果，算法见前文。
4	uint8	帧尾	固定为：0xFF、0xFF、0xFF、0x53

2.2 报文：心跳包（所有终端）

示例：

0xFF,0xFF,0xFF,0x5A,0x11,0x00,0x00,0x00,0x00,0x04
0x00,0x00,0x20,0xFF,0xFF,0xFF,0x53,

解析：

长度 = 17

终端类型代码 = 0：台变监测终端

报文类型代码 = 0：终端心跳包

报文格式版本 = 0

终端通信地址 = 1024

2.3 报文：时钟查询命令包（所有终端）

在终端需要校准时钟时，会发送此命令，以与服务器的时钟同步。为了减少通信延迟所带来的误差，终端会检查从发送命令到收到应答的延迟，若延迟>10 秒，则过一段时间再重试，直到满足要求。为确保服务器时钟准确，所有服务器应在每天的 23 点 50 分同步到网络时间。

版本 0，结构如下：

长度 (字节)	数据类型	项目	描述
1	uint8	时间值格式	当前版本总是=0，即：unixstamp 格式

示例：

0xFF,0xFF,0xFF,0x5A,0x12,0x00,0x01,0x00,0x00,0x04
0x00,0x00,0x00,0x81,0xFF,0xFF,0xFF,0x53,

解析：

长度 = 18

终端类型代码 = 0：台变监测终端

报文类型代码 = 1：时钟查询命令包

报文格式版本 = 0

终端通信地址 = 1024

报文：

时间值格式 = 0

2.4 报文：状态查询应答包（所有终端）

版本 0，结构如下：

长度 (字节)	数据类型	项目	描述
			（以下为运行状态数据）
2	uint16	终端状态码	终端当前的运行状态
1	uint8	终端 CPU 使用率	终端当前的 CPU 使用率，百分比，范围=[0,100]
1	uint8	网络信号强度	当前 4G 或 5G 信号的强度，百分比，范围=[0,100]
4	uint32	应答时刻	unixstamp 格式时间值
			（以下为统计数据）
4	uint32	统计数据保存时刻	统计数据最后一次保存到 EEPROM 的 CPU 时刻 本字段仅供内部使用
4	uint32	终端最后上电时刻	unixstamp 格式时间值 若该值=0，表明上电后未实现时钟同步。
4	uint32	终端累计上电次数	终端上电的累计次数
4	uint32	终端累计错误次数	终端出现硬件错误的累计次数
2	uint16	终端最后错误码	终端最后一次的错误码
4	uint32	终端最后错误发生时刻	unixstamp 格式时间值 若该值=0，表明上电后未实现时钟同步。
8	uint64	DTU 累计发送流量	DTU 累计发送的数据量，单位=字节
4	uint32	DTU 累计错误次数	DTU 出现错误的累计次数
2	uint16	DTU 最后错误码	DTU 通信程序最后一次的错误码
4	uint32	DTU 最后错误发生时刻	unixstamp 格式时间值 若该值=0，表明上电后未实现时钟同步。
4	uint32	DTU 最近第 1 次(当前的连接)在线时长	DTU 保持连续在线的时间长度，单位=秒
4	uint32	DTU 最近第 2 次在线时长	同上
4	uint32	DTU 最近第 3 次在线时长	同上
4	uint32	DTU 最近第 4 次在线时长	同上
			（以下为配置数据）
4	uint32	终端生产日期	unixstamp 格式时间值
4	uint32	终端通信地址	合法值范围=[1,999999999]，例如：123456789。 在终端外壳上印刷的终端地址，长度总是 9 位数字。
2	uint16	心跳周期	合法值=[3,3600]，单位=秒。
2	uint16	上传周期	合法值=[3,3600]，单位=秒。 当前版本，实际只支持以下值：60、180、300。
2	uint16	上传延时	合法值=[0,50000]，单位=毫秒。 终端在采集数据后，延时指定的时间，再上传数

台区精益化管理系统 通信协议

			据包。
4	uint32	主站 IP	例如：IP= “255. 1. 2. 3” 则： 值=0xFF010203 注意：IP 的左边的值保存到高字节
2	uint16	主站端口号	= [1024, 65535]
4	uint8	备用 IP	(同上)
2	uint16	备用端口号	(同上)
20	uint8	APN 用户名	最多 20 个 ASC2 字符，以空白为结束符
20	uint8	APN 密码	最多 20 个 ASC2 字符，以空白为结束符
1	uint8	APN 鉴权方式	=0 不鉴权 =1 PAP 方式：采用明文传输用户名和密码 =2 CHAP 方式：加密传输用户名和密码
1	uint8	运营商代码	=0 移动 =1 联通 =2 电信
1	uint8	SIM 卡绑定标志	=0 未绑定 =1 终端已与下列 SIM 卡绑定
20	uint8	SIM 卡 ICCID 编码	由 20 个 ASC2 字符组成，大部分为数字。 若未绑定，则此项值无意义

示例：

0xFF,0xFF,0xFF,0x5A,0xAA,0x00,0x02,0x00,0x15,0xCD
0x5B,0x07,0x00,0x00,0x01,0x63,0xEF,0xF0,0x9C,0x60
0x00,0x00,0x00,0x00,0xD0,0xF0,0x9C,0x60,0x06,0x00
0x00,0x00,0x01,0x00,0x00,0x00,0x10,0x00,0x6C,0xF0
0x9C,0x60,0xB5,0x17,0x00,0x00,0x00,0x00,0x00,0x00
0x57,0x00,0x00,0x00,0x0A,0x00,0x30,0xEE,0x9C,0x60
0x1F,0x00,0x00,0x00,0x1C,0x01,0x00,0x00,0xA4,0x00
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x66,0xEE,0x5F
0x15,0xCD,0x5B,0x07,0x46,0x00,0x3C,0x00,0x0A,0x00
0x13,0x62,0x36,0x6A,0x74,0xAF,0x00,0x00,0x00,0x00
0x6C,0x75,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00
0x00,0x00,0x00,0x02,0x00,0x31,0x32,0x33,0x34,0x35
0x36,0x37,0x38,0x31,0x32,0x33,0x34,0x35,0x36,0x37
0x38,0x31,0x32,0x33,0x34,0x8D,0xFF,0xFF,0xFF,0x53

解析：

长度 = 170

终端类型代码 = 0：台变监测终端

报文类型代码 = 2：状态查询应答包

报文格式版本 = 0

终端通信地址 = 123456789

报文：

终端状态码 = 0
CPU 使用率 = 1%
网络信号强度 = 99%
上传时刻 = 2021-5-13 9:27:11
统计数据保存 CPU 时刻 = 0S
终端最后上电时刻 = 2021-5-13 9:26:40
终端累计上电次数 = 6
终端累计错误次数 = 1
终端最后错误码 = 16
终端最后错误发生时刻 = 2021-5-13 9:25:0
DTU 累计发送流量 = 6069 字节
DTU 累计错误次数 = 87
DTU 最后错误码 = 10
DTU 最后错误发生时刻 = 2021-5-13 9:15:28
DTU 最近第 1 次在线时长 = 31S
DTU 最近第 2 次在线时长 = 284S
DTU 最近第 3 次在线时长 = 164S
DTU 最近第 4 次在线时长 = 0S
终端生产日期 = 2021-1-1 0:0:0
终端通信地址 = 123456789
心跳周期 = 70
上传周期 = 60
上传延迟 = 10
主站 IP = 106.54.98.19
主站端口号 = 44916
备用 IP = 0.0.0.0
备用端口号 = 30060
APN 用户名 =
APN 密码 =
APN 鉴权方式 = 0 不鉴权
运营商代码 = 2 电信
SIM 卡绑定方式 = 0 不绑定
SIM 卡 ICCID 编码 = “12345678123456781234”

2.5 报文：定期采集数据包（台变监测终端）

版本 0，结构如下：

长度 (字节)	数据类型	项目	描述
4	uint32	采集时刻	unixstamp 格式时间值 注意：若采集时刻=0，则主站应先将其修改为收到数据包的时刻，再做后续处理。后同。
2	uint16	台变外壳温度	合法值范围=[0,50000]，实际温度=（此值-10000）/100。例如值=12345，表示温度为 23.45 度
2	uint16	环境温度	合法值范围=[0,20000]，实际温度=（此值-10000）/100。例如值=12345，表示温度为 23.45 度
2	uint16	环境湿度	合法值范围=[0,10000]，实际湿度=此值/100。例如：5432，表示湿度=54.32

数据示例：

0xFF,0xFF,0xFF,0x5A,0x1B,0x00,0x03,0x00,0x15,0xCD
0x5B,0x07,0xE4,0xF0,0x9C,0x60,0xE0,0x2E,0x77,0x32
0xDA,0x16,0x84,0xFF,0xFF,0xFF,0x53,

解析：

长度 = 27

终端类型代码 = 0：台变监测终端

报文类型代码 = 3：定期上传数据包

报文格式版本 = 0

终端通信地址 = 123456789

报文：

采集时刻 = 2021-5-13 9:27:0

台变温度 = 20℃

环境温度 = 29.19℃

环境湿度 = 58.5%

2.6 报文：定期采集数据包（总表监测终端）

版本 0，结构如下：

长度 (字节)	数据类型	项目	描述
4	uint32	采集时刻	unixstamp 格式时间值
2	uint16	环境温度	合法值范围=[0,20000]，实际温度=(此值-10000)/100。例如值=12345，表示温度为 23.45 度
2	uint16	环境湿度	合法值范围=[0,20000]，实际湿度=此值/100。例如：5432，表示湿度=54.32
4	uint32	总表组合有功电能	合法值范围=[0,199999999]，实际值=(此值-100000000)/100，单位=KWh。
4	uint32	总表短时平均功率	合法值范围=[0,19999999]，实际值=(此值-10000000)，单位=W。 采集时刻之前 15 分钟的平均有功功率。
2	uint16	A 相电压	合法值范围=[0,9999]，实际值=此值/10，单位=V。
2	uint16	B 相电压	(同上)
2	uint16	C 相电压	(同上)
4	uint32	A 相瞬时有功功率	合法值范围=[0,19999999]，实际值=(此值-10000000)，单位=W。
4	uint32	B 相瞬时有功功率	(同上)
4	uint32	C 相瞬时有功功率	(同上)
2	uint16	总功率因数	合法值范围=[0,1000]，实际值=此值/1000。
2	uint16	A 相功率因数	(同上)
2	uint16	B 相功率因数	(同上)
2	uint16	C 相功率因数	(同上)

2.7 报文：定期采集数据包（分支监测终端）

版本 0，结构如下：

长度 (字节)	数据类型	项目	描述
4	uint32	采集时刻	unixstamp 格式时间值
2	uint16	环境温度	合法值范围=[0,20000]，实际温度=(此值-10000)/100。例如值=12345，表示温度为 23.45 度
2	uint16	环境湿度	合法值范围=[0,10000]，实际湿度=此值/100。例如：5432，表示湿度=54.32
4	uint32	分支组合有功电能	合法值范围=[0,199999999]，实际值=(此值-100000000)/100，单位=KWh。
4	uint32	分支短时平均功率	合法值范围=[0,19999999]，实际值=(此值-10000000)，单位=W。 采集时刻之前 15 分钟的平均有功功率。
2	uint16	A 相电压	合法值范围=[0,9999]，实际值=此值/10，单位=V。
2	uint16	B 相电压	(同上)
2	uint16	C 相电压	(同上)
4	uint32	A 相瞬时有功功率	合法值范围=[0,19999999]，实际值=(此值-10000000)，单位=W。
4	uint32	B 相瞬时有功功率	(同上)
4	uint32	C 相瞬时有功功率	(同上)

2.8 报文：定期采集数据包（表箱监测终端）

版本 0，结构如下：

长度 (字节)	数据类型	项目	描述
4	uint32	采集时刻	unixstamp 格式时间值
2	uint16	环境温度	合法值范围=[0,20000]，实际温度=(此值-10000)/100。例如值=12345，表示温度为 23.45 度
2	uint16	环境湿度	合法值范围=[0,10000]，实际湿度=此值/100。例如：5432，表示湿度=54.32
4	uint32	表箱组合有功电能	合法值范围=[0,199999999]，实际值=(此值-100000000)/100。
4	uint32	表箱短时平均功率	合法值范围=[0,19999999]，实际值=(此值-10000000)，单位=W。 采集时刻之前 15 分钟的平均有功功率。
2	uint16	表箱线损率	合法值范围=[0,20000]，实际值=(此值-10000)/10000。
2	uint16	A 相电压	合法值范围=[0,9999]，实际值=此值/10，单位=V。
2	uint16	B 相电压	(同上)
2	uint16	C 相电压	(同上)
4	uint32	A 相瞬时有功功率	合法值范围=[0,1999999]，实际值=(此值-1000000)/10，单位=W。
4	uint32	B 相瞬时有功功率	(同上)
4	uint32	C 相瞬时有功功率	(同上)
8	uint64	电表 0 通信地址	bit[63:56] = 电表 0 类型 =0 单相表 =1 三相表 只有 0 号和 3 号端口可以接三相表 bit[55:0] = 电表 0 通信地址 合法值范围=[0,999999999999] =0 表示表箱该端口为空，未连接电表
4	uint32	电表 0 短时平均功率	合法值范围=[0,19999999]，实际值=(此值-10000000)，单位=W。 采集时刻之前 15 分钟的平均有功功率。
2	uint16	电表 0 失准率	合法值范围=[0,20000]，实际值=(此值-10000)/10000。
2	uint16	电表 0 温度	合法值范围=[0,50000]，实际温度=(此值-10000)/100。例如值=12345，表示温度为 23.45 度
80	...	(电表 1-5)	(同上)

示例：

0xFF,0xFF,0xFF,0x5B,0x95,0x00,0x03,0x00,0x4E,0x61
0xBC,0x00,0x53,0x51,0x8B,0x60,0xE0,0x2E,0x88,0x13
0x40,0xC3,0xF7,0x05,0x3E,0xAC,0x98,0x00,0x04,0x29
0xCA,0x08,0x5C,0x08,0x10,0x09,0x74,0x72,0x0F,0x00
0xDA,0x9D,0x0F,0x00,0x40,0xC9,0x0F,0x00,0x00,0x00
0x00,0x00,0x40,0xE2,0x01,0x00,0x52,0x9B,0x98,0x00
0xD8,0x27,0x58,0x34,0x00,0x00,0x00,0x00,0x40,0xE2
0x01,0x00,0x52,0x9B,0x98,0x00,0xD8,0x27,0x58,0x34
0x00,0x00,0x00,0x00,0x40,0xE2,0x01,0x00,0x52,0x9B
0x98,0x00,0xD8,0x27,0x58,0x34,0x00,0x00,0x00,0x00
0x40,0xE2,0x01,0x00,0x52,0x9B,0x98,0x00,0xD8,0x27
0x58,0x34,0x00,0x00,0x00,0x00,0x40,0xE2,0x01,0x00
0x52,0x9B,0x98,0x00,0xD8,0x27,0x58,0x34,0x00,0x00
0x00,0x00,0x40,0xE2,0x01,0x00,0x52,0x9B,0x98,0x00
0xD8,0x27,0x58,0x34,0x00,0xFF,0xFF,0xFF,0x53,

解析：

长度 = 149

终端类型代码 = 3：表箱监测终端

报文类型代码 = 3：定期采集数据包

报文格式版本 = 0

终端通信地址 = 1024

报文：

采集时刻 = 2021-4-30 00:37:39

温度 = 20

湿度 = 50

表箱组合有功电能 = 1234.56

表箱短时平均功率 = 5566

A 相电压 = 225

B 相电压 = 214

C 相电压 = 232

A 相瞬时有功功率 = 1234

B 相瞬时有功功率 = 1234

C 相瞬时有功功率 = 1234

电表 0 类型 = 0 单相表

电表 0 通信地址 = 123456

电表 0 短时平均功率 = 1234

电表 0 失准率 = 0.02

电表 0 温度 = 34

(电表 1-5, 与电表 0 相同)

2.9 报文：设置心跳周期应答包（所有终端）

若出现格式错误、校验错误，终端将丢弃命令包，不返回任何应答。

参数版本 0，结构如下：

长度 (字节)	数据类型	项目	描述
1	uint8	设置结果	=0 成功 =1 失败，原因例如：参数错误
2	uint16	心跳周期	(同设置命令)

示例：

0xFF,0xFF,0xFF,0x5A,0x14,0x00,0x04,0x00,0x00,0x04
0x00,0x00,0x00,0x1E,0x00,0xE1,0xFF,0xFF,0xFF,0x53

解析：

长度 = 20

终端类型代码 = 0：台变监测终端

报文类型代码 = 4：设置心跳周期应答包

报文格式版本 = 0

终端通信地址 = 1024

报文：

设置结果 = 成功

心跳周期 = 30 s

2.10 报文：设置采集周期应答包（所有终端）

若出现格式错误、校验错误，终端将丢弃命令包，不返回任何应答。

参数版本 0，结构如下：

长度 (字节)	数据类型	项目	描述
1	uint8	设置结果	=0 成功 =1 失败，原因例如：参数错误
2	uint16	采集周期	(同设置命令)
2	uint16	上传延时	(同设置命令)

示例：

0xFF,0xFF,0xFF,0x5A,0x16,0x00,0x05,0x00,0x00,0x04
0x00,0x00,0x00,0xB4,0x00,0x80,0x0D,0xC9,0xFF,0xFF
0xFF,0x53,

解析：

收到数据包 No. 4

长度 = 22

终端类型代码 = 0：台变监测终端

报文类型代码 = 5：设置采集周期应答包

报文格式版本 = 0

终端通信地址 = 1024

报文：

设置结果 = 成功

采集周期 = 180 s

上传延时 = 3456 s

2.11 报文：设置通信信道应答包（所有终端）

若出现格式错误、校验错误，终端将丢弃命令包，不返回任何应答。

注意：终端在发送此应答包后，将自动重启，以便按新的通信信道与主站连接。

参数版本 0，结构如下：

长度 (字节)	数据类型	项目	描述
1	uint8	设置结果	=0 成功 =1 失败，原因例如：参数错误
4	uint32	主站 IP	(同设置命令)
2	uint16	主站端口号	(同设置命令)
4	uint32	备用 IP	(同设置命令)
2	uint16	备用端口号	(同设置命令)

示例：

0xFF,0xFF,0xFF,0x5A,0x1E,0x00,0x06,0x00,0x00,0x04
0x00,0x00,0x00,0xC0,0xA8,0x00,0x01,0x4C,0x27,0xC0
0xA8,0x00,0x02,0x4C,0x27,0x5D,0xFF,0xFF,0xFF,0x53

解析：

收到数据包 No. 5

长度 = 30

终端类型代码 = 0：台变监测终端

报文类型代码 = 6：设置通信信道应答包

报文格式版本 = 0

终端通信地址 = 1024

报文：

设置结果 = 成功

主站 IP = 192.168.0.1

主站端口号 = 10060

主站 IP = 192.168.0.2

备用端口号 = 10060

2.12 报文：电表召测应答包（表箱监测终端）

版本 0，结构如下：

长度 (字节)	数据类型	项目	描述
4	uint32	采集时刻	unixstamp 格式时间值
1	uint8	表箱端口号	= [0,5]
6	BCD 码	电表通信地址	此地址是表箱指定的端口所连接的电表的通信地址， =0 表示表箱该端口为空，未连接电表。
4	uint32	召测数据标识	例如：0x03300201。
1	uint8	召测数据长度	=0 无召测数据，可能的原因：不支持的数据标识、 未连接电表、或召测时出错。 =[1,220] 长度
1-220	uint8	召测数据	召测数据长度，可根据数据包长度来推算。

示例：

0xFF,0xFF,0xFF,0x5A,0x21,0x00,0x07,0x00,0x00,0x04
0x00,0x00,0xF1,0x02,0x00,0x00,0x05,0x79,0xDF,0x0D
0x86,0x48,0x70,0x78,0x56,0x34,0x12,0x00,0xAC,0xFF
0xFF,0xFF,0x53,

解析：

长度 = 33

终端类型代码 = 0：台变监测终端

报文类型代码 = 7：电表召测应答包

报文格式版本 = 0

终端通信地址 = 1024

报文：

采集时刻 = 1970-1-1 0:12:33

表箱端口号 = 5

电表通信地址 = 123456789012345

召测数据标识 = 0x12345678

召测数据长度 = 0

3、下行数据包

3.1 下行数据包结构

服务器向终端发送的数据包，结构如下：

长度 (字节)	数据类型	项目	描述
4	uint8	帧头	固定为：0xFF、0xFF、0xFF、0x5B
1	uint8	数据包长度	数据包的全部数据的长度，含帧头、CRC 校验码、帧尾。合法值=[18,33]
1	uint8	(保留)	(填 0)
1	uint8	报文类型	合法值如下： 0：状态查询命令包 1：时钟查询应答包 2：设置心跳周期命令包 3：设置采集周期命令包 4：设置通信信道命令包 5：电表召测命令包
1	uint8	报文格式版本	合法值范围=[0,250]，当前均为 0
4	uint32	终端通信地址	合法值范围=[1,999999999]，例如：123456789。 在终端外壳上印刷的终端地址，长度总是 9 位数字。 如果终端收到数据包后，发现通信地址不符，终端将不会应答。
1-16		报文内容	详见后文
1	uint8	CRC8 校验码	对本字节之前的所有字节（包括帧头），执行 CRC8 运算的结果，算法见前文。
4	uint8	帧尾	固定为：0xFF、0xFF、0xFF、0x53

3.2 报文：状态查询命令包（所有终端）

服务器可以通过此命令，来检查终端是否在线，或查询终端的当前参数。结构如下：

长度 (字节)	数据类型	项目	描述
1	uint8	查询的项目编号	当前版本总是=0

示例：

0xFF,0xFF,0xFF,0x5B,0x12,0x00,0x00,0x00,0x00,0x04
0x00,0x00,0x00,0x22,0xFF,0xFF,0xFF,0x53,

3.3 报文：时钟查询应答包（所有终端）

若服务器收到“时钟查询命令包”，则返回此应答。

长度 (字节)	数据类型	项目	描述
4	uint32	当前时刻	unixstamp 格式时间值

示例：

0xFF,0xFF,0xFF,0x5B,0x15,0x00,0x01,0x00,0x4E,0x61
0xBC,0x00,0xB6,0xED,0x8A,0x60,0x58,0xFF,0xFF,0xFF
0x53,

3.4 报文：设置心跳周期命令包（所有终端）

结构如下：

长度 (字节)	数据类型	项目	描述
2	uint16	心跳周期	合法值=[3,3600]，单位=秒。

示例：

0xFF,0xFF,0xFF,0x5B,0x13,0x00,0x02,0x00,0x00,0x04
0x00,0x00,0x1E,0x00,0x3F,0xFF,0xFF,0xFF,0x53,

3.5 报文：设置采集周期命令包（所有终端）

结构如下：

长度 (字节)	数据类型	项目	描述
2	uint16	采集周期	合法值=[3,3600]，单位=秒。 当前版本，实际只支持以下值：60、180、300。
2	uint16	上传延时	合法值=[0,30]，单位=秒。 终端在采集数据后，延时指定的时间，再上传数据包。

示例：

0xFF,0xFF,0xFF,0x5B,0x15,0x00,0x03,0x00,0x00,0x04
0x00,0x00,0x3C,0x00,0x80,0x0D,0x1A,0xFF,0xFF,0xFF
0x53,

3.6 报文：设置通信信道命令包（所有终端）

注意：终端在收到此命令包后，先发送应答包，然后自动重启，以便按新的通信信道与主站连接。主站在发送此命令时一定要确保参数正确，如果设置了错误的 IP 或端口号，终端将与主站失联。解决此问题的唯一办法是：通过 ISP 编程器来修改终端的通信信道参数。

结构如下：

长度 (字节)	数据类型	项目	描述
4	uint32	主站 IP	例如：IP=“255.1.2.3”则：值=0xFF010203 注意：IP 的左边的值保存到高字节
2	uint16	主站端口号	=[1024, 65535]
4	uint32	备用 IP	（同上）
2	uint16	备用端口号	（同上）

示例：

```
0xFF,0xFF,0xFF,0x5B,0x1D,0x00,0x04,0x00,0x00,0x04
0x00,0x00,0xC0,0xA8,0x00,0x01,0x4C,0x27,0xC0,0xA8
0x00,0x02,0x4C,0x27,0x80,0xFF,0xFF,0xFF,0x53,
```

3.7 报文：电表召测命令包（表箱监测终端）

只允许对表箱监测终端发送此命令。结构如下：

（在当前版本中，此命令未完全实现，终端可以对此命令正常应答，但给出的召测数据为空。）

长度 (字节)	数据类型	项目	描述
1	uint8	表箱端口号	=[0, 5]
3	uint8	保留	填充 0
4	uint32	召测数据标识	例如：0x03300201，表示 DI3=0x03、DI0=0x01。
8	uint8	保留	填充 0

示例：

```
0xFF,0xFF,0xFF,0x5B,0x21,0x00,0x05,0x00,0x00,0x04
0x00,0x00,0x05,0x00,0x00,0x00,0x60,0x00,0x00,0x00
0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x3A,0xFF
0xFF,0xFF,0x53,
```