MR7901 与平台的通信协议

V1.14

（2020.06.08）

山东瀚岳智能科技股份有限公司

目　录

1.目的

此文件主要介绍 MR79XX 产品(或其它类似设备)与平台服务器之间的通信格式与注意事项，为工程师完成 MR79XX(或其它类似设备)平台软件开发提供参考。

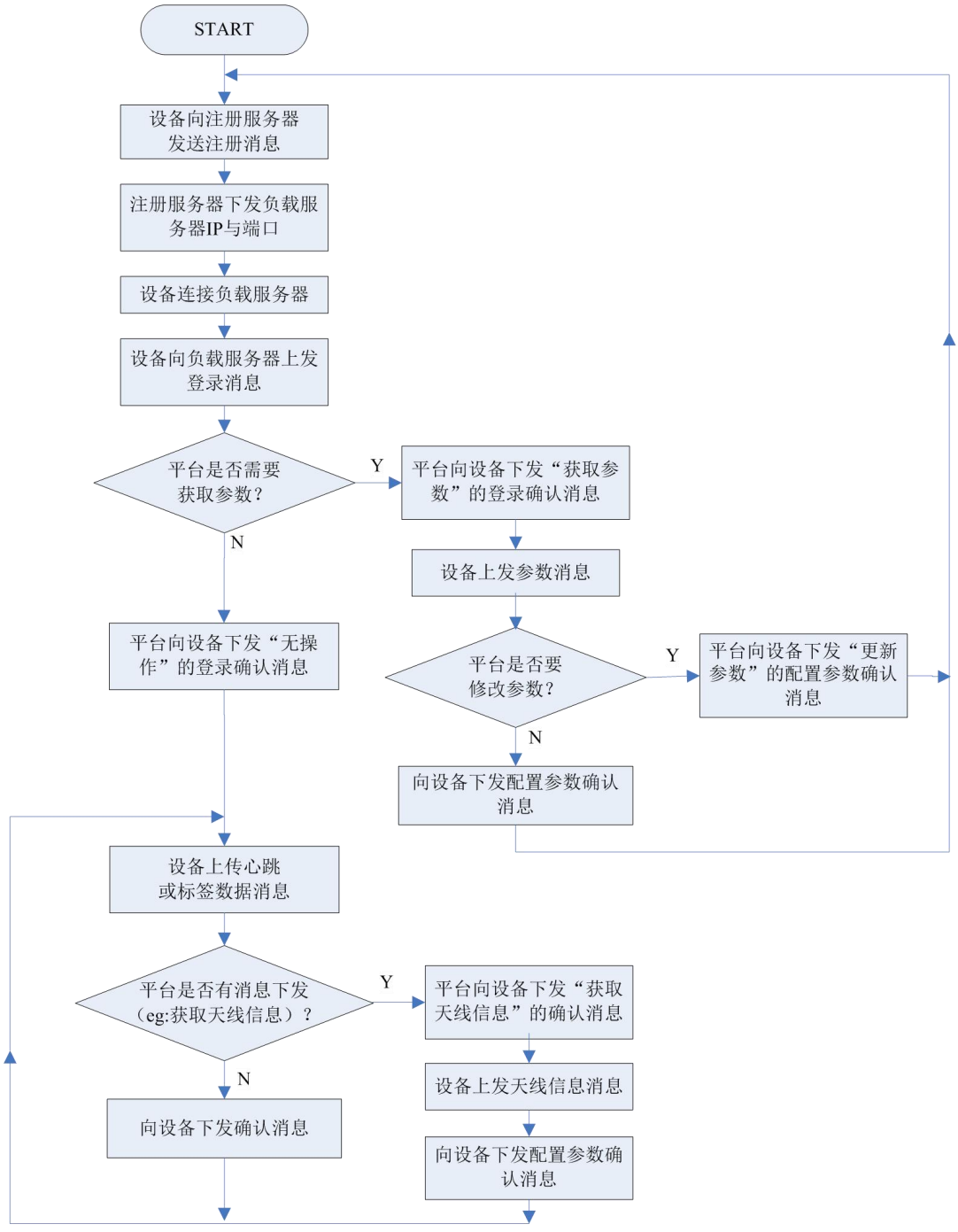
2.必要说明

1) MR79xx 与平台直接的通信方式有：GPRS、LAN 或其它方式；
2) 服务器：平台软件（这里包含“负载均衡服务器”与“负载服务器”）；
3) 终端/设备：MR79xx (或其它类似设备)；
4) 负载均衡服务器：注册服务器，接收从 MR79xx (或其它类似设备)发送过来的注册消息的服务器，并为设备分配连接的负载服务器，**小型系统可以省略**。
5) 负载服务器：接收从 MR79xx (或其它类似设备)发送过来的登录、心跳、数据、配置等消息的服务器。
6) 本协议基于 **TCP 数据包**，以下文件中的数据包格式均以**十六进制**描述。

3.通信流程

通信采用“客户端”—“服务器”模式进行通信，**平台侧为服务器，MR79xx为客户端**。通信是由客户端主动向服务器发起。

MR79xx上电后，需要向平台提交注册申请，设备注册成功后，才能登录平台。设备登录成功后，可以与平台之间进行数据交互。**数据交互采用一问一答的方式，由设备发起，平台应答**。下面是业务流程举例示意图：



通信流程举例

1. 没有负载均衡服务器的，在设备注册时，直接下发本服务器地址；
2. “参数”是指设备的工作参数，包括 IP 地址、数据过滤机制等；
3. 设备没有数据上传时，会以固定的时间间隔上报心跳数据包。

4.通信数据包格式

4.1 数据包格式

终端与平台之间的通信数据包是由“起始标识”、“报文头”、“报文体”和“校验”4个部分组成。其中，“起始标识”固定为0x55,0xAA。“校验”是报文头与报文体的CRC16校验，格式如下：

起始标识	报文头	报文体	校验
2 Bytes	28 Bytes	可变长度	2 Bytes

说明：

1. 起始标识：固定为 0x55,0xAA；
2. 报文头的长度固定为28Bytes；
3. 报文体的长度可变；
4. 校验是按照CRC16 CCITT标准-0x1021（初始值是0xFFFF），校验算法请看后面章节（第11章）介绍；
5. 校验计算从“报文头”开始，到“报文体”最后一个字节。

4.2 报文头

报文头是由报文长度、命令码、协议版本、终端系列号（或设备ID）等组成，报文头格式如下：

报文头（28 Bytes）			
序号	字段	长度（字节）	描述
1	报文总长度	2	含报文头与报文体的字节数（不含起始标识符与校验）
2	命令码	2	表示该报文所要执行或应答的命令，如登录、数据上报、更新等。
3	报文流水号	4	0x00000000到0xFFFFFFFF，发送方各自维护自己的流水号，每次成功的通信后，自动加1，到0xFFFFFFFF后，变为0x00000000。
4	报文协议版本	2	注： V2.0 （专用于MR7902）
5	报文安全标识	2	不加密的报文默认为0x0000
6	设备ID	16	16位ASCII码

字段说明：

- **命令码**：由 MR7901 向平台发送的命令码最高位为 0，而平台回应给 MR7901 是命令码是在该命令码的最高位置 1。如，设备向平台发起注册请求的命令码为 0x0008，而平台回应的命令码为 0x8008。
- **协议版本**：标识报文发送方使用的报文协议版本，接收方可根据该编号进行相应的处理或拒绝。

  协议版本用两个字节表示，高字节作为主版本号，低字节作为次版本号。版本号均

  为数字，例如 2.1 版本表示为 02 01。

  注： V2.0 （专用于 MR7902）

安全标识：用于在报文头中标识该终端及报文的相关安全信息，以及对上一报文的安全验证结果。一般不推荐使用，可向厂家索取更详细资料。

eg：55 AA 00 22 00 08 00 00 00 00 00 01 00 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 01 01 56 56 32 12 A7 5C

sof(H)	sof(L)	len(H)	len(L)	cmd(H)	cmd(L)	seq (MSB)		
55	AA	00	22	00	08	00	00	00
seq (LSB)	pro_ver (H)	pro_ver (L)	sec_flag (H)	sec_flag (L)	dev_id (MSB)			
00	00	01	00	00	38	36	31	36
39	34	30	33	34	32	33	35	38
		dev_id (LSB)	desc_code* (H)	desc_code* (L)	reg_code* (MSB)			reg_code* (LSB)
39	36	00	01	01	56	56	32	12
crc16(H)	crc16(L)							
A7	5C							

此报文头为： 00 22 00 08 00 00 00 00 00 01 00 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00

其中：

报文长度为 ： 0x0022
报文命令码为: 0x0008
报文流水号为: 0x00000000
报文版本为 ： 0.1
安全标识 ： 0x0000，即 本终端不加密

设备 id　　：　“861694034205896”

4.3 报文体

报文体，根据不同的命令码，所含的报文体是不同的，具体的格式请看后面（第7章）的命令说明。

5.数据交互

具体介绍不同命令的报文体格式。

注意：

设备向服务器发送的消息，服务器必须要有相应的回应，否则设备会重复发送相同的消息。

5.1 注册 （0x0008/ 0x8008）

5.1.1 命令帧定义

由设备向平台发起，命令码:0x0008，平台确认码：0x8008。

设备向服务器（负载均衡服务器）发送注册消息，服务器收到后，回应注册状态与负载服务器的IP与端口，设备收到消息后，按照新的IP与端口，重新建立连接。

注意：

如果设备注册不成功，会持续发送注册消息。

设备注册的报文体，包括2字节设备类型描述码和4字节注册码，注册码由设备ID经过固定算法运算而得。具体算法由系统单独定义。

命令码： 0x0008

报文体：如下表

数据段	字节数	描述
设备描述码	2	高字节为设备类型 **0x01** —— 数据网关 **0x02** —— RFID读头 **0x03** —— 计算机 低字节为设备型号编码， **0x01** —— MR7901 0x02 —— MR7901P **0x03 —— MR7902** **0x04** —— MR7901K（校园考勤） **0x05** —— HX402 **0x06** —— MR3202E (资产管理)

		0x07 —— HT101 **0x08** —— MR7901K-1（一体机电动车方向判断） **0x09** —— MR7901P-1（读取MR1054x标签） 0x10 —— HX102（测温考勤一体机） ...
注册码	4	

eg: 55 AA 00 22 00 08 00 00 00 01 00 01 80 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 01 02 78 56 34 12 7E 32

sof(H)	**sof(L)**	**len(H)**	**len(L)**	**cmd(H)**	**cmd(L)**	**seq (MSB)**		
55	AA	00	22	00	08	00	00	00
seq (LSB)	**pro_ver (H)**	**pro_ver (L)**	**sec_flag (H)**	**sec_flag (L)**	**dev_id (MSB)**			
01	00	01	80	00	38	36	31	36
39	34	30	33	34	32	33	35	38
		dev_id (LSB)	**desc_code (H)**	**desc_code (L)**	**reg_code (MSB)**			**reg_code (LSB)**
39	36	00	01	02	78	56	32	12
crc16(H)	**crc16(L)**							
7E	32							

起始标识

起始标识sof : 0x55AA

报文头

报文长度len : 0x0022

命令码 cmd : 0x0008

报文流水号seq : 0x00000001

协议版本pro_ver : 0x0001 (V0.1)

安全标识seq_flag : 0x8000 (本终端支持加密，没有开启加密（明文传输），本地存储为出厂秘钥)

设备ID dev_id : 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 (转为字符串为: “861694034205896”)

报文体

设备描述码desc_code : 01 02 （设备类型：01物联网网关，型号类型为：02即MR7901P）

注册码reg_code : 78 56 34 12

校验

crc16 : 0x7E32

5.1.2 平台确认包定义

平台确认报文体包括注册结果和平台当前实时时间，以及分配给设备登录的负载服务器IP与端口。

确认码： 0x8008

报文体：如下表

数据段	字节数	描述
注册结果	1	**0x00** —— 注册成功（如果是注册成功，返回负载服务器IP与端口） **0xFE** —— 注册码错误 **0xFF** —— 注册拒绝
实时时间	6	年月日时分秒，年基于2000（平台的当前实时时间）
负载服务器IP	32	字符串类型 eg： “218.17.157.214”
负载服务器端口	2	无符号整型 低字节在前，高字节在后

eg： 55 AA 00 45 80 08 00 00 00 01 00 01 80 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 00 12 0B 0D 09 1C 23 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 13 75 A6

sof(H)	sof(L)	len(H)	len(L)	cmd(H)	cmd(L)	seq (MSB)		
55	AA	00	45	80	08	00	00	00
seq (LSB)	**pro_ver (H)**	**pro_ver (L)**	**sec_flag (H)**	**sec_flag (L)**	**dev id(MSB)**			
01	00	01	80	00	38	36	31	36
39	34	30	33	34	32	33	35	38
		dev id(LSB)	**reg_status**	**time （MSB）**				
39	36	00	00	12	0B	0D	09	1C
time （LSB）	**IP(MSB)**	**...**	**IP(LSB)**	**port(L)**	**port(H)**	**crc16(H)**	**crc16(L)**	
23	32	...	00	24	13	75	A6	

起始标识

起始标识sof : 0x55AA

报文头

报文长度len : 0x0045
命令码 cmd : 0x8008
报文流水号seq : 0x00000001
协议版本pro_ver : 0x0001 (V0.1)
安全标识seq_flag : 0x8000 (无加密，明文传输)
设备ID dev_id : 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 (转为字符串为: “861694034205896”)

报文体

注册结果reg_status : 00 注册成功
时间 time : 12 0B 0D 09 1C 23 平台的当前时间，分别对应年、月、日、时、分、秒，起始时间是2000（2018年11月13日，09:28:35）
负载服务器IP : 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (“218.17.157.214”)
负载服务器端口port : 24 13 即0x1324 （十进制为4900）（注意： 低字节在前）

校验

crc16 : 0x75A6

5.2 登录 （0x0001/ 0x8001）

由设备向平台发起，命令码:0x0001，平台确认码：0x8001。

设备注册成功后，会向负载服务器发送登录消息，登录成功后，会向服务器（负载服务器）发送心跳或其它数据。

注意：

设备如果登录不成功（没有收到正确的回应），设备会重复发送10次登录请求消息（命令码0x0001），10次登录不成功后，会重新向负载均衡服务器（注册服务器），发送注册消息。

5.2.1 命令包定义

登录报文体包括设备的软件版本号和设备的配置参数列表的 CRC16 校验。

命令码： 0x0001

报文体： 如下表

数据段	字节数	描述
软件版本	2	主板本号和次版本号
配置参数的CRC16校验	2	配置参数列表的CRC16校验，服务器可据此判定是否需要更新参数（高字节在前）。

eg: 55 AA 00 20 00 01 00 00 00 00 02 01 80 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 01 05 02 69 E4 23

sof(H)	sof(L)	len(H)	len(L)	cmd(H)	cmd(L)	seq (MSB)		
55	AA	00	20	00	01	00	00	00
seq (LSB)	pro_ver (H)	pro_ver (L)	sec_flag (H)	sec_flag (L)	dev_id (MSB)			
02	00	01	80	00	38	36	31	36
39	34	30	33	34	32	33	35	38
		dev_id (MSL)	ver (H)	ver (L)	parm_crc 16(H)	parm_crc 16(L)	crc16 (H)	crc16 (L)
39	36	00	01	05	02	69	E4	23

起始标识

起始标识sof : 0x55AA

报文头

报文长度len : 0x0020
命令码 cmd : 0x0001
报文流水号seq : 0x00000002
协议版本pro_ver : 0x0001 (V0.1)
安全标识seq_flag : 0x8000 (本终端支持加密，没有开启加密（明文传输），本地存储为出厂秘钥)
设备ID dev_id : 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 (转为字符串为: “861694034205896”)

报文体

软件版本ver : 01 05 （设备软件版本V1.5）
配置参数crc16校验 : 02 69

校验

crc16 : 0xE423

5.2.2 平台确认包定义

平台确认报文体包括登录结果(1字节)和平台当前实时时间。

确认码： 0x8001

报文体：如下表

数据段	字节数	描述
登录结果	1	**0x00** —— 登录成功，无操作请求 **0x01** —— 登录成功，要求更新系统配置参数 **0x02** —— 登录成功，要求更新主机固件

		0x03 —— 登录成功，要求上传设备硬件信息 **0x10** —— 登录成功，要求更新用户配置参数 **0xFE** —— 登录错误 **0xFF** —— 登录拒绝（设备收到拒绝登录消息，3分钟后再次发送注册消息）
实时时间	6	年月日时分秒，年基于2000（平台当前的实时时间）

eg: 55 AA 00 23 80 01 00 00 00 02 00 01 80 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 00 12 0B 0D 09 1C 30 81 CB

sof(H)	**sof(L)**	**len(H)**	**len(L)**	**cmd(H)**	**cmd(L)**	**seq (MSB)**		
55	AA	00	23	80	01	00	00	00
seq (LSB)	**pro_ver (H)**	**pro_ver (L)**	**sec_flag (H)**	**sec_flag (L)**	**dev_id (MSB)**			
00	00	01	00	00	38	36	31	36
39	34	30	33	34	32	33	35	38
		dev_id (LSB)	**login_status**	**time（MSB）**				
39	36	00	00	12	0B	0D	09	1C
time（LSB）	**crc16 (H)**	**crc16 (L)**						
30	81	CB						

起始标识

起始标识sof : 0x55AA

报文头

报文长度len : 0x0023

命令码 cmd : 0x8001

报文流水号seq : 0x00000000

协议版本pro_ver : 0x0001 (V0.1)

安全标识seq_flag : 0x0000

设备ID dev_id : 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 (转为字符串为: “861694034205896”)

报文体

登录状态login_status : 00 （登录成功）

实时时间time : 12 0B 0D 09 1C 30 分别对应年、月、日、时、分、秒，起始时间是2000（2018年11月13日，09:28:48）

校验

crc16 : 0x81CB

需要设备升级的确认包

eg2: 55 AA 00 23 80 01 00 00 00 02 00 01 80 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 02 12 0B 0D 09 1C 30 E1 28

5.3 心跳 （0x0003/ 0x8003）

由设备向平台发起，命令码:0x0003，平台确认码：0x8003。

注意：

设备如果发送心跳消息后，没有收到平台正确回应消息，会重复发送5次心跳消息（命令码0x0003），5次后，会重新向负载服务发送登录消息（命令码0x0001）。

5.3.1 命令包定义

心跳报文体包括设备的工作状态（2字节）和设备当前状态。

命令码： 0x0003

报文体： 如下表

数据段	字节数	描述
设备工作状态	2	格式说明： **低 4 位，连接方式：** 第 0bit： GPRS 连接，1 有效 第 1bit： LAN(有线或网线)连接，1 有效 第 2bit： 保留 第 3bit： 保留 第 4bit： 标签传输标识，为 0：向平台传输标签记录；1：不向平台传输标签记录 第 5bit： 设备断电标识，为 0：设备正常供电，1：设备外部供电断开 第6～7bit：保留 第8～11bit：电池电压，0～10，分别代表还有0到100%的电量。（电量与电池电压对应关系参照第10章, MR7901P 不带电池，不支持此功能） 第12～15bit：保留 **eg：** 00 01 —— GPRS连接，上报标签数据 00 11 —— GPRS连接，不上报标签数据

		08 03 —— GPRS连接,有线连接，上报标签数据，电池电量80%
设备状态	2	第0～3bit： 数据包传输方式（只能一个bit有效） 第0bit ： 通过gprs发过来的数据包 第1bit ： 通过有线网络发过来的数据包 第2bit ： 保留 第3bit ： 保留 第 4～7bit: 保留 第8～15bit： gprs信号强度，正常范围：0～31,为99时，获取信号强度失败 eg: 11 01 —— 通过gprs传输此心跳包， gprs信号强度17
设备版本	2	
设备时间	6	年，月，日，时，分，秒（设备当前的实时时间）

eg: 55 AA 00 28 00 03 00 00 00 03 00 01 80 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 00 01 10 01 01 05 12 0B 0D 09 1C 31 6D EF

sof(H)	sof(L)	len(H)	len(L)	cmd(H)	cmd(L)	seq (MSB)		
55	AA	00	28	00	03	00	00	00
seq (LSB)	**pro_ver (H)**	**pro_ver (L)**	**sec_flag (H)**	**sec_flag (L)**	**dev_id (MSB)**			
03	00	01	80	00	38	36	31	36
39	34	30	33	34	32	33	35	38
		dev_id (LSB)	**work_state （H）**	**work_state （L）**	**dev_state （H）**	**dev_state （L）**	**time （MSB）**	
39	36	00	00	01	01	05	12	0B
			time （LSB）	**crc16 (H)**	**crc16 (L)**			
0D	09	1C	31	6D	EF			

起始标识

起始标识sof : 0x55AA

报文头

报文长度len : 0x0028

命令码 cmd : 0x0003

报文流水号seq : 0x00000003

协议版本pro_ver : 0x0001 (V0.1)
安全标识seq_flag : 0x8000 (本终端支持加密，没有开启加密（明文传输），本地存储为出厂秘钥)
设备ID dev_id : 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 (转为字符串为: “861694034205896”)

报文体

设备工作状态work_status : 00 01
gprs 连接
上传标签数据
外部供电正常
电池电量为0（MR7901P不带电池，不支持此功能）

设备状态 : 10 01
0x10 : gprs信号强度，即16；
0x01 : gprs传输

软件版本ver : 01 05 (设备软件版本V1.5)
设备时间time : 12 0B 0D 09 1C 31 分别对应年、月、日、时、分、秒，起始时间是2000（2018年11月13日，09:28:49）

校验

crc16 : 0x6DEF

5.3.2 平台确认包定义

平台确认报文体包括操作指示（1字节）和当前实时时间（6字节，年月日时分秒，年基于2000)。

确认码： 0x8003

报文体：如下表

数据段	字节数	描述
操作指示	1	**0x00** —— 没有操作指示 **0x01** —— 要求更新系统配置参数 **0x02** —— 要求更新主机固件 **0x03** —— 复位设备(设备收到后，不回应，直接重启) **0x04** —— 更新天线固件 **0x05** —— 获取天线信息(版本、增益、rssi门限) **0x06** —— 设置设备时间(设备收到后，设置时间，不回应) **0x07** —— 更新上报标签标识 **0x08** —— 清除缓存标签数据(设备收到后，清除缓存的标签数据，不回应) **0x09** —— 更新IP2 **0x0A** —— 要求更新加密传输标识（控制是否启用加密） **0x0B** —— 要求更新加密秘钥（必须启用加密后，设备才响应）

		0x10 —— 要求更新用户配置参数 **0x11** —— 获取设备状态 **0x12** —— 要求上传设备硬件信息 **0x20** —— 要求发送消息到标签 **0x21** —— 要求上传待发送的标签消息条数 **0x22** —— 要求清除待发送的标签消息
实时时间	6	年月日时分秒，年基于2000（平台当前实时时间）

eg: 55 AA 00 23 80 03 00 00 00 03 00 01 80 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 00 12 0B 0D 09 1C 31 07 F2

sof(H)	**sof(L)**	**len(H)**	**len(L)**	**cmd(H)**	**cmd(L)**	**seq (MSB)**		
55	AA	00	23	80	03	00	00	00
seq (LSB)	**pro_ver (H)**	**pro_ver (L)**	**sec_flag (H)**	**sec_flag (L)**	**dev_id (MSB)**			
03	00	01	80	00	38	36	31	36
39	34	30	33	34	32	33	35	38
		dev_id (LSB)	**ask**	**time （MSB）**				
39	36	00	00	12	0B	0D	09	1C
time （LSB）	**crc16 (H)**	**crc16 (L)**						
31	07	F2						

起始标识

起始标识sof : 0x55AA

报文头

报文长度len : 0x0023

命令码 cmd : 0x8003

报文流水号seq : 0x00000003

协议版本pro_ver : 0x0001 (V0.1)

安全标识seq_flag : 0x8000 （无加密，明文传输）

设备ID dev_id : 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 (转为字符串为: “861694034205896”)

报文体

操作指示ask : 00 无操作

平台实时时间time : 12 0B 0D 09 1C 31 分别对应年、月、日、时、分、秒，起始时间是2000（2018年11月13日，09:28:49）

校验

crc16 : 0x07F2

5.4 数据上报 （0x0004/ 0x8004）

由设备向平台发起，命令码:0x0004，平台确认码：0x8004。

注意：

设备如果发送数据消息，但没有收到平台正确回应消息，会重复发送5次数据消息（命令码0x0004），5次后，会重新向负载服务发送登录消息（命令码0x0001）。

5.4.1 命令包定义

数据上报报文体包括若干数据TLV。

命令码： 0x0004

报文体：如下表

数据段	字节数	描述
TLV	2+2+XX	标签类型（2Bytes），标签数据长度（2Btyes），标签数据（长度看第8章TLV索引） 由具体数据内容定义，具体格式请看第8章（TLV格式说明）
TLV	2+2+XX	
……		

TLV结构如下：

TLV类型(2字节)	LENGTH(2字节)	VALUE(长度由LENGTH定义）

eg： 55 AA 00 46 00 04 00 00 00 04 00 01 80 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 8B 01 00 11 01 20 78 2B 6A A4 2F 00 00 00 A9 12 0B 0D 09 1C 31 8B 01 00 11 01 20 EB 14 4A 33 64 00 00 00 B8 12 0B 0D 09 1C 31 81 4C

sof(H)	sof(L)	len(H)	len(L)	cmd(H)	cmd(L)	seq (MSB)		
55	AA	00	46	00	04	00	00	00
seq (LSB)	**pro_ver (H)**	**pro_ver (L)**	**sec_flag (H)**	**sec_flag (L)**	**dev_id (MSB)**			
04	00	01	80	00	38	36	31	36
39	34	30	33	34	32	33	35	38
		dev_id (LSB)	**TLV (MSB)**		**…**	**TLV (MSL)**	**crc16 (H)**	**crc16 (L)**
39	36	00	8B	01	…	31	83	3F

起始标识

起始标识sof : 0x55AA

报文头

报文长度len : 0x0046

命令码 cmd : 0x0004

报文流水号seq : 0x00000004

协议版本pro_ver : 0x0001 (V0.1)

安全标识seq_flag : 0x8000 (本终端支持加密，没有开启加密（明文传输），本地存储为出厂秘钥)

设备ID dev_id : 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 (转为字符串为: “861694034205896”)

报文体

TLV数据 : 8B 01 00 11 01 20 78 2B 6A A4 2F 00 00 00 A9 12 0B 0D 09 1C 31 8B 01 00 11 01 20 EB 14 4A 33 64 00 00 00 B8 12 0B 0D 09 1C 31 (有2条标签记录，具体格式请看后面的第8章标签说明)

其中第一条TLV为: 8B 01 00 11 01 20 78 2B 6A A4 2F 00 00 00 A9 12 0B 0D 09 1C 31 (解析如下：

TLV类型 ： 0x8B01 电子标签

TLV数据长度 ： 0x0011

TLV数据 ： 01 20 78 2B 6A A4 2F 00 00 00 A9 12 0B 0D 09 1C 31 格式参看8.2节标签数据格式说明)

校验

crc16 : 0x814C

5.4.2 平台确认包定义

确认码： 0x8004

报文体：与心跳包报文体相同。

5.5 配置参数 （0x000A/ 0x800A）

由设备向平台发起，命令码:0x000A，平台确认码：0x800A。

当平台需要获取或配置设备参数时，在登录包、心跳包、数据包的应答中填充的操作指示码。设备收到操作指示码后，向平台发送相应的参数信息。

5.5.1 命令包定义 0x000A

报文体包含参数类型与参数。

命令码： 0x000A

报文体：如下表

序号	数据段	字节数	描述
1	参数类型 parm_type	1	**0x10** —— 上报用户参数 0X80 —— 上报配置确认消息
2	参数	x	**第1个字节是0x10时：** 182Bytes，用户配置参数，具体格式说明请看第9章 配置参数格式说明 **第1个字节是0x80时：** 1 Bytes，1 配置参数成功， 0 配置参数失败

1. 上报用户参数 0x10

报文体：如下表

序号	数据段	字节数	描述
1	参数类型 parm_type	1	**0x10 —— 上报用户参数**
2	参数	182	具体格式，请参看第7章，配置参数说明

eg7: 55 AA 00 D3 00 0A 00 00 00 03 00 01 80 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 10 55 01 01 05 01 00 B4 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 00 00 01 C0 A8 01 C7 FF FF FF 00 C0 A8 01 01 64 00 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24 13 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F8 11 00 2E 12 3C 00 25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 02 00 02 00 FF FF 10 4D 52 37 39 30 31 50 2D 30 33 43 30 30 32 35 00 A8 A8 A8 A8 1F 1F 1F 1F 00 A1 00 05 00 00 16 9D

sof(H)	sof(L)	len(H)	len(L)	cmd(H)	cmd(L)	seq (MSB)		
55	AA	00	D3	00	0A	00	00	00
seq (LSB)	**pro_ver (H)**	**pro_ver (L)**	**sec_flag (H)**	**sec_flag (L)**	**dev_id (MSB)**			
03	00	01	80	00	38	36	31	36

39	34	30	33	34	32	33	35	38
		dev_id (LSB)	**parm_type**	**parm ...**	**crc16 (H)**	**crc16 (L)**		
39	36	00	10	...	16	9D		

起始标识

起始标识sof : 0x55AA

报文头

报文长度len : 0x00D3

命令码 cmd : 0x000A

报文流水号seq : 0x00000003

协议版本pro_ver : 0x0001 (V0.1)

安全标识seq_flag : 0x8000

设备ID dev_id : 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 (转为字符串为: "861694034205896")

报文体

参数类型**parm_type**

10 : 0. （**上传用户参数**），帧中第31个字节（从0开始计算）

parm : (具体格式说明请看第9章 配置参数格式说明)

55 : 1. 帧中第32个字节,参数特征值，读取配置参数时，固定为0x55

01 : 2. 帧中第33个字节,工作模式为：

1>. GPRS传输（低四位定义： 0x01: GPRS 0x02: LAN）

2>. 向平台传输标签记录

3>. 不加密（不加密报文体，采用明文传输）

01 05 : 3. 帧中第34个字节开始,固件版本V1.5(主版本号1,从版本5)

01 : 4. 帧中第36个字节，蜂鸣器标识，打开蜂鸣器（

0x00: 关闭，

0x01： 开启）

00 : 5. 帧中第37个字节，GPRS模块类型：0x00 : SIM800C

B4 00 : 6. 帧中第38个字节开始,标签去重过滤时间0x00B4,即180秒（低字节在前，高字节在后），是判断标签离开基站的判断时间

38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 : 7. 帧中第40个字节开始，设备ID," 861694034205896"

00 00 : 8. 帧中第56个字节开始,基站停留定时上报功能关闭（V3.3版）

01 : 9. 帧中第58个字节，DHCP使能 （0x00: 关闭， 0x01： 开启，适用于LAN）

C0 A8 01 C7 : 10. 帧中第59个字节开始，LAN本地IP，192.168.1.199

FF FF FF 00 : 11. 帧中第63个字节开始，LAN子网掩码 255.255.255.0

C0 A8 01 01 : 12. 帧中第67个字节开始，LAN网关192.168.1.1

64 00 : 13. 帧中第71个字节开始，LAN本地IP端口 0x0064，即100（低

	字节在前，高字节在后）
32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	: 14. 帧中第73个字节开始,GPRS服务器1的IP,“218.17.157.214”，平台IP（均衡服务器地址）
F8 11	: 15. 帧中第105个字节开始，GPRS服务器1的端口, 0x11F8即4600 （低字节在前，高字节在后），平台端口
32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	: 16. 帧中第107个字节开始,LAN 服务器1的IP, “218.17.157.214”,平台IP（均衡服务器地址）
F8 11	: 17. 帧中第139个字节开始,LAN服务器1的端口, 0x11F8,即4600（低字节在前，高字节在后）
00 2E 12 3C 00 25	: 18. 帧中第141个字节开始,LAN 本地 MAC 地址 00-2E-12-3C-00-25
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	: 19. 帧中第147个字节开始，保留1
02 00 02 00 02 00 FF FF	: 20. 帧中第175个字节开始，天线固件版本，分别对应1～4号天线的固件版本,每个天线版本占2个字节，为FF FF时，表示读取改天线版本失败。即1～4号天线固件版本为：V2.0, V2.0, V2.0,无（4号天线读取失败，可能是4号通道没有接天线）
10	: 21. 帧中第183个字节，GPRS信号强度0x10(16)
4D 52 37 39 30 31 50 2D 30 33 43 30 30 32 35 00	: 22. 帧中第184个字节开始，设备编号“MR7901P-03C0025”
A8 A8 A8 A8	: 23. 帧中第200个字节开始，天线1,2,3,4的rssi过滤门限，即分别是-88dBm, -88dBm, -88dBm, -88dBm
1F 1F 1F 1F	: 24. 帧中第204个字节开始,天线1,2,3,4的gain，即分别是31dBm, 31dBm,31dBm,31dBm
00	: 25. 帧中第208个字节，蓝牙输出标签标识，0x00不输出标签, 0x01输出标签
A1	: 26. 帧中第209个字节,通信连接状态,0xA1: 设备通过GPRS与平台已经建立通信连接（如果是0xA2：设备与平台通过LAN建立通信连接， 0xA3:设备与平台通过GPRS、LAN这两种通信连接）
00	: 27. 帧中第210个字节，标签过滤标识，0x00：不使用过滤
05	: 28. 帧中第211个字节，标签过滤间隔时间0x05，即5秒
00 00	: 29. 帧中第212个字节开始，保留2

校验

crc16	: 0x169D

2. 确认消息 0x80

当收到平台的配置消息，如配置系统参数、配置IP2、配置天线参数等消息后，设备会回应如下消息给平台，回应平台配置参数的结果。

注意：

设备回应此消息后，会立即重启，且按照配置正确的参数运行。

报文体：如下表

序号	数据段	字节数	描述
1	参数类型 parm_type	1	**0x80** —— **上报配置确认消息**
2	配置参数返回状态 return_opt	1	**0x01** —— 配置参数成功 **0x00** —— 配置参数失败

eg10: 55 AA 00 1E 00 0A 00 00 00 04 00 01 80 00 34 33 35 35 31 30 33 30 30 33 45 30 30 33 39 00 80 01 E7 69

sof(H)	sof(L)	len(H)	len(L)	cmd(H)	cmd(L)	seq (MSB)		
55	AA	00	1E	00	0A	00	00	00
seq (LSB)	**pro_ver (H)**	**pro_ver (L)**	**sec_flag (H)**	**sec_flag (L)**	**dev_id (MSB)**			
04	00	01	80	00	38	36	31	36
39	34	30	33	34	32	33	35	38
		dev_id (LSB)	**parm_type**	**return_opt**	**crc16 (H)**	**crc16 (L)**		
39	36	00	80	01	E7	69		

起始标识

起始标识sof : 0x55AA

报文头

报文长度len : 0x001E
命令码 cmd : 0x000A
报文流水号seq : 0x00000004
协议版本pro_ver : 0x0001 (V0.1)
安全标识seq_flag : 0x8000
设备ID dev_id : 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 （转为字符串为:“861694034205896”）

报文体

参数类型**parm_type** : 80 **上报配置确认消息**(用于回应设备平台已经收到配置参

数)

配置参数返回状态**return_opt** : 01 配置参数成功

校验

crc16 : 0xE769

5.5.2 平台确认包定义 0x800A

平台收到设备上发的配置参数的消息（命令码为0x000A）后，根据需要可下发配置系统参数、配置天线参数等配置消息。

报文体包含参数类型与参数。

确认码： 0x800A

报文体：如下表

序号	数据段	字节数	描述
1	类型	1	**0x10** —— 配置用户参数 0X80 —— 应答消息
2	参数	x	**第1个字节是0x10时：** 182Bytes，用户配置参数 **第1个字节是0x80时：** 1Byte, 1：平台收到配置参数成功； 0：

1. 配置用户参数 0x10

用于配置用户部分参数。

报文体：如下表

序号	数据段	字节数	描述
1	参数类型 parm_type	1	**0x10 —— 配置用户参数**
2	参数	182	具体格式，请参看第7章，配置参数说明

注意：设备收到正确的消息后，会重启。

eg5: 55 AA 00 D3 80 0A 00 00 00 03 00 01 80 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 10 55 01 01 05 01 01 3C 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 00 00 01 C0 A8 01 C7 FF FF FF 00 C0 A8 01 02 DC FF 32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 24 13 4D 54 49 49 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 23 6D 74 69 32 36 35 34 36 33 39 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 14 4D 52 37 39 30 31 50 2D 30 33 43 30 30 32 35 00 A8 A8 A8 A8 1F 1F 1F 1F 00 A1 00 05 00 00 AB B9

sof(H)	sof(L)	len(H)	len(L)	cmd(H)	cmd(L)	seq (MSB)		
55	AA	00	D3	80	0A	00	00	00
seq (LSB)	**pro_ver (H)**	**pro_ver (L)**	**sec_flag (H)**	**sec_flag (L)**	**dev_id (MSB)**			
03	00	01	80	00	38	36	31	36
39	34	30	33	34	32	33	35	38
		dev_id (LSB)	**parm_type**	**parm ...**	**crc16 (H)**	**crc16 (L)**		
39	36	00	10	...	AB	B9		

起始标识

起始标识sof : 0x55AA

报文头

报文长度len : 0x00D3
命令码 cmd : 0x800A
报文流水号seq : 0x00000003
协议版本pro_ver : 0x0001 (V0.1)
安全标识seq_flag : 0x8000
设备ID dev_id : 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 (转为字符串为: "861694034205896")

报文体

参数类型**parm_type**

00 : 0. (**设置用户参数**) 帧中第31个字节（从0开始计算）

parm : (具体格式说明请看第9章 配置参数格式说明)

55 : 1. 帧中第32个字节,参数特征值，读取配置参数时，固定为0x55
01 : 2. 帧中第33个字节,工作模式为：GPRS传输，且向平台传输标签记录（低四位定义： 0x01: GPRS 0x02: LAN）
01 05 : 3. 帧中第34个字节开始,固件版本V1.5(主版本号1,从版本5)
01 : 4. 帧中第36个字节，蜂鸣器标识，打开蜂鸣器（0x00: 关闭，0x01： 开启）
00 : 5. 帧中第37个字节，GPRS模块类型：0x00 : SIM800C
B4 00 : 6. 帧中第38个字节开始,标签去重过滤时间0x00B4,即180秒（低字节在前，高字节在后），是判断标签离开基站的判断时间
38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 : 7. 帧中第40个字节开始，设备ID," 861694034205896"

00 00 : 8. 帧中第56个字节开始,基站停留定时上报功能关闭（V3.3版）

01 : 9. 帧中第58个字节，DHCP使能 （0x00: 关闭， 0x01： 开启，适用于LAN）

C0 A8 01 C7 : 10. 帧中第59个字节开始，LAN本地IP，192.168.1.199

FF FF FF 00 : 11. 帧中第63个字节开始，LAN子网掩码 255.255.255.0

C0 A8 01 01 : 12. 帧中第67个字节开始，LAN网关192.168.1.1

64 00 : 13. 帧中第71个字节开始，LAN本地IP端口 0x0064，即100（低字节在前，高字节在后）

32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 14. 帧中第73个字节开始,GPRS服务器1的IP,“218.17.157.214”，平台IP（均衡服务器地址）

F8 11 : 15. 帧中第105个字节开始，GPRS服务器1的端口, 0x11F8即4600 （低字节在前，高字节在后），平台端口

32 31 38 2E 31 37 2E 31 35 37 2E 32 31 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 16. 帧中第107个字节开始,LAN 服务器1的IP,“218.17.157.214”,平台IP（均衡服务器地址）

F8 11 : 17. 帧中第139个字节开始，LAN服务器1的端口, 0x11F8,即4600（低字节在前，高字节在后）

00 2E 12 3C 00 25 : 18. 帧中第141个字节开始,LAN本地MAC地址00-2E-12-3C-00-25

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 : 19. 帧中第147个字节开始，保留1

02 00 02 00 02 00 FF FF : 20. 帧中第175个字节开始，天线固件版本，分别对应1～4号天线的固件版本,每个天线版本占2个字节，为FF FF时，表示读取改天线版本失败。即1～4号天线固件版本为：V2.0, V2.0, V2.0,无（4号天线读取失败，可能是4号通道没有接天线）

10 : 21. 帧中第183个字节，GPRS信号强度0x10(16)

4D 52 37 39 30 31 50 2D 30 33 43 30 30 32 35 00 : 22. 帧中第184个字节开始，设备编号“MR7901P-03C0025”

A8 A8 A8 A8 : 23. 帧中第200个字节开始，天线1,2,3,4的rssi过滤门限，即分别是-88dBm, -88dBm, -88dBm, -88dBm

1F 1F 1F 1F : 24. 帧中第204个字节开始,天线1,2,3,4的gain，即分别是31dBm, 31dBm,31dBm,31dBm

00 : 25. 帧中第208个字节，蓝牙输出标签标识，0x00不输出标签, 0x01输出标签

A1 : 26. 帧中第209个字节,通信连接状态,0xA1: 设备通过GPRS与平台已经建立通信连接（如果是0xA2： 设备与平台通过LAN建立通信连接， 0xA3:设备与平台通过GPRS、LAN这两

种通信连接）

00 ：27. 帧中第210个字节，标签过滤标识，0x00：不使用过滤

05 ：28. 帧中第211个字节，标签过滤间隔时间0x05，即5秒

00 00 ：29. 帧中第212个字节开始，保留2

校验

crc16 ：0xABB9

2. 平台确认消息 0x80

平台收到设备上发的配置参数消息，如上报系统参数、IP2参数、天线信息等。用于告知设备平台已经收到上报的配置消息。

报文体：如下表

序号	数据段	字节数	描述
1	参数类型 parm_type	1	**0x80 —— 下发平台确认消息**

eg6: 55 AA 00 1D 80 0A 00 00 00 04 00 01 80 00 38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 80 25 00

sof(H)	sof(L)	len(H)	len(L)	cmd(H)	cmd(L)	seq (MSB)		
55	AA	00	1D	80	0A	00	00	00
seq (LSB)	**pro_ver (H)**	**pro_ver (L)**	**sec_flag (H)**	**sec_flag (L)**	**dev_id (MSB)**			
04	00	01	80	00	38	36	31	36
39	34	30	33	34	32	33	35	38
		dev_id (LSB)	**parm_type**	**crc16 (H)**	**crc16 (L)**			
39	36	00	80	25	00			

起始标识

起始标识sof ：0x55AA

报文头

报文长度len ：0x001D

命令码 cmd ：0x800A

报文流水号seq ：0x00000004

协议版本pro_ver ：0x0001 (V0.1)

安全标识seq_flag ：0x8000

设备ID dev_id ：38 36 31 36 39 34 30 33 34 32 30 35 38 39 36 00 （转为字符串为:“861694034205896”）

报文体

参数类型**parm_type** ：80 **平台确认消息**（用于回应设备,告知设备平台已经收到配

置参数）

校验

crc16 : 0x2500

6.TLV 索引

6.1 TLV 类型列表与格式

6.1.1 格式

TLV类型(2字节)	LENGTH(2字节)	VALUE(长度由LENGTH定义）

6.1.2 类型索引

类型	TAG	LENGTH	VALUE
RFID物品监控	0x8801	17	天线Channel(1byte)+标签类型(1byte)+id(4bytes)+sum(1byte)+激励地址(2bytes)+标签状态（1Bytes）+rssi(1byte)+接收时间(6bytes)
电流标签监控	0x8901	16	1字节信号强度+4字节标签ID +5字节标签传感信息+6字节采集时间
健康手环数据	0x8A01	18	1字节信号强度+4字节手环ID+1字节类型+2字节数据+6字节采集时间+6字节接收时间
电子标签	0x8B01	17	天线Channel(1byte)+标签类型(1byte)+id(4bytes)+sum(1byte)+激励地址/携带信息(2bytes)+电压状态（1Bytes）+rssi(1byte) +接收时间(6bytes)
考勤标签	0x8B02	17	考勤/天线Channel(1byte)+标签类型(1byte)+id(4bytes)+sum(1byte)+激励地址/携带信息(2bytes)+电压状态（1Bytes）+rssi(1byte) +接收时间(6bytes)
MR1054X标签	0x8B03	23	天线Channel(1byte)+标签ID(15byte) +rssi(1byte) +接收时间(6bytes)

电子标签 eg1： 8B 01 00 11 01 20 78 2B 6A A4 2F 00 00 00 A9 11 01 0E 13 26 09

TLV类型(2字节)	LENGTH(2字节)	VALUE(长度由LENGTH定义）
8B 01	00 11	01 20 78 2B 6A A4 2F 00 00 00 A9 11 01 0E 13 26 09

解析如下：

TLV类型 : 0x8B01 电子标签
TLV数据长度 : 0x0011
TLV数据 : 01 20 78 2B 6A A4 2F 00 00 00 A9 12 0B 0D 09 1C 31（格式参看电子标签数据格式说明)

考勤标签 eg2： 8B 02 00 11 81 20 78 2B 6A A4 2F 00 00 00 A9 11 01 0E 13 26 09

TLV类型(2字节)	LENGTH(2字节)	VALUE(长度由LENGTH定义）
8B 02	00 11	81 20 78 2B 6A A4 2F 00 00 00 A9 11 01 0E 13 26 09

解析如下：
TLV类型 : 0x8B02 考勤标签
TLV数据长度 : 0x0011
TLV数据 : 81 20 78 2B 6A A4 2F 00 00 00 A9 11 01 0E 13 26 09 （格式参看考勤标签数据格式说明)

6.2 TLV--电子标签格式说明

电子标签（类型为 0x8B01）格式说明（共 17 个字节）。

6.2.1 2.4G 有源电子标签数据格式

1. 标签类型列表

这里主要是 2.4G 有源电子标签类（如学生卡，电动车标签等）的数据格式。

标签数据格式：

1	2	3	4	5	6	7	8	9
天线通道号 (1byte)	标签类型 (1byte)	标签 ID (4bytes)	ID 校验和 (1byte)	携带信息 (2bytes)	标签状态 (1byte)	RSSI (1byte)	接收时间 (6bytes)	说 明
	0x20			激 励地址				学生卡
	0x21			电流信息				电流标签 携带信息为电流，是无符号数，第一个字节为高字节; 单位: mA eg 0x23 0x22 -> 0x2322 -> 转为十进制为 8994mA
	0x30			激励地				电动车车卡

				址				
	0x31			激励地址				电动车钥匙卡（人卡）
	0x40			预留				自营学生卡
	0x42			温度信息				温度标签 携带信息为温度； 是无符号数，高字节在前，低字节在后； 实际温度需要除以 **100** **单位：度（℃）** **范围： 20～50℃（传感器异常时为 655.35）** eg: 0x0E 0x89 -> 0xE89 (3721) -> 37.21℃）
	0x50			激励地址				资产管理标签
	0x60			预留				**市民卡** 使用 IC 卡号（十进制）

2. 注意说明：

1. ID 校验和是 标签类型 + 标签 ID 这 4 个字节的校验和（计算方法看第 11.2 章）；
2. 天线通道号说明：

最高位（7bit） ：进出基站的状态；

低四位（0～3bit）：天线号，为 1,2,3,4 分别对应东、南、西、北这 4 个天线）

进出基站状态/天线 Channel			
7 bit	**6 bit**	**5,4 bit**	**3～0 bit**
进出基站状态： 1： 进基站读取范围 0： 出基站读取范围	基站停留标识： 1：基站停留 0：不是基站停留	保留	读取标签的天线通道号

eg: 0x01 ， 出基站读取范围，最后一次是从 1 号天线读到的

注意：

1>. 判断进出基站需要将 7bit， 6bit 同时考虑;

2>. 基站停留标识为 1 时，进出基站状态无效。

3. 标签状态说明：

标签状态字节格式说明								
类型	**7bit**	**6bit**	**5bit**	**防拆标志 4bit**	**3bit**	**2bit**	**1bit**	**低电压报警标志 0bit**

				1: 拆除报警 0: 正常				1: 低电压报警 0: 正常

3. 举例说明：

电动车/学生卡标签 eg1： 01 20 78 2B 6A A4 2F 00 00 00 A9 12 0B 0D 09 1C 31

天线通道号 (1byte)	标签类型 (1byte)	标签 ID (4bytes)	ID 校验和 (1byte)	携带信息 (2bytes)	标签状态 (1byte)	RSSI (1byte)	接收时间 (6bytes)
01	20	78 2B 6A A4	2F	00 00	00	A9	12 0B 0D 09 1C 31

说明：

01 ： 0x01 ， 出基站读取范围，最后一次是从 1 号天线读到的

20 ： 标签类型， 学生卡；

78 2B 6A A4 ： 标签 ID: 78 2B 6A A4 -> 0x782B6AA4 转为十进制为 2016111268

2F ： 20 78 2B 6A A4 校验和

00 00 ： 携带信息，激励地址, 0x0000:非有效激励

00 ： 标签状态，正常

A9 ： 信号强度，-87dBm（单字节有符号数）

12 0B 0D 09 1C 31 ：标签接收（读取）时间，分别是年、月、日、时、分、秒，年是基于 2000 开始，2018 年 11 月 13 日 09 :28 : 49

电流标签 eg2： 01 21 78 2B 6A A4 2E 23 22 00 A9 12 0B 0D 09 1C 31

天线通道号 (1byte)	标签类型 (1byte)	标签 ID (4bytes)	ID 校验和 (1byte)	携带信息 (2bytes)	标签状态 (1byte)	RSSI (1byte)	接收时间 (6bytes)
01	21	78 2B 6A A4	2E	23 22	00	A9	12 0B 0D 09 1C 31

说明：

01 ： 0x01 ， 出基站读取范围，最后一次是从 1 号天线读到的

21 ： 电流标签

78 2B 6A A4 ： 标签 ID: 78 2B 6A A4 -> 0x782B6AA4 转为十进制为 2016111268

2E ： 21 78 2B 6A A4 校验和

23 22 ： 携带信息，电流，0x2322，即 8994mA

00 ： 标签状态，正常

A9 ： 信号强度，-87dBm（单字节有符号数）

12 0B 0D 09 1C 31 ：标签接收（读取）时间，分别是年、月、日、时、分、秒，年是基于 2000 开始，2018 年 11 月 13 日 09 :28 : 49

温度标签 eg3： 84 42 78 2B 6A A4 0D 24 56 80 A9 12 0B 0D 09 1C 31

天线通道号 (1byte)	标签类型 (1byte)	标签 ID (4bytes)	ID 校验和 (1byte)	携带信息 (2bytes)	标签状态 (1byte)	RSSI (1byte)	接收时间 (6bytes)
84	42	78 2B 6A A4	0D	24 56	80	A9	12 0B 0D

							09 1C 31

说明：

84 ： 0x84 ， 进门

(此字节：进门为 0x84， 从 4 号天线读取到的)

42 ： 温度标签

78 2B 6A A4 ： 标签 ID: 78 2B 6A A4 -> 0x782B6AA4 转为十进制为 2016111268

0D ： 42 78 2B 6A A4 校验和

0E 24 ： 温度信息，即 0x0E24 转为十进制数为 3620，转换为温度为 36.2℃

80 ： 标签状态，电压正常， 进门

A9 ： 信号强度，-87dBm（单字节有符号数）

12 0B 0D 09 1C 31 ：标签接收（读取）时间，分别是年、月、日、时、分、秒，年是基于 2000 开始，2018 年 11 月 13 日 09 :28 : 49

标签状态字节格式说明							
类型	7bit	6bit	5bit	防拆标志 4bit	3bit	2bit	1bit	低电压报警标志 0bit
				1: 拆除报警 0: 正常				1: 低电压报警 0: 正常

牛耳温度标签 eg4： 84 52 78 2B 6A A4 FD 0E 89 80 A9 12 0B 0D 09 1C 31

天线通道号 (1byte)	标签类型 (1byte)	标签 ID (4bytes)	ID 校验和 (1byte)	携带信息 (2bytes)	标签状态 (1byte)	RSSI (1byte)	接收时间 (6bytes)
84	52	78 2B 6A A4	FD	0E 89	80	A9	12 0B 0D 09 1C 31

说明：

84 ： 0x84 ， 进门

(此字节：进门为 0x84， 从 4 号天线读取到的)

52 ： 牛耳温度标签

78 2B 6A A4 ： 标签 ID: 78 2B 6A A4 -> 0x782B6AA4 转为十进制为 2016111268

FD ： 52 78 2B 6A A4 校验和

0E 89 ： 温度信息，即 0x0E 89 转为十进制数为 37.21，转换为温度为 37.21℃

80 ： 标签状态，电压正常， 进门

A9 ： 信号强度，-87dBm（单字节有符号数）

12 0B 0D 09 1C 31 ：标签接收（读取）时间，分别是年、月、日、时、分、秒，年是基于 2000 开始，2018 年 11 月 13 日 09 :28 : 49

标签状态字节格式说明							
类型	7bit	6bit	5bit	防拆标志 4bit	3bit	2bit	1bit	低电压报警标志 0bit
				1: 拆除报警 0: 正常				1: 低电压报警 0: 正常

6.3 TLV--考勤标签格式说明

考勤标签（类型为 0x8B02）格式说明（共 17 个字节）。

6.3.1 2.4G 有源电子卡标签数据格式

这里主要是 2.4G 有源电子标签类（如自营学生卡，温度标签等）的数据格式。
标签数据格式：

1	2	3	4	5	6	7	8	9
天线通道号 (1byte)	标签类型 (1byte)	标签 ID (4bytes)	ID 校验和 (1byte)	携带信息 (2bytes)	标签状态 (1byte)	RSSI (1byte)	接收时间 (6bytes)	说　明
	0x40			保留				自营学生卡
	0x42			温度信息				温度标签 （携带信息为温度，高字节在前，低字节在后。实际温度需要除以 100 eg: 0x0E 0x24 -> 0xE24 (3620) -> 36.2℃）

注：

1. ID 校验和是 标签类型 + 标签 ID 这 4 个字节的校验和（计算方法看第 11.2 章）；
2. 天线通道号说明：

最高位（7bit） ：进出基站的状态；
低四位（0～3bit）：天线号，为 1,2,3,4 分别对应东、南、西、北这 4 个天线）

进出基站状态/天线 Channel			
7 bit	6 bit	5,4 bit	3～0 bit
进出考勤标识： 1： 进门 0： 出门	单边考勤标识： 1： 单边考勤 0： 不是单边考勤	保留	读取标签的天线通道号

eg: 0x01 ， 出基站读取范围，最后一次是从 1 号天线读到的

注意：

1. *判断进出考勤需要将 7bit， 6bit 同时考虑;*
2. *当单边考勤标识为 1 时，进出考勤标识无效。*

3. 标签状态说明：

标签状态字节格式说明								
类型	7bit	6bit	5bit	防拆标志 4bit	3bit	2bit	1bit	低电压报警标志 0bit
				1: 拆除报警				1: 低电压报警

				0: 正常				0: 正常

自营学生卡 eg 1: 81 40 78 2B 6A A4 0F 00 00 00 A9 11 01 0E 13 26 09

考勤 / 天线通道号 (1byte)	标签类型 (1byte)	标签 ID (4bytes)	ID 校验和 (1byte)	保留 (2bytes)	标签状态 (1byte)	RSSI (1byte)	考勤时间 (6bytes)
81	40	78 2B 6A A4	0F	00 00	00	A9	11 01 0E 13 26 09

81 : 即进门，从 1 号天线读到
40 : 标签类型，自营学生卡
78 2B 6A A4 : 标签 ID
0F : 40 78 2B 6A A4 校验和
00 00 : 保留
00 : 无电压报警 （低电压为 0x01，正常为 00）
A9 : 信号强度，-87dBm（单字节有符号数）
11 01 0E 13 26 09 : 考勤时间，分别是年、月、日、时、分、秒，年是基于 2000 开始，2017 年 1 月 14 日 19 : 38 : 09

温度标签 eg2 : 41 42 78 2B 6A A4 0D 0E 24 80 A9 12 0B 0D 09 1C 31

天线通道号 (1byte)	标签类型 (1byte)	标签 ID (4bytes)	ID 校验和 (1byte)	携带信息 (2bytes)	标签状态 (1byte)	RSSI (1byte)	接收时间 (6bytes)
41	42	78 2B 6A A4	0D	0E 24	80	A9	12 0B 0D 09 1C 31

说明：
82 : 0x41 ， 单边考勤，从 1 号天线读取到的
42 : 温度标签
78 2B 6A A4 : 标签 ID: 78 2B 6A A4 -> 0x782B6AA4 转为十进制为 2016111268
0D : 41 78 2B 6A A4 校验和
0E 24 : 温度信息，即 0x0E24 转为十进制数为 3620，转换为温度为 36.2℃
80 : 标签状态，电压正常， 进门
A9 : 信号强度，-87dBm（单字节有符号数）
12 0B 0D 09 1C 31 : 标签接收（读取）时间，分别是年、月、日、时、分、秒，年是基于 2000 开始，2018 年 11 月 13 日 09 :28 : 49

温度标签状态字节格式说明							
类型	7bit	6bit	5bit	防拆标志 4bit	3bit	2bit	1bit	低电压报警标志 0bit
	1: 进门 0: 出门			1: 拆除报警 0: 正常				1: 低电压报警 0: 正常

6.4 TLV--物品管理标签格式说明

物品管理标签（类型为 0x8801）格式说明（共 17 个字节）。

eg： 01 50 E3 AF 22 32 CA 00 00 00 B2 11 01 0E 13 26 09

天线通道号 (1byte)	标签类型 (1byte)	标签 ID (4bytes)	ID 校验和 (1byte)	激励地址 (2bytes)	标签状态 (1byte)	RSSI (1byte)	接收时间 (6bytes)
01	50	E3 AF 22 32	FA	00 00	00	B2	11 01 0E 13 26 09

说明：

01 ： **天线编号，在资产管理系统一般是一个天线，填 1.**

50 ： 标签类型， 为资产标签，不建议软件通过此标识来区分标签类型，应该通过上一级的 TAG(TLV 类型 0x8801)来区分；

E3 AF 22 32 ： 标签 ID

CA ： 50 E3 AF 22 32 校验和

00 00 ： 激励地址，非激励

00 ： 标签状态，正常

B2 ： 信号强度，-78dBm（单字节有符号数）

11 01 0E 13 26 09 ：标签接收（读取）时间，分别是年、月、日、时、分、秒，年是基于 2000 开始，2017 年 1 月 14 日 19 : 38 : 09

标签状态说明：

标签状态字节格式说明								
类型	7bit	6bit	5bit	防拆标志 4bit	3bit	2bit	1bit	低电压报警标志 0bit
				1: 拆除报警 0: 正常				1: 低电压报警 0: 正常

7.配置参数格式说明

以下为设备的配置参数格式说明。

说明：

R　　：只读

R/W　：可读写

序号	数据段	字节数	读写属性	类型	描述
1	参数特征值	1	R/W	数值	写入时，保持 0x55 不变，可正常配置参数， 写入时，非 0x55，即恢复出厂默认参数； 读取时，固定为 0x55
2	通信模式	1	R/W	数值	低 4 位，只读，传输方式： 第 1bit：只读，GPRS 连接，1 有效 第 2bit：只读，LAN 连接，1 有效 第 3bit：保留 第 4bit：保留 第 5bit：可读写，标签传输标识 0：向平台传输标签记录； 1：不向平台传输标签记录 第 6bit：可读写，加密标识 0：不加密，即报文体为明文； 1：加密，即报文体为密文 第 7～8bit：保留 eg：0x11,表示 GPRS 连接，不向平台传输标签记录。 eg: 0x01,标识 GPRS 连接，向平台传输标签记录
3	固件版本	2	R	数值	固件版本，主版本号在前 eg: 01 05，　V1.5
4	蜂鸣器标识	1	R/W	数值	1：开启蜂鸣器，0：关闭蜂鸣器
5	GPRS 模块类型	1	R	数值	0x00 : SIM800C, 0x01: SIM7600CE 0x02: EC20
6	去重窗口（离开基站判断时间）	2	R/W	数值	标签去重过滤窗口，单位：秒；　0x0000 时不过滤，低字节在前，高字节在后 取值范围：20～65535
7	设备 ID	16	R/W	字符串	15 位产品序号，为 ASCII，后 1 个字节填 0x00 eg:　“861694034205896”
8	基站停留超时时间	2	R/W	数值	标签停留在基站，按照此值间隔时间上报给平台低字节在前，高字节在后。

					单位：秒 取值范围：0，60～65535 0： 不使用此功能 60～65535： 超时时间
9	DHCP 使能	1	R/W	数值	1：打开， 0：关闭，适用于 LAN
10	LAN 本地 IP	4	R/W	数值	用于 LAN 网络参数配置
11	LAN 子网掩码	4	R/W	数值	用于 LAN 网络参数配置
12	LAN 网关	4	R/W	数值	用于 LAN 网络参数配置
13	LAN 本地端口	2	R/W	数值	本地 IP 端口，适用于 LAN，低字节在前，高字节在后 （取值范围 0～65536） eg: *24 13，即 0x1324(HEX) = 4900 (DEC)*
14	GPRS 服务器 1 的 IP	32	R/W	字符串	IP 或域名，字符串
15	GPRS 服务器 1 的端口	2	R/W	数值	低字节在前，高字节在后 （取值范围 0～65536）
16	LAN 服务器 1 的 IP	32	R/W	字符串	IP 或域名，字符串
17	LAN 服务器 1 的端口	2	R/W	数值	低字节在前，高字节在后 （取值范围 0～65536）
18	LAN 本地 mac 地址	6	R/W	数值	用于 LAN 网络参数配置
19	保留 1	28	-	-	-
20	天线版本	8	R	数值	分别对应 4 个天线的固件版本 每个天线的版本占 2 个字节 eg：02 00 即 V2.0，如果是 FF FF 表示读取天线版本失败（可能是没有连接天线）
21	GPRS 信号强度	1	R	数值	00 或 99 表示 GPRS 无信号 99 表示读取 gprs 信号失败 正常取值范围 0～31
22	设备编号	16	R	字符串	eg: “MR7901P-03C0025”
23	天线 RSSI 门限	4	R/W	带符号数值	取值范围:-1～-128 分别对应天线 1,2,3,4 的信号强度 RSSI 过滤门限值； eg: -88
24	天线 gain	4	R/W	数值	取值范围 0~31，分别对应天线 1,2,3,4 的信号增益值
25	蓝牙输出标签标识	1	R/W	数值	0：不能通过蓝牙输出标签 1：可以通过蓝牙输出标签，此时天线读取的标签，将只能通过蓝牙输出，gprs、lan 禁止输出标签

26	通信状态	1	R	数值	与平台直接的连接状态 低 4 位，连接方式 第 1bit：只读，GPRS 连接，1 有效 第 2bit：只读，LAN 连接，1 有效 第 3bit：保留 第 4bit：保留 高 4 位，固定为 A eg: 0xA0 无连接 0xA1 有 GPRS 连接 0xA2 有 LAN 连接 0xA3 有 GPRS ，LAN 连接
27	标签过滤标识	1	R/W	数值	1：使用过滤（即有方向判断过滤） 0：不使用过滤(上传一进,一出)
28	标签过滤间隔时间	1	R/W	数值	单位：秒
29	保留 2	2	-	-	

8.指令汇总

序号	命令码 cmd	描述
1	0x0008	终端注册请求
2	0x8008	平台确认终端注册
3	0x0001	终端登录请求
4	0x8001	平台确认终端登录
5	0x0003	终端发送心跳
6	0x8003	平台确认心跳
7	0x0004	终端发送标签数据
8	0x8004	平台确认收到标签
9	0x000D	升级固件
10	0x800D	平台确认升级固件
11	0x000A	上报配置参数
12	0x800A	平台确认配置参数
13	0x0009	请求标签消息
14	0x8009	平台回应标签标签消息

9.校验算法

9.1 CRC16 校验算法

与平台通信的数据包，采用 CRC16 校验。以下介绍两种校验算法，推荐使用方法 2，方法 2 采用查表方式，比方法 1 快 8 倍。

9.1.1 C 语言函数 方法 1

```
/*******************************************************************************
** Function name      :  crc16_ccitt
** Descriptions       :  循环冗余校验-16    （CCITT 标准-0x1021）
** input parameters   :  buf   要校验的数据
**                          len  校验数据的长
** output parameters :  无
** Returned value     :   校验值
*******************************************************************************/
uint16_t crc16_ccitt(uint8_t *buf, uint16_t len)
{
    uint16_t i, j;
    uint16_t crc_reg = 0xFFFF;
    uint16_t crc_val;

    for (i = 0; i < len; i++)
    {
        crc_val = buf[i] << 8;

        for (j = 0; j < 8; j++)
        {
            if (((int16_t)(crc_reg ^ crc_val)) < 0)
                crc_reg = (crc_reg << 1) ^ 0x1021;
            else
                crc_reg <<= 1;
            crc_val <<= 1;
        }
    }
```

```
    return crc_reg;
}
```

9.1.2 C 语言函数 方法 2：查表法

```
/*******************************************************************************
** Function name      :  CRC16
** Descriptions       :  循环冗余校验-16    （CCITT 标准-0x1021）
** input parameters   :  Data  要校验的数据
**                          Length 校验数据的长
** output parameters :  无
** Returned value     :   校验值
*******************************************************************************/
const uint16_t crc16_table[]=     //* CRC16 CCITT 标准-0x1021
{
    0x0000, 0x1021, 0x2042, 0x3063, 0x4084, 0x50a5, 0x60c6, 0x70e7,
    0x8108, 0x9129, 0xa14a, 0xb16b, 0xc18c, 0xd1ad, 0xe1ce, 0xf1ef,
    0x1231, 0x0210, 0x3273, 0x2252, 0x52b5, 0x4294, 0x72f7, 0x62d6,
    0x9339, 0x8318, 0xb37b, 0xa35a, 0xd3bd, 0xc39c, 0xf3ff, 0xe3de,
    0x2462, 0x3443, 0x0420, 0x1401, 0x64e6, 0x74c7, 0x44a4, 0x5485,
    0xa56a, 0xb54b, 0x8528, 0x9509, 0xe5ee, 0xf5cf, 0xc5ac, 0xd58d,
    0x3653, 0x2672, 0x1611, 0x0630, 0x76d7, 0x66f6, 0x5695, 0x46b4,
    0xb75b, 0xa77a, 0x9719, 0x8738, 0xf7df, 0xe7fe, 0xd79d, 0xc7bc,
    0x48c4, 0x58e5, 0x6886, 0x78a7, 0x0840, 0x1861, 0x2802, 0x3823,
    0xc9cc, 0xd9ed, 0xe98e, 0xf9af, 0x8948, 0x9969, 0xa90a, 0xb92b,
    0x5af5, 0x4ad4, 0x7ab7, 0x6a96, 0x1a71, 0x0a50, 0x3a33, 0x2a12,
    0xdbfd, 0xcbdc, 0xfbbf, 0xeb9e, 0x9b79, 0x8b58, 0xbb3b, 0xab1a,
    0x6ca6, 0x7c87, 0x4ce4, 0x5cc5, 0x2c22, 0x3c03, 0x0c60, 0x1c41,
    0xedae, 0xfd8f, 0xcdec, 0xddcd, 0xad2a, 0xbd0b, 0x8d68, 0x9d49,
    0x7e97, 0x6eb6, 0x5ed5, 0x4ef4, 0x3e13, 0x2e32, 0x1e51, 0x0e70,
    0xff9f, 0xefbe, 0xdfdd, 0xcffc, 0xbf1b, 0xaf3a, 0x9f59, 0x8f78,
    0x9188, 0x81a9, 0xb1ca, 0xa1eb, 0xd10c, 0xc12d, 0xf14e, 0xe16f,
    0x1080, 0x00a1, 0x30c2, 0x20e3, 0x5004, 0x4025, 0x7046, 0x6067,
    0x83b9, 0x9398, 0xa3fb, 0xb3da, 0xc33d, 0xd31c, 0xe37f, 0xf35e,
    0x02b1, 0x1290, 0x22f3, 0x32d2, 0x4235, 0x5214, 0x6277, 0x7256,
    0xb5ea, 0xa5cb, 0x95a8, 0x8589, 0xf56e, 0xe54f, 0xd52c, 0xc50d,
    0x34e2, 0x24c3, 0x14a0, 0x0481, 0x7466, 0x6447, 0x5424, 0x4405,
    0xa7db, 0xb7fa, 0x8799, 0x97b8, 0xe75f, 0xf77e, 0xc71d, 0xd73c,
```

```
    0x26d3, 0x36f2, 0x0691, 0x16b0, 0x6657, 0x7676, 0x4615, 0x5634,
    0xd94c, 0xc96d, 0xf90e, 0xe92f, 0x99c8, 0x89e9, 0xb98a, 0xa9ab,
    0x5844, 0x4865, 0x7806, 0x6827, 0x18c0, 0x08e1, 0x3882, 0x28a3,
    0xcb7d, 0xdb5c, 0xeb3f, 0xfb1e, 0x8bf9, 0x9bd8, 0xabbb, 0xbb9a,
    0x4a75, 0x5a54, 0x6a37, 0x7a16, 0x0af1, 0x1ad0, 0x2ab3, 0x3a92,
    0xfd2e, 0xed0f, 0xdd6c, 0xcd4d, 0xbdaa, 0xad8b, 0x9de8, 0x8dc9,
    0x7c26, 0x6c07, 0x5c64, 0x4c45, 0x3ca2, 0x2c83, 0x1ce0, 0x0cc1,
    0xef1f, 0xff3e, 0xcf5d, 0xdf7c, 0xaf9b, 0xbfba, 0x8fd9, 0x9ff8,
    0x6e17, 0x7e36, 0x4e55, 0x5e74, 0x2e93, 0x3eb2, 0x0ed1, 0x1ef0
};

uint16_t   CRC16(uint8_t   * Data,   uint16_t   Length)
{
    uint16_t   crc;
    uint8_t   da;

        crc = 0xFFFF;
        while(Length--!=0)
        {
            da=(uint8_t) (crc/256);
            crc <<= 8;
            crc ^= crc16_table[da^*Data];
            Data++;
        }

    return crc;
}
```

9.1.3 JAVA 方法

```
/**************************************************************************
 * CRC-CCITT 标准计算 JAVA
 *
 *
 *输入：需要加入校验的字节数组 data
 *
 *输出：返回 2 个字节的十六进制的校验码
 *************************************************************************/
private static String getCrc(byte[] data) {
    int crc = 0xFFFF;           //crc 计算初值
```

```
    for (int i = 0; i < data.length; i++) {
            crc = (data[i] << 8) ^ crc;
            for (int j = 0; j < 8; ++j) {
              if ((crc & 0x8000) != 0)
                    crc = (crc << 1) ^ 0x1021;
              else
                    crc <<= 1;
                }
           }
           return Integer.toHexString(crc & 0xFFFF).toUpperCase();
    }
```

9.2 和校验算法

标签数据中用到和校验。

9.2.1 C 语言计算函数

```
/*******************************************************************************
** Function name       :   CheckSum
** Descriptions        :   和校验
** input parameters    :   uBuff 要校验的数据
**                         uBuffLen 校验数据的长
** output parameters :   无
** Returned value      :    校验值
*******************************************************************************/
  uint8    CheckSum(uint8 *uBuff, uint16 uBuffLen)
  {
       uint16 i;
       uint8 uSum=0;

      for(i=0;i<uBuffLen;i++)
      {
            uSum = uSum + uBuff[i];
      }
      uSum = (~uSum) + 1;

      return uSum;
  }
```

9.2.2 JAVA 计算方法

```
/**********************************************************
 * 标签数据中的校验和 JAVA 算法
 *
 * @param sendbyte   需要计算校验和区间：1 个字节的标签 TYPE + 4 个字节的标签 ID
 *
 * @return           计算出的校验和
 *                     20 E3 AF 22 32 的校验和：FA(10 进制是 -6）
**********************************************************/
protected static byte sendRcvByteNum(byte[] sendbyte) {
        byte sum = 0;
        for (int i = 0; i < sendbyte.length; i++) {
            sum += sendbyte[i];
        }
        byte rebyte = (byte) (~sum + 1);
        System.out.println("校验位：" + rebyte);
        return rebyte;
    }

//计算出的校验和 20 E3 AF 22 32 的校验和：FA(10 进制是 -6）
public static void main(String[] args) {
        byte[] b = new byte[5];
        b[0] = 0x20;
        b[1] = (byte) 0xE3;
        b[2] = (byte) 0xAF;
        b[3] = 0x22;
        b[4] = 0x32;
        sendRcvByteNum(b);
    }
```

10. 附录

10.1 电池电量与电池电压对应关系

MR7901 上的电池电压与通过心跳消息中（或上传设备硬件信息中）电池电量的对应关系如下：

电池电量	电池实际电压（单位 V）
10	≥ 8.00
9	≥ 7.75, ＜8.00
8	≥ 7.50, ＜7.75
7	≥ 7.25, ＜7.50
6	≥ 7.00, ＜7.25
5	≥ 6.75, ＜7.00
4	≥ 6.50, ＜7.75
3	≥ 6.25, ＜6.50
2	≥ 6.00, ＜6.25
1	≥ 5.75, ＜6.00
0	＜5.75

说明：

1. 电池电压低于 5.75V，即电池电量低于 1 时，设备不能正常工作；
2. 当电池电量低于 9 时，可判断外部供电的电源断电了（或掉电了）。