

# 涂鸦串口通讯协议

协议生成时间：2021年01月25日 10:57

## 产品信息

产品名称：富奥星zigbee\_bootloader测试

产品ID：bttqbchl

产品功能：

dpID	功能名称	数据传输类型	数据类型	功能属性	备注
150	工厂操作	可下发可上报	enum	枚举范围：aa, bb, cc, dd, ee, f f, gg, hh	工厂操作菜单
151	计数器	只上报	value	数值范围：0-6 5535，间距：1，单位：次	自由计数器
152	故障上报	只上报	fault	标签：aa, bb, c c	
153	字串上报	只上报	string	最大长度：255	

## 通讯协议

### • 串口通讯约定

波特率：9600

数据位：8

奇偶校验：无

停止位：1

数据流控：无

MCU：控制板控制芯片，与涂鸦模块通过串口对接

低功耗唤醒机制：仅对于低功耗设备有效，强电设备不需要唤醒IO；PWM1用于模块唤醒MCU，PWM2用于MCU唤醒模块；默认高电平，低电平持续10ms以上有效；唤醒持续时长100ms，每次数据交互之前，都需要先通过IO唤醒，再发送数据；

超时机制：被动上报（同步应答）超时时间100ms，主动上报（异步应答）超时时间5s；

### • 帧格式说明

字段	长度(byte)	说明
帧头	2	固定为0x55aa
版本	1	升级拓展用
序列号	2	传输数据序列号（顺序递增）
命令字	1	具体帧类型
数据长度	2	大端

数据	xxxx	
校验和	1	从帧头开始按字节求和得出的结果对 256 求余

● 通讯协议-基础协议

1. 查询产品信息

- 1.1 product ID:对应涂鸦开发者平台 PID（产品标识），由涂鸦开发者平台生成，用于云端记录产品相关信息；
- 1.2 串口协议软件版本号格式定义:采用点分十进制形式，” x.x.x” ( $0 \leq x \leq 9$ )，x 为十进制数。
- 1.3 产品信息有product ID和串口协议软件版本号构成。

例：{“p”:”BDzkjuLY”, “v”:”2.0.0”}

p 表示产品 ID 为 BDzkjuLY， v 表示 mcu 版本为 2.0.0；

55	AA	02	00	00	01	00	1C	7B	22	70	22	3A	22	42	44		
帧头		版本号		序列号		命令字		数据长度		{	”	P	”	:	”	B	D
7A	6B	6A	75	4C	59	22	2C	22	76	22	3A	22	32	2E	30		
z	k	j	u	L	Y	”	,	”	v	”	:	”	2	.	0		
2E	30	22	7D	89													
.	0	”	}	检验位													

2. 报告模块网络状态

模块网络状态有三种：

- 0x00：设备为未入网状态；
- 0x01：设备为已入网状态；
- 0x02：设备网络状态异常；

- 2.1 设备未入网状态：第一次上电、或者入网失败、或者离网的情况下，设备状态为未入网状态；并将该状态下发至MCU。
- 2.2 设备为已入网状态：设备入网成功之后，状态为已；设备入网成功之后，状态为已；并将该状态下发至 MCU MCU。
- 2.3 当模块检测到MCU重启或MCU断线再上的过程，则主动下发模块网络状态至MCU。
- 2.4 当模块的网络状态发生变化，则主动下发模块网络状态至MCU。

3. 设备联网状态

设备联网状态有两种：

- 3.1 0x00：将模块软复位，清除堆栈数据，保存网络状态；
- 3.2 0x01：将模块配置为开始配网状态；

4. 命令下发和状态上报

针对该产品功能的命令下发和状态上报协议详见下方《通讯协议（产品功能部分）指令收发表》。

5. MCU工作状态上报条件

- 5.1 当模块网络状态发生改变时（未入网-》入网）：MCU接收到模块网络状态指令后，需要上报所有功能的状态（开关，模式等功能）；
- 5.2 被动上报：当MCU收到模块端下发的控制命令，执行相应动作后，mcu需要将新的状态上报给模块端；

5.3 主动上报：MCU状态发生变化（非app控制，比如控制板按键）时，mcu需要主动上报；

5.4 定时上报：如有定时功能，MCU需要每分钟上报倒计时剩余时间，以分钟为单位。

6. ZigBee模块产测

扫描指定信道的SSID，返回扫描结果和信号强度百分比，主要用于产品生产过程中的ZigBee RF功能测试；该项测试需要借助于涂鸦ZigBee产测Dongle；

7. MCU OTA升级

MCU升级需要在涂鸦开发者平台上传MCU升级固件，然后在APP上点击检查固件升级；

7.1 设备配网完成之后MCU将当前版本号主动推送给网关（网关也会主动读取）；

7.2 网关收到收到APP的推送之后，会通知MCU升级固件的信息（PID、版本号、固件大小、固件校验和等）；

7.3 MCU发起升级固件请求，包含固件pid、要升级的固件版本号、数据偏移量、数据大小（一帧数据请求最大为 50 个字节）等信息；

7.4 升级完成之后，MCU需要将升级的状态和新固件的版本号上报给模块端；

8. 获取本地时间（可选）

支持获取网络本地时间和UTC时间，结果返回8个字节，前4个字节为标准时间戳，后四个字节为本地时间戳，以秒为单位。

9. 通讯协议（基础协议）指令收发表

序列号根据实际数据填写

		帧头 版本	序列号	命令字	数据长度	数据	校验和
查询产品信息	模块发送	0x55aa 0x02	0xXXX X	0x01	0x0000	N/A	校验和
	MCU上报	0x55aa 0x02	0xXXX X	0x01	0x001c	格式: {"p": "BDzkjuLY", "v": "2.0.0"}	校验和
报告模块网络状态	模块发送	0x55aa 0x02	0xXXX X	0x02	0x0001	0x00:不在网; 0x01:在网	校验和
	MCU返回	0x55aa 0x02	0xXXX X	0x02	0x0000	N/A	校验和
配置ZigBee模块	MCU发送	0x55aa 0x02	0xXXX X	0x03	0x0001	0x00:reset模块; 0x01:重置并配网;	校验和
	模块返回	0x55aa 0x02	0xXXX X	0x03	0x0000	N/A	校验和
命令下发	模块发送	0x55aa 0x02	0xXXX X	0x04	0xXXXX	实际DP数据信息，参考协议指令收发表;	校验和
状态上报（被动）	MCU发送	0x55aa 0x02	0xXXX X	0x05	0xXXXX	实际DP数据信息，参考协议指令收发表;	校验和
	模块返回	0x55aa 0x02	0xXXX X	0x05	0x0001	0x01	校验和
状态上报（主动）	MCU发送	0x55aa 0x02	0xXXX X	0x06	0xXXXX	实际DP数据信息，参考协议指令收发表;	校验和
	模块返回	0x55aa 0x02	0xXXX X	0x06	0x0001	0x01	校验和
ZigBee功能产测（注：扫描指定信道的指定SSID）	MCU发送	0x55aa 0x02	0xXXX X	0x08	0x0001	00x0b	校验和
	模块返回	0x55aa 0x02	0xXXX X	0x08	0x0002	数据长度为2字节：Data[0]: 0x00失败, 0x01成功; 当Data[0]为0x01, 即成功时, Data[1]表示信号强度 (0-100, 0信号最差, 100信号最强) 当Data[0]为0x00, 即失败时, Data[1]为0x00 表示未扫描到指定的ssid, Data[1]为0x01表示模块未烧录授权key	校验和
MCU OTA版本	模块发送	0x55aa 0x02	0xXXX X	0x0B	0x0000	N/A	校验和

请求	MCU返回	0x55aa 0x02	0xXXX X	0x0B	0x0001	MCU 版本号	校验和
MCU OTA升级通知	模块发送	0x55aa 0x02	0xXXX X	0x0C	0x0011	data[0]-data[7]:pid; data[8]:版本号, 01.00.0001(bit)->1.0.1(十进制); data[9]-data[12]:固件大小; data[13]-data[16]:固件校验和, 从固件第一个字节按字节求和得出的结果对2 <sup>32</sup> 求余;	校验和
	MCU返回	0x55aa 0x02	0xXXX X	0x0C	0x0001	0x00:成功; 0x01:失败;	校验和
MCU OTA固件内容请求	MCU发送	0x55aa 0x02	0xXXX X	0x0D	0x000E	data[0]-data[7]:pid; data[8]:版本号, 01.00.0001(bit)->1.0.1(十进制); data[9]-data[12]:固件偏移量; data[13]:数据包长度(不超过 50 字节);	校验和
	模块返回	0x55aa 0x02	0xXXX X	0x0D	0x00 0xXX	data[0]: status, 0x00成功, 0x01失败; data[1]-data[8]:pid; data[9]:01.00.0001(bit)->1.0.1(十进制); data[10]-data[13]:固件偏移量; data[14]-data[0xXX]:固件内容;	校验和
MCU OTA固件升级结果上报	MCU发送	0x55aa 0x02	0xXXX X	0x0E	0x000A	data[0]: status, 0x00成功, 0x01失败; data[1]-data[8]:pid; data[9]:01.00.0001(bit)->1.0.1(十进制);	校验和
	模块返回	0x55aa 0x02	0xXXX X	0x0E	0x0001	0x00:成功; 0x01:失败;	校验和
获取本地时间(可选)	MCU上报	0x55aa 0x02	0xXXX X	0x24	0x0000	N/A	校验和
	模块发送	0x55aa 0x02	0xXXX X	0x24	0x0008	数据长度为8 字节: 前四个字节为标准时间戳, 后四个字节为本地时间戳	校验和

• 通讯协议-功能协议

通讯协议(产品功能部分)指令收发表

ID	功能名称		帧头版本	序列号	命令字	数据长度	dpID	数据类型	功能长度	功能指令	校验
150	工厂操作	模块发送	0x55aa 0x02	0xXXXX	0x04	0x00 0x05	0x96	0x04	0x00 0x01	aa:0x00 bb:0x01 cc:0x02 dd:0x03 ee:0x04 ff:0x05 gg:0x06 hh:0x07	校验和
		MCU上报	0x55aa 0x02	0xXXXX	0x05	0x00 0x05	0x96	0x04	0x00 0x01		校验和
151	计数器	MCU上报	0x55aa 0x02	0xXXXX	0x05	0x00 0x08	0x97	0x02	0x00 0x04	0x0-0xffff	校验和
152	故障上报	MCU上报	0x55aa 0x02	0xXXXX	0x05	0x00 0x05	0x98	0x05	0x00 0x01	bit0:aa bit1:bb bit2:cc	校验和
153	字串上报	MCU上报	0x55aa 0x02	0xXXXX	0x05	N	0x99	0x03	N	0x00-0xff	校验和