成都亿佰特电子科技有限公司
Chengdu Ebyte Electronic Technology Co.,Ltd.

E72 V1.0 用户手册
(ZigBee3.0 自组网模块)

目录

1.模块介绍

1.1 ZigBee 简介

ZigBee 技术是一种近距离、低复杂度、低功耗、低速率、低成本的双向无线通讯技术。

在 ZigBee 网络中存在三种逻辑设备类型：Coordinator(协调器)，Router(路由器)和 End-Device(终端设备)。ZigBee 网络由一个 Coordinator 以及多个 Router 和多个 End_Device 组成。

各类型设备功能如下：

（1）Coordinator(协调器)

协调器负责启动整个网络。它也是网络的第一个设备。协调器选择一个信道和一个网络 ID(也称之为 PAN ID，即 Personal Area Network ID)，随后启动整个网络。

协调器也可以用来协助建立网络中安全层和应用层的绑定(bindings)。

注意，协调器的角色主要涉及网络的启动和配置。一旦这些都完成后，协调器的工作就像一个路由器(或者消失 go away)。由于 ZigBee 网络本身的分布特性，因此接下来整个网络的操作就不在依赖协调器是否存在。

（2）Router(路由器)

路由器的功能主要是：允许其他设备加入网络，多跳路由和协助它自己的由电池供电的儿子终端设备的通讯。

通常，路由器希望是一直处于活动状态，因此它必须使用主电源供电。但是当使用树群这种网络模式时，允许路由间隔一定的周期操作一次，这样就可以使用电池给其供电。

（3）End-Device(终端设备)

终端设备没有特定的维持网络结构的责任，它可以睡眠或者唤醒，因此它可以是一个电池供电设备。

1.2 产品特点

序号	产品特点	特点描述
1	支持 ZigBee 3.0	组网管理模组支持 ZigBee 3.0 规范，具备强大的组网能力，以及互联互通能力。支持高达 200 个 ZigBee 3.0 设备组网，并支持涂鸦，飞利浦，麦乐克等第三方 ZigBee 设备组网。（**注意：本模块只能作为协调器和路由器设备**）
2	组网管理	模组工作在 ZigBee 协调器模式，支持其它 ZigBee 设备组网，并对所有组网节点进行设备管理。设备加入网络，退出网络，组网管理器都会有相应消息产生。
3	按需组网	组网管理器可以在需要设备接入时开放网络接入，不需要组网时可以关闭网络，或 180 秒后自动关闭网络。
4	网络自愈功能	节点丢失不影响组网管理器的正常运作，丢失的节点重新上电或移动回原空间位置可重新被组网管理器识别。 组网管理器掉电或关机，不影响已组网的设备正常运行。 组网管理器恢复出厂后再新建网络，如原网络中已有设备运行，旧网络与新网络的设备可共存于同一空间互不影响。
5	设备识别功能	检测所有已组网设备，识别设备类型（路由器，终端节点），识别设备支持的功能（普通数传模组，灯，开关），可扩展高级的 SE 认证功能（合法设备，非法设备）
6	并发通信	发送数据时，组网管理器可同时向多个目标发起不同的消息，异步并行等待目标返回。其中某个目标出现异常时不会影响其它目标的通讯。异常目标也会返回系统对应的消息并报告上位机。接收数据时可根据收到多个不同目标的消息，串口输出各个源设备的地址。
7	终端节点支持	组网管理器支持 48 个终端节点直连，并为其保存数据。

8	终端节点数据保留	组网管理器可为直连的休眠终端保存数据 7 秒，单个终端最多可保存 8 条数据，或者同时为 40 个终端保存至少 1 条数据，若超出，自动清除最先的数据！数据保存时间过后，数据堆自动清空并向上位机发出对应的提醒消息，用以判断休眠终端是否正常运行。
9	自动重发功能	在单播（点播）模式下可开启自动重传功能，设备发送到下一节点失败时自动重发，每条消息重发次数为 3 次，重传间隔时间 6 秒。在等待重传的间隙时间内可与其它节点通讯。
10	自动路由	模块支持网络路由功能。路由器和协调器承载网络数据路由功能，用户可进行多跳组网。
11	支持加密协议	模块采用 AES 128 位加密功能，能改对网络加密及防监听。不同的组网管理器使用不同的密钥，保证不同网络互不干扰。组网管理器恢复出厂后可重新创建密钥，一个组网管理器可以创建多个互不干扰的网络（无协调器网络）。
12	支持串口配置	模块内置串口指令，用户可通过出串口指令配置（查看）模块的参数及功能。
13	多类型数据通信	支持全网广播，组播及点播（单播）功能。
14	信道检测	信道检测可用于检测空间中已存在的其它 ZigBee 网络，可作为自动信道的选择条件。
15	自动优选信道	组网管理器创建网络时支持 11~26 等 16 个信道（2405~2480MHZ）的自动选择，可同时使能多个信道，并自动选择干扰最小的信道。
16	网络 PAN_ID 更改	网络 PAN_ID 可选择手动模式和自动模式，自动模式下组网管理器通过开关允许入网的窗口主动搜索入网节点，手动模式下入网节点和组网管理器设置相同 PANID 可实现指定组网。
17	高速串口波特率	组网管理器的串口波特率高达 230400，对多目标同时收发数据提供了足够的数据带宽。
18	实时监测设备入网	组网时，组网管理器可以实时获得入网设备的 MAC 地址，短地址，设备的全部端口信息（包括 Profile 和 cluster 支持信息），并可判断设备是第一次入网还是网络恢复。
19	入网设备地址管理	组网管理器可以在模块上查询已组网设备的 MAC 地址和短地址，最大支持 254 个设备的组网和查询。
20	设备信息与状态管理	侦测入网设备的状态，包括但不限于数传模组的波特率、透传模式、目标；灯具类设备的亮度、通断状态；传感器类设备的检测值，用电量等。
21	设置节点与节点直接通讯（Bind）	可设置任意入网节点将消息发给另一入网节点，采用 MAC 地址锁定方式即使目标设备掉线也不会解除锁定，同时还能查询各个入网节点的锁定目标
22	单指令多数据	利用 ZigBee 的传输特性，一条指令可以控制多个状态，极大利用了 ZigBee 250kbps 的传输效率
23	通信错误诊断	组网管理器发送任何无线消息失败时，都有状态反馈。包括点播模式未通信成功，广播模式下遭遇广播风暴，或者无线信道有干扰，以及无线传输速率跟不上应用下发速率，都会有错误消息返回。

1.3 支持产品系列

序号	产品型号	射频芯片	频率（Hz）	空速（bps）	功率（dBm）	天线形式
1	E72-2G4M20S1E	CC2652P	2.4G	250K	20	PCB

2. 功能及命令结构简介

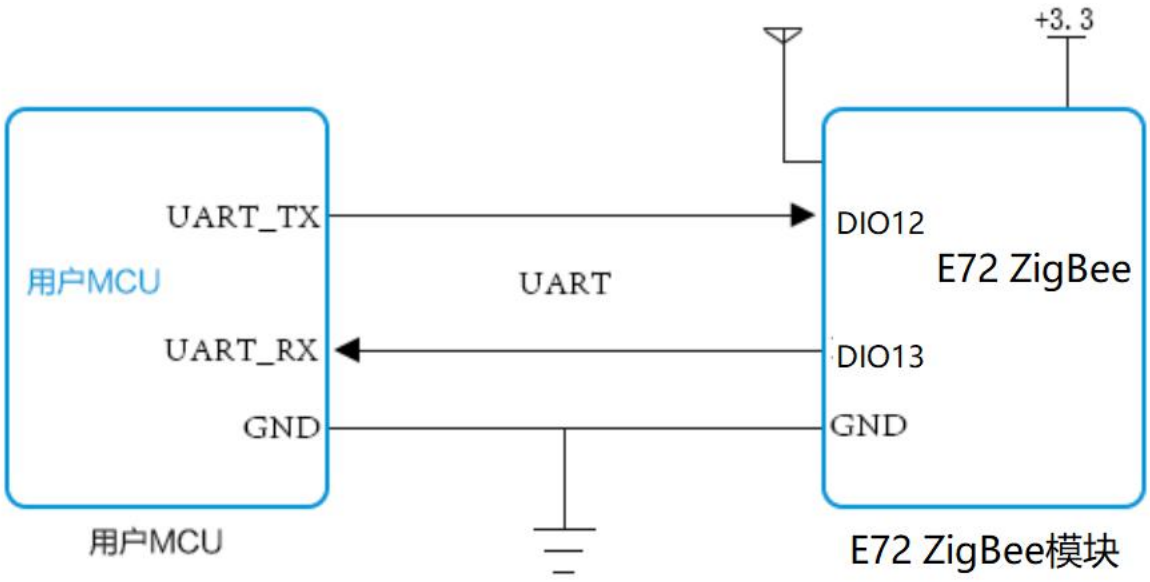
2.1 功能引脚表

组网管理器基于 E72-2G4M20S1E 模组，引脚封装参考硬件说明文档《E72-2G4M20S1E_User Manual_CN_v1.0》，组网管理器固件需要用到该模组以下 IO 口。

引脚	功能指示	描述（复用功能引脚只能规定为最后一次修改的功能）	输入/输出
DIO12	UART_RX	串口输入信号引脚	I
DIO13	UART_TX	串口输出信号引脚	O
DIO15	BOOTLOADER	进入 BootLoader 信号接口，低电平有效	I
DIO7	STATUS_LED	状态指示灯，低电平有效。长亮为待机状态，快速闪烁表示正在创建新网络或加入网络，1S 周期闪烁表示允许入网状态	O

2.2 引脚连接说明

2.2.1 串口连接说明



2.2.2 引脚位置说明

E72 ZigBee 组网模块采用 UART 串口通信方式，用户可通过任意带 UART 功能的 MCU 与其连接，进行数据交互， E72 DIO_12、DIO_13 为 E72 内部串口的 RX、TX 引脚，具体连接方式如上图所示。

3 串口命令格式与配置模式

3.1 串口指令格式

ZigBee 模组串口为全双工串口，因实际使用中存在大量数据交互，因此串口命令无论输入还是输出均采用命令帧的格式，并且具有保证命令帧完整的机制，上位机发送给模组的命令必须具备完整的帧结构。同时在实际 ZigBee 组网环境中，ZigBee 模组接收的消息是随机不可预测的，因此 ZigBee 模组的串口会有高概率的随机输出（TX）消息。

命令帧结构：

名称	帧头	帧长度	帧载荷
	SFD	LEN	payload
字节数	1	1	变长

帧头：以 0x55 作为命令开头

帧长度：帧长度即帧载荷长度，最大值 255。

帧载荷：帧载荷即串口帧的有效数据（含校验），当模组收到帧载荷字节数与帧长度相等，即接收完一帧完整的命令帧

命令模式：

ZigBee 模组有 3 种命令模式，分别是输入命令，反馈命令和异步命令。

输入命令：上位机向模组输入的命令帧，输入时为一个完整的命令帧。

反馈命令：模组收到输入命令后向上位机反馈的命令，每条输入命令都有反馈命令产生。原则上需要连续向模组输入一条命令后必须等待反馈命令，但模组本身对粘连的连续两帧命令进行容错，因此可能出现连续输入多条命令后连续反馈多条命令。反馈命令的等待时间即为模组内部 CPU 执行时间，最长可达 10 秒。

异步命令：模组随机发送给上位机的命令，该命令可能与输入命令有一定的因果关系，也有可能没有关系，更多的是不确定因素，因此异步命令可以当做一个随机事件来处理。

帧载荷结构与串口命令：

名称	帧载荷			
	Payload			
	命令类型	命令码	命令数据	校验码
	Cmd type	cmd code	Cmd data	check
字节数	1	1	0~252	1

命令类型：根据命令的模式和工作机制，进行分类。输入命令和反馈命令的命令类型从 0x00~0x7F，异步命令的范围是 0x80~0xFF。

命令码：执行命令的编码，1 字节。

命令数据：该命令执行的附带参数，最小 0 字节，最大 252 字节

校验码：校验码为 Payload 中不包含校验码自身部分的 XOR8 校验

帧载荷大小范围：由于每条命令都包含命令类型，命令码和校验码，因此帧载荷最小 4 字节，最大 255 字节。

3.2 命令类型

命令模式	命令类型	描述符	命令类型名称
输入命令/反馈命令	0x00	TYPE_CFG	本地配置命令
	0x01	TYPE_ZDO_REQ	网络管理命令
	0x02	TYPE_ZCL_SEND	设备状态与控制命令
异步命令	0x80	TYPE_NOTIFY	系统通知命令
	0x81	TYPE_ZDO_RSP	网络管理返回
	0x82	TYPE_ZCL_IND	接收设备状态与控制
	0x8F	TYPE_SEND_CNF	发送确认

输入命令与异步命令的因果关系：

异步命令 TYPE_NOTIFY 可能与输入命令 TYPE_CFG 存在因果关系

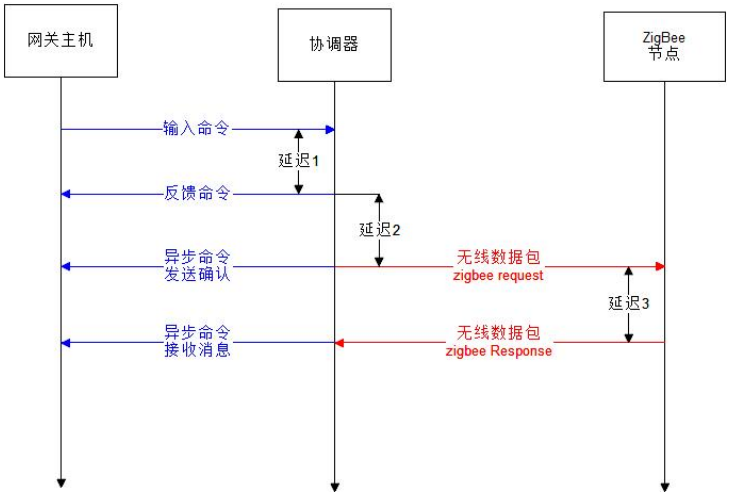
异步命令 TYPE_ZDO_RSP 一定是输入命令 TYPE_ZDO_REQ 导致，但 TYPE_ZDO_REQ 命令不一定产生 TYPE_ZDO_RSP

异步命令 TYPE_ZCL_IND 是收到设备发过来的消息，可能与输入命令 TYPE_ZCL_SEND 相关，也有可能无关。TYPE_ZCL_IND 中的参数 SeqNum 与 TYPE_ZCL_SEND 中的 SeqNum 相等，则说明该异步命令是由输入命令导致的。

每次有效的输入 TYPE_ZDO_REQ 命令或 TYPE_ZCL_SEND 命令都会产生 TYPE_SEND_CNF，因此 TYPE_SEND_CNF 可用于任务阻塞或缓存释放，在同时对多个目标发送特别有用。

输入命令 TYPE_ZDO_REQ 和 TYPE_ZCL_SEND 都是无线传输命令，无线传输本身具有有延迟，乱序的可能，结果就表现在与之对应的异步命令上。

远程命令流程图（网络管理命令，设备状态与控制命令）



3.3 命令码目录

本地配置命令：

命令码	描述符	命令名称
0x00	CFG_STATUS	查询模组当前状态
0x01	CFG_START	模组开机/软启动
0x02	CFG_OPEN_NET	打开网络/开始组网
0x03	CFG_CLOSE_NET	关闭网络/停止组网

0x04	CFG_RESET	复位/恢复出厂
0x05	CFG_NODE_TYPE	设置模组类型
0x06	CFG_CHANNEL	查询与设置信道
0x07	CFG_GET_PANID	查询 PANID
0x08	CFG_SET_PANID	设置 PANID
0x09	CFG_VIEW_GROUP	查看模组加组
0x0A	CFG_ADD_GROUP	模组加组
0x0B	CFG_REMOVE_GROUP	模组退组
0x0C	CFG_RF_SCAN	信道扫描测试
0x0D	CFG_TX_POWER	设置发射功率
0x20	CFG_GET_UTC	获取当前 UTC 时间
0x21	CFG_SET_UTC	设置 UTC 时间
0x22	CFG_GET_ADDRTABLE	读取本地地址表
0x28	CFG_EZ_MODE	重传设备通知消息

网络管理命令：

命令码	描述符	命令名称
0x00	ZDO_NWK_ADDR_REQ	查询节点短地址
0x01	ZDO_IEEE_ADDR_REQ	查询节点 IEEE 地址
0x02	ZDO_NODE_DESC_REQ	查询节点网络配置信息
0x04	ZDO_SIMPLE_DESC_REQ	查询节点端口信息
0x05	ZDO_ACTIVE_EP_REQ	查询节点端口数
0x21	ZDO_BIND_REQ	设置节点常连接绑定
0x22	ZDO_UNBIND_REQ	取消节点常连接绑定
0x33	ZDO_MGMT_BIND_REQ	查看节点常连接绑定
0x34	ZDO_MGMT_LEAVE_REQ	删除节点

设备状态与控制命令（ZCL）：

命令码	描述符	命令名称
0x00	ZCL_READ_ATTR_REQ	读取属性
0x01	ZCL_WRTIE_ATTR_REQ	修改属性
0x02	ZCL_READ_REPORT_REQ	查询属性上报规律
0x03	ZCL_WRITE_REPORT_REQ	修改属性上报规律
0x04	ZCL_DISC_ATTR_REQ	查看全部属性
0x05	ZCL_DISC_ATTR_EX_REQ	查看全部属性（带扩展）
0x0F	ZCL_CMD	发送控制命令

系统通知命令：

命令码	描述符	命令名称
0x00	NOTIFY_BOOT	设备启动
0x01	NOTIFY_NET_STATUS	网络状态变更
0x02	NOTIFY_NET_OPEN	打开关闭网络通知
0x03	NOTIFY_NODE_JOIN	检测到模组入网

0x04	NOTIFY_NODE_ADDR	模组短地址更新
0x05	NOTIFY_DEVICE_JOIN	设备入网信息
0x06	NOTIFY_LEAVE	模组离网通知
0x0C	NOTIFY_SCAN_INFO	扫描结果通知

网络管理返回：

命令码	描述符	命令名称
0x00	ZDO_NWK_ADDR_RSP	查询节点短地址
0x01	ZDO_IEEE_ADDR_RSP	查询节点 IEEE 地址
0x02	ZDO_NODE_DESC_RSP	查询节点网络配置信息
0x04	ZDO_SIMPLE_DESC_RSP	查询节点端点信息
0x05	ZDO_ACTIVE_EP_RSP	查询节点端点数
0x21	ZDO_BIND_RSP	设置节点常连接
0x22	ZDO_UNBIND_RSP	取消节点常连接
0x33	ZDO_MGMT_BIND_RSP	查看节点常连接
0x36	ZDO_MGMT_LEAVE_RSP	删除节点返回

接收设备状态与控制（ZCL）：

命令码	描述符	命令名称
0x00	ZCL_READ_ATTR_RSP	读取属性返回
0x01	ZCL_WRTIE_ATTR_RSP	修改属性返回
0x02	ZCL_READ_REPORT_RSP	查询属性上报规律返回
0x03	ZCL_WRITE_REPORT_RSP	修改属性上报规律返回
0x04	ZCL_DISC_ATTR_RSP	查看全部属性返回
0x05	ZCL_DISC_ATTR_EX_RSP	查看全部属性返回（带扩展）
0x0A	ZCL_REPORT_IND	属性主动上报
0x0B	ZCL_DEFAULT_RSP	系统默认返回帧
0x0F	ZCL_CMD_IND	接收控制命令

发送确认：

命令码	描述符	命令名称
0x01	ZDO_SEND_CNF	网络管理命令发送确认
0x02	ZCL_SEND_CNF	设备状态控制发送确认

3.4 AF Status 状态表

错误返回状态表：ACK 返回和通用命令反馈，专有命令反馈，均适合此表	
状态值	状态描述
0x00	操作成功
0x01	操作失败
0x02	参数错误
0x10	内存错误

0x11	内存满
0x12	模式不支持
0xc2	该命令无效
0xcd	目标设备不存在
0xb7	目标设备没收到消息（开启 APS ACK 才有）
0xe1	信道干扰
0xe9	没收到 MAC ACK
0xf0	设备休眠导致发送超时
0xf1	发送队列满了

3.5 ZDO 执行返回状态表

ZDO 状态表		
状态 ID	描述符	功能解释
0x00	ZDP_SUCCESS	操作成
0x80	ZDP_INVALID_REQTYPE	无效操作
0x81	ZDP_DEVICE_NOT_FOUND	设备未找到
0x82	ZDP_INVALID_EP	不正确的端点
0x83	ZDP_NOT_ACTIVE	端点不存在
0x84	ZDP_NOT_SUPPORTED	设备不支持该命令
0x85	ZDP_TIMEOUT	设备处理超时
0x86	ZDP_NO_MATCH	设备处理匹配失败
0x88	ZDP_NO_ENTRY	设备不存在该项信息
0x89	ZDP_NO_DESCRIPTOR	短地址不是当前设备的
0x8a	ZDP_INSUFFICIENT_SPACE	无存储空间
0x8b	ZDP_NOT_PERMITTED	当前状态不支持该操作
0x8c	ZDP_TABLE_FULL	表格存储已满
0x8d	ZDP_NOT_AUTHORIZED	操作未被认证通过
0x8e	ZDP_BINDING_TABLE_FULL	绑定表已满

3.6 ZCL 数据类型表

ZCL 属性数据类型表					
类别	数据类型	ID	字节数	无效值	Report 对齐
NULL	nodata	0x00	0		0
普通数据	data8	0x08	1		0
	data16	0x09	2		0
	data24	0x0a	3		0

	data32	0x0b	4		0
	data40	0x0c	5		0
	data48	0x0d	6		0
	data56	0x0e	7		0
	data64	0x0f	8		0
逻辑数据	bool	0x10	1	0xff	0
二进制位数据	bit8	0x18	1		0
	bit16	0x19	2		0
	bit24	0x1a	3		0
	bit32	0x1b	4		0
	bit40	0x1c	5		0
	bit48	0x1d	6		0
	bit56	0x1e	7		0
	bit64	0x1f	8		0
无符号整数	uint8	0x20	1		4
	uint16	0x21	2		4
	uint24	0x22	3		4
	uint32	0x23	4		4
	uint40	0x24	5		8
	uint48	0x25	6		8
	uint56	0x26	7		8
	uint64	0x27	8		8
有符号整数	int8	0x28	1		4
	int16	0x29	2		4
	int24	0x2a	3		4
	int32	0x2b	4		4
	int40	0x2c	5		8
	int48	0x2d	6		8
	int56	0x2e	7		8
	int64	0x2f	8		8
枚举	enum8	0x30	1	0xff	0
	enum16	0x31	2	0xffff	0
浮点	semi	0x38	2		4
	single	0x39	4		4
	double	0x3a	8		8
字符串	octstr	0x41	第一字节	头为 0xff	0

	string	0x42	第一字节	头为 0xff	0
	octstr16	0x43	第一双字节	头为 0xffff	0
	string16	0x44	第一双字节	头为 0xffff	0
序列型	uint8_array	0x48	2+内容长度总和	头为 0xffff	0
	struct	0x4C	2+内容长度总和	头为 0xffff	0
时间	ToD	0xe0	4	0xffffffff	4
	date	0xe1	4	0xffffffff	4
	UTC	0xe2	4	0xffffffff	4
标识符	clusterID	0xe8	2	0xffff	0
	attriID	0xe9	2	0xffff	0
	bacOID	0xea	4	0xffffffff	0
其它数据	EUI64	0xf0	8	0xffffffff	0
	key128	0xf1	16		0

3.7 ZCL 错误状态码

ZCL 状态表		
Value	描述	出现的情况
0x00	操作成功	全部命令
0x01	操作失败	全部命令
0x7E	该操作未授权	读写 Attribute 时
0x80	命令格式不正确	发送专有命令
0x81	不支持此 ZCL 专有命令	发送专有命令
0x82	不支持此 ZCL 通用命令	发送通用命令
0x83	不支持厂商定义 ZCL 专有命令	发送带厂商 ID 专有命令
0x84	不支持厂商定义 ZCL 通用命令	发送带厂商 ID 通用命令
0x85	无效字段	专有命令的参数错误
0x86	不支持的 Attribute	通用命令
0x87	错误的输入值	全部命令
0x88	Attribute 只读	写 Attribute 时
0x89	空间不足	专有命令（带存储功能）
0x8A	存在重复项	专有命令（带存储功能）

0x8B	没找到	专有命令（带存储功能）
0x8C	Attribute 不支持主动上报	配置主动上报或读配置
0x8D	数据类型无效	通用命令带数据类型
0x8E	选项无效	专有命令
0x8F	Attribute 只写	读 Attitude 时
0x90	启动状态不一致	
0x91	Out Of Band	
0x92	不一致错误	
0x93	拒绝此操作	
0x94	超时	
0x95	Abort	OTA 时
0x96	无效的 image 数据	OTA 时
0x97	等待数据	OTA 或其它大数据传输
0x98	没有 image 文件	OTA 时
0x99	需要更多的 image 数据	OTA 时
0xc0	硬件错误	
0xc1	软件错误	
0xc2	校准错误	

3.8 数传模组的 ZCL 结构

项目	值
Endpoint ID	1（预留 endpoint=2 给串口 2）
Profile ID	0x0104
Device ID	0x0500
In Cluster	0x0000 (Basic) 0x0003(Identify) 0xFC08(数据透传，manuCode=0x2000)
Out Cluster	0x0003 0xFC08(数据透传，manuCode=0x2000)

模块属性参数：

Cluster = 0xFC08，manucode = 0x2000				
属性 ID	描述符	名称	数据类型	操作
0x0000	Baud	波特率	uint32	R
0x0001	targetAddr	默认目标短地址	uint16	RW
0x0002	targetEP	默认目标端口	uint8	RW
0x0003	sendMode	透传模式	bool	RW
0x0004	LP Level	低功耗模式	Enum8	RW

ZCL 控制命令：

命令 ID	命令方向	描述符	功能
0x00	C2S	Send Data	数据发送
0x00	S2C	Data Notify	默认透传
0x01	C2S	Set Baud req	设置波特率
0x01	S2C	Set baud rsp	返回波特率

3.9 地址格式

3.9.1 IEEE 地址（MAC 地址）

ZigBee 节点的 IEEE 地址在出厂时就有，是一个 8 字节的地址，且具有全球唯一性。

3.9.2 短地址和 PANID

ZigBee 协调器创建网络时会生成一个 PANID，设备组网的本质就是获得了协调器相同的 PANID。同时 ZigBee 设备还会获得一个 16bit 的短地址，在 ZigBee mesh 网络中的数据传输需要使用短地址模式。

3.9.3 端口：

一个 ZigBee 设备上可以存在多个端口，相当于虚拟设备。例如常见的多孔插座，多路开关，一个设备上只用了 1 个 ZigBee 芯片，但是通过支持多个 endpoint 的方式实现了多个虚拟设备。端口号从 1~240 是引用层，0 号端口用于设备网络管理，242 号端口用于 green power 设备管理，255 号端口是用于广播

3.9.4 虚拟地址：

一个 ZigBee 设备组网后会有短地址，可以把短地址+端口作为访问控制虚拟设备的地址，虚拟地址是一个 24bit 的地址，由短地址+端口构成。另外如果协调器发送广播来控制设备，目标端口建议填 0xFF 即广播端口，这样可以使同一个设备上的多个虚拟设备，都收到广播控制。另外，组播发送的端口也为 0xFF。

3.9.5 虚拟设备 SN 号：

虚拟地址为亿佰特根据 ZCL 规范设备特性而制定的地址管理机制以方便 ZCL 规范的设备管理。根据每个 ZigBee 设备上 8 字节 IEEE 地址以及设备上各个功能和外设的端口号，组合而成的 9 字节（72bit）的虚拟设备序列号。格式为“端口号+IEEE 地址（8 字节小端模式）”。

在“常连接绑定”设置时，可通过设置源虚拟设备 SN 和目标虚拟设备 SN 号的方式设置绑定。由于该功能也可以指定源设备与分组进行绑定，因此 ZigBee 分组也可以当做一个虚拟设备来管理，并为其分配一个虚拟设备 SN 号， 其格式为“0xFF + 组 ID(低)+组 ID（高）+0xFFFFFFFFFFFF(6 字节）”。

设备虚拟 SN 号									
	端口号	IEEE[0]	IEEE[1]	IEEE[2]	IEEE[3]	IEEE[4]	IEEE[5]	IEEE[6]	IEEE[7]

具体设备	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX
分组	0xFF	0xXX	0xXX	0xFF	0xFF	0xFF	0xFF	0xFF	0xFF

- 虚拟 SN 的端口号为 0x01~0xF0，表示目标是一个真实存在的虚拟设备
- 虚拟 SN 号端口为 0xFF，表示目标是一个分组
- 目标是分组时，IEEE[0]和 IEEE[1]表示组 ID

3.9.6 组地址与组播：

ZigBee 的组播模式运行在 APS 层，即 ZigBee 组播是针对端口的组播。组地址是 16bit，范围 0~65535。使用组播时需要将设备的端口加入到指定分组中，且组播仅能在 ZCL 命令下进行控制。在组播应用中，一个多端口的设备，可以把不同端口分配到不同分组中。但如果要对一个设备上的多个端口进行同时控制，必须先把这些端口加入到同一个组中。例如 ZigBee 多孔插座，可以把不同的插孔添加到不同分组。

4. 用户指令集

4.1 本地配置命令

4.1.1 查询模组当前状态

命令码：0x00

功能：

该命令用于查询模组的状态和参数，包括模块的 MAC 地址，是否组网；信道，PANID，短地址是什么；密钥是什么；

输入命令：

名称	cmd data
	命令数据
	NULL
	空
字节数	0

反馈命令：

名称	cmd data							
	命令数据							
	Net status	DevType	IEEE Addr	Channel	PANID	ShortAddr	Ext PANID	NWK Key
	网络状态	设备类型	MAC 地址	信道	PANID	短地址	扩展 PANID	网络密钥
字节数	1	1	8	1	2	2	8	16

网络状态：0x00 – 已组网，0xFF – 未组网

设备类型：0x00 – 协调器，0x01 – 路由器，0x02-终端节点

MAC 地址：模组 MAC 地址，出厂就固定，全球唯一

信道：模组当前信道，未组网时没有

PANID：模组当前 PANID，未组网时没有

短地址：模组当前短地址，未组网时没有

扩展 PANID：未组网时没有

网络密钥：未组网时没有 0

命令示例：（紫色：负载长度　红色：命令类型+命令码　蓝色：校验码）

发送指令：55 03 00 00 00

接收指令：

未组网：55 0D 00 00 FF(组网状态) 00(设备类型) 28 EA E2 1A 00 4B 12 00(MAC 地址) 9C

已组网：55 2A 00 00 00(组网状态) 00(设备类型) 28 EA E2 1A 00 4B 12 00(MAC 地址) 19(信道) 93 61PANID 00 00 短地址 28 EA E2 1A 00 4B 12 00(扩展 PANID) C6 CD 93 B5 2F 37 9E F6 E9 A6 CE 3A 15 33 CF 55(网络密钥) B1

4.1.2 模组开机/软启动

命令码：0x01

功能：

模组上电后处于待机状态，无论之前是否组过网。待机状态不会发出异步命令，防止上位机也在上电启动过程中收到大量数据。

输入命令：

名称	cmd data
	命令数据
	AutoStart
	自动启动
字节数	1

自动启动：设为 1 下次上电后自动启动，设置为 0 关闭自动启动。

反馈命令：

名称	cmd data
	命令数据
	Status
	状态
字节数	0

状态：0 – 启动成功 2-已经启动过了 0xFF – 启动无效

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送指令：55 04 00 0101(自动启动) 00

接收指令

启动成功：55 04 00 0100(Status) 01

该返回命令后面会跟随一条“网络状态变更”的异步反馈命令：55 29 80 系统通知 01 网络状态变更 00 未组网 1A 1F 79 25 00 4B 12 00 00 MAC 地址 FE FF FE FF 9A CD E6 F3 79 3C 1E 8F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 **17**

已启动过了：55 04 00 01 02 03

4.1.3 打开网络/开始组网

命令码：0x02

功能：

协调器打开网络允许设备加网（出厂协调器会创建新网络），路由和终端节点则加入网络。协调器创建网络，以及路由和终端节点入网会有时延，最终结果在“系统通知命令”的“网络状态变更”中获取。路由在入网后再执行该命令，可以延长协调器打开网络的时间。

输入命令：

名称	cmd data
	命令数据
	NULL
	空
字节数	1

反馈命令：

名称	cmd data
	命令数据
	Status
	状态
字节数	1

状态：0x00 – 操作有效，0xFF– 操作无效。该命令需在软启动后才有效

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送指令：55 03 00 02 02

接收指令解析：

反馈命令：55 04 00 02 00(成功) 02

异步通知 1：55 04 80(系统通知) 02(打开网络通知) B4(网络窗口时间) 36　**(0xB4=180 秒加网窗口)**

异步通知 2：55 29 80(系统通知) 01(网络状态) 02(网络打开) 1A 1F 79 25 00 4B 12 00(MAC 地址) 0E(信道) A7 CE(PAN_ID) 00 00(短地址) 9A CD E6 F3 79 3C 1E 8F(扩展 PANID) 86 BC 4D CE 83 8A 56 21 38 A8 78 8A 1D 59 8D EE(网络密钥) F0

等待 180 秒后会收到关闭网络的系统通知

55 04 80(系统通知) 02(打开网络通知) 00(网络窗口关闭) 82

注意：协调器新建网络时，E72 模组的 DIO7 接上 LED 灯会快速闪烁；允许组网的时间内，LED 会以 1S 为周期持续闪烁直到网络自动或手动关闭。

4.1.4 关闭网络/停止组网

命令码：0x03

功能：

关闭组网允许，路由和终端节点上操作该命令可能会导致后续设备无法入网。

输入命令：

名称	cmd data
	命令数据
	NULL
	空
字节数	0

反馈命令：

名称	cmd data
	命令数据
	Status
	状态
字节数	0

状态：0 – 操作有效，0xFF – 操作无效

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送指令：55 03 00 03 03

接收指令解析：

已组网收到如下

收到反馈指令：55 04 00 03 00(成功) 03

收到异步指令：55 04 80(系统通知) 02(打开网络通知) 00(网络窗口关闭) 82

未组网收到如下

收到反馈指令：55 04 00 03 C2(无效) C1

收到异步指令：55 04 80(系统通知) 02(打开网络通知) 00(网络窗口关闭) 82

4.1.5 恢复出厂设置

命令码：0x04

功能：

模组复位，退网或恢复出厂设置。恢复出厂时，模组设置的参数全部恢复成默认值

输入命令：

名称	cmd data		
	命令数据		
	mode	PANID	Channel
	复位模式	Pan ID	信道
字节数	1	2	1

复位模式：0x00 - 复位； 0x01- 退网； 0x02 – 恢复出厂

PANID：模组当前的 PANID，复位时填入 0xFFFF 即可，需要退网或在已组网时需要恢复出厂，要填入模组当前 PANID。

信道：模组当前信道，复位时填入 0，需要退网或在已组网时需要恢复出厂，要填入模组当前信道。

反馈命令：

名称	cmd data
	命令数据
	Status
	状态
字节数	0

状态：0x00 – 操作有效，0xFF – 操作无效。

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

复位模式

发送指令：55 07 00 04 00(复位模式) FF FF(PAN_ID) FF(信道) FB

收到反馈指令: 55 04 00 04 00(成功) 04

收到异步指令：55 0D 80 00(启动通知) 06(复位模式) 1C(软件版本) 1A 1F 79 25 00 4B 12 00(MAC 地址) 9A

退网模式

发送指令: 55 07 00 04 01(退网模式) F5 8A(PANID) 0B(信道) 71

收到反馈指令：55 04 00 04 00(操作成功) 04

收发异步指令：55 0D 80 00(启动通知) 06(看门狗复位) 1C(软件版本) 1A 1F 79 25 00 4B 12 00 (MAC 地址) 9A

恢复出厂

发送指令: 55 07 00 04 02(恢复出厂模式) 93 86(PANID) 0B(信道) 18

反馈指令: 55 04 00 04 00(成功) 04

间隔几秒陆续收到两个 00 是协调器正在清除 FLASH 中的全部组网与设置记录

收发异步指令：55 0D 80 00(启动通知) 06(看门狗复位) 1C(软件版本) 26 30 79 25 00 4B 12 00(MAC 地址) 85

4.1.6 查询与设置信道

命令码：0x06

功能：

使能或除能模组的信道，需要在创建网络或组网前设置，可在待机模式设置。模组默认支持 7 个优选信道（11,14,15,19,20,24,25），该命令可使能或除能多个优选信道，反馈命令携带已使能的信道。

输入命令：

名称	cmd data	
	命令数据	
	Set	ChannelList
	设置	信道列表
字节数	1	变长 N

设置：0 – 除能信道，1 – 使能信道，2 – 覆盖信道（列表不能为 0）

信道：设置除能或使能的信道列表，从 11~26 有效。

反馈命令：

名称	cmd data	
	命令数据	
	status	ChannelList
	状态	信道列表
字节数	1	变长 N

状态：0 – 设置有效， 0xFF-设置无效

信道列表：当前模组使能信道列表，最大 16 字节

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

查询信道（信道列表为空）

发送指令: 55 04 00 06 00(除能) 06

收到反馈: 55 0B 00 06 00(成功) 0B 0E 0F 13 14 18 19(信道列表) 0A

除能信道

发送指令: 55 06 00 06 00(除能) 13 14(信道列表) 01

收到反馈: 55 09 00 06 00(成功) 0B 0E 0F 18 19(信道列表) 0D

覆盖信道

发送指令: 55 06 00 06 02(覆盖) 11 12(信道列表) 07

收到反馈: 55 06 00 06 00(成功) 11 12(信道列表) 05

4.1.7 查询 PANID

命令码：0x07

功能：

设置模组组网用的 PANID，默认 0xFFFF 为随机模式。设置 PANID 需要在协调器建立网络前且在待机模式下设置。

输入命令：

名称	cmd data
	命令数据
	NULL
	空
字节数	0

参数：无

反馈命令：

名称	cmd data	
	命令数据	
	status	PANID
	状态	Pan ID
字节数	1	2

状态：0 – 查询有效，1 – 查询无效

PAN ID：模组 PANID，默认值 0xFFFF

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送指令: 55 03 00 07 07

收到反馈: 55 06 00 07 00(查询成功) C1 BE(PANID) 78

未组网反馈为: FF FF

4.1.8 设置 PANID

命令码：0x08

功能：

模组在协调器模式下指定 PANID 建立网络，，该操作需在建立网络前进行。

输入命令：

名称	cmd data
	命令数据
	PANID
	Pan ID
字节数	2

PANID：预设 PANID 值

反馈命令：

名称	cmd data
	命令数据
	status
	状态
字节数	1

状态：0 – 设置有效，1 – 设置无效

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送指令: 55 05 00 08 98 89(PANID) 19

收到反馈: 55 04 00 08 00(成功) 08

4.1.9 查看本机已加组

命令码：0x09

功能：查看本机加入的组，本机加组后才可接收该组的组播消息。

输入命令格式：

名称	cmd data
	命令数据
	EP_idx
	本机端口索引
字节数	1

本机端口索引：本机端口索引默认为 0x00

反馈命令：

名称	cmd data		
	命令数据		
	Status	Group Num	Group List
	状态	加组数量	加组列表
字节数	1	1	2*N

状态：0x00 – 查询有效，有后续数据，0xFF-查询无效

加组数量：模组上该端口加入的组的总数

加组列表：模组上该端口的加组列表

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送指令：　55 04 00 09 00(本机端口索引) 09

收到反馈: 55 0B 00 09 00(查询有效) 03(加组数量) 0F 00 0E 00 0D 00(加组列表有 3 个数据) 06

4.1.10 本机加组

命令码：0x0A

功能：指定模组上某个端口加组

输入命令格式：

名称	cmd data	
	命令数据	
	EP_idx	Group ID
	本机端口索引	组 ID
字节数	1	2

反馈命令：

名称	cmd data
	命令数据
	Status
	状态
字节数	1

状态：0 – 操作有效，0xFF – 操作无效

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

协调器加入组 0x0100 中

发送指令：55 06 00 0A 00(端口索引) 00 10(组 ID) 1B

收到反馈：　55 04 00 0A 00(成功) 0A

4.1.11 本机退组

命令码：0x0B

功能：指定模组上某个端口退出指定分组

输入命令格式：

名称	cmd data	
	命令数据	
	EP_idx	Group ID
	端口索引	组 ID
字节数	1	2

端口索引：默认值 0

组 ID：需要退出组的 ID 号

反馈命令：

名称	cmd data
	命令数据
	Status
	状态
字节数	1

状态：0 - 操作有效，1 - 模组端口已不在该组，0xFF - 操作无效

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

协调器退出 0x0100 组

发送指令：55 06 00 0B 00(端口索引) 00 10(组 ID) 1B

收到反馈：　55 06 00 0B 00(成功) 00

4.1.12 扫描信道

命令码：0x0C

功能：

扫描信道，判断该信道有哪些协调器和路由器，是否干净。该命令会以“扫描结果通知”的异步命令返回结果。

输入命令：

名称	cmd data		
	命令数据		
	ChannelList	Duration	Mode
	扫描信道列表	每个信道侦听时间	扫描模式
字节数	4	1	1

扫描信道列表：32 位信道列表，对应的信道使能为 1，例如扫描 11~26 信道则填入 0x07FFF800，该值为 0 时强制扫描默认信道（11、14、15、19、20、24、25 共 7 个即“飞利浦信道”）。

每个信道侦听时间：每个信道侦听时间=(2^Duration)*15.36 毫秒，时间越长扫描速度就越慢，扫描到的设备就越多

扫描模式：0-信标扫描模式，该模式会在“扫描结果通知”中返回很多信标，其它-无任何效果

反馈命令：

名称	cmd data
	命令数据
	Status
	状态
字节数	0

状态：0x00 – 操作有效，0xFF – 操作无效。

注意：上一次扫描如果未结束就进行下一次扫描必然会导致操作无效，扫描结束以收到“扫描结束”通知为准。

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

扫描 7 个默认信道（飞利浦信道），每个信道扫描 2^7*15.36 毫秒，预计总共耗时 14 秒

发送指令：55 09 00 0C 00 00 00 00(扫描列表为默认信道) 07(帧听时间) 00 0B

收到反馈：55 04 00 0C 00(扫描有效) 0C

收到异步命令（有效信标）：55 12 80 0C 00(扫描成功) 0E(信道) 83 CE(PANID) 1C 67(短地址) 45 5A 44 09 00 4B 12 00(扩展 PANID) A3(信号强度) 1C

收到异步命令（扫描结束）： 55 09 80 0C 00(扫描成功) FF FF FF FE FF(扫描结束) 72

4.1.13 查询/设置发射功率

命令码：0x0D

功能：查询或设置模组发射功率

输入命令格式：

名称	cmd data	
	命令数据	
	Mode	Power
	模式	功率
字节数	1	1

模式：0x00 - 查询 ， 0x01 - 设置

功率：设置范围为 0x0E~0x14，对应 14dbm~20dbm，协调器默认为 14dbm。

反馈命令：

名称	cmd data
	命令数据
	Status
	状态
字节数	1

状态：0x00 – 操作有效，0xFF – 操作无效

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

设置功率

发送指令：55 04 00 0D 01(配置模式) 14(发射功率 20dbm) 18

收到反馈：　55 04 00 0D 00(成功) 0D

备注：　功率等级为 0x0E~0x14 超过最大值设置不生效且保持之前的设置功率

4.1.14 获取当前 UTC 时间

命令码：0x20

功能：

查询协调器当前的 UTC 时间

输入命令：

名称	cmd data
	命令数据

	null
	空
字节数	0

参数：无

反馈命令：

名称	cmd data	
	命令数据	
	Status	UTC
	执行状态	UTC 时间
字节数	1	4

执行状态：0 – 执行有效，0xFF – 执行无效

UTC 时间：协调器的 UTC32 时间

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送指令：55 03 00 20 20

收到反馈：　55 08 00 20 00(成功) E7 12 00 00(UTC 时间) D5

4.1.15 设置 UTC 时间

命令码：0x21

功能：

设置协调器的 UTC 时间，使协调器对 ZigBee 设备提供 UTC 服务。

注意事项：

由于协调器本身没有 RTC 时钟，但是协调器又要为其它组网设备提供时间服务，因此上位机需定期校准设置协调器的 UTC 时间。若上位机不支持该功能，可能会导致入网设备的运行时间与真实时间不符。

输入命令：

名称	cmd data
	命令数据
	UTC
	UTC 时间
字节数	4

UTC 时间：需要设置的 UTC 时间

反馈命令：

名称	cmd data
	命令数据
	Status
	执行状态
字节数	1

执行状态：0x00 – 执行有效，0xFF – 执行无效

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送指令：55 07 00 21 00 00 00 00(UTC 时间) 21

收到反馈：55 04 00 21 00(成功) 21

4.1.16 读取入网地址表

命令码：0x22

功能：

查询已入网节点的 MAC 地址和短地址，一条一条的查，总共 255（0~254）条。如果入网设备不是 ZigBee 3.0 且第一次入网父节点不是协调器，查不到。另外该表可能会存在僵尸节点的可能。

输入命令：

名称	cmd data	
	命令数据	
	addr_idx	mode
	地址编号	查询模式
字节数	2	1

地址编号：查询协调器保存的地址编号，0x0000~0x00FE 有效

查询模式：0x00 – 普通查询， 0x01- 带标志位查询

反馈命令：

名称	cmd data				
	命令数据				
	status	addr_idx	short_addr	MAC	Flag
	状态	地址编号	节点短地址	节点 MAC 地址	标志位
字节数	1	2	2	8	1

状态：0 – 有入网节点，2 – 无入网节点，0xFF-超出存储范围

地址编号：存储的地址编号

节点短地址：入网节点的短地址

节点 MAC 地址：入网节点的 MAC 地址

标志位：大于或等于 8 为经历过第一次入网认证的合法设备，小于 8 可疑设备

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

普通查询

发送指令：　55 06 00 22 00 00(地址编号) 00(查询模式) 22

收到反馈：55 10 00 22 00(成功) 00 00(地址编号) ED 1B(短地址) 6A 90 B2 FE FF AC 33 BC(MAC 地址) BE

带标志位查询

发送指令：　55 06 00 22 00 00(地址编号) 01(查询模式) 23

收到反馈：55 11 00 22 00(成功) 00 00(地址编号) ED1B(短地址) 6A 90 B2 FE FF AC 33 BC(MAC 地址) 0B(标志位) B5

注意事项：如何制造一个可疑设备

- **加入一个终端节点设备，保证读取入网地址表时能读到它的短地址和 MAC 地址**
- **在终端节点完全关机或者收不到信号的时候，协调器根据 MAC 地址删除这个终端节点**
- **从入网地址表中读取该设备之前的地址编码，发现 MAC 地址记录没有了**

- **重新上电该终端节点，并在协调器收到与该终端节点相关的任何信息**

然后再读取全部入网地址表

发送指令：55 06 00 22 02 00(地址编号) 01(查询模式) 21

收到反馈：55 11 00 22 00(成功) 02 00(地址编号) 32 8C(短地址) D0 27 47 0B 00 4B 12 00(MAC 地址) 03(可疑设备) 7F

备注： 查询协调器保存的地址编号，0x0000~0x00FE 有效（即地址编号最大 FE 00），对应地址若无设备则反馈命令全为 FF

4.1.16 重传设备通知消息

命令码：0x28

功能：设备信息通知在节点第一次入网时才会有，如果错过该消息，可以重新申请设备再次报一次，需确保节点处于正常工作中才有效。

输入命令：

名称	cmd data
	命令数据
	MAC
	节点 MAC 地址
字节数	8

节点 MAC 地址：需要重传的节点的 MAC 地址

反馈命令：

名称	cmd data
	命令数据
	Status
	执行状态
字节数	1

执行状态：0x00 – 操作有效，请等待设备上传，0xFF – 设备不存在

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送指令：55 0B 00 28 13 B7 57 22 00 4B 12 00(节点 MAC 地址) A0

指令反馈：55 04 00 28 00(成功) 28

异步命令：55 24 80 05(设备信息通知) 01(终结标记) 01 13 B7 57 22 00 4B 12 00(设备 SN 号) BE 82(短地址) 01(端口号) 04 01(设备轮廓) 00 01(设备 ID) 04(输入簇数量) 0000 0300 0400 08FC(输入簇表) 03(输出簇数量) 0000 0300 08FC(输出簇表) 37

4.2 系统通知命令

4.2.1 设备启动通知

命令码：0x00

功能：

模组上电时的通知消息，包含模组的 MAC 地址

异步命令：

名称	cmd data		
	命令数据		
	resetMode	Version	IEEE Addr
	复位模式	软件版本	MAC 地址
字节数	1	1	8

复位模式：　1 – Reset 引脚，2 – VDDS 掉电复位　4 – VDDR 掉电复位 5-时钟丢失复位 6-软复位（看门狗复位），7-热启动。该字段可以检测模组异常重启。

MAC 地址：模块的 MAC 地址

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

例如使用指令复位时

收到异步命令：55 0D 80 00 06(软复位) 10(软件版本) 26 30 79 25 00 4B 12 00(MAC 地址) 85

4.2.2 网络状态变更通知

命令：0x01

功能：

模组组网成功，模组组网失败，已入网的模组打开网络，都会产生该异步命令

异步命令：

名称	cmd data						
	命令数据						
	Net status	IEEE Addr	Channel	PANID	ShortAddr	Ext PANID	NWK Key
	网络状态	MAC 地址	信道	PANID	短地址	扩展 PANID	网络密钥
字节数	1	8	1	2	2	8	16

网络状态：0x00– 未组网，0x01 – 已组网， 0x02 – 网络打开

MAC 地址: 模组 MAC 地址，出厂就固定，全球唯一

信道：模组当前信道，组网失败时为 0

PANID：模组当前 PANID，组网失败时为 0xFFFF

短地址：模组当前短地址，组网失败时为 0xFFFE

扩展 PANID：组网失败时为全 0

网络密钥：组网失败时为全 0

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

协调器打开网络通知：55 29 80 01 02(网络打开) C6 B4 E2 0A 00 4B 12 00(MAC 地址) 14(信道) 16 B3(PANID)　00 00(短地址) C6 B4 E2 0A 00 4B 12 00(扩展 PANID) 1B F0 09 64 46 CB 73 77 A7 66 F8 CA 01 B7 80 F6(网络密钥) 0E

协调器重启通知：55 29 80 01 01(已组网) C6 B4 E2 0A 00 4B 12 00 (MAC 地址) 14(信道) 16 B3(PANID) 00 00(短地址) C6 B4 E2 0A 00 4B 12 00(扩展 PANID) 1B F0 09 64 46 CB 73 77 A7 66 F8 CA 01 B7 80 F6(网络密钥) 0D

4.2.3 打开关闭网络通知

命令码：0x02

功能：

协调器打开网络后，该异步命令通知打开网络的窗口时间。如果有新设备加网，新设备可能会增加协调器的窗口时间。另外已入网的路由和终端也可以使用协调器打开网络的指令增加协调器打开网络的窗口时间，但协调器的网络如果关闭，路由和终端是打不开的。协调器关闭网络时也会发出该命令，切窗口时间变成 0。

异步命令：

名称	cmd data
	命令数据
	timeout
	窗口时间
字节数	1

窗口时间：协调器网络打开的窗口时间，为 0 时表示关闭网络。

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送关闭入网允许指令反馈：　55 04 80 02 00(窗口时间) 82

备注：　协调器默认有 3 分钟窗口时间，时间到了协调器会打印通知

4.2.4 节点入网通知

命令码：0x03

功能：

检测到模组或节点入网或重新入网，End Device 切换父节点，Router 重新同步都会导致重新入网。上位机务必注意节点第一次入网，通常只有第一次入网经历的设备才是合法设备。

异步命令：

名称	cmd data			
	命令数据			
	IEEE Addr	Nwk Addr	Parent Addr	Join mode
	MAC 地址	短地址	父节点地址	入网模式
字节数	8	2	2	1

MAC 地址：入网设备的 MAC 地址

短地址：入网设备的短地址

父节点地址：入网设备的父节点地址，踢掉 End Device 需要父节点地址

入网模式：0 – 第一次入网，1-重新入网，2 – 重新入网且从新同步密钥（管理器预留密钥更换功能）

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

检测节点入网通知：55 10 80 03 0F 4E 03 1C 00 4B 12 00(MAC 地址) 2A 25(入网节点短地址) 00 00(父节点短地址) 00(第一次入网) 8B

检测节点重新入网(节点重启)：55 10 80 03 0F 4E 03 1C 00 4B 12 00(MAC 地址) 2A 25(入网节点短地址) 00 00(父节点短地址) 01(重新入网) 8A

4.2.5 节点短地址更新通知

命令码：0x04

功能：

模组或节点入网时向协调器上报 MAC 地址或短地址，以及运行过程中短地址发生变更，都会以该命令作为通知。上位机收到该命令后应该及时更新 MAC 地址与短地址映射关系。

异步命令：

名称	cmd data		
	命令数据		
	IEEE Addr	Nwk Addr	Node Type
	MAC 地址	短地址	节点类型
字节数	8	2	1

MAC 地址：目标节点的 MAC 地址

短地址：目标节点的短地址

节点类型：1 – 路由，2-不休眠终端节点，3-休眠终端节点

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

短地址更新通知: 55 0E 80 04 0F 4E 03 1C 00 4B 12 00(MAC 地址) 2A 25(短地址) 02(节点类型) 8E

4.2.6 设备信息通知

命令码：0x05

功能：

入网节点上的详细信息，包括该入网设备所有端口（Endpoint）所属的 Profile 以及支持的簇（cluster）。根据该信息可以判断入网设备是什么，支持哪些功能。该消息在设备新入网的瞬间产生，且有可能会一个节点产生多条消息。若上位机丢失该消息，可通过“重传设备通知消息”重新获取该消息。

异步命令：

名称	cmd data									
	命令数据									
	EndFlag	DevSN	Shortaddr	Endpoint	ProfileID	DeviceID	In Cluster List		Out Cluster List	
	终结标记	设备 SN 号	短地址	端口号	设备轮廓	设备 ID	输入簇表		输出簇表	
							数量	列表	数量	列表
字节数	1	9	2	1	2	2	1	2*N	1	2*N

终结标记：单节点入网会携带多个端口，该标记为 1 表示该节点的端口上报结束。

DevSN：设备虚拟 SN 号，见虚拟 SN

短地址：设备短地址

端口号：设备的端口号，端口号可以和短地址组合使用，当做 24bit 的设备地址

设备轮廓：profile ID，应用层只需要关注 0x0104 即可

设备 ID：表示设备的功能，由 ZCL 协议规范决定。

输入簇表：设备支持的输入簇

输出簇表：设备支持的输出簇

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

设备信息通知:

55 24 80 05 01(终结标记) 01 13 B7 57 22 00 4B 12 00(设备 SN 号) BE 82(短地址) 01(端口号) 04 01(设备轮廓) 00 01(设备 ID) 04(输入簇数量) 00 00 03 00 04 00 08 FC(输入簇列表) 03(输出簇数量) 00 00 03 00 08 FC(输出簇列表) 37

4.2.7 节点离网通知

命令码：0x06

功能：

设备主动离网，协调器会收到该消息，设备每次离网可能会发出多包该消息。如果设备主动离网时不在协调器的覆盖范围，协调器收不到该消息，但数传模组可正常离网。

异步命令：

名称	cmd data	
	命令数据	
	IEEE Addr	
	MAC 地址	
字节数	8	

MAC 地址：离网设备的 MAC 地址

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

离网通知例举：55 0B 80 06 0F 4E 03 1C 00 4B 12 00(MAC 地址) 81

4.2.7 扫描结果通知

命令码：0x0C

功能：

返回信道扫描结果，信标扫描模式下会返回多个信标。协调器和路由器都会有信标产生，根据信标数量可以大概知道空间内有多少个协调器路由器，分布在哪些信道，以及他们的 PANID 和短地址是什么，信号强度有多强。

异步命令：

名称	cmd data					
	命令数据					
	Status	Channel	PanID	nwkAddr	extPANID	LQI
	扫描状态	信道	PANID	短地址	扩展 PANID	信号强度
字节数	1	2	2	2	8	1

扫描状态：0-扫描到有效信标，0xFF-扫描结束

信道：扫描到信标所属的信道，0xFF 表示扫描结束

PANID：扫描到信标所属的 PANID，0xFFFF 表示扫描结束

短地址：扫描到信标的短地址，0xFFFE 表示扫描结束

扩展 PANID：扫描到信标的扩展 PANID，扫描结束时无该项信息

信号强度：扫描到的信标 LQI 信号强度，255 为最强，0 为最弱，距离越近越强。

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

反馈：55 12 80 0C 00(成功) 0E(信道) 83 CE(PANID) 1C 67(短地址) 45 5A 44 09 00 4B 12 00(扩展 PANID) A3(信号强度) 1C

4.3 网络管理命令

4.3.1 网络命令格式解析

统一命令头格式：

网络管理命令下发输入命令，第一次收到反馈命令，第二次收到异步命令“发送确认”，第三次收到异步命令“网络管理返回”。每一次接收到的命令，决定是否会收到下一次命令。

4.3.1.1 输入命令格式：

名称	cmd data	
	命令数据	
	Nwk Addr	Cmd param
	短地址	命令参数
字节数	2	变长

命令参数：不同命令参数不同，后面针对不同命令的参数作解析

4.3.1.2 反馈命令格式：

名称	cmd data	
	命令数据	
	status	handle
	执行状态	命令编号
字节数	1	1

执行状态：0x00 – 执行有效，后续必会产生发送确认。其它值 – 执行无效，见 AF 状态表

命令编号：系统为该命令分配的编号，可在发送确认和网络管理命令返回中追溯对应的输入命令。

4.3.1.3 发送确认格式：

名称	cmd data		
	命令数据		
	Nwk Addr	AF status	handle
	短地址	发送结果	命令编号
字节数	2	1	1

短地址：发送目标的短地址

发送结果：无线发送结果，见 AF 状态表

命令编号：系统为该命令分配的编号，可在发送确认和网络管理命令返回中追溯对应的输入命令。

备注：发送确认返回 E1 (信道干扰),E9(未收到 ACK),CD(终端节点不在线)对应参见 3.4 AF Status 状态表

4.3.1.4 接收网络管理命令返回：

名称	cmd data

	命令数据			
	Nwk Addr	handle	Zdo status	Cmd param
	短地址	命令编号	执行结果	命令参数
字节数	2	1	1	变长

短地址：返回命令的设备短地址

命令编号：与发送时系统分配的一致，发端产生什么收端就返回什么

执行结果：收端对该命令的执行结果，可能返回“不支持”，见 ZDO 状态表

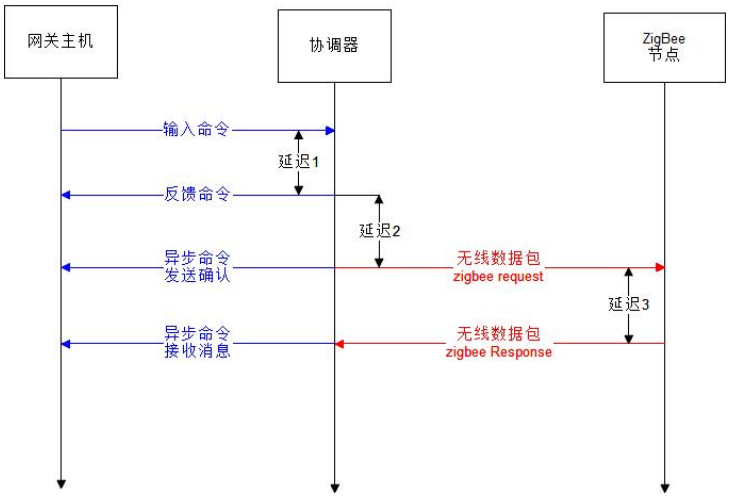
命令参数：执行结果为 0 时，该参数才有效。

命令发送与接收说明：

网络管理命令，由上位机发给数传模组或组网管理器，反馈命令的作用仅表示该命令是否正确输入，模组是否处于可发送消息的状态。发送确认则表示该消息是否发送出去，甚至是否发给了目标（未丢在半路上）。接收返回命令则是对方设备对命令的执行结果。

注意事项：

- 任何一条反馈命令的 status 为 0（成功）时，必然会产生一条发送确认，其它结果则不会产生发送确认。
- 发送确认是对无线命令是否发送成功的确认，若发送确认的 AF Status 状态为非成功，则可以放弃等待返回消息，重新发送请求。
- 对于“内存满”（0x11），“信道干扰”（0xE1），“没收到 ACK”（0xE9）等错误，有可能是该时段内网络通信频繁导致，可以择机重传，只要未出现连续相同错误即为正常。
- 对于“目标设备不存在”（0xCD）错误，说明该发送短地址对应的设备无效。首先检查该短地址对应设备是否存在，然后检查该设备的短地址是否变更，可使用“查询节点短地址”的方式更新设备短地址



4.3.2 查询节点短地址

命令码：0x00

功能：

根据 IEEE 地址查询目标节点的短地址，该命令输入短地址需使用 0xFFFD 广播地址。

输入命令：

名称	cmd param
	命令内容

	IEEE Addr
	MAC 地址
字节数	8

MAC 地址：被查询节点的 MAC 地址

返回命令：

名称	cmd param	
	命令内容	
	IEEE Addr	reserve
	MAC 地址	保留位
字节数	8	2

MAC 地址：被查询节点的 MAC 地址，被查询节点的短地址在命令头中

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送命令：55 0D 01 00 FD FF(广播地址) 3D 01 70 0F 00 4B 12 00(目标设备 MAC 地址) 19

反馈命令：55 05 01 00 00(状态成功) 05(命令编号) 04

发送确认：55 07 8F 01 FD FF(广播地址) 05(命令编号) 00(发送成功) 89

收到返回：55 11 81 00 00 A0(目标短地址) 05(命令编号) 00(执行成功) 3D 01 70 0F 00 4B 12 00(目标 MAC 地址) B3 00(保留字节位) 8D

4.3.3 查询节点 MAC 地址

命令码：0x01

功能：

根据短地址查询目标节点的 MAC 地址

输入命令：

名称	cmd param
	命令内容
	NULL
	空
字节数	0

返回命令：

名称	cmd param	
	命令内容	
	IEEE Addr	reserve
	MAC 地址	保留位
字节数	8	2

MAC 地址：被查询节点的 MAC 地址

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送命令: 55 05 01 01 7B 20(目标短地址) 5B

反馈命令: 55 05 01 01 00(状态成功) 1A(命令编号) 1A

发送确认：55 07 8F 01 7B 20(目标短地址) 1A(命令编号) 00(发送成功) CF

收到返回：55 11 81 01 7B 20(目标短地址) 1A(命令编号) 00(执行成功) 3D 01 70 0F 00 4B 12 00(目标 MAC 地址) AB 00(保留) 70

4.3.4 查询节点网络配置信息

命令码：0x02

功能：

查询节点的网络配置信息

输入命令：

名称	cmd param
	命令内容
	nwk_add
	短地址
字节数	2

返回命令：

名称	cmd param						
	命令内容						
	logicalType	freqBand	stackRev	manCode	maxBufSize	maxInSize	maxOutSize
	逻辑类型	频带	ZigBee 版本	厂商码	最大命令长度	最大接收	最大发送
字节数	1	1	1	2	1	2	2

逻辑类型：0 – 协调器，1 – 路由， 2-终端节点， 3-低功耗节点

频带：节点的工作频带位图，bit1 - 800MHz，bit4 - 900MHz，bit8 – 2.4GHz

ZigBee 版本：转换成十进制，大于等于 21 则符合 ZigBee 3.0

厂商码：节点厂商码，可用于私有协议的簇

最大命令长度：对方设备网络支持网络管理命令最大长度

最大接收：对方设备支持最大数据接收长度

最大发送：对方设备支持最大发送数据长度

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送命令：55 05 01 02 27 84(目标短地址) A0

反馈命令：55 05 01 02 00(状态成功) 12(命令编号) 11

55 07 8F 01 27 84(目标短地址) 12(命令编号) 00(发送成功) 3F

55 11 81 02 27 84(目标短地址) 12(命令编号) 00(执行成功) 02(逻辑类型) 08(频带) 15(版本) 00 20(厂商码) 50(最大命令长度) A0 00(最大接收长度) A0 00(最大发送长度) 5D

4.3.5 查询节点端口信息

命令码：0x04

功能：

查询节点上某个指定端点的信息。包括其所属的 profile，支持的 cluster。

输入命令：

名称	cmd param
	命令内容
	Endpoint
	端口号
字节数	1

端口号：被查询的目标设备的端口号

返回命令：

名称	cmd param							
	命令内容							
	Endpoint	ProfileID	deviceID	device version	In Cluster List		Out Cluster List	
	端口号	设备轮廓	设备 ID	设备信息版本	输入簇表		输出簇表	
					数量	列表	数量	列表
字节数	1	2	2	1	1	2*N	1	2*N

端口号：被查询的设备端口号

设备轮廓：profile ID，应用层只需要关注 0x0104 即可

设备 ID：表示设备的功能，由 ZCL 协议规范决定。

设备信息版本：设备描述信息的版本号，0 为 v1.0 版

输入簇表：设备支持的输入簇

输出簇表：设备支持的输出簇

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送命令：　55 06 01 04 27 84(目标短地址) 01(目标端口) A7

反馈命令：　55 05 01 04 00(状态成功) 15(命令编号) 15

发送确认：55 07 8F 0127 84 15(命令编号) 00(发送成功) 38

收到返回：55 1D 81 0427 84 15(命令编号) 00(执行成功) 01(目标端口) 04 01(设备轮廓) 00 01(设备 ID) 00(设备版本) 04(输入簇数量) 0000 0300 0400 08FC(输入簇列表) 03(输出簇数量) 0000 0300 08FC(输出簇列表) 35

4.3.6 查询节点端口数

命令码：0x05

功能：

查询节点上的全部端口

输入命令：

名称	cmd param
	命令内容
	nwk_add
	短地址
字节数	2

返回命令：

名称	cmd param

	命令内容	
	Endpoint Num	Endpoint List
	端口数	端口列表
字节数	1	N

端口数：被查询节点端口数量

端口列表：被查询节点的端口列表

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送命令：55 05 01 05 27 84(短地址) A7

反馈命令：55 05 01 05 00(状态成功) 1A(命令编号) 1E

发送确认：55 07 8F 01 27 84(短地址) 1A(命令编号) 00(发送成功) 37

接收返回：55 09 81 05 27 84(短地址) 1A(命令编号) 00(执行成功) 01(端口数) 01(端口列表) 3D

4.3.7 设置节点常连接绑定

命令码：0x21

功能：

使用 ZigBee Bind 的方式，设置两个节点上的端口常连接绑定。

输入命令：

名称	cmd param		
	命令内容		
	Src devSN	Cluster ID	Dst devSN
	源虚拟 SN	簇 ID	目标虚拟 SN
字节数	9	2	9

源虚拟 SN：常连接的源虚拟设备的 SN 号，虚拟 SN，源虚拟 SN 在“设备信息通知”中可以获取到。

簇 ID：常连接通信用的簇 ID

目标虚拟 SN：目标设备的虚拟 SN 号，虚拟 SN，目标可以是一个具体的虚拟设备，也可以是一个分组，目标 SN 填入 9 个字节 0x00 自动替换成协调器的虚拟 SN。

返回命令：

名称	cmd param
	命令内容
	NULL
	空
字节数	0

参数：无，直接从统一头部中的“执行结果”判断结果

命令示例：（紫色：负载长度　红色：命令类型+命令码　蓝色：校验码）

发送命令：55 19 01 21 76 C2(目标短地址) 01 1A E7 45 0A 00 4B 12 00(源虚拟 SN) 08FC(簇 ID)　01 49 71 F8 0A 00 4B 12 00(目标虚拟 SN) 18

反馈命令：55 05 01 21 00(状态成功) 05(命令编号) 25

发送确认：55 07 8F 01 76 C2(目标短地址) 05(命令编号) 00(发送成功) 3F

接收返回：55 07 81 21 76 C2(目标短地址) 05(命令编号) 00(执行成功) 11

备注：设置常连接前需将对应终端设备目标端口设置为 FE 目标短地址设置为 FF FE 进入绑定 Mac 通信模式，常连接只允许设置一个对象

4.3.8 取消节点常连接绑定

命令码：0x22

功能：

解除已存在的常连接绑定，格式与设置常连接绑定一样

输入命令：

名称	cmd param		
	命令内容		
	Src devSN	Cluster ID	Dst devSN
	源虚拟 SN	簇 ID	目标虚拟 SN
字节数	9	2	9

源虚拟 SN：常连接的源虚拟设备的 SN 号，见虚拟 SN。

簇 ID：常连接通信用的簇 ID

目标虚拟 SN：目标设备的虚拟 SN 号，见虚拟 SN，目标 SN 填入 9 个字节 0x00 自动替换成协调器的虚拟 SN。

返回命令：

名称	cmd param
	命令内容
	NULL
	空
字节数	0

参数：无，直接从统一头部中的“执行结果”判断结果

命令示例：（紫色：负载长度　红色：命令类型+命令码　蓝色：校验码）

发送命令：55 19 01 22 76 C2(目标短地址) 01 1A E7 45 0A 00 4B 12 00(源虚拟 SN) 08 FC(簇 ID) 01 49 71 F8 0A 00 4B 12 00(目标虚拟 SN) 1B

反馈命令：55 05 01 22 00(状态成功) 08(命令编号) 2B

发送确认：55 07 8F 01 76 C2(目标短地址) 08(命令编号) 00(发送成功) 32

接收返回：55 07 81 21 76 C2(目标短地址) 08(命令编号) 00(执行成功) 1F

4.3.8 查看节点常连接绑定

命令码：0x33

功能：

查看已存在的常连接绑定，以一条一条的列表的形式输出所有的常连接绑定关系。

注意事项：

由于绑定通信采用 MAC 地址方式，源设备会自动通过广播查找的方式根据 MAC 地址查找目标。不存在的 MAC 累积越

多会形成广播风暴，影响正常通信。因此须对网络定期维护，定期查询网络中所有设备是否绑定了不存在的 MAC 并删除。

输入命令：

名称	cmd param
	命令内容
	StartIdx
	起始索引
字节数	1

起始索引：查询常连接记录的起始编号，返回时可返回多条记录，多次查询可以查完一个节点上的所有常连接关系。

返回命令：

名称	cmd param					
	命令内容					
	TotalNum	StartIdx	ListNum	List Data		
	记录总数	起始索引	返回条数	常连接记录		
				源虚拟 SN	簇 ID	目标虚拟 SN
字节数	1	1	1	20*N		
				9	2	9

记录总数：节点上建立的常连接总数

起始索引：当前返回记录的起始编号

返回条数：当前返回记录条数

源虚拟 SN：记录的源虚拟 SN

簇 ID：记录的链接的簇 ID

目标虚拟 SN：记录的目标虚拟 SN

命令示例：（紫色：负载长度　红色：命令类型+命令码　蓝色：校验码）

发送命令：55 06 01 33 76 C2(目标短地址) 00(起始索引) 86

反馈命令：55 05 01 33 00(状态成功) 0C(命令编号) 3E

发送确认：55 07 8F 01 76 C2 (目标短地址) 0C(命令编号) 00(发送成功) 36

接收返回：55 1E 81 33 76 C2(目标短地址) 0C(命令编号) 00(执行成功) 01(记录总数) 00(起始索引) 01(返回条数) 011AE745 0A004B1200(源虚拟 SN) 08 FC(簇 ID) 014971F80A004B1200(目标虚拟 SN) 86

4.3.9 删除节点

命令码：0x34

功能：

根据 MAC 地址删除指定节点，如果被删除的设备是终端节点，该命令的短地址要发给它的父节点，填父节点短地址。

输入命令：

名称	cmd param		
	命令内容		
	IEEE	rejoin	removechild
	MAC 地址	重入网	删子节点
字节数	8	1	1

MAC 地址：需要删除的节点的 MAC 地址

重入网：默认填 0

删子节点：默认填 0

返回命令：

名称	cmd param
	命令内容
	NULL
	空
字节数	0

参数：无，直接从统一头部中的“执行结果”判断结果

命令示例：（紫色：负载长度　红色：命令类型+命令码　蓝色：校验码）

发送命令：55 0F 01 34 00 00(父节点短地址) 13 B7 57 22 00 4B 12 00(节点 MAC) 00(重入网) 00(删子节点) BD

反馈命令：55 05 01 34 00(状态成功) 09(命令编号) 3C

发送确认：55 07 8F 01 00 00(父节点短地址) 09(命令编号) 00(发送成功) 87

接收返回：55 07 81 34 00 00(父节点短地址) 09(命令编号) 00(执行成功) BC

稍等几秒然后收到模组离网通知

55 0B 80 06(离网通知) 13 B7 57 22 00 4B 12 00(节点 MAC) 0E

备注：由于不确定删除设备父节点短地址，可以使用 FD FF 广播短地址删除

4.3.10 信道干扰检测

命令码：0x38

功能：

检测各个信道的质量和各个信道上的 2.4G 干扰，返回各个信道的环境 LQI 值。该命令仅支持点播，可以发给协调器自己（即短地址=0x0000）。由于扫描信道需要目标设备在多个信道上切换，目标若是休眠终端设备，在扫描过程中传输其它数据，可能会导致出错。

输入命令：

名称	cmd param		
	命令内容		
	channel mask	duration	count
	信道列表	检测时间	扫描次数
字节数	4	1	1

信道列表：32 位信道列表，对应的信道使能为 1，例如扫描 11~26 信道则填入 0x07FFF800，该值为 0 时强制扫描 11~26 信道，建议值 0x07FFF800。

检测时间：每个信道侦听时间=(2^duration)*15.36 毫秒，时间越长扫描速度就越慢，该值最大为 5 即每个信道侦听 490ms。

扫描次数：反复扫描次数，范围（1~5），建议填 0x01

返回命令：

名称	cmd param

	命令内容				
	channel mask	total transmit	total fails	channel count	energy list
	信道列表	累计发送	累计发送失败	信道数量	信道质量列表
字节数	4	2	2	1	变长

信道列表：32 位信道列表，对应的信道使能为 1。

累计发送：累计发送数据包数量

累计发送失败：累计发送失败的数量（这个可以查看丢包率）

信道数量：返回扫描的信道数量，结合返回的信道列表，可匹配信道质量列表中对应的信道

信道质量列表：信道上的信号强度，用 LQI 值来表示，最大 0xFF。

命令示例：（紫色：负载长度 红色：命令类型+命令码 蓝色：校验码）

发送命令：55 0B 01 38 00 00(目标短地址) 00 F8 FF 07(信道列表) 05(检测时间) 01(扫描次数) 3D

反馈命令：55 05 01 38 00(状态成功) 12(命令编号) 2B

发送确认：55 07 8F 01 00 00(目标短地址) 12(命令编号) 00(发送成功) 9C

接收返回：55 20 81 38 00 00(目标短地址) 12(命令编号) 00(执行成功) 00 F8 FF 07(信道列表) C8 04(累计发送) 00 00(累计发送失败) 10(信道数量) 7F BD AB 91 B9 99 CC BD 83 86 B6 E1 AB 66 66 B6(信道质量列表) 91

注意：

- 信道信号强度列表为 LQI 值，0xFF 为信号最强。可使用该值除以 0xFF 得到的比值，比值超过 80%算极为糟糕的信道，优先选择信号最小的信道创建网络。
- 从收到发送确认开始，到收到接收返回，需要等待至少的时间为（2^5)*15.36*16 = 7864.32ms，加上串口传输的延迟和 ZigBee 指令传输延迟，实际需要等待 8~9 秒。

4.4 设备状态管理与设备控制（ZCL 命令）

4.4.1 ZCL 协议结构及相关解释

✧ Endpoint（端口）：一个 ZigBee 设备上可能存在多个应用外设，它们可能具备相同和不同的功能。例如多孔插座上面每个孔都具备相同的控制功能，通过短地址和 MAC 地址定位到插座，通过端口定位到插孔。

✧ Profile（剖面）：用于标注端口的应用协议类型，设备端会拒绝执行来自不同 profile 的指令。每个 Endpoint 都有固定的 Profile，具备多端口的设备，可同时支持多个 Profile。

✧ Cluster（簇）：簇用于描述设备支持的功能集群，通常一种功能中会包含多种控制方式，多个物理量或状态，它们之间都有很强的相关性。一个端口可以支持多个簇，表示它支持的功能有哪些。簇分“Input（输入）”和“Output（输出）”两种类型，输入型的簇表示该设备的该端口为受控的一方，输出型的簇表示该端口为发起控制的一方。原则上一个端口不能既当控制者又当受控者，否则容易造成“自锁”。

✧ Attribute（属性）：在 ZCL 协议中，每个属性代表目标设备的一个状态参数或者物理量。具有相关性的状态或物理量通常被编入同一个簇，访问属性的命令（读取，修改，查看，上报）可以一条命令同时携带相同簇下的多个属性参数，所有簇都有统一的属性访问命令结构格式。若单个设备上可能存在多个雷同属性，通常会分配在不同的端口。例如目标设备为多孔插座，每个插孔的开合状态和用电量有各自独立的参数，它们会使用相同的簇 ID 和属性 ID，但目标端口不同，通过设置不同目标端口获取所需对应目标的状态参数。

✧ 控制命令：属性和控制命令，都是一个簇中提供的对设备操作的手段。由于属性通常对应设备中的静态变量，大小固定且数据短小，因此在向受控设备发起变长的消息，或受控设备需要返回变长消息均通过控制命令来实现。与属性访问命令不

同，控制命令没有统一的命令结构，不同簇有不同的控制命令结构。控制命令携带的参数先改变目标设备的物理状态，物理状态改变时再同步到对应的属性上，因此一些不能通过修改属性的方式来控制目标设备就要用到控制命令，而且控制命令可携带更复杂的控制参数，而属性必须为表 3.5 中的固定格式数据。

✧ ZCL 控制的因果性：带有输出簇的设备（精准到端口）向带有输入簇的设备（端口）发送控制命令，导致输入命令的一方某个或多个物理状态发生变化，变化的物理量的值同步到该簇下对应的属性上，导致网络内其它任何设备访问受控设备上该物理状态对应的属性，都是反映该受控设备当前的物理状态。

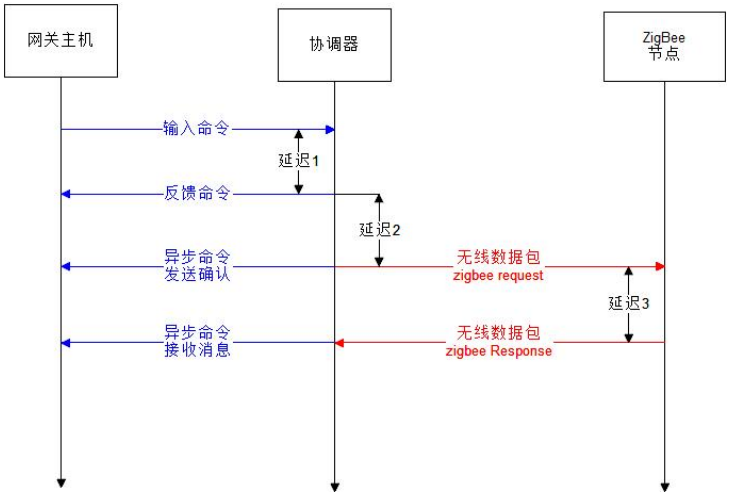
4.4.2 ZCL 命令格式解析

统一命令头格式：

ZCL 命令旨在使用有限多的命令格式，组合出千变万化的不同设备的控制命令，包括对设备中的 Attribute（属性）进行访问，以及发起对这些设备的控制。

ZCL 命令包括“输入命令”，“反馈命令”，以及“发送确认”和“接收命令”两种异步命令，共 4 种不同格式。对设备的访问采用短地址+端口号的 24bit 虚拟地址方式。

ZCL 命令支持单播，组播，广播 3 种传输方式。其中组播和广播的端口为 0xFF。



① **输入命令格式：**

输入命令会产生从协调器到设备的 ZCL 无线命令，其统一头格式如下

名称	cmd data								
	命令数据								
	mode	shortAddr	Endpoint	SeqNum	Direction	ClusterID	ManuCode	AckMode	Ext data
	发送模式	目标短地址	目标端口	帧序号	命令方向	簇 ID	厂商码	应答模式	扩展数据
字节数	1	2	1	1	1	2	2	1	变长

发送模式：0x00 – 普通模式、0x40 – APS 加密、0x80 – 跳过路由转发、0xC0 – APS 加密且跳过路由转发

目标短地址：发送目标短地址，0xFFFC~0xFFFF 为广播（0xFFFE 为无效地址）

目标端口：发送目标的端口，填入 0xFF 且短地址不为广播时，则采用组播发送

帧序号：上位机产生帧序号，如果收到 ZCL 帧的帧序号和短地址，端口与发送相等，则该消息为目标设备的回复消息。

命令方向：参照 ZCL 构架，0 - C2S（攻->受），1 – S2C（受->攻）

簇 ID：发送消息的簇 ID

厂商码：发送消息的厂商码，目标设备需要支持厂商码才有效，默认填 0x0000。

应答模式：0 –使用 Default Response 作应答，1-使用 APS Ack 作应答。

扩展数据：不同命令的扩展数据不同，后续的命令解析，只针对扩展数据部分作解析

② **反馈命令格式：**

名称	cmd data	
	命令数据	
	status	SeqNum
	执行状态	帧序号
字节数	1	1

执行状态：0 – 执行有效，会产生发送确认，其它见 AF 状态

帧序号：上位机发送对应命令时填入的帧序号

③ **发送确认格式：**

名称	cmd data					
	命令数据					
	mode	shortAddr	Endpoint	SeqNum	Direction	AF status
	发送模式	目标短地址	目标端口	帧序号	命令方向	发送结果
字节数	1	2	1	1	1	1

发送模式：与发送时一样

目标短地址：发送目标短地址，与发送时一样

目标端口：发送目标的端口，与发送时一样

帧序号：与发送命令时一致

命令方向：与发送命令时的一致

发送结果：无线发送结果，见 **AF 状态表**

④ **异步命令“接收 ZCL 消息”格式：**

协调器收到 ZCL 消息时，会转换成以下的统一头格式

名称	cmd data								
	命令数据								
	mode	shortAddr	Endpoint	SeqNum	Direction	ClusterID	ManuCode	Rssi	Ext data
	对方模式	源短地址	源端口	命令编号	命令方向	簇 ID	厂商码	信号强度	扩展数据
字节数	1	2	1	1	1	2	2	1	变长

对方模式：0x00-普通接收、0x10-收到广播、0x20-信号强度有效、0x30-收到广播且信号强度有效

源短地址：对方设备的短地址

源端口：对方设备的端口

帧序号：收到消息的帧序号，如果收到帧序号、源地址、源端口与发送时相同，且命令方向相反，则为发送命令的返回命令。

命令方向：参照 ZCL 构架，0 - C2S（攻->受），1 – S2C（受->攻）

簇 ID：接收消息的簇 ID

厂商码：收到消息的厂商码，需要源设备支持才行

信号强度：收到消息的信号强度 RSSI 值

扩展数据：不同命令的扩展数据不同，后续的命令解析，只针对扩展数据部分作解析

4.4.3 ZCL 命令类型与功能目录

ZCL 命令解析，仅针对输入命令和接收消息中的“扩展数据”部分进行解析。某些命令之间存在收发因果关系，因此具有收发因果关系的命令统一解析。

功能	命令码	发送	接收
读取目标属性	0x00	ZCL_READ_ATTR_REQ	ZCL_READ_ATTR_RSP
修改目标属性	0x01	ZCL_WRTIE_ATTR_REQ	ZCL_WRTIE_ATTR_RSP
查询属性上报规律	0x02	ZCL_READ_REPORT_REQ	ZCL_READ_REPORT_RSP
修改属性上报规律	0x03	ZCL_WRITE_REPORT_REQ	ZCL_WRITE_REPORT_RSP
查看全部属性	0x04	ZCL_DISC_ATTR_REQ	ZCL_DISC_ATTR_RSP
查看全部属性（带扩展）	0x05	ZCL_DISC_ATTR_EX_REQ	ZCL_DISC_ATTR_EX_RSP
属性主动上报	0x0A	无	ZCL_REPORT_IND
系统默认返回	0x0B	无	ZCL_DEFAULT_RSP
发送控制命令	0x0F	ZCL_CMD	无
接收控制命令	0x0F	无	ZCL_CMD_IND

✧　“查询属性上报规律”和“修改属性上报规律”需目标设备支持该功能，本无线模组仅支持该命令的发送和返回命令的接收，无示例指令。

4.4.4 读取目标属性

命令码：0x00

功能：读 ZCL 属性参数，可以读取一个端口上指定簇中的多个参数

输入命令格式：

名称	ext data	
	扩展数据	
	AttrNum	AttrID List
	属性数量	属性 ID 列表
字节数	1	2*N

属性数量：一次读取的属性数量，实际读到的属性只能小于或等于该值。

属性列表：属性 ID 构成的 uint16 数组列表

反馈命令格式：

名称	ext data				
	扩展数据				
	AttrNum	Attr List * N			
	属性数量	属性列表			
		属性 ID	ZCL 状态	数据类型	数据值
字节数	1	2	1	1	变长

属性数量：读到的属性数量，如果设备部支持读命令中包含的某些属性 ID，返回命令也不包含这些属性。

属性 ID：读到的 16 位属性 ID

ZCL 状态：见 ZCL 错误码，只有“操作成功”才有后面的数据

数据类型：数据类型，见《ZCL 数据类型表》

数据值：该属性对应的数值，大小由数据类型中“字节数”一项决定

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

读取 **Cluster ID 0xFC08** 下的所有属性：(读 0x0000, 0x0001, 0x0002, 0x0003, 0x0004)

发送命令：55 19 02 00 00(发送模式) 7B 20(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 08 FC (簇 ID) 00 20(厂商码) 00(应答模式) 05(读属性个数) 00 00 01 00 02 00 03 00 04 00(属性 ID 列表) 2F

反馈命令：55 05 02 00 00(状态成功) A2(帧序号) A0

发送确认：55 0A 8F 02 00(发送模式) 7B 20(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 00(发送成功) 75

接收返回：55 2C 82 00 00(对方模式) 7B 20(源短地址) 01(源端口) A2(帧序号) 01(命令方向) 08 FC(簇 ID) 00 20(厂商码) FF(RSSI) 05(属性个数) 00 00(属性 ID) 00(ZCL 状态) 23(数据类型) 00 C2 01 00(波特率) 01 00(属性 ID) 00(ZCL 状态) 21(数据类型) FF FF(透传目标短地址) 02 00(属性 ID) 00(ZCL 状态) 20(数据类型) FF(透传目标端口) 03 00(属性 ID) 00(ZCL 状态) 10(数据类型) 00(串口命令模式) 04 00(属性 ID) 00(ZCL 状态) 30(数据类型) 00(低功耗等级) 6F

读取 **Cluster ID 0x0000** 下的所有属性：(读 0x0000, 0x0001, 0x0002, 0x0003, 0x0004, 0x0005, 0x0006, 0x0007)

发送命令：55 1F 02 00 40(发送模式) ED BD(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 00 00(簇 ID) 00 00(厂商码) 00(应答模式) 08(属性个数) 0000 0100 0200 0300 0400 0500 0600 0700 属性列表 B9

反馈命令：55 05 02 00 00(状态成功) A2(帧序号) A0

发送确认：55 0A 8F 02 40(发送模式) ED BD(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 00(发送成功) 3E

接收返回：55 5F 82 00 00(对方模式) ED BD(源短地址) 01(源端口) A2(帧序号) 01(命令方向) 00 00(簇 ID) 00 00(厂商码) FF (RSSI) 08(属性个数) 00 00(属性 ID) 00(ZCL 状态) 20(数据类型) 01(ZigBee 版本) 01 00(属性 ID) 00(ZCL 状态) 20(数据类型) 10(软件版本) 02 00(属性 ID) 00(ZCL 状态) 20(数据类型) 16(协议版本) 03 00(属性 ID) 00(ZCL 状态) 20(数据类型) 01(硬件版本) 04 00(属性 ID) 00(ZCL 状态) 42(数据类型字符串) 10(字符串长度) 77 77 77 2E 45 62 79 74 65 2E 63 6F 6D 20 20 20(厂商名称) 05 00(属性 ID) 00(ZCL 状态) 42(数据类型字符串) 10(字符串长度) 45 31 38 2D 5A 69 67 62 65 65 2D 44 61 74 61 2E(产品型号) 06 00(属性 ID) 00(ZCL 状态) 42(数据类型字符串) 08(字符串长度) 32 30 32 32 30 34 32 34(编译日期) 07 00(属性 ID) 00(ZCL 状态) 30(数据类型) 01(电源方式) E7

厂商名称：10(数据长度) 77 77 77 2E 45 62 79 74 65 2E 63 6F 6D 20 20 20 转换为 ASIIC **www.Ebyte.com**

产品型号：10(数据长度) 45 31 38 2D5A 69 67 62 65 65 2D 44 61 74 61 2E 转换为 ASIIC **E18-Zigbee-Data.**

编译日期：08(数据长度) 32 30 32 32 30 34 32 34 转换为 ASIIC **20220424**

备注:

1、若目标短地址使用 FD FF 广播方式读取会导致网络内除协调器外所有设备都会反馈，不建议使用广播方式查询修改设备信息；

2、一次性读取多个属性时，发送命令中端口索引+发送模式需要使用“0x40”进行发送，否则会出现发送读取命令失败；

3、Cluster ID 0x0000 下的属性不支持终端设备读取自身的属性，但终端设备可以读取其他设备；

4、端口索引+发送模式：如使用 ZCL 命令进行数据通信传输，需要使用端口索引+发送模式：0x40 模式进行发送。

4.4.5 修改目标属性

命令码：0x01

功能：修改指定的属性，可一次修改多个属性，但目标设备中该属性必须存在且可写，数据类型也必须和目标设备中的一致。如果出现修改无效，返回命令中会带上哪些属性修改无效。

输入命令格式：

名称	ext data	
	扩展数据	
	AttrNum	Attr List * N
	属性数量	属性列表

		属性 ID	数据类型	数据值
字节数	1	2	1	变长

属性数量：需要修改的属性数量

属性 ID：需要修改的属性 ID

数据类型：数据类型，见《ZCL 数据类型表》

数据值：该属性对应的数值，大小由数据类型中“字节数”一项决定

反馈命令格式：

名称	ext data		
	扩展数据		
	AttrNum	Attr List * N	
	属性数量	属性列表	
		属性 ID	ZCL 状态
字节数	1	2	1

属性数量：修改无效的属性数量，返回仅包含修改无效的属性，如果该值为 0 则全 OK。

属性 ID：修改的属性 ID

ZCL 状态：错误原因，见 3.6 章节《ZCL 错误状态码》

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

① 修改目标设备波特率

发送命令：55 13 02 01 00(发送模式) 78 B8(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 08 FC(簇 ID) 00 20(厂商码) 00(应答模式) 01(属性数量) 00 00(属性 ID) 23(数据类型) 80 25 00 00(波特率) B4

反馈命令：55 05 02 01 00(状态成功) A2(帧序号) A1

发送确认：55 0A 8F 02 00(发送模式) 78 B8(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 00(发送成功) EE

接收返回：55 12 82 01 00(对方模式) 78 B8(源短地址) 01(源端口) A2(帧序号) 01(命令方向) 08(簇 ID) 00 20(厂商码) FF (RSSI) 01(属性个数) 00 00(属性 ID) 88(ZCL 错误) 43

备注：因修改设备波特率不支持直接修改，需要使用发送控制命令进行修改。故直接使用修改属性命令设置不成功，返回 0x88 错误“只读”。

② 修改透传目标短地址

发送命令：55 13 02 01 00(发送模式) 78 B8(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 08 FC(簇 ID) 00 20(厂商码) 00(应答模式) 01(属性数量) 01 00(属性 ID) 21(数据类型) FD FF (透传目标短地址) 97

反馈命令：55 05 02 01 00(状态成功) A2(帧序号) A1

发送确认：55 0A 8F 02 00(发送模式) 78 B8(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 00(发送成功) EE

收到返回：55 0F 82 01 00(对方模式) 78 B8(源短地址) 01(源端口) A2(帧序号) 01(命令方向) 08(簇 ID) 00 20(厂商码) FF (RSSI) 00(属性个数) CA

备注：修改成功，返回修改失败的属性个数为 0 个

③ 修改透传目标端口

发送命令：55 13 02 01 00(发送模式) 78 B8(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 08 FC(簇 ID) 00 20(厂商码) 00(应答模式) 01(属性数量) 02 00(属性 ID) 20(数据类型) 11(透传目标端口) 86

反馈命令：55 05 02 01 00(状态成功) A2(帧序号) A1

发送确认：55 0A 8F 02 00(发送模式) 78 B8(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 00(发送成功) EE

收到返回：55 0F 82 01 00(对方模式) 78 B8(源短地址) 01(源端口) A2(帧序号) 01(命令方向) 08(簇 ID) 00 20(厂商码) FF (RSSI)

00(属性个数) CA

④　修改透传模式

发送命令：55 13 02 01 00(发送模式) 78 B8(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 08 FC(簇 ID) 00 20(厂商码) 00(应答模式) 01(属性数量) 03 00(属性 ID) 10(数据类型) 01(透传模式) A7

反馈命令：55 05 02 01 00(状态成功) A2(帧序号) A1

发送确认：55 0A 8F 02 00(发送模式) 78 B8(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 00(发送成功) EE

收到返回：55 0F 82 01 00(对方模式) 78 B8(源短地址) 01(源端口) A2(帧序号) 01(命令方向) 08(簇 ID) 00 20(厂商码) FF (RSSI) 00(属性个数) CA

⑤　修改低功耗等级

发送命令：55 13 02 01 00(发送模式) 78 B8(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 08 FC(簇 ID) 00 20(厂商码) 00(应答模式) 01(属性数量) 04 00(属性 ID) 30(数据类型) 01(功耗等级) B7

反馈命令：55 05 02 01 00(状态成功) A2(帧序号) A1

发送确认：55 0A 8F 02 00(发送模式) 78 B8(目标短地址) 01(目标端口) A2(帧序号) 00(命令方向) 00(发送成功) EE

收到返回：55 0F 82 01 00(对方模式) 78 B8(源短地址) 01(源端口) A2(帧序号) 01(命令方向) 08(簇 ID) 00 20(厂商码) FF (RSSI) 01(属性个数) 04 00(属性 ID) 88(ZCL 错误) 70

备注：修改设备低功耗等级需要使用发送控制命令进行修改。

4.4.6 查询属性上报规律

命令码：0x02

功能：

查询属性自动上报的规律，前提是被查询的属性支持自动上报

输入：

名称	ext data	
	扩展数据	
	AttrNum	AttrIDList
	属性数量	属性 ID 列表
字节数	1	2*N

属性数量：查询的属性数量。

属性列表：查询的属性的 ID

返回：

名称	ext data						
	扩展数据						
	AttrNum	AttrList * N					
	属性数量	属性列表					
		属性 ID	ZCL 状态	最小时间	最大时间	数据类型	变量值
字节数	1	2	1	2	2	1	对齐变长

属性数量：返回查询的属性数量

属性 ID：返回的属性 ID

ZCL 状态：见《ZCL 错误状态码》，只有“操作成功”才有后面的数据

最小时间：该属性连续上报的最小间隔时间，该时间可以过滤状态值连续抖动导致数据上报。

最大时间：该属性上报的最大间隔时间，可作为心跳周期使用

数据类型：变量值的数据类型，见《ZCL 数据类型表》

变量值：属性值变化超过变量值触发上报，该值需按照《ZCL 数据类型表》中“Report 对齐”中的大小，按 4 字节进行对齐。

指令示例（暂无）

4.4.7 修改属性上报规律

命令码：0x03

功能：

修改属性自动上报规律，前提是被查询的属性支持自动上报，设置失败的属性会出现在返回命令中

输入：

名称	ext data					
	扩展数据					
	AttrNum	AttrList * N				
	属性数量	属性列表				
		属性 ID	最小时间	最大时间	数据类型	变量值
字节数	1	2	2	2	1	对齐变长

属性数量：设置的属性数量

属性 ID：设置的属性 ID

最小时间：该属性连续上报的最小间隔时间，该时间可以过滤状态值连续抖动导致数据上报。

最大时间：该属性上报的最大间隔时间，可作为心跳周期使用

数据类型：变量值的数据类型，见《ZCL 数据类型表》

变量值：属性值变化超过变量值触发上报，该值需按照《ZCL 数据类型表》中“Report 对齐”中的大小，按 4 字节进行对齐。

如果对齐长度为 0，则该属性不需要设置变量值。

返回：

名称	ext data		
	扩展数据		
	AttrNum	AttrList * N	
	属性数量	属性列表	
		属性 ID	ZCL 状态
字节数	1	2	1

属性数量：该数量仅包含设置无效的属性数量

属性 ID：设置无效的属性 ID

ZCL 状态：错误原因，见《ZCL 错误状态码》

指令示例（暂无）

4.4.8 查看全部属性

命令码：0x04

功能：

查看目标设备支持的全部属性，可分多包进行查看。

输入命令格式：

名称	ext data	
	扩展数据	
	AttrNum	AttrID
	属性数量	起始属性 ID
字节数	1	2

属性数量：期望查询的属性个数 01

起始属性 ID：从起始的属性 ID 开始查

反馈命令格式：

名称	ext data			
	扩展数据			
	End Flag	AttrNum	AttrList * N	
	结束标志	属性个数	查询列表	
			属性 ID	数据类型
字节数	1	1	2	1

结束标志：返回的查询结果中，包含了该 cluster 下最后一个属性

属性个数：本次查询返回的属性个数

属性 ID：返回的属性 ID

数据类型：该属性 ID 对应的数据类型，见数据类型表

命令示例：（紫色：负载长度　红色：命令类型+命令码　蓝色：校验码）

发送命令：55 11 02 04 00(发送模式) 6C 35(目标短地址) 01(目标端口) 95(帧序号) 00(命令方向) 08 FC(簇 ID) 00 20(厂商码) 00(应答模式) 08(读取个数) 00 00(起始属性 ID) 17

反馈命令：55 05 02 04 00(状态成功) 95(帧序号) 93

发送确认：55 0A 8F 02 00(发送模式) 6C 35(目标短地址) 01(目标端口) 95(帧序号) 00(命令方向) 00(发送成功) 40

收到返回：55 1F 82 04 20(对方模式) 6C 35(源短地址) 01(源端口) 95(帧序号) 01(命令方向) 08 FC(簇 ID) 00 20(厂商码) BD(RSSI) 01(结束标志) 05(属性个数) 00 00(属性 ID) 23(数据类型) 01 00(属性 ID) 21(数据类型) 02 00(属性 ID) 20(数据类型) 03 00(属性 ID) 10(数据类型) 04 00(属性 ID) 30(数据类型) 01

4.4.9 查看全部属性（带扩展）

命令码：0x05

功能：

查看目标设备支持的全部属性，返回查询结果中包含各个属性是否支持可写和主动上报。

输入命令格式：

名称	ext data	
	扩展数据	
	AttrNum	AttrID
	属性数量	起始属性 ID
字节数	1	2

属性数量：期望查询的属性个数

起始属性 ID：从起始的属性 ID 开始查

反馈命令格式：

名称	ext data				
	扩展数据				
	End Flag	AttrNum	AttrList * N		
	结束标志	属性个数	查询列表		
			属性 ID	数据类型	操作
字节数	1	1	2	1	1

结束标志：返回的查询结果中，包含了该 cluster 下最后一个属性

属性个数：本次查询返回的属性个数

属性 ID：返回的属性 ID

数据类型：该属性 ID 对应的数据类型，见《数据类型表》

操作：bit0-可读，bit1-可写，bit2-支持主动上报

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送查看设备全部状态(增强):

发送命令：55 11 02 05 00(发送模式) E9 8E(目标短地址) 01(目标端口) 95(帧序号) 00(命令方向) 08 FC(簇 ID) 00 20(厂商码) 00(应答模式) 08(读取属性个数) 00 00(起始属性 ID) 28

反馈命令：55 05 02 05 00(状态成功) 95(帧序号) 92

发送确认：55 0A 8F 02 00(发送模式) E9 8E(目标短地址) 01(目标端口) 95(帧序号) 00(命令方向) 00(发送成功) 7E

收到返回：55 24 82 05 00(对方模式) E9 8E(源短地址) 01(源端口) 95(帧序号) 01(命令方向) 08 FC (簇 ID) 00 20(厂商码) FF(RSSI) 01(结束标志) 05(属性个数) 00 00(属性 ID) 23(数据类型) 01(操作只读) 01 00(属性 ID) 21(数据类型) 03(操作可读写) 02 00(属性 ID) 20(数据类型) 03(可读写) 03 00(属性 ID) 10(数据类型) 03(操作可读写) 04 00(属性 ID) 30(数据类型) 01(操作只读) 5F

备注：由于代表波特率和低功耗等级的属性为“只读”，故之前测试“修改属性”这两项不成功

4.4.10 状态主动上报

命令码：0x0A

功能：

设备自动上报属性，属性状态值变化超过变量值，或到达最大时间，会上报状态值。

接收：

名称	ext data			
	扩展数据			
	AttrNum	AttrList * N		
	属性数量	属性列表		
		属性 ID	数据类型	数据值
字节数	1	2	1	变长

属性数量：读到的属性数量，如果设备部支持读命令中包含的某些属性 ID，返回命令也不包含这些属性。

属性 ID：读到的 16 位属性 ID

数据类型：数据类型，见《数据类型表》

数据值：该属性对应的状态值，大小由数据类型中“字节数”一项决定

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

接收数据透传模组的心跳包：（心跳包内容为透传模组的低功耗等级）

收到命令：55 13 82 0A 20(对方模式) 0F DC(源短地址) 01(源端口) 08(帧序号) 01(命令方向) 08 FC(簇 ID) 00 20(厂商码) 9C(信号强度) 01(属性个数) 04 00(属性 ID) 30(数据类型) 01(数据值) 0F

4.4.11 默认返回帧

命令码：0x0B

功能：

目标设备返回的默认返回帧，目标设备不支持该命令，或发送短开启了 Default Request 作应答，都会触发该返回帧。该命令的帧序号用于溯源对应的发送命令

接收：

名称	ext data	
	扩展数据	
	ZCL status	Cmd ID
	ZCL 状态	命令 ID
字节数	1	1

ZCL 状态：见 3.6《ZCL 错误状态码》

命令 ID：返回对应的命令 ID，该值仅对“控制命令”有意义，对于其它涉及属性状态的命令没有意义，属性状态命令通过帧序号来回溯。

4.4.12 发送控制命令

命令码：0x0F

功能：

发送设备控制命令，每条命令可携带变长的命令参数，命令参数是相对属性状态比较复杂，可以是多个变量，也可以是数组，也可以是数据流。对错误的设备发送错误的控制命令，或者输入命令中的“应答模式”设置为 0，会收到默认返回帧，可以通过默认返回帧中的 cmd ID 和帧序号来检测是否与发送的控制命令对应。

发送控制命令格式：

名称	ext data	
	扩展数据	
	Cmd ID	Cmd param
	命令 ID	命令参数
字节数	1	变长

命令 ID：控制命令的命令 ID

命令参数：控制命令携带的参数，命令参数内容，根据 cluster，cmd ID，manufacture Code 的不同而决定

接收控制命令格式：

名称	ext data

	扩展数据	
	Cmd ID	Cmd param
	命令 ID	命令参数
字节数	1	变长

命令 ID：收到的控制命令的命令 ID

命令参数：收到的控制命令携带的参数，命令参数内容，根据 cluster，cmd ID，manufacture Code 的不同而决定

指令示例：由于发送控制命令与接收控制命令具有相关性，故在接收控制命令中合并发送命令的示例

4.4.13 接收控制命令

命令码：0x0F

功能：

接收控制命令，收到的控制命令可能是发送命令的返回消息，也有可能是远端设备主动通知。可通过帧序号来判断收到的控制命令是否发送命令的返回消息。通常受控设备收到控制命令后，不返回控制命令就返回默认返回帧。

接收：

名称	ext data	
	扩展数据	
	Cmd ID	Cmd param
	命令 ID	命令内容
字节数	1	变长

命令 ID：收到的控制命令的命令 ID

命令内容：收到的控制命令携带的参数内容，根据 cluster，cmd ID，manufacture Code 的不同而决定

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

控制对象：E18 无线数传模组

① 发送**控制命令**修改透传模组**波特率**:

发送命令：55 10 02 0F 00(发送模式) CB A6(目标短地址) 01(目标端口) AB(帧序号) 00(命令方向) 08 FC(簇 ID) 00 20(厂商码) 00(应答模式) 02 (命令 ID) 80 25 00 00(命令参数=波特率) B9

反馈命令: 55 05 02 0F 00(状态成功) AB(帧序号) A6

发送确认：55 0A 8F 02 00(发送模式) CB A6(目标短地址) 01(目标端口) AB(帧序号) 00(命令方向) 00(发送成功) 4A

收到返回：55 14 82 0F 20(对方模式) CB A6(源短地址) 01(源端口) AB(帧序号) 01(命令方向) 08 FC(簇 ID) 00 20(厂商码) FC (RSSI) 02(命令 ID)　00(命令参数 1=执行成功)　80 25 00 00(命令参数 2=波特率) E4

② 发送**控制指令**修改透传模组**低功耗等级**:

发送命令：55 10 02 0F 00(发送模式) 2B DC(目标短地址) 01(目标端口) AA(帧序号) 00(命令方向) 08 FC(簇 ID) 00 20(厂商码) 00(应答模式) 03(命令 ID) 03(命令参数=功耗等级) 85

反馈命令：55 05 02 0F 00(状态成功) AA(帧序号) A7

发送确认：55 0A8F 02 00(发送模式) 2B DC(目标短地址) 01(目标端口) AA(帧序号) 00(命令方向) 00(发送成功) D1

接收返回：55 10 82 0F 20(对方模式) 2B DC(源短地址) 01(源端口) AA(帧序号) 01(命令方向) 08 FC(簇 ID) 00 20(厂商码) FC (RSSI) 03(命令 ID) 00(命令参数=执行成功) DB

③ 广播**控制指令**用于**标记设备**：（广播控制时可能会受到干扰或数据堵塞）

发送命令：55 11 02 0F 00(发送模式) FD FF(广播目标短地址) FF(广播目标端口) A1(帧序号) 00(命令方向) 03 00(簇 ID) 00 00(厂商码) 00(应答模式) 00(命令 ID) 00 00(命令参数=持续时间) 53

反馈命令：55 05 02 0F 00(状态成功) A1(帧序号) AC

发送确认：55 0A 8F 02 00(发送模式) FD FF(目标短地址) FF(广播目标端口) A1(帧序号) 00(命令方向) 00(广播成功) D1

备注: IDENTIFY 簇用于标记设备，设备在标记状态下，E18 透传模块指示灯会进行闪烁

④ 接收**控制指令**模块**透传数据**发送过来的“HelloWorld”

收到命令：55 19 82 0F 20(对方模式) CC 52(源短地址) 01(源端口) 10(帧序号) 01(命令方向) 08 FC(簇 ID) 00 20(厂商码) DA(RSSI) 00(命令 ID) 48 65 6C 6C 6F 57 6F 72 6C 64(命令参数=HelloWorld) 2D

4.4.14 ZCL 属性与控制

按照簇（ClusterID）分类，对各个簇下的属性和控制命令进行列举

4.4.14.1 Cluster=0x0000

功能：该簇定义了设备的出厂信息，几乎所有的设备都必须支持该簇（BASIC 簇）

属性表：

Cluster = 0000，Server				
AttrID	描述符	名称	数据类型	操作
0x0000	ZCL Version	ZigBee 版本	uint8	只读
0x0001	Application Version	软件版本	uint8	只读
0x0002	Stack Version	协议版本	uint8	只读
0x0003	Hardware Version	硬件版本	uint8	只读
0x0004	Manufacturer Name	厂商名称	string	只读
0x0005	Modle Identifier	产品型号	string	只读
0x0006	Date Code	编译日期	string	只读
0x0007	Power Source	电源方式	enum8	只读

4.4.14.2 Cluster=0x0003

功能：用于标记设备，设备在标记状态下，可被人肉发现，也可被其它 ZigBee 设备发现并与它建立常连接（IDENTIFY 簇）

属性表：

Cluster = 0003，Server				
AttrID	描述符	名称	数据类型	操作
0x0000	Identify Time	标记时间	Uint16	读写

发送控制命令：

Cluster = 0003，Client->Server			
cmdID	描述符	名称	参数
0x00	Identify	标记设备	uint16 IdentifyTime: 标记模式持续时间

接收控制命令：

Cluster = 0003，Sever->Client

cmdID	描述符	名称	参数
0x00	IdentifyQueryresponse	返回查询标记设备	uint16 timeout：剩余标记时间

4.4.14.3Cluster=0x0004

功能：

用于设备的分组管理

属性表：

Cluster = 0004，Server				
AttrID	描述符	名称	数据类型	操作
0x0000	NameSupport	支持分组命名	bit8	只读

“支持分组命名”可以在设备加组时，在设备中保存一个字符串的分组名称，实际价值不大

发送控制命令：

Cluster = 0004，Client->Server			
cmdID	描述符	名称	参数
0x00	AddGroup	设备加组	uint16 groupID：设备加组的组 ID string name：分组名称
0x01	ViewGroup	查询组信息	uint16 groupID：被查询的组 ID（查分组名用）
0x02	GetMembership	查看（全部）分组	uint8 count：查询分组数，查全部时填 0 uint16 groupList[ ]：待查询的分组数组
0x03	RemoveGroup	移除一个分组	uint16 groupID：移除组的组 ID
0x04	RemoveAll	删除全部分组	无
0x05	AddGroupIdentify	标记状态设备加组	uint16 groupID：设备加组的组 ID string name：分组名称

- 设备加组时，分组名称可以不加，只需要组 ID 就够了，实在要加，连头不超过 16 个字符。
- 查看分组时，count 填 0 查询全部分组，非 0 则查询 groupList 中的分组是否存在于在设备中。
- 查询组信息命令用于查询分组名，没多大作用。
- 标记状态设备加组建议使用广播发送，该命令无对应返回，单播时只能收到“默认返回”

接收控制命令：

Cluster = 0004，Sever->Client			
cmdID	描述符	名称	参数
0x00	AddGroupRsp	设备加组返回	uint8 status：ZCL 状态 uint16 groupID：设备加组的组 ID
0x01	ViewGroupRsp	查询组信息返回	uint8 status：ZCL 状态 uint16 groupID：被查询的组 ID string name：查询到的分组名称
0x02	GetMembershipRsp	查看（全部）分组返回	uint8 capacity：还能加多少组 uint8 count：设备加组数量 uint16 groupList[ ]：设备加入的分组
0x03	RemoveGroupRsp	移除一个分组返回	uint8 status：ZCL 状态 uint16 groupID：移除组的组 ID

4.4.14.4 Cluster=0xFC08

功能：亿佰特数据透传专用

属性表：

Cluster = 0xFC08，manuCode=0x2000, Server				
AttrID	描述符	名称	数据类型	操作
0x0000	Baud	波特率	uint32	只读
0x0001	targetAddr	默认目标短地址	uint16	读写
0x0002	targetEP	默认目标端口	uint8	读写
0x0003	sendMode	透传模式	bool	读写
0x0004	LP Level	低功耗模式	enum8	只读

波特率支持 9600，19200，38400，57600，115200

透传模式：0-命令模式，1-透传模式

低功耗模式：0 -1 秒唤醒（心跳包 2 分钟），1 - 3.33 秒唤醒（心跳包 4 分钟），2 - 5 秒唤醒（心跳包 6 分钟），3 - 一直休眠（有 8 分钟的心跳包）

发送控制命令：

Cluster = 0xFC08，manuCode=0x2000, Client->Server			
cmdID	描述符	名称	参数
0x00	UartSend	透传发送	uint8 data[]: 透传数据
0x01	SetDstAddr	设置默认目标	uint16 dstAddr: 目标短地址 uint8 endpoint: 目标端口
0x02	SetBaud	设置波特率	uint32 baud: 设置的新波特率，重启生效
0x03	SetLP_Level	设置低功耗模式	uint8 LP_level: 低功耗等级
0x04	Reset	模组重启	uint8 extAddr[8]: 模组的 MAC 地址

波特率需设置正确值，所以不能直接修改属性

低功耗模式需设置正确值，所以不能直接修改属性

模组重启不能广播发送，需要填对 MAC 地址，即使广播也只能重启一个

接收控制命令：

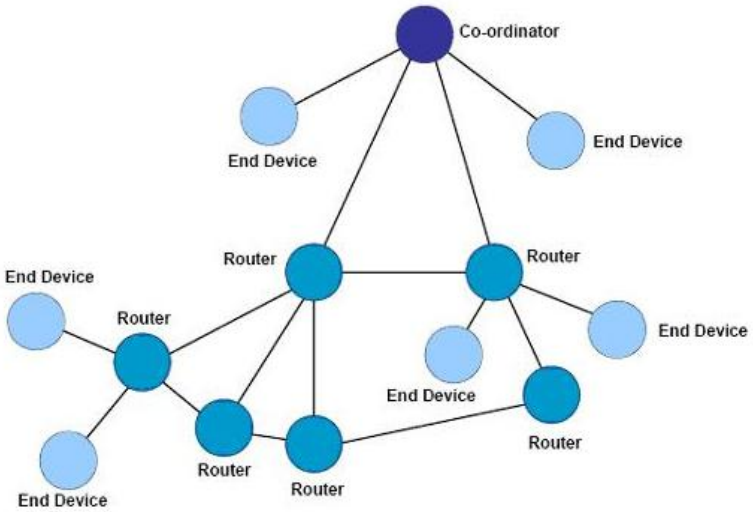
Cluster = 0xFC08，manuCode=0x2000, Sever->Client			
cmdID	描述符	名称	参数
0x00	UartNotify	透传接收	uint8 data[]: 透传数据
0x01	SetDstAddrRsp	设置默认目标返回	uint8 status: ZCL 状态
0x02	SetBaudRsp	设置波特率返回	uint8 status: ZCL 状态
0x03	SetLP_LevelRsp	设置低功耗返回	uint8 status: ZCL 状态

5.用户须知

5.1 ZigBee 网络角色以及注意事项

序号	描述
1	本模块采用 ZigBee 网络组网，仅实现协调器、路由器功能。
2	Zigbee 网络为 Mesh 结构，不受网络深度影响，路由节点接入越多支持的子节点越多。（终端子节点总数 48，最大组网数 200）
3	协调器可为休眠终端保存数据 7 秒。
4	广播性能：5 秒内最大广播不超过 100 包，实际取决于接入设备的广播接收能力。
5	协调器在网络中是唯一的，短地址固定为 0000。
6	若点播地址为 FFFF，FFFD，FFFC，则分别对应三种广播模式。若需要组播发送，目标端口设置为 0，目标短地址设置为组 ID。
7	网络参数 PANID 为 FFFF 时为自动生成 PANID，若需要手动设置 PANID 需要保证空间内无该 PANID 的协调器和路由器存在，包括上次加入过本协调器的路由器。
8	网络中所有设备都开启了广播功能，多个设备同时广播或单个设备较高频率的广播都可能导致网络严重堵塞，请尽量避免这种情况。
9	所有的无线命令都会产生发送确认，发送目标不同发送确认的返回时间也不同，甚至出现乱序。向某个具体目标发送无线命令后建议等待发送确认再向该目标发送下一条命令。但是向多个不同目标发送命令则不需要等待发送确认即可给下一个目标发送命令。比如在发送目标中有路由节点和休眠节点时，路由节点的返回比休眠节点快。
10	ZigBee 网络中通信，单包数据发送周期不能过快（一般建议在 1 秒以上，或等待该设备的发送确认或异步返回），过快可能造成数据的丢失。（特别注意，网络中节点太多，广播周期过快可能会造成网络不稳定。）
11	根据节点入网通知和设备信息通知，判断入网节点是第一次入网还是网络恢复。有第一次入网记录的设备可以算作合法设备。在删除节点时如果节点刚好关机或不在线，可以认为这个设备已经非法了，下次再次收到该设备的任何信息（包括入网通知不是第一次入网）立即发送删除指令

5.2 网络结构

本模块网络结构为网状网结构（MESH）
MESH 网状网络拓扑结构的网络具有强大的功能，网络可以通过“多级跳”的方式来通信；该拓扑结构还可以组成极为复杂的网络；网络还具备自组织、自愈功能；
网络结构图 

5.3 设备通信入门

5.3.1 设置协调器

上位机软件连接协调器模组：

1、选择相应串口；

2、选择当前使用的模块型号（组网管理器）

3、选择波特率（组网管理器为 230400）；

4、打开串口；

图 5-1

配置协调器模式

1、　读取当前模块参数，返回有效长地址；

2、　选择需要设置的设备类型（当前我们选择协调器）；

3、　设置软启动模式（建议选择“自动”）

4、　写入参数（把设置的设备类型写入模块）；

5、　配置完成后，要 Reset 复位或重新上电组网管理器模组

图 5-2

协调器新建网络

1、　设置信道，可使能，除能和覆盖三种方式，不选则为只读当前使能信道，建议选择除能。

2、　选择要使用的信道，如需要除能 11 信道，就点亮 11

3、 点击信道按钮设置信道，当前为除能模式，配置信道成功后信道列表中被使能的信道会被点亮。

4、 点击打开网络，等待协调器创建网络后会显示“打开网络成功”。

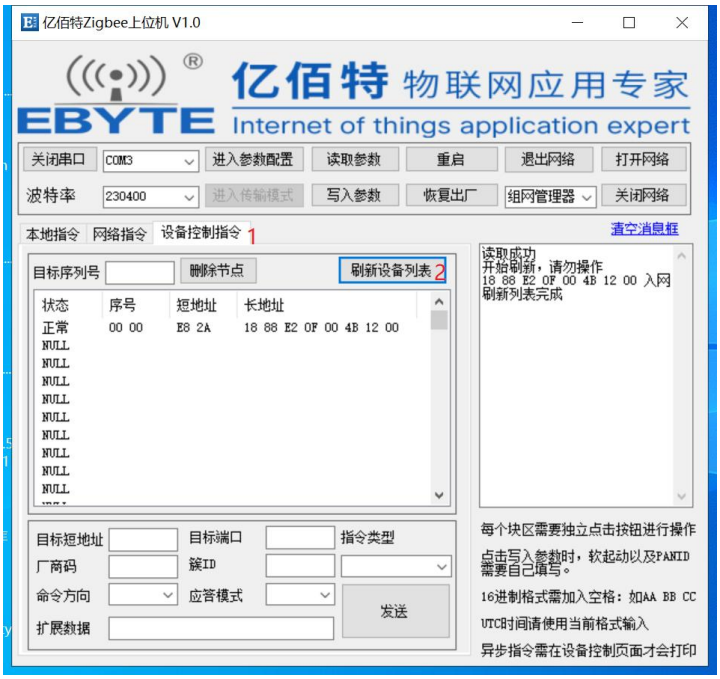
5、 点击读取参数，会获得协调器的 PANID，短地址，拓展 ID，当前工作信道，网络状态显示已组网

5.3.2 设备入网与控制

设备组网

1、在打开网络成功后的 180 秒内，切换到设备控制指令界面。

2、在入网设备端操作加网（按键或控制指令），然后点击刷新设备列表，可反复操作直到设备列表显示有对应入网的设备 MAC 地址为止，消息框中会显示新加设备的 MAC 地址。



向入网设备发送 Identify 指令

1、 输入目标短地址

2、 输入目标端口，目标是 E18 数传模组，只有端口 1 可用

3、 指令类型为控制指令

4、 Identify 指令为标准指令，的厂商码为 0。

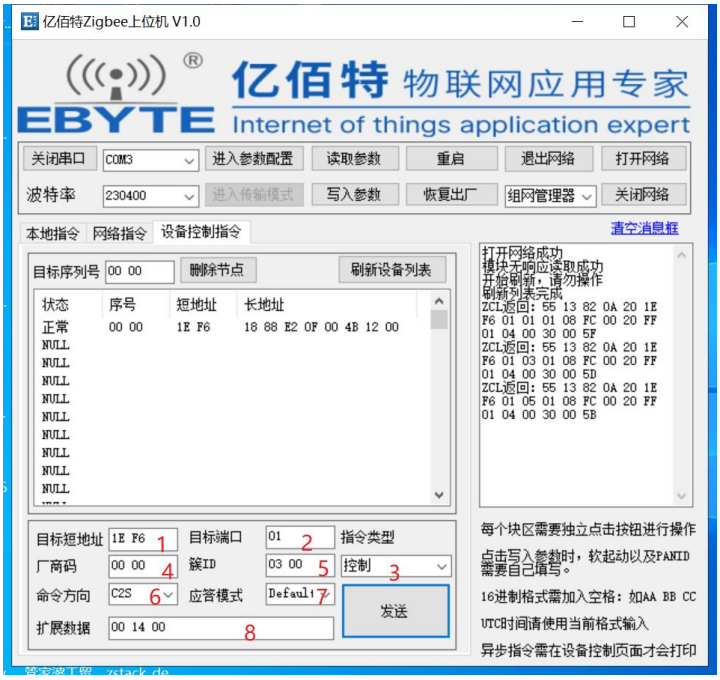
5、 Identify 指令的属于 cluster 0x0003 的指令集，输入小端模式，应为 03 00

6、 Identify cluster 位于目标设备的输入端，目标设备为受控端，因此选择 C2S

7、 应答模式选择 Default

8、 Identify 命令的命令 ID 为 0x00，命令参数为 2 字节（小端模式）的 Identify 时间，故输入 00 14 00，即持续 20 秒的 Identify

9、 点击发送，可以看到 E18 模组的 LED 在闪烁，说明 E18 模组进入了 Identify 模式。该模式下 E18 模组可以被肉眼看到，也可以被其它 ZigBee 节点找到。



查询 E18 模组的参数

1、 输入目标 E18 模组的短地址

2、 输入目标端口 01

3、 输入私有协议的厂商码 0x2000，小端模式下应输入 00 20

4、 输入亿佰特透传簇，该簇的 cluster ID 为 0xFC08，输入小端模式 08 FC

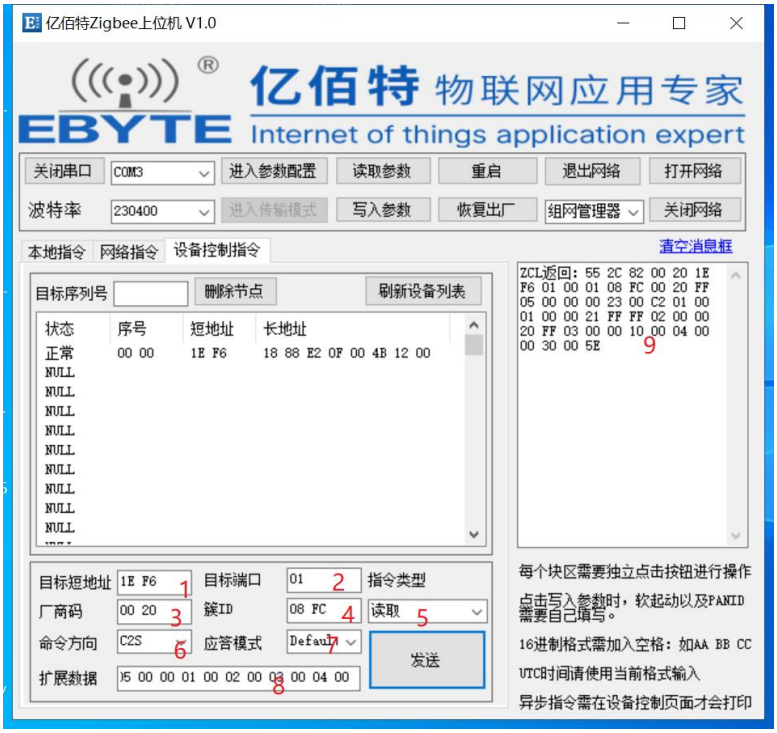
5、 指令类型选择读取

6、 命令方向 C2S

7、 应答模式 Default

8、 读取亿佰特透传 cluster 下的 5 个属性 0x0000, 0x0001，0x0002, 0x0003, 0x0004，因此输入 05 00 00 01 00 02 00 03 00 04 00

9、 点击发送后收到返回消息，簇 0xFC08 下的属性 0x0000 的值为 00 C2 01 00，对应波特率 115200；属性 0x0001 值为 FF FF，对应透传目标地址为 0xFFFF 即广播透传；属性 0x0002 值为 FF，对应目标端口为 0xFF 即广播端口；属性 0x0003 值为 00，对应透传模式为 FALSE；属性 0x0004 值为 0，对应低功耗等级为最快的 1 秒唤醒一次。



设置 E18 为透传

1、 输入目标 E18 模组的短地址

2、 输入目标端口 01

3、 输入私有协议的厂商码 0x2000，小端模式下应输入 00 20

4、 输入亿佰特透传簇，该簇的 cluster ID 为 0xFC08，输入小端模式 08 FC

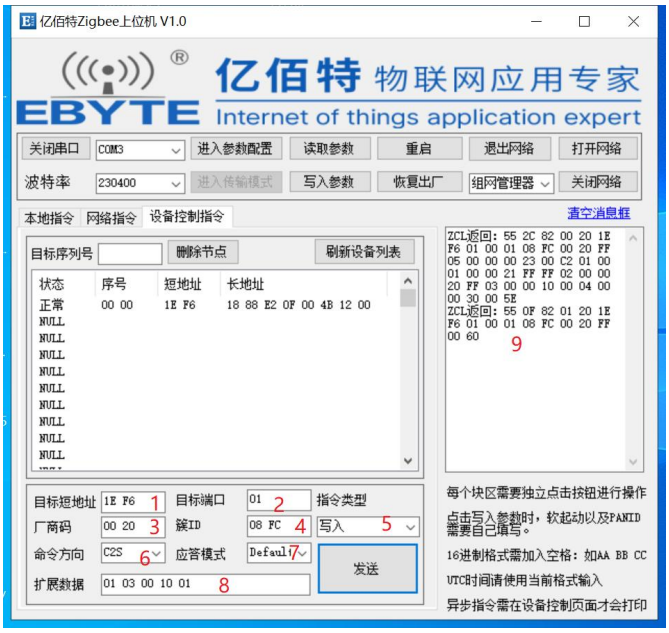
5、 指令类型选择写入

6、 命令方向 C2S

7、 应答模式 Default

8、 修改透传模式对应的属性 0x0003，根据读取命令发现属性 0x0003 的数据类型为 0x10（BOOl 型），需要修改其值为 TRUE，故输入 01 03 00 10 01，

9、 点击发送后收到返回消息，修改失败的属性共 0 条，故认为修改透传模式成功。



向 E18 模组发送透传数据

1、 设输入目标 E18 模组的短地址

2、 输入目标端口 01

3、 输入私有协议的厂商码 0x2000，小端模式下应输入 00 20

4、 输入亿佰特透传簇，该簇的 cluster ID 为 0xFC08，输入小端模式 08 FC

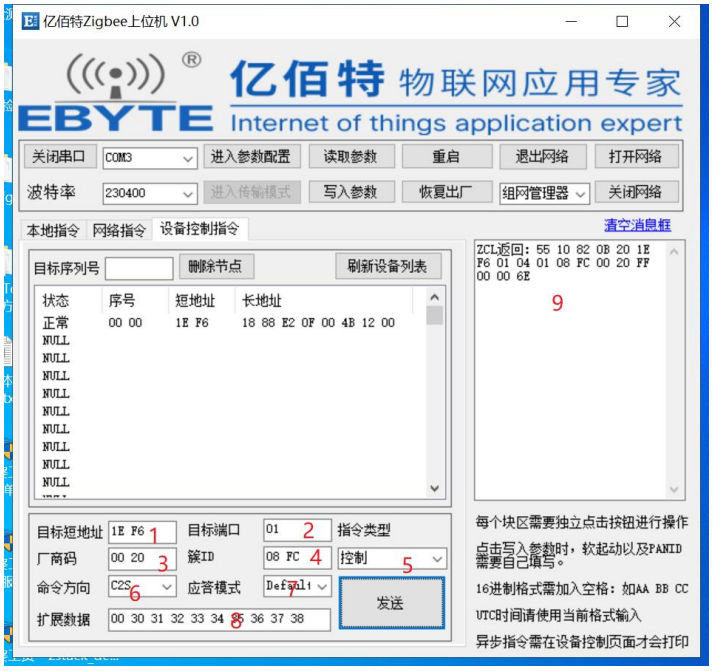
5、 指令类型选择控制

6、 命令方向 C2S

7、 应答模式 Default

8、 输入透传发送的命令 ID 0x00，以及要透传的数据 31 32 33 34 35 36 37 38，然后点发送

9、 消息框收到默认返回帧，状态为 0x00 表示 E18 收到并正确执行了该命令，命令 ID 为 0x00。同时在 E18 的一端可以看到打印的透传字符串”12345678”

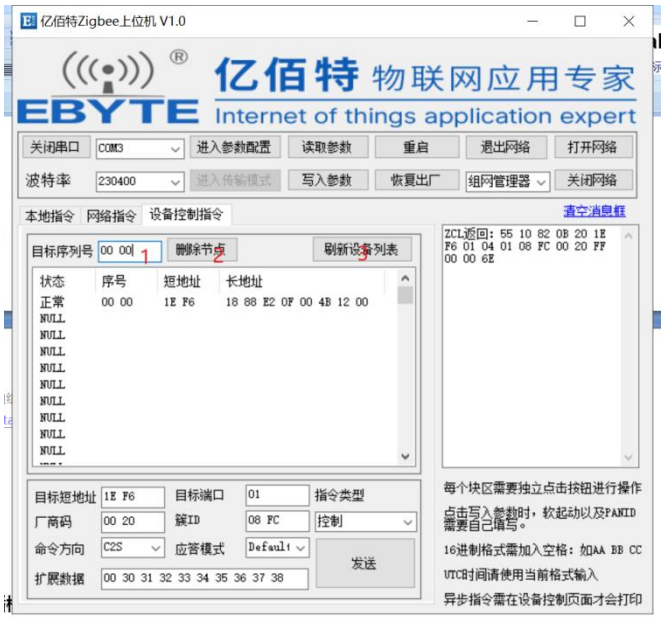


删除已组网的设备

1，　根据设备列表中的序号，在目标序号中输入要删除的设备的序号

2，　点击删除节点

3，　然后刷新设备列表，设备列表中如果再无显示，说明删除成功



删除后，设备列表中不再显示先前入网的设备，被删除的目标设备也变成“未组网”状态

5.3.3 广播模式

三种广播模式下各类型设备接收数据区分表：

广播模式	设备类型		
	路由	终端	休眠终端

0xFFFF	Yes	Yes	Yes
0xFFFD	Yes	Yes	No
组播	Yes	Yes	No
0xFFFC	Yes	No	No

备注：用户使用广播模式通信步骤

1、设置目标短地址：0xFFFF（全网所有设备接收）、0xFFFD（除休眠终端以外所有设备接收）、0xFFFC（除休眠终端、终端设备以外所有设备接收）；

2、设置目标端口：目标端口默认设置为“FF”；

3、进入传输模式后即可开始进行数据广播（出厂数据传输模式默认“0xFFFF”模式广播）；

6.定制合作

★公司客户如需进行产品定制，请联系我司。

★亿佰特已与多家知名企业达成深度合作。

7. 关于我们

亿佰特（EBYTE）是一家专业提供无线数传方案及产品的公司

- ◆自主研发数百个型号的产品及软件；
- ◆无线透传、WiFi、蓝牙、Zigbee、PKE、数传电台……等多系列无线产品；
- ◆拥有近百名员工，数万家客户，累计销售产品数百万件；
- ◆业务覆盖全球 30 多个国家与地区；
- ◆通过了 ISO 9001 质量管理体系、ISO 14001 环境体系认证；
- ◆拥有多项专利与软件著作权，通过国际 FCC/CE/ROHS 等权威认证。

最专业的无线应用
微信公众平台
免费样品 技术资讯

【公司电话】028-61399028　　【公司传真】028-64146160
【官方网站】www.ebyte.com　　【在线商城】cdebyte.taobao.com
【技术支持】support@cdebyte.com　　【李经理】raylee@cdebyte.com
【公司地址】四川省 成都市 高新西区 西芯大道 4 号创新中心 B333-D347