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

E18 系列指令手册
(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（**休眠终端**）或者唤醒，因此它可以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	角色切换	用户可通过串口指令让设备在协调器，路由器和终端的三种类型中任意切换。
2	按需组网	支持按键和指令进行建立网络和查找加入网络。
3	网络自愈功能	失去网络自动重连功能。网络中间节点丢失，其他网络自动加入或保持原网络。（孤立节点自动加入原网络，非孤立节点保持原有网络。） 协调器丢失，原网络存在非孤立节点，协调器可再次加入该网络或者相同用户设置的原网络 PAN_ID 的协调器加入原有网络。
4	超低功耗	设备在终端状态下，可设置为低功耗模式，可根据用户使用时间更改设备休眠时间，低功耗模式下待机功耗小于 2.5uA。在父节点数据保存时间内都能在用户设置时间内接收到自己应当受到的消息。
5	数据保留机制	设备在协调器和路由器状态下，与休眠模式下的终端配合使用，对终端设备的数据进行保存，并在终端休眠唤醒后将数据发送到终端。 最多保存 4 条数据，若超出，将不再保存接收到的数据！数据保存时间过后，数据堆自动清空。
6	自动重发功能	在单播（点播）模式下，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 2 次。
7	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。若模块端无条件做目标地址设置的情况下，协调器可向任意模块指派透传目标。
8	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。相同网络密匙的设备方能正常组网通信。

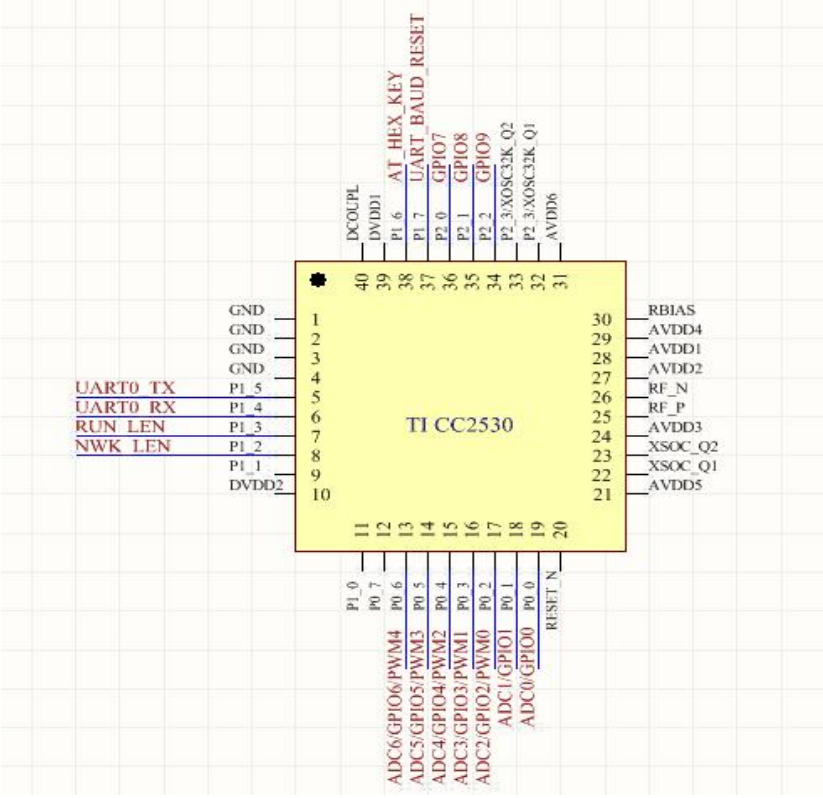
9	支持串口配置	模块内置串口指令，用户可通过出串口指令配置（查看）模块的参数及功能。
10	多类型数据通信	支持全网广播，组播及点播（单播）功能。在广播模式下还支持几种传输方式，详情请参考 5.3.3 章节。
11	信道更改	支持 11~26 等 16 个信道更改（2405~2480MHZ），不同信道对应不同频段。
12	网络 PAN_ID 更改	网络 PAN_ID 的任意切换,用户可自定义 PAN_ID 加入相应网络或者将自动选择 PAN_ID 加入网络。
13	串口波特率更改	用户可自行设置波特率，最高可达 115200，默认位数为 8 位，停止位 1 位，无校验位。
14	短地址收索	用户可根据已加入网络的模块 MAC 地址（唯一的，固定的）查找出相应的短地址。
15	模块复位	用户可通过串口命令对模块进行复位操作。
16	恢复出厂设置	用户可通过串口命令对模块进行出厂设置的恢复。
17	波特率复位	可通过 P1.7 引脚实现波特率复位（115200），在模块上电期间，保持 P1.7 拉低的状态，直到网络指示灯、匹配指示灯都亮起后，P1.7 引脚按键松开，指示灯熄灭，复位完成。注意此过程是在协议栈初始化前执行，所以指示灯熄灭后，请等待 1S 后再对模块进行指令操作。

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	E18-MS1-PCB	CC2530	2.4G	250K	4	PCB
2	E18-MS1- IPX	CC2530	2.4G	250K	4	IPEX
3	E18-MS1PA2-PCB	CC2530	2.4G	250K	20	PCB
4	E18-MS1PA2-IPX	CC2530	2.4G	250K	20	IPEX
5	E18-2G4Z27SP	CC2530	2.4G	250K	27	PCB
6	E18-2G4Z27SI	CC2530	2.4G	250K	27	IPEX
★　E18 系列的无线模块经软件调试好以后均可互通，不同功率可搭配使用　★						

2. 功能及命令结构简介

2.1 功能引脚图

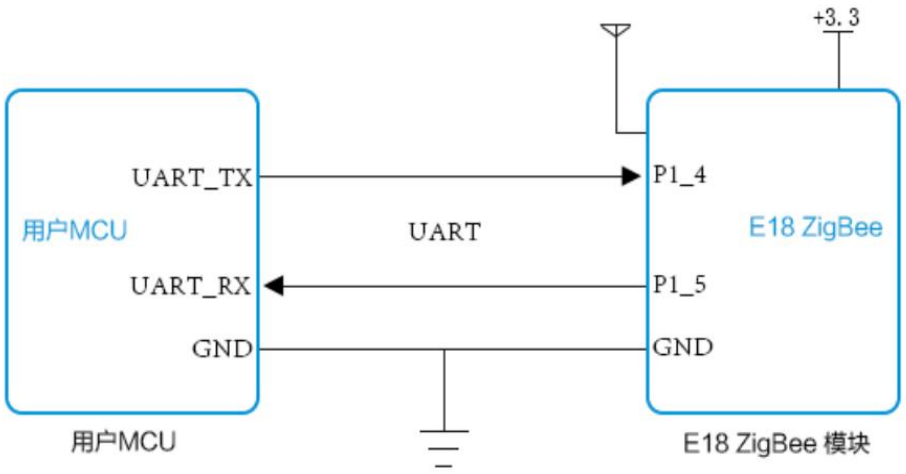


引脚	CC2530 引脚名称	模块 引脚名称	输入/输出	引脚用途
1	GND	GND		地线，连接到电源参考地
2	VCC	VCC		供电电源，必须 1.8～3.6V 之间
3	P2.2	GPIO	I/O	DC-下载程序或Debug时钟接口
4	P2.1	GPIO	I/O	DD-下载程序或Debug数据接口
5	P2.0	GPIO	I/O	N/C
6	P1.7	NWK_KEY	I	用于手动加入、退出、快速匹配按键。 未组网：短按表示加入网络或者创建网络操作； 已组网：短按表示快速匹配； 长按表示离开当前网络； 注：低电平有效，100ms ≤ 短按 ≤ 3000ms，5000 ≤ 长按。
7	P1.6	GPIO	I/O	N/C
8	NC	NC		N/C
9	NC	NC		N/C
10	P1.5	UART0_TX	I	串口 TX 脚

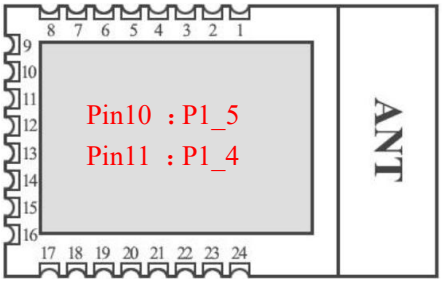
11	P1.4	UART0_RX	O	串口 RX 脚
12	P1.3	RUN_LED	O	用于指示模块入网状态，快闪256（10Hz频率）烁表示正在加入网路或创建网络中，慢闪12次（2Hz频率）表示模块已加入网络或创建网络成功。 低电平点亮；
13	P1.2	NWK_LED	O	用于指示模组的一键配对状态，前提是两个模组要加入同一个协调器，然后才能一键配对，透传模式下相互透传。 低电平点亮；
14	P1.1	GPIO	I/O	模块内部已连接PA发射控制引脚； E18-MS1-PCB/E18-MS1-IPX内部无PA；
15	P1.0	GPIO	I/O	模块内部已连接PA接收控制引脚； E18-MS1-PCB/E18-MS1-IPX内部无PA；
16	P0.7	HGM	O	PA的HGM引脚； E18-MS1-PCB/E18-MS1-IPX内部无PA，此引脚作GPIO口使用；
17	P0.6	GPIO	I/O	N/C
18	P0.5	GPIO	I/O	N/C
19	P0.4	GPIO	I/O	N/C
20	P0.3	GPIO	I/O	N/C
21	P0.2	GPIO	I/O	N/C
22	P0.1	GPIO	I/O	N/C
23	P0.0	GPIO	I/O	N/C
24	RESET	RESET	I	复位端口（低电平有效）

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



E18-MS1 系列

E18 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， E18 P1_4、P1_5 引脚分别为 E18 内部串口的 RX、TX 引脚。具体连接方式如上图所示。

E18 系列模块引脚模块引脚表

1	GND	13	P1.2
2	VCC	14	P1.1
3	P2.2	15	P1.0
4	P2.1	16	P0.7
5	P2.0	17	P0.6
6	P1.7	18	P0.5
7	P1.6	19	P0.4
8	NC	20	P0.3
9	NC	21	P0.2
10	P1.5	22	P0.1
11	P1.4	23	P0.0
12	P1.3	24	RESET

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 3 字节，最大 255 字节。

串口粘包的处理

ZigBee 模块的 TX 输出口，可能会在一个极短的时间段内，连续输出多条指令，包括串口反馈命令和异步命令。上位机收到串口命令时按照连续的“帧头”、“帧长度”、“帧载荷”的方式，从连续收到的命令中提取出完整的帧载荷，再对帧载荷进行处理。上位机可以设计一个超时机制，在 5 个 ms 内如果未收到新的命令，可从新从帧头开始接收命令并提取完整的帧载荷。

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

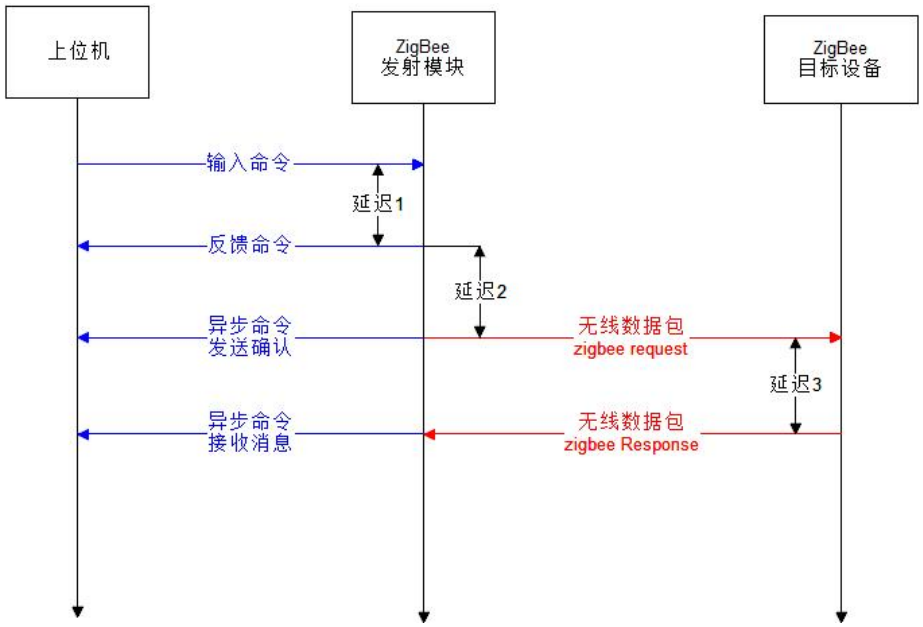
异步命令 TYPE_ZDO_RSP 一定是输入命令 TYPE_ZDO_REQ 导致，但 TYPE_ZDO_REQ 命令不一定产生 TYPE_ZDO_RSP

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。

串口命令的三层返回示意图



- 输入串口命令后，命令先在模块内部 MCU 中处理。若模块正常工作则在延迟 1 后输出反馈命令。延迟 1 约 1~2 毫秒左右，有反馈命令表示模块正常运行。反馈结果见《AF 状态表》。
- 若模块正常运行，串口命令转换成无线信号，并通过射频信号发送出去。由于 ZigBee 的传输速度慢，需要等待延迟 2 后信号才会发送出去。信号无论是否发送出去都会产生发送确认命令，用于诊断信号是否发出去。延迟 2 的时间随机性极大，包括信号传输，路由转发，信号重传，最好的情况几个毫秒，最差可到 20 秒。发送确认的诊断结果见《AF 状态表》
- 信号发送到目标后，目标会返回处理结果的消息。延迟 3 包含了对方设备信号传输的延迟，还有对方设备处理的延迟，如对方设备读写 FLASH，驱动传感器等针对外设的操作。该消息的结果，可参考《ZCL 状态表》

3.3 命令码

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
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
0x0D	CFG_SET_POWER	设置查询发射功率
0x0F	CFG_TEST	测试模式

0x10	CFG_READ_ATTR	读取设备属性
0x11	CFG_WRITE_ATTR	修改设备属性
0x14	CFG_FIND_BIND	自动建立连接

网络管理命令：

0x00	ZDO_NWK_ADDR_REQ	查询节点短地址
0x01	ZDO_IEEE_ADDR_REQ	查询节点 IEEE 地址

设备状态与控制命令：

命令码	描述符	命令名称
0x00	ZCL_READ_ATTR_REQ	读取设备状态
0x01	ZCL_WRTIE_ATTR_REQ	修改设备状态
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
0x04	NOTIFY_NODE_ADDR	模组短地址更新
0x06	NOTIFY_LEAVE	模组离网通知
0x10	NOTIFY_FIND_BIND	自动建立连接

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

接收设备状态与控制：

命令码	描述符	命令名称
0x00	ZCL_READ_ATTR_RSP	读取设备状态
0x01	ZCL_WRTIE_ATTR_RSP	修改设备状态
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

AF 状态表包含在反馈命令和发送确认命令中，用于检测 ZigBee 模组的各种异常。通常在 ZigBee 通信应用中，应保证模组本机正常工作。例如串口写入数据量大于 ZigBee 的传输速率，ZigBee 模组工作在有密集蓝牙或 WIFI 的环境，目标设备掉线，都有可能导致通信异常。用户可根据返回命令的异常状态，判断

导致通信失败的原因。

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
0x1A	MAC 层资源不足
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 ZCL 数据类型表

ZCL 数据类型表用于描述 Zigbee 设备端的属性（Attribute）的数据大小。当使用 ZCL 命令管理目标设备状态时，需要对目标设备的属性（Attribute）进行“读”，“写”，“查”等基础操作时，需要根据目标设备的属性数据类型，处理对应大小的数据值。

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	头为 0xffff	0

			长度总和		
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

3.6 ZCL 错误状态码

ZCL 错误码包含在接收到的返回 ZCL 命令中，当向目标设备发送该错误码代表目标设备收到了控制指令，但是该指令执行无效。

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	

3.7　E18 数传模组的数据结构与数传功能设置

E18 数传模块仅有数据传输功能且只有一个 UART 输入输出口，不具备其它外设控制功能，因此只支持一个 ZigBee 端口，其信息如下。

ZigBee 协议信息	
Endpoint ID	1
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)

透传相关的属性：

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	目标地址	uint16	RW
0x0002	targetEP	目标模式	uint8	RW
0x0003	sendMode	透传模式	bool	RW
0x0004	LP Level	低功耗模式	Enum8	RW

支持的控制命令：

命令 ID	命令方向	描述符	功能
0x00	C2S	Send Data	数据发送
0x01	C2S	Set Target	设置目标
0x02	C2S	Set Baud req	设置波特率
0x03	C2S	Set Low Power	设置低功耗模式

如何设置透传模式：

- 模块自己可以通过“设置本地属性”命令，设置波特率，目标地址，目标模式，透传模式和低功耗模式。
- 如需要远程设置透传，除透传模式可以通过 ZCL 写属性命令来设置，其余的属性必须通过 ZCL 控制命令来写入。特别是波特率只支持 9600,19200,38400,57600 和 115200，如果设置其它值则无效。
- 使用远程命令控制模块，命令中的 manufacture code 务必设置为 0xFC08。
- 为了确保设置的正确性，模块自己可以通过“读取本地属性”命令来查看设置结果和当前串口状态。远程设备则可通过 ZCL 命令查询该模块的透传状态。
- 通过本地指令或远端指令，将透传模式对应的属性设置为 1（TRUE），模块进入透传模式。
- 模块一旦进入透传模式后，串口指令失效，模块本机需要连发 3 个“+”符合退出透传模式。也可以在远程设备上向该模块发送 ZCL 写属性指令，修改透传模式对应的属性为 0（FALSE）。
- 命令模式下的模组可以和透传模式下的模组通信，命令模式下的模组按照 ZCL 命令格式向透传模式下的模组发送“数据发送”命令，透传模式下的模组可以输出命令模式模组的 Payload 部分数据。
- 命令模式下的模组，可接收透传模式下的模组的点播，组播和广播数据，并以 ZCL 接收命令格式输出数据。

目标地址与目标端口设置表：

目标地址	目标端口	透传发送效果
0xFFFF	不等于 0	广播到所有设备，包含休眠终端
0xFFFD	不等于 0	广播到所有非休眠设备
0xFFFC	不等于 0	广播到协调器和所有路由设备
0x0000~0xFFF8	1	短地址点播透传
0x0001~0xFFF8	0	组播
0xFFFE	0xFE	透传到 MAC 地址锁定目标（需协调器设置目标绑定）

设置低功耗模式的效果

低功耗模式	唤醒周期	上传心跳包周期
0	1 秒	2 分钟
1	3.3 秒	4 分钟
2	5 秒	6 分钟
3	∞秒	8 分钟

心跳包示例解析：55 13 82 0A 00 端口索引+发送模式 BD ED 目标短地址 01 目标端口 94 命令编号 01 命令方向 08 FC ClusterID 00 20 厂商码 FF 目标端口 01 读属性个数 04 00 属性 ID 30 数据类型 00 低功耗等级 52

4. 用户指令集

为方便用户使用情况，E18 ZigBee 模块使用了两种模式，即透传和 HEX 指令格式。（默认指令模式）

用户在指令模式下可以通过**设置本地属性指令**“55 07 00 11 00 03 00 01 13”进入透传模式。在透传模式下发送“+++”可以直接进入命令模式；

备注：下列命令中文字部分是对命令进行解析，方便用户更好的理解发送与反馈命令的含义，用户使用时请只使用 HEX 部分。

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、密钥是什么、

输入命令格式：

名称	cmd data
	命令数据
	NULL
	空
字节数	0

反馈命令格式：

名称	cmd data							
	命令数据							
	Net status	DevType	IEEE Addr	Channel	PANID	Short Addr	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， 0x03 – 休眠终端节点

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：未组网时值为 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）

发送命令：55 03 00 00 00

反馈命令：

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 61 PANID 00 00 短地址 28 EA E2 1A 00 4B 12 00 扩展 ID C6 CD 93 B5 2F 37 9E F6 E9 A6 CE 3A 15 33 CF 55 密钥 B1

4.1.2 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。**创建、加入网络失败会有重加、重创建机制，最多重新尝试 5 次，5 次失败后需要手动在再次尝试。**

输入命令格式：

名称	cmd data
	命令数据
	NULL
	空
字节数	0

反馈命令格式：

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)

发送命令：55 03 00 02 02

反馈命令：55 04 00 02 00 组网成功 02

异步反馈命令：55 29 80 01 02 网络打开 28 EA E2 1A 00 4B 12 00 MAC 地址 13 信道 C9 45 PANID 00 00 短地址 28 EA E2 1A 00 4B 12 00 扩展 PANID 2A 83 DE 81 59 20 3A 58 92 1A 2C 4B 5E 77 B9 A6 密钥 28

异步反馈命令：55 04 80 02 B4 网络窗口时间 36　（B4 默认 180s）

备注：用户使用该指令后，模块网络状态指示灯（P1.3 引脚）会动作。未组网时，网络指示灯快闪进行查找网络（终端/路由器）或组建网络（协调器），网络组建或查询加入成功后网络状态指示灯慢闪。已组网，恢复网络，网络指示灯直接慢闪提示用户。

4.1.3 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。

输入命令格式：

名称	cmd data
	命令数据
	NULL
	空
字节数	0

反馈指令格式：

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)

发送命令：55 03 00 03 03

反馈命令：55 04 00 03 00 状态 03

异步反馈命令：55 04 80 02 00 网络窗口时间 82　（关闭网络，允许入网窗口时间清零）

4.1.4 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。

输入命令格式：

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

mode：0x00 - 模组复位； 0x01- 模组退网； 0x02 – 模组恢复出厂

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 0x00，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

反馈命令格式：

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)

发送命令：55 07 00 04 00 模式 93 61 PANID 19 信道 EF　(复位)

55 07 00 04 01 模式 93 61 PANID 19 信道 EE　(退网)

55 07 00 04 02 模式 93 61 PANID 19 信道 ED　(恢复出厂设置)

反馈命令：55 04 00 04 00 状态 04

异步反馈命令：55 05 80 00 00 设备类型 10 软件版本号 90

4.1.5 设置设备类型

命令码：0x05

功能：设置模组为协调器，路由或终端节点（休眠或非休眠）。该设置需要在设备组网前设置，设置设备类型后需要重启模块，以保证协议栈能刷新设备类型，如果不进行重启会导致加入网络失败；

输入命令格式：

名称	cmd data
	命令数据
	Type
	设备类型
字节数	1

设备类型：0x00 – 协调器， 0x01 – 路由器， 0x02 – 终端节点， 0x03 – 休眠终端节点

反馈命令格式：

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)

发送命令：55 04 00 05 00 设备类型 05　　(协调器)

55 04 00 05 01 设备类型 04　　(路由器)

55 04 00 05 02 设备类型 07　　(终端)

55 04 00 05 03 设备类型 06　　(休眠终端)

反馈命令：55 04 00 05 00 修改成功 05　　(修改成功后请用查询状态指令查询设备类型)

备注：

1、设备类型设置为休眠终端，模块在加入网络后才会开始进入休眠模式，第一组网成功后模块会先进入 1 秒的唤醒周期，时间持续为 1 分钟，在此 1 分钟时间内属于协调器与终端节点的信息配置交互时间，用户可以在此段时间内通过协调器（组网管理器）剔除休眠终端，一分钟后模块会自动进入用户设置的低功耗等级所对应的休眠周期（如果协调器想要删除该休眠节点，需要休眠节点自行通过指令、按键、休眠终端主动唤醒后进行离网操作）；

2、如果休眠节点已经加入网络，但是休眠节点掉电后重新上电，那么休眠节点在恢复网络后，会有 30 秒的时间是属于协调器与终端节点的信息配置交互时间，与上述一致。

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 个优选信道值（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。

输入命令格式：

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：0x00 – 除能信道，0x01 – 使能信道，0x02 – 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 0x0B~0x1A (11-26)有效。

反馈命令格式：

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：0x00 – 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)

发送命令: 55 04 00 06 00 查询 06

反馈命令: 55 0B 00 06 00 成功 0B 0E 0F 13 14 18 19 信道列表 0A

发送命令: 55 05 00 06 01 使能 15 信道列表 12

反馈命令: 55 0C 00 06 00 成功 0B 0E 0F 13 14 15 18 19 信道列表 1F

发送命令: 55 06 00 06 00 除能 13 14 信道列表 01

反馈命令: 55 09 00 06 00 成功 0B 0E 0F 18 19 信道列表 0D

发送命令: 55 06 00 06 02 覆盖 11 12 信道列表 07

反馈命令: 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或节点加入网络前。可在待机模式下设置。

输入命令格式：

名称	cmd data
	命令数据
	NULL
	空
字节数	0

反馈命令格式：

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

状态：0x00 – 设置有效， 0xFF-设置无效

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)

发送命令: 55 03 00 07 07

反馈命令: 55 06 00 07 00 查询成功 C1 BE PANID 78

未组网时查询反馈 PANID：FE FF

4.1.8 设置 PANID

命令码：0x08

功能：模组在协调器模式下建立网络，或路由和终端节点模式下加入网络，设置一个指定 PANID，该操作需在建立网络或加入网络前进行。

输入命令格式：

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

PANID：预设 PANID 值

反馈命令格式：

名称	cmd data
	命令数据
	status
	状态
字节数	1

状态：0x00 – 设置有效， 0xFF-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)

发送命令: 55 05 00 08 98 89 PANID 19

反馈命令: 55 04 00 08 00 成功 08

4.1.9 查看模块加组

命令码：0x09

功能：查看模组加入的组，加组操作可在本地或远端操作。

输入命令格式：

名称	cmd data
	命令数据
	EP_idx
	端口索引
字节数	1

端口索引：对应模块的 endpoint 的序号（非端口号），默认透传口为 0x00，预留 1 给第二串口用，预留 2,3 给 PWM，GPIO 和 ADC 用。

反馈命令格式：

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)

发送命令: 55 04 00 09 00 端口索引 09

反馈命令: 55 05 00 09 00 查询有效 00 09

未加组反馈: 00　　加组后反馈组 ID

4.1.10 模块加组

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
	端口索引	组 ID
字节数	1	2

反馈命令格式：

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)

发送命令: 55 06 00 0A 00 端口索引 00 10 组 ID 1A

反馈命令: 55 04 00 0A 00 成功 0A

备注：若使用组播通信，需要把目标短地址设置为已加组的组 ID，目标端口设置为 0xFF

4.1.11 模块退组

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

反馈命令格式：

名称	cmd data
	命令数据
	Status
	状态
字节数	1

状态：0x00 - 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)

发送命令: 55 06 00 0B 00 端口索引 00 10 组 ID 1B

反馈命令: 55 04 00 0B 00 成功 0B

4.1.12 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：0 - 查询 ， 1 - 设置

功率范围: 0x00~0x14

反馈命令格式：

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)

发送命令: 55 05 00 0D 01 11 功率等级 1D

反馈命令: 55 05 00 0D 00 操作有效 11 功率等级 1C

发送命令: 55 04 00 0D 00 0D

反馈命令: 55 05 00 0D 00 14 功率等级 19

备注：　功率等级为 0x00~0x14 超过最大值设置不生效且保持之前的设置功率，使用上位机配置范围 0x0E~0x14。

4.1.13 工厂模式

命令码：0x0F

功能：用于测试模组发射功率及频率准确度

输入命令格式：

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

信道: 模组支持信道 0x0B~0x1A（11-26）

功率: 功率等级为 0x00~0x14

模式: 默认值 0x00

反馈命令格式：

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)

发送命令: 55 06 00 0F 0B 信道 14 功率 00 模式 10

反馈命令: 55 04 00 0F 00 操作有效 0F

备注：　工厂模式下将一直处于发射状态，退出该模式需要复位模块

4.1.14 读取本地属性

命令码：0x10

功能：读取模组上的 ZCL 属性状态参数

输入命令格式：

名称	cmd data	
	命令数据	
	EP_idx	AttrID
	端口索引	参数 ID
字节数	1	2

端口索引：模组的端口索引序号，默认值 0

参数 ID：模组的 ZCL 属性 ID

反馈命令格式：

名称	cmd data	
	命令数据	
	Status	Data
	执行状态	参数数据
字节数	1	n

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)

读取目标短地址命令:　55 06 00 10 00 端口索引 01 00 AttrID 11

反馈命令：55 06 00 10 00 成功 FF 00 目标短地址 EF

备注：若未设置目标短地址，出厂默认值为 FF FF

读取波特率命令：55 06 00 10 00 端口索引 00 00 AttrID 10

反馈命令：55 08 00 10 00 成功 00 C2 01 00 波特率 D3

读取目标短地址命令：55 06 00 10 00 端口索引 01 00 AttrID 11

反馈命令：55 06 00 10 00 成功 B2 30 目标短地址 92

读取目标端口命令：55 06 00 10 00 端口索引 02 00 AttrID 12

反馈命令：55 05 00 10 00 成功 01 目标端口 11

备注：若未设置目标端口号，出厂默认值为 FF

读取串口模式命令：55 06 00 10 00 端口索引 03 00 AttrID 13

反馈命令：55 05 00 10 00 成功 00 串口模式 10

备注：串口模式：0- 命令模式，1- 透传模式

读取低功耗等级命令：55 06 00 10 00 端口索引 04 00 AttrID 14

反馈命令：55 05 00 10 00 成功 01 低功耗等级 11

低功耗等级: 0 – 1 秒周期唤醒（2 分钟心跳包）

1 – 3.3 秒周期唤醒（4 分钟心跳包）

2 – 5 秒周期唤醒（6 分钟心跳包）

3 – 一直休眠（8 分钟心跳包）

4.1.15 设置本地属性

命令码：0x11

功能：设置模组的 ZCL 状态参数

输入命令格式：

名称	cmd data		
	命令数据		
	EP_idx	AttrID	Data
	端口索引	参数 ID	参数数据
字节数	1	2	n

端口索引：模组的端口索引序号，默认值 0

参数 ID：模组的 ZCL 属性 ID

参数数据：想要修改的参数的数据

反馈命令格式：

名称	cmd data
	命令数据
	Status
	执行状态
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)

设置串口波特率：55 0A 00 11 00 端口索引 00 00 AttrID 00 C2 01 00 波特率 D2

返回：55 04 00 11 00 成功 11

设置目标短地址命令：55 08 00 11 00 端口索引 01 00 AttrID B2 30 目标短地址 92

返回：55 04 00 11 00 成功 11

设置目标端口命令：55 07 00 11 00 端口索引 02 00 AttrID 01 目标端口 12

返回：55 04 00 11 00 成功 11

设置透传模式命令：55 07 00 11 00 端口索引 03 00 AttrID 01 透传模式 13

返回：55 04 00 11 00 成功 11

设置低功耗等级命令：55 07 00 11 00 端口索引 04 00 AttrID 02 低功耗等级 17

返回：55 04 00 11 00 成功 11

全波特率配置命令表：

通信波特率	本地属性配置命令	命令反馈	备注
9600(0x002580)	55 0A 00 11 00 00 00 80 25 00 00 B4	55 04 00 11 00 11	波特率不一致不影响通信、波特率设置后重启生效
19200(0x004B00)	55 0A 00 11 00 00 00 00 4B 00 00 5A	55 04 00 11 00 11	
38400(0x009600)	55 0A 00 11 00 00 00 00 96 00 00 87	55 04 00 11 00 11	
57600(0x00E100)	55 0A 00 11 00 00 00 00 E1 00 00 F0	55 04 00 11 00 11	
115200(0x01C200)	55 0A 00 11 00 00 00 00 C2 01 00 D2	55 04 00 11 00 11	

4.1.16 自动建立连接

命令码：0x14

功能：模组自动建立常连接，两个模组先后一起操作可建立常连接，操作超时会删除之前的常连接。建立常连接的结果，通过异步命令通知。

输入命令格式：

名称	cmd data
	命令数据
	EP_idx
	端口索引
字节数	1

端口索引：模组的端口索引序号，默认值 0

反馈命令格式：

名称	cmd data	
	命令数据	
	Status	EP_idx
	执行状态	端口索引
字节数	1	1

执行状态：0x00 – 执行有效，0xFF – 执行无效

端口索引：模组的端口索引序号

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 04 00 14 00 端口索引 14

反馈命令：55 04 00 14 00 端口索引 14

异步反馈命令：55 06 80 10 0C A8 目标短地址 01 目标端口 35

异步反馈命令：55 10 82 0F 00 0C A8 目标短地址 01 目标端口 13 命令编号 01 命令方向 08 FC ClusterID 00 20 厂商码 FC RSSI 01cmdID 00 状态 13

按键触发：

异步反馈命令：55 06 80 10 0C A8 01 35

异步反馈命令：55 10 82 0F 00 0C A8 01 07 01 08 FC 00 20 FC 01 00 07

备注：

1、使用自动建立通信连接后，用户可以直接使用指令使配对双方进入透传模式，即可开始进行相互数据通信。

2、指示灯：模块寻找自动配对中，指示灯快闪（100ms 亮/灭）；当模块找到配对设备时，指示灯慢闪（333ms 亮/灭）； 如设备真正被查找，指示灯熄灭。

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

异步反馈命令：

名称	cmd data	
	命令数据	
	Device Type	Verson
	设备类型	软件版本号
字节数	1	1

设备类型：0x00 – 协调器，1 – 路由器，2 – 终端　3 – 休眠终端

软件版本号：当前版本号 10（V1.0）

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

异步反馈命令：55 05 80 00 02 设备类型 10 软件版本 92

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

异步反馈命令：

名称	cmd data						
	命令数据						
	Net status	IEEE Addr	Channel	PANID	Short Addr	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：0 – 未组网，1 – 已组网， 2 – 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)

异步反馈命令：

打开网络命令通知：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 拓展 PANID 1B F0 09 64 46 CB 73 77 A7 66 F8 CA 01 B7 80 F6 网络密钥 0E

重启命令通知：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 拓展 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。

异步反馈命令：

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。(最大网络开放时间 0xB4 -180s)

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

异步反馈命令：55 04 80 02 B4 网络窗口时间 36　（B4 默认 180s）

4.2.4 模块短地址更新通知

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。

异步反馈命令：

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 - 路由器，　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)

异步反馈命令：55 0E 80 04 C6 DE E2 08 00 4B 12 00 MAC 地址 1A 47 短地址 02 节点类型 70

4.2.6 模块离网通知

命令码：0x06

功能：设备主动离网（需要使用退网指令或按键），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。

异步反馈命令：

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)

异步反馈命令：55 0B 80 06 51 20 9F 0C 00 4B 12 00 MAC 地址 3D

4.2.7 自动建立连接通知

命令码：0x10

功能：数传模组常连接状态通知，先发起常连接的模组为被动模式，后发起的为主动模式。

异步反馈命令：

名称	cmd data	
	命令数据	
	Nwk Addr	EP
	目标短地址	端口
字节数	2	1

端口索引：模组的端口索引序号

指令示例：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

异步反馈命令：55 06 80 10 0C A8 目标短地址 01 目标端口 35

异步反馈命令：55 10 82 0F 00 0C A8 目标短地址 01 目标端口 13 命令编号 01 命令方向 08 FC ClusterID 00 20 厂商码 FC RSSI 01cmdID 00 状态 13

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。

输入发送命令格式：

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

串口反馈命令格式：

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，会产生发送确认，其它值 – 执行无效

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。

发送确认命令格式：

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 **3.4 AF Status 状态表**

aboveabove 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。

接收返回命令格式：

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”

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。

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，该命令需在帧头的短地址域（Nwk Addr）输入 0xFFFD 广播地址，否则输入无

效。

输入发送命令格式：（仅表示命令参数）

名称	cmd param
	命令参数
	IEEE Addr
	MAC 地址
字节数	8

MAC 地址：被查询节点的 MAC 地址

接收返回命令格式：（仅表示命令参数）

名称	cmd param
	命令参数
	IEEE Addr
	MAC 地址
字节数	8

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 05 命令编号 04

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

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

备注：终端不支持查询自己的短地址

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

输入发送命令格式：（仅表示命令参数）

名称	cmd param
	命令参数
	NULL
	空
字节数	0

接收返回命令格式：（仅表示命令参数）

名称	cmd param
	命令参数
	IEEE Addr
	MAC 地址
字节数	8

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 1A 命令编号 1A

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

收到返回命令：55 11 81 01 7B 20 目标短地址 1A 命令编号 00 成功 3D 01 70 0F 00 4B 12 00 目标 MAC 地址 AB Startidx 00 assocnum 70

备注：终端不支持查询自己的 MacAddr

4.3.4 查询目标支持的簇（cluster）

命令码：0x04

功能：查询目标设备支持的簇

输入发送命令格式：（仅表示命令参数）

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

接收返回命令格式：（仅表示命令参数）

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，只需要关心值为 0x0104 的即可

设备 ID：端口的设备类型 ID，可用区分目标设备支持的功能。

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

例：使用 E18 模组查询一个带 PWM 功能的 ZigBee 模块，目标模组的 1 号端口为数据透传，2 号端口为 PWM 输出

查询 1 号端口：(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 3B B1 目标短地址 01 目标端口 8E

反馈命令：55 05 01 04 00 状态 04 命令编号 01

发送确认：55 07 8F 01 3B B1 目标短地址 00 状态 04 命令编号 00

收到返回命令：55 1D 81 04 3B B1 目标短地址 04 命令编号 00 成功 01 目标端口 04 01 设备轮廓 50 00 设备类型 00 设备

版本 04 输入簇大小 00 00 03 00 07 00 08 FC 输入簇 03 输出簇大小 03 00 06 00 08 00 输出簇 A5

数据解析 1：

目标模块短地址为 0xB13B，1 号端口为数据透传，设备轮廓为 0x0104 即 ZigBee HA 应用类设备，设备类型 0x0050 为数据传输类设备。有 4 个输入簇分别为 0x0000，0x0003，0x0007，0xFC08。最后一个簇 0xFC08 表示该设备是个数据透传类设备。输出簇中有 0x0003，0x0006 和 0x0008。0x0006 和 0x0008 表示该设备可以输出灯光的控制指令。

查询 2 号端口：(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 3B B1 目标短地址 02 目标端口 8D

反馈命令：55 05 01 04 00 状态 05 命令编号 00

发送确认：55 07 8F 01 3B B1 目标短地址 00 状态 05 命令编号 01

收到返回命令：55 1D 81 04 3B B1 目标短地址 05 命令编号 00 成功 02 目标端口 04 01 设备轮廓 01 01 设备类型 00 设备版本 06 输入簇大小 00 00 03 00 04 00 05 00 06 00 08 00 输入簇 00 输出簇大小 07

数据解析 2：

目标模块短地址为 0xB13B，2 号端口为 PWM 控制，设备轮廓同样为 0x0104 即 ZigBee HA 设备，设备类型是 0x0101 即可调光灯设备。有 6 个输入簇分别为 0x0000，0x0003，0x0004，0x0005，0x0006，0x0008，该信息说明模块支持 PWM。

4.3.5 查询设备支持端口数

命令码：0x05

功能：查询目标设备支持的簇

输入发送命令格式：（仅表示命令参数）

名称	cmd param
	命令内容
	NULL
	空
字节数	0

接收返回命令格式：（仅表示命令参数）

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：目标设备的端口总数量

端口列表：目标设备的端口列表

例：使用 E18 模组查询一个带 3 路 PWM 输出的数传模块 (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 3B B1 目标短地址 8E

反馈命令：55 05 01 05 00 状态 06 命令编号 02

发送确认：55 07 8F 01 3B B1 目标短地址 00 状态 06 命令编号 02

收到返回命令：55 0C 81 05 3B B1 目标短地址 06 命令编号 00 成功 04 端口数量 01 02 03 04 端口列表 08

数据解析：

目标设备是一个带 PWM 输出的数传模块，共 4 个端口，1 个用于数据透传，3 个用于 PWM 控制输出。

4.4 设备状态管理与设备控制（ZCL 命令）

4.4.1 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。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。

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								
	EP_Idx	shortAddr	Endpoint	SeqNum	Direction	ClusterID	ManuCode	AckMode	Ext data
	本机端口 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

本机端口：本机端口索引，低 4 位有效，默认为 0

发送模式：bit6 – APS 加密，bit7-强行发送（不路由不转发）

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

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，会产生发送确认，其它值 – 执行无效

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。

发送确认格式：

名称	cmd data					
	命令数据					
	EP_Idx	shortAddr	Endpoint	handle	Direction	AF status

	端口索引 发送模式	目标短地址	目标端口	命令编号	命令方向	发送结果
字节数	1	2	1	1	1	1

本机端口：本机端口索引，低 4 位有效，与发送时一样

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

命令编号：系统为该命令分配的编号

命令方向：该命令的发送方向，0 - C2S（攻->受），1 – S2C（受->攻）

发送结果：无线发送结果，见 **3.4 AF Status 状态表**

异步命令“接收 ZCL 消息”：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								
	EP_Idx	shortAddr	Endpoint	SeqNum	Direction	ClusterID	ManuCode	Rssi	Ext data
	接收端口 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

接收端口：本机接收端口的索引，低 4 位有效

对方模式：bit – 4，收到广播或组播，bit-5 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，如果收到帧序号与发送过的消息相同，且源地址和源端口与发

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

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

4.4.2 ZCL 命令解析

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。

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，写，查，上报）可以一条命令同时携带相同簇下的多个属性参数。

单个目标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。

功能	命令码	发送	接收
读取设备属性	0x00	ZCL_READ_ATTR_REQ	ZCL_READ_ATTR_RSP
修改设备属性	0x01	ZCL_WRTIE_ATTR_REQ	ZCL_WRTIE_ATTR_RSP

发送控制命令	0x0F	ZCL_CMD	无
接收控制命令	0x0F	无	ZCL_CMD_IND

4.4.3 读取设备属性

命令码：0x00

功能：读 ZCL 属性即状态参数，可以读取一个端口上指定簇中的多个状态参数

输入发送命令格式：（仅表示扩展数据部分）

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

收到返回命令格式：（仅表示扩展数据部分）

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 **3.6 ZCL 错误状态码**，只有“操作成功”才有后面的数据

数据类型：数据类型，见 **3.5 ZCL 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)

读取 **Cluster ID 0xFC08** 下的所有属性：

发送命令:55 19 02 00 00 端口索引+发送模式 7B 20 目标短地址 01 目标端口 A2 命令编号 00 命令方向 08 FC ClusterID 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 A2 命令编号 A0

发送确认命令：55 0A 8F 02 00 端口索引+发送模式 7B 20 目标短地址 01 目标端口 A2 命令编号 00 命令方向 00 状态 75

异步命令反馈：55 2C 82 00 00 端口索引+发送模式 7B 20 目标短地址 01 目标端口 A2 命令编号 01 命令方向 08 FC ClusterID 00 20 厂商码 FF RSSI 05 属性个数 00 00 属性 ID 00 状态 23 数据类型 00 C2 01 00 波特率 01 00 属性 ID 00 状态 21 数据类型 FF FF 目标短地址 02 00 属性 ID 00 状态 20 数据类型 FF 目标端口 03 00 属性 ID 00 状态 10 数据类型 00 模式 04 00 属性 ID 00 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：

发送命令：55 1F 02 00 00 端口索引+发送模式 00 00 目标短地址 01 目标端口 A1 命令编号 00 命令方向 00 00 ClusterID 0000 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 AA

反馈命令：55 05 02 00 00 状态 A1 命令编号 A3

发送确认命令：55 0A 8F 02 00 端口索引+发送模式 00 00 目标短地址 01 目标端口 A1 命令编号 00 命令方向 00 状态 2D

异步命令反馈：55 5F 82 00 00 端口索引+发送模式 00 00 目标短地址 01 目标端口 A1 命令编号 01 命令方向 00 00 ClusterID 00 00 厂商码 FF RSSI 08 属性格式 00 00 属性 ID 00 状态 20 数据类型 01 ZigBee 版本 01 00 属性 ID 00 状态 20 数据类型 10 软件版本 02 00 属性 ID 00 状态 20 数据类型 16 协议版本 03 00 属性 ID 00 状态 20 数据类型 01 硬件版本 04 00 属性 ID 00 状态 42 数据类型 10 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 状态 42 数据类型 10 46 57 43 4F 44 45 3D 37 34 30 36 2D 30 2D 31 30 产品型号 06 00 属性 ID 00 状态 42 数据类型 08 32 30 32 32 30 35 31 33 编译日期 07 00 属性 ID 00 状态 30 数据类型 01 电源方式 C0

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) 46 57 43 4F 44 45 3D 37 34 30 36 2D 30 2D 31 30 转换为 ASIIC **FWCODE=7406-0-10**

编译日期：08(数据长度) 32 30 32 32 30 34 32 34 转换为 ASIIC **20220513**

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、远程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。

4.4.4 修改设备属性

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。

输入发送命令格式：（仅表示扩展数据部分）

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 **3.5 ZCL 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

收到返回命令格式：（仅表示扩展数据部分）

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 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)

修改设备状态： 修改 Cluster ID 0xFC08 中的目标设备波特率

发送命令: 55 13 02 01 00 端口索引+发送模式 78 B8 目标短地址 01 目标端口 A2 命令编号 00 命令方向 08 FC ClusterID 00 20 厂商码 00 状态 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 A2 帧序号 A1

发送确认命令：55 0A 8F 02 00 端口索引+发送模式 78 B8 目标短地址 01 目标端口 A2 命令编号 00 命令方向 00 状态 EE

异步 ZCL 命令反馈：55 12 82 01 00 端口索引+发送模式 78 B8 目标短地址 01 目标端口 A2 命令编号 01 命令方向 08 FC ClusterID 00 20 厂商码 FF RSSI 01 属性个数 00 00 属性 ID 88 只读 43

备注：修改设备波特率需要使用发送控制命令进行修改。

修改设备状态： 修改 Cluster ID 0xFC08 中的目标短地址

发送命令:55 13 02 01 00 端口索引+发送模式 78 B8 目标短地址 01 目标端口 A2 命令编号 00 命令方向 08 FC ClusterID 00 20 厂商码 00 状态 01 属性数量 01 00 属性 ID 21 数据类型 FD FF 目标短地址 97

反馈命令: 55 05 02 01 00 状态 A2 命令编号 A1

发送确认命令：55 0A 8F 02 00 端口索引+发送模式 78 B8 目标短地址 01 目标端口 A2 命令编号 00 命令方向 00 状态 EE

异步 ZCL 命令反馈：55 0F 82 01 00 端口索引+发送模式 78 B8 目标短地址 01 目标端口 A2 命令编号 01 命令方向 08 FC ClusterID 00 20 厂商码 FF RSSI 00 状态 CA

修改设备状态： 修改 Cluster ID 0xFC08 中的目标端口

发送命令: 55 13 02 01 00 端口索引+发送模式 78 B8 目标短地址 01 目标端口 A2 命令编号 00 命令方向 08 FC ClusterID 00 20 厂商码 00 状态 01 属性数量 02 00 属性 ID 20 数据类型 11 端口号 86

反馈命令: 55 05 02 01 00 状态 A2 命令编号 A1

发送确认命令：55 0A 8F 02 00 端口索引+发送模式 78 B8 目标短地址 01 目标端口 A2 命令编号 00 命令方向 00 状态 EE

异步 ZCL 命令反馈：55 0F 82 01 00 端口索引+发送模式 78 B8 目标短地址 01 目标端口 A2 命令编号 01 命令方向 08 FC ClusterID 00 20 厂商码 FF RSSI 00 状态 CA

修改设备状态： 修改 Cluster ID 0xFC08 中的透传模式

发送命令: 55 13 02 01 00 端口索引+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 ClusterID 00 20 厂商码 00 状态 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 A2 命令编号 A1

发送确认命令：55 0A 8F 02 00 端口索引+发送模式 78 B8 目标短地址 01 目标端口 A2 命令编号 00 命令方向 00 状态 EE

异步 ZCL 命令反馈：55 0F 82 01 00 端口索引+发送模式 78 B8 目标短地址 01 目标端口 A2 命令编号 01 命令方向 08 FC ClusterID 00 20 厂商码 FF RSSI 00 状态 CA

修改设备状态： 修改 Cluster ID 0xFC08 中的低功耗等级

发送命令: 55 13 02 01 00 端口索引+发送模式 2B DC 目标短地址 01 目标端口 A2 命令编号 00 命令方向 08 FC ClusterID 00 20 厂商码 00 状态 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 A2 命令编号 A1

发送确认命令：55 0A 8F 02 00 端口索引+发送模式 2B DC 目标短地址 01 目标端口 A2 命令编号 00 命令方向 00 状态 D9

异步 ZCL 命令反馈：55 12 82 01 00 端口索引+发送模式 2B DC 目标短地址 01 目标端口 A2 命令编号 01 命令方向 08 FC ClusterID 00 20 厂商码 FF RSSI 01 属性数量 04 00 属性 ID 88 只读 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。

4.4.5 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：(紫色：负载长度　红色：命令类型+命令码　蓝色：校验码)

发送**控制命令**修改**波特率**:

发送命令: 55 10 02 0F 00 端口索引+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 ClusterID 00 20 厂商码 00 应答 02 cmdID 80 25 00 00 波特率 B9

反馈命令: 55 05 02 0F 00 状态 AB 命令编号 A6

发送确认命令：55 0A 8F 02 00 端口索引+发送模式 CB A6 目标短地址 01 目标端口 AB 命令编号 00 命令方向 00 状态 4A

异步 ZCL 命令反馈：55 14 82 0F 20 端口索引+发送模式 CB A6 目标短地址 01 目标端口 AB 命令编号 01 命令方向 08 FC Cluster ID 00 20 厂商码 FC RSSI 02 cmdID 00 成功 80 25 00 00 波特率 E4

发送**控制指令**修改**低功耗等级**:

发送命令: 55 10 02 0F 00 端口索引+发送模式 2B DC 目标短地址 01 目标端口 AA 命令编号 00 命令方向 08 FC Cluster ID 00 20 厂商码 00 应答 03 cmdID 03 功耗等级 85

反馈命令: 55 05 02 0F 00 状态 AA 命令编号 A7

发送确认命令：55 0A 8F 02 00 端口索引+发送模式 2B DC 目标短地址 01 目标端口 AA 命令编号 00 命令方向 00 状态 D1

异步 ZCL 命令反馈：55 10 82 0F 20 端口索引+发送模式 2B DC 目标短地址 01 目标端口 AA 命令编号 01 命令方向 08 FC ClusterID 00 20 厂商码 FC RSSI 03 cmdID 00 状态 DB

备注：不建议远程修改波特率(无法修正可能导致出现问题)，远程设置低功耗等级 3 级后(远程无法再对其进行操作)。

发送**控制指令**用于**标记设备**:

发送命令:55 11 02 0F 00 端口索引+发送模式 FD FF 目标短地址(在网设备全标记) FF 目标端口 A1 命令编号 00 命令方向 03 00 ClusterID 00 00 厂商码 00 应答 00 cmdID 00 00 持续时间 53

反馈命令: 55 05 02 0F 00 状态 A1 命令编号 AC

发送确认命令：55 0A 8F 02 00 端口索引+发送模式 FD FF 目标短地址 FF A1 命令编号 00 命令方向 00 状态 D1

备注: IDENTIFY 簇用于标记设备，设备在标记状态下，模块指示灯会进行闪烁（P1.2 引脚），也可被其它 ZigBee 设备发现并与它建立常连接。

4.4.6 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

4.4.6.1 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

4.4.6.1 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

4.4.6.1 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：

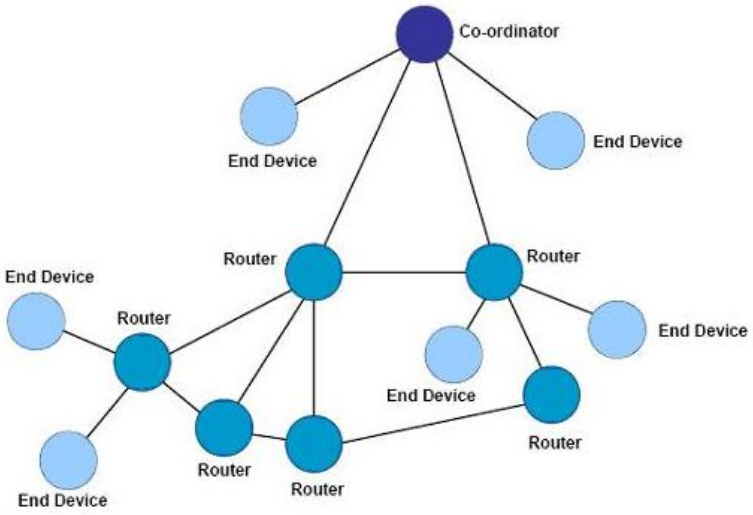
Cluster = 0xFC08，manuCode=0x2000, Sever->Client			
cmdID	描述符	名称	参数
0x00	UartNotify	透传接收	uint8 data[]: 透传数据
0x01	SetDstAddrRsp	设置默认目标返回	uint8 status: ZCL 状态
0x02	SetBaudRsp	设置波特率返回	uint8 status: ZCL 状态
0x03	SetLP_LevelRsp	设置低功耗返回	uint8 status: ZCL 状态

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，网络由一个协调器加任意个其他设备组成（路由器和终端）。
2	具有自组织，自路由，网络多跳功能。（默认支持网络深度为 5，子节点总数 20，子路由节点数 6）
3	父节点设备（协调器与路由器）可为休眠终端保存数据 7 秒。
4	只有休眠终端设备具有休眠功能，休眠等级分为 4 级，具体请参考 4.1.14 章节，用户可自行设置，出厂默认 0（1 秒唤醒周期）。 备注：建议休眠时间必须小于父节点数据保存时间，否则会影响数据接收。
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。
7	网络参数 PANID 为 FFFF 时为自动分配。若设备 PANID 不同则不能组网。
8	网络中所有透传模式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	休眠模式后，可通过串口唤醒。 备注：休眠状态下，串口唤醒的第一帧数据无效（唤醒帧小于等于 2 个字节）。唤醒时间持续 500ms，在 500ms 内设备将不再需要使用唤醒帧。
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），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	设备透传模式下通信单包最长允许字节：77Byte。如果超过 77Byte，会造成数据通信失败。 若使用命令模式下 ZCL 发送控制命令进行数据传输，超过 77Byte 需要使用 APS 加密模式发送（端口索引+发送模式：0x40），具体指令见 4.4 章节。
12	休眠终端第一次入网后第一分钟的唤醒周期为 1 秒，在该时间内协调器须完成入网设备的基本设置和查询，防止设备在进入低功耗后无法受控。
13	在广播通信时，若网络在存在休眠终端，且休眠终端想要接收广播数据，建议用户广播数据的时间间隔为休眠周期的两倍；
14	使用 E18 模块作为协调器，集中式集体组网，建议用户一次性入网设备个数不超过 10 个，一次性集体入网设备过多会导致入网时间长且有入网失败的风险。如一次性入网设备超过 10 个，建议用户使用组网管理器作为协调器。
15	E18 模块作为协调器，支持 7 个子设备同时向协调器点播数据（实测每个设备发送数据为 30Byte）。如使用场景需要更多设备并发，请使用组网管理器作为协调器。
16	使用快速配对功能，不建议同时操作设备数量超过两个，尽量保证是两个设备进行配对，否则会产生连接到不可预料的配对对象。（配对完成后可使用上位机查询目标端口、短地址是否修改成功）。

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

本次教程采用 E18 系列模块作为终端节点，组网管理器作为协调器搭配使用，教程中将详细介绍上位机使用方法及指令解析，以便于用户快速入门。

5.3.1 上位机入门（点播）

一、上位机简介

该配置上位机主要分为三个控制及配置面板：**本地指令、网络指令、设备控制命令。**

本地指令：网络参数、模块本地属性（波特率、低功耗等级、目标端口、功率、目标短地址）、信道、组信息的读取与配置；

网络指令：节点地址查询，设置常连接（通过组网管理器去指定一对终端节点相互匹配 MAC 地址通信）；

设备控制指令：网络节点网络状态显示（组网管理器支持）、各类 ClusterID 属性管理控制。

二、上位机使用（本地指令）

1、打开上位机后，依次选择设备串口号、波特率、模块型号；

2、执行“进入参数配置”（也可通过发送串口指令“+++”进入命令模式），右侧状态框会提示进入配置模式成功；

3、执行“读取参数”（也可通过发送串口命令“55 03 00 00 00”查询模块当前状态命令），右侧状态框会提示读取参数成功；

4、执行“查询”（也可通过发送串口命令“55 06 00 10 00 00 00 10”读取波特率、“55 06 00 10 00 01 00 11”读取目标短地址、“55 06 00 10 00 02 00 12”读取目标端口、“55 04 00 0D 00 0D”读取功率、“55 06 00 10 00 04 00 14”读取低功耗唤醒周期）；

5、根据需求配置“模组类型”：协调器、路由器、终端节点、休眠节点；

6、选择好模组类型后，执行“写入参数”（也可通过发送串口指令“55 05 00 05 00 05”协调器、“55 04 00 05 01 04”路由器、“55 05 00 05 02 07”终端、“55 04 00 05 03 06”休眠终端）。操作具体见下**图 1-1、图 1-2**

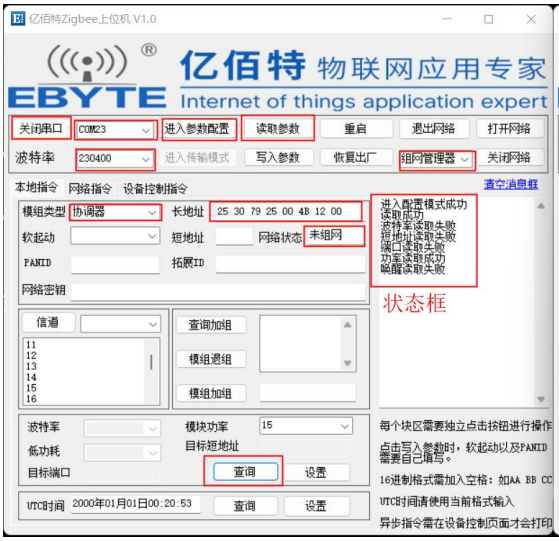


图 1-1 组网管理器

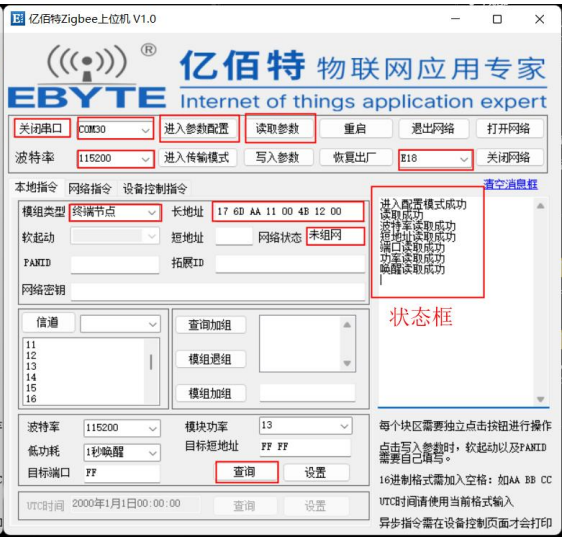


图 1-2 E18 系列模块

三、上位机组网操作（本地指令）

协调器、终端组建网络步骤：

1、选择相应串口；

2、选择波特率（E18 系列模块出厂默认波特率 115200），组网管理器只支持 230400；

3、选择当前使用的模块型号（支持 E18 与组网管理器），再执行打开串口；

4、模块进入配置模式（命令模式）；

5、读取当前模块参数；

6、选择需要设置的设备类型（当前我们选择协调器）；

7、写入参数（把设置的设备类型写入模块），串口命令格式请参照上文描述；

8、设备类型设置完成后，模块进行重启（“55 07 00 04 00 FF FF 19 1D”重启刷新协议栈）；

9、打开网络（协调器开始组建网络、终端开始查询加入网络），执行完成后，上位机会提示打开网络成功，具体上位机配置方法见图 1-3；

10、执行“读取参数”（也可通过发送串口命令“55 03 00 00 00”查询模块当前状态命令，可查询模块当前网络状态、PANID、短地址、MAC 地址、扩展 ID、网络密钥），操作结果如下**图 1-3**，网络组建成功，同一网络下，PANID、网络密钥一致。

图 1-3

11、**组网管理器**提供设备入网、退网通知，方便用户管理模块；注意：**此功能需要在“设备控制指令”面板下才能显示。**

备注：

1、终端节点配置方式与协调器一致，但是注意在协调器与终端进行组网时，协调器组建网络成功后的网络开放时间为 180 秒，因此终端节点在加入协调器网络时需要注意时间限制，如果终端节点在协调器组建网络 180 秒后执行打开网络，请先对协调器执行打开网络（可以刷新协调器允许入网时间），再对终端设备执行打开网络；

2、如果需要设置固定 PANID、信道组网，请先再组建网络前进行 PANID、信道设置；

3、信道配置可以通过上位机进行配置（入网前），先在信道功能下拉框选择除能、使能、覆盖信道功能，再选取下方信道列表

中需要的信道编号，然后执行点击“信道”（也可通过串口发送指令“55 05 00 06 01 15 12”使能信道，具体请查看官网软件用户手册）。

终端与终端相互点播通信网络参数配置：

1、在设备组网成功后，协调器、终端都点击“查询”（查询模块的本地属性，具体请查看上述**串口指令**描述）；

2、设备目标短地址：终端 1 目标短地址设置为“B9 CD”（也可通过串口指令“55 08 00 11 00 01 00 B9 CD 64”），终端 2 目标短地址设置为“8E DA”（也可通过串口指令“55 08 00 11 00 01 00 8E DA 44”）；

3、设置目标端口：统一设置为“01”；

4、终端节点双方都执行“进入传输模式”（也可通过串口指令“55 07 00 11 00 03 00 01 13”进入传输模式指令）；

图 1-4

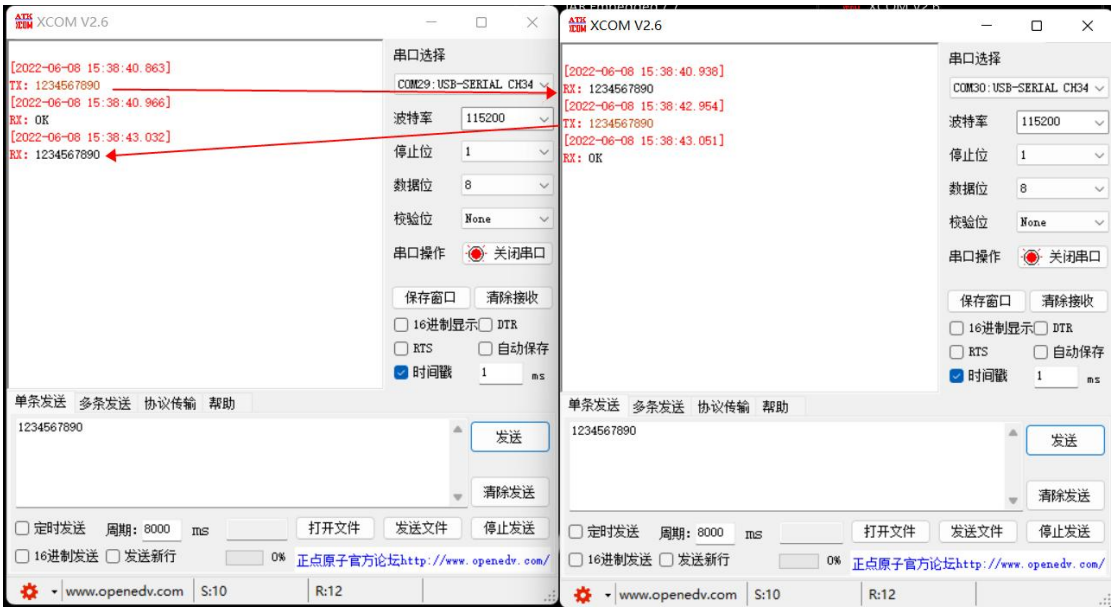


图 1-5

备注：

1、设置目标短地址时，短地址两个字节之间需要使用空格分开（仅限上位机使用）；

2、设置目标端口，通信双方必须保证一致为“01”端口；

5.3.2 组播通信教程

终端与终端组播通信步骤：

1、在模块加组填写框内填写需要加入组 ID，用户自定义两个字节 HEX，需要空格分开；

2、填写完成后执行“模块加组”，状态框会有提示加组成功（也可通过串口发送命令“55 06 00 0A 00 11 22 1A”模块加组）；

3、设置目标短地址：在填写框内写入组 ID 作为目标短地址；

4、设置目标端口：在填写框内写入“00”或者“FF”作为目标短地址（**组播只支持此两个端口号**）；

5、填写完成后，执行“设置”（右边提示栏会有写入各项参数成功提示），该串口指令上文已经详细描述；

6、模块双方都执行“进入传输模式”，串口命令：55 07 00 11 00 03 00 01 13，操作演示如**图 1-6** 所示。

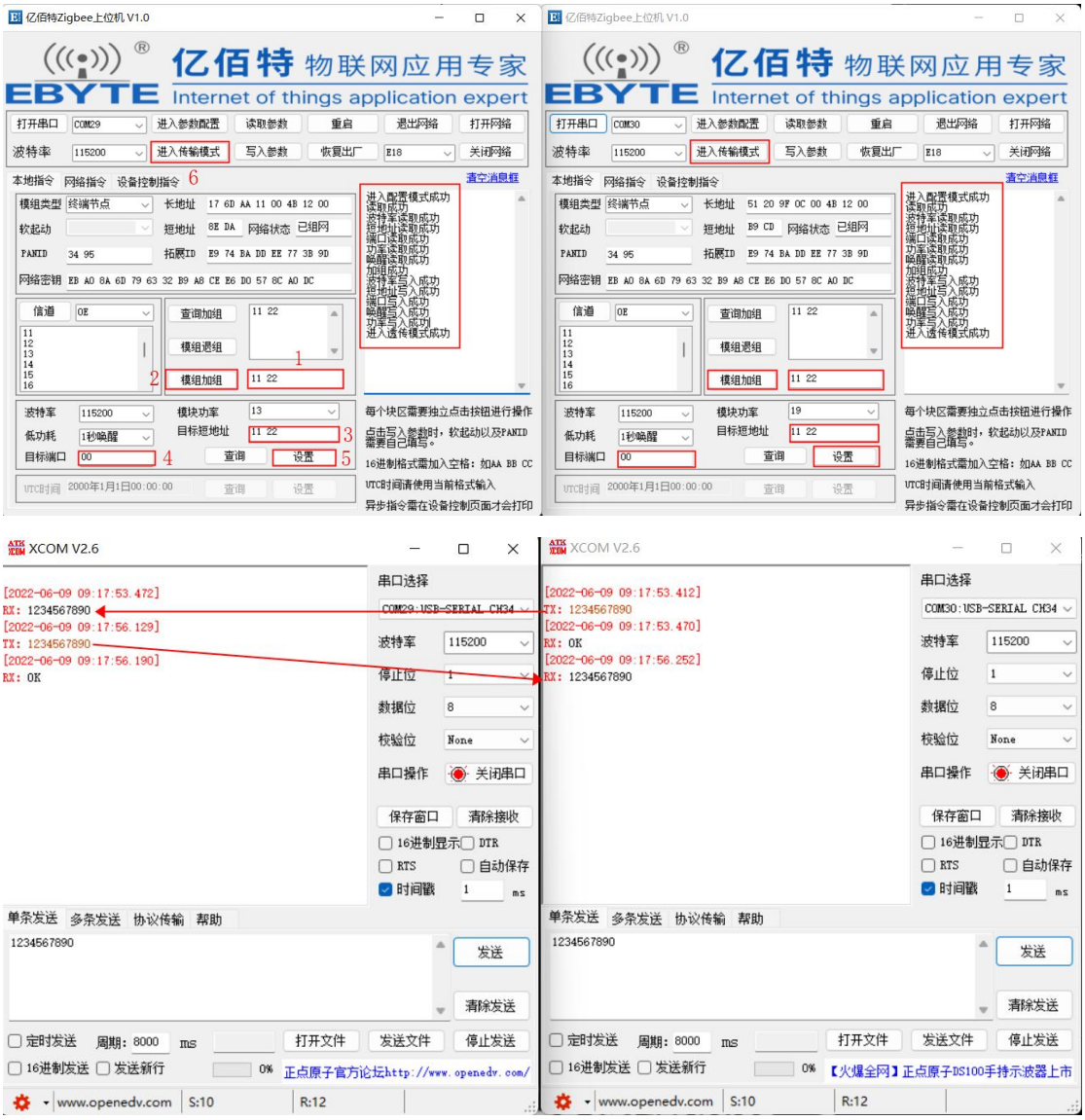


图 1-6

备注：

1、终端双方上述操作一致，完成上述操作后，双方都进行“进入传输模式”操作，即可使用串口调试助手进行组播通信；

2、组播通信可以多个模块加入同一组，形成多个模块组播通信。

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）；

5.3.4 上位机网络指令

一、网络指令

1、节点地址查询功能，在第一个填写框内填写需要被查询模块的短地址或者 MAC 地址；

2、执行“节点地址查询”，在后方显示框会直接显示查询到的短地址或者 MAC 地址，串口指令：“55 0D 01 00 FD FF 51 20 9F 0C 00 4B 12 00 B8“查询节点短地址，” 55 05 01 01 B9 CD 74”查询节点 MAC 地址。

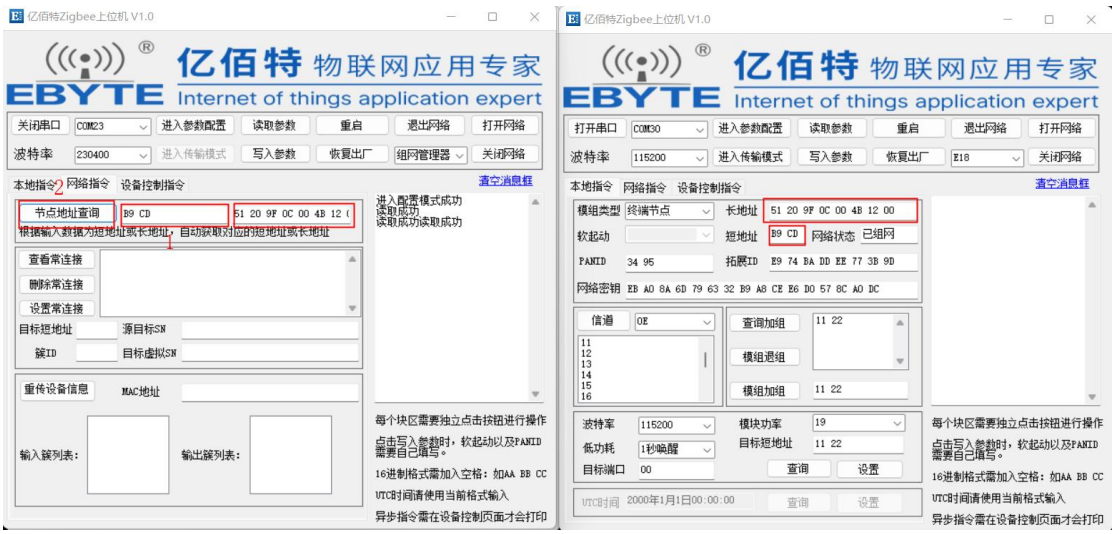


图 1-7

注意：节点地址查询功能不支持终端节点查询自身节点地址信息。

二、组网管理器设置常连接功能

该功能用于组网管理器指派网络中的其他节点双方进行通信绑定。

1、目标短地址、源目标 SN，源目标 SN 是由目标短地址模块的 MAC 地址前加上”01“端口号构成；

2、簇 ID：统一填写”08 FC “，目标虚拟 SN 是由目标短地址模块的 MAC 地址前加上”01“端口号构成。注意，此处目标虚拟 SN，它是目标短地址模块需要绑定的模块 MAC 地址。

3、填写完成后执行”设置常连接“操作，设置成功后，可通过”查看常连接“进行查看绑定模块参数。见**图 1-8**

4、组网管理器指派完成后，相互绑定模块的本地属性中目标短地址、目标端口需要都配置为”FE FF“与”FE “。见**图 1-9**

5、串口指令解析：” 55 19 01 21 0D DA 01 51 20 9F 0C 00 4B 12 00 08 FC 01 17 6D AA 11 00 4B 12 00 20” 与 ” 55 19 01 21 96 C9 01 17 6D AA 11 00 4B 12 00 08 FC 01 51 20 9F 0C 00 4B 12 00 A8 “可以设置常连接相互绑定。 ” 55 06 01 33 0D DA 00 86 “与” 55 06 01 33 96 C9 00 86 “可以查看目标短地址下的常连接绑定设备。

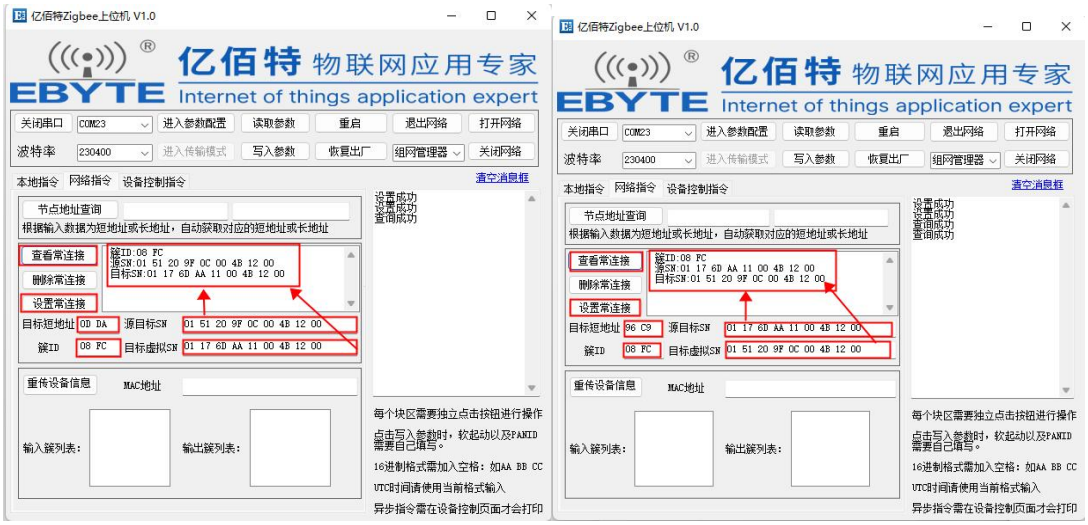


图 1-8

图 1-9

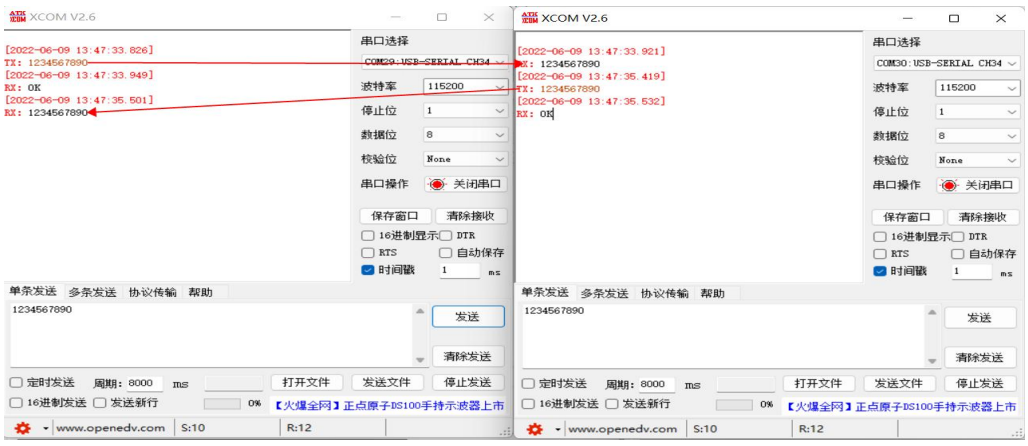


图 1-10

三、设备信息重传功能

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，同时可以通过该功能查看输入、输出簇列表。

1、MAC 地址：填写需要查询的模块 MAC 地址。

2、填写完成后，执行”重传设备信息“。也可发送串口指令：” 55 0B 00 28 17 6D AA 11 00 4B 12 00 B0 “。见**图 1-11**

图 1-11

5.3.5 上位机设备控制指令

一、组网管理器-网络设备列表

注意：

1、操作刷新列表后，需要等待设备扫描所有入网设备，时间较长。

2、组网管理器可以通过目标序列号进行节点删除，同时设备的入网信息及 ZCL 层网络返回通知信息会在右边状态框中进行提示（用户可以查看官网软件用户手册）。

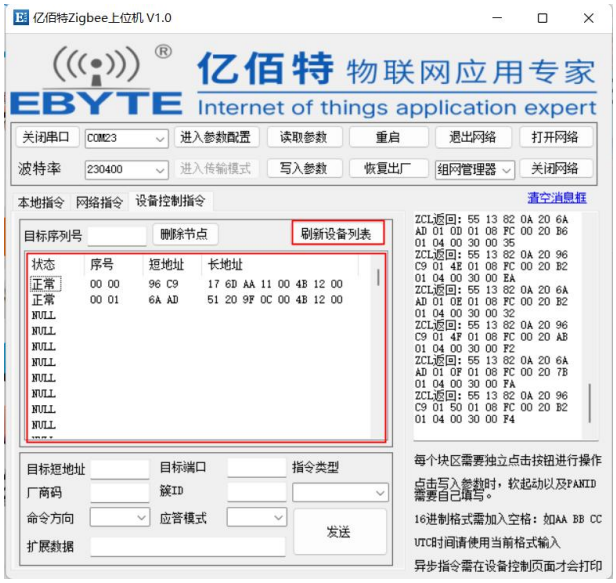


图 1-12

二、设备控制命令使用

数据传输-簇 ID：0xFC08

1、组网管理器通过设备控制指令给终端节点点播数据。见**图 1-13**

2、目标短地址”6A AD“点播对象，广播目标短地址”FD FF“、”FF FF“（具体广播类型请查看上文-广播模式）

3、串口指令解析：” 55 10 02 0F 00 6A AD 01 AB 00 08 FC 00 20 00 01 01 02 03 04 05 06 07 B5 “组网管理器通过该” 发送控制命令“进行数据传输（具体解析请查看软件用户手册指令描述）。

4、可根据“CMD ID”选择不同的发送控制命令：00-数据透传、01-设置目标短地址和端口、02-设置波特率、03-设置低功耗等级、04-模块重启。

图 1-13

Identify 设备标记-簇 ID：0x0003

通过该设备控制命令可以实现设备标记查询，方便用户对模块进行物理定位，**P1.2 引脚指示灯会在用户设定参数的时间内闪烁。**

1、目标短地址”6A AD“点播对象，广播目标短地址”FD FF“、”FF FF“（具体广播类型请查看上文-广播模式）

2、厂商码：除 0xFC08 的厂商码为 0x2000,其余均默认为 0x0000;

3、扩展数据是由 CMD ID+用户参数组成。具体请参照**图 1-14 及手册指令详解**

4、串口指令解析：“55 11 02 0F 00 端口索引+发送模式 FD FF 目标短地址(在网设备全标记) FF 目标端口 A1 命令编号 00 命令方向 03 00 ClusterID 00 00 厂商码 00 应答 00 cmdID 00 00 持续时间 53”目标短地址根据用户自定义选择；

图 1-14

注意：持续标记时间“05 00”中“05”是低 16 位，“00”是高 16 位，此参数是 P1.2 引脚指示灯闪烁 5 秒。

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】028-61543675
【公司传真】028-64146160
【官方网站】www.cdebyte.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