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

亿佰特 ZigBee 3.0 系列 HEX 模式串口命令

目录

1. 串口格式与模式配置

1.1 串口设置模式与波特率

- 波特率：组网管理器 230400，数传模块 115200
- 数据位：8 位模式
- 停止位：1 位模式
- 校验位：无
- 流控制：无

1.2 串口命令格式

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。

1.2.1 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

1.2.2 帧超时与帧间隔

模组接收命令帧时，收到任何字节都会开始接收定时，上位机需要向模块发送以 0x55 开头的一条具有完整帧结构的串口数据流。数据流不能有间断，否则模块会出现接收断包错误，并返回[55,03,FF,FF,00]的错误码。另外模组在向上位机回返命令帧时，如有连续的命令帧返回，每条命令帧之间的间隔时间均大于 200us。

1.2.3 串口帧载荷的构成

帧头 SFD （1 字节）	帧长 LEN （1 字节）	帧载荷 Payload （变长 3~255 字节）			
		命令类型 cmd type （1 字节）	命令码 cmd code （1 字节）	命令数据 cmd Data （变长 0~252 字节）	校验码 check （1 字节）

帧载荷由“命令类型”，“命令码”，“命令数据”和“校验码”4 个部分组成，每条命令均包含这 4 个单元。

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。

命令编码：

命令对应的编码，长度 1 字节，每条命令都有唯一的命令编码。

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：

命令载荷中包含命令类型，命令编码，命令数据的全部的 XOR8 校验和，长度 1 字节。

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。

1.2.4 三种命令模式

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。

输入命令无效的反馈：

向模块输入了不支持的命令，会反馈无效命令，格式如下：

[0x55, 0x03, '命令类型', '命令码', '校验']

即命令类型和命令码与输入命令相同，但不包含任何命令数据的反馈

输入命令校验不正确则会返回异步命令：0x55, 0x03, 0xFF, 0xFE, 0x01

输入命令发生断包或者超时则会返回异步命令：0x55, 0x03, 0xFF, 0xFF, 0x00

1.3 命令类型与命令码目录

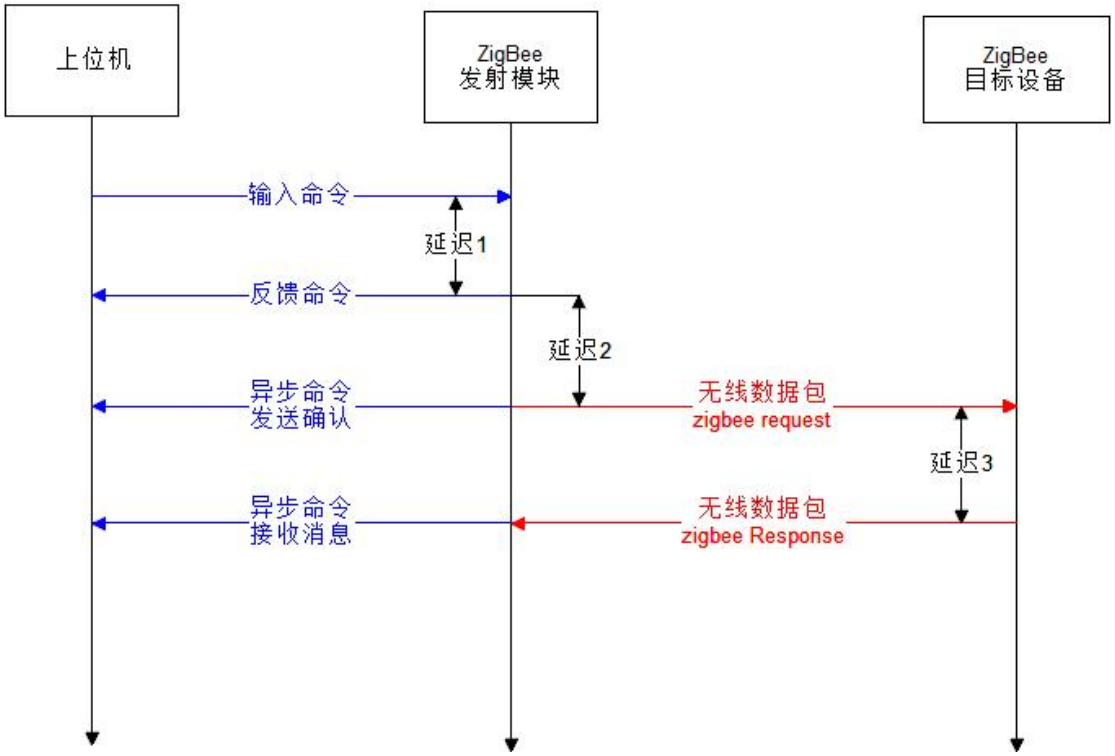
1.3.1 命令类型目录

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	ZCL 发送命令
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	ZCL 接收命令
	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。

无线通信的串口命令流程



延迟 1：该阶段中上位机输入命令需要在模块的 MCU 中进行预处理（加密和缓存查询），平均在 2~5 毫秒，其中 E72-2G4M20S1E 反应最快，实测平均约 1.5ms。

延迟 2：该延迟由信道拥堵程度，网络规模决定，点播模式下目标为非休眠设备时 1ms~50ms，目标为休眠设备时，可长达 7 秒多。广播或组播模式下，E72-2G4M20S1E 和 E18 系列约 5~10ms，E180ZG120 为 1 秒。

延迟 3：该延迟由接收端目标设备决定，最快不到 1 秒，最慢可达 10 秒多。如遇对方设备无法支持的命令，有可能不会产生返回，即延迟时间会延长到∞秒。

1.3.2 常用输入命令目录

本地配置命令

命令码	描述符	命令名称
0x00	CFG_STATUS	查询模组本机当前状态
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	设置本机节点类型
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	查看本机加组
0x0A	CFG_ADD_GROUP	本机加组
0x0B	CFG_REMOVE_GROUP	本机退组
仅数传模组支持的命令		
0x10	CFG_READ_ATTR	读取本地属性参数
0x11	CFG_WRITE_ATTR	设置本地属性参数
0x12	CFG_GET_BIND	查看常连接目标
0x13	CFG_SET_BIND	设置常连接目标
0x14	CFG_FIND_BIND	自动常连接
~~0x15~~	~~CFG_POLL~~	~~终端节点唤醒接收一次~~
0x16	CFG_AT_MODE	进入 AT 模式
仅组网管理器支持的命令		
0x20	CFG_GET_UTC	获取当前 UTC 时间
0x21	CFG_SET_UTC	设置 UTC 时间
0x22	CFG_GET_ADDRTAB	读取节点地址表
0x23	CFG_GET_KEYTAB	读取节点密钥表
0x28	CFG_EZ_MODE	重传设备信息

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

发送 ZCL 命令

命令码	描述符	命令名称
0x00	ZCL_READ_ATTR_REQ	读取设备属性参数
0x01	ZCL_WRTIE_ATTR_REQ	修改设备属性参数
0x02	ZCL_READ_REPORT_REQ	查询设备属性上报规律
0x03	ZCL_WRITE_REPORT_REQ	修改设备属性上报规律
0x04	ZCL_DISC_ATTR_REQ	查看设备全部属性
0x05	ZCL_DISC_ATTR_EX_REQ	查看全部属性（带扩展）
0x06	ZCL_DISC_CMD_REC_REQ	查看设备接收控制命令
0x07	ZCL_DISC_CMD_GEN_REQ	查看设备发送控制命令
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
0x10	NOTIFY_FIND_BIND	常连接通知
0x11	NOTIFY_IDENTIFY	标记模式

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 ZCL 命令

命令码	描述符	命令名称
0x00	ZCL_READ_ATTR_RSP	读取设备属性返回
0x01	ZCL_WRTIE_ATTR_RSP	修改设备属性返回
0x02	ZCL_READ_REPORT_RSP	查询设备属性上报规律返回
0x03	ZCL_WRITE_REPORT_RSP	修改设备属性上报规律返回
0x04	ZCL_DISC_ATTR_RSP	查看设备全部属性返回
0x05	ZCL_DISC_ATTR_EX_RSP	查看设备全部属性返回（带扩展）
0x06	ZCL_DISC_CMD_REC_RSP	查看设备接收控制命令返回
0x07	ZCL_DISC_CMD_GEN_RSP	查看设备发送控制命令返回
0x0A	ZCL_REPORT_IND	收到设备属性主动上报
0x0B	ZCL_DEFAULT_RSP	系统默认返回帧
0x0F	ZCL_CMD_IND	收到控制命令

发送确认命令目录以及发送状态表

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	ZCL 发送确认

无线发送状态表	
状态值	状态描述
0x00	操作成功
0x01	操作失败
0x02	参数错误
以下是 TI 平台（E72 和 E18 系列）的错误码	
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
以下是 Silabs（E180-ZG120 系列）的错误码	
0x03	查表未找到
0x18	缓存不够用
0x66	数据发送失败

1.4 ZigBee 协议中的常用寻址格式与大小端格式

ZigBee 应用中，通常需要指定将某个控制或消息发送到某个节点上面的具体外设或传感器上，或者接收某个节点上某个外设或传感器的消息，因此 ZigBee 协议规范中需要使用以下寻址方式，方便对网络中的设备进行精准管理和控制。

在 HEX 格式的串口命令中，所有的输入输出寻址格式数据，都是小端模式。

1.4.1 IEEE 地址（8 字节）：

IEEE 地址即 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。

1.4.2 PANID（2 字节）：

ZigBee 协调器创建网络时会生成一个 2 字节的 PANID，节点加入协调器生成的网络后获得与协调器相同的 PANID，并且和协调器工作在相同信道。

1.4.3 短地址（2 字节）

ZigBee 设备加入网络后会获得一个 2 字节的短地址，由于 ZigBee 是 Mesh 网络，因此在 ZigBee 网络中的数据传输需要根据短地址来进行通信，才能获得正确的路由转发路径。在同一个网络中，一个 IEEE 地址对应一个短地址。

1.4.4 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。其中用于设备控制的端口号从 1~240 有效，三个特殊的端口分包是 0 号端口（ZDO 端口）用于网络管理，242 号端口（GP 端口）用于 Green Power 协议转换，255 号端口（广播端口）用于对全部端口的同时控制，如同时打开一个多路开关上面的所有开关。

1.4.5 虚拟设备 SN 号：

虚拟设备 SN 号是亿佰特为了设备管理的方便性，根据 ZigBee 协议规范标准之上提出的设备管理机制。

每个 ZigBee 设备上都有 8 字节 IEEE 地址，同时设备固件上又固定了各个虚拟设备的端口号，因此 IEEE 地址+端口号可以作为虚拟设备的 SN 号。在小端模式下，虚拟 SN 号格式为“端口号”+“IEEE 地址（小端模式）”）

SN 号可以用于设备的“常连接绑定”（Bind）设置，指定源虚拟设备和目标虚拟设备。常连接绑定的目标也可以是一个分组，因此常连接目标为分组时，端口为 0xFF，IEEE 地址的第 0 和第 1 为组 ID，其余均为 0xFFFF

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]
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

2. 本地命令解析

2.1 本地配置命令

2.1.1 查询模组当前状态（命令码 0x00）

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

参数：无

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：0 – 已组网，0xFF – 未组网
设备类型：0 – 协调器，1 – 路由器，2-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

2.1.2 模组开机/软启动（命令码 0x01）

命令码：0x01
备注：**仅 E72-2G4M20S1E 支持**
功能：
模组上电后处于待机状态，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 0xFF – 启动无效

2.1.3 开始配网（命令码 0x02）

命令码：0x02

功能：

协调器执行该命令会打开入网允许权限，并在 180 秒内允许同样在配网状态下的路由器和终端节点入网。如果协调器是出厂无网络状态，执行该命令同时会新建一个网络，并生成新的 PANID，信道，网络密钥，扩展 PANID。

路由和终端节点执行该命令会尝试加入一个协调器创建的网络，协调器也必须在配网模式下才能成功加入网络。

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，可以延长协调器允许入网的时间。

E72-2G4M20S1E(Link72)模组 V1.4 固件新增白名单配网模式，在该模式下协调器会拦截 MAC 地址不在白名单中的入网设备，允许在白名单中的设备入网。

输入命令：

名称	cmd data
	命令数据
	Mode
	配网模式（可选）
字节数	1

配网模式：0-默认模式，直接配网（指令不包含配网模式时默认该模式）。1-协调器开启白名单配网。

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（模组当前状态不适合配网）。

2.1.4 停止配网（命令码 0x03）

命令码：0x03
功能：

配网模式下的协调器执行该命令可以阻止新设备加入协调器。

未入网的路由和终端节点执行该命令无任何效果，刚入网的路由和终端节点执行该命令也可让协调器阻止新设备加入。

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。

2.1.5 复位/恢复出厂（0x04）

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

mode：0 - 模组复位； 1- 模组退网； 2 – 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 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：0 – 操作有效，0xFF – 操作无效。

2.1.6 设置节点类型（命令码 0x05）

命令码：0x05
备注：仅 E180ZG120 和 E18 系列支持
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，可以在待机模式下设置。

输入命令：

名称	cmd data
	命令数据
	Type
	设备类型
字节数	1

设备类型：0 – 协调器， 1- 路由， 2 – 终端节点， 3 – 休眠终端节点

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。

2.1.7 查询与设置信道（命令码 0x06）

命令码：0x06

备注：仅 E72-2G4M20S1E 和 E18 系列支持

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（信道列表不能为 0）

信道列表：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

2.1.8 查询 PANID（命令码 0x07）

命令码：0x07

备注：仅 E72-2G4M20S1E 和 E18 系列支持

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：

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

2.1.9 设置 PANID（命令码 0x08）

命令码：0x08
备注：仅 E72-2G4M20S1E 和 E18 系列支持
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，可在待机模式进行。

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

2.1.10 查看模组加组（命令码 0x09）

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：

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 0，预留 1 给第二串口用，预留 2,3 给 PWM，GPIO 和 ADC 用

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：0 – 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

2.1.11 模组加组（命令码 0x0A）

命令码：0x0A
功能：

指定模组上某个端口加组

输入命令：

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：对应模块的 endpoint 的序号（非端口号）
组 ID：模组要加入的组

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。

2.1.12 模组退组（命令码 0x0B）

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：

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：对应模块的 endpoint 的序号（非端口号）
组 ID：模组要退出的组

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，1-模组端口已不在该组，0xFF – 操作无效。

2.1.13 信道扫描测试（命令码 0x0C）

命令码：0x0C
备注：仅 E72-2G4M20S1E 支持
功能：扫 ZigBee 信道信标，判断是否有其它 ZigBee 网络存在，可在协调器启动网络前辅助协调器设置信道。扫描结果在“信标扫描通知”中查看。

输入命令：

名称	cmd data
	命令数据

	Channel List	Duration	Mode
	信道列表	侦听时间	扫描模式
字节数	4	1	1

信道列表：32 位信道使能位图列表，11 信道对应值为 0x00000800，以此类推。
侦听时间：每个信道侦听时间，时间计算为(2^Duration)*15.36 毫秒。
扫描模式：0-信标扫描模式，1-预留其它 2.4G 信号检测模式。

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。

2.1.14 设置和查询当前发射功率（命令码 0x0D）

命令码：0x0D
功能：查询或设置模组发射功率
输入命令：

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

模式：0 - 查询当前功率， 1 - 设置功率
功率：设置

设置范围：
E72-2G4M20S1E 设置范围（0x0E~0x14）
E18 系列低功率版设置范围（0x00~0x05）
E18 系列大功率版设置范围（0x00~0x14）

反馈命令：

名称	cmd data	
	命令数据	
	Status	Power
	状态	功率
字节数	1	1

状态：0 – 操作有效，0xFF – 操作无效。
功率：读取到的当前功率。

2.1.15 读取本地属性（命令码 0x10）

命令码：0x10

备注：E180ZG120 和 E18 系列支持

功能：

读取模组上的 ZCL 状态参数

输入命令：

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 0

参数 ID：数据传输相关属性 ID，见《亿佰特自定义属性》

反馈命令：

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

执行状态：0 – 执行有效，其它 – 执行无效

Data：参数值

2.1.16 设置本地属性（命令码 0x11）

命令码：0x11

备注：E180ZG120 和 E18 系列支持

功能：

设置模组的 ZCL 状态参数

输入命令：

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 0

参数 ID：数据传输相关属性 ID，见《亿佰特自定义属性》
llz:这里严重怀疑上图端口索引和参数ID位置交换了,或者AttrID采用了小端模式
参数数据：修改的参数的数据

反馈命令：

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：0 – 执行有效，其它 – 执行无效
端口索引：模组的端口索引序号

2.1.17 自动绑定目标（命令码 0x14）

命令码：0x14
备注：E180ZG120 和 E18 系列支持
功能：
本机数传模组与其它数传模组自动建立数据透传关系，其中 E180ZG120 模组除可绑定其它数传模组（含 E180ZG120 和 E18 系列）还可自动绑定 ZigBee 照明设备。

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
	执行状态
字节数	1

执行状态：0 – 执行有效，0xFF – 执行无效

2.1.18 进入 AT 命令模式（命令码 0x16）

命令码：0x16
备注：仅 E180ZG120B 支持
功能：

进入 AT 命令控制模式。该命令会导致《亿佰特自定义属性》中传输模式变成“true”。

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
	执行状态
字节数	1

执行状态：0 – 执行有效，0xFF – 执行无效

2.1.19 获取当前 UTC 时间（命令码 0x20）

命令码：0x20

备注：仅 E72-2G4M20S1E 支持

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

2.1.20 设置 UTC 时间（命令码 0x21）

命令码：0x21

备注：仅 E72-2G4M20S1E 支持

功能：

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

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：0 – 执行有效，0xFF – 执行无效

2.1.21 读取入网节点地址表（命令码 0x22）

命令码：0x22

备注：E72-2G4M20S1E 和 E180ZG120B 支持

功能：

查询已入网节点的 MAC 地址和短地址，一条一条的查，E72-2G4M20S1E 总共 255 条，E180-ZG120B 共 80 条。需要注意的是在 E180-ZG120B 上该表是不支持掉电保存的，上位机读到这个表后建议保存在上位机中。

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：0 – 普通查询， 1- 带标志位查询（仅 E72 管理器支持）

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（仅 E72 管理器支持）

2.1.22 读取入网节点密钥（0x23）

命令码：0x23
备注：E72-2G4M20S1E 和 E180ZG120B 支持
功能：
该功能存在问题，下次升级时再完善。

2.1.23 重传设备信息通知（命令码 0x28）

命令码：0x28
备注：
E72-2G4M20S1E（LINK72）支持该指令，E180-ZG120 系列模组升级 V1.2 版固件也可支持该指令。
功能：
“设备信息通知”（见《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：0 – 操作有效，请等待设备上传。0xFF – 查询失败，设备可能不存在（E180-ZG120 做协调器时可以多试 1~2 次（间隔 3~6 秒再试）有可能成功）

2.1.24 设置模组 PWM 输出占空比（命令码 0x18）

命令码：0x18

备注：仅 E180ZG120B 模组支持，休眠终端模式下切勿使用该功能

功能：

设置 E180ZG120 模组的 3 路 PWM 输出占空比，范围 0~255。

输入命令：

名称	cmd data	
	命令数据	
	PWM Index	Value
	PWM 编号	数值
字节数	1	1

PWM 编号：0 – 端口 2 的 PWM，1 – 端口 3 的 PWM， 2-端口 4 的 PWM。

数值：0~255 有效，每一档对应 1/255。

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：0 – 操作有效， 0xFF – 操作无效

2.1.25 模组 PWM 标记模式（命令码 0x19）

命令码：0x19

备注：仅 E180ZG120B 模组支持，休眠终端模式下切勿使用该功能

功能：

E180ZG120 模组的 3 路 PWM 进入 Identify 模式，最大只能持续 255 秒。进入 Identify 模式后该路 PWM 以 1 秒周期闪烁，并可被自动绑定的设备发现建立绑定。

输入命令：

名称	cmd data	
	命令数据	
	PWM Index	Time
	PWM 编号	持续时间
字节数	1	1

PWM 编号：0 – 端口 2 的 PWM，1 – 端口 3 的 PWM， 2-端口 4 的 PWM。
持续时间：该端口进入 Identify 模式的持续时间

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：0 – 操作有效， 0xFF – 操作无效

2.1.26 添加白名单记录（0x29）

命令码：0x29
备注：
仅 E72-2G4M20S1E(Link72) 模组 V1.4 固件支持，旧固件可免费升级至该版本
功能：
协调器在配网状态下对入网节点进行 MAC 地址过滤，符合白名单的才能被添加。添加白名单只能在白名单配网打开的时候才能添加，配网模式结束后，添加的白名单会被全部清除，需要在下次打开白名单配网时重新添加。

输入命令：

名称	cmd data
	命令数据
	Whitelist Item
	白名单记录
字节数	8

白名单记录：需要被允许加入的节点的 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：0 – 添加成功，0xFF – 添加失败

2.1.27 锁定扩展 PANID 加网（0x1A）

命令码：0x1A

备注：

仅 V1.2 固件的 E180-ZG120 支持该功能，E180ZG120 在路由节点或终端节点模式下通过锁定协调器的 64bit 扩展 PANID 方式加入指定网络。锁定了扩展 PANID 的 E180ZG120 模块会自动持续配网，直到成功加入网络为止。

功能：

该命令可以查看和设置锁定的扩展 PANID，在路由和终端节点模式下设置为某个协调器的扩展 PANID 时，模组只能加入到这个协调器。该值设置成全 0 时，取消扩展 PANID 锁定。

输入命令：

名称	cmd data	
	命令数据	
	mode	Ext PANID
	模式	扩展 PANID
字节数	1	8

模式：0 - 查询当前锁定的扩展 PANID，1-设置扩展 PANID

扩展 PANID：8 Byte 扩展 PANID，设置模式下有效

反馈命令：

名称	cmd data	
	命令数据	
	Status	Ext PANID
	执行状态	当前扩展 PANID
字节数	1	8

执行状态：0 - 执行有效，0xFF - 执行无效

当前扩展 PANID：当前锁定 PANID，全 0 则没有锁定，只在查询模式下显示该字段。

2.2 系统通知命令

2.2.1 设备启动（命令码 0x00）

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	版本	MAC 地址
字节数	1	1	8

复位模式：由芯片类型决定，不同芯片复位模式不同。
版本：模组的软件版本
MAC 地址：模块的 MAC 地址

2.2.2 网络状态变更（命令码 0x01）

命令：0x01
功能：
模组组网成功，模组组网失败，已入网的模组开始配网，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：0– 未组网，1 – 已组网， 2 – 配网模式
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

2.2.3 允许入网时间窗口通知（命令码 0x02）

命令码：0x02
功能：
协调器开始配网后，该异步命令通知允许入网的窗口时间。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配网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，且窗口时间变成 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。

2.2.4 检测节点入网（命令码 0x03）

命令码：0x03

备注：E72-2G4M20S1E 和 E180ZG120 支持

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。

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）

2.2.5 节点短地址通知（命令码 0x04）

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

2.2.6 设备信息通知（命令码 0x05）

命令码：0x05

备注：仅 E72-2G4M20S1E 支持

功能：

节点第一次入网自动获取节点上的外设信息，包含设备 ID 信息，各个端口下支持的簇信息。

异步命令：

名称	cmd data									
	命令数据									
	EndFlag	DevSN	Short addr	Endpoint	ProfileID	DeviceID	In Cluster List		Out Cluster List	
	终结标记	设备 SN 号	短地址	端口号	端口轮廓	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，见《端口》

端口轮廓：profile ID，应用层只需要关注 0x0104 即可，见《端口轮廓》

设备 ID：表示设备的功能，由 ZCL 协议规范决定，见表《Device ID 表》。

输入簇表：设备支持的输入簇，包含簇数量和簇列表，见《簇 cluster》和《Server 端和 Client 端》。

输出簇表：设备支持的输出簇，包含簇数量和簇列表，见《簇 cluster》和《Server 端和 Client 端》。

2.2.7 模组离网通知（命令码 0x06）

命令码：0x06

备注：E72-2G4M20S1E 和 E180ZG120 支持

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

2.2.8 自动绑定目标结果通知（命令码 0x10）

命令码：0x10

备注：E18 和 E180ZG120 支持

功能：

自动绑定目标时找到的目标结果，该目标为数据透传和 AT 命令控制（E180ZG120）的目标。

异步命令：

名称	cmd data		
	命令数据		
	targetAddr	targetEP	clusterID
	目标短地址	目标端口	簇 ID
字节数	2	1	2

目标短地址：找到的目标短地址

目标端口：找到目标端口

簇 ID：建立连接的簇 ID，该字段仅 E180ZG120 支持，值为 0xFC08 即建立透传，0x0006 和 0x0008 则建立照明类设备的 AT 命令控制。

2.2.9 信标扫描通知（命令码 0x0C）

命令码：0x0C

备注：仅 E72-2G4M20S1E(Link72)支持

功能：

“信道扫描测试”的返回结果，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。扫描结束后会产生终结信号命令。

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。

2.2.10 系统后台调试消息（命令码 0x0F）

命令码：0x0C
备注：仅 E72-2G4M20S1E(Link72)支持
功能：
协调器运行时输出的后台调试消息

异步命令：

名称	cmd data	
	命令数据	
	debug code	debug data
	调试码	调试数据
字节数	2	变长

调试码：后台输出的调试码，目前只有三种
调试数据：后台输出的调试数据

三种调试消息：
① ，自动获取端口总数失败：
调试码：0x0001
调试数据格式与内容：

名称	调试数据
	MAC 地址
字节数	8

描述：
新节点入网时协调器会自动获取入网节点的端口数，当获取端口数失败时，会输出该节点的 MAC 地址。但是协调器获取入网节点端口数具有重传机制，即使发生一次失败也不要紧，只有出现连续 3 次的获取失败，有可能该节点入网无效（可能是入网后立即退网）。

② ，自动获取端口信息失败：
调试码：0x0002
调试数据格式与内容：

名称	调试数据	
	MAC 地址	端口号
字节数	8	1

描述：
新节点入网时协调器会自动获取入网节点的各个端口的信息（端口轮廓，设备 ID，簇

表），当获取端口信息失败时，会输出该端口的 MAC 地址和端口号。但是协调器获取入网节点端口信息具有重传机制，即使发生一次失败也不要紧，只有出现连续 3 次的获取失败，有可能该节点出现故障（可能是入网后立即退网）。

③ ，自动绑定通知

调试码：0x0003

调试数据格式与内容：

名称	调试数据			
	AF 状态	MAC 地址	端口号	绑定簇
字节数	1	8	1	2

描述：

新节点入网时，协调器会自动命令入网节点的端口绑定协调器。然后入网节点端口上的绑定簇下的关键属性可以自动上报到协调器，作为设备状态改变通知和心跳包使用。自动绑定的端口必须支持以下输入簇：

簇 ID	簇名称
0x0006	开关通断簇
0x0008	亮度控制簇
0x0101	锁具控制簇
0x0102	遮阳控制簇
0x0300	RGB 控制簇
0x0400	光照度传感簇
0x0402	温度传感簇
0x0500	安防报警簇

2.2.11 白名单拦截通知（命令码 0x07）

命令码：0x07

备注：仅 E72-2G4M20S1E(Link72) V1.4 固件支持

功能：

E72-2G4M20S1E(Link72) （V1.4 固件）在开启白名单配网模式的情况下，检测到未经过白名单。可以和“添加白名单记录（2.1.26）”配合使用，在检测到拦截后再去添加白名单。但是会导致入网节点发生配网失败，入网节点配网失败后需要立即重新尝试配网。

异步命令：

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

MAC 地址：被拦截的 MAC 地址

3. 网络管理命令（ZDO 命令）

3.1 ZDO 命令简介

ZDO 是 ZigBee Device Object 的缩写，用于对 ZigBee 设备的组网管理。具备以下几个特点

- ZDO 使用 0 号端口和 0x0000 的端口轮廓，作为一个特殊端口，每个 ZigBee 设备都必须拥有 ZDO 端口才能完成 ZDO 命令的交互。
- ZDO 命令均使用短地址进行通信，绝大多数 ZDO 命令都是具备 Request 和 Response 两种形式，即采用“一问一答”的方式进行通信交互。
- ZDO 命令可以用来查询入网设备的 MAC 地址和短地址，特别是某些 ZigBee 设备在复杂网络环境中会发生短地址变更的错误，可通过 ZDO 命令进行补救。
- 协调器通过 ZDO 命令可查询入网设备的全部端口以及该端口的端口轮廓，设备 ID，以及支持的簇，从而判断入网设备具备哪些功能。
- 协调器可通过 ZDO 命令设置入网节点的常连接绑定，可对各个节点上的各个端口的绑定关系，进行设置、解除、查看三种基本操作。

3.2 ZDO 命令的统一头格式

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。

3.2.1 输入命令格式

网络管理命令的输入命令格式

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

短地址：控制目标的短地址，小端模式
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

3.2.2 反馈命令格式

网络管理命令的反馈命令格式

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：0 – 执行有效，会产生发送确认，其它值 – 见《无线发送状态表》
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。

3.2.3 发送确认格式

网络管理命令的异步命令“发送确认”格式

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

短地址：发送目标的短地址
命令编号：系统为该命令分配的编号
发送结果：无线发送结果，见《无线发送状态表》

3.2.4 接收网络管理响应命令

网络管理命令的异步响应命令格式

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：响应命令的设备短地址
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，参考下面的《执行结果状态表》
命令参数：执行结果为 0 时，该参数才有效。

执行结果状态表

数值	意义
0x00	操作成功有效
0x80	无效的请求操作
0x81	设备未找到
0x82	无效的端口号（查询节点端口信息）
0x83	该端口无法被查询（查询节点端口信息）
0x84	该指令不支持
0x85	操作超时
0x86	绑定匹配失败（设置常连接）
0x88	该绑定关系不存在（取消常连接）

0x8C	空间不足（设置常连接）

3.2.5 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）。接收响应命令则是对方设备对命令的执行结果。

3.3 网络管理命令解析

网络管理命令解析仅针对输入命令和网络管理命令响应中的命令参数部分进行解析

3.3.1 查询节点短地址（命令码 0x00）

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
	命令参数
	IEEE Addr
	MAC 地址
字节数	8

MAC 地址：被查询节点的 MAC 地址

响应命令：

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

3.3.2 查询节点 MAC 地址（命令码 0x01）

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
	命令参数
	NULL
	空
字节数	0

命令参数：无

响应命令：

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

3.3.3 查询节点网络配置信息（命令码 0x02）

命令码：0x02

备注：仅 E72-2G4M20S1E(Link72) 支持

功能：

查询节点的网络配置信息

输入命令：

名称	cmd param
	命令参数
	NULL
	空
字节数	0

命令参数：无

响应命令：

名称	cmd param						
	命令参数						
	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

3.3.4 查询节点端口信息（命令码 0x04）

命令码：0x04
功能：
查询节点上指定端口的详细信息。

输入命令：

名称	cmd param
	命令参数
	Endpoint
	端口号
字节数	1

端口号：目标设备的端口号

响应命令：

名称	cmd param							
	命令参数							
	Endpoint	ProfileID	deviceID	deviceVersion	In Cluster List		Out Cluster List	
	端口号	端口轮廓	设备 ID	设备版本	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：设备的端口号，见《端口》
端口轮廓：profile ID，应用层只需要关注 0x0104 即可，见《端口轮廓》
设备 ID：表示设备的功能，由 ZCL 协议规范决定，见表《Device ID 表》。
设备版本：设备的版本
输入簇表：设备支持的输入簇，包含簇数量和簇列表，见《簇 cluster》和《Server 端和 Client 端》。
输出簇表：设备支持的输出簇，包含簇数量和簇列表，见《簇 cluster》和《Server 端和 Client 端》。

3.3.5 查询节点端口数（命令码 0x05）

命令码：0x05
功能：
查询节点支持的全部端口，见《端口》的说明。

输入命令：

名称	cmd param
	命令参数
	NULL
	空
字节数	0

命令参数：无

响应命令：

名称	cmd param	
	命令参数	
	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

3.3.6 设置节点常连接绑定（命令码 0x21）

命令码：0x21
备注：E72-2G4M20S1E(Link72) 和 E180ZG120B 支持
功能：
使用 ZigBee Bind 的方式，设置两个节点上的端口常连接绑定，节点通过 MAC 地址加端口号的方式记住对方，并将自己的一个端口与对方端口连接永久常连接。建立绑定关系的两个端口可以在同一个节点上，但是两个端口务必形成控制者与执行者的关系，见《Server 端和 Client 端》。由于常连接绑定需要记住对方的 MAC 地址和端口号并用自己的端口去绑定对方，因此管理绑定时增加了虚拟 SN 的概念，见《虚拟 SN》。

输入命令：

名称	cmd param		
	命令参数		
	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》。源虚拟 SN 不能是分组，必须对

应实际设备。
簇 ID：常连接通信用的簇 ID，见《簇(cluster)》
目标虚拟 SN：目标设备的虚拟 SN 号，见《虚拟 SN》，目标可以是一个分组，目标 SN 如果填全 0x00 是协调器自己，这样设置导致被设置对象把数据统统传给协调器。

响应命令：

名称	cmd param
	命令参数
	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

3.3.7 解除节点常连接绑定（命令码 0x22）

命令码：0x22
备注：E72-2G4M20S1E(Link72) 和 E180ZG120B 支持
功能：
解除已存在的常连接绑定，必须是目标节点保存了绑定记录才有解除绑定的意义

输入命令：

名称	cmd param		
	命令参数		
	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：由于常连接绑定需要记住对方的 MAC 地址和，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》，目标可以是一个分组，目标 SN 如果填全 0x00 是协调器自己，这样设置导致被设置对象把数据统统传给协调器。

响应命令：

名称	cmd param
	命令参数
	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

3.3.8 查看节点常连接绑定（命令码 0x33）

命令码：0x33

备注：E72-2G4M20S1E(Link72) 和 E180ZG120B 支持

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。

输入命令：

名称	cmd param
	命令参数
	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，响应时可返回多条记录，多次查询可以查完一个节点上的所有常连接关系。

响应命令：

名称	cmd param					
	命令参数					
	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 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：节点上发起绑定源端口的虚拟 SN 号

簇 ID：建立绑定的簇 ID

目标 SN：绑定目标的虚拟 SN 号，可以是单个设备端口，也可以是一个分组

3.3.9 删除节点（命令码 0x34）

命令码：0x34

功能：

根据 MAC 地址删除指定节点

注意事项：

被删除的节点如果是终端节点或休眠终端节点（“模组短地址通知（命令码 0x04）”中“节点类型”一项为 2 或 3）需要在命令头的“短地址”域输入终端节点的父节点地址。父节点可以在收到“检测节点入网（命令码 0x03）”中获取，包括终端节点在运行过程中

出现父节点切换也能通过该方式获得。因终端节点的父节点在运行过程中变数较大，ZigBee 模组（含协调器模式的模组）不负责记录各个节点的父节点，为保障正确删除节点，上位机务必做好记录。

对于版本较新的 ZigBee 3.0 R22 的终端节点，也可在“短地址”域直接填入其自身短地址。

输入命令：

名称	cmd param		
	命令参数		
	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

响应命令：

名称	cmd param
	命令参数
	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

3.3.10 查看网络链路（0x31）

命令码：0x31
备注：仅限 E72-2G4M20S1E(Link72) 支持
功能：

查看某个节点的链路关系表，使用该功能可以把整个网络拓扑获取到。

输入命令：

名称	cmd param
	命令参数
	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链路关系。

响应命令：

名称	cmd param							
	命令参数							
	TotalNum	StartIdx	ListNum	List Data				
	记录总数	起始索引	返回条数					
				短地址	MAC 地址	节点类型	节点关系	网络深度	信号强度
字节数	1	1	1	20*N					
				2	8	1	1	1	1

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
短地址：链接节点的短地址
MAC 地址：链接节点的 MAC 地址
节点类型：链接节点的节点类型，0-协调器、1-路由器、2-终端节点（含休眠终端）
节点关系：链接节点的关系，0-父节点、1-子节点、2-邻居节点、3-无关节点
网络深度：节点的网络深度
信号强度：链接节点的平均信号强度，最大 255 等效 100%即质量最好。

4. ZigBee 控制与管理（ZCL 协议）

4.1 ZCL 规范介绍与表格

ZCL（ZigBee Cluster Library）规范为 ZigBee 协议中应用层规范，该规范中定义了各种不同的 ZigBee 设备如何区分识别，如何控制，以及如何表示其当前控制状态或物理状态，如传感器读数，照明设备的明暗亮灭等。通过对 ZCL 指令内容的任意排列组合，亿佰特全系 ZigBee 模组可支持多达 60000+种 ZigBee 设备类型 16000000+种设备控制指令，包括了现有市面的各种 ZigBee 设备以及将来会出现的 ZigBee 设备。

4.1.1 ZCL 架构简介

端口轮廓：（Profile）

ZigBee 节点上的每一个端口，都有自己的端口轮廓用于描述该端口的用途。其中除了 Profile=0xC05E 用于 Touch Link 入网，Profile=0xA1E0 用于 GP 端口，其余 Profile 均可用于应用层控制。两个 Endpoint 必须 Profile 相同才能交互应用层数据，其中 ZigBee 智能家居应用（Home Automatic）的 Profile=0x0104，亿佰特的数据传输模组为满足与其它厂商设备互通，也使用该 Profile 作为数据传输使用。

设备 ID（device ID）：

设备 ID 存在于 ZigBee 设备的每个端口上，一个端口有且只有一个设备 ID，用于定义这个端口具体对应的设备种类。详见《Device ID 表》

簇（cluster）：

用于定义 ZigBee 设备的功能，一个 ZigBee 设备上的任意端口（端口号在 1~240）支持 1 个或多个簇，表示该设备支持某个功能。一个簇下通常包含若干个物理状态和控制指令，不同的簇表示的功能不同（例如 ZigBee 设备的 CPU 温度和传感器检测环境温度是两个不同的簇）。每个端口上有两个簇表，分别是输入簇表（in cluster）和输出簇表（out cluster）。输入簇说明该设备具有某个功能的受控和执行能力，是该功能的执行者；输出簇是某个功能的发起能力，是该功能的控制者。

Server 端（执行端或提供者）和 Client 端（控制端或使用者）：

当某个簇出现在端口的输入簇表中，则表示该端口在该簇上是 Server 端，即该簇对应功能服务的提供者，也就是执行端。相反某个簇出现在端口的输出簇表中，则表示该端口在该簇上是 Client 端，即该簇对应功能服务的使用者，也就是控制端。ZCL 命令中需要标记命令方向，即 Server- to-Client（S2C）和 Client-to-Server（C2S），用于表示该命令是提供者发起的还是使用者发起的。

厂商码（manufacture code）：

厂商码用于设备制造厂商添加自定义的簇时使用，在 ZigBee 标准簇不能满足应用的时候，厂商可以自定义簇（从簇 ID=0xFC00 开始）。为防止不同厂商使用相同自定义簇发生“撞簇”，因此厂商可以在自定义簇上增加厂商码字段来防撞。

属性（Attribute）：

属性是用于表示某个簇下的一个实际状态，因此属性的大小固定，通常在设备中是以一个全局变量的形式存在。属性可以用于表示设备的当前状态，如温度，亮度，通断等。属性可以被定义成符合 C 语言规范的变量类型，如 char 型，bool 型，int 型，浮点型，字符串型……，每个属性都有固定的数据类型（Data Type），见《数据类型表》。

每个属性都有一个 16bit 的属性 ID，每个簇下的执行端和控制端均可定义各自的属性，并且属性 ID 可复用且可以使用不同的数据类型。

通用命令（Global Command）：

通用命令用于对设备端属性的访问和控制，包括读属性，写属性，属性主动上报给固定目标，设置属性上报规律，查询属性上报规律，统计全部属性等功能。通用命令是直接控制属性的，而且只能操作固定大小的属性值，同时在设备上面属性通常又对应了全局变量。为了防止对设备端执行危险操作，因此极少通过写属性的方式去控制设备或者改变设备的物理状态。另外，一条通用命令可携带同一个簇下的多个属性，即 SIMD（单指令多数据）操作。

控制命令（Special Command）：

控制命令不直接针对属性进行操作，而是通过命令 ID 加附带的命令参数对目标设备进行控制，因此相比通用命令更具有实用性。每个簇下可以定义 256 条控制命令，加上命令方向的不同，控制端设备和执行端设备总共可定义 512 条不同的控制命令。而且每条命令可以附带不同长度的命令参数。

使用控制命令控制目标设备，可以直接作用于目标设备的物理状态上。例如使用控制命令来改变目标设备的 PWM 脉宽，或者在控制命令中附带开锁密码，执行端设备的 PWM 脉宽改变或者锁定状态发送改变，会同步到对应的属性上，再通过通用命令访问对应的属性，就可获知控制结果。

控制命令只能由控制端发给执行端，但是通用命令可由第三个设备发给控制端和执行端。

常连接绑定（Bind）：

常连接绑定用于设置某个节点上某个端口通过固定簇 ID 与另一个端口绑定。源端口通过 MAC 地址和端口号记住对方。由于成品的 ZigBee 设备 MAC 地址和端口不会改变，因此即使目标设备当前不在网络中也能生效，但是目标设备必须加入到和源设备相同的网络才能正常通信。常连接绑定需具备以下特点。

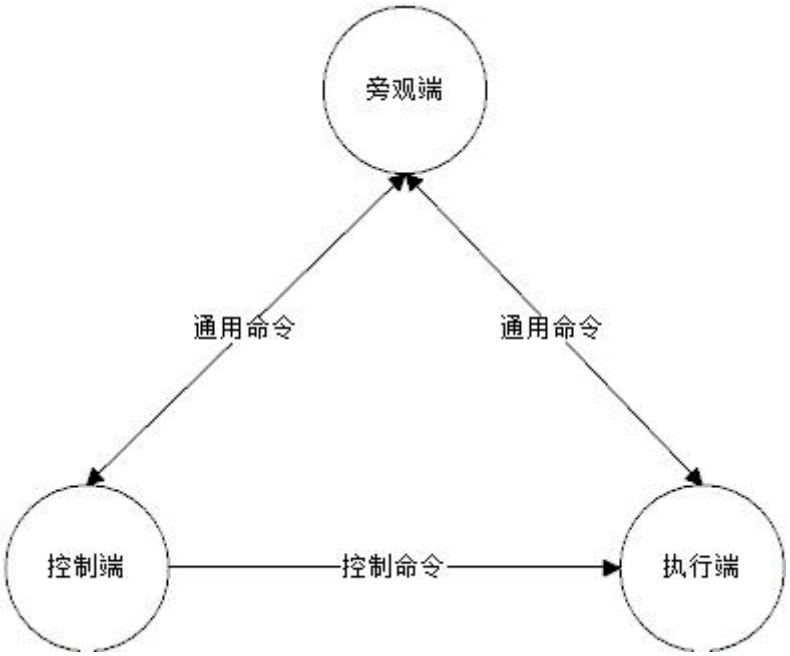
- 源端口和目标端口可以在同一个节点上，即它们的 MAC 地址相同。
- 源端口和目标端口必须是 Server 和 Client 的关系，用于绑定的簇必须存在于源端口的输入簇表或输出簇表中。

设置绑定有以下两种方式：

- 协调器下发指令：协调器通过“设置绑定”，“解除绑定”，“查看绑定”三条 ZDO 命令，对包括自己在内的节点端口进行绑定设置和管理，ZDO 命令的接收对象为绑定源端口，如果需要设置双向交互（如数据透传），需要设置两个端口都绑定对方。
- 节点发起绑定：数传模块可以通过“一键绑定”功能，自动搜索对方端口。源端口为数传模块自己的端口 1（支持亿佰特自定义簇），目标端口可以是其它数传模块的端口 1，也可以是 ZigBee 照明设备（包括 E180ZG120 的 PWM 控制端口）。

大小端模式：

ZCL 命令中，需要输入输出的参数除目标短地址，还有簇 ID，厂商码，属性 ID，输入输出格式均为小端模式。



4.1.2 ZCL 相关表项

Device ID 表			
分类	Device	设备名	Device ID
Generic	On/Off Switch	通断开关	0x0000
	Level Control Switch	级数控制器（旋钮）	0x0001
	On/Off Output	开关输出端	0x0002
	Level Controllable Output	旋钮输出端	0x0003
	Scene Selector	场景控制器	0x0004
	Configuration Tool	配置工具	0x0005
	Remote Control	遥控器	0x0006
	Combined Interface		0x0007
	Range Extender	中继器	0x0008
	Mains Power Outlet	电源输出设备	0x0009
	Door Lock	门锁	0x000A
	Door Lock Control	门锁控制器	0x000B
	Simple Sensor	普通传感器	0x000C
	Consumption Awareness Device	消费感知设备	0x000D
	Home Gateway	家庭网关	0x0050
	Smart Plug	智能插座	0x0051
	White Goods	白色家电	0x0052
Light 照明类	On/Off Light	开关灯	0x0100
	Dimmable Light	调光灯	0x0101
	Color Dimmable Light	彩色灯	0x0102
	On/Off Light Switch	开关灯控制器	0x0103
	Dimmer Switch	调光灯控制器	0x0104
	Color Dimmer	彩色控制器	0x0105
	Light Sensor	光传感器	0x0106
	Occupancy Sensor		0x0107
Closures 门窗类	Shade	遮阳设备	0x0200
	Shade Controller	遮阳控制器	0x0201
	Window Cover	窗帘	0x0202
	Window Cover control	窗帘控制器	0x0203
HVAC 暖通类	Heating/Cooling Unit	冷暖控制器	0x0300
	Thermostat	温控器	0x0301
	Temperature Sensor	温控传感器	0x0302
	Pump	泵	0x0303
	Pump Controller	泵控制器	0x0304
	Pressure Sensor	压力传感器	0x0305

	Flow Sensor	流量传感器	0x0306
IAS 安防类	IAS Control and Indicating Equipment	安防控制器	0x0400
	IAS Ancillary Control Equipment	安防网关	0x0401
	IAS Zone	安防传感器	0x0402
	IAS Warning Device	安防警报器	0x0403

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

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	

常见 cluster ID 表			
cluster ID	描述	功能	manufacture code
0x0000	ZCL_CLUSTER_ID_GEN_BASIC	设备基础信息	无
0x0003	ZCL_CLUSTER_ID_GEN_IDENTIFY	设备标记（ident）	无
0x0004	ZCL_CLUSTER_ID_GEN_GROUPS	组功能协议	无
0x0005	ZCL_CLUSTER_ID_GEN_SCENES	场景功能协议	无
0x0006	ZCL_CLUSTER_ID_GEN_ON_OFF	开关灯协议	无

0x0008	ZCL_CLUSTER_ID_GEN_LEVEL_CONTROL	调亮度协议	无
0x0019	ZCL_CLUSTER_ID_OTA	OTA 升级	无
0x0400	ZCL_CLUSTER_ID_MS_ILLUMINANCE_MEASUREMENT	光感协议	无
0x0500	ZCL_CLUSTER_ID_SS_IAS_ZONE	安防类协议	无
0x1000	ZCL_CLUSTER_ID_TOUCHLINK	Touch Link 功能	无
0xFC08	ZCL_CLUSTER_ID_EBYTE	亿佰特透传	0x2000

4.1.3 亿佰特串口数据传输 ZCL 簇规范

亿佰特串口数据传输设备遵照 ZigBee 标准规范，严格遵守 ZCL 协议规则，自定义了串口数据传输的簇，其定义如下

厂商码： 0x2000
串口数据传输簇 ID： 0xFC08

串口数据传输相关属性：

亿佰特自定义属性（执行端）					
AttrID	描述符	名称	数据类型	操作	初始值
0x0000	Baud	波特率	uint32	R	115200
0x0001	targetAddr	目标短地址	uint16	RW	0xFFFF
0x0002	targetEP	目标端口	uint8	RW	0xFF
0x0003	sendMode	透传模式	bool	RW	FALSE
0x0004	LP Level	低功耗模式	Enum8	RP	0
0x0005	target IEEE	目标 MAC 地址	EUI64	R	0x0000000000000000

- 波特率为了防止设置错误值，只能通过控制命令修改，控制命令具有纠错功能，一旦设置了错误波特率可被修正为最接近的正确波特率。
- 目标短地址默认为广播地址，设置成 0xFFFE 时则为透传给绑定目标。
- 目标端口为 1~240 时点播模式到对应目标端口，通常设置成 1 就可以了。如果设置成 0 则为组播模式，目标短地址就是组地址。
- 透传模式设置成 TRUE 则为透传模式或 AT 命令模式
- 低功耗模式共 4 个档次，分别是 0, 1, 2, 3。0 为 1 秒唤醒 2 分钟心跳，1 为 3 秒唤醒 4 分钟心跳，2 为 5 秒唤醒 6 分钟心跳，3 为不唤醒 8 分钟心跳。
- 目标 MAC 地址仅 E180ZG120 支持，仅显示当前通信的目标 MAC。

串口数据传输相关控制命令：

cmdID	Dir	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	响应波特率设置结果
0x02	C2S	Set Target req	设置目标短地址和端口

0x02	S2C	Set Target rsp	响应目标短地址和端口设置结果
0x03	C2S	Set LP req	设置低功耗模式
0x03	S2C	Set LP rsp	响应低功耗模式设置结果

4.2 ZCL 命令的统一帧头格式

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+端口号的发送方式。

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。

4.2.1 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								
	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，1 – S2C

簇 ID：发送消息的簇 ID，小端模式。

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；

2–不作任何应答即同时关闭 Default Response 和 APS Ack，适用于高速传输且对数据传输稳定性无要求的应用场景，该模式仅 E180-ZG120A/E180-ZG120B 模块 V1.2 固件，E18 全系列 V1.4 固件，E72-2G4M20S1E(LINK72) V1.4 固件支持。

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。

4.2.2 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：0 – 执行有效会产生发送确认，其它值 – 执行无效见《无线发送状态表》
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。

4.2.3 异步命令“发送确认”格式

发送确认可作为向某个目标发送的忙状态阻塞，如果发送时使能了应答模式，可从发送结果中获取发送帧是否到达目标，但会消耗更多的无线资源，延迟也会加大。

名称	cmd data					
	命令数据					
	EP_Idx	shortAddr	Endpoint	handle	Direction	AF status
	本机端口 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，1 – S2C
发送结果：无线发送状态表，见《无线发送状态表》

4.2.4 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	帧序号	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，1 – S2C
簇 ID：接收消息的簇 ID，小端模式。
厂商码：收到消息的厂商码，需要源设备支持才行
送目标相同，命令方向相反，则收到的消息为返回帧。
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

4.3 ZCL 命令功能介绍与解析

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。

ZCL 命令可分为“通用命令”和“控制命令”两类，命令码从 0x00 到 0x0B 均为通用命令，可直接访问属性；0x0F 为控制命令，收发双向对等，不同簇下控制命令携带的参数不同。

功能	命令码	发送	接收	类型
读取设备状态	0x00	ZCL_READ_ATTR_REQ	ZCL_READ_ATTR_RSP	通用命令
修改设备状态	0x01	ZCL_WRTIE_ATTR_REQ	ZCL_WRTIE_ATTR_RSP	通用命令
查询状态上报规律	0x02	ZCL_READ_REPORT_REQ	ZCL_READ_REPORT_RSP	通用命令
修改状态上报规律	0x03	ZCL_WRITE_REPORT_REQ	ZCL_WRITE_REPORT_RSP	通用命令
查看全部状态	0x04	ZCL_DISC_ATTR_REQ	ZCL_DISC_ATTR_RSP	通用命令
查看全部状态带扩展	0x05	ZCL_DISC_ATTR_EX_REQ	ZCL_DISC_ATTR_EX_RSP	通用命令
状态主动上报	0x0A	无	ZCL_REPORT_IND	通用命令
系统默认返回	0x0B	无	ZCL_DEFAULT_RSP	通用命令
发送控制命令	0x0F	ZCL_CMD_SEND	无	控制命令
接收控制命令	0x0F	无	ZCL_CMD_IND	控制命令

4.3.1 读取设备属性（命令码 0x00）

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：

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：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，属性 ID 为小端模式输入。

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	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，小端模式。
ZCL 状态：见《ZCL 状态表》，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：该属性对应的状态值，大小由数据类型中“字节数”一项决定

4.3.2 修改设备属性（命令码 0x01）

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：

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：需要修改的属性数量
属性 ID：需要修改的属性 ID，小端模式输入。
数据类型：数据类型，见《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

返回：

名称	ext data		
	扩展数据		
	AttrNum	AttrList * N	
	错误数量	属性列表	
		属性 ID	ZCL 状态

字节数	1	2	1

错误数量：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：修改无效的属性 ID，小端模式。
ZCL 状态：错误原因，见《ZCL 状态表》

4.3.3 查询属性上报规律（命令码 0x02）

命令码：0x02
备注：仅 E72-2G4M20S1E(Link72) 和 E180ZG120 支持
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，支持自动上报的属性在被查询时会返回 ZCL 状态成功并附带有效的上报规律参数。支持自动上报的属性，需要把该属性所在的端口和该属性的簇绑定（见设置绑定）到接收目标才能启动自动上报（E72-2G4M20S1E(Link72) 作为协调器时会自动设置对方端口绑定属性上传的簇到协调器的接收端口）。

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，小端模式输入。

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，小端模式。
ZCL 状态：见《ZCL 状态表》，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。

4.3.4 修改属性上报规律（命令码 0x03）

命令码：0x03

备注：仅 E72-2G4M20S1E(Link72) 和 E180ZG120 支持

功能：

修改属性自动上报规律，可修改属性自动上报的周期，以及触发上报的属性值变化量。在《ZCL 数据类型表》中“Report 对齐”一项中，如该属性的类型对应的“Report 对齐”为 0，则只支持上报周期的修改，不支持属性值变化量的修改。

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，小端模式输入。

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	
	错误数量	属性列表	
		属性 ID	ZCL 状态
字节数	1	2	1

错误数量：设置无效的属性数量，返回仅包含设置无效的属性

属性 ID：设置无效的属性 ID，小端模式。

ZCL 状态：错误原因，见《ZCL 状态表》

4.3.5 查看全部属性（命令码 0x04）

命令码：0x04

备注：仅 E72-2G4M20S1E(Link72) 支持

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：

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，小端模式输入。

返回：

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：该标志为 1 则表示本次返回的属性 ID 中包含了该簇最后一个属性 ID
属性个数：本次查询返回的属性个数
属性 ID：返回的属性 ID，小端模式。
数据类型：该属性 ID 对应的数据类型

4.3.6 查看全部状态带扩展字段（命令码 0x05）

命令码：0x05
备注：仅 E72-2G4M20S1E(Link72) 支持
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：

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，小端模式输入。

返回：

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	支持操作
字节数	1	1	2	1	1

结束标志：该标志为 1 则表示本次返回的属性 ID 中包含了该簇最后一个属性 ID
属性个数：本次查询返回的属性个数
属性 ID：返回的属性 ID，小端模式。
数据类型：该属性 ID 对应的数据类型
支持操作：bit0 使能=可读，bit1 使能=可写，bit2 使能=支持主动上报

4.3.7 收到属性主动上报（命令码 0x0A）

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。由于只有 E72-2G4M20S1E(Link72) 作为协调器时会自动设置对方端口绑定属性上传的簇到协调器的接收端口，E180ZG120 和 E18 模组作为协调器时需要进行“设置绑定”才能收到

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：收到上报的属性数量，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：收到上报的 16 位属性 ID，小端模式。
数据类型：数据类型，见《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

4.3.8 默认返回帧（命令码 0x0B）

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	
	cmd ID	ZCL status
	命令 ID	ZCL 状态
字节数	1	1

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。
ZCL 状态：见《ZCL 状态表》

4.3.9 发送控制命令（命令码 0x0F）

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：

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，根据簇，厂商码，命令 ID 的不同而决定。

4.3.10 收到控制命令（命令码 0x0F）

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，根据簇，厂商码，命令 ID 的不同而决定。

4.4 各个簇下的属性与控制命令

按照簇（cluster）分类，对各个簇下的属性和控制命令进行列举

4.4.1 基本信息簇（BASIC 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

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

发送控制命令：无

接收控制命令：无

4.4.2 设备标记簇（IDENTIFY 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

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
0x01	IdentifyQuery	查询标记设备	无

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

特别说明：

- “查询标记设备”时，可广播或组播查询
- 仅有处于标记模式的设备会返回“返回查询标记设备”消息

4.4.3 分组管理簇（GROUP Cluster = 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

4.4.4 场景管理簇（SCENES Cluster = 0x0005）

功能：

设备的场景管理功能，在场景模式下设备输出一个预设的物理状态，多个设备可通过组播或广播输入一个预设的物理状态，达到同时控制不同输出的效果。

属性表：

Cluster = 0005，Server				
AttrID	描述符	名称	数据类型	操作
0x0000	SceneCount	场景数量	uint8	只读
0x0001	CurrentScene	当前场景	uint8	只读
0x0002	CurrentGroup	当前场景分组	uint16	只读
0x0003	SceneValid	处于场景模式中	bool	只读
0x0004	NameSupport	支持场景名	bit8	只读

- 一个场景由 8bit 场景 ID+16bit 组 ID 构成，即某个场景需要在特定的分组下才有效。同时相当于把场景扩展到 24bit。

发送控制命令：

Cluster = 0005，Client->Server			
cmdID	描述符	名称	参数

0x00	AddScene	添加场景	uint16 groupID：场景所在分组，设备必须先加组 uint8 sceneID：场景 ID uint16 transTime：场景渐变时间 string sceneName：字符串场景名 uint8 sceneData[]：场景数据，放在命令帧最后
0x01	ViewScene	读取场景	uint16 groupID：场景所在分组 uint8 sceneID：读取的场景 ID
0x02	RemoveScene	移除场景	uint16 groupID：移除场景所在分组 uint8 sceneID：移除的场景 ID
0x03	RemoveAllScene	移除所有场景	uint16 groupID：移除场景所在分组
0x04	StoreScene	保存当前场景	uint16 groupID：场景所在分组，设备必须先加组 uint8 sceneID：场景 ID
0x05	RecallScene	执行场景	uint16 groupID：场景所在分组 uint8 sceneID：场景 ID
0x06	GetSceneMembership	查询所有场景	uint16 groupID：场景所在分组

- 场景数据格式由设备自己决定，设备保存某几个 cluster 下的 attribute 作为场景数据。执行时相当于把 attribute 还原至保存时的状态。

接收控制命令：

Cluster = 0005， Server->Client			
cmdID	描述符	名称	参数
0x00	AddSceneRsp	添加场景返回	uint8 status: ZCL 状态 uint16 groupID：场景所在分组 uint8 sceneID：场景 ID
0x01	ViewSceneRsp	读取场景返回	uint8 status: ZCL 状态 uint16 groupID：场景所在分组 uint8 sceneID：读取的场景 ID uint16 transTime：场景渐变时间 string sceneName：字符串场景名 uint8 sceneData[]：场景数据
0x02	RemoveSceneRsp	移除场景返回	uint8 status: ZCL 状态 uint16 groupID：移除场景所在分组 uint8 sceneID：移除的场景 ID
0x03	RemoveAllSceneRsp	移除所有场景返回	uint8 status: ZCL 状态 uint16 groupID：移除场景所在分组
0x04	StoreSceneRsp	保存当前场景返回	uint8 status: ZCL 状态 uint16 groupID：场景所在分组 uint8 sceneID：场景 ID
0x06	GetSceneMembershipRsp	查询所有场景返回	uint8 status: ZCL 状态 uint8 capacity：还能加多少个场景 uint16 groupID：场景所在分组 uint8 sceneCount：已有场景个数 uint8 sceneList[]：已有场景列表

场景数据结构

场景数据是一个数组，满足以下结构

```
{
    uint16 clusterID,
    uint8   size,
    uint8   data[]
}
```

其中 size 决定 data 的大小，场景数据是由多个这样的结构体构成，总共最大 32 字节，可同时保存多个 cluster 下的多个 attribute。

4.4.5 开关通断控制簇（ON_OFF cluster = 0x0006）

功能：

设备开关状态控制

属性表：

Cluster = 0x0006, Server				
AttrID	描述符	名称	数据类型	操作
0x0000	OnOff	开关状态	bool	读+报+场景

发送控制命令：

Cluster = 0006，Client->Server			
cmdID	描述符	名称	参数
0x00	Off	关闭	无
0x01	On	打开	无
0x02	Toggle	反向	无

接收控制命令：（无）

4.4.6 亮度控制簇（LEVEL cluster = 0x0008）

功能：

设备亮度控制

属性表：

Cluster = 0x0008, Server				
AttrID	描述符	名称	数据类型	操作
0x0000	currentLevel	当前亮度	uint8	读+报+场景

发送控制命令：

Cluster = 0008， Client->Server			
cmdID	描述符	名称	参数
0x00	MoveToLevel	调至亮度	uint8 level：目标亮度 uint16 transTime：渐变时间
0x01	Move	调相对亮度	enum8 mode：模式，0-上升，1-下降 uint8 rate：调节比率
0x02	Step	单步亮度	enum8 mode：模式，0-上升，1-下降 uint8 step：单步比率 uint16 transTime：渐变时间
0x03	Stop	停止渐变	无
0x04	MoveToLevelOnOff	调至亮度带开关	uint8 level：目标亮度 uint16 transTime：渐变时间
0x05	MoveOnOff	调相对亮度带开关	enum8 mode：模式，0-上升，1-下降 uint8 rate：调节比率
0x06	StepOnOff	单步亮度带开关	enum8 mode：模式，0-上升，1-下降 uint8 step：单步比率 uint16 transTime：渐变时间
0x07	Stop	停止渐变	无

接收控制命令：（无）

4.4.7 亿佰特数据传输控制簇（EBYTE cluster = 0xFC08 / manuCode=0x2000）

功能：

亿佰特数据透传自定义簇

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+上报
0x0005	target IEEE	目标 MAC 地址显示	EUI64	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，1-3.33 秒唤醒，2-秒唤醒，3-一直休眠

目标 MAC 显示仅 E180ZG120 模组支持，E180ZG120 可绑定多个目标，目标 MAC 地址仅显示

最近通信的目标

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

- 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

接收命令：

Cluster = 0xFC08， manuCode=0x2000, Sever->Client			
cmdID	描述符	名称	参数
0x00	Data Notify	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

修订历史

版本	修订日期	修订说明	维护人
1.0	2022-11-02	初版	Bin
1.1	2022-12-28	错误更正	Bin

关于我们

销售热线：4000-330-990
公司电话：028- 61543675
技术支持：support@cdebyte.com
官方网站：https://www.ebyte.com
公司地址：四川省成都市高新西区西区大道 199 号 B5 栋

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

