产品应用笔记

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

HEX指令模式下的配网与识别

前言：

本节介绍亿佰特Zigbee模组如何配网与设备识别。主要操作都在协调器上进行，通过协调器去控制节点入网，以及协调器如何知道哪些节点入网，协调器如何知道入网的节点具体设备信息。

准备材料：

一个E18系列模组、E180ZG120A/B模组或E72-2G4M20S1E(Link72)组网管理模组当成协调器使用,再另备一个E180-ZG120A/B模组作为入网节点（路由节点或终端节点均可）。

准备工作：

保证模组在HEX指令模式，模组出厂默认HEX指令模式。其中E18系列模组支持透传模式，若模组在透传模式，向其UART RX口发送”+++”字符串（3字节”+”符号）切换至HEX指令模式。E180-ZG120A/B支持AT指令模式和透传模式，若模组在透传模式则向其UART发送”+++”切换至HEX指令模式，若模组在AT指令模式则发送”AT+EXIT”切换至HEX指令模式。

第一步、设置模组的设备类型：

准备模组A和模组B，确认模组处于HEX指令模式，若模组未处于HEX指令模式，请将模组切换到HEX指令模式。将模组A配置为协调器，模组B配置为路由器或终端节点。

① 模组复位

指令	应答
55 07 00 04 00 FF FF 00 04	55 04 00 04 00 04
说明：收到应答后，模组开始复位	

复位成功后收到异步指令“设备启动通知”

异步
设备启动：55 0D 80 00 01 10 F3 4C 60 FE FF 14 43 0C 14 固件版本 模组MAC地址
说明：收到设备启动，模组复位完成

② 将模组A配置为协调器

指令	应答
55 04 00 05 00 05 协调器	55 04 00 05 00 05 设置成功

③ 将模组B配置为非休眠终端节点

指令	应答
55 04 00 05 02 07 终端节点	55 04 00 05 00 05 设置成功

④ 将模组B配置为路由器

指令	应答
55 04 00 05 01 04 终端节点	55 04 00 05 00 05 设置成功

注意：把模组设置成协调器，路由器，终端节点，休眠终端后，必须再复位一下模组才能生效。指令复位，按键复位，上电复位均可。

第二步、模组配网：

① 模组A开始配网，模组A成功建立网络

指令	应答
55 03 00 02 02	55 04 00 02 00 02
收到2条异步指令	
收到<系统通知-网络状态变更>： 55 29 80 01 01 F3 4C 60 FE FF 14 43 0C 19 91 14 00 00 22 44 EA D4 CA FD 93 2D D0 68 B2 72 8E E0 6F 99 E4 F9 EC AA EE 25 27 EF F0 01 表示已组网 F3 4C 60 FE FF 14 43 0C 为模组A（协调器）MAC 19 为信道 91 14 为PANID 00 00 为短地址 22 44 EA D4 CA FD 93 2D 为扩展PANID D0 68 B2 72 8E E0 6F 99 E4 F9 EC AA EE 25 27 EF 为网络密钥 说明：协调器在0x19=25信道建立网络，PANID为0x1491，短地址为0x0000	
收到<系统通知-允许入网时间窗口通知>： 55 04 80 02 B4 36 允许入网180秒 说明：模组A成功建立网络	

② 模组B开始配网，模组B加入网络

指令	应答
55 03 00 02 02	55 04 00 02 00 02
收到异步指令	
收到<系统通知-网络状态变更>： 55 29 80 01 02 E9 CE D6 FE FF 14 43 0C 19 91 14 2C 6A 22 44 EA D4 CA FD 93 2D D0 68 B2 72 8E E0 6F 99 E4 F9 EC AA EE 25 27 EF 9B 02 表示第一次入网 E9 CE D6 FE FF 14 43 0C 表示模组B（终端节点）MAC 19 为信道 91 14 为PANID 2C 6A 为短地址 22 44 EA D4 CA FD 93 2D 为扩展PANID D0 68 B2 72 8E E0 6F 99 E4 F9 EC AA EE 25 27 EF 为网络密钥 **说明：**模组B加入网络成功，模组B以终端节点的方式加入到协调器A中，信道、PANID、扩展PANID，网络密钥与协调器雷同，短地址为0x6A2C	

③ 模组A检测到模组B入网

模组	接收数据
模组A	收到<系统通知-检测节点入网>： 55 10 80 03 E9 CE D6 FE FF 14 43 0C 2C 6A 00 00 00 6E E9 CE D6 FE FF 14 43 0C 为模组B的MAC 2C 6A 为模组B的短地址 00 00 为父节点短地址 00 表示第一次入网 说明：终端节点模组B通过协调器模组A作为父节点入网，协调器模组A检测到终端节点模组B
	收到<系统通知-节点短地址通知>: 55 0E 80 04 E9 CE D6 FE FF 14 43 0C 2C 6A 02 6B E9 CE D6 FE FF 14 43 0C 为模组B的MAC 2C 6A 为模组B的短地址 02 为非休眠终端节点 **解析：**模组B作为一个非休眠的终点节点加入网络，该消息是模组B广播到全网络，协调器

	和路由节点都能收到。若模组B在运行过程中修改了自己的短地址，或重新上电，都会向全网络通知该消息。

当B通过路由入网，A检测到B入网：

模组	接收数据
模组A	收到<系统通知-检测节点入网>： 55 10 80 03 E9 CE D6 FE FF 14 43 0C 88 FC 52 19 00 17 E9 CE D6 FE FF 14 43 0C 为模组B的MAC 88 FC 为模组B的短地址 52 19 为父节点短地址 00 表示第一次入网 说明：B通过路由入网，协调器可以检测到B是通过哪个父节点入网的
	第二次收到<系统通知-检测节点入网>： 55 10 80 03 E9 CE D6 FE FF 14 43 0C 88 FC 52 19 00 17 说明：节点通过路由入网，符合zigbee 3.0规范的路由器会向协调器提交两次验证请求，协调器也会收到两次相同的节点入网信息。
	收到<系统通知-节点短地址通知>： 55 0E 80 04 E9 CE D6 FE FF 14 43 0C 88 FC 02 59 E9 CE D6 FE FF 14 43 0C 为模组B的MAC 88 FC 为模组B的短地址 02 为非休眠终端节点

协调器检测节点入网的注意事项：

<系统通知-节点短地址通知>受限于广播风暴，当多个模组同时入网时，该消息可能不能被广播出去，导致协调器收不到该消息，因此不能作为检测节点入网的依据。而<系统通知-检测节点入网>，是以协调器检测到模组入网请求作为判断条件，其中存在模组入网失败的风险。因此建议协调器若需要成功检测模组入网，可以在收到<系统通知-节点短地址通知>的5秒后，根据入网模组的短地址发送任何请求查询类指令，只要有返回消息，即可认定模组成功入网。

第三步、识别入网节点

使用E180-ZG120系列模组或E18系列模组作为协调器时：

协调器获取入网节点的应用端口列表

指令	应答
发送<ZDO命令-查询节点端口数>： 55 05 01 05 88 FC 70 目标短地址 **解析：**该命令没有命令参数，只有命令ID和短地址	55 05 01 05 00 02 06 命令有效 命令编号 **解析：**该命令输入有效，模组为该命令分配的查询编号为0x02

等待异步指令……

收到2条异步指令
等待若干毫秒，收到<ZDO发送确认>： 55 07 8F 01 88 FC 02 00 F8 目标短地址 命令编号 发送成功 **解析：**该命令被成功发送出去，等待目标回复执行结果
再等待若干毫秒，收到<ZDO响应-查询节点端口数>: 55 0C 81 05 88 FC 02 00 04 01 02 03 04 F2 对方短地址 命令编号 对方执行成功 端口数 端口列表 **解析：**B有4个应用端口，分别为端口1，端口2，端口3，端口4

协调器A查看节点B的4个应用端口，分别是什么

先查看节点B的端口1：

指令	应答
发送<ZDO命令-查询节点端口信息>: 55 06 01 04 88 FC 01 70 目标短地址 目标端口	55 05 01 04 00 03 06 命令有效 命令编号

解析：查询节点B（短地址0xFC88）的应用端口1	解析：该命令输入有效，模组为该命令分配的查询编号为0x03
收到2条异步指令	
收到<ZDO发送确认>: 55 07 8F 01 88 FC 03 00 F9 目标短地址 命令编号 发送成功 说明：协调器在0x19=25信道建立网络，PANID为0x1491，短地址为0x0000	
收到<ZDO响应-查询节点端口信息>: 55 21 81 04 88 FC 03 00 01 04 01 50 00 00 05 00 00 03 00 04 00 07 00 08 FC 04 03 00 06 00 08 00 08 FC AA 88 FC 为对方短地址 03 为命令编号 00 为对方执行成功 01 为目标端口 04 01 为应用端口轮廓 50 00 为设备ID 00 为设备版本 05 为输入簇大小 00 00 03 00 04 00 07 00 08 FC 为输入簇列表 04 为输出簇大小 03 00 06 00 08 00 08 FC 为输出簇列表 解析：查询到节点B的端口1的信息，端口轮廓为0x0104是一个ZCL Home Automatic的应用，设备ID为0x0050对应“家庭网关”设备，设备版本为0，输入簇列表共5个簇分别为{0x0000, 0x0003, 0x0004, 0x0007, 0xFC08}，输出簇4个分别为{0x0003,0x0006,0x0008,0xFC08}。通过查表，我们可以分析出节点B的端口1支持“基本信息(0x0000)”、“设备标记(0x0003)”、“分组管理(0x0004)”、“开关输出(0x0007)”、“数据传输(0xFC08)”共5种本地功能，以及可以对外输出“设备标记(0x0003)”、“开关控制(0x0006)”、“亮度控制(0x0008)”、“数据传输(0xFC08)”共4种功能。	

注意事项：

对于某些使用Silicon Labs芯片的zigbee入网设备上，可能出现<ZDO发送确认>和<ZDO响应>发生颠倒的现象，这个是Silicon Labs的ZigBee系列产品的BUG，属于正常现象。建议正确使用方法是，使用<ZDO命令>点播查询目标节点时，等待<ZDO响应>的超时18秒，若在等待过程中<ZDO发送确认>返回了错误的状态，提前结束等待，后续收到的响应消息当成无效消息处理。

然后查看模组B的端口2：

模组B的端口3，端口4与端口2完全相同

指令	应答
发送<ZDO命令-查询节点端口信息>: 55 06 01 04 88 FC 02 70	55 05 01 04 00 04 01
收到2条异步指令	
收到<ZDO响应-查询节点端口信息>: 55 19 81 04 88 FC 04 00 02 04 01 01 01 00 05 03 00 04 00 05 00 06 00 08 00 00 FB 目标端口 应用端口轮廓 设备ID 设备版本 输入簇大小 输入簇列表 输出簇大小 说明：协调器在0x19=25信道建立网络，PANID为0x1491，短地址为0x0000	
收到<ZDO发送确认>: 55 07 8F 01 88 FC 04 00 FE 解析：本次查询出现了<ZDO发送确认>和<ZDO响应>颠倒的现象。查询目标端口2，其轮廓为0x0104同样是ZCL Home Automatic应用，设备ID为0x0101对应”调光灯”这种设备应用。5个输入簇{0x0003,0x0004,0x0005,0x0006,0x0008}表示其支持“设备标记(0x0003)”、“分组管理(0x0004)”、“场景快照(0x0005)”、“开关控制(0x0006)”、“亮度控制(0x0008)”。端口2的输出簇为空。	

各个簇功能简述：

基本信息(0x0000)：记录和保存设备出厂信息，版本，生产日期的功能

设备标记(0x0003)：设备切换标记状态，可以被肉眼发现，以及被同网络其它设备找到
分组管理(0x0004)：设备编组管理功能，编组后可以收到组播的消息，不需要收组播消息时可退出编组
场景快照(0x0005)：设备设置保存一个复杂的物理状态，然后可通过一条指令迅速切换至该状态
开关控制(0x0006)：设备输出一个可在0和1状态切换的状态
开关输出(0x0007)：设备模拟一个按键或开关的功能
亮度控制(0x0008)：设备输出一个在0~255之间切换的状态，例如PWM波。
数据传输(0xFC08)：设备通过串口输入输出数据

补充教程：E72-2G4M20S1E(Link72)自动识别入网设备

使用E72-2G4M20S1E(Link72)模组作为协调器，E180-ZG120A/B模组以路由器的方式入网。E72-2G4M20S1E(Link72)具有强大的并行处理能力，可以在大量节点配网的同时自动查询入网节点的全部应用端口。E72-2G4M20S1E(Link72)需要先软启动才能运行，用来保护启动中的上位机，如果上位机不需要被保护，可以开启自动启动。

第一步：启动E72-2G4M20S1E(Link72)并进入配网模式

E72-2G4M20S1E(Link72)软启动：

指令	应答
55 04 00 01 01 00 开启自动启动	55 04 00 01 00 01 **解析：**发送软启动后等待3秒才收到反馈，说明E72-2G4M20S1E(Link72)已经创建过网络，正在重启之前的网络。
收到异步指令	
收到<系统通知-网络状态变更>: 55 29 80 01 01 ED 53 D1 26 00 4B 12 00 0B F6 E8 00 00 06 83 C1 60 B0 58 2C 16 E2 72 8B A2 7C D0 8E 20 26 A5 0E 9C FA 2F 56 72 28	

然后E72-2G4M20S1E(Link72)开始配网：

同时模组E180ZG120配置成路由器，并开始配网

指令	应答
55 03 00 02 02	55 04 00 02 00 02
收到2条异步指令	
收到<系统通知-允许入网时间窗口通知>: 55 04 80 02 B4 36	
收到<系统通知-网络状态变更>: 55 29 80 01 02 ED 53 D1 26 00 4B 12 00 0B F6 E8 00 00 06 83 C1 60 B0 58 2C 16 E2 72 8B A2 7C D0 8E 20 26 A5 0E 9C FA 2F 56 72 2B	

第二步：E72-2G4M20S1E(Link72)检测节点入网

协调器检测到新节点入网:

数据接收	
收到<系统通知-检测节点入网>	55 10 80 03 4D 4D 60 FE FF 14 43 0C A7 B1 00 00 00 AF MAC地址 短地址 第一次入网
收到<系统通知-节点短地址通知>	55 0E 80 04 4D 4D 60 FE FF 14 43 0C A7 B1 01 A9 MAC地址 短地址 路由节点
解析：E72-2G4M20S1E(Link72)协调器检测到MAC地址4D 4D 60 FE FF 14 43 0C的路由节点入网，短地址0xB1A7	

第三步：E72-2G4M20S1E(Link72)自动获取入网节点信息

协调器自动检测到入网节点的应用端口1的信息：

数据接收	
收到<系统通知-设备信息通知>	55 28 80 05 00 01 4D 4D 60 FE FF 14 43 0C A7 B1 01 04 01 50 00 05 00 00 03 00 04 00 07 00 08 FC 04 03 00 06 00 08 00 08 FC F0 终结标志 虚拟SN 短地址 端口号 端口轮廓 设备ID 输入簇大小 输入簇列表 输出簇大小 输出簇列表
解析：入网节点的端口1信息，端口号和MAC地址从新整合成了虚拟SN方便云端管理。同时该消息中可以获取到该应用端	

口的应用轮廓，设备ID，输入簇和输出簇，和前面查看端口1的示例完全一致。入网节点的端口1为“家庭网关”类设备，支持“基本信息(0x0000)”、“设备标记(0x0003)”、“分组管理(0x0004)”、“开关输出(0x0007)”、“数据传输(0xFC08)”共5种本地功能，以及可以对外输出“设备标记(0x0003)”、“开关控制(0x0006)”、“亮度控制(0x0008)”、“数据传输(0xFC08)”共4种功能。

收到端口2的信息：

数据接收	
收到<系统通知-设备信息通知>	55 20 80 05 00 02 4D 4D 60 FE FF 14 43 0C A7 B1 02 04 01 01 01 05 03 00 04 00 05 00 06 00 08 00 00 A5 终结标志还没完 虚拟SN 设备ID 输入簇大小 输入簇列表 输出簇大小
解析：节点的端口2使用了与端口1不同的虚拟SN，设备ID为”调光灯”,支持“分组管理(0x0004)”、“场景快照(0x0005)”、“开关控制(0x0006)”、“亮度控制(0x0008)”共5种应用功能，无输出控制功能	

收到端口3的信息：

数据接收	
收到<系统通知-设备信息通知>	55 20 80 05 00 03 4D 4D 60 FE FF 14 43 0C A7 B1 03 04 01 01 01 05 03 00 04 00 05 00 06 00 08 00 00 A5
解析：端口3与端口2的功能完全雷同	

收到端口4的信息：

数据接收	
收到<系统通知-设备信息通知>	55 20 80 05 01 04 4D 4D 60 FE FF 14 43 0C A7 B1 04 04 01 01 01 05 03 00 04 00 05 00 06 00 08 00 00 A4 终结标志结束
解析：端口4与端口2，端口3功能完全雷同，端口4为入网节点最后一个应用端口，入网节点共4个应用端口	

亿佰特Zigbee 3.0系列模组在HEX模式下除满足模组自身之间的组网，同时也兼容第三方的ZigBee 3.0产品。完整的“配网->识别”流程适用于所有的Zigbee设备组网。若使用环境中可保证参与组网的设备均为亿佰特Zigbee 3.0系列模组，可跳过“识别”这一步。也可通过使用AT命令的方式，快速配网。

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：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.