User Manual

ZM32 深入使用手册

ZigBee 无线模块

UM01010101 V1.01 Date: 2020/03/16 产品用户手册

类别	内容
关键词	ZM32，无线模块，使用手册
摘要	详细介绍 ZM32 的使用方法和配置命令

ZLG

修订历史

文档版本	日期	原因
V1.00	2019/08/01	创建文档
V1.01	2020/03/16	加入流程图，加入新的配置白名单命令，描述广播限制
V1.02	2020/10/15	章节 5.2 d)中删除可配置“本地地址”的描述

目录

1. 如何使用此文档

本文档旨在帮助用户深入学习 ZM32 系列 ZigBee 模块的使用方法，通过 WirelessCfg 无线配置工具（以下简称配置工具）的辅助，深入探索 ZM32 系列 ZigBee 模块的使用逻辑、各指令使用特点。

第 2～5 章节简单介绍了产品、评估板以及配置工具使用。

第 6～13 章节中，关于配置工具的每一项上位机操作均链接到命令集，可以快速查看命令使用详情，便于用户的编码工作。

第 14 章节详细了 ZM32 系列 ZigBee 模块的所有命令，详细阅读本章内容，对用户的编码工作有很大帮助。

2. 产品简介

ZM32 系列是广州致远电子基于 Silicon Labs EFR32 系列无线 SoC 开发的一系列低功耗、高可靠性的 ZigBee 模块，并提供一个完整的基于 IEEE802.15.4 标准 ISM 频段的应用集成方案。产品经过系列权威射频仪器的检验和认证，并结合多年的市场经验和该行业用户的实际需求，将无线产品极复杂的通讯协议集成到内置的 SoC 中，支持串口透明传输模式，并集成快捷易用的自组网功能，提供多路可配置的 AD、IO、PWM 接口，化繁为简，大幅简化无线产品复杂的开发过程，使您的产品以更低的成本快速投入市场，由于超小的体积和超低功耗设计，在各种智能设备中得到广泛应用。

图 2.1　ZM32 系列 ZigBee 模块实物图

3. 透传模块基础知识

3.1 模块特点

标准 ZigBee 设备类型包括协调器、路由器和终端，而建立一个 ZigBee 网络除了必须要有协调器之外，其他按需加入路由器或终端即可。其特点如下：

- **节点容量大**

当 ZigBee 采用 16bit 短地址管理方式，在轮询机制下，理论上节点容量高达 65535 个。

- **完全透传**

模块采用 3 线制串口全透明传输方式，即发送接收数据的长度和内容完全一致。其优势在于可以创建自己的协议格式，不再局限于固定第三方协议。

- **无需二次开发**

模块所有网络参数均可使用配套的 WirelessCfg 配置工具或串口配置命令进行配置。当节点数量不多时，通过配置工具配置 PAN ID、通道号等参数，即可马上投入使用。当节点多到一定的数量时，如果逐个节点进行配置，则显然非常麻烦，此时推荐使用串口配置命令或配置工具，启动自组网功能，即可快速实现现场实时动态配置及自组网。

- **数据安全度高**

模块提供了 3 种密钥验证方式，确保数据的安全性。

方式 1：模块登录密码，使能后，必须登录才可修改模块参数。

方式 2：配置密钥，配置密钥使用 AES-128 进行加密，所有模块必须确保配置密钥相同才可以加入网络中。

方式 3：网络密钥，网络传输的数据均按 AES-128 进行加密，该密钥只有协调器有效，当从节点加入网络后，协调器会将该密钥下发到从节点。

- **快速添加路由**

模块采用了即放即用的智能路由算法，当两个节点之间的距离超出通信范围时，只要在两个节点之间加入路由设备，其它任何网络参数都不要修改即可恢复通信，显然此路由方式特别便于施工。

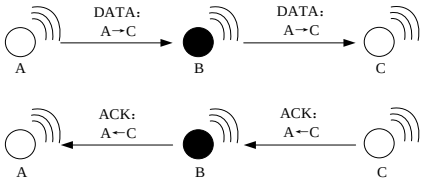

图 3.1 模块通讯示意图

当 A 节点向 C 节点发送数据时，无需知道是否存在 B 节点，只需将目标节点指向 C，则 B 节点会根据源地址和目标地址进行转发，详见图 3.1。当扩展到多级通讯时，同样是 A 节点，只需设置好目标节点即可与该节点通讯，节点 B 和节点 C 负责转发，详见图 3.2。

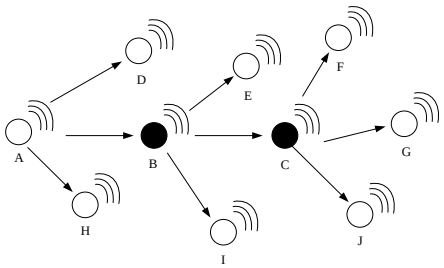

图 3.2 多级通讯示意图

模块采用全透传组网通讯，即可构建多种型态的网络拓扑结构。

- **P2P 结构**

在 P2P（Peer to Peer）点对点对等网络环境中，同处于同一个网络内的所有路由设备都处于对等的地位，整个网络不依赖专用的集中服务器。网络中的路由设备既能充当网络服务的请求者，又对其它设备的请求作出响应提供资源和服务。

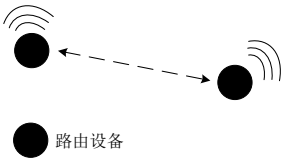

图 3.3　点对点通讯示意图

如图 3.3 所示的 ZigBee 点对点结构是最基本的拓扑结构，专用于构建两个节点之间的通信，该方式节点参数固定，只要将两个节点的目标互相指向即可实现通信。

注：路由和路由点对点，不需要依赖集中服务器，终端则需要依赖集中服务器（集中服务器，其实就是父节点或路由）。

- **星型网络拓扑结构**

星型结构是最古老的一种连接方式，大家每天都使用的电话就属于这种结构，一般网络环境都被设计成星型拓扑结构，因此星型结构是广泛而又首选的网络拓扑设计之一。

在星型拓扑结构中，网络中的各节点通过点对点的方式连接到一个中央节点上，由该中央节点向目的节点传送信息。中央节点执行集中式通信控制策略，因此中央节点相当复杂，负担比各节点重得多，在星型网中任何两个节点要进行通信都必须经过中央节点控制。

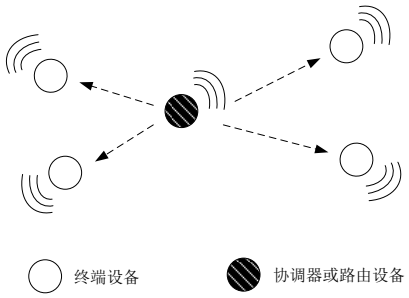

图 3.4　星型网络拓扑结构

如图 3.4 所示的星型拓扑结构也称为主从结构，该拓扑网络属于集中控制型网络，整个网络由中心节点执行集中式通信控制管理，各节点之间的通信都要通过中心节点。ZM32 系列 ZigBee 模块使用中，若从机数量超过 50 台，为保证通讯稳定，推荐使用混合型拓扑结构。

- **中继路由结构**

中继（Relay）是两个交换中心之间的一条传输通路，中继线是承载多条逻辑链路的一条物理连接。在日常生活中，我们经常需要通过家里的电话和朋友聊天，或者通过办公室的电话和公司外的客户联系，要实现这些通话都离不开中继。在无线通信中，中继的概念是指允许大量的用户在一个小区内共享相对较小数量的信道，即从可用信道库中给每个用户按需分配信道。

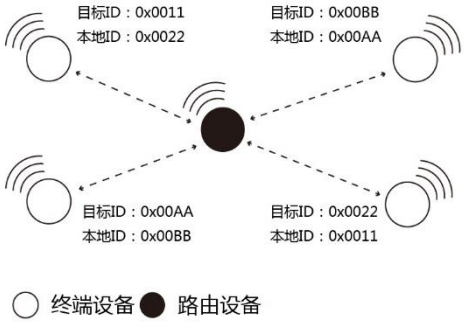

图 3.5　中继路由结构

如图 3.5 所示的是最基础的中继路由拓扑图，且终端可任意切换通信目标，实现任意节点互相通信。

- **混合型网络拓扑结构**

如图 3.6 所示的是将两种或几种网络拓扑结构混合起来构成的一种网络拓扑结构，又称为混合型网络，其不仅具备星型网络的简洁与低功耗，而且兼备 Mesh 网络的超远距离传输能力和自修复能力。在混合型网络中，路由器组成网状结构，而终端则在其周围呈现星型分布。路由中继扩展了网络的传输距离，同时提供了容忍故障的能力，在某些路由出现问题或强干扰时，通信路径会进行自动调整，以确保信息到达。

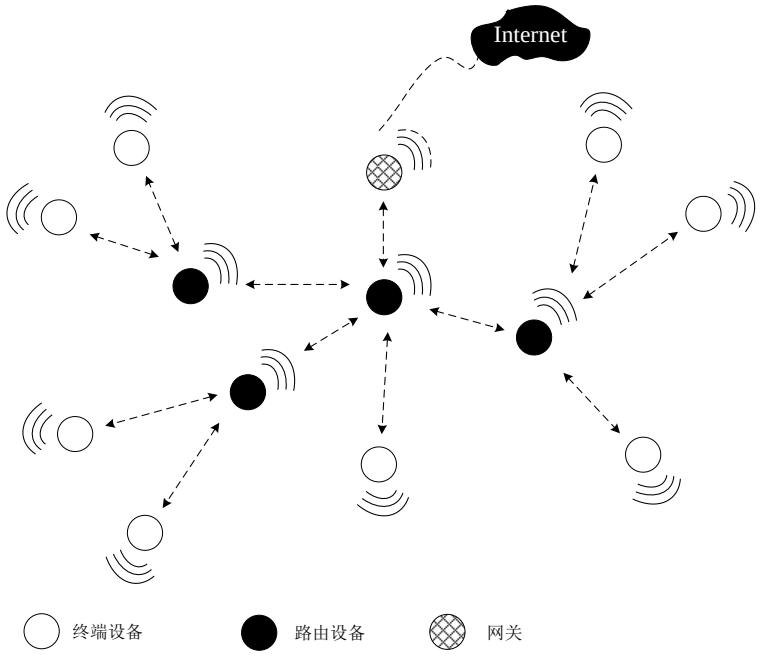

图 3.6　Mesh 网络拓扑结构

3.2　节点类型说明

设备分为 3 种类型终端设备（End Device）、路由设备（Router）和协调器设备(Coordinator)，网络可通过 ZigBee 网关接入互联网，详见表 3.1。

表 3.1　节点类型说明

节点类型	说明
终端设备（End Device）	终端设备的主要任务是发送和接收消息，不允许其它节点与终端设备相连，当没有数据收发时，则进入休眠状态；当需要收发数据时，则通过 MCU 唤醒进入工作状态。
路由设备（Router）	允许其它节点与路由设备相连，以扩大网络的覆盖范围，其主要任务为转发报文，起到中继路由作用，并具备终端设备的所有功能。 **注意 1：**路由器必须保持活动状态，保证终端报文实时转发，因此不允许进入休眠状态。如果一个节点通往另一个节点存在多条路径时，当其中一条路径故障，网络会自动调整到其它最优的路径进行传输，以确保数据到达。 **注意 2：**ZigBee 通信效率会随着路由级数的增加而下降，所以路由器必须按需布局。
协调器设备（Coordinator）	起着建立网络的作用，控制着是否允许其它节点加入网络中，存储网络内所有设备的信息，并具备路由设备的所有功能。其主要任务为管理网络，记录节点信息，转发报文，并起到中继路由作用。 **注意：**协调器必须保持活动状态，确保报文的实时转发，因此不允许进入休眠状态。如果一个节点通往另一个节点存在多条路径时，即便其中一条路径出现故障，则网络会自动调整到其它路径传输，以确保数据到达。

注：模块默认出厂设置为终端设备，若是需要用到路由设备、协调器设备，需要重新进行配置。

3.3 软件基本配置参数

模块提供了丰富的可配置的参数，可根据实际的应用需求灵活运用，以构建不同形式的网络，详见表 3.2。以下所有配置参数均可通过配置工具或指令进行配置。

表 3.2 模块主要配置参数

配置信息	参数范围	功能说明
PAN ID	0x0000~0xFFFF	PAN ID 即 ZigBee 局域网 ID，用于判断自身所属的网络的标识。可互相通信的节点，PAN ID 必须相同，且必须保证在同一工作区域内的相邻网络的 PAN ID 不同。0xFFFF 为无效的 PAN ID，当配置成 0xFFFF 则设备离开当前网络。
本地网络地址	0x0000~0xFFFF	用于区分网络中各个节点，节点短地址即为本地网络地址，只读，未加入网络中，则网络地址为 0xFFFF。
目标网络地址	0x0000~0xFFFF	当前的通信目标网络地址，可通过配置命令随时切换。
本地 MAC 地址	64bit MAC	默认使用出厂 MAC 地址。支持修改，仅加入网络前设置生效，设置成全 FF 将恢复出厂 MAC 地址。
目标 MAC 地址	64bit MAC	当前的通信目标 MAC 地址，可通过配置命令随时切换。
设备类型	0、1、2	设备类型为 0，即为终端设备；设备类型为 1，即为路由设备；设备类型为 2，即为协调器设备。
通道号	CH 11~26	ZigBee 提供 16 个物理信道，必须在同一通道下的节点才可能互相通信。在同一工作区域内的相邻网络，建议使用不同的通道，以免相互干扰导致通信效率降低。比如：工作区域内存在大量的 2.4G Wi-Fi 热点，可能会降低 ZigBee 的通信效率，这时可选择 CH11、15、20、25、26，可有效减少干扰。
发送模式	0、1、2、3	单播模式就是在单个发送者和单个接受者之间的通信，广播模式就是一个发送者和多个接受者之间的通信。发送模式为 0，即为单播模式；发送模式为 1，即为广播给所有设备；发送模式为 2，广播给所有非睡眠设备；发送模式为 3，广播给协调器和所有路由器；发送模式为 4，即组播模式。
传输速率	250Kbps	ZigBee 无线通信速率固定为 250Kbps。
发送功率	0~26 级	模块提供 27 级功率可调。 0x00：-30dBm、0x01：-25dBm、0x02：-20dBm、0x03：-15dBm、0x04：-10dBm、 0x05：-5dBm、 0x06：0dBm、0x07：5dBm、0x08：10dBm、 0x09：15dBm、 0x0A：19dBm；0x10：0dBm、0x11：1dBm、 0x12：2dBm、 0x13：3dBm、0x14：4dBm、 0x15：5dBm、 0x16：6dBm、0x17：7dBm、 0x18：8dBm、 0x19：9dBm、 0x1A：10dBm、 0x1B：11dBm、 0x1C：12dBm、 0x1D：13dBm、0x1E：14dBm、 0x1F：15dBm。
目标组号	0x0000~0xFFFF	当前的通信分组(在组播模式下)，可通过配置命令随时切换。

3.4 模块状态指示

模块有 STATE 管脚，可接 LED 指示灯，用于指示当前模块的状态，如表 3.3 所示。

表 3.3 STATE 状态指示

设备类型	状态	STATE 管脚状态（循环指示）
路由器、终端设备	升级模式	3s 高电平后，周期①变化 5 次
	无配置网络信息	3s 高电平后，周期变化 4 次
	连接中	3s 高电平后，周期变化 3 次
	已经加入网络	3s 高电平后，周期变化 2 次
协调器	升级模式	3s 低电平后，周期②变化 5 次
	无配置网络信息	3s 低电平后，周期变化 4 次
	建网中	3s 低电平后，周期变化 3 次
	建网完成	3s 低电平后，周期变化 2 次
	允许加入 （只有建网完成才会有该状态）	3s 低电平后，周期变化 1 次

Note：

1.一个周期为 200ms 低电平+200ms 高电平。

2.一个周期为 200ms 高电平+200ms 低电平。

4. 评估板简介

4.1 评估板介绍

ZM32A Demo Board 是 ZM32 系列 ZigBee 模块配套的评估套件，该评估套件可以评估该模块的所有功能，包括无线收发、IO 功能、ADC 功能、PWM 功能，将模块的休眠、唤醒等功能以按键方式呈现，方便进行该类功能评估，评估板提供了指示灯，可以快速判断模块的运行状态。评估板安装后如图 4.1 所示。

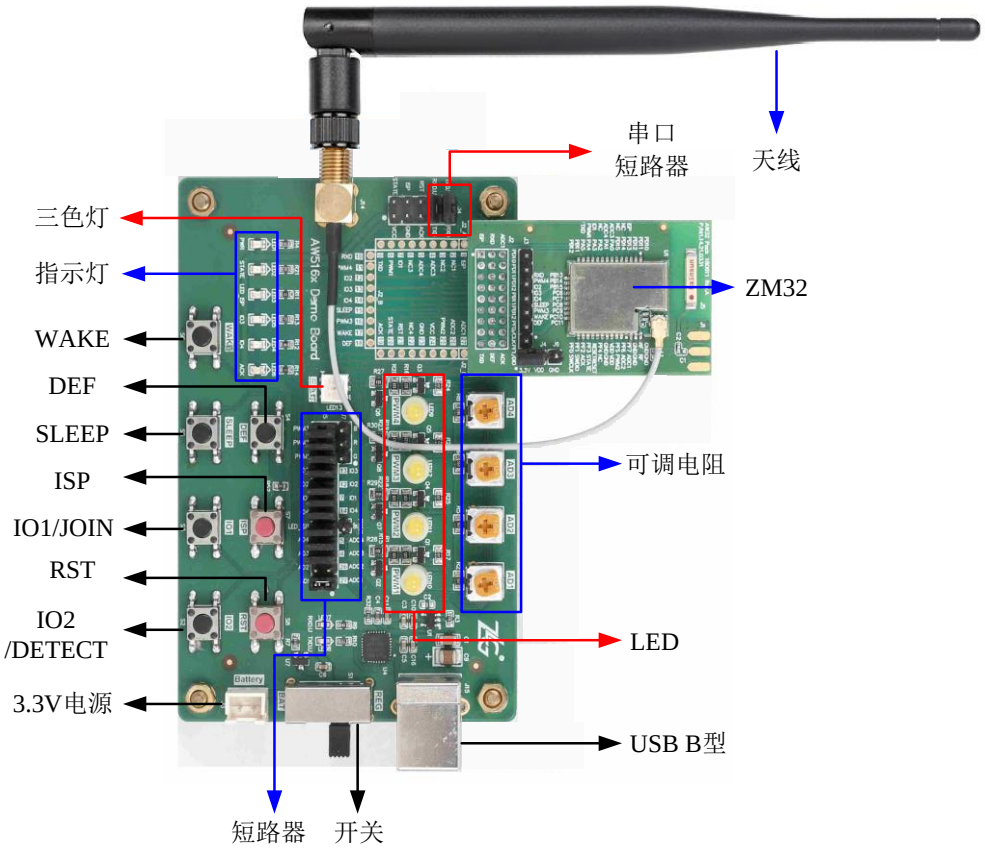

图 4.1 评估板实物图

4.2 评估板功能简介

评估板各区域功能描述，详见表 4.1。

表 4.1 评估板功能描述

类别	名称	功能介绍
灯	三色灯	评估 PWM1、2、3 的输出，需要将短路器对应短接 G、R、B。
	指示灯	具有 PWR（电源）、STATE（工作状态）、LED_ISP（ISP 功能）、IO3、IO4 和 ACK 的指示功能。
	LED	分别对应 4 路 PWM，评估 PWM 输出功能。
按键	WAKE	下降沿唤醒休眠的终端设备，低电平防止终端进入休眠。
	DEF	3s 低电平恢复出厂。
	SLEEP	低电平进入休眠模式，仅终端有效。
	ISP	拉低管脚并复位，复位后仍保持 100ms 以上的低电平可进入升级模式。
	IO1	I/O1，自组网时作为 JOIN：协调器允许入网、终端/路由加网。
	RST	复位，保持 10ms 低电平复位。
	IO2③	I/O2，自组网时作为 DETECT：协调器建网。
外接电源	3.3V 电源	用于外部直流电源接入。
电源开关	开关	使用 USB B 型口时，需要拨到 REG 端；使用外接电源时，需要拨到 BAT 端。
USB	USB B 型	USB 输入，同时提供整板供电。
可调电阻	可调电阻	通过调整电阻值，评估 ADC 采集功能。
模块	ZM32	评估套件中默认是 ZM32P2S24E 模块，需要搭配外接天线使用。
串口短路器	串口短路器	TXD.U 表示由 USB 转的串口发送，TXD 表示 ZM32 模块串口的发送，RXD.U 与 RXD 同理。
天线	天线	评估套件默认配备 5.0dBi 棒状天线。

5. 配置工具简介

5.1 配置工具功能简介

配置工具以可视化的方式提供了 ZM32 系列 ZigBee 模块所有命令配置，方便用户快速上手，无需代码也能快速验证各项操作。

同时，为了一站式评估 ZM32 模块，配置工具新增了**距离测试**、**网络拓扑**、**帧编辑器**、**帧解释器**四项特色功能，全景呈现 ZM32 模块的优异性能。

5.1.1 距离测试功能

测试本地设备与远程设备间的 RSSI 值，以此判断设备间通信的信号强度，为现场施工布局提供有利的参考。一般，我们根据 RSSI 值将信号划分为三个等级，如表 5.1 所示。

表 5.1 评估板功能描述

RSSI/dBm	信号等级
RSSI＞-75	优
-75≥RSSI＞-85	中
-85≥RSSI	差

同时，距离测试功能提供了丢包率测试，更加直观判断设备间通信质量。各类曲线为用户直观展示了测试的过程数据，如图 5.1 所示。

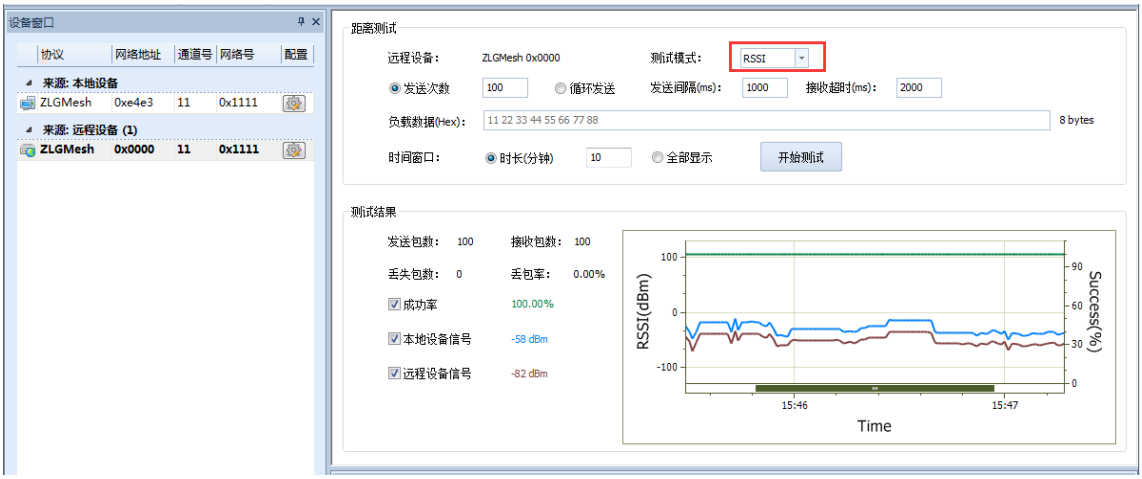

图 5.1 距离测试界面

5.1.2 网络拓扑功能

距离测试功能只能点对点进行测试，当需要查看整个网络的总体情况，需要用到网络拓扑功能。配置工具支持搜索全网络中的设备，并显示设备间的连接关系及对应的信号质量，同时支持测试数据导出到表格。网络拓扑功能增加了**自动布局**和**导入地图**两大特色功能。

通过自动布局功能，能够将错乱无章的拓扑显示进行自动布局，最终呈现出清晰的网络拓扑结构，如图 5.2 所示。

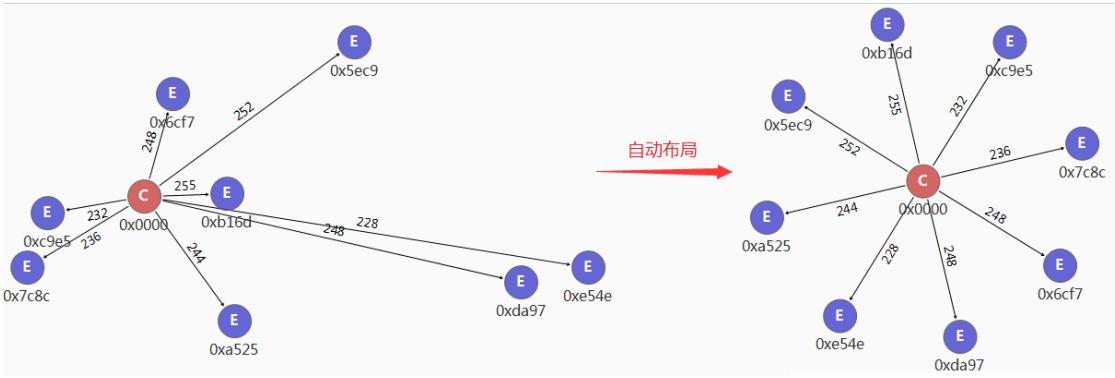

图 5.2　网络拓扑自动布局

通过导入地图背景，能够将任意的施工图导入进来，同时在拓扑图中任意拖动设备，将设备放到指定的位置，让用户的设备安装位置、信号质量、拓扑结构一目了然，如图 5.3 所示。

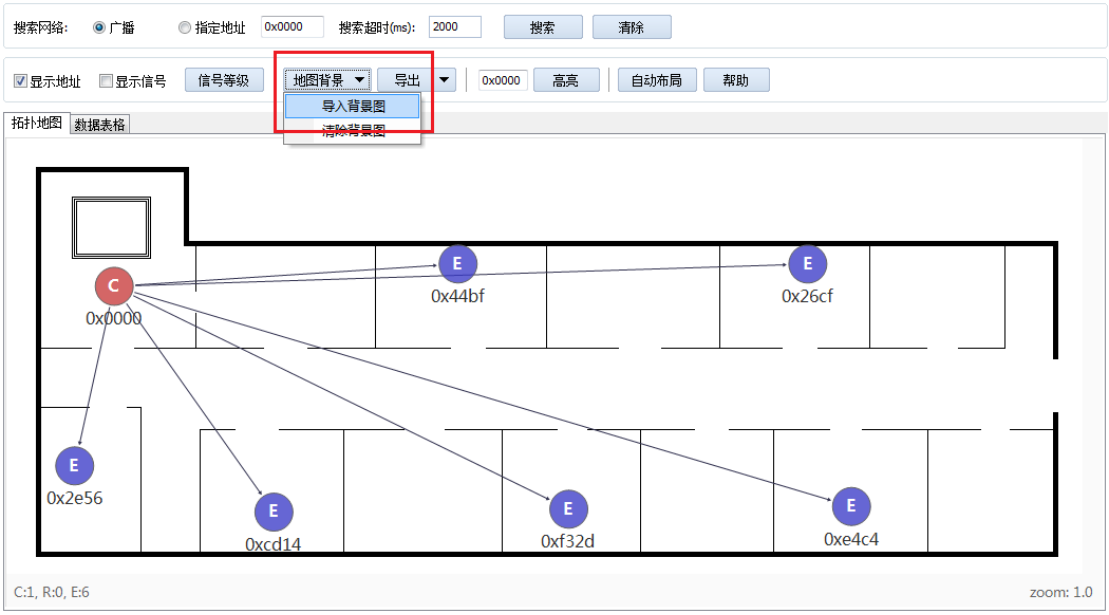

图 5.3　导入背景图功能

5.1.3 帧编辑器功能

针对部分命令，由于需要填入比较长的数据，可以通过*帧编辑器*，可视化地编辑用户的帧数据，如图 5.4 所示。

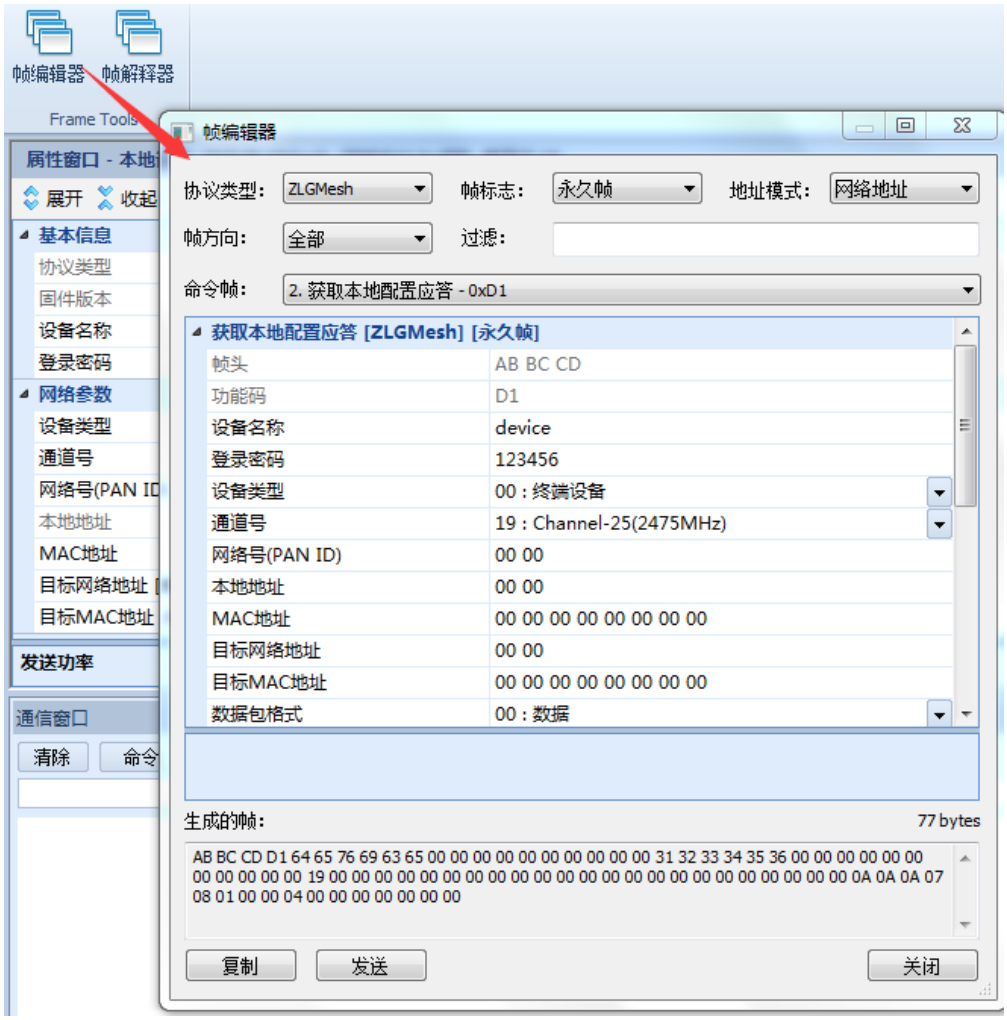

图 5.4　帧编辑器功能

5.1.4 帧解释器功能

模块的应答报文往往包含了众多内容，通过帧解释器，能够可视化应答报文内容，方便用户快速获知自己想要的数据内容，如图 5.5 所示。

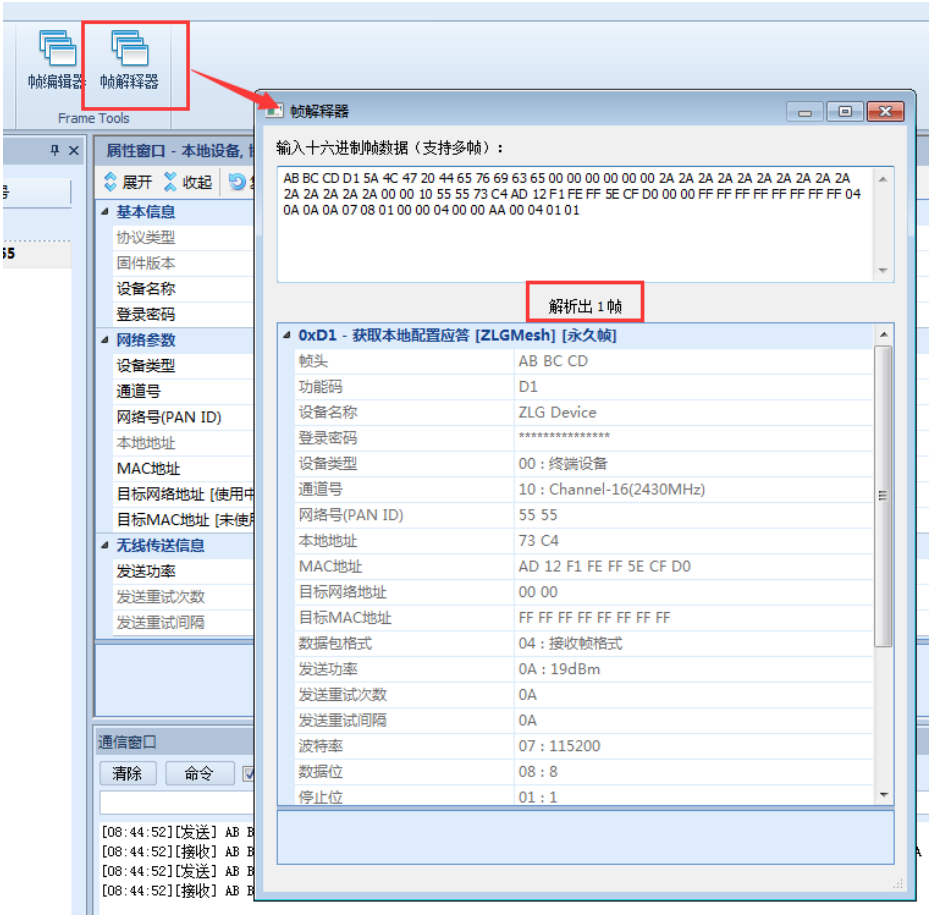

图 5.5　帧解释器功能

5.2　配置工具使用简介

将焊接有模块的 Pack 板安装在 ZM32A Demo Board 上，再安装合适的天线，如图 5.6 所示。

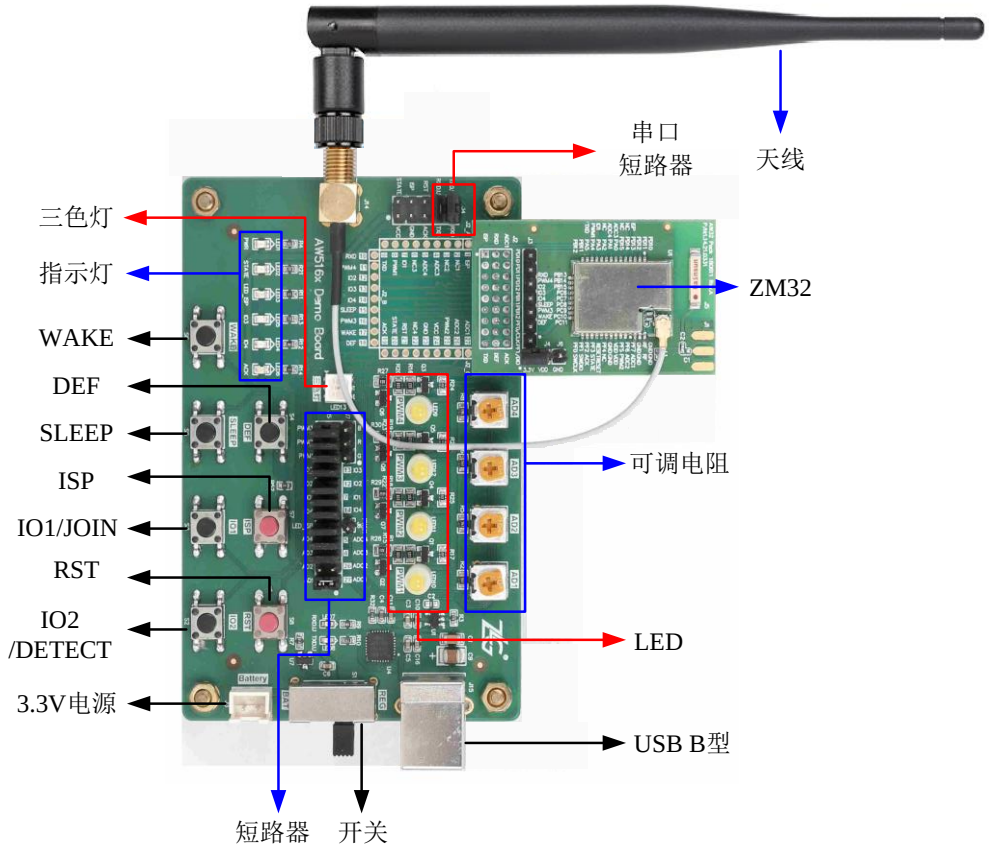

图 5.6　ZM32A Demo Board 安装图

驱动安装完成后，即可通过评估套件配套的 USB 线将评估板连接到 PC 机，ZM32 系列 ZigBee 模块提供了简易的图形配置工具 WirelessCfg，通过该配置工具可以方便地对模块的运行参数进行配置，配置工具设置参数使用永久配置协议，被配置的参数在模块掉电时不会丢失。配置步骤如下：

a)　将模块的串口通过电平转换后连接到电脑，将模块上电，打开配置软件的*连接*标签页，串口号、波特率、数据位、校验位、停止位等根据模块的串口参数进行设定，设定好串口参数后，点击*打开串口*按钮，详见图 5.7 所示。

图 5.7 串口参数配置

b) 点击*连接设备*按钮获取模块目前的固件类型，确认模块固件是否为“ZLGMesh”，如图 5.8 所示。

c) 点击*设备配置*即可进入配置。该按键共两处，分别位于界面左上角和*连接设备*的下方。如图 5.8 红色框所示。

图 5.8 获取固件类型

d) 在设备配置界面可以进行设备的“工作类型”、“通道号”、“PAN ID”、“目标网络地址”等参数的配置，修改完成后，需要点击属性窗口工具栏上的*保存配置*，才能使得参数生效，如图 5.9 所示。

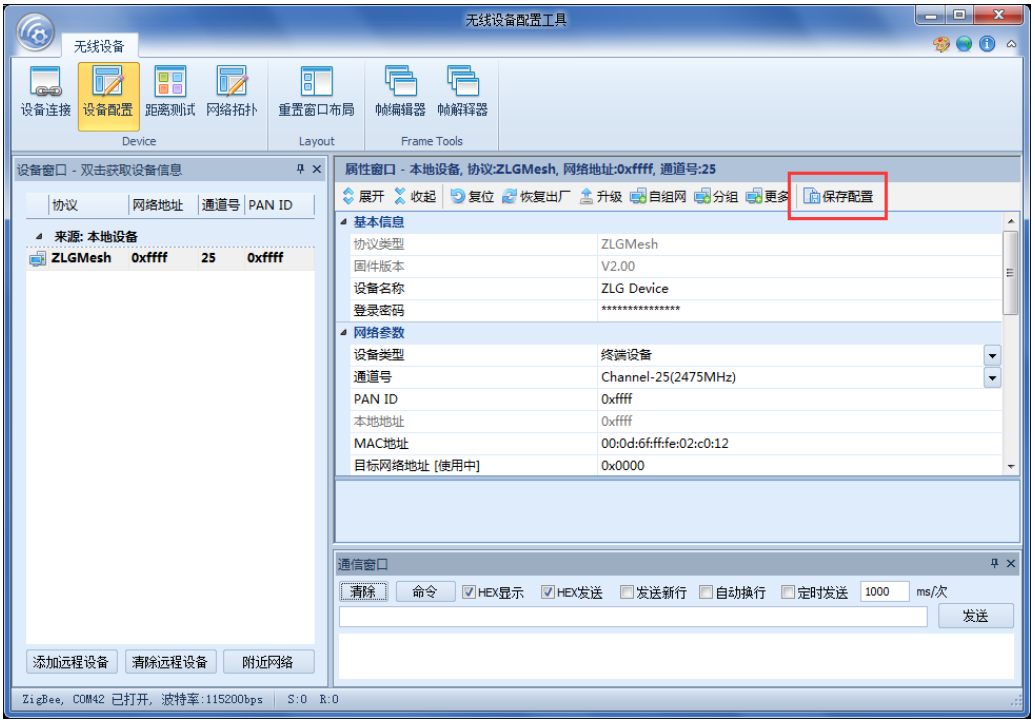

图 5.9 模块基本信息

6. 如何组网

6.1 协调器建立网络

这一节描述如何使用协调器建立起一个 ZigBee 网络，本章节的所有讲解均基于模块是恢复出厂后的状态，如需了解模块是如何恢复出厂，请参考章节 11。

6.1.1 非自组网方式

a) 配置工具属性窗口选择工作类型为协调器设备，然后点击*保存配置*，如图 6.1 所示，该过程对应的操作命令：修改配置->复位。

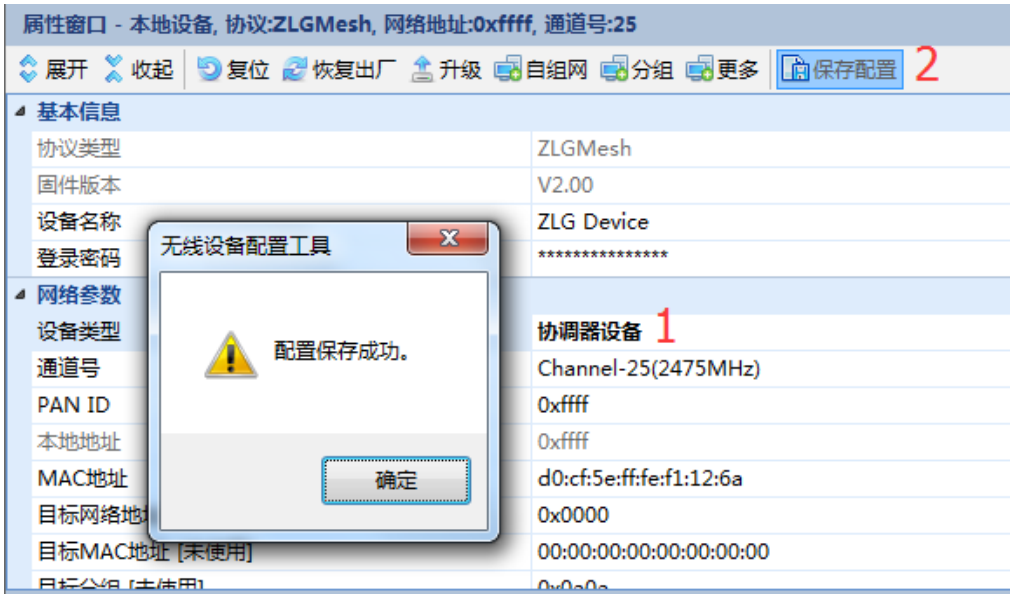

图 6.1 修改工作类型

b) 修改预配置密钥和网络密钥，建议用户不要使用出厂配置的密钥，提高安全性，该过程对应的操作命令：设置模块密钥。

(一) 预配置密钥: 设备的预配置密钥与协调器的预配置密钥相同，才可以成功加入网络，设备必须加网前配置才有效。

(二) 网络密钥: 协调器的网络密钥，会发送到成功加入网络的设备保存，用来加密通讯报文，协调器必须正式建网前配置才有效。

配置工具属性窗口点击*更多*，在更多配置里修改这两种密钥，如图 6.2 所示。

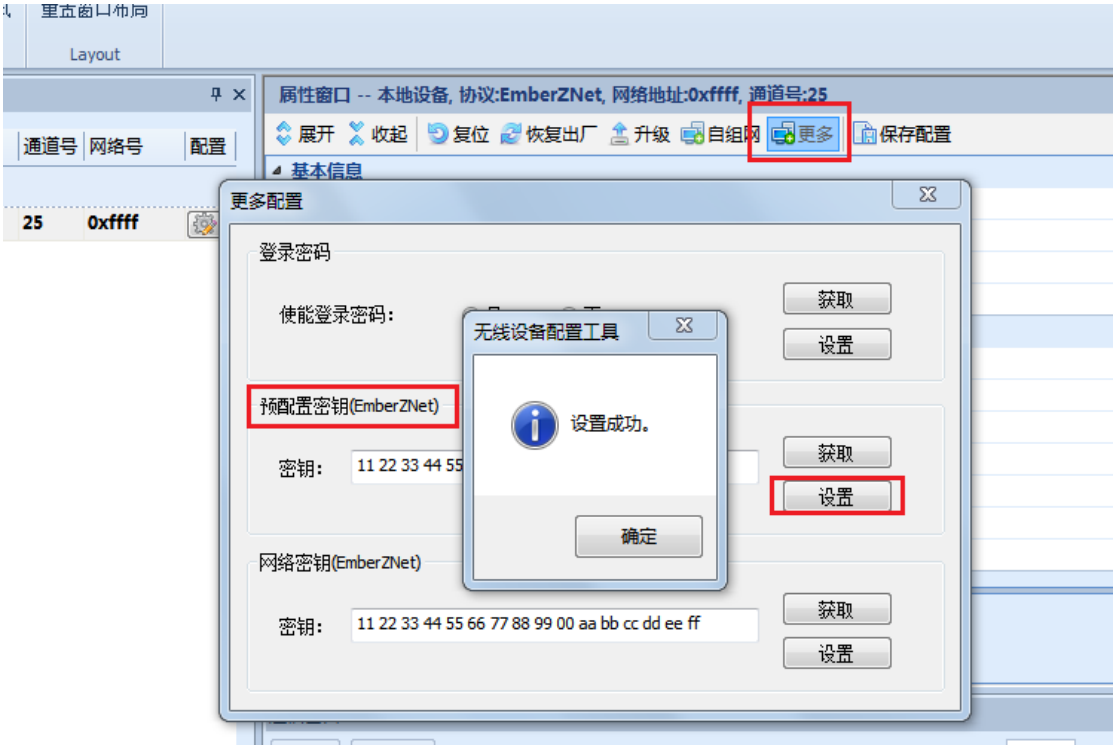

图 6.2　修改密钥

注：这两种密钥需要设备在未加入/建立网络前配置，其中网络密钥只支持协调器设备配置。

c)　配置工具属性窗口设置合适的 PAN ID 和通道号，然后点击*保存配置*如图 6.3 所示，该过程对应的操作命令：修改配置->复位。

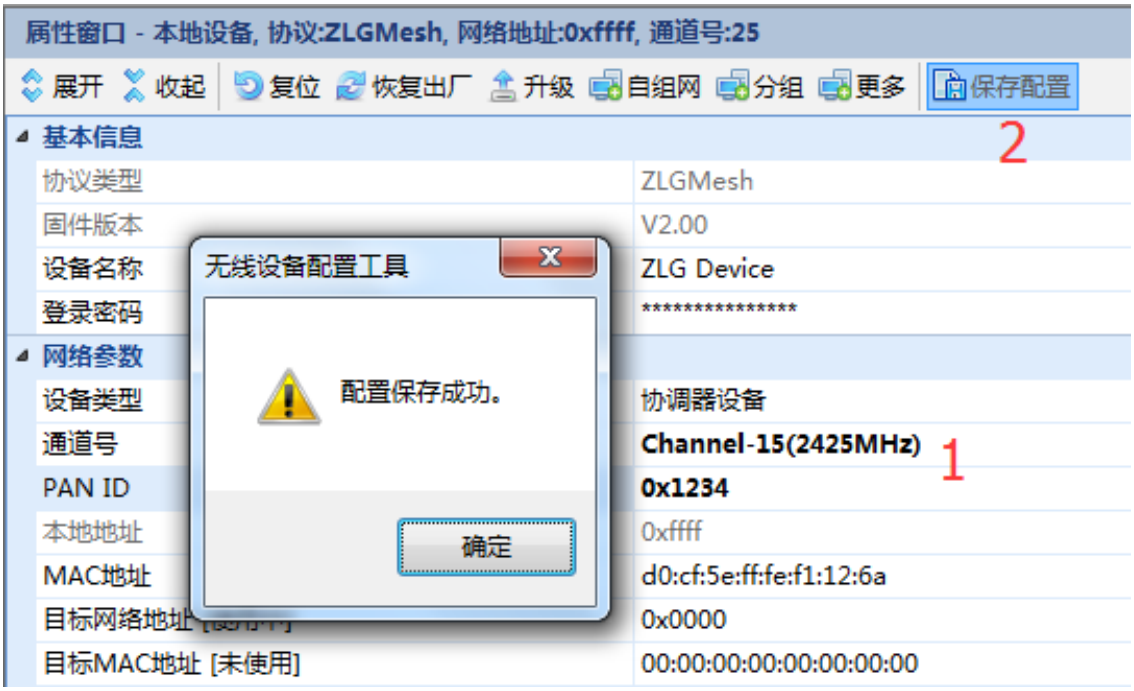

图 6.3　修改网络参数

当协调器的本地地址变成 0x0000 时，网络就建立好了，如图 6.4 所示。

网络参数	
设备类型	协调器设备
通道号	Channel-15(2425MHz)
PAN ID	0x1234
本地地址	0x0000
MAC地址	d0:cf:5e:ff:fe:f1:12:6a
目标网络地址 [使用中]	0x0000

图 6.4　协调器建立网络

6.1.2 自组网方式

这种方式建立网络，首先按照非自组网方式配置好协调器类型，以及网络密钥，然后点击自组网，在自组网配置里选择“普通自组网”，如图 6.5 所示。最后将 ZM32 的 DETECT 引脚拉低 3 秒就可以建立起一个网络了，之后允许其他设备加入，需要将 JOIN 引脚一直拉低，该过程对应的操作命令：修改配置->复位->设置模块密钥->配置自组网->复位。

图 6.5　配置自组网

6.2 路由/终端加入网络

这一节描述如何使路由设备/终端设备加入一个 ZigBee 网络，本章节的所有讲解均基于模块是恢复出厂后的状态，如需了解模块是如何恢复出厂，请参考章节 11。

6.2.1 非自组网方式

a) 在配置工具的属性窗口，将设备类型设置为路由设备或者终端设备，如图 6.6 所示，该过程对应的操作命令：修改配置->复位。

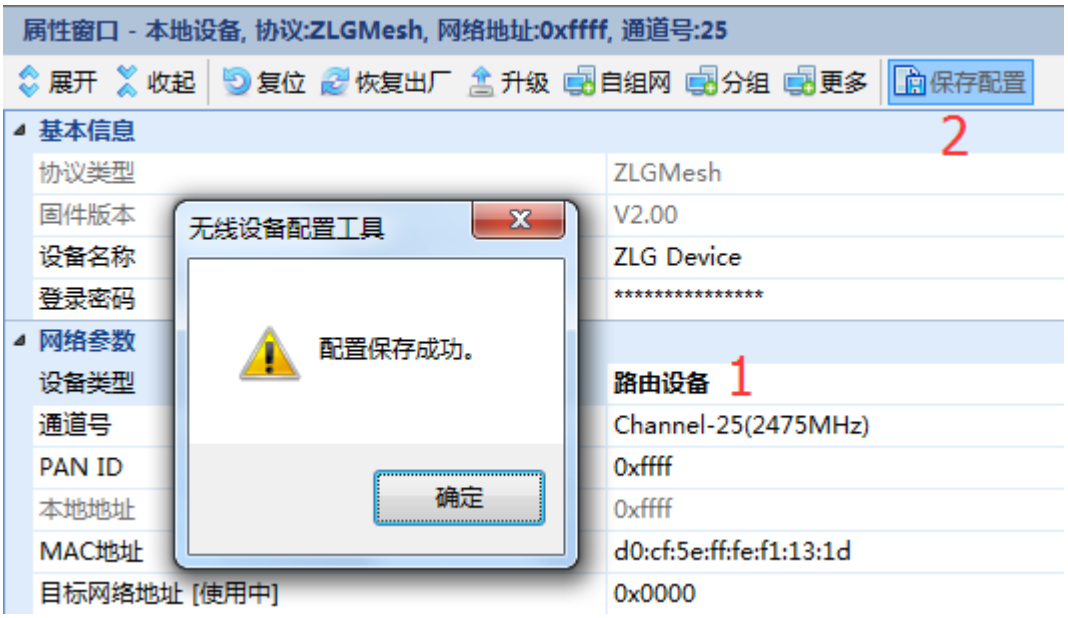

图 6.6　路由/终端设备

b)　配置工具属性窗口点击*更多*，在更多配置里修改预配置密钥，如图 6.2 所示，该过程对应的操作命令：设置模块密钥。

c)　配置工具属性窗口选择要加入网络的通道号和 PAN ID，然后点击*保存配置*，如图 6.7 所示，该过程对应的操作命令：修改配置->复位。

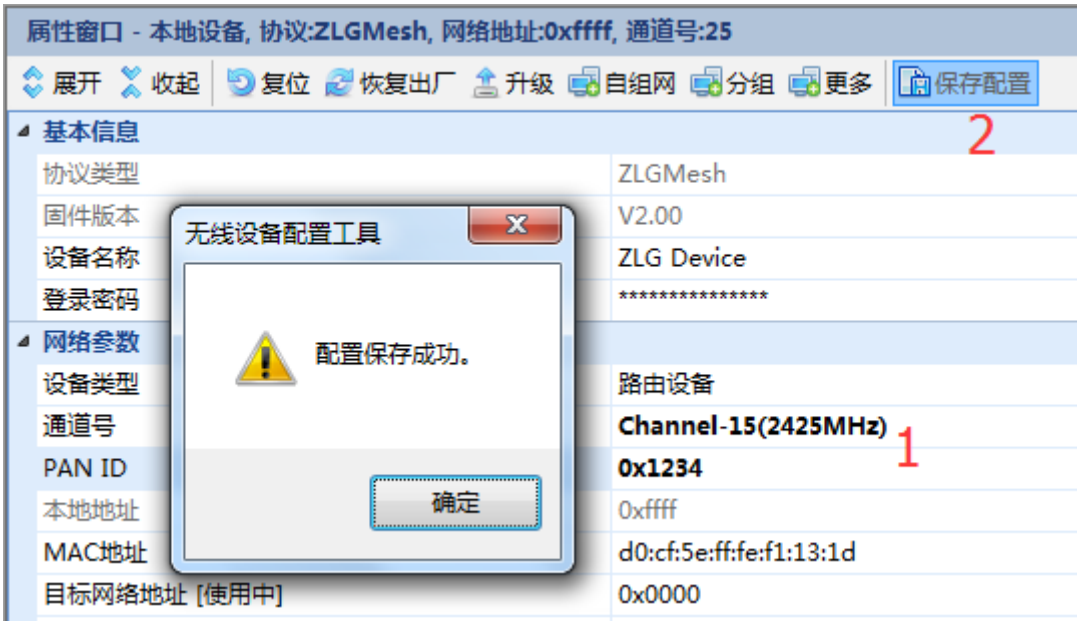

图 6.7　修改网络参数

当设备的本地地址变成 **非 0xFFFF** 时，就已经加入了网络，如图 6.8 所示。

图 6.8　加入网络

6.2.2 自组网方式

首先按照非自组网方式配置工作类型，以及网络密钥，然后仿照建立网络的协调器自组网做法，配置“普通自组网”，如图 6.5 所示，最后将 ZM32 的 JOIN 引脚拉低持续 100 ms，就会尝试加入附近允许加入的网络，该过程对应的操作命令：修改配置->复位->设置模块密钥->配置自组网->复位。

7. 发送数据

7.1 透明发送模式

7.1.1 单播给目标网络地址

可以与指定的某一网络地址设备通信，例如：协调器可以修改目标网络地址为 0x0000，然后发送数据给自己，如图 7.1 所示，该过程对应的操作命令：修改配置->复位。

图 7.1 单播给指定目标网络地址

网络参数：

目标网络地址：0x0000

发送模式：

数据传输方式：单播模式

数据目标地址选择：目标网络地址

数据包格式：数据

保存配置后，就可以在通信窗口收发。

7.1.2 单播给目标 MAC 地址

可以指定单播到某一 MAC 地址设备上，例如：可以修改目标 MAC 地址为本地设备的 MAC 地址，然后发送数据给自己，如图 7.2 所示，该过程对应的操作命令：修改配置->复位。

图 7.2　单播给指定目标 MAC 地址

网络参数：

目标 MAC 地址：指定的目标 MAC 地址

发送模式：

数据传输方式：单播模式

数据目标地址选择：目标 MAC 地址

数据包格式：数据

保存配置后，就可以在通信窗口收发。

7.1.3 广播发送

广播给所有设备。

例如：把数据广播给网络内所有设备(除了自己)，可以设置广播给所有设备，如图 7.3 所示，该过程对应的操作命令：修改配置->复位。

图 7.3　广播

发送模式：

数据传输方式：广播给所有设备

7.1.4 组播给目标分组

数据会传输给目标分组内的所有设备。

首先，需要给接收设备设置分组，例如 0x0001，详情请参考章节 9 如何分组。

接着，设置发送设备的目标组号和组播模式，如图 7.4 所示，该过程对应的操作命令：修改配置->复位。

图 7.4　组播给目标分组

网络参数：

目标组号：网络内存在的一个分组，例如 0x0001

发送模式：

数据传输方式：组播模式

7.2　数据带网络地址的发送模式

通过串口发送的数据前 2 个字节带有网络地址，如图 7.5 所示，该过程对应的操作命令：修改配置->复位。

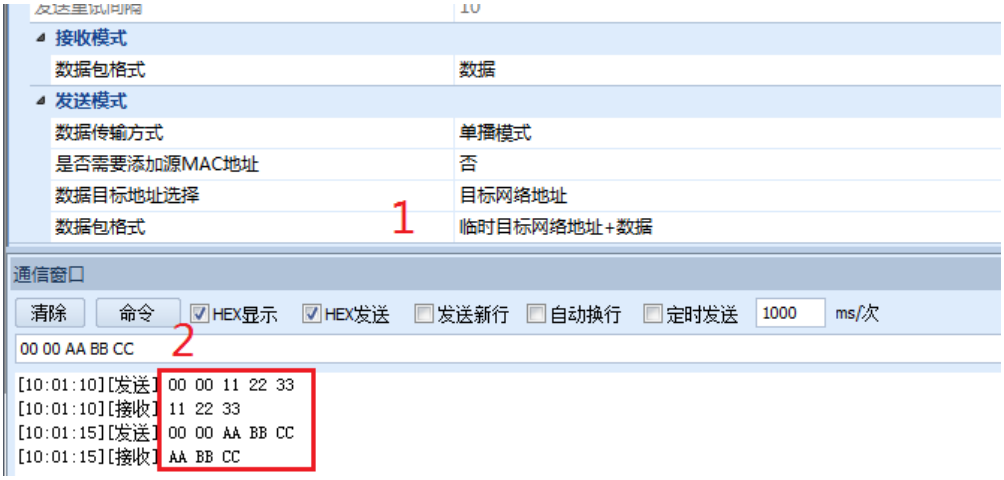

图 7.5　发送网络地址+数据

发送模式：

数据传输方式：单播模式

数据包格式：临时目标网络地址+数据

7.3　数据带 MAC 地址的发送模式

通过串口发送的数据里面带有 MAC 地址，如果希望接收方知道自己的 MAC 地址，就需要添加源 MAC 地址，如图 7.6 所示，该过程对应的操作命令：修改配置->复位。

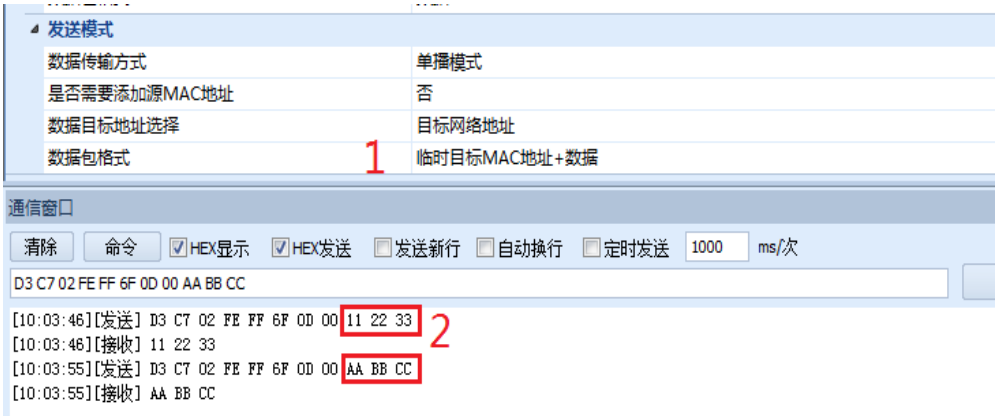

图 7.6　发送 MAC 地址+数据

发送模式：

数据传输方式：单播模式

是否需要添加源 MAC 地址：是

数据包格式：临时目标 MAC 地址+数据

7.4　数据带帧格式的发送模式

7.4.1 单播/广播发送帧

数据要按照帧格式发送到串口，可以指定目标网络地址、目标 MAC 地址来进行单播或者广播，帧格式请参考章节 14.3.1。数据发送如图 7.7 所示，该过程对应的操作命令：修改配置->复位。

图 7.7　发送帧

发送模式：

数据传输方式：单播模式

数据包格式：发送帧格式

7.4.2 组播发送帧

数据要依照按照帧格式发送到串口，可以指定目标分组，帧格式请参考章节 14.3.2。需要先给接收设备设置分组，例如 0x0001，详情请参考章节 9 如何分组。

数据发送如图 7.8 所示，该过程对应的操作命令：修改配置->复位。

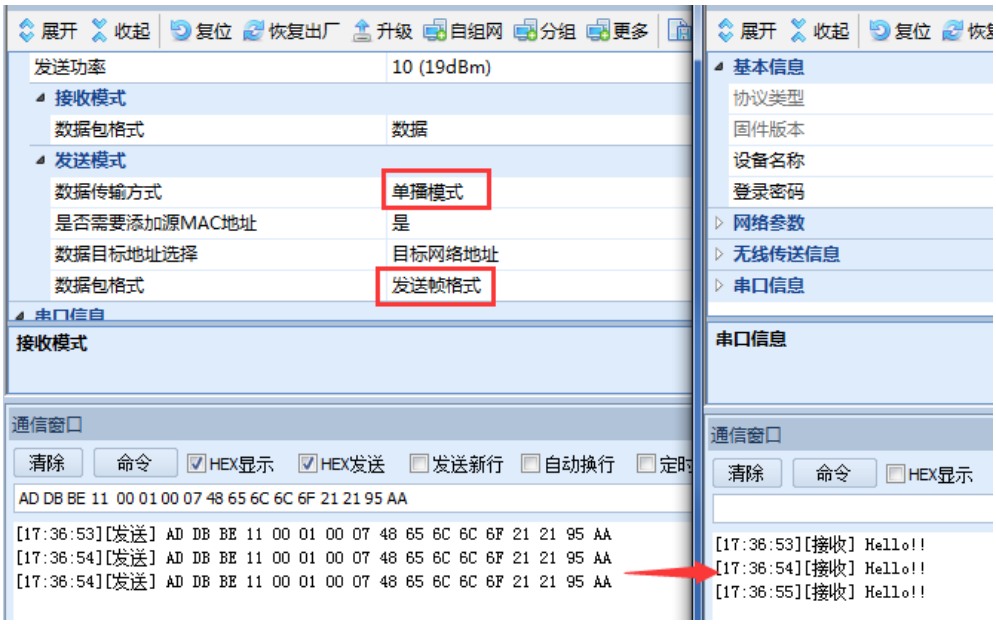

图 7.8　组播发送帧

发送模式：

数据传输方式：单播模式

数据包格式：发送帧格式

8. 接收数据

8.1 透明接收

无线接收到数据后，会发到串口，如图 8.1 所示，该过程对应的操作命令：修改配置->复位。

图 8.1 透明接收

接收模式：

数据包格式：数据

8.2 接收源网络地址+数据

无线接收到数据后，会在数据前面加入发送方的网络地址，然后从串口输出，如图 8.2 所示，该过程对应的操作命令：修改配置->复位。

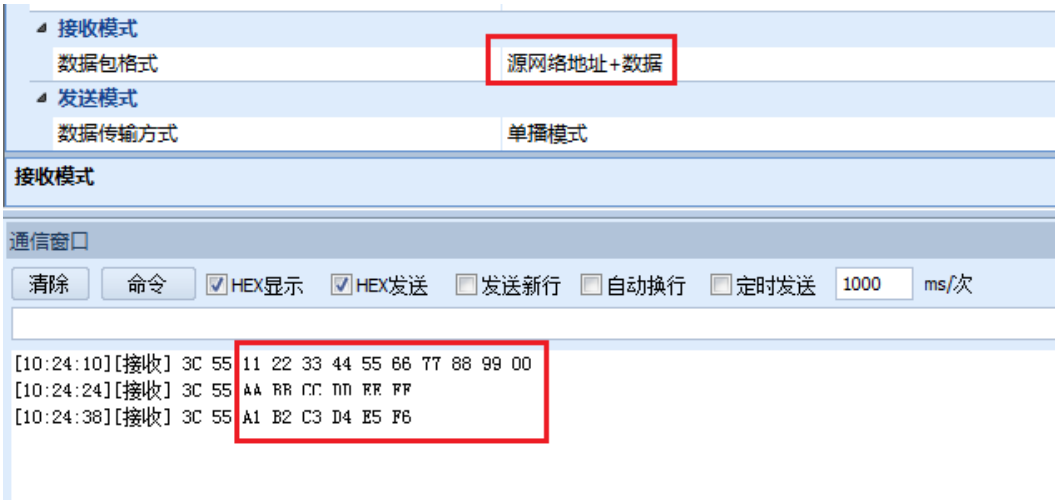

图 8.2 接收源网络地址+数据

接收模式：

数据包格式：源网络地址+数据

8.3 接收源 MAC 地址+数据

无线接收到数据后，会在数据前面加入发送方的 MAC 地址，然后从串口输出，如图 8.3 所示，该过程对应的操作命令：修改配置->复位。

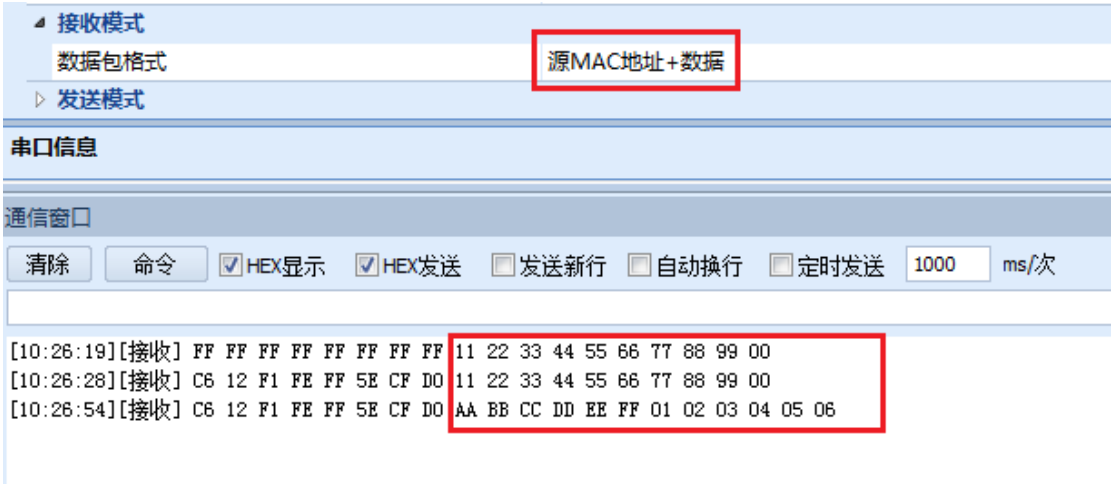

图 8.3 接收源 MAC 地址通讯

接收模式：

数据包格式：源 MAC 地址+数据

8.4 接收源网络地址+源 MAC 地址+数据

无线接收到数据后，会在数据前面加入发送方的网络地址和 MAC 地址，然后从串口输出，如图 8.4 所示，该过程对应的操作命令：修改配置->复位。

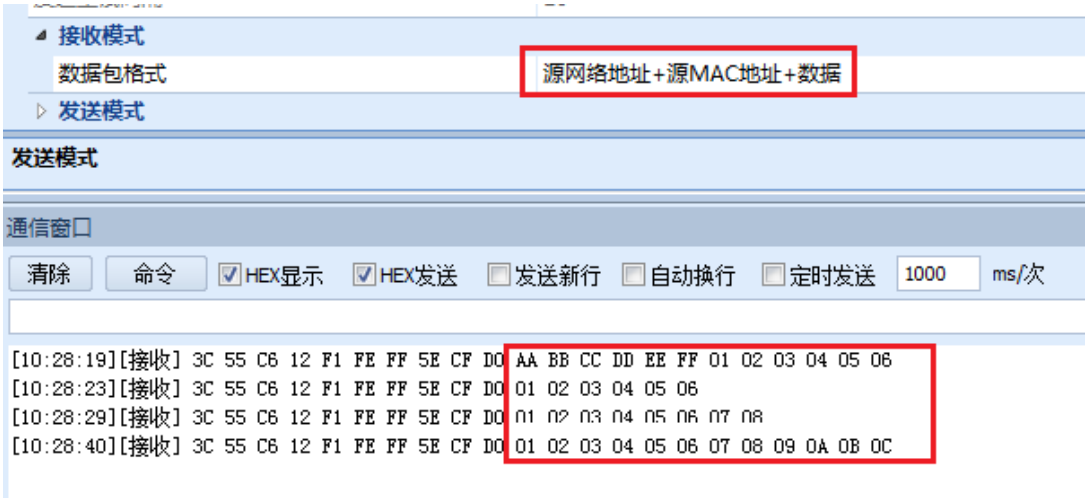

图 8.4 接收源网络地址+源 MAC 地址+数据

接收模式：

数据包格式：源网络地址+源 MAC 地址+数据

8.5 接收帧

透传数据的接收支持以帧格式接收。设备会将接收到的数据按照接收帧的格式打包起来，然后从串口输出。

8.5.1 接收单播/广播数据

如果接收数据是通过单播，或者广播发送的，就会接收到如下数据帧，帧格式请参考章节 14.3.2，如图 8.5 所示，该过程对应的操作命令：修改配置->复位。

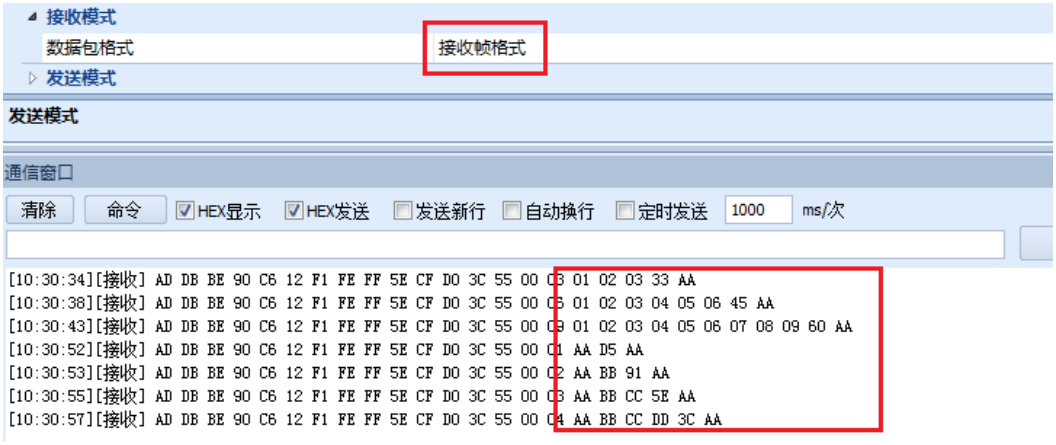

图 8.5 接收帧

接收模式：

数据包格式：接收帧格式

8.5.2 接收组播数据

如果接收数据是通过组播发送的，就会接收到如下数据帧，帧格式请参考章节 14.3.4，

注意需要先给设备设置分组 0x0001，详情请参考章节 9 如何分组。如图 8.6 所示，该过程对应的操作命令：修改配置->复位。

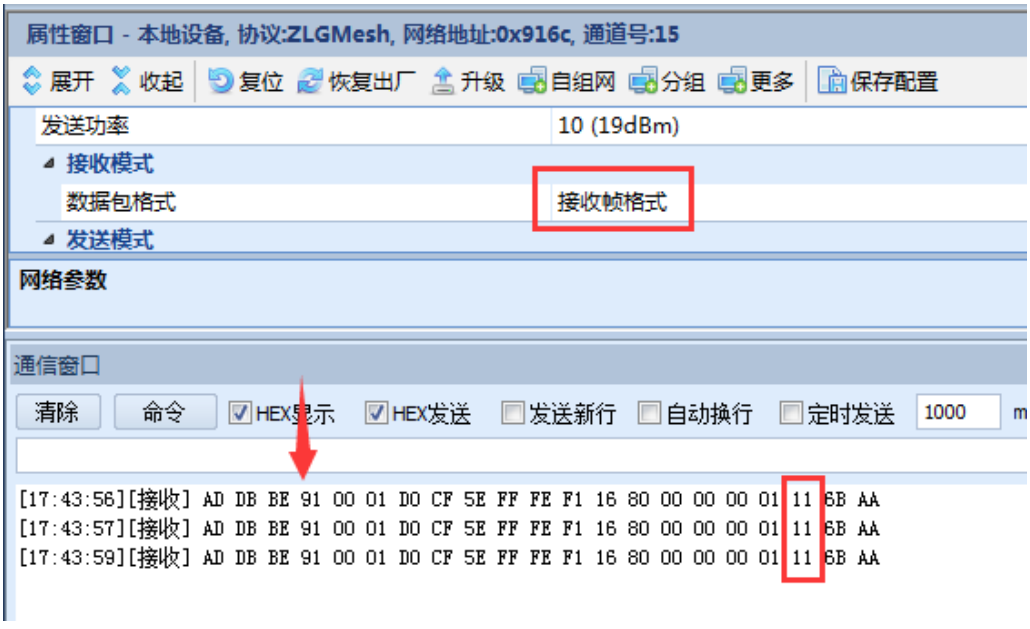

图 8.6 组播接收帧

接收模式：

数据包格式：接收帧格式

9. 如何分组

分组是网络内所有设备集合的一个子集。比如：网络内总共有 3 台设备 D1，D2，D3，那么可以建立分组 G1，加入设备 D1，D2；建立分组 G2，加入设备 D3；建立分组 G3，加入设备 D1，D2，D3。每台设备可以加入不同分组，目前最多只能加入 5 个分组，详情请查阅配置分组命令。

那么如何给设备分组呢？可以参考以下内容。

9.1 本地分组

对本地设备进行分组，先选中本地设备，然后点击*分组*，接着点击*添加*，如图 9.1 所示，该过程对应的操作命令：配置分组。

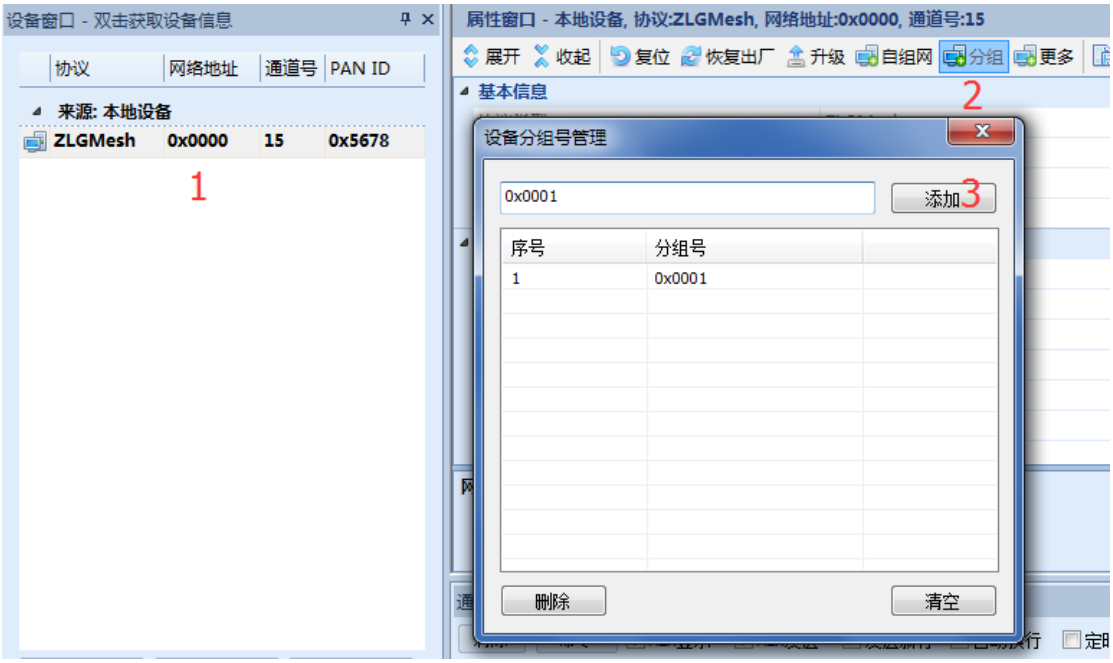

图 9.1 本地分组

9.2 远程分组

对远程设备进行分组，先搜索出远程设备，选中要分组的远程设备，然后点击*分组*，如图 9.2 所示，该过程对应的操作命令：配置分组。

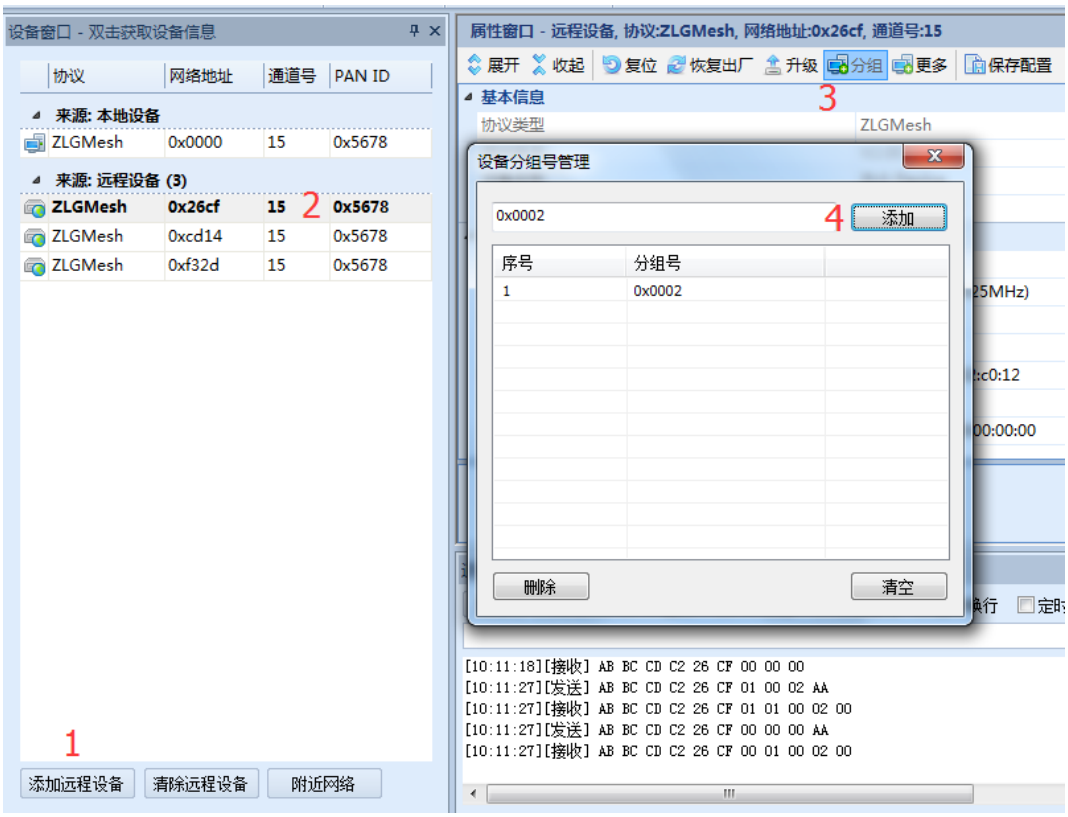
设备窗口 - 双击获取设备信息
协议
网络地址
通道号
PAN ID
来源: 本地设备
ZLGMesh
0x0000
15
0x5678
来源: 远程设备 (3)
ZLGMesh
0x26cf
15
0x5678
ZLGMesh
0xcd14
15
0x5678
ZLGMesh
0xf32d
15
0x5678
1
2
添加远程设备
清除远程设备
附近网络
属性窗口 - 远程设备, 协议:ZLGMesh, 网络地址:0x26cf, 通道号:15
展开
收起
复位
恢复出厂
升级
分组
更多
保存配置
3
基本信息
协议类型
ZLGMesh
设备分组号管理
0x0002
4
添加
序号
分组号
1
0x0002
删除
清空
[10:11:18][接收] AB BC CD C2 26 CF 00 00 00
[10:11:27][发送] AB BC CD C2 26 CF 01 00 02 AA
[10:11:27][接收] AB BC CD C2 26 CF 01 01 00 02 00
[10:11:27][发送] AB BC CD C2 26 CF 00 00 00 AA
[10:11:27][接收] AB BC CD C2 26 CF 00 01 00 02 00

图 9.2　远程分组

10. 如何升级

升级功能，需要准备好正确的升级文件。

10.1 本地升级

对本地设备进行升级，先选中本地设备，然后点击*升级*，如图 10.1 所示，该过程对应的操作命令：进入升级模式->固件升级->根据 XModem 发送固件。

图 10.1　本地升级

10.2 远程升级

对远程设备进行单独升级，先搜索出远程设备，选中要升级的远程设备，然后点击*升级*，如图 10.2 所示，该过程对应的操作命令：进入升级模式->固件升级->根据 XModem 发送固件。

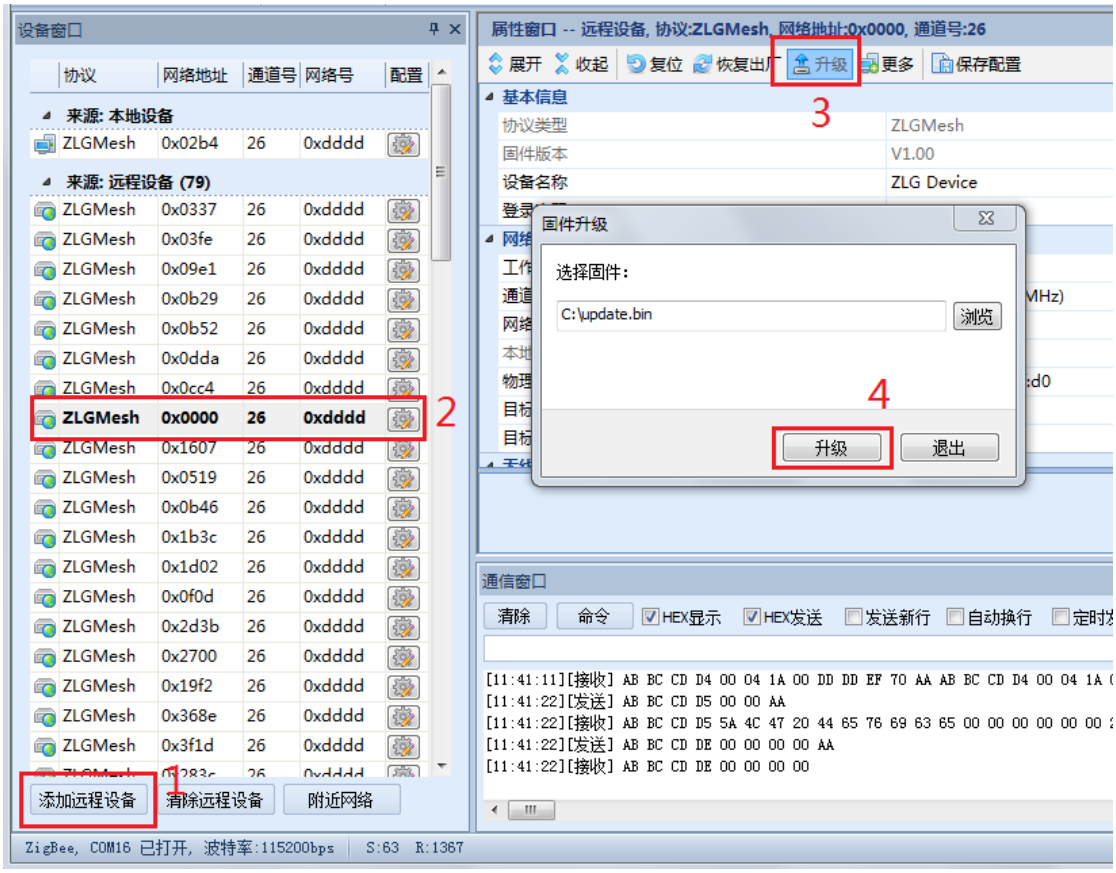
设备窗口
协议
网络地址
通道号
网络号
配置
来源: 本地设备
ZLGMesh 0x02b4 26 0xdddd
来源: 远程设备 (79)
ZLGMesh 0x0337 26 0xdddd
ZLGMesh 0x03fe 26 0xdddd
ZLGMesh 0x09e1 26 0xdddd
ZLGMesh 0x0b29 26 0xdddd
ZLGMesh 0x0b52 26 0xdddd
ZLGMesh 0x0dda 26 0xdddd
ZLGMesh 0x0cc4 26 0xdddd
ZLGMesh 0x0000 26 0xdddd
ZLGMesh 0x1607 26 0xdddd
ZLGMesh 0x0519 26 0xdddd
ZLGMesh 0x0b46 26 0xdddd
ZLGMesh 0x1b3c 26 0xdddd
ZLGMesh 0x1d02 26 0xdddd
ZLGMesh 0x0f0d 26 0xdddd
ZLGMesh 0x2d3b 26 0xdddd
ZLGMesh 0x2700 26 0xdddd
ZLGMesh 0x19f2 26 0xdddd
ZLGMesh 0x368e 26 0xdddd
ZLGMesh 0x3f1d 26 0xdddd
2
1
添加远程设备
清除远程设备
附近网络
属性窗口 -- 远程设备, 协议:ZLGMesh, 网络地址:0x0000, 通道号:26
展开
收起
复位
恢复出厂
升级
更多
保存配置
3
基本信息
协议类型
ZLGMesh
固件版本
V1.00
设备名称
ZLG Device
固件升级
选择固件:
C:\update.bin
浏览
4
升级
退出
通信窗口
清除
命令
HEX显示
HEX发送
发送新行
自动换行
[11:41:11][接收] AB BC CD D4 00 04 1A 00 DD DD EF 70 AA AB BC CD D4 00 04 1A
[11:41:22][发送] AB BC CD D5 00 00 AA
[11:41:22][接收] AB BC CD D5 5A 4C 47 20 44 65 76 69 63 65 00 00 00 00 00 00
[11:41:22][发送] AB BC CD DE 00 00 00 00 AA
[11:41:22][接收] AB BC CD DE 00 00 00 00
ZigBee, COM16 已打开, 波特率:115200bps
S:63 R:1367

图 10.2　远程升级

11. 恢复出厂

11.1 本地设备恢复出厂

对本地设备进行升级，先选中本地设备，然后点击*恢复出厂*，如图 11.1 所示，该过程对应的操作命令：恢复出厂设置->复位。

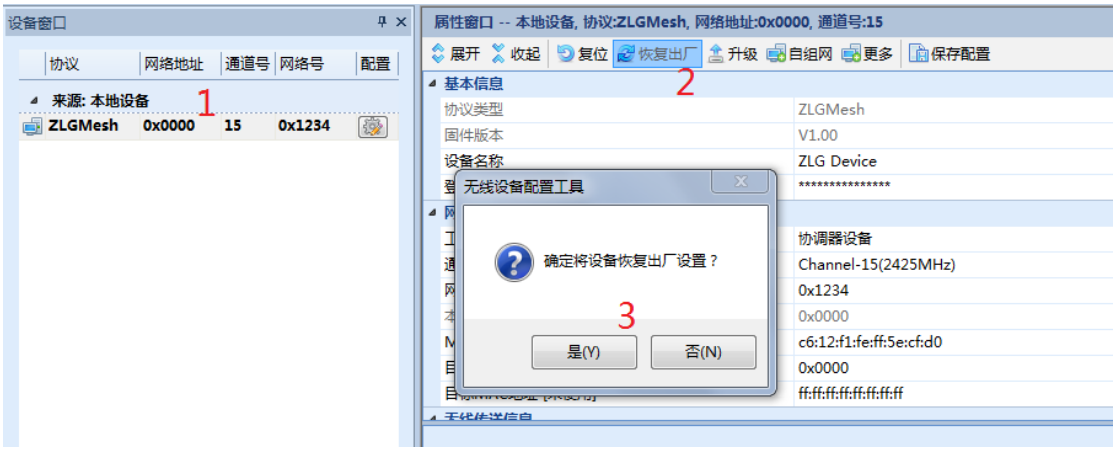

图 11.1　本地设备恢复出厂

11.2 远程设备恢复出厂

对远程设备恢复出厂，先搜索出远程设备，选中要恢复出厂的远程设备，然后点击*恢复出厂*，如图 11.2 所示，该过程对应的操作命令：恢复出厂设置->复位。

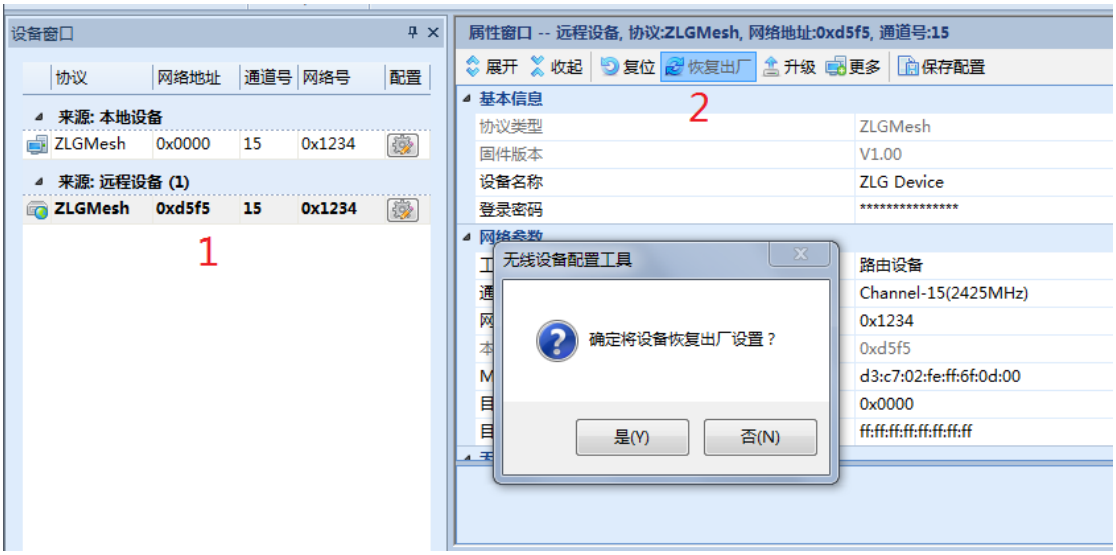

图 11.2　远程设备恢复出厂

12. 备份/还原数据

12.1 备份数据

准备一台协调器，点击*更多*，然后*备份*，保存到文件，如图 12.1 所示，该过程对应的操作命令：备份数据。

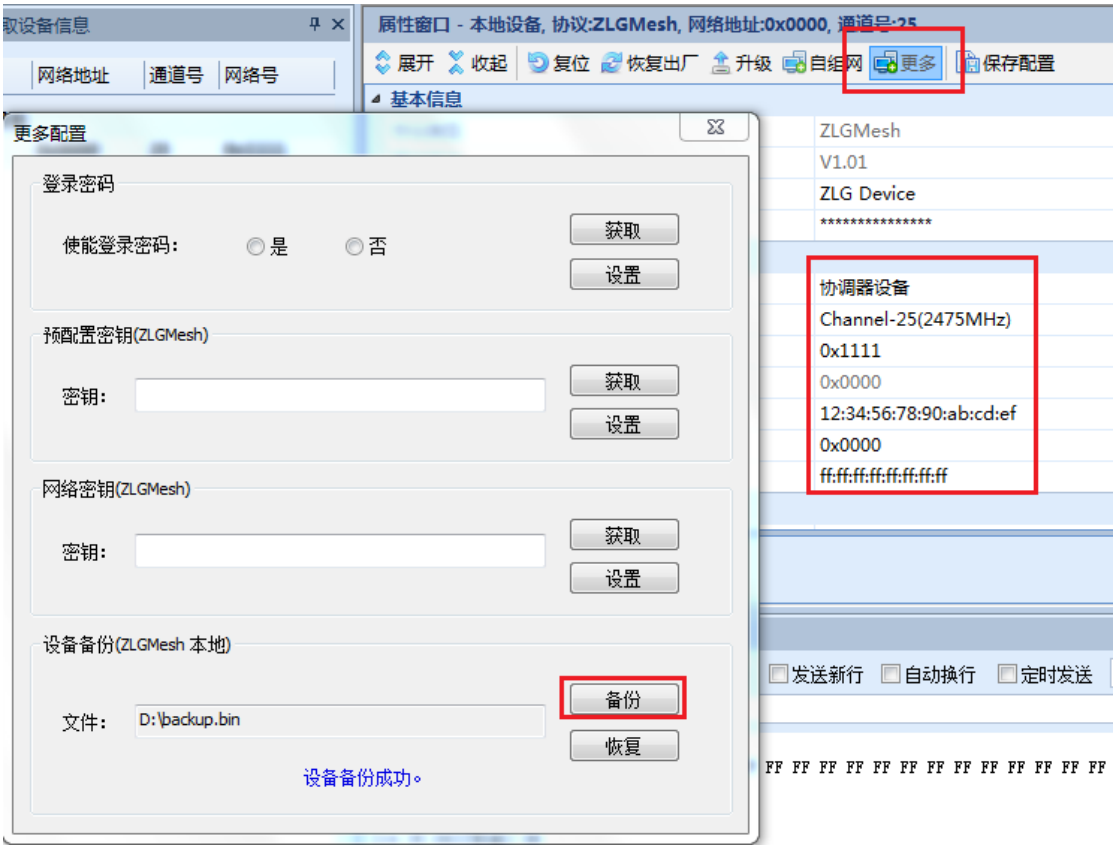

图 12.1　备份协调器

12.2 恢复数据

找一台新设备，点击*更多*，然后*恢复*，选择前面保存的文件，如图 12.2 所示，该过程对应的操作命令：恢复数据->复位。

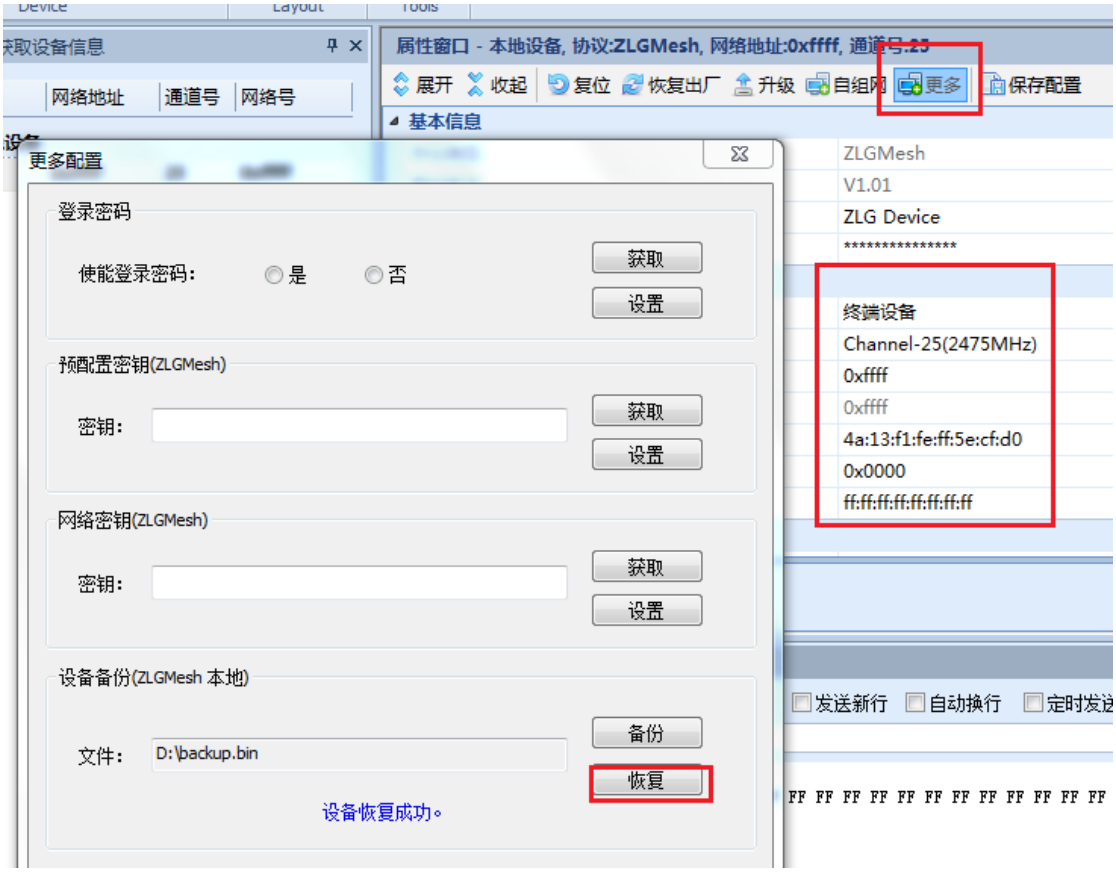

图 12.2　恢复协调器

当恢复成功后，重新获取设备信息，可以看到新设备变成了原来的协调器，如图 12.3 所示，该过程对应的操作命令：读取本地配置。

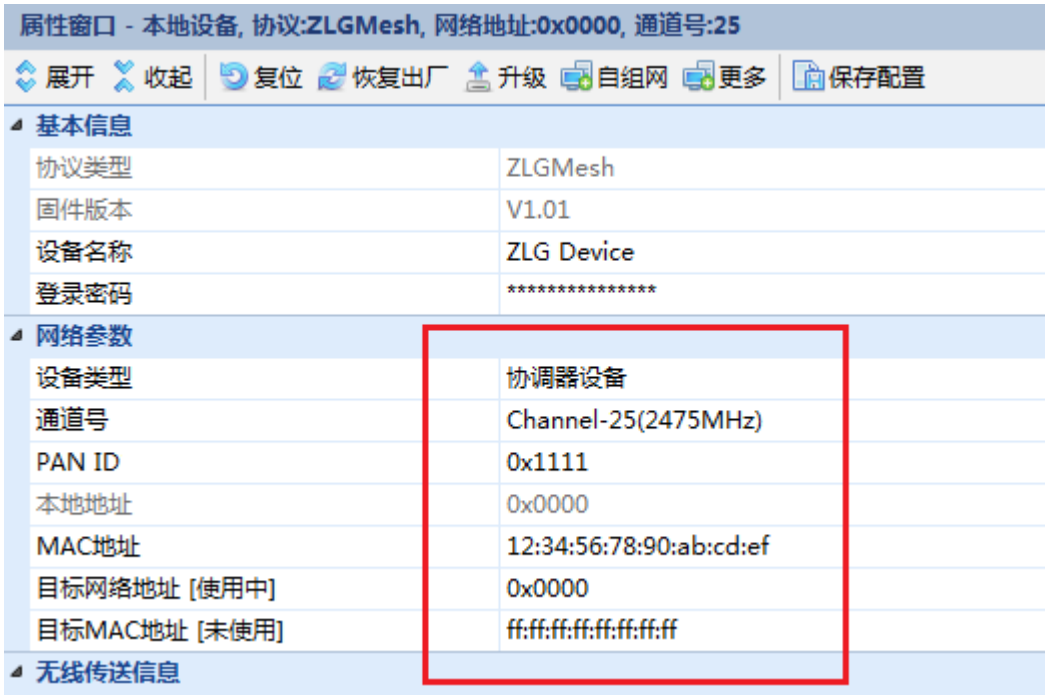

图 12.3　恢复成功

13. ADC/IO 数据上报

模块提供了采集 IO/AD 数据的命令，参考命令“IO/AD 采集设置”，采集到的数据会按照配置的方式上传。

13.1 上报给指定网络地址

配置定时上报或触发上报数据，然后发送给指定的网络地址，如图 13.1 所示，该过程对应的操作命令：修改配置->IO/AD 采集设置->复位。

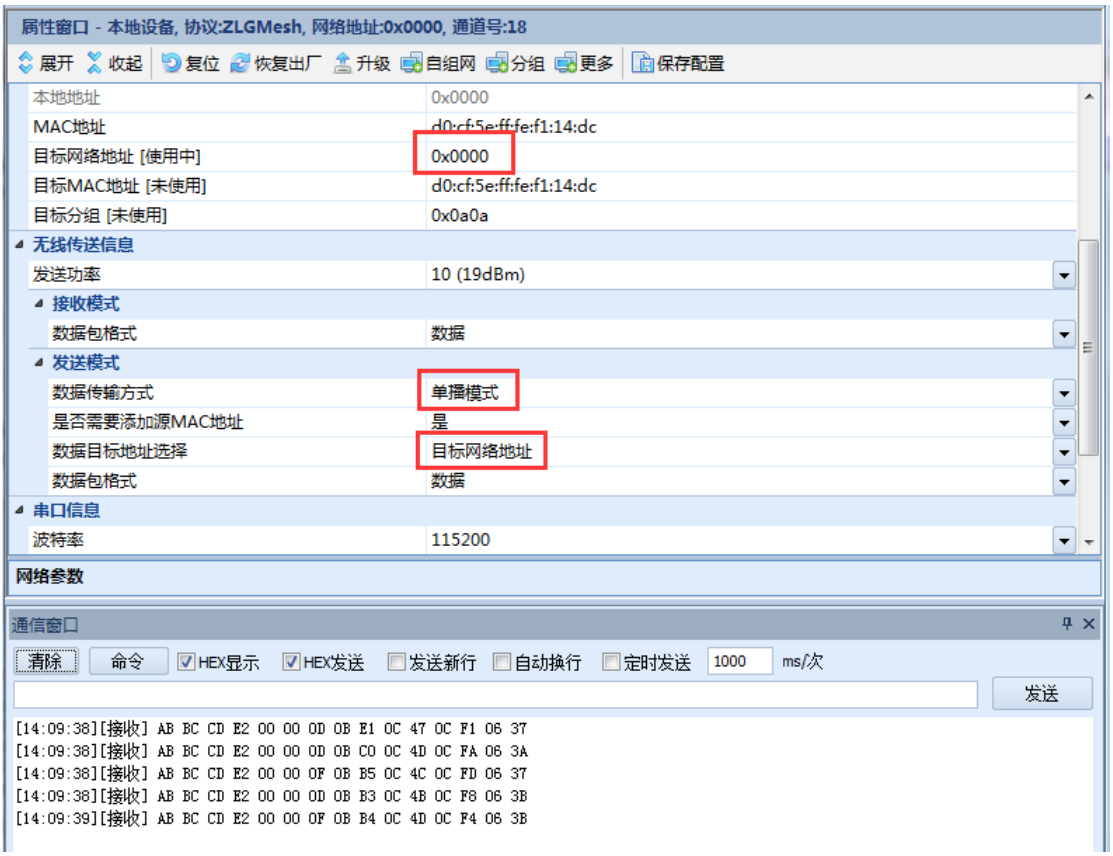

图 13.1 指定网络地址上报

网络参数：

目标网络地址：目标设备的网络地址(本例是本地设备的网络地址)

发送模式：

数据传输方式：单播模式

数据目标地址选择：目标网络地址

13.2 上报给指定 MAC 地址

配置定时上报或触发上报数据，然后发送给指定的 MAC 地址，如图 13.2 所示，该过程对应的操作命令：修改配置->IO/AD 采集设置->复位。

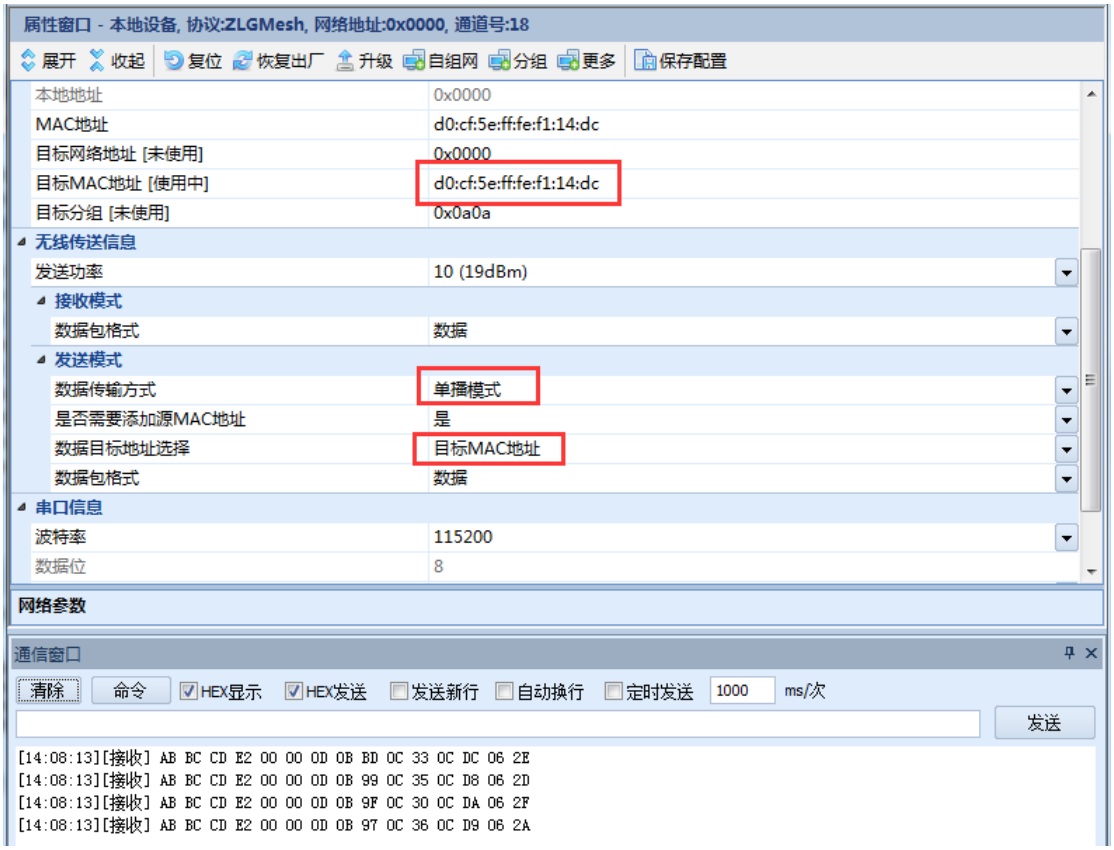

图 13.2　指定 MAC 地址上报

网络参数：

目标网络地址：目标设备的 MAC 地址(本例是本地设备的 MAC 地址)

发送模式：

数据传输方式：单播模式

数据目标地址选择：目标 MAC 地址

13.3 广播上报

配置定时上报或触发上报数据，然后广播发送数据如图 13.3 所示，该过程对应的操作命令：修改配置->IO/AD 采集设置->复位。

图 13.3　广播上报

发送模式：

数据传输方式：广播给所有设备

13.4 组播上报

配置定时上报或触发上报数据，然后组播发送数据，如图 13.4 所示，该过程对应的操作命令：修改配置->IO/AD 采集设置->复位。

图 13.4　组播上报

网络参数：

目标分组：网络内存在的一个分组，这里是 0x0001

发送模式：

数据传输方式：组播模式

14. 命令集

14.1 临时参数配置协议与命令

ZM32 系列 ZigBee 模块临时参数配置协议命令帧格式详见表 14.1，协议标志占用 3 个字节，即：DE DF EF，命令标识符占用 1 个字节，其相应的参数占用 N 个字节。

表 14.1 临时参数配置命令格式（CMD）

3 字节（协议标志）	1 字节	N 字节
DE DF EF	命令标识符	参数

ZM32 模块支持两种参数配置协议；永久参数配置协议和临时参数配置协议。

永久参数配置协议配置的参数是保存在模块的非易失性存储区，配置参数可掉电保存，模块上电后使用永久参数运行。由于非易失性存储介质的特点，频繁擦除，写入会影响存储介质的寿命，最后失效，所以建议不要频繁使用永久参数配置命令。

如果需要频繁修改运行时的工作参数，可以使用临时参数配置协议。

临时参数配置协议配置的参数是保存在模块的RAM里，掉电不能保存；用户在使用了临时参数配置命令后，工作参数会马上更新，但当发生复位、重启等操作后，临时配置失效，工作参数恢复成原有配置，通常临时参数是用户需要经常改变的参数。

临时参数配置协议与命令，分为基于 MAC 地址通讯命令集、基于网络地址通讯命令集，和本地命令集。

当使用基于 MAC 地址通讯的命令时，00:00:00:00:00:00:00:00 代表协调器，FF:FF:FF:FF:FF:FF:FF:FE 代表本地设备执行。

当使用基于网络地址通讯的命令时，0xFFFE 代表本地设备执行。

注意，使用广播/组播方式发送数据时，10 秒内最多发送 9 次。

各命令类型的命令标识符详见表 14.2。

表 14.2 临时参数配置协议与命令标识

命令类型	命令标识符	备注
配置发送选项	0x22	
配置目标组号	0x23	
进入测试模式（致远内部使用）	0xD0	致远内部使用命令，用户不要使用
修改目标网络地址	0xD2	
进入休眠	0xD8	无应答
设置发送模式	0xD9	
设置广播命令应答延时	0xF7	
基于 MAC 地址通讯命令集		
设置 I/O 输入输出	0x54	
读取 I/O 状态	0x55	

设置 I/O 状态	0x56	

续上表

读取 AD	0x57	
查询路由表(只有路由及协调器有效)	0x5C	
搜索存在的网络	0x5D	
查询节点的接收信号强度	0x5E	
设置接收模式	0x73	
设置目标 MAC 地址	0x74	
命令的应答时间	0x76	
获取网络地址	0xFE	
基于网络地址通讯命令集		
设置 I/O 输入输出	0xD4	
读取 I/O 状态	0xD5	
设置 I/O 状态	0xD6	
读取 AD	0xD7	
查询路由表(只有路由及协调器有效)	0xDC	
搜索存在的网络	0xDD	
查询节点的接收信号强度	0xDE	
设置接收模式	0xF3	
设置目标 MAC 地址	0xF4	
获取网络拓扑	0xF5	
命令的应答时间	0xF6	

临时参数配置帧应答返回详见表 14.3，协议标志占用 3 个字节，即：DE DF EF，命令标识符占用 1 个字节，其返回值占用 1 个字节。

表 14.3 临时配置命令应答格式（RSP）

3 字节（协议标志）	1 字节	N 字节
DE DF EF	命令标识符	返回值

14.1.1 配置发送选项

Profile ID 默认值为 0xC105，Cluster ID 默认值为 0x0011，源端点默认值为 0xE8，目标端点默认值为 0xE8，配置发送选项的命令如表 14.4 所示。

表 14.4 配置发送选项

3 字节（协议标志）	1 字节	1 字节	2 字节
DE DF EF	22	RW	Profile ID
2 字节	1 字节	1 字节	6 字节
Cluster ID	源端点	目标端点	保留

R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令其他字段忽略。

配置发送选项的应答报文如表 14.5 所示。

表 14.5 配置发送选项的应答报文

3 字节（协议标志）	1 字节	2 字节	2 字节
DE DF EF	22	Profile ID	Cluster ID
1 字节	1 字节	6 字节	
源端点	目标端点	保留	

命令示例：读取发送选项

CMD： DE DF EF 22 00 00 00 00 00 00 00 00 00 00 00 00

RSP： DE DF EF 22 C1 05 00 11 01 01 00 00 00 00 00 00

14.1.2 配置目标组号

当模块使用组播模式发送数据时，会使用到已配置的目标组号，数据将会组播给符合目标组号的设备，即分组号匹配目标组号的设备均会接收该数据。

例如：设备 A 使用组播模式发送数据 0xAA，目标组号为 0x0001；那么，分组 0x0001 的设备，将会接收数据 0xAA。

修改目标组号的命令如表 14.6 所示。

表 14.6 配置目标组号

3 字节（协议标志）	1 字节	2 字节
DE DF EF	23	目标组号 0x0000~0xFFFF

配置目标组号的应答报文如表 14.7 所示。

表 14.7 配置目标组号的应答报文

3 字节（协议标志）	1 字节	2 字节
DE DF EF	23	状态 0x00：设置成功 其它：设置失败

命令示例：配置目标组号

CMD： DE DF EF 23 00 01

RSP： DE DF EF 23 00

14.1.3 修改目标网络地址

修改目标网络地址的命令如表 14.8 所示。

表 14.8 修改目标网络地址

3 字节（协议标志）	1 字节	2 字节
DE DF EF	D2	网络地址 0x0000~0xFFFF

目标网络地址：

0xFFFF 代表广播给所有设备；

0xFFFD 代表广播给所有非睡眠设备；

0xFFFC 代表广播给协调器和路由设备；

0xFFFB 代表组播，使用目标组号。

修改目标网络地址的应答报文如表 14.9 所示。

表 14.9 修改目标网络地址的应答报文

3 字节（协议标志）	1 字节	1 字节
DE DF EF	D2	状态 0x00：设置成功 其它：设置失败

命令示例：设置目标网络地址为 0x2001。

```
CMD： DE DF EF D2 20 01
RSP： DE DF EF D2 00
```

14.1.4 进入休眠

设置进入休眠的命令如表 14.10 所示。

表 14.10 进入休眠

3 字节（协议标志）	1 字节	1 字节
DE DF EF	D8	状态 0x01：进入休眠 其他：无效

休眠命令无返回，进入休眠后保存临时参数配置，可通过拉低唤醒管脚（WAKE）进行唤醒，也可通过设置定时唤醒或者 IO 唤醒。

命令示例：设置进入休眠

```
CMD： DE DF EF D8 01
```

14.1.5 设置发送模式

当希望通过串口转发数据到其他远程设备时，或者本地设备产生的数据需要分发时，可以设置发送模式的相关功能，满足用户不同的通讯需求。设置发送模式的命令如表 14.11 所示。

表 14.11 设置发送模式

3 字节（协议标志）	1 字节	1 字节
DE DF EF	D9	发送模式

发送模式的位域如表 14.12 所示，保留位填 0。

表 14.12 发送模式的位域

Bit 7	Bit 5~6 数据包格式	Bit 4 数据的目标地址选择	Bit 3 是否需要添加源 MAC 地址	Bit 0~2 数据传输方式
保留	0：数据（根据数据的目标地址进行发送） 1：指定网络地址+数据 2：指定 MAC 地址+数据 3：发送帧格式	0：目标网络地址(DEV_INFO.DstAddr) 1：目标 MAC 地址(DEV_INFO.DstIEEE)	0：不添加源 MAC 地址 1：添加源 MAC 地址	0：单播模式 1：广播给所有设备 2：广播给所有非睡眠设备 3：广播给协调器和所有路由器 4：组播模式

数据传输方式：用户需要串口转发的数据，或者 IO/ADC 采集数据，将会传输到指定的一台设备或者一组设备。

1. 单播模式：数据只会传输给网络地址或者 MAC 地址匹配的设备。
2. 广播给所有设备：数据会传输给网络内所有设备。
3. 广播给非睡眠设备：数据会传输给网络内所有非睡眠设备。
4. 广播给协调器和路由器：数据会传输给网络的协调器和所有路由器。
5. 组播模式：数据会传输给目标分组内的所有设备。

是否需要添加源 MAC 地址：当用户希望远程设备转发到串口的数据包包含有效的 MAC 地址时，则需要添加源 MAC 地址。

数据目标地址选择：用户通过串口转发的数据，或者 IO/ADC 采集数据，需要传输到指定的一台目标设备，用目标地址来指示这台设备。用户可以自行选择，用网络地址或者 MAC 地址来作为目标地址。单播模式下有效。

1. 目标网络地址：数据会发送至设备配置信息中的目标网络地址(DEV_INFO.DstAddr)，参见表 14.66。
2. 目标 MAC 地址：数据会发送至设备配置信息中的目标 MAC 地址(DEV_INFO.DstIEEE)，参见表 14.66。

数据包格式：用户可以指定从串口发送的数据包的格式，从而改变数据的发送方式，单播模式下有效。

1. 数据：串口数据包只有普通数据，将会根据预设的方式（数据传输方式/是否添加源 MAC 地址/数据目标地址）进行传输。

   例如：从串口发送数据 AA BB CC，会根据预先配置好的方式（单播/带有源 MAC 地址/目标 MAC 地址）传输。

2. 临时目标网络地址+数据：串口数据包，包含指定设备的网络地址和普通数据。

当串口发送有效的数据包时，会临时改变目标网络地址，然后传输到指定设备。

例如：从串口发送 00 00 AA BB CC，会临时改变目标网络地址为 00 00，然后传输数据 AA BB CC。

3. 临时目标 MAC 地址+数据：串口数据包，包含指定设备的 MAC 地址和普通数据。当串口发送有效的数据包时，会临时改变目标 MAC 地址，然后传输到指定设备。

   例如：从串口发送 11 22 33 44 55 66 77 88 AA BB CC，会临时改变目标 MAC 地址为 11:22:33:44:55:66:77:88，然后传输数据 AA BB CC。

4. 发送帧格式：透传数据需要按照发送帧格式发向串口。当目标网络地址是 0xFFFE 时，目标 MAC 地址将作为透传数据发送的目的地址。

   例如：从串口发送 AD DB BE 10 00 00 00 00 00 00 00 00 00 00 03 AA BB CC 8A AA，会向网络地址 0x0000 传输数据 AA BB CC；或者从串口发送 AD DB BE 10 11 22 33 44 55 66 77 88 FF FE 00 03 AA BB CC EB AA，会向 MAC 地址 11:22:33:44:55:66:77:88 传输数据 AA BB CC。

设置发送模式的应答报文如表 14.13 所示。

表 14.13 设置发送模式的应答报文

3 字节（协议标志）	1 字节	1 字节
DE DF EF	D9	状态 0x00：设置成功 其它：设置失败

命令示例：设置发送模式为单播发送模式、向目标网络地址发送、不包含本地 MAC 地址。

```
CMD： DE DF EF D9 00
RSP： DE DF EF D9 00
```

14.1.6 设置广播命令应答延时

计算延时时间的方式如下。

当移动方向是向左移时：

延时时间(ms)=(本地网络地址<<移动位数) * 1ms

当移动方向是向右移时：

延时时间(ms)=(本地网络地址>>移动位数) * 1ms

例如：协调器发起广播命令获取网络拓扑，终端设备的网络地址是 0x8000，移动方向是向右移，移动位数是 5，延时时间等于(0x8000>>5)*1ms，即延时 1024ms 后，终端设备就会将应答发送给协调器。

设置广播应答命令延时的命令如表 14.14 所示。

表 14.14 设置广播命令应答延时

3 字节（协议标志）	1 字节	1 字节
DE DF EF	F7	延时参数： Bit-7：移动方向 Bit-6~Bit-3：保留 Bit-2~Bit-0：移动位数

移动方向：0 是向右移动，1 是向左移动。

如果本地设备加入了某个网络内，就会发起一次广播，网络内的设备接收到这条命令，就会设置相应延时；本命令没有应答，并且会清空当前延时等待的命令应答。

命令示例：设置广播命令应答延时为，(本地网络地址>>5) * 1ms。

```
CMD： DE DF EF F7 05
```

14.1.7 基于 MAC 地址通讯命令集

1. 设置 I/O 输入输出

设置 I/O 输入输出的命令如表 14.15 所示。

表 14.15 设置 I/O 输入输出

3 字节（协议标志）	1 字节	8 字节	1 字节
DE DF EF	54	MAC 地址	IO 状态 0x00：输入 0x01：输出

I/O 输入输出，bit0~bit3 为 IO1~IO4，其相应位为 1，表示 I/O 为输出；其相应位为 0，表示 I/O 为输入。

本命令当前支持广播，暂不支持组播（支持广播的命令会特别说明）。

MAC 地址：

FF:FF:FF:FF:FF:FF:FF:FF 代表广播给所有设备；

FF:FF:FF:FF:FF:FF:FF:FD 代表广播给所有非睡眠设备；

FF:FF:FF:FF:FF:FF:FF:FC 代表广播给协调器和路由设备；

注意的是，广播情况下，远程设备将不会返回应答报文。

设置 I/O 输入输出的应答报文如表 14.16 所示。

表 14.16 设置 I/O 输入输出的应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节
DE DF EF	54	MAC 地址	状态 0x00：设置成功 其它：设置失败

命令示例：将目标节点的 IO1 设置成输出，IO2~IO4 设置成输入。

CMD： DE DF EF 54 12 34 56 78 90 AB CD EF 01
RSP： DE DF EF 54 12 34 56 78 90 AB CD EF 00

2. 读取 I/O 状态

读取 I/O 状态的命令如表 14.17 所示。

表 14.17 读取 I/O 状态

3 字节（协议标志）	1 字节	8 字节
DE DF EF	55	MAC 地址

读取 I/O 状态的命令的应答报文如表 14.18 所示。

表 14.18 读取 I/O 状态的应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节
DE DF EF	55	MAC 地址	IO 状态 0x00：低电平 0x01：高电平

1 字节 I/O 状态，bit0~bit3 位为 IO1~IO4。可读取本地 I/O 或远程 I/O，需先将 I/O 口设置成输入状态。

命令示例：读取目标节点 12:34:56:78:90:AB:CD:EF 的 IO 状态。

CMD： DE DF EF 55 12 34 56 78 90 AB CD EF
RSP： DE DF EF 55 12 34 56 78 90 AB CD EF 01 // IO1 为高电平，IO2~IO4 为低电平

3. 设置 I/O 状态

设置 I/O 状态的命令如表 14.19 所示。

表 14.19 设置 I/O 状态

3 字节（协议标志）	1 字节	8 字节	1 字节
DE DF EF	56	MAC 地址	状态 0x00：低电平 0x01：高电平

本命令当前支持广播，暂不支持组播（支持广播的命令会特别说明）。

MAC 地址：

FF:FF:FF:FF:FF:FF:FF:FF 代表广播给所有设备；

FF:FF:FF:FF:FF:FF:FF:FD 代表广播给所有非睡眠设备；

FF:FF:FF:FF:FF:FF:FF:FC 代表广播给协调器和路由设备；

注意的是，广播情况下，远程设备将不会返回应答报文。

设置 I/O 状态的应答报文如表 14.20 所示。

表 14.20 设置 I/O 状态的应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节
DE DF EF	56	MAC 地址	状态 0x00：设置成功 其它：设置失败

命令示例：将目标节点的 IO1 设置成高电平，IO2~IO4 设置成低电平。

CMD： DE DF EF 56 12 34 56 78 90 AB CD EF 01
RSP： DE DF EF 56 12 34 56 78 90 AB CD EF 00

4. 读取 AD

读取 AD 的命令如表 14.21 所示。

表 14.21 读取 AD

3 字节（协议标志）	1 字节	8 字节	1 字节
DE DF EF	57	MAC 地址	AD 通道号（1~4）

读取 AD 的应答报文如表 14.22 所示。

表 14.22 读取 AD 的应答报文

3 字节（协议标志）	1 字节	8 字节	2 字节
DE DF EF	57	MAC 地址	AD 值

可设置本地或远程 12 位 AD，参考电压 2.5V。

命令示例：读取目标节点 12:34:56:78:90:AB:CD:EF 的 CH0 AD 值

CMD： DE DF EF 57 12 34 56 78 90 AB CD EF 00
RSP： DE DF EF 57 12 34 56 78 90 AB CD EF 00 9E

5. 查询路由表(只有路由及协调器有效)

查询路由表的命令如表 14.23 所示。由于实际路由表大小可能会超出数据处理范围，所以分成块来处理，每个块占用 16 条路由记录，块序号从 0 开始。当前路由表最多能提供 128 条路由记录，所以有 8 个块，块序号从 0~7。

表 14.23 查询路由表

3 字节（协议标志）	1 字节	8 字节	1 字节
DE DF EF	5C	MAC 地址	块序号

查询路由表的应答报文中路由表条目数量是块里面有效的路由表条目数量，最多有 16 条，应答报文如表 14.24 所示。

表 14.24 查询路由表的应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节
DE DF EF	5C	MAC 地址	块序号	路由表条目数量 N 0x00~0xFF
2 字节	2 字节	2 字节	2 字节	
第一条 目标网络地址 0x0000~0xFFFF	第一条 下一跳网络地址 0x0000~0xFFFF	第 N 条 目标网络地址 0x0000~0xFFFF	第 N 条 下一跳网络地址 0x0000~0xFFFF	

命令示例：获取网络地址为 12:34:56:78:90:AB:CD:EF 路由表块 0 的记录

CMD： DE DF EF 5C 12 34 56 78 90 AB CD EF 00

RSP： DE DF EF 5C 12 34 56 78 90 AB CD EF 00 01 00 00 1F 03

6. 搜索存在的网络

根据要求的通道掩码，搜索对应通道存在的网络，其命令如表 14.25 所示。

表 14.25 搜索存在的网络

3 字节（协议标志）	1 字节	8 字节	2 字节	2 字节
DE DF EF	5D	MAC 地址	通道掩码①	每个通道的搜索时间（ms）②

注①：通道掩码：每个 bit 代表一个通道，如 bit0 代表通道 11，bit15 代表通道 26；

注②：每个通道的搜索时间:30ms，46ms，76ms，138ms，261ms，506ms，998ms，1981ms，3947ms，7879ms，15744ms，31472ms，62929ms

搜索的应答报文如表 14.26 所示。

表 14.26 搜索存在的网络的应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	2 字节	2 字节	1 字节	1 字节
DE DF EF	5D	MAC 地址	存在的网络条目数量 N 0x00~0xFF	网络 ID 0x0000~ 0xFFFF	网络地址 0x0000~ 0xFFFF	通道号 (11~26)	RSSI 接收信号强度 (dBm) 0x00~0xFF(有符号)
1 字节	…	…	2 字节	2 字节	1 字节	1 字节	1 字节
网络是否允许加入 0x0 不允许 0x01 允许	…	…	第 N 条 网络 ID 0x0000~ 0xFFFF	第 N 条 网络地址 0x0000~ 0xFFFF	第 N 条 通道号 (11~26)	第 N 条 RSSI 接收信号强度(dBm) 0x00~0xFF(有符号)	第 N 条 网络是否允许加入 0x00 不允许 0x01 允许

命令示例：搜索存在的网络

```
CMD：DE DF EF 5D 12 34 56 78 90 AB CD EF FF FF 01 05
RSP： DE DF EF 5D 12 34 56 78 90 AB CD EF 02 11 22 00 00 0B D8 01 15 32 00 00 0B D0 01
```

7. 查询节点的接收信号强度

查询节点的接收信号强度命令如表 14.27 所示。

表 14.27 查询节点的接收信号强度

3 字节（协议标志）	1 字节	8 字节
DE DF EF	5E	MAC 地址

查询节点的接收信号强度的应答报文如表 14.28 所示。

表 14.28 查询节点的接收信号强度的应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节
DE DF EF	5E	MAC 地址	本地接收信号强度（dBm） 0x00~0xFF（有符号）	远程接收信号强度（dBm） 0x00~0xFF（有符号）

本地接收信号强度是指本机模块接收到目标模块数据时对应的接收信号强度。

远程接收信号强度是指目标模块接收到本机模块数据时对应的接收信号强度。如果经过路由跳转，则指上一级进来的信号强度。

命令示例：查询节点的接收信号强度

```
CMD： DE DF EF 5E 12 34 56 78 90 AB CD EF        // 获取模块的接收信号强度
RSP： DE DF EF 5E 12 34 56 78 90 AB CD EF BA BD
    // 获取到的本地接收信号强度为-70dBm 远程为-67dBm
```

8. 设置接收模式

当模块接收到透传数据时，会进行根据接收模式的相关设置进行处理，然后发送到通过串口连接的用户设备。设置接收模式的命令如表 14.29 所示。

表 14.29 设置接收模式

3 字节（协议标志）	1 字节	8 字节	1 字节
DE DF EF	73	MAC 地址	接收模式

接收模式的位域如表 14.30 所示，保留位填 0。

表 14.30 接收模式的位域

Bit 3~7	Bit 0~2 数据包格式
保留	0：数据 1：源网络地址+数据 2：源 MAC 地址+数据 3：源网络地址+源 MAC 地址+数据 4：接收帧格式

数据包格式：用户可以指定接收到的原始数据，跟一些有用信息打包在一起，然后才发

送到串口。其中，当数据源(设备)并没有在"是否添加源 MAC 地址"中设置添加源 MAC 地址，则数据包会打包一个无效的 MAC 地址 FF:FF:FF:FF:FF:FF:FF:FF。

1. 数据：透传接收到的原始数据。

   例如：本地设备收到某个远程设备传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 AA BB CC。

2. 源网络地址+数据：原始数据的前面会加上数据源(设备)的网络地址。

   例如：本地设备收到协调器(0x0000)传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 00 00 AA BB CC。

3. 源 MAC 地址+数据：原始数据的前面会加上数据源(设备)的 MAC 地址。

   例如：本地设备收到设备(11:22:33:44:55:66:77:88)传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 11 22 33 44 55 66 77 88 AA BB CC。

4. 源网络地址+源 MAC 地址+数据：原始数据的前面会加上数据源(设备)的网络地址和 MAC 地址。

   例如：本地设备收到协调器(0x0000/11:22:33:44:55:66:77:88)发过来的数据(0xAA 0xBB 0xCC)，则串口会输出 00 00 11 22 33 44 55 66 77 88 AA BB CC。

5. 接收帧格式：原始的数据会格式化成接收帧。

   例如：本地设备接收到协调器(0x0000/11:22:33:44:55:66:77:88)发过来的数据(0xAA 0xBB 0xCC)，则串口会输出 AD DB BE 90 11 22 33 44 55 66 77 88 00 00 00 03 AA BB CC 6E AA。

设置接收模式的应答报文如表 14.31 所示。

表 14.31 设置接收模式的应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节
DE DF EF	73	MAC 地址	状态 0x00：设置成功 其它：设置失败

命令示例：设置接收数据包头显示网络地址

```
CMD：  DE DF EF 73 12 34 56 78 90 AB CD EF 01
RSP：  DE DF EF 73 12 34 56 78 90 AB CD EF 00
```

9. 设置目标 MAC 地址

设置目标 MAC 地址的命令如表 14.32 所示。

表 14.32 设置目标 MAC 地址

3 字节（协议标志）	1 字节	8 字节	8 字节
DE DF EF	74	MAC 地址	目标 MAC 地址

目标 MAC 地址：

FF:FF:FF:FF:FF:FF:FF:FF 代表广播给所有设备；

FF:FF:FF:FF:FF:FF:FF:FD 代表广播给所有非睡眠设备；

FF:FF:FF:FF:FF:FF:FF:FC 代表广播给协调器和路由设备；

FF:FF:FF:FF:FF:FF:FF:FB 代表使用目标组号，发送组播；

00:00:00:00:00:00:00:00 代表协调器。

设置目标 MAC 地址的应答报文如表 14.33 所示。

表 14.33　设置目标 MAC 地址的应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节
DE DF EF	74	MAC 地址	状态 0x00：设置成功 其它：设置失败

命令示例：设置目标 MAC 地址

CMD：　DE DF EF 74 12 34 56 78 90 AB CD EF 11 22 33 44 55 66 77 88

RSP：　DE DF EF 74 12 34 56 78 90 AB CD EF 00

10. 命令的应答时间

命令的应答时间的命令如表 14.34 所示。

表 14.34　应答时间

3 字节（协议标志）	1 字节	8 字节
DE DF EF	76	MAC 地址

应答时间是从本地设备发起命令，直到接收到应答报文所经过的时间，单位是 1ms。当从串口接收到应答时间命令时，将会更新参考时间戳，等收到远程设备的应答报文后，就会用当前时间戳减去参考时间戳，得到应答时间。

应答时间的应答报文如表 14.35 所示。

表 14.35　应答时间的应答报文

3 字节（协议标志）	1 字节	8 字节	2 字节
DE DF EF	76	MAC 地址	应答时间 单位 ms

命令示例：设备 12:34:56:78:90:AB:CD:EF 的应答时间

CMD：　DE DF EF 76 12 34 56 78 90 AB CD EF

RSP：　DE DF EF 76 12 34 56 78 90 AB CD EF 00 54

11. 获取网络地址

获取网络地址的命令如表 14.36 所示。

表 14.36　获取网络地址

3 字节（协议标志）	1 字节	8 字节
DE DF EF	FE	MAC 地址

这条命令能够指定 MAC 地址，然后获取该设备的网络地址。

获取网络地址的应答报文如表 14.37 所示。

表 14.37 获取网络地址的应答报文

3 字节（协议标志）	1 字节	8 字节	2 字节
DE DF EF	FE	MAC 地址	网络地址

命令示例：获取设备 11:22:33:44:55:66:77:88 的网络地址。

CMD： DE DF EF FE 11 22 33 44 55 66 77 88
RSP： DE DF EF FE 11 22 33 44 55 66 77 88 20 01

14.1.8 基于网络地址通讯命令集

1. 设置 I/O 输入输出

设置 I/O 输入输出的命令如表 14.38 所示。

表 14.38 设置 I/O 输入输出

3 字节（协议标志）	1 字节	2 字节	1 字节
DE DF EF	D4	网络地址 0x0000~0xFFFF	IO 状态 0x00：输入 0x01：输出

I/O 输入输出，bit0~bit3 为 IO1~IO4，其相应位为 1，表示 I/O 为输出；其相应位为 0，表示 I/O 为输入。

本命令支持广播，暂不支持组播（当前支持广播的命令很少）。

网络地址：

0xFFFF 代表广播给所有设备；

0xFFFD 代表广播给所有非睡眠设备；

0xFFFC 代表广播给协调器和路由设备；

注意：广播情况下，远程设备将不会返回应答报文。

设置 I/O 输入输出的应答报文如表 14.39 所示。

表 14.39 设置 I/O 输入输出的应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节
DE DF EF	D4	网络地址 0x0000~0xFFFF	状态 0x00：设置成功 其它：设置失败

命令示例：设置 I/O 输入输出

CMD： DE DF EF D4 20 01 01 //将目标节点 2001 的 IO1 设置成输出，IO2~IO4 设置成输入
RSP： DE DF EF D4 20 01 00

2. 读取 I/O 状态

读取 I/O 状态的命令如表 14.40 所示。

表 14.40 读取 I/O 状态

3 字节（协议标志）	1 字节	2 字节
DE DF EF	D5	网络地址 0x0000~0xFFFF

读取 I/O 状态的命令的应答报文如表 14.41 所示。

表 14.41 读取 I/O 状态的应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节
DE DF EF	D5	网络地址 0x0000~0xFFFF	IO 状态 0x00：低电平 0x01：高电平

1 字节 I/O 状态，bit0~bit3 位为 IO1~IO4。可读取本地 I/O 或远程 I/O，需先将 I/O 口设置成输入状态。

命令示例：读取 I/O 状态

CMD： DE DF EF D5 20 01 //读取目标节点 2001 的 IO 状态。
RSP： DE DF EF D5 20 01 01 // IO1 为高电平，IO2~IO4 为低电平

3. 设置 I/O 状态

设置 I/O 状态的命令如表 14.42 所示。

表 14.42 设置 I/O 状态

3 字节（协议标志）	1 字节	2 字节	1 字节
DE DF EF	D6	网络地址 0x0000~0xFFFF	状态 0x00：低电平 0x01：高电平

本命令支持广播，暂不支持组播（当前支持广播的命令很少）。

网络地址：

0xFFFF 代表广播给所有设备；

0xFFFD 代表广播给所有非睡眠设备；

0xFFFC 代表广播给协调器和路由设备；

注意：广播情况下，远程设备将不会返回应答报文。

设置 I/O 状态的应答报文如表 14.43 所示。

表 14.43 设置 I/O 状态的应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节
DE DF EF	D6	网络地址 0x0000~0xFFFF	状态 0x00：设置成功 其它：设置失败

命令示例：将目标节点 2001 的 IO1 设置成高电平，IO2~IO4 设置成低电平。

```
CMD：  DE DF EF D6 20 01 01
RSP：  DE DF EF D6 20 01 00
```

4. 读取 AD

读取 AD 的命令如表 14.44 所示。

表 14.44 读取 AD

3 字节（协议标志）	1 字节	2 字节	1 字节
DE DF EF	D7	网络地址 0x0000~0xFFFF	AD 通道号（1~4）

读取 AD 的应答报文如表 14.45 所示。

表 14.45 读取 AD 的应答报文

3 字节（协议标志）	1 字节	2 字节	2 字节
DE DF EF	D7	网络地址 0x0000~0xFFFF	AD 值

可设置本地或远程 12 位 AD，参考电压 2.5V。

命令示例：读取 AD

```
CMD：  DE DF EF D7 20 01 00                    // 读取目标节点 2001 的 CH0AD 值
RSP：  DE DF EF D7 20 01 00 9E
```

5. 查询路由表(只有路由及协调器有效)

查询路由表的命令如表 14.46 所示。由于实际路由表大小可能会超出数据处理范围，所以分成块来处理，每个块占用 16 条路由记录，块序号从 0 开始。当前路由表最多能提供 **128** 条路由记录，所以有 8 个块，块序号从 0~7。

表 14.46 查询路由表

3 字节（协议标志）	1 字节	2 字节	1 字节
DE DF EF	DC	网络地址 0x0000~ 0xFFFF	块序号

查询路由表的应答报文中路由表条目数量是块里面有效的路由表条目数量，最多有 16 条，应答报文如表 14.47 所示。

表 14.47 查询路由表的应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节
DE DF EF	DC	网络地址 0x0000~0xFFFF	块序号	路由表条目数量 N 0x00~0xFF
2 字节	2 字节	2 字节	2 字节	
第一条 目标网络地址 0x0000~0xFFFF	第一条 下一跳网络地址 0x0000~0xFFFF	第 N 条 目标网络地址 0x0000~0xFFFF	第 N 条 下一跳网络地址 0x0000~0xFFFF	

命令示例：获取网络地址为 0x 2002 路由表块 0 的记录

CMD： DE DF EF DC 20 02 00

RSP： DE DF EF DC 20 02 00 01 00 00 1F 03

6. 搜索存在的网络

根据要求的通道掩码，搜索对应通道存在的网络，其命令如表 14.48 所示。

表 14.48 搜索存在的网络

3 字节（协议标志）	1 字节	2 字节	2 字节	2 字节
DE DF EF	DD	网络地址 0x0000~ 0xFFFF	通道掩码①	每个通道的搜索时间（ms）②

注1 ：通道掩码：每个 bit 代表一个通道，如 bit0 代表通道 11，bit15 代表通道 26；

注2 ：每个通道的搜索时间:30ms，46ms，76ms，138ms，261ms，506ms，998ms，1981ms，3947ms，7879ms，15744ms，31472ms，62929ms

搜索的应答报文如表 14.49 所示。

表 14.49 搜索存在的网络的应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	2 字节	2 字节	1 字节	1 字节
DE DF EF	DD	网络地址 0x0000~ 0xFFFF	存在的网络条目数量 N 0x00~0xFF	网络 ID 0x0000~ 0xFFFF	网络地址 0x0000~ 0xFFFF	通道号 (11~26)	RSSI 接收信号强度 (dBm) 0x00~0xFF(有符号)
1 字节	…	…	2 字节	2 字节	1 字节	1 字节	1 字节
网络是否允许加入 0x0 不允许 0x01 允许	…	…	第 N 条 网络 ID 0x0000~ 0xFFFF	第 N 条 网络地址 0x0000~ 0xFFFF	第 N 条 通道号 (11~26)	第 N 条 RSSI 接收信号强度 (dBm) 0x00~0xFF(有符号)	第 N 条 网络是否允许加入 0x0 不允许 0x01 允许

命令示例：搜索存在的网络

CMD：DE DF EF DD 20 01 FF FF 01 05

RSP： DE DF EF DD 20 01 02 11 22 00 00 0B D8 01 15 32 00 00 0B D0 01

7. 查询节点的接收信号强度

查询节点的接收信号强度命令如表 14.50 所示。

表 14.50 查询节点的接收信号强度

3 字节（协议标志）	1 字节	2 字节
DE DF EF	DE	网络地址 0x0000~0xFFFF

查询节点的接收信号强度的应答报文如表 14.51 所示。

表 14.51 查询节点的接收信号强度的应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节
DE DF EF	DE	网络地址 0x0000~0xFFFF	本地接收信号强度 （dBm） 0x00~0xFF （有符号）	远程接收信号强度 （dBm） 0x00~0xFF （有符号）

本地接收信号强度是指本机模块接收到目标模块数据时对应的接收信号强度。

远程接收信号强度是指目标模块接收到本机模块数据时对应的接收信号强度。如果经过路由跳转，则指上一级进来的信号强度。

命令示例：查询节点的接收信号强度

```
CMD：  DE DF EF DE 20 02          // 获取模块的接收信号强度
RSP：  DE DF EF DE 20 02 BA BD    // 获取到的本地接收信号强度为-70dBm 远程为-67dBm
```

8. 设置接收模式

当模块接收到透传数据时，会进行根据接收模式的相关设置进行处理，然后发送到通过串口连接的用户设备。设置接收模式的命令如表 14.52 所示。

表 14.52 设置接收模式

3 字节（协议标志）	1 字节	2 字节	1 字节
DE DF EF	F3	网络地址 0x0000~0xFFFF	接收模式

接收模式的位域如表 14.53 所示，保留位填 0。

表 14.53 接收模式的位域

Bit 3~7	Bit 0~2 数据包格式
保留	0：数据 1：源网络地址+数据 2：源 MAC 地址+数据 3：源网络地址+源 MAC 地址+数据 4：接收帧格式

数据包格式：用户可以指定接收到的原始数据，跟一些有用信息打包在一起，然后才发送到串口。其中，当数据源(设备)并没有在"是否添加源 MAC 地址"中设置添加源 MAC 地址，则数据包会打包一个无效的 MAC 地址 FF:FF:FF:FF:FF:FF:FF:FF。

1. 数据：透传接收到的原始数据。

   例如：本地设备收到某个远程设备传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 AA BB CC。

2. 源网络地址+数据：原始数据的前面会加上数据源(设备)的网络地址。

   例如：本地设备收到协调器(0x0000)传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 00 00 AA BB CC。

3. 源 MAC 地址+数据：原始数据的前面会加上数据源(设备)的 MAC 地址。

   例如：本地设备收到设备(11:22:33:44:55:66:77:88)传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 11 22 33 44 55 66 77 88 AA BB CC。

4. 源网络地址+源 MAC 地址+数据：原始数据的前面会加上数据源(设备)的网络地址和 MAC 地址。

   例如：本地设备收到协调器(0x0000/11:22:33:44:55:66:77:88)发过来的数据(0xAA 0xBB 0xCC)，则串口会输出 00 00 11 22 33 44 55 66 77 88 AA BB CC。

5. 接收帧格式：原始的数据会格式化成接收帧。

   例如：本地设备接收到协调器(0x0000/11:22:33:44:55:66:77:88)发过来的数据(0xAA 0xBB 0xCC)，则串口会输出 AD DB BE 90 11 22 33 44 55 66 77 88 00 00 00 03 AA BB CC 6E AA。

设置接收模式的应答报文如表 14.54 所示。

表 14.54 设置接收模式的应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节
DE DF EF	F3	网络地址 0x0000~0xFFFF	状态 0x00：设置成功 其它：设置失败

命令示例：设置接收模式

```
CMD：  DE DF EF F3 20 01 01 //设置接收数据包头显示网络地址
RSP：  DE DF EF F3 20 01 00 //  设置成功
```

9. 设置目标 MAC 地址

设置目标 MAC 地址的命令如表 14.55 所示。

表 14.55 设置目标 MAC 地址

3 字节（协议标志）	1 字节	2 字节	8 字节
DE DF EF	F4	网络地址 0x0000~0xFFFF	目标 MAC 地址

目标 MAC 地址：

FF:FF:FF:FF:FF:FF:FF:FF 代表广播给所有设备；

FF:FF:FF:FF:FF:FF:FF:FD 代表广播给所有非睡眠设备；

FF:FF:FF:FF:FF:FF:FF:FC 代表广播给协调器和路由设备；

FF:FF:FF:FF:FF:FF:FF:FB 代表使用目标组号，发送组播；

00:00:00:00:00:00:00:00 代表协调器。

设置目标 MAC 地址的应答报文如表 14.56 所示。

表 14.56 设置目标 MAC 地址的应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节
DE DF EF	F4	网络地址 0x0000~0xFFFF	状态 0x00：设置成功 其它：设置失败

命令示例：设置目标 MAC 地址

CMD： DE DF EF F4 20 01 11 22 33 44 55 66 77 88
RSP： DE DF EF F4 20 01 00

10. 获取网络拓扑

获取网络拓扑的命令如表 14.57 所示。

表 14.57 获取网络拓扑

3 字节（协议标志）	1 字节	2 字节	1 字节
DE DF EF	F5	网络地址 0x0000~0xFFFF	选项 0：网络地址获取 1：广播获取

获取网络拓扑命令可以改变选项字段，改变获取网络拓扑信息的方式。选项为 0，表示通过网络地址，获取指定设备的拓扑信息；选项为 1，表示通过广播获取网络的拓扑信息。

获取网络拓扑的应答报文如表 14.58 所示。

表 14.58 获取网络拓扑的应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	2 字节	1 字节
DE DF EF	F5	网络地址 0x0000~0xFFFF	设备类型	保留	邻居个数
2 字节	1 字节	2 字节	1 字节		
第一条 邻居网络地址 0x0000~0xFFFF	第一条 LQI 0~255	第 N 条 邻居网络地址 0x0000~0xFFFF	第 N 条 LQI 0~255		

当选项为 0，通过广播获取拓扑信息时，设备都会将自己的网络地址、设备类型，还有附近的邻居设备的网络地址以及 LQI 信息应答回来。

命令示例：用广播获取网络拓扑

CMD： DE DF EF F5 FF FF 01
RSP： DE DF EF F5 00 00 02 00 00 01 AB CD F5 // 协调器返回网络拓扑信息
RSP： DE DF EF F5 AB CD 00 00 00 01 00 00 F9 // 终端返回网络拓扑信息

命令示例：指定网络地址获取指定设备的拓扑信息

CMD： DE DF EF F5 00 00 00
RSP： DE DF EF F5 00 00 02 00 00 01 AB CD F5 // 协调器返回网络拓扑信息

11. 命令的应答时间

命令的应答时间的命令如表 14.59 所示。

表 14.59 应答时间

3 字节（协议标志）	1 字节	2 字节
DE DF EF	F6	网络地址

应答时间是从本地设备发起命令，到收到该网络地址的设备应答报文，经过的时间，单位是 1ms。当从串口接收到应答时间命令时，将会更新参考时间戳，等收到远程设备的应答报文后，就会用当前时间戳减去参考时间戳，得到应答时间。

应答时间的应答报文如表 14.60 所示。

表 14.60 应答时间的应答报文

3 字节（协议标志）	1 字节	2 字节	2 字节
DE DF EF	F6	网络地址 0x0000~0xFFFF	应答时间 单位 ms

命令示例：设备 0x2001 的应答时间

CMD： DE DF EF F6 20 01

RSP： DE DF EF F6 20 01 00 54

14.2 永久参数配置协议与命令

ZM 系列 ZigBee 模块永久参数配置除了可以使用配置工具进行配置外（使用配置工具 WirelessCfg 配置的都是永久配置命令），也可以使用命令的方式进行配置。永久参数配置协议命令帧格式详见表 14.61。

表 14.61 配置协议命令

3 字节（协议标志）	1 字节	N 字节	1 字节
AB BC CD	命令标识符	命令实体	帧尾

ZM32 模块支持两种参数配置协议；永久参数配置协议和临时参数配置协议。

永久参数配置协议配置的参数是保存在模块的非易失性存储区，配置参数可掉电保存，模块上电后使用永久参数运行。由于非易失性存储介质的特点，频繁擦除，写入会影响存储介质的寿命，最后失效，所以建议不要频繁使用永久参数配置命令。

如果需要频繁修改运行时的工作参数，可以使用临时参数配置协议。

临时参数配置协议配置的参数是保存在模块的 RAM 里，掉电不能保存；用户在使用了临时参数配置命令后，工作参数会马上更新，但当发生复位、重启等操作后，临时配置失效，工作参数恢复成原来的样子，通常临时参数是用户需要经常改变的参数。

永久参数配置协议与命令，分为基于 MAC 地址通讯命令集、基于网络地址通讯命令集，和本地命令集。

当使用基于 MAC 地址通讯的命令时，00:00:00:00:00:00:00:00 代表协调器，FF:FF:FF:FF:FF:FF:FF:FE 代表本地设备执行。

当使用基于网络地址通讯的命令时，0xFFFE 代表本地设备执行。

各命令类型的命令标识符详见表 14.62。

表 14.62 配置协议命令标识

命令类型	命令标识符	备注
读取本地配置	0xD1	
启用白名单	0x20	
配置白名单	0x21	
配置发送选项	0x22	
配置白名单(新)	0x23	
请求更新远程路由到本地路由的路径	0x26	
配置自组网	0x27	设置后复位才有效，可替代启用自组网命令
主机允许从机加入网络	0xE6	
查询主从机状态	0xE8	
备份	0xFA	
恢复	0xFB	
基于 MAC 地址通讯命令集		
配置通道	0x40	
配置 PAN ID	0x41	
配置分组	0x42	
配置目标组号	0x43	
搜索网络内的设备	0x54	
获取远程配置信息	0x55	
修改配置	0x56	设置后复位才有效
复位	0x59	无应答
恢复出厂设置	0x5A	设置后复位才有效
模块密码使能	0x5E	
模块登录	0x5F	
I/O 方向设置	0x61	设置后复位才有效
IO/AD 采集设置	0x62	设置后复位才有效
I/O 控制输出	0x63	

续上表

PWM 控制输出	0x64	
设置目标网络地址	0x69	
读取设备类型	0x6A	
查询子终端节点的 MAC 地址(只有路由及协调器有效)	0x6B	
查询父节点 MAC 地址	0x6C	
查询网络地址	0x6D	
设置模块密钥	0x6E	建网、加网前配置才有效
读取模块密钥	0x6F	
进入升级模式	0x71	
固件升级	0x72	
设置接收模式	0x73	
设置目标 MAC 地址	0x74	
设置发送模式	0x75	
启用黑名单	0x77	
配置黑名单	0x78	
基于网络地址通讯命令集		
配置通道	0xC0	
配置 PAN ID	0xC1	
配置分组	0xC2	
配置目标组号	0xC3	
搜索网络内的设备	0xD4	
获取远程配置信息	0xD5	
修改配置	0xD6	设置后复位才有效，可以使用该命令修改 MAC 地址
复位	0xD9	无应答
恢复出厂设置	0xDA	设置后复位才有效
模块密码使能	0xDE	恢复出厂设置，默认不使能模块密码，设置后复位有效
模块登录	0xDF	如果模块使能了密码，需要先登录才能修改配置
I/O 方向设置	0xE1	设置后复位才有效
IO/AD 采集设置	0xE2	设置后复位才有效
I/O 控制输出	0xE3	

续上表

PWM 控制输出	0xE4	
设置目标网络地址	0xE9	
读取设备类型	0xEA	
查询子终端节点网络地址(只有路由及协调器有效)	0xEB	
查询父节点网络地址	0xEC	
查询 MAC 地址	0xED	
设置模块密钥	0xEE	建网、加网前配置才有效
读取模块密钥	0xEF	
进入升级模式	0xF1	
固件升级	0xF2	
设置接收模式	0xF3	
设置目标 MAC 地址	0xF4	
设置发送模式	0xF5	
设置广播应答延时	0xF6	
启用黑名单	0xF7	
配置黑名单	0xF8	

各配置命令帧返回的应答帧中包含有各种操作的响应状态，各响应状态如表 14.63 所示。

表 14.63 配置命令响应状态

响应状态	错误码
正常 OK	0x00
长度错误 LENGTH _FAUSE	0x01
地址错误 ADDRESS _FAUSE	0x02
校验错误 CHECK_FAUSE	0x03
写错误 WRITE_FAUSE	0x04
其他错误 OTHER_FAUSE	0x05
不支持 NOTSUP_FAUSE	0x06
无效参数 INVAL_FAUSE	0x07

14.2.1 读取本地配置

其读取命令如表 14.64 所示。

表 14.64　读取本地配置

3 字节（协议标志）	1 字节	1 字节（帧尾）
AB BC CD	D1	AA

其读取的应答报文如表 14.65 所示。

表 14.65　读取本地配置应答报文

3 字节（协议标志）	1 字节	68 字节	1 字节	2 字节	2 字节
AB BC CD	D1	DEV_INFO 结构信息	运行状态	协议类型	固件版本

DEV_INFO 结构信息详见表 14.66。

运行状态：

0x55：处于升级模式下，仅支持读取本地配置以及升级命令

0xF1：所读配置参数不可靠，需要复位

0xAA：正常配置参数

固件版本：采用 8421-BCD 编码。MSB 的 8 位分成 2 个 4 位，用来编码主版本号；LSB 的 8 位分成 2 个 4 位，用来编码副版本号；例如："02 10" 代表固件版本 "V2.10"。

协议类型：0x0004

表 14.66　DEV_INFO 结构信息

信息	偏移地址	长度（字节）	备注	默认值
DevName	0	16	设备名称	ZLG Device
DevPwd	16	16	设备密码	88888(带‘*’则设置无效)
DevType	32	1	设备类型①	终端设备
Chan	33	1	通道号	0x19 (CH 25)
PAN_ID	34	2	PAN ID	0xFFFF(无效)
MyAddr	36	2	本地网络地址	0xFFFF(无效)
MyIEEE	38	8	本地 MAC 地址	芯片唯一地址 (设置全 FF 即恢复成默认)
DstAddr	46	2	目标网络地址	0x0000
DstIEEE	48	8	目标 MAC 地址	0000000000000000
RecvMode	56	1	接收模式②	0x00
PowerLevel	57	1	发射功率③	0x0A
DstGroup	58	2	目标组号	0x0A0A
Serial_Rate	60	1	串口波特率④	0x07

续上表

Serial_DataB	61	1	串口数据位⑤	0x08
Serial_StopB	62	1	串口停止位⑥	0x01
Serial_ParityB	63	1	串口校验位⑦	0x00
SendMode	64	1	发送模式⑧	0x00
Serial_Interval	65	1	帧超时时间(ms)⑨	0x04
Reserved	66	1	保留	0x00
Reserved	67	1	保留	0x00

Note：

1、设备类型分为：

0x00 终端设备；

0x01 路由设备；

0x02 协调器；

默认为终端设备。

2、接收模式（具体描述可参考表 14.200）：

bit0～2 数据包格式：

b000 数据;

b001 源网络地址+数据;

b010 源 MAC 地址+数据;

b011 源网络地址+源 MAC 地址+数据;

b100 接收帧格式，具体的命令格式可参考 14.3.2

3、配置工具中发射功率分为 11 个档位

0x00：-30dBm、0x01：-25dBm、0x02：-20dBm、 0x03：-15dBm、0x04：-10dBm、 0x05：-5dBm、0x06：0dBm、0x07：5dBm、0x08：10dBm、0x09：15dBm、0x0A：19dBm；

0x10: 0dBm、0x11: 1dBm、0x12: 2dBm、0x13: 3dBm、0x14: 4dBm、0x15: 5dBm、0x16: 6dBm、0x17: 7dBm、0x18: 8dBm、0x19: 9dBm、0x1A: 10dBm、0x1B: 11dBm、0x1C: 12dBm、0x1D: 13dBm、0x1E: 14dBm、0x1F: 15dBm

4、串口波特率，对应波特率：

0x01: 2400;
0x02: 4800;
0x03: 9600;
0x04: 19200;
0x05: 38400;
0x06: 57600;
0x07: 115200;
0x08: 230400;

5、串口数据位：仅支持 8；

6、串口停止位：1～2；

7、串口校验位：0x00 表示无校验、0x01 表示奇校验、0x02 表示偶校验；

8、发送模式（具体描述可参考表 14.205）：

bit0～2 数据传输方式：

b000 单播模式;

b001 广播给所有设备;

b010 广播给所有非睡眠设备;

b011 广播给协调器和所有路由器

续上表

b100 组播模式

bit3 是否需要添加源 MAC 地址:

b0 不添加源 MAC 地址;

b1 添加源 MAC 地址

bit4 数据的目标地址选择:

b0 目标网络地址(DEV_INFO.DstAddr);

b1 目标 MAC 地址(DEV_INFO.DstIEEE)

DEV_INFO 请参考表 14.66

bit5～6 单播数据包格式:

b00 数据（根据数据的目标地址进行发送）

b01 临时网络地址+数据

b10 临时 MAC 地址+数据

b11 发送帧格式，具体的命令格式可参考章节 14.3.1

9、帧超时时间:

配置工具中选择不同波特率会默认不同的帧超时时间

2400:60ms、4800:40ms、9600:15ms、19200:10ms、38400:6ms、57600:5ms、115200:4ms、230400:3ms

用户也可自定义时间，但最小时间为 2ms,低于 2ms 均自动设置成 2ms。

命令示例：读取本地配置

CMD：AB BC CD D1 AA

RSP： AB BC CD D1 5A 4C 47 20 44 65 76 69 63 65 00 00 00 00 00 00 38 38 38 38 38 00 00 00 00 00 00 00 00 00 00 00 01 19 10 01 20 01 00 38 1C 25 00 15 8D 00 20 02 00 00 00 00 00 00 00 00 00 00 03 03 0A 06 08 01 00 00 04 00 00 AA 00 01 01 00

14.2.2 启用白名单

当新的终端或者路由设备向协调器发起请求入网时，协调器会检查白名单中是否包含待加入设备的 MAC 地址，如果有，则会同意待加入设备入网，否则拒绝入网。

当前命令用来控制白名单是否生效，仅对协调器有效；对终端或者路由设备使用，响应状态返回不支持。

启用白名单命令如表 14.67 所示。

表 14.67 启用白名单

3 字节（协议标志）	1 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	20	R/W	使能	AA

R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令 IO 参数忽略。

当使能字节为 0 时，不启用白名单功能；为 1 时，模块启用白名单功能。

协调器的白名单功能默认是不启用的。对在启用白名单功能后，申请入网的设备有效。该命令复位后生效。

启用白名单应答报文如表 14.68 所示。

表 14.68 启用白名单应答报文

3 字节（协议标志）	1 字节	1 字节	1 字节
AB BC CD	20	使能	响应状态

在修改配置信息之后，没有进行复位，将无法操作命令，并且响应状态返回其他错误。

响应状态详见表 14.63。

命令示例：查询白名单是否使能

CMD： AB BC CD 20 00 00 AA

RSP： AB BC CD 20 00 00

14.2.3 配置白名单

当前命令用来操作白名单，仅对协调器有效；对终端或者路由设备使用，响应状态返回不支持。

最多支持 255 条。

配置白名单命令如表 14.69 所示。

表 14.69 配置白名单

3 字节（协议标志）	1 字节	1 字节	8 字节	1 字节（帧尾）
AB BC CD	21	控制选项 R/A/C/D	MAC 地址	AA

控制选项 R/C/A/D：

0x00：表示读白名单(Read)，忽略 MAC 地址字段；

0x01：表示写入一条白名单项(Add)，MAC 地址字段为设备的 MAC 地址；

0x02：表示清空白名单(Clear)，忽略 MAC 地址字段；

0x03：表示删除一条白名单项(Delete)，MAC 地址字段为设备的 MAC 地址；

配置白名单应答报文如表 14.70 所示。

表 14.70 配置白名单应答报文

3 字节（协议标志）	1 字节	1 字节	1 字节	8 字节	...	8 字节	1 字节
AB BC CD	21	控制选项 R/A/C/D	数量	第一条 MAC 地址	...	第 N 条 MAC 地址	响应状态

控制选项 R/C/A/D：

0x00：表示读白名单(Read)，数量字节表明后面有多少条 MAC 地址；

0x01：表示写入一条白名单项(Add)，数量字节为 1；

0x02：表示清空白名单(Clear)，数量字节为 0；

0x03：表示删除一条白名单项(Delete)，数量字节为 1；

在修改配置信息之后，没有进行复位，将无法操作命令，并且响应状态返回其他错误。

响应状态详见表 14.63。

命令示例：写入白名单的记录

CMD： AB BC CD 21 01 12 34 56 78 90 AB CD EF AA

RSP： AB BC CD 21 01 01 12 34 56 78 90 AB CD EF 00

14.2.4 配置白名单(新)

因为另外一条配置白名单的命令，最多只能读取 255 条记录，所以新增这条命令，支持读取最多 65535 条记录。

当前模块内部最多存放 340 条。

当存放超过 255 条记录，应当使用这一条命令。

当前命令用来操作白名单，仅对协调器有效；对终端或者路由设备使用，响应状态返回不支持。

配置白名单命令如表 14.71 所示。

表 14.71 配置白名单(新)

3 字节（协议标志）	1 字节	1 字节	8 字节	1 字节（帧尾）
AB BC CD	23	控制选项 R/A/C/D	MAC 地址	AA

控制选项 R/C/A/D：

0x00：表示读白名单(Read)，忽略 MAC 地址字段；

0x01：表示写入一条白名单项(Add)，MAC 地址字段为设备的 MAC 地址；

0x02：表示清空白名单(Clear)，忽略 MAC 地址字段；

0x03：表示删除一条白名单项(Delete)，MAC 地址字段为设备的 MAC 地址；

配置白名单应答报文如表 14.72 所示。

表 14.72 配置白名单(新)应答报文

3 字节（协议标志）	1 字节	1 字节	2 字节	2 字节	8 字节	...	8 字节	1 字节
AB BC CD	23	控制选项 R/A/C/D	数量	保留	第一条 MAC 地址	...	第 N 条 MAC 地址	响应状态

控制选项 R/C/A/D：

0x00：表示读白名单(Read)，数量字节表明后面有多少条 MAC 地址；

0x01：表示写入一条白名单项(Add)，数量字节为 1；

0x02：表示清空白名单(Clear)，数量字节为 0；

0x03：表示删除一条白名单项(Delete)，数量字节为 1；

在修改配置信息之后，没有进行复位，将无法操作命令，并且响应状态返回其他错误。

响应状态详见表 14.63。

命令示例：写入白名单的记录

CMD： AB BC CD 23 01 12 34 56 78 90 AB CD EF AA

RSP： AB BC CD 23 01 00 01 00 00 12 34 56 78 90 AB CD EF 00

命令示例：读取白名单

CMD： AB BC CD 23 00 FF FF FF FF FF FF FF FF AA

RSP： AB BC CD 23 00 00 01 00 00 12 34 56 78 90 AB CD EF 00

14.2.5 配置发送选项

Profile ID 默认值为 0xC105，Cluster ID 默认值为 0x0011，源端点默认值为 0xE8，目标端点默认值为 0xE8，配置发送选项的命令如表 14.73 所示。

表 14.73 配置发送选项

3 字节（协议标志）	1 字节	1 字节	2 字节	2 字节
AB BC CD	22	RW	Profile ID	Cluster ID
1 字节	1 字节	6 字节	1 字节	
源端点	目标端点	保留	AA	

R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令其他字段忽略。

配置发送选项的应答报文如表 14.74 所示。

表 14.74 配置发送选项的应答报文

3 字节（协议标志）	1 字节	2 字节	2 字节
AB BC CD	22	Profile ID	Cluster ID
1 字节	1 字节	6 字节	1 字节
源端点	目标端点	保留	状态 0x00：设置成功 其它：设置失败

命令示例：读取发送选项

CMD： AB BC CD 22 00 00 00 00 00 00 00 00 00 00 00 00 AA

RSP： AB BC CD 22 C1 05 00 11 01 01 00 00 00 00 00 00 00

14.2.6 请求更新远程路由到本地路由的路径

该命令只对协调器与路由设备有效。

请求更新远程路由到本地路由的路径的命令如表 14.75 所示。

表 14.75 请求更新远程路由到本地路由的路径

3 字节（协议标志）	1 字节	1 字节	1 字节	1 字节
AB BC CD	26	RW	周期更新时间 (单位 10s)	AA

R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令

时，该命令其他字段忽略。

周期更新时间，以 10 秒为单位：

0x00：表示当前立即发起一次路径更新请求；

0xFF：表示关闭定时周期请求更新远程路由到本地路由的路径;

其他取值，表示路由设备每隔周期=T*10(s)，发起一次更新远程路由到本地设备的路径的请求。

请求更新远程路由到本地路由的路径应答报文如表 14.76 所示。

表 14.76　请求更新远程路由到本地路由的路径应答报文

3 字节（协议标志）	1 字节	1 字节	1 字节
AB BC CD	26	周期更新时间	0x00：设置成功 其它：设置失败

命令示例：读取周期更新时间

```
CMD:    AB BC CD 26 00 00 AA
RSP:    AB BC CD 26 FF 00
```

14.2.7 配置自组网

配置自组网命令如表 14.77 所示。

表 14.77　配置自组网

3 字节（协议标志）	1 字节	1 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	27	R/W	自组网使能	设备类型	AA

当自组网使能字节为 0 时，模块的自组网功能关闭；

当自组网使能字节为 1 时，模块进入普通自组网；

当自组网使能字节为 2 时，模块进入快速自组网模式，用有自组网功能，而且在没有加入网络的时候，主动去加入附近的网络，不需要通过指定引脚控制；

模块的自组网功能默认是关闭。

设备类型参见表 14.66 中的 DevType，其中协调器作为主机模块，路由器、终端则作为从机模块。

配置自组网的应答报文如表 14.78 所示。

表 14.78　配置自组网应答报文

3 字节（协议标志）	1 字节	1 字节	1 字节	1 字节
AB BC CD	27	自组网使能	设备类型	响应状态

响应状态详见表 14.63。

命令示例：读取自组网使能情况和设备类型

```
CMD:    AB BC CD 27 00 00 00 AA
RSP:    AB BC CD 27 00 00 00
```

自组网功能，协调器作为主机模块，路由器，终端设备作为从机模块，在主机到终端信号不可达时，可加入路由器进行信号传递。如图 14.1 所示。

模块在自组网模式下，主机模块自动选择周围没有被使用的 PAN ID 和通道号形成一个独立的网络，并能自动分配一个唯一的网络地址给从机模块，使能自组网功能后就不需要进行任何的配置操作，从机模块在加入网络后就能跟主机进行通讯。

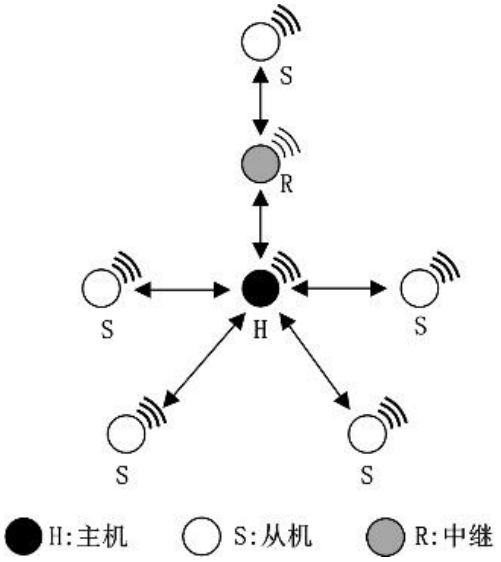

图 14.1　自组网拓扑结构

主机模块有两个工作流程，分别通过 JOIN 管脚和 DETECT 管脚控制。

当 JOIN 管脚为低电平时，主机模块工作在组网模式，此时主机模块允许从机模块加入网络，当 JOIN 管脚变为高电平时，主机模块进入正常工作流程，此时从机模块不能再加入网络。

当模块检测到 DETECT 管脚有大于 3s 的低电平时，主机模块工作在重获取网络参数模式，此时主机模块会重新随机生成新的 PAN ID（0x0000~0xFFFF）和通道号（11~26），并检测生成的 PAN ID 和通道号是否已被其他网络使用，如果已经有网络在使用，则重新生成，主机模块在重新生成 PAN ID 和通道号后，需要把该主机下的所有从机都需要执行入网操作。

模块：JOIN 管脚使用 IO1 管脚，DETECT 管脚使用 IO2 管脚。

模块有 STATE 管脚，可接 LED 指示灯，用于指示当前模块的组网状态，如表 3.3 所示。

主机模块组网模式的工作流程为：

（1）把模块使能自组网功能，并配置为主机模块；当主机模块检测到 DETECT 管脚低电平时间大于 3s 时，主机模块进入重新分配网络参数模式，其他情况则进入正常工作模式（重新分配网络参数模式分配成功也会进入正常工作模式）；

（2）正常工作模式包含组网工作任务以及主机的正常工作任务；

（3）主机模块如果接收到从机模块的入网请求，把当前使用的 PAN ID、通道号、给该从机分配的唯一的本地网络地址，和主机的网络地址发送给从机模块；

（4）主机模块在组网状态期间如果 JOIN 管脚变为高电平，主机模块结束接受从机的入网请求，退出组网状态，主机模块使用随机获取到的 PAN ID 和通道号进入正常的工作状

态；

主机模块组网工作流程如图 14.2 所示。

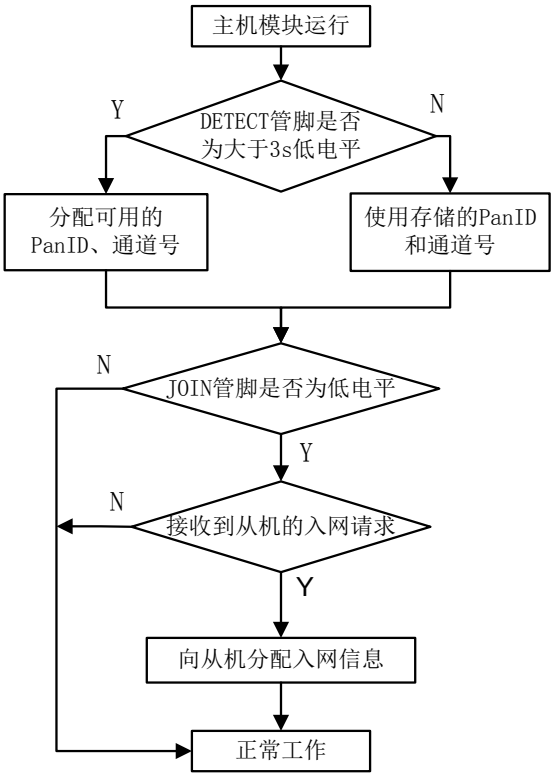

图 14.2　主机模块组网工作流程

主机模块重获取网络参数的工作流程为：

（1）主机模块检测到 DETECT 管脚有大于 3s 的低电平时，主机模块进入重获取网络参数状态；

（2）主机模块随机生成一个 PAN ID（0x0000~0xFFFF）和通道号（11~26），然后进行搜索网络，判断是否有相同的 PAN ID 和通道号正在使用，若有则重复步骤 2，如果没有则认为该 PAN ID 和通道号空闲，可以使用，把生成的 PAN ID 和通道号进行存储，主机模块本地网络地址为 0x0000，用于主机模块在正常工作状态时使用；

（3）主机模块在重获取网络参数后，会把存储的所有从机信息删除。

主机模块重获取网络参数工作流程如图 14.3 所示。

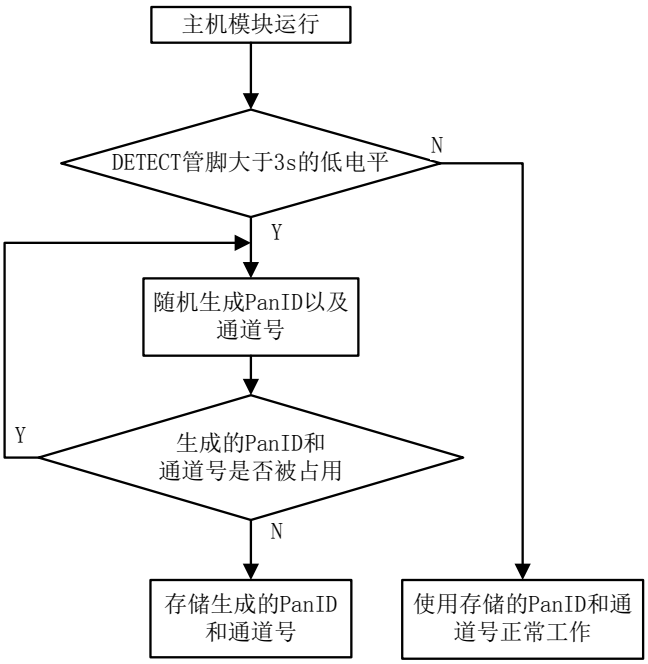

图 14.3　主机模块重获取网络参数工作流程

从机模块的工作流程：

从机模块有两个工作模式，一个是入网申请，一个是退网申请，通过 JOIN 管脚的电平状态决定工作模式。当 JOIN 管脚为低电平，低电平持续时间在 3s 以下（短低电平）时，从机模块工作在入网申请状态；当JOIN管脚为低电平，低电平持续时间在3s以上（长低电平）时，从机模块工作在退网申请状态；如果 JOIN 管脚为高电平，从机模块使用存储的 PAN ID 和通道号进入正常工作状态。

入网申请：

（1）把模块使能自组网功能，并配置为从机模块；当从机模块检测到 JOIN 管脚为低电平，且低电平持续时间小于 3s（短低电平）时从机模块进入入网申请状态；如果 JOIN 管脚为高电平，从机模块使用存储的 PAN ID 和通道号进入正常工作状态；

（2）从机模块进入入网申请状态后，会进行扫描附近存在的允许加入的网络，获取对应的 PAN ID 以及通道号并向主机模块发起入网请求（每 2 秒发送一次）；

（3）从机模块如果入网成功，则结束入网请求，否则再向主机模块发起入网申请请求，6 秒后仍无法入网，则重复步骤 2；

（4）从机模块入网成功后，从机模块把获取到的 PAN ID、通道号和从机网络地址存储，并进入正常的工作状态，从机的目标地址配置为主机的网络地址 0x0000；

从机模块入网流程如图 14.4 所示。

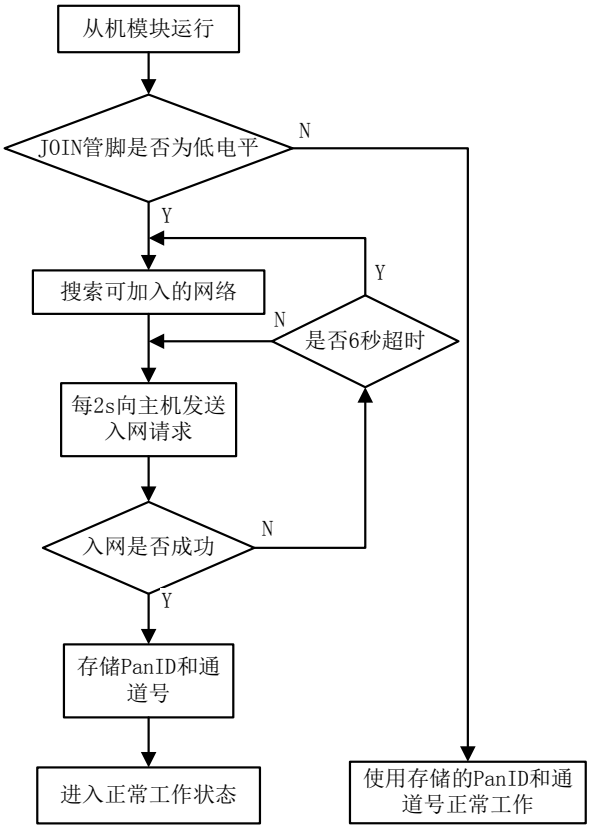

图 14.4　从机模块入网流程

退网申请：

（1）当从机模块检测到 JOIN 管脚为低电平，且低电平持续时间大于 3s（长低电平）时从机模块进入退网申请状态；如果 JOIN 管脚为高电平，从机模块使用存储的 PAN ID 和通道号进入正常工作状态；

（2）从机模块向主机模块发起退网申请；

（3）主机模块在接收到从机模块的退网申请时，把从机模块的信息从主机上删除，并向从机模块回应退网成功应答；

（4）从机模块接着在 100ms 等待主机的应答，等待超时或者成功接收到主机的退网应答，从机模块均会把存储的入网参数删除，并使用默认的参数运行。

从机模块退网流程如图 14.5 所示。

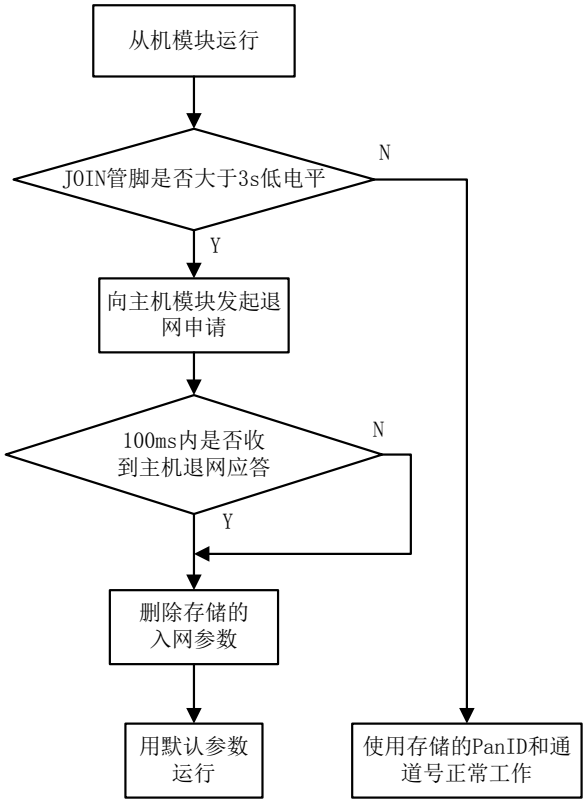

图 14.5　从机模块退网流程

14.2.8 主机允许从机加入网络

ZM32 系列 ZigBee 模块的协调器作为主机模块，路由器、终端则作为从机模块。在禁能自组网情况下，主机允许从机加入网络；但是开启了自组网功能后，必须通过下发命令或者 IO 口开启允许加入。主机模块使用命令的方式使能主机允许从机加入网络，命令如表 14.79 所示。

表 14.79　主机允许从机加入网络

3 字节（协议标志）	1 字节	2 字节	1 字节（帧尾）
AB BC CD	E6	允许加入网络开启的窗口时间（s）	AA

当给主机发送了允许加入网络命令后，主机开始接受从机的入网请求，到达这个窗口时间后，主机不再接受从机的入网请求，窗口时间结束后，主机进入正常的工作状态。

当时间设置为 0 时，主机禁止从机加入网络。

当时间设置为 0xFFFF 时，主机一直允许从机加入网络。

主机允许从机加入网络返回应答如表 14.80 所示。

表 14.80　主机允许从机加入网络应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节
AB BC CD	E6	允许加入网络开启的窗口时间（s）	响应状态

响应状态详见表 14.63。

命令示例：主机允许从机加入网络

```
CMD：    AB BC CD E6 FF FF AA   /* 一直允许加入 */
RSP：    AB BC CD E6 FF FF 00
```

14.2.9 查询主从机状态

ZM32 系列 ZigBee 模块，协调器作为主机模块，路由器、终端则作为从机模块。通过该命令可查询主机或从机当前的状态，命令如表 14.81 所示。

表 14.81 查询主从机状态

3 字节（协议标志）	1 字节	1 字节（帧尾）
AB BC CD	E8	AA

查询主机或从机当前的状态的应答如表 14.82 所示。

表 14.82 主机允许从机加入网络命令应答报文

3 字节（协议标志）	1 字节	1 字节	1 字节
AB BC CD	E8	状态	响应状态

响应状态详见表 14.63。

当模块配置为主机时，返回的状态值如表 14.83 所示。

表 14.83 主机返回的状态值

1 字节	说明
00	主机空闲，不允许从机加入网络
01	主机允许从机加入网络
02	主机已退出网络

当模块配置为从机时，返回的状态值如表 14.84 所示。

表 14.84 从机返回的状态值

1 字节	说明
00	从机正在加入网络
01	从机已加入网络
02	从机已退出网络

命令示例：查询主从机状态

```
CMD：AB BC CD E8 AA
RSP：  AB BC CD E8 00 00 /* 主机空闲 */
RSP：  AB BC CD E8 02 00 /* 从机已退出网络 */
```

14.2.10 备份数据

备份数据命令如表 14.85 所示。

表 14.85 备份数据

3 字节（协议标志）	1 字节	2 字节	1 字节（帧尾）
AB BC CD	FA	协议类型	AA

该命令备份本地设备数据，如果应答报文响应状态是正常，那么接下来将会进入备份过程。

协议类型：0x0004

备份设备应答报文如表 14.86 所示。

表 14.86 备份数据应答报文

3 字节（协议标志）	1 字节	2 字节	4 字节	1 字节
AB BC CD	FA	协议类型	备份文件大小	响应状态

响应状态详见表 14.63。

命令示例：备份本地设备数据

```
CMD:  AB BC CD FA 00 04 AA
RSP:  AB BC CD FA 00 04 00 00 30 80 00 // 接下来进入备份过程
```

14.2.11 恢复数据

恢复数据，其命令如表 14.87 所示。

表 14.87 恢复数据

3 字节（协议标志）	1 字节	2 字节	1 字节（帧尾）
AB BC CD	FB	协议类型	AA

该命令恢复本地设备数据，如果应答报文响应状态是正常，那么接下来将会进入恢复过程。

协议类型：0x0004

恢复数据应答报文如表 14.88 所示。

表 14.88 恢复数据应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节
AB BC CD	FB	协议类型	响应状态

响应状态详见表 14.63。

命令示例：恢复本地设备数据

```
CMD:  AB BC CD FB 00 04 AA
RSP:  AB BC CD FB 00 04 00 // 接下来进入恢复过程
```

14.2.12 基于 MAC 地址通讯命令集

1. 配置通道

配置通道的命令如表 14.89 所示。

表 14.89 配置通道

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节	2 字节	1 字节（帧尾）
AB BC CD	40	MAC 地址	R/W	通道	保留	AA

R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令；当为读参数命令时，通道字段忽略。

通道最小值是 CH11（0x0B），最大值是 CH26（0x1A），其他值无效。

配置通道应答报文如表 14.90 所示。

表 14.90 配置通道应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	2 字节	1 字节
AB BC CD	40	MAC 地址	通道	保留	响应状态

响应状态详见表 14.63。

命令示例：配置通道

```
CMD：AB BC CD 40 12 34 56 78 90 AB CD EF 01 12 00 00 AA
RSP： AB BC CD 40 12 34 56 78 90 AB CD EF 12 00 00 00
```

2. 配置 PAN ID

配置 PAN ID 的命令如表 14.91 所示。

表 14.91 配置 PAN ID

3 字节（协议标志）	1 字节	8 字节	1 字节	2 字节	2 字节	1 字节（帧尾）
AB BC CD	41	MAC 地址	R/W	PAN ID	保留	AA

R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令 PAN ID 字段忽略。

PAN ID：填入 0xFFFF 会退网。

注意：该命令复位后有效。

配置 PAN ID 应答报文如表 14.92 所示。

表 14.92 配置 PAN ID 应答报文

3 字节（协议标志）	1 字节	8 字节	2 字节	2 字节	1 字节
AB BC CD	41	MAC 地址	PAN ID	保留	响应状态

响应状态详见表 14.63。

命令示例：配置 PAN ID

```
CMD：AB BC CD 41 12 34 56 78 90 AB CD EF 01 12 34 00 00 AA
RSP： AB BC CD 41 12 34 56 78 90 AB CD EF 12 34 00 00 00
```

3. 配置分组

可以给设备设置不同的分组号，让设备加入不同的分组，当网络内有其他设备使用组播

发送数据，那么所在目标组号的设备都可以接收到数据。

例如：设备 A 使用组播模式发送数据 0xAA，目标组号为 0x0001；那么，分组号为 0x0001 的设备，将会接收数据 0xAA。

注意：当前设备**最多可配置 5 个分组号**，且建议分组号是 **0x0001~0xFFF7**。

配置分组的命令如表 14.93 所示。

表 14.93 配置分组

3 字节(协议标志)	1 字节	8 字节	1 字节	2 字节	1 字节（帧尾）
AB BC CD	42	MAC 地址	控制选项 R/A/C/D	分组号 0x0001~0xFFF7	AA

控制选项 R/C/A/D：

0x00：表示读分组，忽略分组号字段；

0x01：表示添加一个分组号(Add)，即设备加入一个分组；

0x02：表示清空分组(Clear) ，即设备退出所有分组；

0x03：表示删除一个分组号(Delete)，即设备退出一个分组。

配置分组应答报文如表 14.94 所示。

表 14.94 配置分组应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节	2 字节	...	2 字节	1 字节
AB BC CD	42	MAC 地址	控制选项 R/A/C/D	数量	第一个 分组号	...	第 N 个 分组号	响应状态

响应状态详见表 14.63。

命令示例：配置分组

```
CMD：AB BC CD 42 12 34 56 78 90 AB CD EF 00 00 00 AA
RSP： AB BC CD 42 12 34 56 78 90 AB CD EF 00 02 00 01 00 02 00
```

4. 配置目标组号

当使用组播模式传输数据的情况下，目标组号生效，数据将会组播给符合目标组号的设备，即自身组号匹配目标组号的设备均会接收该数据。

例如：设备 A 使用组播模式发送数据 0xAA，目标组号为 0x0001；那么，分组号为 0x0001 的设备，将会接收数据 0xAA。

配置目标组号的命令如表 14.95 所示。

表 14.95 配置目标组号

3 字节（协议标志）	1 字节	8 字节	1 字节	2 字节	1 字节（帧尾）
AB BC CD	43	MAC 地址	R/W	目标组号	AA

R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，忽略目标组号。

配置目标组号应答报文如表 14.96 所示。

表 14.96 配置目标组号应答报文

3 字节（协议标志）	1 字节	8 字节	2 字节	1 字节
AB BC CD	43	MAC 地址	目标组号	响应状态

响应状态详见表 14.63。

命令示例：配置目标组号

CMD：AB BC CD 43 12 34 56 78 90 AB CD EF 01 00 01 AA

RSP： AB BC CD 43 12 34 56 78 90 AB CD EF 00 01 00

5. 搜索网络内的设备

模块接收到本命令后，会发出广播搜索包，相同 PAN ID 与相同通道的模块收到该广播命令后均会应答，应答内容会将自己的相关基本信息返回到搜索发起目标节点，其搜索命令如表 14.97 所示。

表 14.97 搜索网络内的设备

3 字节（协议标志）	1 字节	1 字节（帧尾）
AB BC CD	54	AA

搜索的应答报文如表 14.98 所示，可以根据应答报文返回的内容，查看在本网段内所有该系列模块的基本设备信息，然后依次判断网段内模块的工作状态是否正常。

表 14.98 搜索应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节
AB BC CD	54	协议类型	通道号	速率
2 字节	2 字节	8 字节	1 字节	
PAN ID	本机网络地址	本机 MAC 地址	运行状态	

运行状态：

0xF1：所读配置参数不可靠，需要复位

0xAA：正常配置参数

协议类型：0x0004

命令示例：搜索

CMD：AB BC CD 54 AA

RSP： AB BC CD 54 00 04 0B 00 10 01 20 02 12 34 56 78 90 AB CD EF AA

6. 获取远程配置信息

为了获取其它节点的信息，可以通过向本机模块发送此命令，如表 14.99 所示。

表 14.99 获取远程配置

3 字节（协议标志）	1 字节	8 字节	1 字节（帧尾）
AB BC CD	55	MAC 地址	AA

远程的节点返回包含自己所有信息的数据包，应答报文如表 14.100 所示。

表 14.100 获取远程配置应答报文

3 字节（协议标志）	1 字节	68 字节	1 字节	2 字节	2 字节
AB BC CD	55	DEV_INFO 结构信息	运行状态	协议类型	固件版本

运行状态：

0xF1：所读配置参数不可靠，需要复位

0xAA：正常配置参数

固件版本：采用 8421-BCD 编码。MSB 的 8 位分成 2 个 4 位，用来编码主版本号；LSB 的 8 位分成 2 个 4 位，用来编码副版本号；例如："02 10" 代表固件版本 "V2.10"。

协议类型：0x0004

命令示例：获取远程配置信息

CMD：AB BC CD 55 12 34 56 78 90 AB CD EF AA

RSP： AB BC CD 55 5A 4C 47 20 44 65 76 69 63 65 00 00 00 00 00 00 38 38 38 38 38 00 00 00 00 00 00 00 00 00 00 00 00 00 0B 10 01 20 02 12 34 56 78 90 AB CD EF 20 01 00 00 00 00 00 00 00 00 00 03 03 0A 07 08 01 00 00 04 00 00 AA 00 04 01 00

7. 修改配置

修改配置的命令如表 14.101 所示。

注：设备的 MAC 地址只能通过该命令修改。

表 14.101 修改配置

3 字节（协议标志）	1 字节	8 字节	68 字节	1 字节（帧尾）
AB BC CD	56	MAC 地址	DEV_INFO 结构信息	AA

修改本机配置时，只需在命令中填本地 MAC 地址即可。修改的应答报文如表 14.102 所示。

表 14.102 修改配置应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节
AB BC CD	56	MAC 地址	响应状态

响应状态详见表 14.63。

命令示例：修改配置

CMD： AB BC CD 56 12 34 56 78 90 AB CD EF 5A 4C 47 20 44 65 76 69 63 65 00 00 00 00 00 00 38 38 38 38 38 00 00 00 00 00 00 00 00 00 00 00 00 00 19 10 01 20 01 00 5B 28 61 00 15 8D 00 20 02 00 00 00 00 00 00 00 00 00 03 05 0A 07 08 01 00 00 04 00 00 AA

RSP： AB BC CD 56 12 34 56 78 90 AB CD EF 00

8. 复位

复位的命令如表 14.103 所示。

表 14.103 复位

3 字节（协议标志）	1 字节	8 字节	2 字节	1 字节（帧尾）
AB BC CD	59	MAC 地址	协议类型	AA

复位命令无需应答。

协议类型：0x0004

命令示例：复位

CMD： AB BC CD 59 12 34 56 78 90 AB CD EF 00 04 AA

9. 恢复出厂设置

恢复出厂设置的命令如表 14.104 所示。

表 14.104 恢复出厂设置

3 字节（协议标志）	1 字节	8 字节	2 字节	1 字节（帧尾）
AB BC CD	5A	MAC 地址	协议类型	AA

协议类型：0x0004

恢复出厂设置应答报文如表 14.105 所示。

表 14.105 恢复出厂设置应答报文

3 字节（协议标志）	1 字节	8 字节	2 字节	1 字节
AB BC CD	5A	MAC 地址	协议类型	响应状态

响应状态详见表 14.63。

命令示例：恢复出厂设置

CMD： AB BC CD 5A 12 34 56 78 90 AB CD EF 00 04 AA

RSP： AB BC CD 5A 12 34 56 78 90 AB CD EF 00 04 00

10. 模块密码使能

模块支持配置设定的密码是否有效的功能，如果模块使能了密码，在修改配置时需要先执行模块登录命令后才能进行操作，如果模块没有使能密码，不需要执行模块登录命令，可直接修改配置。如果忘记了密码，只能通过执行恢复出厂设置命令，模块恢复出厂设置后，密码不使能。模块默认的密码为：88888。

模块密码使能命令如表 14.106 所示。

表 14.106 模块密码使能

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	5E	MAC 地址	R/W	密码使能	AA

密码使能字节为 0，表示不使能密码，为 1 表示使能密码。该命令支持读取参数和设置参数，R/W 字节为 0，表示读参数，为 1 表示写参数。如果模块已经使能了密码，执行模块密码使能写命令时也需要先执行模块登录命令。

模块密码使能应答报文如表 14.107 所示。

表 14.107 模块密码使能应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节
AB BC CD	5E	MAC 地址	密码使能	响应状态

响应状态详见表 14.63。

命令示例：设置模块密码使能

CMD： AB BC CD 5E 12 34 56 78 90 AB CD EF 01 01 AA

RSP： AB BC CD 5E 12 34 56 78 90 AB CD EF 01 00

11. 模块登录

当模块使能了密码，在修改模块配置时需要先执行模块登录命令后才能进行操作。

模块登录的命令如表 14.108 所示。

表 14.108 模块登录

3 字节（协议标志）	1 字节	8 字节	1 字节	16 字节	1 字节（帧尾）
AB BC CD	5F	MAC 地址	R/W	密码	AA

该命令支持读取和设置参数，R/W 字节为 0，表示读参数，为 1 表示写参数。读参数时密码字段不起作用，读参数时响应状态如果返回 0，表示模块已经登录，如果响应状态返回非 0，表示模块没有登录；如果需要执行修改配置、模块密码使能等操作时，要先执行模块登录写命令，使用正确的密码登录模块。16 字节的密码只能为 ASCII 编码，密码最长是 15 字节，以 0 结束。

模块登录应答报文如表 14.109 所示。

表 14.109 模块登录应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节
AB BC CD	5F	MAC 地址	响应状态

响应状态详见表 14.63。

命令示例：用“ 88888”密码登录模块。

CMD： AB BC CD 5F 12 34 56 78 90 AB CD EF 01 38 38 38 38 38 00 00 00 00 00 00 00 00 00 00 AA

RSP： AB BC CD 5F 12 34 56 78 90 AB CD EF 00

12. I/O 方向设置

设置 IO 方向的命令如表 14.110 所示。

表 14.110 I/O 方向设置

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	61	MAC 地址	R/W	IO	AA

IO 字节的 bit0~bit3 为 IO1~IO4，bit0 表示 IO1，bit1 表示 IO2，bit2 表示 IO3，bit3 表示 IO4。其相应位为 1，表示 I/O 为输出；其相应位为 0，表示 I/O 为输入，可设置本地 I/O 或远程 I/O。R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令 IO 字节的参数忽略。

I/O 方向设置应答报文如表 14.111 所示。

表 14.111 I/O 方向设置应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节
AB BC CD	61	MAC 地址	IO	响应状态

响应状态详见表 14.63。

命令示例：设置 IO1 为输出，其他 IO 为输入

CMD： AB BC CD 61 12 34 56 78 90 AB CD EF 01 01 AA

RSP： AB BC CD 61 12 34 56 78 90 AB CD EF 01 00

13. IO/AD 采集设置

模块有 4 路 IO 和 4 路 AD，IO/AD 采集设置命令可设定模块 IO 触发上传 IO 和 AD 状态及根据配置的周期时间定时上传 IO 和 AD 状态，设置的命令如表 14.112 所示。

表 14.112 IO/AD 采集设置

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节	2 字节	1 字节	1 字节（帧尾）
AB BC CD	62	MAC 地址	R/W	IO	周期	是否休眠	AA

IO 字节的 bit0~bit3 为 IO1~IO4，bit0 表示 IO1，bit1 表示 IO2，bit2 表示 IO3，bit3 表示 IO4；当这些位为 1 时，表示上升沿触发，为 0 时，表示下降沿触发。bit4~bit7 为 IO1~IO4 的触发禁能，bit4 表示 IO1，bit5 表示 IO2，bit6 表示 IO3，bit7 表示 IO4，当这些位为 1 时，表示将输入触发禁能，不会上报数据，只能通过命令查询输入状态，为 0 时，表示输入触发使能，将会根据输入引脚的上升沿或者下降触发，然后上报数据。

周期的单位为 100ms，最大可设置的值为 65535，即设置的最大周期为 6553500ms。

是否休眠字节指示模块是否处于休眠状态，该字节为 1 表示模块处于休眠状态，IO 根据配置的状态发生变化时唤醒模块，并向目标节点地址发送 IO/AD 采集帧，如果周期大于 0，模块除了可以 IO 唤醒外，还会根据周期定时定时唤醒，然后向目标节点地址发送 IO/AD 采集帧，当发送完 IO/AD 采集帧后，模块进入休眠状态，该字节为 0 表示模块不休眠。

模块的工作模式分为以下四种情况：

在模块设置休眠的情况下分两种情况：

- 周期大于 0，模块按照设定周期定时唤醒并上传 IO 和 AD 数据或根据 IO 触发状态 IO 唤醒并上传 IO 和 AD 数据，数据上传完毕模块进入定时休眠；
- 周期等于 0，模块只能根据 IO 触发状态 IO 唤醒并上传 IO 和 AD 数据，然后模块进入休眠。

在模块设置不休眠的情况下分两种情况：

- 周期大于 0，模块根据设定的周期定时上传 IO 和 AD 数据，并且串口透明转发数据；
- 周期等于 0，模块不定时上传 IO 和 AD 数据，只能串口透明转发数据。命令中 R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令；当为读参数命令时，该命令 IO、周期、是否休眠等参数忽略。

设置该命令后模块处于休眠状态时，通过把 WAKE 引脚拉低，唤醒模块，方便对模块进行配置或透传数据，配置完成后，把 WAKE 引脚拉高或悬空，模块根据配置的参数重新

进入休眠状态。

只有把 IO 通过 I/O 方向设置命令设置为输入后，才能根据设定的边沿状态触发模块唤醒。IO/AD 采集设置应答报文如表 14.113 所示。

表 14.113 IO/AD 采集设置应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	2 字节	1 字节	1 字节
AB BC CD	62	MAC 地址	IO	周期	是否休眠	响应状态

响应状态详见表 14.63。

模块 IO 触发或定时发送的 IO/AD 采集帧格式如表 14.114 所示。

表 14.114 IO/AD 采集帧格式

3 字节（协议标志）	1 字节	8 字节	1 字节	2 字节	2 字节	2 字节	2 字节
AB BC CD	62	MAC 地址	IO	AD0	AD1	AD2	AD3

IO 字节的 bit0~bit3 为 IO1~IO4，bit0 表示 IO1，bit1 表示 IO2，bit2 表示 IO3，bit3 表示 IO4。该字节返回模块 IO 当前的电平值，1 为高电平，0 为低电平。

AD0~AD3 表示返回模块 4 路的 AD 转换值，返回为 10 位的 AD 转换值，需要自行转换为电压值，模块 ADC 的参考电压为 2.5V。

命令示例：配置 0x2001 地址的模块 IO1 为下降沿触发，IO2 为上升沿触发，IO3 为下降沿触发，IO4 为上升沿触发，模块定期上传 IO/AD 数据，周期为 5s，模块需要休眠。

```
CMD：  AB BC CD 62 12 34 56 78 90 AB CD EF 01 0A 01 F4 01 AA
RSP：  AB BC CD 62 12 34 56 78 90 AB CD EF 0A 01 F4 01 00
```

当模块发生 IO 触发或周期时间到时，往目标地址上传采集帧：

```
UPLOAD：  AB BC CD 62 12 34 56 78 90 AB CD EF 0A 02 00 02 00 02 00 02 00
```

14. I/O 控制输出

I/O 控制输出命令如表 14.115 所示。

表 14.115 I/O 控制输出

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	63	MAC 地址	R/W	IO	AA

IO 字节的 bit0~bit3 为 IO1~IO4，其相应位为 1，表示 I/O 为输出高电平；其相应位为 0，表示 I/O 为输出低电平，在调用该命令前需要先调用 I/O 方向设置命令把相应的 IO 设置为输出。R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令 IO 参数忽略。I/O 控制输出应答报文如表 14.116 所示。

表 14.116 I/O 控制输出应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节
AB BC CD	63	MAC 地址	IO	响应状态

响应状态详见表 14.63。

命令示例：I/O 控制输出

```
CMD：AB BC CD 61 12 34 56 78 90 AB CD EF 01 02 AA    /*  IO2 设置为输出  */
RSP：  AB BC CD 61 12 34 56 78 90 AB CD EF 02 00
CMD：AB BC CD 63 12 34 56 78 90 AB CD EF 01 02 AA  /*  IO2 输出高电平  */
RSP：  AB BC CD 63 12 34 56 78 90 AB CD EF 02 00
```

15. PWM 控制输出

模块有 4 路的 PWM 输出，使用 PWM 输出配置命令可使能每路 PWM 的输出，设置的命令如表 14.117 所示。

表 14.117　PWM 控制输出命令

3 字节（协议标志）	1 字节	8 字节	1 字节	4 字节	1 字节	4 字节
AB BC CD	64	MAC 地址	R/W	PWM1 频率	PWM1 占空比	PWM2 频率
1 字节	4 字节	1 字节	4 字节	1 字节	1 字节（帧尾）	
PWM2 占空比	PWM3 频率	PWM3 占空比	PWM4 频率	PWM4 占空比	AA	

四路 PWM 的通道号为 1~4；PWM 频率的单位为 Hz，通道 1、2 必须是同频率，可不同占空比，频率范围可设定从 586Hz~384000Hz，通道 3、4 必须是同频率，可不同占空比，频率范围可设定从 586Hz ~384000Hz；占空比的值可设定从 1~99，表示占空比的百分比。当每路的 PWM 信号的频率为 0 时，表示不输出 PWM 信号。R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令的频率、占空比等参数忽略。

PWM 控制输出应答报文如表 14.118 所示。

表 14.118　PWM 控制输出应答报文

3 字节（协议标志）	1 字节	8 字节	4 字节	1 字节	4 字节
AB BC CD	64	MAC 地址	PWM1 频率	PWM1 占空比	PWM2 频率
1 字节	4 字节	1 字节	4 字节	1 字节	1 字节
PWM2 占空比	PWM3 频率	PWM3 占空比	PWM4 频率	PWM4 占空比	响应状态

响应状态详见表 14.63。

命令示例：配置 PWM 的输出，PWM1 周期为 1000Hz，占空比是 20%，PWM2 周期为 1000Hz，占空比为 50%，PWM3 周期为 3000Hz，占空比为 60%，PWM4 周期为 3000Hz，占空比为 80%。

```
CMD：  AB BC CD 64 12 34 56 78 90 AB CD EF 01 00 00 03 E8 14 00 00 03 E8 32 00 00 0B B8 3C 00 00 0B B8 50 AA
RSP：  AB BC CD 64 12 34 56 78 90 AB CD EF 00 00 03 E8 14 00 00 03 E8 32 00 00 0B B8 3C 00 00 0B B8 50 00
```

16. 设置目标网络地址

设置数据发送的目标网络地址，其命令如表 14.119 所示。

表 14.119 设置目标网络地址

3 字节（协议标志）	1 字节	8 字节	2 字节	1 字节（帧尾）
AB BC CD	69	MAC 地址	目标网络地址	AA

设置的回应报文如表 14.120 所示。

表 14.120 目标网络地址设置应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节
AB BC CD	69	MAC 地址	响应状态

目标网络地址：

0xFFFF 代表广播给所有设备；

0xFFFD 代表广播给所有非睡眠设备；

0xFFFC 代表广播给协调器和路由设备；

0xFFFB 代表使用目标组号，发送组播。

响应状态详见表 14.63。

命令示例：设置目标网络地址

```
CMD：AB BC CD 69 12 34 56 78 90 AB CD EF 20 01 AA
RSP： AB BC CD 69 12 34 56 78 90 AB CD EF 00
```

17. 读取设备类型

读取对应 MAC 地址的设备类型，如 MAC 地址为本地设备的 MAC 地址，则读取本机的设备类型，其命令如表 14.121 所示。

表 14.121 读取设备类型

3 字节（协议标志）	1 字节	8 字节	1 字节（帧尾）
AB BC CD	6A	MAC 地址	AA

读取的应答报文如表 14.122 所示。

表 14.122 读取设备类型的应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节
AB BC CD	6A	MAC 地址	设备类型

设备类型参见表 14.66 中的 DevType。

命令示例：读取设备类型

```
CMD：AB BC CD 6A 12 34 56 78 90 AB CD EF AA
RSP： AB BC CD 6A 12 34 56 78 90 AB CD EF 01
```

18. 查询子终端节点的 MAC 地址(只有路由及协调器有效)

ZM32 系列一个协调器或者一个路由器最多可连接 **50** 个终端子节点。查询路由、协调

器的拥有的所有子终端节点的 MAC 地址命令如表 14.123 所示。

表 14.123　查询子终端节点 MAC 地址

3 字节（协议标志）	1 字节	8 字节	1 字节（帧尾）
AB BC CD	6B	MAC 地址	AA

查询子终端节点数量是有效的节点数量，应答报文如表 14.124 所示。

表 14.124　查询子终端节点 MAC 地址应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	2 字节	…	2 字节
AB BC CD	6B	MAC 地址	子终端节点数量 N 0x00~0xFF	子终端节点 MAC 地址	…	第 N 个子终端节点 MAC 地址

命令示例：获取 MAC 地址为 12:34:56:78:90:AB:CD:EF 拥有的所有子终端节点

CMD：　AB BC CD 6B 12 34 56 78 90 AB CD EF AA

RSP：　AB BC CD 6B 12 34 56 78 90 AB CD EF 01 11 22 33 44 55 66 77 88

19. 查询父节点 MAC 地址

查询父节点 MAC 地址的命令如表 14.125 所示。

表 14.125　查询父节点 MAC 地址

3 字节（协议标志）	1 字节	8 字节	1 字节（帧尾）
AB BC CD	6C	MAC 地址	AA

查询父节点 MAC 地址，应答报文如表 14.126 所示。

表 14.126　查询父节点 MAC 地址的应答报文

3 字节（协议标志）	1 字节	8 字节	8 字节
AB BC CD	6C	MAC 地址	父节点的 MAC 地址

命令示例：查询父节点 MAC 地址

CMD：　AB BC CD 6C 12 34 56 78 90 AB CD EF AA

RSP：　AB BC CD 6C 12 34 56 78 90 AB CD EF 11 22 33 44 55 66 77 88

20. 查询网络地址

查询 MAC 地址对应的网络地址的命令如表 14.127 所示。

表 14.127　查询网络地址

3 字节（协议标志）	1 字节	8 字节	1 字节（帧尾）
AB BC CD	6D	MAC 地址	AA

查询网络地址对应的 MAC 地址，应答报文如表 14.128 所示。

表 14.128　查询网络地址的应答报文

3 字节（协议标志）	1 字节	8 字节	2 字节

AB BC CD	6D	MAC 地址	网络地址

命令示例：获取 MAC 地址 12:34:56:78:90:AB:CD:EF 的网络地址

CMD： AB BC CD 6D 12 34 56 78 90 AB CD EF AA

RSP： AB BC CD 6D 12 34 56 78 90 AB CD EF 20 02

21. 设置模块密钥

模块拥有两种类型的密钥：1、为预配置的密钥（加网使用）；2、网络密钥（数据传输使用）。

预配置密钥主机从机均具备，同一个网络内必须相同，该密钥只有在加网、建网前进行配置才有效。

网络密钥只有主机才具备写属性，加网成功后会下发该密钥给从机，该密钥只有建网前进行配置才有效。

注：如果在加网中或加入网络后，修改密钥（预配置密钥或网络密钥）只会在离网之后，重新入网时生效。

默认预配置密钥为：0x7a, 0x68, 0x69, 0x79, 0x75, 0x61, 0x6e, 0x64, 0x69, 0x61, 0x6e, 0x7a, 0x69, 0x2d, 0x68, 0x69

默认网络密钥为：0x68, 0x65, 0x6c, 0x6c, 0x6f, 0x2d, 0x77, 0x77, 0x77, 0x2e, 0x7a, 0x6c, 0x67, 0x2e, 0x63, 0x6e

设置模块密钥命令如表 14.129 所示。

表 14.129 设置模块密钥

3 字节（协议标志）	1 字节	8 字节	1 字节	16 字节	1 字节（帧尾）
AB BC CD	6E	MAC 地址	密钥类型	密码	AA

密钥类型：1 表示预配置密钥，2 表示网络密钥

设置模块密钥应答报文如表 14.130 所示。

表 14.130 设置模块密钥应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节
AB BC CD	6E	MAC 地址	响应状态

响应状态详见表 14.63。

命令示例：设预配置密钥

CMD：AB BC CD 6E 12 34 56 78 90 AB CD EF 01 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 AA

RSP： AB BC CD 6E 12 34 56 78 90 AB CD EF 00

22. 读取模块密钥

模块拥有两种类型的密钥：1、为预配置的密钥（加网使用）；2、网络密钥（数据传输使用）。读取模块密钥命令如表 14.131 所示。

表 14.131 读取模块密钥

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节（帧尾）
AB BC CD	6F	MAC 地址	密钥类型	AA

密钥类型：1 表示预配置密钥，2 表示网络密钥。

读取模块密钥应答报文如表 14.132 所示。

表 14.132　读取模块密钥应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	16 字节
AB BC CD	6F	MAC 地址	密钥类型	密码

响应状态详见表 14.63。

命令示例：读取模块密钥

CMD：　AB BC CD 6F 12 34 56 78 90 AB CD EF 01 AA

RSP：　AB BC CD 6F 12 34 56 78 90 AB CD EF 01 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38

23. 进入升级模式

模块支持串口和空中升级两种方式，在进行固件升级前，需要先进入升级模式，再发送固件升级命令。

模块支持两种方式进入升级模式：

1. 通过无线或串口发送进入升级模式命令；

2. 将 ISP 管脚拉低，之后复位模块，并保持 ISP 管脚处于低电平 100ms 以上。

无线方式进入升级模式的方法为：使用本机模块向目标模块发送进入升级模式命令，目标模块接收到命令后，即进入升级模式。

串口方式进入升级模式的方法为：利用串口向模块发送进入升级模式命令，MAC 地址为本机 MAC 地址，收到命令后，即进入升级模式。

进入升级模式的命令如表 14.133 所示。

表 14.133　进入升级模式

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节（帧尾）
AB BC CD	71	MAC 地址	设备类型	AA

设备类型参见表 14.66 中的 DevType，可通过读取设备类型命令或读取本地配置命令获取，当 MAC 地址为本机模块的地址时，执行的是本机模块的串口升级，当 MAC 地址为其他地址时，通过本机模块对指定地址的模块进行空中升级。

当固件升级失败，模块将一直处于升级模式，按照正常升级流程再升级即可。

进入升级模式的应答报文如表 14.134 所示。

表 14.134　进入升级模式的应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节
AB BC CD	71	MAC 地址	响应状态

响应状态详见表 14.63。

24. 固件升级

模块支持串口和空中升级两种方式。当目标模块进入升级模式后，开始发送固件升级命令，升级模块的固件。发送固件升级的命令如表 14.135 所示。

表 14.135　固件升级

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节（帧尾）
AB BC CD	72	MAC 地址	设备类型	AA

设备类型参见表 14.66 中的 DevType，可通过读取设备类型命令或读取本地配置命令获取，当 MAC 地址为本机模块的地址时执行的是本机模块的串口升级，当网络地址为其他地址时，通过本机模块对指定地址的模块进行空中升级。

模块接收到升级命令后开始使用 XModem 协议进行升级。

通过本机模块对远程模块进行空中升级时，通过串口给本机模块发送升级命令，本机模块把命令转发给目标模块后，目标模块就通过本机模块透传使用 XModem 协议进行升级。

升级结束后模块返回的应答报文如表 14.136 所示。

表 14.136 升级完成应答

3 字节（协议标志）	1 字节	8 字节	1 字节
AB BC CD	72	MAC 地址	升级结果

升级结束后模块返回的应答报文，升级结果的值如表 14.137 所示。

表 14.137 升级结果的值

1 字节	说明
0x00	固件升级成功
0x03	固件校验错误
0x05	固件升级失败
0x0A	固件与芯片型号不符

25. 设置接收模式

当模块接收到透传数据时，会进行根据接收模式的相关设置进行处理，然后发送到通过串口连接的用户设备。设置接收模式如表 14.138 所示。

表 14.138 设置接收模式

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	73	MAC 地址	R/W	接收模式	AA

该命令支持读取和设置参数，R/W 字节为 0 表示读参数，为 1 表示写参数。读参数时，接收模式位域不起作用。

接收模式的位域如表 14.139 所示。

表 14.139 接收模式的位域

Bit 3~7	Bit 0~2 数据包格式
保留	0：数据 1：源网络地址+数据

	2：源 MAC 地址+数据 3：源网络地址+源 MAC 地址+数据 4：接收帧格式

数据包格式：用户可以指定接收到的原始数据，跟一些有用信息打包在一起，然后才发送到串口。其中，当数据源(设备)并没有在"是否添加源 MAC 地址"中设置添加源 MAC 地址，则数据包会打包一个无效的 MAC 地址 FF:FF:FF:FF:FF:FF:FF:FF。

1. 数据：透传接收到的原始数据。

   例如：本地设备收到某个远程设备传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 AA BB CC。

2. 源网络地址+数据：原始数据的前面会加上数据源(设备)的网络地址。

   例如：本地设备收到协调器(0x0000)传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 00 00 AA BB CC。

3. 源 MAC 地址+数据：原始数据的前面会加上数据源(设备)的 MAC 地址。

   例如：本地设备收到设备(11:22:33:44:55:66:77:88)传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 11 22 33 44 55 66 77 88 AA BB CC。

4. 源网络地址+源 MAC 地址+数据：原始数据的前面会加上数据源(设备)的网络地址和 MAC 地址。

   例如：本地设备收到协调器(0x0000/11:22:33:44:55:66:77:88)发过来的数据(0xAA 0xBB 0xCC)，则串口会输出 00 00 11 22 33 44 55 66 77 88 AA BB CC。

5. 接收帧格式：原始的数据会格式化成接收帧。

   例如：本地设备接收到协调器(0x0000/11:22:33:44:55:66:77:88)发过来的数据(0xAA 0xBB 0xCC)，则串口会输出 AD DB BE 90 11 22 33 44 55 66 77 88 00 00 00 03 AA BB CC 6E AA。

接收模式应答报文如表 14.140 所示。

表 14.140 设置接收模式应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节
AB BC CD	73	MAC 地址	接收模式	响应状态

响应状态详见表 14.63。

命令示例：设置接收模式

CMD： AB BC CD 73 12 34 56 78 90 AB CD EF 01 01 AA

RSP： AB BC CD 73 12 34 56 78 90 AB CD EF 01 00

26. 设置目标 MAC 地址

设置数据发送的目标 MAC 地址，其命令如表 14.141 所示。

表 14.141 设置目标 MAC 地址

3 字节（协议标志）	1 字节	8 字节	1 字节	8 字节	1 字节（帧尾）
AB BC CD	74	MAC 地址	R/W	目标 MAC 地址	AA

该命令支持读取和设置参数，R/W 字节为 0，表示读参数，为 1 表示写参数。读参数时，目标 MAC 地址不起作用。当发送模式是单播的时候，会把没有进行任何转发处理的数据，直接转发到该预先配置好的目标 MAC 地址。

设置目标 MAC 地址应答报文如表 14.142 所示。

表 14.142　设置目标 MAC 地址应答报文

3 字节（协议标志）	1 字节	8 字节	8 字节	1 字节
AB BC CD	74	MAC 地址	目标 MAC 地址	响应状态

目标 MAC 地址：

FF:FF:FF:FF:FF:FF:FF:FF 代表广播给所有设备；

FF:FF:FF:FF:FF:FF:FF:FD 代表广播给所有非睡眠设备；

FF:FF:FF:FF:FF:FF:FF:FC 代表广播给协调器和路由设备；

FF:FF:FF:FF:FF:FF:FF:FB 代表使用目标组号，发送组播；

00:00:00:00:00:00:00:00 代表协调器。

响应状态详见表 14.63。

命令示例：将数据转发到该目标 MAC 地址 11:22:33:44:55:66:77:88

CMD： AB BC CD 74 12 34 56 78 90 AB CD EF 01 11 22 33 44 55 66 77 88 AA

RSP： AB BC CD 74 12 34 56 78 90 AB CD EF 11 22 33 44 55 66 77 88 00

27. 设置发送模式

当希望通过串口转发数据到其他远程设备时，或者本地设备产生的数据需要分发时，可以设置发送模式的相关功能，满足用户不同的通讯需求。设置发送模式命令如表 14.143 所示。

表 14.143　设置发送模式

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	75	MAC 地址	R/W	发送模式	AA

该命令支持读取和设置参数，R/W 字节为 0，表示读参数，为 1 表示写参数。读参数时，发送模式不起作用，保留位填 0。

发送模式的位域如表 14.144 所示。

表 14.144　发送模式的位域

Bit 7	Bit 5~6 数据包格式	Bit 4 数据的目标地址选择	Bit 3 是否需要添加源 MAC 地址	Bit 0~2 数据传输方式
保留	0：数据（根据数据的目标地址进行发送） 1：指定网络地址+数据 2：指定 MAC 地址+数	0：目标网络地址(DEV_INFO.DstAddr) 1：目标 MAC 地址(DEV_INFO.DstIEEE)	0：不添加源 MAC 地址 1：添加源 MAC 地址	0：单播模式 1：广播给所有设备 2：广播给所有非睡眠设备 3：广播给协调器和

	据 3：发送帧格式			所有路由器 4：组播模式

数据传输方式：用户需要串口转发的数据，或者 IO/ADC 采集数据，将会传输到指定的一台设备或者一组设备。

1. 单播模式: 数据只会传输给网络地址或者 MAC 地址匹配的设备。
2. 广播给所有设备：数据会传输给网络内所有设备。
3. 广播给非睡眠设备：数据会传输给网络内所有非睡眠设备。
4. 广播给协调器和路由器：数据会传输给网络的协调器和所有路由器。
5. 组播模式：数据会传输给目标分组内的所有设备。

是否需要添加源 MAC 地址：当用户希望远程设备转发到串口的数据包包含有效的 MAC 地址时，则需要添加源 MAC 地址。

数据目标地址选择：用户通过串口转发的数据，或者 IO/ADC 采集数据，需要传输到指定的一台目标设备，用目标地址来指示这台设备。用户可以自行选择，用网络地址或者 MAC 地址来作为目标地址。单播模式下有效。

1. 目标网络地址：数据会发送至设备配置信息中的目标网络地址(DEV_INFO.DstAddr)，参见表 14.66。
2. 目标 MAC 地址：数据会发送至设备配置信息中的目标 MAC 地址(DEV_INFO.DstIEEE)，参见表 14.66。

数据包格式：用户可以指定串口发送的数据包的格式，从而改变数据的发送方式，单播模式下有效。

1. 数据：串口数据包只有普通数据，将会根据预设的方式(数据传输方式/是否添加源 MAC 地址/数据目标地址)进行传输。

   例如：从串口发送数据 AA BB CC，会根据预先配置好的方式(单播/带有源 MAC 地址/目标 MAC 地址)传输。
2. 临时目标网络地址+数据：串口数据包，包含指定设备的网络地址和普通数据。当串口发送有效的数据包时，会临时改变目标网络地址，然后传输到指定设备。

   例如：从串口发送 00 00 AA BB CC，会临时改变目标网络地址为 00 00，然后传输数据 AA BB CC。
3. 临时目标 MAC 地址+数据：串口数据包，包含指定设备的 MAC 地址和普通数据。当串口发送有效的数据包时，会临时改变目标 MAC 地址，然后传输到指定设备。

   例如：从串口发送 11 22 33 44 55 66 77 88 AA BB CC，会临时改变目标 MAC 地址为 11:22:33:44:55:66:77:88，然后传输数据 AA BB CC。
4. 发送帧格式：透传数据需要按照发送帧格式发向串口。当目标网络地址是 0xFFFE 时，目标 MAC 地址将作为透传数据发送的目的地址。

   例如：从串口发送 AD DB BE 10 00 00 00 00 00 00 00 00 00 00 03 AA BB CC 8A AA，会向网络地址 0x0000 传输数据 AA BB CC；或者从串口发送 AD DB BE 10 11 22 33 44 55 66 77 88 FF FE 00 03 AA BB CC EB AA，会向 MAC 地址 11:22:33:44:55:66:77:88 传输数据 AA BB CC。

设置发送模式应答报文如表 14.145 所示。

表 14.145 设置发送模式应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节
AB BC CD	75	MAC 地址	发送模式	响应状态

响应状态详见表 14.63。

命令示例：将数据单播到配置的目标网络地址，不包含源 MAC 地址

CMD：AB BC CD 75 12 34 56 78 90 AB CD EF 01 00 AA

RSP： AB BC CD 75 12 34 56 78 90 AB CD EF 00 00

28. 启用黑名单

在黑名单里的对应通道的网络，终端设备或者路由设备不会去加入。比如：黑名单里记录了一项记录，通道 11 的网络 0x1234，当终端设备入网时检测到通道 11 存在网络 0x1234，里，是不会去加入的。

当前命令用来控制黑名单是否生效，对终端设备和路由设备有效；对协调器使用，响应状态返回不支持。

启用黑名单命令如表 14.146 所示。

表 14.146 启用黑名单

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	77	MAC 地址	R/W	使能	AA

R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令 IO 参数忽略。

当使能字节为 0 时，不启用黑名单功能；为 1 时，模块启用黑名单功能；

模块的黑名单功能默认是不启用的。

如果启用黑名单功能，当设备复位之后，会检查当前所在网络是否存在于黑名单，如果是，就会退出当前网络。

启用黑名单应答报文如表 14.147 所示。

表 14.147 启用黑名单应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节
AB BC CD	77	MAC 地址	使能	响应状态

在修改配置信息之后，没有进行复位，将无法操作命令，并且响应状态返回其他错误。

响应状态详见表 14.63。

命令示例：查询黑名单是否使能

CMD： AB BC CD 77 12 34 56 78 90 AB CD EF 00 00 AA

RSP： AB BC CD 77 12 34 56 78 90 AB CD EF 00 00

29. 配置黑名单

当前命令用来添加、删除、修改黑名单条目，对终端设备和路由设备有效；对协调器使用，响应状态返回不支持。

如果启用黑名单功能，当设备复位之后，会检查当前所在网络是否存在于黑名单，如果是，就会退出当前网络。

最多支持 10 条。

配置黑名单命令如表 14.148 所示。

表 14.148 配置黑名单

3 字节（协议标志）	1 字节	8 字节	1 字节	2 字节	2 字节	1 字节（帧尾）
AB BC CD	78	MAC 地址	控制选项 R/A/C/D	PAN ID	通道掩码	AA

控制选项 R/C/A/D：

0x00：表示读黑名单(Read)，忽略通道掩码和 PAN ID 字段；

0x01：表示新增或者修改原有的一条黑名单项(Add)；

0x02：表示清空黑名单(Clear)，忽略通道掩码和 PAN ID 字段；

0x03：表示删除一条黑名单项(Delete)，忽略通道掩码和 PAN ID 字段；；

PAN ID，表示相应通道下的网络；另外，0xFFFF 代禁止加入某个通道下的全部网络。

通道掩码，有 16bit，Bit0 对应通道 11，Bit15 对应通道 26。当对应 Bit 为 1 时，表示该通道的网络不会加入；

比如通道掩码是 0x0001，PAN ID 是 0x1234，代表通道 11 的网络 0x1234，成为黑名单成员，终端，路由设备不会对该网络发出入网请求。

比如通道掩码是 0x0001，PAN ID 是 0xFFFF，代表不会加入通道 11 的任何网络。

配置黑名单应答报文如表 14.149 所示。

表 14.149 配置黑名单应答报文

3 字节（协议标志）	1 字节	8 字节	1 字节	1 字节
AB BC CD	78	MAC 地址	控制选项 R/A/C/D	数量
2 字节	2 字节	2 字节	2 字节	1 字节
第一条 PAN ID	第一条 通道掩码	第 N 条 PAN ID	第 N 条 通道掩码	响应状态

在修改配置信息之后，没有进行复位，将无法操作命令，并且响应状态返回其他错误。

响应状态详见表 14.63。

命令示例：查询黑名单配置

CMD： AB BC CD 78 12 34 56 78 90 AB CD EF 00 00 00 00 00 AA

RSP： AB BC CD 78 12 34 56 78 90 AB CD EF 00 01 12 34 FF 7F 00

14.2.13 基于网络地址通讯命令集

1. 配置通道

配置通道命令如表 14.150 所示。

表 14.150 配置通道

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节	2 字节	1 字节（帧尾）
AB BC CD	C0	网络地址	R/W	通道	保留	AA

R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，通道参数不起作用。

通道：最小值是 CH11（0x0B），最大值是 CH26（0x1A），其他值无效。

配置通道应答报文如表 14.151 所示。

表 14.151 配置通道应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	2 字节	1 字节
AB BC CD	C0	网络地址	通道	保留	响应状态

响应状态详见表 14.63。

命令示例：配置通道

```
CMD：  AB BC CD C0 20 02 01 12 00 00 AA
RSP：  AB BC CD C0 20 02 12 00 00 00
```

2. 配置 PAN ID

配置 PAN ID 命令如表 14.152 所示。

表 14.152 配置 PAN ID

3 字节（协议标志）	1 字节	2 字节	1 字节	2 字节	2 字节	1 字节（帧尾）
AB BC CD	C1	网络地址	R/W	PAN ID	保留	AA

R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令 IO 参数忽略。

PAN ID：填入 0xFFFF，设备会退网，复位后有效。

配置 PAN ID 应答报文如表 14.153 所示。

表 14.153 配置 PAN ID 应答报文

3 字节（协议标志）	1 字节	2 字节	2 字节	2 字节	1 字节
AB BC CD	C1	网络地址	PAN ID	保留	响应状态

响应状态详见表 14.63。

命令示例：配置 PAN ID

```
CMD：  AB BC CD C1 20 02 01 12 34 00 00 AA
RSP：  AB BC CD C1 20 02 12 34 00 00 00
```

3. 配置分组

可以给设备设置不同的分组号，让设备加入不同的分组，当网络内有其他设备使用组播发送数据，那么所在目标组号的设备都可以接收到数据。

例如：设备 A 使用组播模式发送数据 0xAA，目标组号为 0x0001；那么，分组号为 0x0001 的设备，将会接收数据 0xAA。

注意：当前设备**最多可配置 5 个分组号**，且建议分组号是 **0x0001~0xFFF7**，其他分组号保留待以后扩展使用。

配置分组命令如表 14.154 所示。

表 14.154 配置分组

3 字节(协议标志)	1 字节	2 字节	1 字节	2 字节	1 字节（帧尾）
AB BC CD	C2	网络地址	控制选项 R/A/C/D	分组号 0x0000~0xFFFF	AA

控制选项 R/C/A/D：

0x00：表示读分组，忽略分组号字段；

0x01：表示添加一个分组号(Add)，即设备加入一个分组；

0x02：表示清空分组(Clear) ，即设备退出所有分组；

0x03：表示删除一个分组号(Delete)，即设备退出一个分组。

配置分组的应答报文如表 14.155 所示。

表 14.155 配置分组应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节	2 字节	...	2 字节	1 字节
AB BC CD	C2	网络地址	控制选项 R/A/C/D	数量	第一条 分组号	...	第 N 条 分组号	响应状态

响应状态详见表 14.63。

命令示例：配置分组

CMD：AB BC CD C2 12 34 00 00 00 AA

RSP： AB BC CD C2 12 34 00 02 00 01 00 02 00

4. 配置目标组号

当使用组播模式传输数据的情况下，目标组号生效，数据将会组播给符合目标组号的设备，即自身组号匹配目标组号的设备均会接收该数据。

例如：设备 A 使用组播模式发送数据 0xAA，目标组号为 0x0001；那么，分组号为 0x0001 的设备，将会接收数据 0xAA。

配置目标组号命令如表 14.156 所示。

表 14.156 配置目标组号

3 字节（协议标志）	1 字节	2 字节	1 字节	2 字节	1 字节（帧尾）
AB BC CD	C3	网络地址	R/W	目标组号	AA

R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，忽略目标组号。

配置目标组号的回应报文如表 14.157 所示。

表 14.157　配置目标组号应答报文

3 字节（协议标志）	1 字节	2 字节	2 字节	1 字节
AB BC CD	C3	网络地址	目标组号	响应状态

响应状态详见表 14.63。

命令示例：配置目标组号

CMD：AB BC CD C3 12 34 01 00 01 AA

RSP：　AB BC CD C3 12 34 00 01 00

5.　搜索网络内的设备

模块接收到本命令后，会发出广播搜索包，相同 PAN ID 与相同通道的模块收到该广播命令后均会应答，应答内容会将自己的相关基本信息返回到搜索发起目标节点，其搜索命令如表 14.158 所示。

表 14.158　搜索网络内的设备

3 字节（协议标志）	1 字节	1 字节（帧尾）
AB BC CD	D4	AA

搜索的应答报文如表 14.159 所示，可以根据应答报文返回的内容，查看在本网段内所有该系列模块的基本设备信息，然后依次判断网段内模块的工作状态是否正常。

表 14.159　搜索应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节	2 字节	2 字节	1 字节
AB BC CD	D4	协议类型	通道号	速率	PAN ID	本机网络地址	运行状态

运行状态：

0xF1：　所读配置参数不可靠，需要复位。

0xAA：正常配置参数。

协议类型：0x0004

命令示例：搜索

CMD：AB BC CD D4 AA

RSP：　AB BC CD D4 00 04 0B 00 10 01 20 02 AA

6.　获取远程配置信息

为了获取其它节点的信息，可以通过向本机模块发送此命令，如表 14.160 所示。

表 14.160　获取远程配置

3 字节（协议标志）	1 字节	2 字节	1 字节（帧尾）
AB BC CD	D5	目标网络地址	AA

远程的节点返回包含自己所有信息的数据包，应答报文如表 14.161 所示。

表 14.161　获取远程配置应答报文

3 字节（协议标志）	1 字节	68 字节	1 字节	2 字节	2 字节
AB BC CD	D5	DEV_INFO 结构信息	运行状态	协议类型	固件版本

运行状态：

0xF1：所读配置参数不可靠，需要复位

0xAA：正常配置参数

协议类型：0x0004

固件版本：采用 8421-BCD 编码。MSB 的 8 位分成 2 个 4 位，用来编码主版本号；LSB 的 8 位分成 2 个 4 位，用来编码副版本号；例如："02 10" 代表固件版本 "V2.10"。

命令示例：获取远程配置信息

CMD：AB BC CD D5 20 02 AA

RSP： AB BC CD D5 5A 4C 47 20 44 65 76 69 63 65 00 00 00 00 00 00 38 38 38 38 38 00 00 00 00 00 00 00 00 00 00 00 00 0B 10 01 20 02 00 38 1C 09 00 15 8D 00 20 01 00 00 00 00 00 00 00 00 00 03 03 0A 07 08 01 00 00 04 00 00 AA 00 04 01 00

7. 修改配置

修改配置的命令如表 14.162 所示。

注：设备的 MAC 地址只能通过该命令修改。

表 14.162 修改配置

3 字节（协议标志）	1 字节	2 字节	68 字节	1 字节（帧尾）
AB BC CD	D6	网络地址	DEV_INFO 结构信息	AA

修改本机配置时，只需在命令中填本地网络地址即可。修改的应答报文如表 14.163 所示。

表 14.163 修改配置应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节
AB BC CD	D6	网络地址	响应状态

响应状态详见表 14.63。

命令示例：修改配置

CMD：AB BC CD D6 20 01 5A 4C 47 20 44 65 76 69 63 65 00 00 00 00 00 00 38 38 38 38 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 10 01 20 01 00 5B 28 61 00 15 8D 00 20 02 00 00 00 00 00 00 00 00 00 03 05 0A 07 08 01 00 00 04 00 00 AA

RSP： AB BC CD D6 20 01 00

8. 复位

复位的命令如表 14.164 所示。

表 14.164 复位

3 字节（协议标志）	1 字节	2 字节	2 字节	1 字节（帧尾）
AB BC CD	D9	网络地址	协议类型	AA

复位命令无需应答。

命令示例：复位

```
CMD：   AB BC CD D9 20 01 00 04 AA                    /* 复位帧无应答 */
```

9. 恢复出厂设置

恢复出厂设置的命令如表 14.165 所示。

表 14.165 恢复出厂设置

3 字节（协议标志）	1 字节	2 字节	2 字节	1 字节（帧尾）
AB BC CD	DA	网络地址	协议类型	AA

协议类型：0x0004

恢复出厂设置应答报文如表 14.166 所示。

表 14.166 恢复出厂设置应答报文

3 字节（协议标志）	1 字节	2 字节	2 字节	1 字节
AB BC CD	DA	网络地址	协议类型	响应状态

响应状态详见表 14.63。

命令示例：恢复出厂设置

```
CMD：   AB BC CD DA 20 01 00 04 AA
RSP：   AB BC CD DA 20 01 00 04 00
```

10. 模块密码使能

模块支持配置设定的密码是否有效的功能，如果模块使能了密码，在修改配置时需要先执行模块登录命令后才能进行操作，如果模块没有使能密码，不需要执行模块登录命令，可直接修改配置。

如果忘记了密码，只能通过执行恢复出厂设置命令，模块恢复出厂设置后，密码不使能。模块默认的密码为：88888。

模块密码使能命令如表 14.167 所示。

表 14.167 模块密码使能

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	DE	网络地址	R/W	密码使能	AA

密码使能字节为 0，表示不使能密码，为 1 表示使能密码。该命令支持读取参数和设置参数，R/W 字节为 0，表示读参数，为 1 表示写参数。如果模块已经使能了密码，执行模块密码使能写命令时也需要先执行模块登录命令。

模块密码使能应答报文如表 14.168 所示。

表 14.168 模块密码使能应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节
AB BC CD	DE	网络地址	密码使能	响应状态

响应状态详见表 14.63。

命令示例：设置模块密码使能

CMD： AB BC CD DE 20 01 01 01 AA

RSP： AB BC CD DE 20 01 01 00

11. 模块登录

当模块使能了密码，在修改模块配置时需要先执行模块登录命令后才能进行操作。

模块登录的命令如表 14.169 所示。

表 14.169 模块登录

3 字节（协议标志）	1 字节	2 字节	1 字节	16 字节	1 字节（帧尾）
AB BC CD	DF	网络地址	R/W	密码	AA

该命令支持读取和设置参数。R/W 字节为 0，表示读参数，为 1 表示写参数。读参数时密码字段不起作用，读参数时响应状态如果返回 0，表示模块已经登录，如果响应状态返回非 0，表示模块没有登录；如果需要执行修改配置、模块密码使能等操作时，要先执行模块登录写命令，使用正确的密码登录模块。16 字节的密码只能为 ASCII 编码，密码最长是 15 字节，以 0 结束。

模块登录应答报文如表 14.170 所示。

表 14.170 模块登录应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节
AB BC CD	DF	网络地址	响应状态

响应状态详见表 14.63。

命令示例：用“ 88888”密码登录模块。

CMD： AB BC CD DF 20 01 01 38 38 38 38 38 00 00 00 00 00 00 00 00 00 00 AA

RSP： AB BC CD DF 20 01 00

12. I/O 方向设置

设置 IO 方向的命令如表 14.171 所示。

表 14.171 I/O 方向设置

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	E1	网络地址	R/W	IO	AA

IO 字节的 bit0~bit3 为 IO1~IO4，bit0 表示 IO1，bit1 表示 IO2，bit2 表示 IO3，bit3 表示 IO4。其相应位为 1，表示 I/O 为输出；其相应位为 0，表示 I/O 为输入，可设置本地 I/O 或远程 I/O。R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令 IO 字节的参数忽略

I/O 方向设置应答报文如表 14.172 所示。

表 14.172 I/O 方向设置应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节

AB BC CD	E1	网络地址	IO	响应状态

响应状态详见表 14.63。

命令示例：设置 IO1 为输出，其他 IO 为输入

CMD： AB BC CD E1 20 01 01 01 AA

RSP： AB BC CD E1 20 01 01 00

13. IO/AD 采集设置

模块有 4 路的 IO 和 4 路的 AD，IO/AD 采集设置命令可设定模块 IO 触发上传 IO 和 AD 状态及根据配置的周期时间定时上传 IO 和 AD 状态，设置的命令如表 14.173 所示。

表 14.173 IO/AD 采集设置

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节	2 字节	1 字节	1 字节（帧尾）
AB BC CD	E2	网络地址	R/W	IO	周期	是否休眠	AA

IO 字节的 bit0~bit3 为 IO1~IO4，bit0 表示 IO1，bit1 表示 IO2，bit2 表示 IO3，bit3 表示 IO4；当这些位为 1 时，表示上升沿触发，为 0 时，表示下降沿触发。bit4~bit7 为 IO1~IO4 的触发禁能，bit4 表示 IO1，bit5 表示 IO2，bit6 表示 IO3，bit7 表示 IO4，当这些位为 1 时，表示将输入触发禁能，不会上报数据，只能通过命令查询输入状态，为 0 时，表示输入触发使能，将会根据输入引脚的上升沿或者下降触发，然后上报数据。

周期的单位为 100ms，最大可设置的值为 65535，即设置的最大周期为 6553500ms。

是否休眠字节指示模块是否处于休眠状态，该字节为 1 表示模块处于休眠状态，IO 根据配置的状态发生变化时唤醒模块，并向目标节点地址发送 IO/AD 采集帧，如果周期大于 0，模块除了可以 IO 唤醒外，还会根据周期定时定时唤醒，然后向目标节点地址发送 IO/AD 采集帧，当发送完 IO/AD 采集帧后，模块进入休眠状态，该字节为 0 表示模块不休眠。

模块的工作模式分为以下四种情况：

在模块设置休眠的情况下分两种情况：

- 周期大于 0，模块按照设定周期定时唤醒并上传 IO 和 AD 数据或根据 IO 触发状态 IO 唤醒并上传 IO 和 AD 数据，数据上传完毕模块进入定时休眠；
- 周期等于 0，模块只能根据 IO 触发状态 IO 唤醒并上传 IO 和 AD 数据，然后模块进入深度休眠。

在模块设置不休眠的情况下分两种情况：

- 周期大于 0，模块根据设定的周期定时上传 IO 和 AD 数据，并且串口透明转发数据；
- 周期等于 0，模块不定时上传 IO 和 AD 数据，只能串口透明转发数据。命令中 R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令 IO、周期、是否休眠等参数忽略。

设置该命令后模块处于休眠状态时，通过把 WAKE 引脚拉低，模块唤醒，方便对模块进行配置或透传数据，配置完成后，把 WAKE 引脚拉高或悬空，模块根据配置的参数重新进入休眠状态。

只有把 IO 通过 I/O 方向设置命令设置为输入后，才能根据设定的边沿状态触发模块唤醒。IO/AD 采集设置应答报文如表 14.174 所示。

表 14.174 IO/AD 采集设置应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	2 字节	1 字节	1 字节
AB BC CD	E2	网络地址	IO	周期	是否休眠	响应状态

响应状态详见表 14.63。

模块 IO 触发或定时发送的 IO/AD 采集帧格式如表 14.175 所示。

表 14.175　IO/AD 采集帧格式

3 字节（协议标志）	1 字节	2 字节	1 字节	2 字节	2 字节	2 字节	2 字节
AB BC CD	E2	网络地址	IO	AD0	AD1	AD2	AD3

IO 字节的 bit0~bit3 为 IO1~IO4，bit0 表示 IO1，bit1 表示 IO2，bit2 表示 IO3，bit3 表示 IO4。该字节返回模块 IO 当前的电平值，1 为高电平，0 为低电平。

AD0~AD3 表示返回模块 4 路的 AD 转换值，返回为 10 位的 AD 转换值，需要自行转换为电压值，模块 ADC 的参考电压为 2.5V。

命令示例：配置 0x2001 地址的模块 IO1 为下降沿触发，IO2 为上升沿触发，IO3 为下降沿触发，IO4 为上升沿触发，模块定期上传 IO/AD 数据，周期为 5s，模块需要休眠。

```
CMD：  AB BC CD E2 20 01 01 0A 01 F4 01 AA
RSP：  AB BC CD E2 20 01 0A 01 F4 01 00
```

当模块发生 IO 触发或周期时间到时，往目标地址上传采集帧：

```
UPLOAD：  AB BC CD E2 20 01 0A 02 00 02 00 02 00 02 00
```

14. I/O 控制输出

I/O 控制输出命令如表 14.176 所示。

表 14.176　I/O 控制输出

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	E3	网络地址	R/W	IO	AA

IO 字节的 bit0~bit3 为 IO1~IO4，其相应位为 1，表示 I/O 为输出高电平；其相应位为 0，表示 I/O 为输出低电平，在调用该命令前需要先调用 I/O 方向设置命令把相应的 IO 设置为输出。R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令 IO 参数忽略。I/O 控制输出应答报文如表 14.177 所示。

表 14.177　I/O 控制输出应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节
AB BC CD	E3	网络地址	IO	响应状态

响应状态详见表 14.63。

命令示例：I/O 控制输出

```
CMD：  AB BC CD E1 20 01 01 02 AA      /*  IO2 设置为输出  */
RSP：  AB BC CD E1 20 01 02 00
CMD：  AB BC CD E3 20 01 01 02 AA      /*  IO2 输出高电平  */
RSP：  AB BC CD E3 20 01 02 00
```

15. PWM 控制输出

模块有 4 路的 PWM 输出，使用 PWM 输出配置命令可使能每路 PWM 的输出，设置的命令如表 14.178 所示。

表 14.178 PWM 控制输出命令

3 字节（协议标志）	1 字节	2 字节	1 字节	4 字节	1 字节	4 字节
AB BC CD	E4	网络地址	R/W	PWM1 频率	PWM1 占空比	PWM2 频率
1 字节	4 字节	1 字节	4 字节	1 字节	1 字节（帧尾）	
PWM2 占空比	PWM3 频率	PWM3 占空比	PWM4 频率	PWM4 占空比	AA	

四路 PWM 的通道号为 1~4；PWM 频率的单位为 Hz，通道 1、2 必须是同频率，可不同占空比，频率范围可设定从 586Hz~384000Hz，通道 3、4 必须是同频率，可不同占空比，频率范围可设定从 586Hz ~384000Hz；占空比的值可设定从 1~99，表示占空比的百分比。当每路的 PWM 信号的频率为 0 时，表示不输出 PWM 信号。R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令时，该命令的频率、占空比等参数忽略。

PWM 控制输出应答报文如表 14.179 所示。

表 14.179 PWM 控制输出应答报文

3 字节（协议标志）	1 字节	2 字节	4 字节	1 字节	4 字节
AB BC CD	E4	网络地址	PWM1 频率	PWM1 占空比	PWM2 频率
1 字节	4 字节	1 字节	4 字节	1 字节	1 字节
PWM2 占空比	PWM3 频率	PWM3 占空比	PWM4 频率	PWM4 占空比	响应状态

响应状态详见表 14.63。

命令示例：配置 PWM 的输出，PWM1 周期为 1000Hz，占空比是 20%，PWM2 周期为 1000Hz，占空比为 50%，PWM3 周期为 3000Hz，占空比为 60%，PWM4 周期为 3000Hz，占空比为 80%。

CMD： AB BC CD E4 20 01 01 00 00 03 E8 14 00 00 03 E8 32 00 00 0B B8 3C 00 00 0B B8 50 AA
RSP： AB BC CD E4 20 01 00 00 03 E8 14 00 00 03 E8 32 00 00 0B B8 3C 00 00 0B B8 50 00

16. 设置目标网络地址

设置数据发送的目标网络地址，其命令如表 14.180 所示。

表 14.180 设置目标网络地址

3 字节（协议标志）	1 字节	2 字节	2 字节	1 字节（帧尾）
AB BC CD	E9	网络地址	目标网络地址	AA

设置的回应报文如表 14.181 所示：

表 14.181 目标网络地址设置应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节

AB BC CD	E9	网络地址	响应状态

目标网络地址：

0xFFFF 代表广播给所有设备；

0xFFFD 代表广播给所有非睡眠设备；

0xFFFC 代表广播给协调器和路由设备；

0xFFFB 代表使用目标组号，发送组播。

响应状态详见表 14.63。

命令示例：设置目标网络地址

CMD：AB BC CD E9 20 02 20 01 AA
RSP： AB BC CD E9 20 02 00

17. 读取设备类型

读取对应网络地址的设备类型，如网络地址为本机地址，则读取本机的设备类型，其命令如表 14.182 所示。

表 14.182 读取设备类型

3 字节（协议标志）	1 字节	2 字节	1 字节（帧尾）
AB BC CD	EA	网络地址 0x0000~0xFFFF	AA

读取的应答报文如表 14.183 所示：

表 14.183 读取设备类型的应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节
AB BC CD	EA	网络地址 0x0000~ 0xFFFF	设备类型

设备类型参见表 14.66 中的 DevType。

命令示例：读取设备类型

CMD：AB BC CD EA 20 01 AA
RSP： AB BC CD EA 20 01 01

18. 查询子终端节点网络地址(只有路由及协调器有效)

ZM32 系列一个协调器或者一个路由器最多可连接 **50** 个终端子节点。查询路由、协调器的拥有的所有子终端节点的网络地址命令如表 14.184 所示。

表 14.184 查询子终端节点网络地址

3 字节（协议标志）	1 字节	2 字节	1 字节（帧尾）
AB BC CD	EB	网络地址 0x0000~0xFFFF	AA

查询子终端节点数量是有效的节点数量，应答报文如表 14.185 所示。

表 14.185 查询子终端节点网络地址应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	2 字节	…	2 字节
AB BC CD	EB	网络地址 0x0000~ 0xFFFF	子终端节点数量 N 0x00~0xFF	子终端节点网络地址 0x0000~ 0xFFFF	…	第 N 个子终端节点网络地址 0x0000~ 0xFFFF

命令示例：查询子终端节点

```
CMD： AB BC CD EB 20 02 AA          // 获取网络地址为 0x2002 拥有的所有子终端节点
RSP： AB BC CD EB 20 02 01 1F 03    // 获取到目标网络地址 0x2002 拥有 1 个子终端节点 0x1F03
```

19. 查询父节点网络地址

查询父节点网络地址的命令如表 14.186 所示。

表 14.186 查询父节点网络地址

3 字节（协议标志）	1 字节	2 字节	1 字节（帧尾）
AB BC CD	EC	网络地址 0x0000~ 0xFFFF	AA

查询父节点网络地址，应答报文如表 14.187 所示。

表 14.187 查询父节点网络地址的应答报文

3 字节（协议标志）	1 字节	2 字节	2 字节
AB BC CD	EC	网络地址 0x0000~0xFFFF	父节点的网络地址 0x0000~0xFFFF

命令示例：查询父节点网络地址

```
CMD：AB BC CD EC 20 02 AA      // 获取网络地址为 0x2002 的父节点网络地址
RSP： AB BC CD EC 20 02 1F 03  // 获取到目标网络地址 0x2002 的父节点网络地址 0x1F03
```

20. 查询 MAC 地址

查询网络地址对应的 MAC 地址的命令如表 14.188 所示。

表 14.188 查询 MAC 地址

3 字节（协议标志）	1 字节	2 字节	1 字节（帧尾）
AB BC CD	ED	网络地址 0x0000~ 0xFFFF	AA

查询网络地址对应的 MAC 地址，应答报文如表 14.189 所示。

表 14.189　查询 MAC 地址的应答报文

3 字节（协议标志）	1 字节	2 字节	8 字节
AB BC CD	ED	网络地址 0x0000~0xFFFF	MAC 地址

命令示例：获取到目标网络地址 0x2002 的 MAC 地址

CMD：　AB BC CD ED 20 02 AA

RSP：　AB BC CD ED 20 02 45 74 17 98 10 1F 03 36

21. 设置模块密钥

模块拥有两种类型的密钥：1、为预配置的密钥（加网使用）；2、网络密钥（数据传输使用）。

预配置密钥主机从机均具备，同一个网络内必须相同，该密钥只有在加网、建网前进行配置才有效。

网络密钥只有主机才具备写属性，加网成功后会下发该密钥给从机，该密钥只有建网前进行配置才有效。

注：如果在加网中或加入网络后，修改密钥（预配置密钥或网络密钥）只会在离网之后，重新入网时生效。

默认预配置密钥为：0x7a, 0x68, 0x69, 0x79, 0x75, 0x61, 0x6e, 0x64, 0x69, 0x61, 0x6e, 0x7a, 0x69, 0x2d, 0x68, 0x69

默认网络密钥为：0x68, 0x65, 0x6c, 0x6c, 0x6f, 0x2d, 0x77, 0x77, 0x77, 0x2e, 0x7a, 0x6c, 0x67, 0x2e, 0x63, 0x6e

设置模块密钥命令如表 14.190 所示。

表 14.190　设置模块密钥

3 字节（协议标志）	1 字节	2 字节	1 字节	16 字节	1 字节（帧尾）
AB BC CD	EE	网络地址	密钥类型	密码	AA

密钥类型：1 表示预配置密钥，2 表示网络密钥。

设置模块密钥应答报文如表 14.191 所示。

表 14.191　设置模块密钥应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节
AB BC CD	EE	网络地址	响应状态

响应状态详见表 14.63。

命令示例：设置模块密钥

CMD：AB BC CD EE 20 01 01 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 AA

RSP：　AB BC CD EE 20 01 00

22. 读取模块密钥

模块拥有两种类型的密钥：1、为预配置的密钥（加网使用）；2、网络密钥（数据传输

使用）。读取模块密钥命令如表 14.192 所示。

表 14.192　读取模块密钥

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节（帧尾）
AB BC CD	EF	网络地址	密钥类型	AA

密钥类型：1 表示预配置密钥，2 表示网络密钥。

读取模块密钥应答报文如表 14.193 所示。

表 14.193　读取模块密钥应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	16 字节
AB BC CD	EF	网络地址	密钥类型	密码

响应状态详见表 14.63。

命令示例：读取模块密钥

```
CMD：  AB BC CD EF 20 01 01 AA /*  读预配置密钥*/
RSP：  AB BC CD EF 20 01 01 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38
```

23. 进入升级模式

模块支持串口和空中升级两种方式，在进行固件升级前，需要先进入升级模式，再发送固件升级命令。

模块支持两种方式进入升级模式：

1. 通过无线或串口发送进入升级模式命令；

2. 将 ISP 管脚拉低，之后复位模块，并保持 ISP 管脚处于低电平 100ms 以上。

无线方式进入升级模式的方法为：使用本机模块向目标模块发送进入升级模式命令，目标模块接收到命令后，即进入升级模式。

串口方式进入升级模式的方法为：利用串口向模块发送进入升级模式命令，网络地址为本机网络地址，收到命令后，即进入升级模式。

进入升级模式的命令如表 14.194 所示。

表 14.194　进入升级模式

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节（帧尾）
AB BC CD	F1	网络地址	设备类型	AA

设备类型参见表 14.66 中的 DevType，可通过读取设备类型命令或读取本地配置命令获取，当网络地址为本机模块的地址时执行的是本机模块的串口升级，当网络地址为其他地址时，通过本机模块对指定地址的模块进行空中升级。

当固件升级失败，模块将一直处于升级模式，按照正常升级流程再升级即可。

进入升级模式的应答报文如表 14.195 所示。

表 14.195　进入升级模式的应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节
AB BC CD	F1	网络地址	响应状态

响应状态详见表 14.63。

24. 固件升级

模块支持串口和空中升级两种方式。当目标模块进入升级模式后，开始发送固件升级命令，升级模块的固件。发送固件升级的命令如表 14.196 所示。

表 14.196 固件升级

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节（帧尾）
AB BC CD	F2	网络地址	设备类型	AA

设备类型参见表 14.66 中的 DevType，可通过读取设备类型命令或读取本地配置命令获取，当网络地址为本机模块的地址时执行的是本机模块的串口升级，当网络地址为其他地址时，通过本机模块对指定地址的模块进行空中升级。

模块接收到升级命令后开始使用 XModem 协议进行升级。

通过本机模块对远程模块进行空中升级时，通过串口给本机模块发送升级命令，本机模块把命令转发给目标模块后，目标模块就通过本机模块透传使用 XModem 协议进行升级。

升级结束后模块返回的应答报文如表 14.197 所示。

表 14.197 升级完成应答

3 字节（协议标志）	1 字节	2 字节	1 字节
AB BC CD	F2	网络地址	升级结果

升级结束后模块返回的应答报文，升级结果的值如表 14.198 所示。

表 14.198 升级结果的值

1 字节	说明
0x00	固件升级成功
0x03	固件校验错误
0x05	固件升级失败
0x0A	固件与芯片型号不符

25. 设置接收模式

当模块接收到透传数据时，会进行根据接收模式的相关设置进行处理，然后发送到通过串口连接的用户设备。设置接收模式如表 14.199 所示。

表 14.199 设置接收模式

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	F3	网络地址	R/W	接收模式	AA

该命令支持读取和设置参数，R/W 字节为 0，表示读参数，为 1 表示写参数。读参数时，接收模式位域不起作用。保留的地方应该保持为 0，当设置的时候，行为不确定。

接收模式的位域如表 14.200 所示。

表 14.200 接收模式的位域

Bit 3~7	Bit 0~2 数据包格式
保留	0：数据 1：源网络地址+数据 2：源 MAC 地址+数据 3：源网络地址+源 MAC 地址+数据 4：接收帧格式

数据包格式：用户可以指定接收到的原始数据，跟一些有用信息打包在一起，然后才发送到串口。其中，当数据源(设备)并没有在"是否添加源 MAC 地址"中设置添加源 MAC 地址，则数据包会打包一个无效的 MAC 地址 FF:FF:FF:FF:FF:FF:FF:FF。

1. 数据：透传接收到的的原始数据。

   例如：本地设备收到某个远程设备传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 AA BB CC。

2. 源网络地址+数据：原始数据的前面会加上数据源(设备)的网络地址。

   例如：本地设备收到协调器(0x0000)传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 00 00 AA BB CC。

3. 源 MAC 地址+数据：原始数据的前面会加上数据源(设备)的 MAC 地址。

   例如：本地设备收到设备(11:22:33:44:55:66:77:88)传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 11 22 33 44 55 66 77 88 AA BB CC。

4. 源网络地址+源 MAC 地址+数据：原始数据的前面会加上数据源(设备)的网络地址和 MAC 地址。

   例如：本地设备收到协调器(0x0000/11:22:33:44:55:66:77:88)发过来的数据(0xAA 0xBB 0xCC)，则串口会输出 00 00 11 22 33 44 55 66 77 88 AA BB CC。

5. 接收帧格式：原始的数据会格式化成接收帧。

   例如：本地设备接收到协调器(0x0000/11:22:33:44:55:66:77:88)发过来的数据(0xAA 0xBB 0xCC)，则串口会输出 AD DB BE 90 11 22 33 44 55 66 77 88 00 00 00 03 AA BB CC 6E AA。

接收模式应答报文如表 14.201 所示。

表 14.201 设置接收模式应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节
AB BC CD	F3	网络地址	接收模式	响应状态

响应状态详见表 14.63。

命令示例：设置接收模式。

CMD： AB BC CD F3 20 01 01 01 AA

RSP： AB BC CD F3 20 01 01 00

26. 设置目标 MAC 地址

设置数据发送的目标 MAC 地址，其命令如表 14.202 所示。

表 14.202 设置目标 MAC 地址

3 字节（协议标志）	1 字节	2 字节	1 字节	8 字节	1 字节（帧尾）
AB BC CD	F4	网络地址	R/W	目标 MAC 地址	AA

该命令支持读取和设置参数，R/W 字节为 0，表示读参数，为 1 表示写参数。读参数时，目标 MAC 地址不起作用。当发送模式是单播的时候，会把没有进行任何转发处理的数据，直接转发到该预先配置好的目标 MAC 地址。

设置目标 MAC 地址应答报文如表 14.203 所示。

表 14.203 设置目标 MAC 地址应答报文

3 字节（协议标志）	1 字节	2 字节	8 字节	1 字节
AB BC CD	F4	网络地址	目标 MAC 地址	响应状态

目标 MAC 地址：

FF:FF:FF:FF:FF:FF:FF:FF 代表广播给所有设备；

FF:FF:FF:FF:FF:FF:FF:FD 代表广播给所有非睡眠设备；

FF:FF:FF:FF:FF:FF:FF:FC 代表广播给协调器和路由设备；

FF:FF:FF:FF:FF:FF:FF:FB 代表使用目标组号，发送组播；

00:00:00:00:00:00:00:00 代表协调器。

响应状态详见表 14.63。

命令示例：将数据转发到该目标 MAC 地址 11:22:33:44:55:66:77:88。

CMD： AB BC CD F4 20 01 01 11 22 33 44 55 66 77 88 AA

RSP： AB BC CD F4 20 01 11 22 33 44 55 66 77 88 00

27. 设置发送模式

当希望通过串口转发数据到其他远程设备时，或者本地设备产生的数据需要分发时，可以设置发送模式的相关功能，满足用户不同的通讯需求。设置发送模式命令如表 14.204 所示。

表 14.204 设置发送模式

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	F5	网络地址	R/W	发送模式	AA

该命令支持读取和设置参数，R/W 字节为 0，表示读参数，为 1 表示写参数。读参数时，发送模式不起作用，保留位填 0。

发送模式的位域如表 14.205 所示。

表 14.205 发送模式的位域

Bit 7	Bit 5~6 数据包格式	Bit 4 数据的目标地址选择	Bit 3 是否需要添加源 MAC 地址	Bit 0~2 数据传输方式
保留	0：数据（根据数据的目标地址进行发送） 1：指定网络地址+数据 2：指定 MAC 地址+数据 3：发送帧格式	0：目标网络地址(DEV_INFO.DstAddr) 1：目标 MAC 地址(DEV_INFO.DstIEEE)	0：不添加源 MAC 地址 1：添加源 MAC 地址	0：单播模式 1：广播给所有设备 2：广播给所有非睡眠设备 3：广播给协调器和所有路由器 4：组播模式

数据传输方式：用户需要串口转发的数据，或者 IO/ADC 采集数据，将会传输到指定的一台设备或者一组设备。

1. 单播模式: 数据只会传输给网络地址或者 MAC 地址匹配的设备。
2. 广播给所有设备：数据会传输给网络内所有设备。
3. 广播给非睡眠设备：数据会传输给网络内所有非睡眠设备。
4. 广播给协调器和路由器：数据会传输给网络的协调器和所有路由器。
5. 组播模式：数据会传输给目标分组内的所有设备。

是否需要添加源 MAC 地址：当用户希望远程设备转发到串口的数据包包含有效的 MAC 地址时，则需要添加源 MAC 地址。

数据目标地址选择：用户通过串口转发的数据，或者 IO/ADC 采集数据，需要传输到指定的一台目标设备，用目标地址来指示这台设备。用户可以自行选择，用网络地址或者 MAC 地址来作为目标地址。单播模式下有效。

1. 目标网络地址：数据会发送至设备配置信息中的目标网络地址(DEV_INFO.DstAddr)，参见表 14.66。
2. 目标 MAC 地址：数据会发送至设备配置信息中的目标 MAC 地址(DEV_INFO.DstIEEE)，参见表 14.66。

数据包格式：用户可以指定从串口发送的数据包的格式，从而改变数据的发送方式，单播模式下有效。

1. 数据：串口数据包只有普通数据，将会根据预设的方式(数据传输方式/是否添加源 MAC 地址/数据目标地址)进行传输。

   例如：从串口发送数据 AA BB CC，会根据预先配置好的方式(单播/带有源 MAC 地址/目标 MAC 地址)传输。
2. 临时目标网络地址+数据：串口数据包，包含指定设备的网络地址和普通数据。当串口发送有效的数据包时，会临时改变目标网络地址，然后传输到指定设备。

   例如：从串口发送 00 00 AA BB CC，会临时改变目标网络地址为 00 00，然后传输数据 AA BB CC。
3. 临时目标 MAC 地址+数据：串口数据包，包含指定设备的 MAC 地址和普通数据。当串口发送有效的数据包时，会临时改变目标 MAC 地址，然后传输到指定

设备。

例如：从串口发送 11 22 33 44 55 66 77 88 AA BB CC，会临时改变目标 MAC 地址为 11:22:33:44:55:66:77:88，然后传输数据 AA BB CC。

4. 发送帧格式：透传数据需要按照发送帧格式发向串口。当目标网络地址是 0xFFFE 时，目标 MAC 地址将作为透传数据发送的目的地址。

例如：从串口发送 AD DB BE 10 00 00 00 00 00 00 00 00 00 00 03 AA BB CC 8A AA，会向网络地址 0x0000 传输数据 AA BB CC；或者从串口发送 AD DB BE 10 11 22 33 44 55 66 77 88 FF FE 00 03 AA BB CC EB AA，会向 MAC 地址 11:22:33:44:55:66:77:88 传输数据 AA BB CC。

设置发送模式应答报文如表 14.206 所示。

表 14.206 设置发送模式应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节
AB BC CD	F5	网络地址	发送模式	响应状态

响应状态详见表 14.63。

命令示例：将数据单播到配置的目标网络地址，不包含本地 MAC 地址。

CMD： AB BC CD F5 20 01 01 00 AA

RSP： AB BC CD F5 20 01 00 00

28. 设置广播应答延时

当使用广播发送的命令需要应答时，例如“搜索网络内的设备”，接收方会延时一段时间才会将应答帧应答给命令发起设备，可以减轻网络拥塞而导致应答丢失的情况。

计算延时时间的方式如下。

当移动方向是向左移时：

延时时间(ms)=(本地网络地址<<移动位数) * 1ms

当移动方向是向右移时：

延时时间(ms)=(本地网络地址>>移动位数) * 1ms

例如：协调器发起广播命令“搜索网络内的设备”，终端设备的网络地址是 0x8000，移动方向是向右移，移动位数是 5，延时时间等于(0x8000>>5)*1ms，即延时 1024ms 后，终端设备就会将应答发送给协调器。

设置广播应答延时如表 14.207 所示。

表 14.207 设置广播应答延时

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	F6	保留	R/W	选项： 0：本地控制 1：广播控制-远程设备不用应答 2：广播控制-远程设备应答	延时参数： Bit-7：移动方向 Bit-6~Bit-3：保留 Bit-2~Bit-0：移动位数	AA

R/W 控制读写方向，需要跟选项字节配合使用。

R/W 字节为 0 时，表示该命令为读参数命令，仅支持选项为 0-本地控制和 2-广播控制-远程设备应答时使用；为 1 表示写参数命令，支持选项为 0-本地控制、1-广播控制-远程设备不用应答和 2-广播控制-远程设备应答时使用，并且会清空当前等待的命令应答。

选项字节为 0 时，表示该命令会控制本地设备，支持 R/W，本地设备会进行应答；为 1 时，会发起一次广播，控制网络内所有设备，支持 W，不支持 R，除了本地设备会应答，其他远程设备不会应答；为 2 时，会发起一次广播，控制网络内所有设备，支持 R/W，远程设备收到后会应答。

延时参数字节按照位划分，Bit-7 代表移动方向，0 是向右移，1 是向左移；Bit-2 到 Bit-0 是移动位数，即最大可移动 7 位。

当本地控制时，本地设备的应答报文如表 14.208 所示。

表 14.208 设置广播应答延时应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节	1 字节
AB BC CD	F6	网络地址	选项	延时参数	响应状态

响应状态详见表 14.63。

命令示例：设置本地设备的广播应答延时。

CMD： AB BC CD F6 00 00 01 00 05 AA

RSP： AB BC CD F6 00 00 00 05 00

命令示例：广播设置广播应答延时，远程设备不应答。

CMD： AB BC CD F6 00 00 01 01 05 AA

RSP： AB BC CD F6 00 00 00 05 00

命令示例：广播设置广播应答延时，远程设备应答。

CMD： AB BC CD F6 00 00 01 02 05 AA

RSP： AB BC CD F6 00 00 00 05 00

RSP： AB BC CD F6 01 23 00 05 00

RSP： AB BC CD F6 45 67 00 05 00

29. 启用黑名单

终端设备或者路由设备不会去加入，在黑名单里的对应通道的网络。比如：黑名单里记录了一项记录，通道 11 的网络 0x1234，当终端设备入网时检测到通道 11 存在网络 0x1234，里，是不会去加入的。

当前命令用来控制黑名单是否生效，对终端设备和路由设备有效；对协调器使用，响应状态返回不支持。

启用黑名单命令如表 14.209 所示。

表 14.209 启用黑名单

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节	1 字节（帧尾）
AB BC CD	F7	网络地址	R/W	使能	AA

R/W 字节为 0，表示该命令为读参数命令，为 1 表示写参数命令，当为读参数命令

时，该命令 IO 参数忽略。

当使能字节为 0 时，不启用黑名单功能；为 1 时，模块启用黑名单功能；

模块的黑名单功能默认是不启用的。

如果启用黑名单功能，当设备复位之后，会检查当前所在网络是否存在于黑名单，如果是，就会退出当前网络。

启用黑名单应答报文如表 14.210 所示。

表 14.210 启用黑名单应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节
AB BC CD	F7	网络地址	使能	响应状态

在修改配置信息之后，没有进行复位，将无法操作命令，并且响应状态返回其他错误。

响应状态详见表 14.63。

命令示例：查询黑名单是否使能。

CMD： AB BC CD F7 20 02 00 00 AA

RSP： AB BC CD F7 20 02 00 00

30. 配置黑名单

当前命令用来添加、删除、修改黑名单条目，对终端设备和路由设备有效；对协调器使用，响应状态返回不支持。

如果启用黑名单功能，当设备复位之后，会检查当前所在网络是否存在于黑名单，如果是，就会退出当前网络。

当前最多支持 10 条。

配置黑名单命令如表 14.211 所示。

表 14.211 配置黑名单

3 字节（协议标志）	1 字节	2 字节	1 字节	2 字节	2 字节	1 字节（帧尾）
AB BC CD	F8	网络地址	控制选项 R/C/A/D	PAN ID	通道掩码	AA

控制选项 R/C/A/D：

0x00：表示读黑名单(Read)，忽略通道掩码和 PAN ID 字段；

0x01：表示新增或者修改原有的一条黑名单项(Add)；

0x02：表示清空黑名单(Clear)，忽略通道掩码和 PAN ID 字段；

0x03：表示删除一条黑名单项(Delete)，忽略通道掩码和 PAN ID 字段；

PAN ID，表示相应通道下的网络；另外，0xFFFF 代禁止加入某个通道下的全部网络。

通道掩码，有 16bit，Bit0 对应通道 11，Bit15 对应通道 26。当对应 Bit 为 1 时，表示该通道的网络不会加入；

比如通道掩码是 0x0001，PAN ID 是 0x1234，代表通道 11 的网络 0x1234，成为黑名单成员，终端，路由设备不会对该网络发出入网请求。

比如通道掩码是 0x0001，PAN ID 是 0xFFFF，代表不会加入通道 11 的任何网络。

配置黑名单应答报文如表 14.212 所示。

表 14.212　配置黑名单应答报文

3 字节（协议标志）	1 字节	2 字节	1 字节	1 字节
AB BC CD	F8	网络地址	控制选项 R/C/A/D	数量
2 字节	2 字节	2 字节	2 字节	1 字节
第一条 PAN ID	第一条 通道掩码	第 N 条 PAN ID	第 N 条 通道掩码	响应状态

在修改配置信息之后，没有进行复位，将无法操作命令，并且响应状态返回其他错误。

响应状态详见表 14.63。

命令示例：查询黑名单配置。

CMD：　AB BC CD F8 20 02 00 00 00 00 00 AA

RSP：　AB BC CD F8 20 02 00 01 12 34 FF AF 00

14.3 特殊帧格式

14.3.1 发送帧

1. 描述

数据的发送支持透明传输和帧格式发送。按照帧格式发送，设备会将负载数据发送到指定地址。

用户通过修改配置命令或者设置发送模式命令，使设备进入帧格式发送模式。

用户可以指定目标网络地址，或者指定目标 MAC 地址发送，目标网络地址的优先级比目标 MAC 地址高；数据长度是指负载数据的字节数；累加和校验，是将从偏移量为 0 开始一直到负载数据最后一个字节，所进行累加的和，一共 8 bit。

当前负载数据在**单播下支持发送 255 字节**，即数据长度字段的最大值是 0x00FF。

当用户不知道目标设备的网络地址，可以在目标网络地址填入 0xFFFE，这时就会启用目标 MAC 地址进行传输。

如果想要广播，可以在目标网络地址，填入 0xFFFF，就可以发送广播了。当前负载数据在**广播下支持发送 74 字节**，即数据长度的最大值是 0x004A，10 秒内最多发送 9 次广播。

想要发送组播，可以使用组播发送帧，填入目标组号，就可以发送组播了。当前负载数据在**组播下支持发送 73 字节**，即数据长度的最大值是 0x0049，10 秒内最多发送 9 次组播。

如果想要发送给协调器，一种方法是在目标网络地址填入 0x0000；或者是在目标网络地址填入 0xFFFE，然后在目标 MAC 地址填入协调器的 MAC 地址。

2. 格式

发送帧格式如表 14.213 所示。

表 14.213　发送帧格式

3 字节（协议标志）	1 字节	8 字节	2 字节	2 字节	n 字节	1 字节	1 字节（帧尾）

AD DB BE	0x10	目标 MAC 地址	目标网络地址	数据长度	负载数据	累加和校验	AA

3. 示例

这个示例演示怎样将数据"Hello"，发送到目标 MAC 地址 12:34:56:78:90:AB:CD:EF，如表 14.214 所示。

表 14.214 发送帧示例

字段	偏移量	示例
协议标志	0	0xAD
	1	0xDB
	2	0xBE
发送帧标志	3	0x10
目标 MAC 地址	4 MSB	0x12
	5	0x34
	6	0x56
	7	0x78
	8	0x90
	9	0xAB
	10	0xCD
	11 LSB	0xEF
目标网络地址	12 MSB	0xFF
	13 LSB	0xFE
数据长度	14 MSB	0x00
	15 LSB	0x05
数据	16	0x48
	17	0x65
	18	0x6C
	19	0x6C
	20	0x6F
累加和校验	21	0x57
帧尾	22	0xAA

发送给协调器可以不用指定它的 MAC 地址，发送帧是：

```
AD DB BE 10 00 00 00 00 00 00 00 00 00 00 03 AA BB CC 8A AA
```

协调器会收到数据：

```
AA BB CC
```

14.3.2 组播发送帧

1. 描述

当进入帧格式发送模式，可以选择使用组播发送帧进行数据的组播传输，不同类型的发送帧用帧内的发送帧标志字段区分。

用户通过修改配置命令或者设置发送模式命令，使设备进入帧格式发送模式。

2. 格式

组播发送帧格式如表 14.215 所示。

表 14.215 组播发送帧格式

3 字节（协议标志）	1 字节	2 字节	2 字节	n 字节	1 字节	1 字节（帧尾）
AD DB BE	11	目标组号	数据长度	负载数据	累加和校验	AA

3. 示例

这个示例演示怎样将数据"Hello"，发送到分组 0x1234，如表 14.216 所示。

表 14.216 组播发送帧示例

字段	偏移量	示例
协议标志	0	0xAD
	1	0xDB
	2	0xBE
发送帧标志	3	0x11
目标组号	4 MSB	0x00
	5 LSB	0x01
数据长度	6 MSB	0x00
	7 LSB	0x05
数据	8	0x48
	9	0x65
	10	0x6C
	11	0x6C
	12	0x6F
累加和校验	13	0x51
帧尾	14	0xAA

分组 0x0001 的设备会收到数据（ASCII）：

```
Hello
```

14.3.3 接收帧

1. 描述

数据的接收支持透明传输和帧格式接收。设备会将接收到的数据按照接收帧的格式打包起来，然后再从串口送出去。

用户通过修改配置命令或者设置接收模式命令，使设备进入帧格式接收模式。

源 MAC 地址是指发送数据的源设备的 MAC 地址，同理，源网络地址是指发送数据的设备的网络地址。

2. 格式

接收帧格式如表 14.217 所示。

表 14.217 接收帧格式

3 字节（协议标志）	1 字节	8 字节	2 字节	2 字节	n 字节	1 字节	1 字节（帧尾）
AD DB BE	0x90	源 MAC 地址	源网络地址	数据长度	负载数据	累加和校验	AA

3. 示例

表 14.218 接收帧示例

字段	偏移量	示例
协议标志	0	0xAD
	1	0xDB
	2	0xBE
发送帧标志	3	0x90
源 MAC 地址	4 MSB	0x12
	5	0x34
	6	0x56
	7	0x78
	8	0x90
	9	0xAB
	10	0xCD
	11 LSB	0xEF
源网络地址	12 MSB	0xA7
	13 LSB	0xB5
数据长度	14 MSB	0x00
	15 LSB	0x03
数据	16	0xAA
	17	0xBB
	18	0xCC
累加和校验	19	0x71

帧尾	20	0xAA

这个示例演示 MAC 地址 12:34:56:78:90:AB:CD:EF，网络地址 0xA7B5 的远程设备发送数据 0xAA 0xBB 0xCC，如果本地设备接收后，会从串口发出下面这一帧数据，如表 14.218 所示。

14.3.4 组播接收帧

1. 描述

当使用帧格式接收数据的时候，如果数据是通过单播或者广播传输的，那么就会接收到前面提到的接收帧，如果数据是通过组播传输的，那么就会收到组播接收帧。

用户通过修改配置命令或者设置接收模式命令，使设备进入帧格式接收模式。

2. 格式

组播接收帧格式如表 14.219 所示。

表 14.219 组播接收帧格式

3 字节（协议标志）	1 字节	2 字节	8 字节	2 字节
AD DB BE	91	分组号	源 MAC 地址	源网络地址
2 字节	n 字节	1 字节	1 字节（帧尾）	
数据长度	负载数据	累加和校验	AA	

3. 示例

这个示例演示 MAC 地址 12:34:56:78:90:AB:CD:EF，网络地址 0x0000 的远程设备发送数据 0xAA 0xBB 0xCC，目的分组是 0x0001；如果本地设备属于分组 0x0001，那么会从串口发出下面这一帧数据，如表 14.220 所示。

表 14.220 组播接收帧示例

字段	偏移量	示例
协议标志	0	0xAD
	1	0xDB
	2	0xBE
发送帧标志	3	0x91
分组号	4	0x00
	5	0x01
源 MAC 地址	6 MSB	0x12
	7	0x34
	8	0x56
	9	0x78
	10	0x90
	11	0xAB

	12	0xCD

续上表

	13 LSB	0xEF
源网络地址	14 MSB	0x00
	15 LSB	0x00
数据长度	16 MSB	0x00
	17 LSB	0x03
数据	18	0xAA
	19	0xBB
	20	0xCC
累加和校验	21	0x16
帧尾	22	0xAA

15. 附录

15.1 专有名词解释

协议类型

用来区分无线设备的协议栈类型，ZM32 的协议类型是 ZLGMesh，不可修改。

固件版本

当前设备运行的固件版本，如果需要升级的话，可以区分设备是否升级成功。

设备名称

设备命令标示字符串，用户可以定义自己的设备标示字符串。

登录密码

当模块登录使能后，需要用正确的登录密码登录之后才可以正常配置。最大可以设置 15 个字符，并且不能包含*号。

工作类型

ZLGMesh 提供三种设备类型：终端设备、路由设备、协调器设备

建立 1 个网络的时候需要有一个协调器(最多一个)，可以有多个路由设备，终端设备加入网络必须要有协调设备，或者路由设备充当父节点。

当设备需要切换工作类型时，会引起设备退网(如果设备已经加入网络)。

通道号

通道号可以选择 CH11 ~ CH26。

设备的工作通道号，不同通道的数据通讯理论上是独立的。当设备需要切换通道时，会引起设备退网(如果设备已经加入网络)。

PAN ID

PAN ID 可以选择 0x0000 ~ 0xFFFF。当配置 0xFFFF 时，设备会退网。

用来区分通道号相同的不同网络，若通道内的网络数量过多，同频干扰将比较严重，易引起网络堵塞，严重的时候会丢失数据。当设备需要改变 PAN ID 时，会引起设备退网(如果设备已经加入网络)。

本地地址

只读，用来跟网络内其他设备区分开。

MAC 地址

每个设备都有唯一的 MAC 地址。设置 FF:FF:FF:FF:FF:FF:FF:FF 会恢复成出厂的 MAC 地址。

在设备加入网络的时候，可以根据用户实际情况配置；修改 MAC 地址将会在下一次建网/加网时起作用，比如：在设备入网之前修改， MAC 地址变化马上生效；但是，在设备入网之后修改， MAC 地址变化会在切换网络时生效。

目标网络地址

透传数据，或者采集报文上传的目标设备的网络地址。

目标 MAC 地址

透传数据，或者采集报文上传的目标设备的 MAC 地址。

目标组号

在组播模式下使用，本地模块给处于目标分组的模块发送数据。

发送功率

发送功率越大，通信距离越远，但是功耗更大。

可选：0(-30 dBm)、1(-25 dBm)、2(-20 dBm)、3(-15 dBm)、 4(-10 dBm)、5(-5 dBm)、6(0 dBm)、7(5 dBm)、 8(10 dBm)、9(15 dBm)、10(19 dBm)、0x10(0dBm)、0x11(1dBm)、0x12(2dBm) 、 0x13(3dBm) 、 0x14(4dBm) 、 0x15(5dBm) 、 0x16(6dBm) 、 0x17(7dBm) 、0x18(8dBm)、0x19(9dBm)、0x1A(10dBm)、0x1B(11dBm)、 0x1C(12dBm)、0x1D(13dBm)、0x1E(14dBm)、0x1F(15dBm)。

接收模式

当模块接收到透传数据时，会进行根据接收模式的相关设置进行处理，然后发送到通过串口连接的用户设备。

数据包格式

用户可以指定接收到的原始数据，跟一些有用信息打包在一起，然后才发送到串口。其中，当数据源(设备)并没有在参数配置时，在是否需要添加源 MAC 地址中选择“是”，数据包会打包一个无效的 MAC 地址 FF:FF:FF:FF:FF:FF:FF:FF。

可以选择四种格式:

数据：透传接收到的的原始数据。例如：本地设备收到某个远程设备传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 AA BB CC。

源网络地址+数据：原始数据的前面会加上数据源(设备)的网络地址。例如：本地设备收到协调器(0x0000)传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 00 00 AA BB CC。

源 MAC 地址+数据：原始数据的前面会加上数据源(设备)的 MAC 地址。例如：本地设备收到设备(11:22:33:44:55:66:77:88)传输过来的数据(0xAA 0xBB 0xCC)，则串口会输出 11 22 33 44 55 66 77 88 AA BB CC。

源网络地址+源 MAC 地址+数据：原始数据的前面会加上数据源(设备)的网络地址和 MAC 地址。例如：本地设备收到协调器(0x0000/11:22:33:44:55:66:77:88)发过来的数据(0xAA 0xBB 0xCC)，则串口会输出 00 00 11 22 33 44 55 66 77 88 AA BB CC。

接收帧格式：原始的数据会格式化成接收帧。例如：本地设备接收到协调器(0x0000/11:22:33:44:55:66:77:88) 发过来的数据(0xAA 0xBB 0xCC)，则串口会发送 AD DB BE 90 11 22 33 44 55 66 77 88 00 00 00 03 AA BB CC 6E AA。

发送模式

当希望通过串口转发数据到其他远程设备时，或者本地设备产生的数据需要分发时，可以设置发送模式的相关功能，满足用户不同的通讯需求。

数据传输格式

用户需要串口转发的数据，或者 IO/ADC 采集数据，将传输给一台设备或者一组设备。

目前支持 5 种格式：

单播模式：数据只会传输给网络地址或者 MAC 地址匹配的设备。

广播给所有设备：数据会传输给网络内所有设备。

广播给非睡眠设备：数据会传输给网络内所有非睡眠设备。

广播给协调器和路由器：数据会传输给网络的协调器和所有路由器。

组播模式：数据会传输给目标分组内的所有设备。

是否需要添加源 MAC 地址：当用户希望远程设备转发到串口的数据包包含有效的 MAC 地址时，则需要添加源 MAC 地址。

数据目标地址选择

用户通过串口转发的数据，或者 IO/ADC 采集数据，需要传输到指定的一台目标设备，用目标地址来指示这台设备。用户可以自行选择，用网络地址或者 MAC 地址来作为目标地址。单播模式下有效。

目标网络地址：数据会发送至设备配置信息中的目标网络地址(DEV_INFO 结构信息.DstAddr)。

目标 MAC 地址: 数据会发送至设备配置信息中的目标 MAC 地址(DEV_INFO 结构信息. DstIEEE)。

数据包格式

用户可以指定从串口发送的数据包的格式，从而改变数据的发送方式，单播模式下有效。

数据: 串口数据包只有普通数据，将会根据预设的方式 (数据传输方式/是否添加源 MAC 地址/数据目标地址)进行传输。

例如：从串口发送数据 AA BB CC，会根据预先配置好的方式(单播/带有源 MAC 地址/目标 MAC 地址)传输。

临时目标网络地址+数据: 串口数据包，包含指定设备的网络地址和普通数据。当串口发送有效的数据包时，会临时改变目标网络地址，然后传输到指定设备。

例如：从串口发送 00 00 AA BB CC，会临时改变目标网络地址为 00 00，然后传输数据 AA BB CC。

临时目标 MAC 地址+数据: 串口数据包，包含指定设备的 MAC 地址和普通数据。当串口发送有效的数据包时，会临时改变目标 MAC 地址，然后传输到指定设备。

例如：从串口发送 11 22 33 44 55 66 77 88 AA BB CC，会临时改变目标 MAC 地址为 11:22:33:44:55:66:77:88，然后传输数据 AA BB CC。

发送帧格式：透传数据需要按照发送帧格式发向串口。当目标网络地址是 0xFFFE 时，目的 MAC 地址将作为透传数据发送的目的地址。

例如：从串口发送 AD DB BE 10 00 00 00 00 00 00 00 00 00 00 03 AA BB CC 8A AA，会向网络地址 0x0000 传输数据 AA BB CC；或者从串口发送 AD DB BE 10 11 22 33 44 55 66 77 88 FF FE 00 03 AA BB CC EB AA，会向 MAC 地址 11:22:33:44:55:66:77:88 传输数据 AA BB CC。

波特率

串口波特率：2400、4800、9600、19200、38400、57600、115200、230400

数据位

串口数据位，8 位

校验位

串口校验位：无、奇校验、偶校验、停止位

停止位

1 位、2 位

帧超时时间

帧数据的超时时间，也是模块接收数据字节的超时时间，范围 2ms ~ 255ms，切换波特率会调整为默认的超时时间。

15.2 组网流程图

15.2.1 配置组网

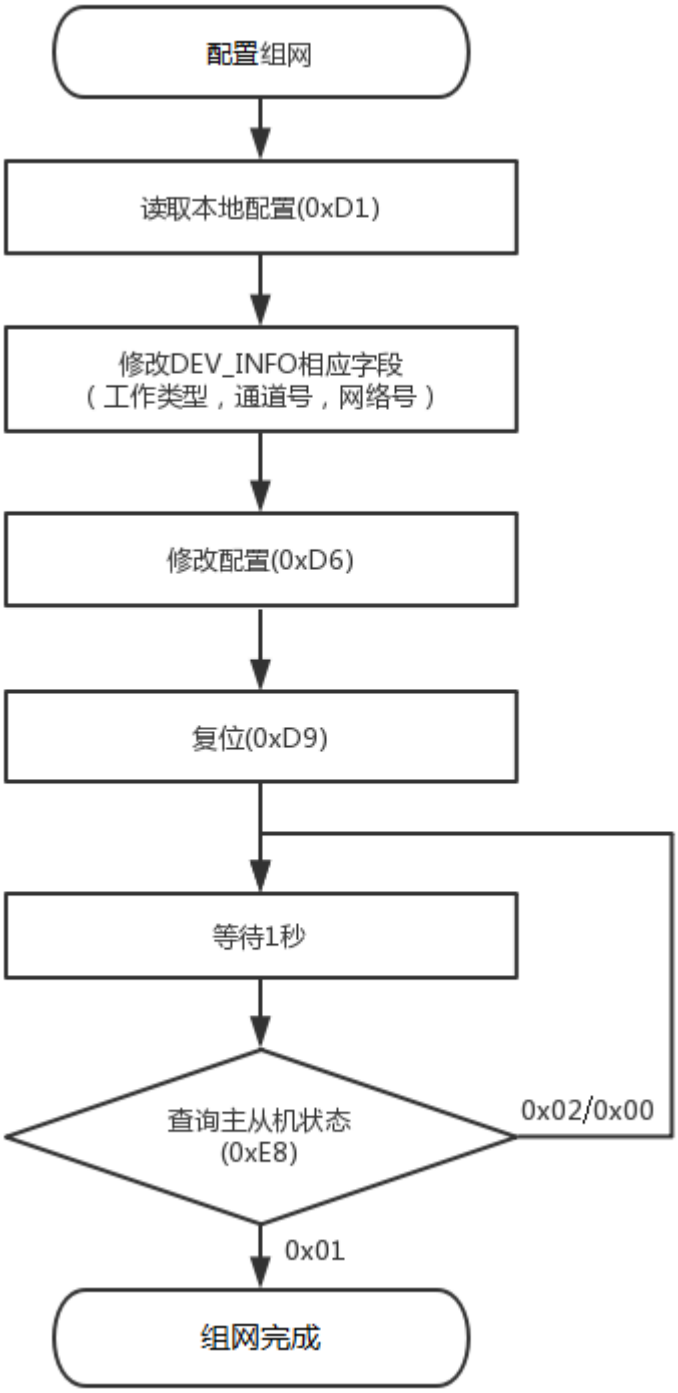

图 15.1　配置组网

15.2.2 普通自组网-主机

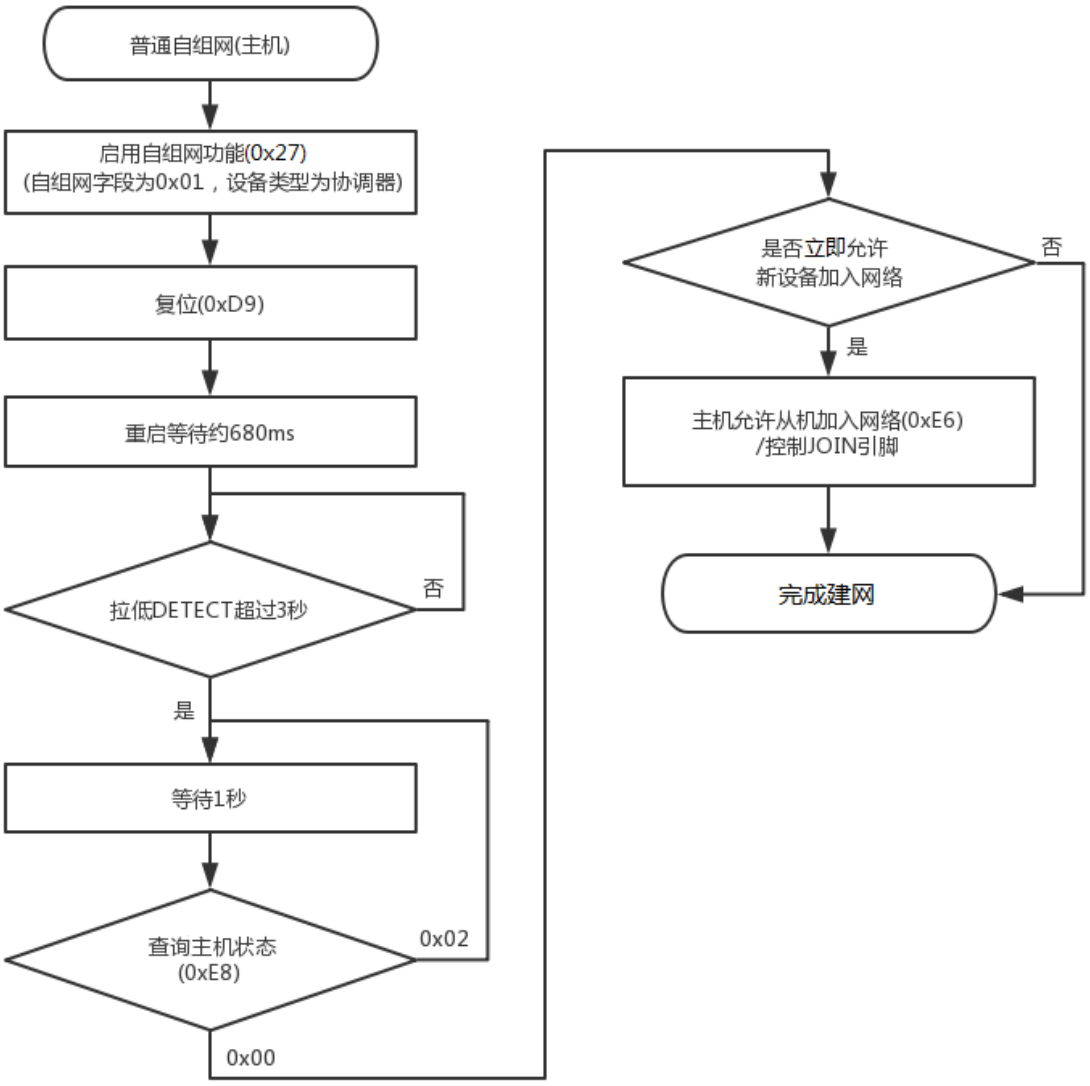

图 15.2 普通自组网-主机

15.2.3 普通自组网-从机

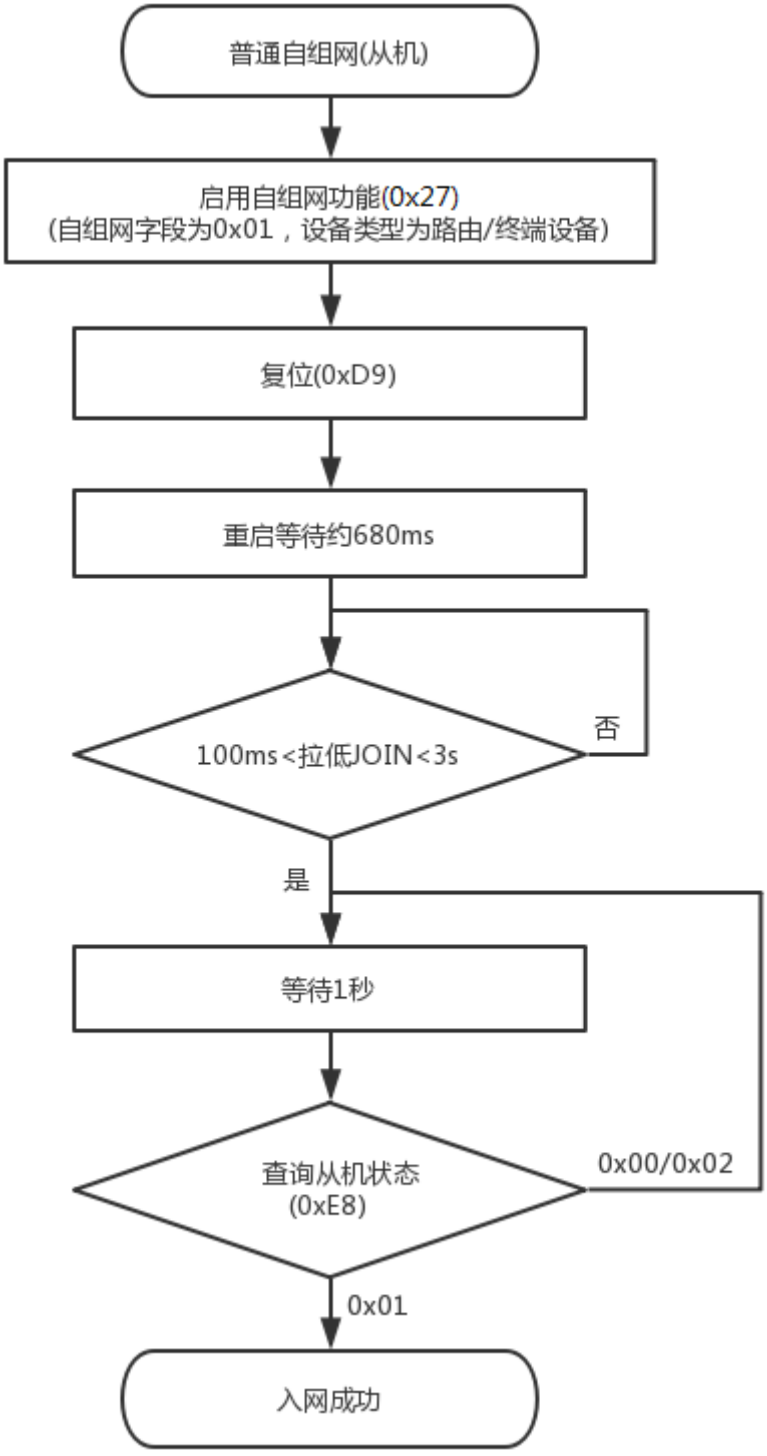

图 15.3　普通自组网-从机

15.2.4 快速自组网-主机

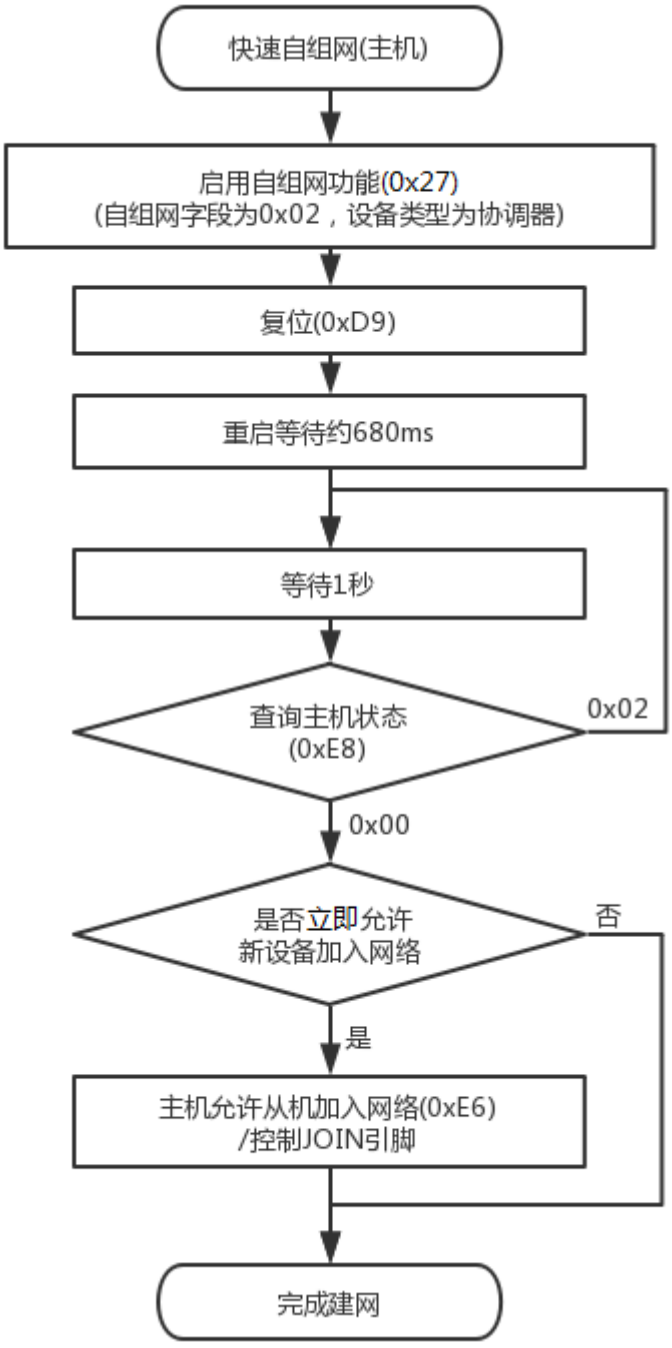

图 15.4 快速自组网-主机

15.2.5 快速自组网-从机

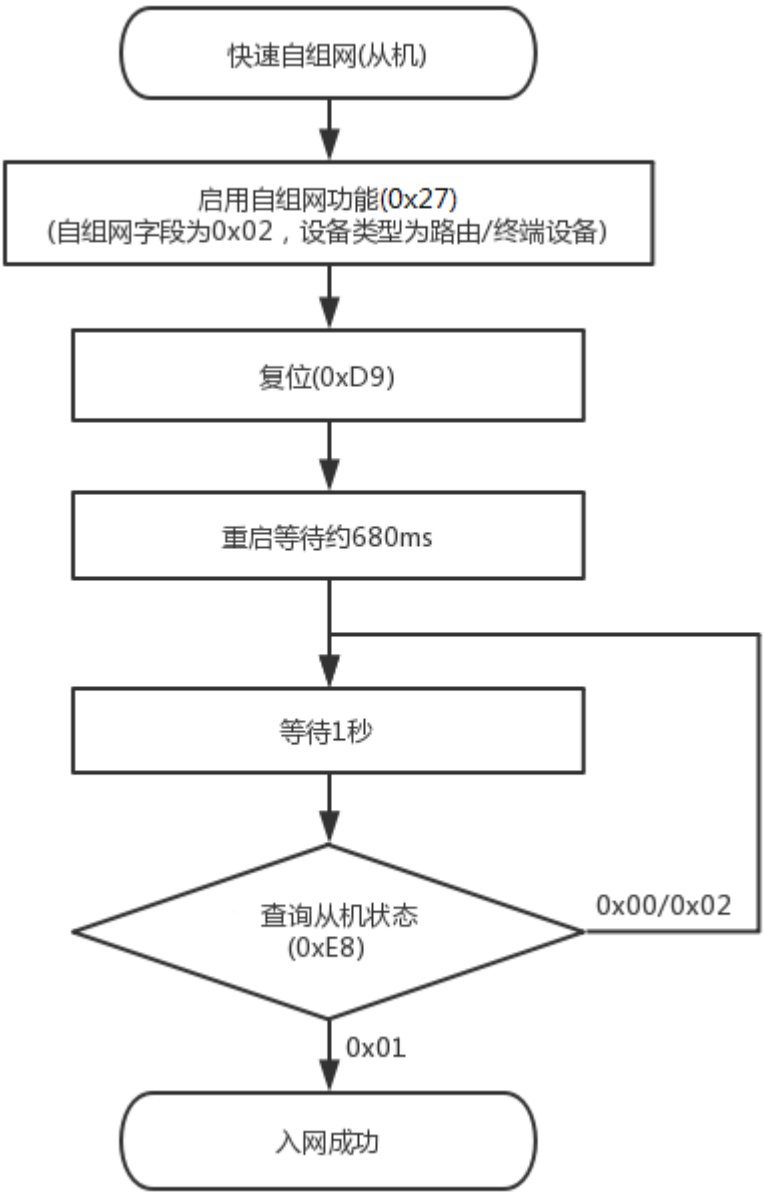

图 15.5 快速自组网-从机

16. 免责声明

广州致远电子有限公司隶属于广州立功科技股份有限公司。本着为用户提供更好服务的原则，广州致远电子有限公司（下称“致远电子”）在本手册中将尽可能地为用户呈现详实、准确的产品信息。但介于本手册的内容具有一定的时效性，致远电子不能完全保证该文档在任何时段的时效性与适用性。致远电子有权在没有通知的情况下对本手册上的内容进行更新，恕不另行通知。为了得到最新版本的信息，请尊敬的用户定时访问致远电子官方网站或者与致远电子工作人员联系。感谢您的包容与支持！