User Manual

ZM516X 系列 ZigBee 无线模块用户手册

FastZigbee 组网固件版

UM01010101 V1.13 Date: 2018/12/19 产品用户手册

类别	内容
关键词	ZM516X 系列 ZigBee 无线模块， FastZigbee 固件
摘要	本文主要描述 ZM516X 系列 ZigBee 无线模块的硬件参数和使用方法。 注意：本文档仅适用于使用以下固件的 ZM516X 系列模块： **FastZigBee 组网固件（模块型号后缀含 -2、-2C）** **固件版本 2.04 以上**

修订历史

版本	日期	原因
V1.00	2014/03/13	创建文档
V1.01	2014/04/22	增加大功率模块机械尺寸
V1.02	2014/08/06	增加模块密码验证功能
V1.03	2014/09/18	增加 IO 操作和 AD 读取功能
V1.04	2014/09/19	增加选型表，增加模块尺寸文件链接
V1.05	2014/12/12	新增 FastZigBee 组网固件说明
V1.06	2015/02/28	文档描述优化
V1.07	2015/06/02	AD 读取功能描述修正
V1.08	2015/08/19	更新选型表，优化 AD 引脚与信号强度值说明
V1.09	2018/02/28	增加模块密码登录命令和 PANID 临时参数配置命令
V1.10	2018/04/24	更新配置工具截图，睡眠、唤醒管脚操作说明
V1.11	2018/08/02	更新功耗、选型表，更新回流焊曲线、参数
V1.12	2018/09/07	修正 D4 搜索命令的说明
V1.13	2018/12/19	修改通信距离参数

目 录

1. 产品简介

1.1 产品概述

ZM516X 系列 ZigBee 无线模块是广州致远电子有限公司基于 NXP JN516X 系列芯片开发的低功耗、高性能型 ZigBee 模块，它提供一个完整的基于 IEEE802.15.4 标准 ISM（2.4-2.5GHz）频段的应用集成方案。支持 FastZigBee、ZNET、JenNet-IP、ZigBee-PRO、RF4CE 等协议，可快速应用于工业控制、工业数据采集、农业控制、矿区人员定位、智能家居，智能遥控器等场合。

ZM516X 系列 ZigBee 模块，将完整的射频收发电路集成在一个模块上，将无线通讯产品复杂的通讯协议内嵌在内置的 MCU 中，化繁为简，大幅简化开发过程，使得用户产品更快的投入市场，增加用户产品的竞争力，更好的把握住先机。

图 1.1 产品外观

1.2 模块命名规则

ZM516X 系列模块有以下命名规则，如所示，本系列所有模块出厂默认参数均遵循产品命名规则，在购买产品前请务必确认产品型号是否与需求一致。

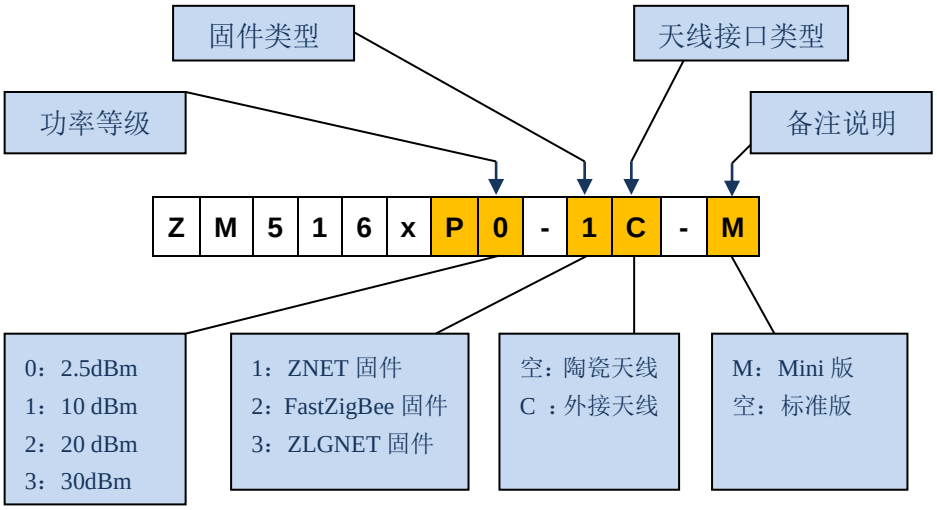

图 1.2 产品命名规则

1.3 产品选型

表 1.1 ZM516X 系列模块产品型号一览表

模块类型	天线类型	发射功率	协议类型	尺寸
ZM5168P0-1	板载 PCB 天线	+2.5 dBm	ZNET	16×32mm
ZM5168P0-1C	μFI 天线接口	+2.5 dBm	ZNET	16×32mm
ZM5168P0-1C-M	μFI 天线接口	+2.5 dBm	ZNET	16×19 mm
ZM5161P0-2 ZM5168P0-2	板载 PCB 天线	+2.5 dBm	FastZigBee	16×32mm
ZM5161P0-2-M	板载陶瓷天线	+2.5 dBm	FastZigBee	16×19 mm
ZM5161P0-2C ZM5168P0-2C	μFI 天线接口	+2.5 dBm	FastZigBee	16×32 mm
ZM5161P0-2C-M	μFI 天线接口	+2.5 dBm	FastZigBee	16×19 mm
ZM5168P1-1C	μFI 天线接口	+10dBm	ZNET	16×28 mm
ZM5161P1-2	板载陶瓷天线	+10dBm	FastZigBee	16×28 mm
ZM5161P1-2C	μFI 天线接口	+10dBm	FastZigBee	16×28 mm
ZM5168P2-1	板载陶瓷天线	+20dBm	ZNET	16×28 mm
ZM5168P2-1C	μFI 天线接口	+20dBm	ZNET	16×28 mm
ZM5161P2-2	板载陶瓷天线	+20dBm	FastZigBee	16×28 mm
ZM5161P2-2C	μFI 天线接口	+20dBm	FastZigBee	16×28 mm
ZM5161P2-3	板载陶瓷天线	+20dBm	ZLGNET	16×28 mm
ZM5161P2-3C	μFI 天线接口	+20dBm	ZLGNET	16×28 mm
ZM5161P3-2C	μFI 天线接口	+30dBm	FastZigBee	16×28 mm

FastZigBee：ZigBee 快速组网协议，多型态网络，实际运用最多，推荐使用；

ZNET：基于 JenNet-IP 的组网协议，可组建树形网络；

ZLGNET：自主研发协议，支持多级跳转；

模块视距通信距离（外接天线版）：P0≈504m，P1≈1.1km，P2≈2km；

板载天线模块一般需嵌入到用户产品当中，通信距离请根据实际应用实测。

1.4 模块尺寸

ZM516X 系列模块包含不同尺寸、不同封装的产品，不同型号的模块外形存在差异，具体外形尺寸说明，请参考以下文件：

按住 Ctrl 并单击可直接访问：

【开发资料】ZM516X 系列模块产品尺寸.rar

2. 硬件描述

2.1 引脚说明

ZM516X 系列模块的引脚分布如图 2.1 所示，产品全系列引脚分布一致，并与 NXP JN5168 系列模块完全 Pin-to-Pin 兼容。

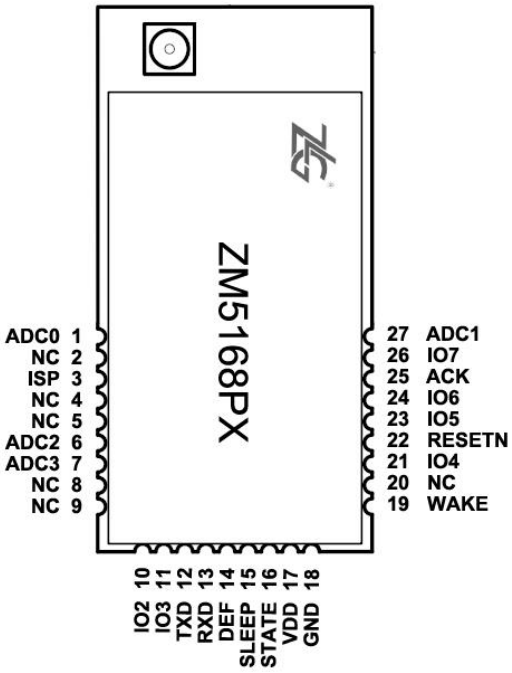

图 2.1 引脚分布图

ZM516X 系列无线模块管脚功能说明如表 2.1 所示，以下说明仅针对使用 FastZigBee 固件的 ZM516X 系列模块，如使用本系列模块自行开发其它协议，可直接参考 NXP《JN5168-001-MXX》模块数据手册。

表 2.1　ZM516X 模块管脚说明

引脚号	引脚名称	方向	功能	描述
1	ADC0	Input	模拟输入	ADC0 输入
2	NC	—	无	
3	ISP	Input	固件升级使用	将该管脚拉低后上电，进入 ISP 固件升级模式
4	NC	—	无	
5	NC	—	无	
6	ADC2	Input	模拟输入	ADC2 输入（V1.70 及以上固件版本支持）
7	ADC3	Input	模拟输入	ADC3 输入（V1.70 及以上固件版本支持）
8	NC	—	无	
9	NC	—	无	
10	IO2	I/O	数字输入输出	
11	IO3	I/O	数字输入输出	
12	TXD	Output	串口发送	TTL 电平
13	RXD	Input	串口接收	TTL 电平
14	DEF	Input	恢复出厂	内部上拉，复位或重新上电时，如果该管脚被拉低，模块参数将被重置为出厂默认。
15	SLEEP	Input	休眠	SLEEP，低电平有效，使模块进入休眠状态；需要把模块进入休眠状态时，把 SLEEP 一直拉低。 注：ZNET 固件只有终端设备才能进入休眠
16	STATE	Output	工作指示灯	可外接指示灯，模块工作时 500ms 闪烁，不使用可悬空
17	VDD	—	电源	
18	GND	—	地	
19	WAKE	Input	唤醒	WAKE，下降沿有效，使模块从休眠中唤醒；需要把模块唤醒时，先把 SLEEP 拉高，再发出 WAKE 下降沿，把模块唤醒。 ZNET 固件只有终端设备才能进入休眠
20	NC	—	无	
21	IO4	I/O	数字输入输出	
22	RESETN	Input	复位输入	低电平有效，模块上电时需提供正确的复位电平，低电平复位时间至少保持 1ms
23	IO5	I/O	数字输入输出	
24	IO6	I/O	数字输入输出	
25	ACK	Output	ACK 接受指示	初始状态为低电平，收到 ACK 回复后产生高电平脉冲。 注意：用户 MCU 可通过检测该管脚判断数据是否已成功到达目标节点。该管脚输出脉冲时间短，直接驱动 LED 无明显效果。
26	IO7	I/O	数字输入输出	
27	ADC1	Input	模拟输入	ADC1 输入

2.2 产品规格

表 2.2 模块典型 DC 特性

VDD=3.3V @ +25°C

典型 DC 特性									
工作模式	ZM516xP0 系列			ZM516xP1 系列			ZM516xP2 系列		
	最小值	典型值	最大值	最小值	典型值	最大值	最小值	典型值	最大值
深度睡眠模式		220nA			444nA			476nA	
发送模式	19mA	21mA	23mA	57mA	59mA	63mA	142mA	144mA	148mA
接收模式	19mA	21mA	23mA	23mA	28mA	31mA	23mA	28mA	31mA

表 2.3 模块典型 RF 特性

典型 RF 特性				
特性	ZM516XP0	ZM516XP1	ZM516XP2	备注
接收灵敏度	-95dBm	-96dBm	-100 dBm	
发送功率	2.5 dBm	10dBm	20dBm	
最大接收功率	10 dBm	5 dBm	5 dBm	
RSSI 范围	-95 dBm 到 -10 dBm	-102 dBm 到-17 dBm	-105 dBm 到-20 dBm	
中心频率偏移	+/-25ppm	+/-25ppm	+/-25ppm	不包括因温度和老化引起的额外+/-15ppm
输出端口阻抗	50Ω	50Ω	50Ω	

2.3 电气特性

2.3.1 极限参数

超出以下条件会导致模块损坏。

参数	最小值	最大值
电源电压	-0.3V	3.6V
管脚电压	-0.3V	VDD+0.3V
存储温度	-40℃	150℃

2.3.2 工作条件

参数	最小值	最大值
电源电压	2.0V	3.6V
环境温度范围	-40℃	85℃

2.4 典型应用

ZM516X 模块提供了透明传输数据的功能，通过模块的串口实现用户数据的无线传输，ZM516X 模块典型应用（以 ZM5168 为例）如图 2.2 所示。

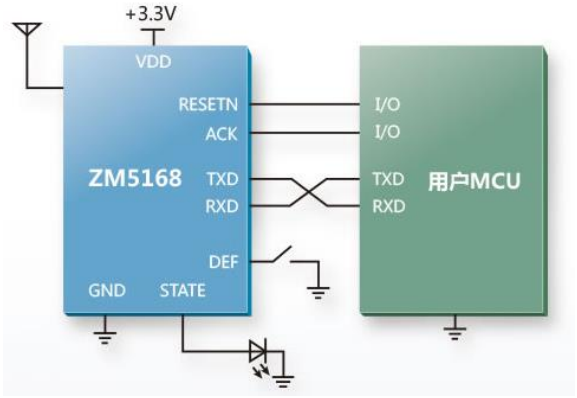

图 2.2 典型应用图

2.5 天线布局规范

2.5.1 PCB 天线布局

ZM516x 系列模块部分型号采用 PCB 板载天线或陶瓷天线设计，具有一个垂直极化近乎全向辐射。这提供了无需任何额外的接地平面，即可达到无线信号辐射的效果，但必须注意安装该类型模块到另一个 PCB 时需遵循规范。

天线周围的区域必须保持与导线或其他金属物体至少 20 毫米。这适用于 PCB 的所有层，而不仅仅是顶层。靠近天线的任何导电物体可能会严重破坏 PCB 天线或陶瓷天线辐射信号的性能，导致通信效果大幅下降。如下图所示，上面三种布局是正确的，下面三种布局是违反规范的。

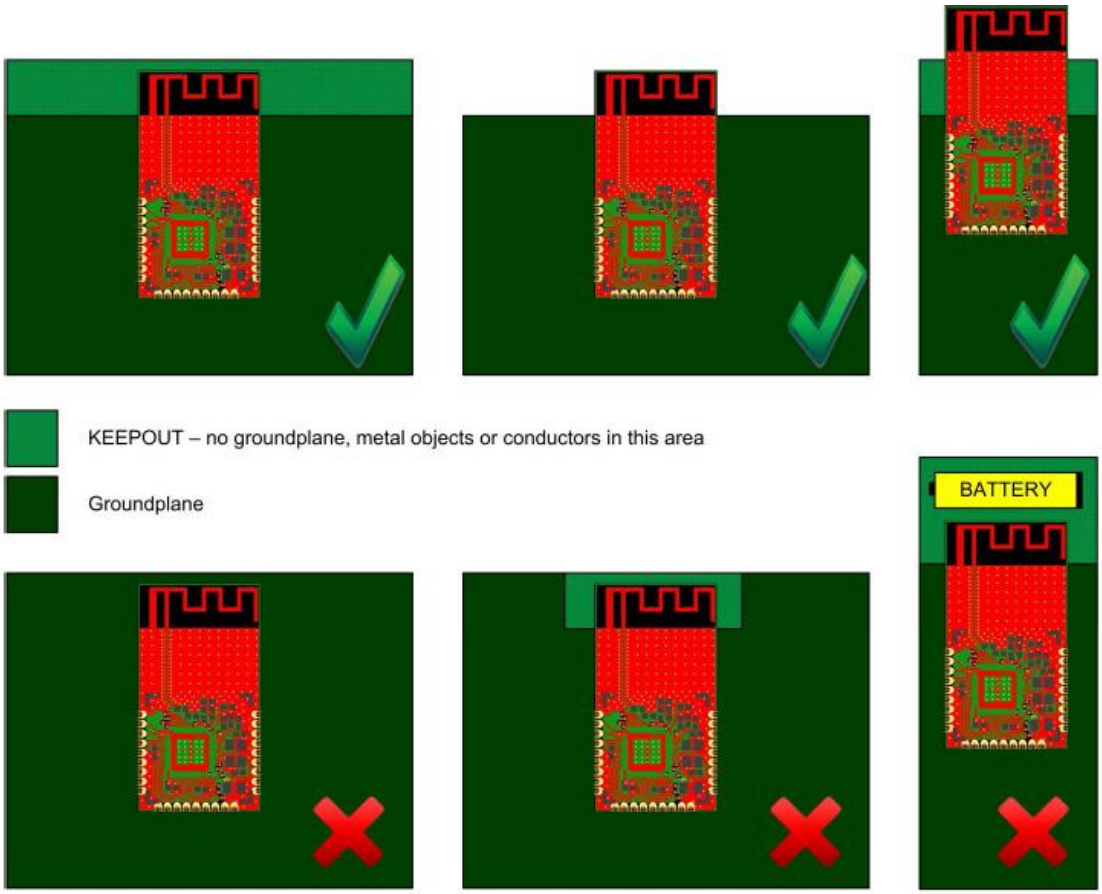

图 2.3 PCB 天线布局规范

2.5.2 外接天线布局

ZM516X 系列模块部分型号带 uFI 天线接口，可外接棒状天线、车台天线等，在使用这类天线时请注意以下几点：

（1） 使用的天线必须保证能工作于 2.4GHz 频段，驻波比（VSWR）建议在 1.5 以下。

（2） 外接天线尽量勿贴近地面、墙面、金属表面，至少保持 30CM 的间距。

（3） uFI 天线接口的模块必须连接天线后方可使用，否则会因能量无法辐射损坏产品。

（4） 吸盘天线应保证其正常吸附于金属表面，以达到最佳通信效果。

（5） 如果发现天线馈线有折损，请停止使用。

2.6 生产制造

2.6.1 推荐回流焊温度曲线

ZM516X 系列产品在回流焊过程中，建议遵循表 2.4 及焊料制造商指南进行操作。

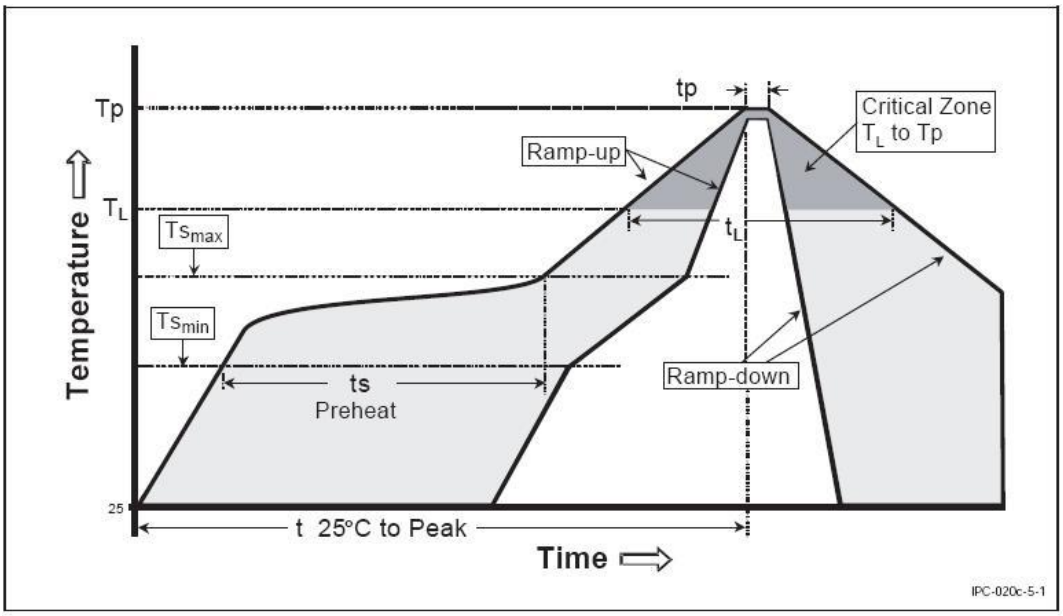

图 2.4 推荐的回流焊温度曲线

表 2.4 回流焊温度与接触时间

Profile Feature	曲线特征	Sn-Pb Assembly	Pb-Free Assembly
Solder Paste	锡膏	Sn63/Pb37	Sn96.5/Ag3/Cu0.5
Preheat Temperature min (Tsmin)	最小预热温度	100℃	150℃
Preheat Temperature max (Tsmax)	最大预热温度	150℃	200℃
Preheat Time (Tsmin to Tsmax) (ts)	预热时间	60-120 sec	60-120 sec
Average ramp-up rate (Tsmax to Tp)	平均上升速率	3℃/second max	3℃/ second max
Liquidous Temperature (TL)	液相温度	183℃	217℃
Time (tL) Maintained Above (TL)	液相线以上的时间	60-90 sec	30-90 sec
Peak temperature (Tp)	峰值温度	220-235℃	230-245℃
Average ramp-down rate (Tp to Tsmax)	平均下降速率	6℃/ second max	6℃/ second max
Time 25℃ to peak temperature	25℃到峰值温度的时间	6 minutes max	8 minutes max

3. FastZigBee 组网协议

由于 ZigBee 无线协议栈的复杂性，以往用户基于 ZigBee 无线协议栈自行开发时，多缺乏对 ZigBee 协议栈的深入认识，导致产品开发周期长、开发难度大，且始终存在网络性能不稳定等诸多隐性问题。这也是我司研发 FastZigBee 协议的初衷，以提供用户稳定可靠的实用型协议。

3.1 网络拓扑

FastZigBee 组网协议是广州致远电子根据多年用户的实际应用，基于 ZigBee 协议栈开发的一套私有透传协议，采用全透传组网通讯，可构建多种型态的网络拓扑结构如图 3.4 FastZigBee 网络拓扑结构所示，其最大的特点是实用性极强、传输效率高、性能可靠稳定、工程布网灵活。

- **P2P 结构**

点对点（P2P）结构是最基本的拓扑结构，可构建两个系统或进程之间的专用通信链路，该方式节点参数基本固定，只要将两节点目标互相指向即可实现通信。

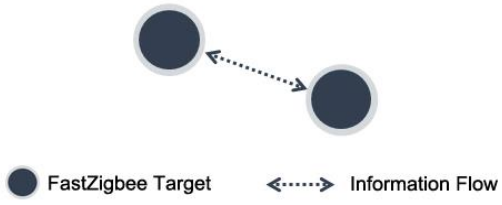

图 3.1　FastZigBee P2P 结构

- **星型网络拓扑结构**

星型拓扑结构也称主从结构，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行控制管理，各节点间的通信都要通过中心节点。一般由主控制中心不断切换通信目标进行轮询控制。

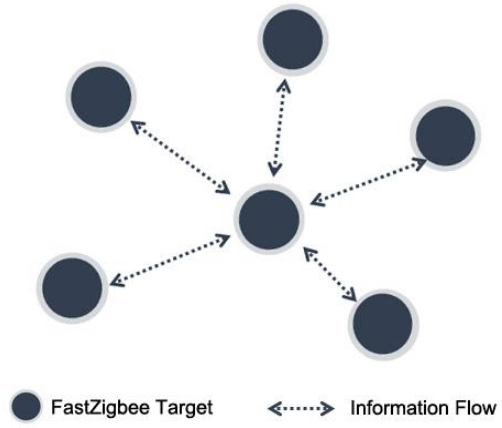

图 3.2　FastZigBee 星型网络拓扑结构

- **中继路由结构**

FastZigBee 还提供一种极其优越的网络扩展方式，当两节点间距离超出可通信距离时，只要在两节点间加入路由设备，其他任何网络参数均不需修改，即可恢复通信，该路由方式对工程施工具有重要意义。如图 3.3 FastZigBee 中继路由结构 为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。

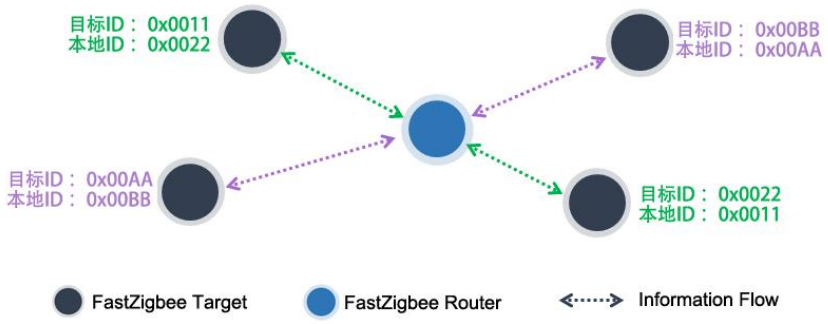

图 3.3 FastZigBee 中继路由结构

- **多级组网拓扑**

多级组网拓扑也称混合型网络，其具备星型网络的简洁与低功耗，也兼备树形网络和 MESH 网络超远距离传输及自修复能力。在混合型网络中，路由器组成网状结构，而无线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。

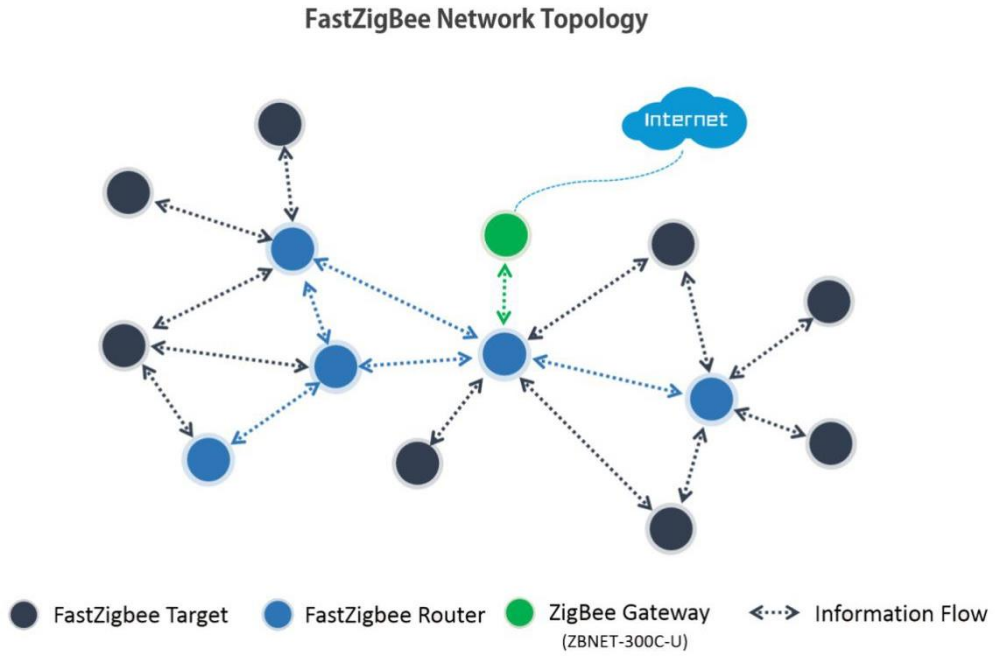

图 3.4 FastZigBee 网络拓扑结构

3.2 节点类型说明

FastZigBee 设备类型分终端设备（Target）和路由设备（Router）两种，角色说明如表 3.1 FastZigBee 协议节点类型说明，并且整个网络可通过 ZigBee 网关（如 ZBNET-300C-U）接入互联网。

表 3.1 FastZigBee 协议节点类型说明

节点类型	说明
终端设备（Target）	（1）终端设备的主要任务是发送和接收消息； （2）终端设备可使用电池供电，为了节省功耗，无数据收发时可以进入休眠状态，在需要收发数据时，可通过 MCU 唤醒进入工作状态。
路由设备（Router）	（1）路由设备允许其他节点与它相连，以扩大网络的覆盖范围，主要任务为转发报文，起中继路由作用。并具备终端设备的所有功能； （2）路由器一般情况必须保持活动状态，以保证终端报文可实时转发，因此一般不进入休眠状态； （3）如果一节点通往另一节点存在多条路径，那么当其中一条路径出现故障时，网络会自动调整到其他路径进行传输，以确保数据到达。 * 注意：ZigBee 网络内并不是存在越多路由器而网络越稳定，ZigBee 通信效率会随路由级数的增加而下降，所以路由器必须按需布局。

3.3 透明传输

FastZigBee 采用全透明传输方式，透明传输：即发送方和接收方数据的长度和内容完全一致，相当于一段无形的传输线。如图 3.5 透明传输示意图，例如从 A 节点发送一串字符到 B 节点，在传输的整个过程将不加任何修饰。

图 3.5 透明传输示意图

透明传输的优势在于，用户可以在这基础上，创建自己需要的协议格式，使用户不局限于固定使用第三方协议。

3.4 软体基本配置参数

FastZigBee 协议提供丰富的可配置参数，用户可根据实际的应用需求灵活运用，以构建不同形式的网络。如表 3.2 FastZigBee 主要配置参数所示，以下所有配置参数均可通过 FastZigBee 配置工具或 AT 指令进行配置。

表 3.2 FastZigBee 主要配置参数

配置信息	参数范围	功能说明
PanID	0x0000~0xFFFF	即 ZigBee 局域网 ID，节点用于判断自身所属网络的标识。可互相通信的节点，PanID 必须相同。且必须保证同一工作区域内的相邻网络 PanID 不同。
本地网络地址	0x0000~0xFFFF	节点短地址，用于区分网络中的各个节点，在同一 PanID 下，本地网络地址必须唯一，引入短地址主要目的是提高 ZigBee 的通信效率。
目标网络地址	0x0000~0xFFFF	当前的通信目标，可通过 AT 指令随时切换
本地物理地址	64bit MAC	模块 MAC 地址，全球唯一标识，不支持修改 FastZigBee 协议不使用
目标物理地址	64bit MAC	FastZigBee 协议不使用
设备类型	0，1	0 = 终端设备 ， 1 = 路由设备
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，以避免相互干扰导致通信效率降低。 例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 CH15、20、25、26，以有效避开干扰。
发送模式	0，1	0 = 单播模式，只有目标地址对应节点才能收到发送的数据 1 = 广播模式，同 PanID 下，所有节点均能收到发送的数据
传输速率	250kbps	ZigBee 无线通信速率固定为 250kbps
发送功率	0~3 级	FastZigBee 设置 0~3 的 4 个功率等级，对应的 P0 模块的发射功率为：-32dBm、-20 dBm、-9 dBm、2.5 dBm；对应的 P2 模块的发射功率为：-12dBm、0 dBm、10 dBm、20dBm；
发送重试次数	0x00~0xFF	数据发送失败后，尝试重新发送的次数，用于保证数据的有效到达，可设置 0~255 次。 提示：模块提供 ACK 指示引脚，用户亦可判断该引脚检测数据是否成功到达。
重试间隔时间	0x00~0xFF(ms)	数据发送失败后，尝试重新发送的时间间隔，可设 0~255ms。

4. 配置工具

ZM516X 系列模块提供了简易的图形配置工具，用户通过该配置工具可以方便地对模块的运行参数进行配置，配置的参数掉电可保存。用户可自行前往我司官网 www.zlg.cn/wireless/down/down/id/13.html 下载“Zigbee 配置工具 WirelessCfg”并解压后安装到自己的电脑。

配置步骤：

1) 把模块的串口通过 RS232 电平转换后，连接到电脑的串口，或者使用我司的评估板通过 USB 连接电脑，上电，打开 WirelessCfg 配置软件，界面如图图 4.1 所示，在打开的【连接】标签页，【设备类型】选择 ZigBee；串口号选择电脑对应的串口，波特率选择模块对应的波特率值（ZM 系列模块出厂默认值为 115200）、数据位、停止位、校验位根据模块的串口参数进行设定（出厂默认值如图），超时时间设置为 2000ms，这个是某些操作如连接设备等发命令后等待应答的最长时间。设定好串口参数后，点击【打开串口】按钮，如图 4.1 所示。

图 4.1 设定配置串口

2) 点击【连接设备】，会弹出对话框，提示“设备连接成功”，点击确定；然后点击【设备配置】，进入可读取、修改模块参数的页面，如图 4.2 所示。如需更改模块的参数，在属性窗口修改后，点击【保存配置】，模块即可按照更改后的配置投入使用，如更改波特率，则需在【连接】页面关闭串口，修改波特率后重新打开串口、连接设备，才能重新读取配置信息。

图 4.2 模块配置

3) 以两个模块相互通信为例，说明如何使用配置工具修改模块配置信息。

取出两块评估板（含 ZM 模块）或者用户自行设计的板子，两个评估板都接上天线或者通过 20dB 衰减器+射频同轴线的方式连接，这里需要特别注意的是：对于 P1/P2 模块，最大的输入功率为+5dBm，两天线不要放置的过近，用同轴线连接时注意衰减量的大小，保证模块不会因为接收功率过大而烧坏。

然后通过 USB 连接电脑，按照前面所述的配置步骤分别读出两个模块的配置信息，接着就是修改配置信息，如图 4.3 所示，图示是打开两个配置工具界面叠放了一部分的显示效果。以单播模式为例，这里注意红色方框的配置需保持一致，红色圆框的本地地址和目标地址交叉一致（如果是广播模式，需保证通道号和网络号一致即可）。

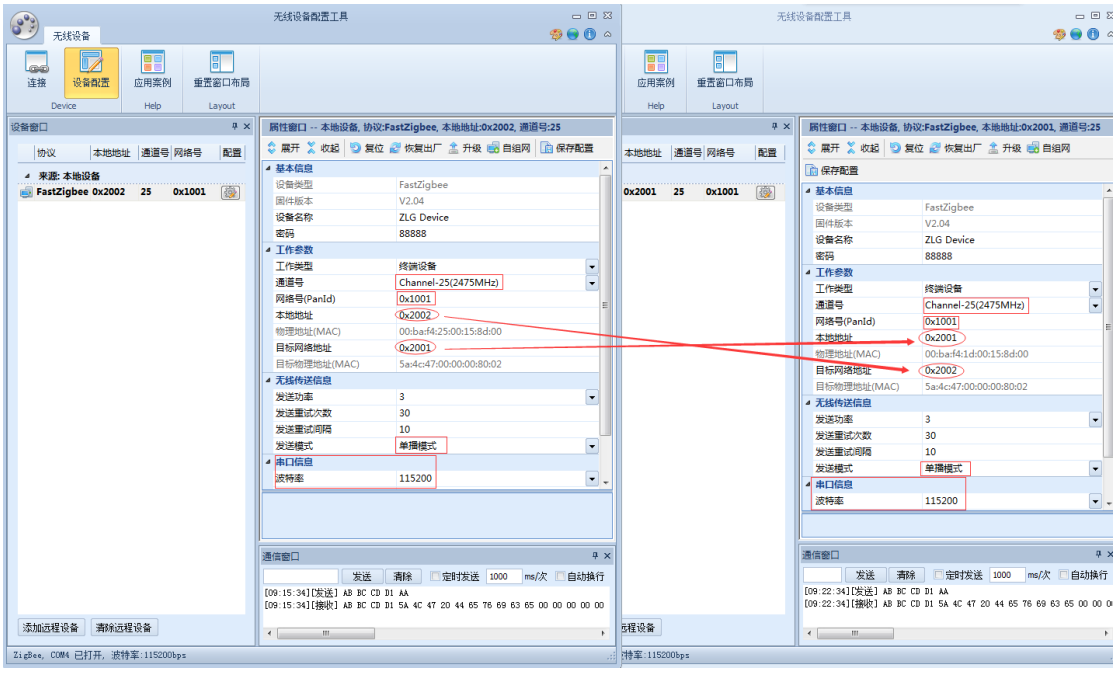

图 4.3 收发模块的配置

4) 配置工具有通信窗口，可以简单使用类似串口助手的收发功能，发送 16 进制数据（如需发送十进制数据，则使用串口助手），如图 4.4 的红色框所示。

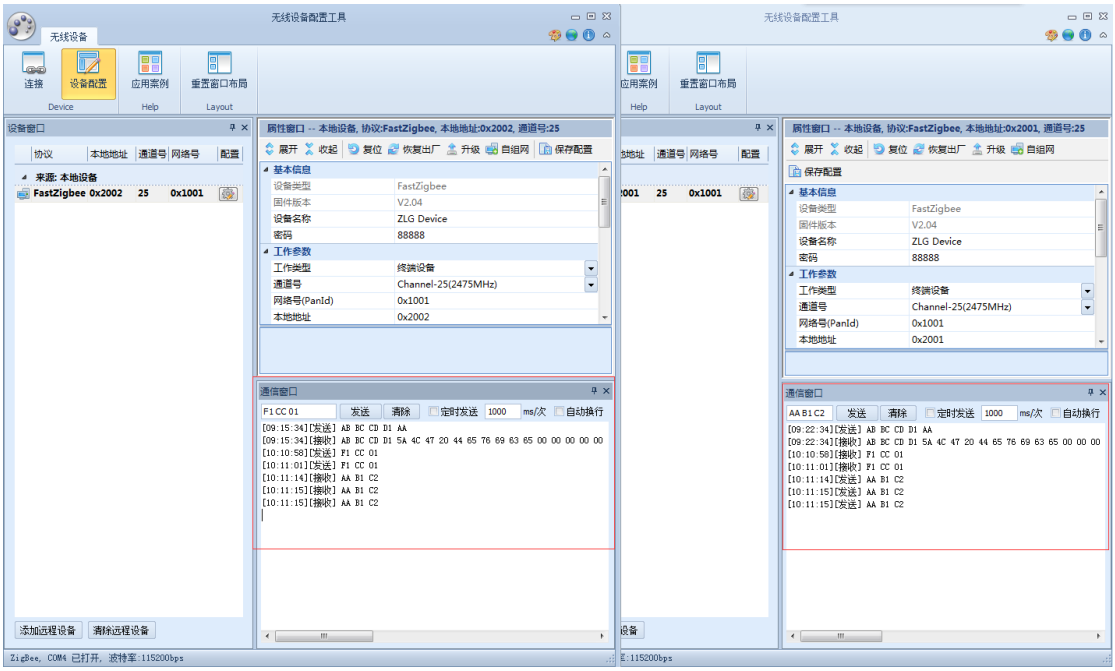

图 4.4 用通信窗口收发数据

5. 参数配置协议

用户与 ZM516X 模块之间的串口协议包括**临时的参数配置协议**和**永久的参数配置协议**。用户可根据不同的需求使用不同的参数修改方式。

- 临时的参数配置协议是用于即时修改模块参数，不写入到模块的 Flash 存储器，掉电不保存；
- 永久的参数配置协议会将模块的参数保存到模块的 Flash 内，掉电保存，使用配置工具进行的配置是修改永久的参数配置。

注意：使用命令前请确认模块运行的固件为 FastZigBee 固件，且版本在 V2.04 以上，固件版本向下兼容，但低于该版本号的固件，可能存在部分功能无效。确认方法如下：

使用 WirelessCfg 配置工具，点击【连接设备】获取模块目前的固件类型，确认模块固件是否为“FastZigBee 设备”。

图 5.1　获取模块固件类型

然后在获取模块详细信息页面查看对应的固件版本信息，如图 5.2，或者可以通过串口发送读取本地配置命令 AB BC CD D1 05，根据回复命令最后两个字节查看。

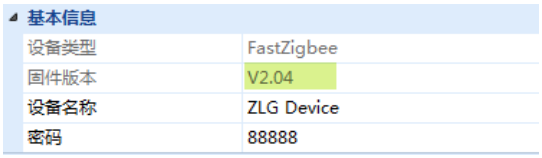

图 5.2　查看固件版本信息

5.1 临时参数配置协议

ZM516X 模块临时的参数配置协议命令帧格式如表 5.1 所示。

表 5.1 临时参数配置命令

3 字节（协议标志）	1 字节	N 字节
DE DF EF	功能码	参数

临时的参数配置帧应答返回如表 5.2 所示。

表 5.2 临时配置命令应答

3 字节（协议标志）	1 字节	1 字节
DE DF EF	功能码	返回值

临时的参数配置协议功能码表如表 5.3 所示。

表 5.3 临时参数配置功能码

功能码	功能描述	命令长度	参数	返回值	说明
0xD1	修改通道	5	1 字节通道号： 0x0B～0x1A	0x00：修改成功 0x06：超出范围	
0xD2	修改目的网络地址	6	2 字节网络地址： 0x0000~ 0xFFFF	0x00：设置成功 其它：设置失败	
0xD3	包头显示源地址	5	0x00：不显示 0x01：显示	0x00：设置成功 其它：设置失败	设置成功后收到的数据包前 2 字节为数据包源节点的网络地址
0xD4	设置 IO 输入输出	7	2 字节地址 + 1 字节 IO 输入输出 第 0~7 位=IO0~IO7 1 = 输出 0 = 输入	0x00：设置成功 其它：设置失败	可设置本地 IO 或远程 IO
0xD5	读取 IO 状态	6	被读节点的地址	1 字节 IO 状态 第 0~7 位 =IO0~IO7 1 = 高电平 0 = 低电平	可读取本地 IO 或远程 IO 需先将 IO 口设置成输入状态
0xD6	设置 IO 状态	7	2 字节地址+ 1 字节 IO 状态值 第 0~7 位分别代第 0~7 位=IO0~IO7 1 = 高电平 0 = 低电平	0x00：设置成功 其它：设置失败	可设置本地 IO 或远程 IO 需先将 IO 口设置成输出状态
0xD7	读取 AD	7	2 字节地址+ AD 通道号（0~1）	2 字节 AD 值	可设置本地或远程 AD，10 位 AD，参考电压 2.47V

0xD8	进入休眠	5	0x01：深度休眠 其他：无效	接收到此命令之后模块进入休眠状态 无返回值	模块进入休眠后，处于低功耗状态
0xD9	设置通讯模式	5	0x00：单播 0x01：广播	0x00：设置成功 其它：设置失败	
0xDA	查询节点的信号强度	6	0x0000	节点信号强度： 0x00~0xFF	0xFF 信号最强，经过路由无意义
0xDB	修改 PANID	6	2 字节 PANID： 0x0000~ 0xFFFF	0x00：设置成功 其它：设置失败	

5.1.1 命令示例

1. 修改通道号

其功能码为 0xD1，命令长度为 5 个字节，其参数为 1 个字节通道号 0x0B～0x1A。返回值为 0x00，表示修改成功；返回值为 0x06，表示超出范围。即：

```
CMD:  DE DF EF D1 1A/*设置网络通道号为 0x1A*/
RSP:  DE DF EF D1 00
```

2. 修改目的网络地址

其功能码为 0xD2，命令长度为 6 个字节，其参数为 2 个字节网络地址 0x0000~0xFFFF，返回值为 0x00，表示设置成功；返回其它值，表示设置失败。即：

```
CMD:  DE DF EF D2 20 01/*设置目标网络地址为 0x2001*/
RSP:  DE DF EF D2 00
```

3. 包头显示源地址

其功能码为 0xD3，命令长度为 5 个字节，其参数为 0x00，表示不显示；其参数为 0x01，表示显示。返回值为 0x00，表示设置成功；返回其它值，表示设置失败。当设置成功后，则收到的数据包前 2 个字节为数据包源节点的网络地址。即：

```
CMD:  DE DF EF D3 01/*设置包头显示源地址*/
RSP:  DE DF EF D3 00
```

设置显示成功后，当模块收到一帧数据时，数据包的前 2 个字节为数据包源节点的网络地址，如下所示。

```
20 01 31 32 33 34 35 36 37 38 39
```

20 01 为源节点的网络地址，31 32 33 34 35 36 37 38 39 为接收到的数据。

4. 设置 IO 输入输出

其功能码为 0xD4，命令长度为 7 个字节，其参数为 2 字节地址＋1 字节 I/O 输入输出，bit0~bit7 为 IO0~IO7，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。返回值为 0x00，表示设置成功；返回其它值，表示设置失败。可设置本地 I/O 或远程 I/O。即：

```
CMD:  DE DF EF D4 20 01 01/*设置 IO 输入输出*/
RSP:  DE DF EF D4 20 01 00
```

将目标节点 2001 的 IO0 设置成输出，IO1~IO7 设置成输入。

5. 读取 IO 状态

其功能码为 0xD5，命令长度为 6 个字节，其参数为被读节点的地址，1 字节 I/O 状态，bit0~bit7 位为 IO0~IO7。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。即：

CMD: DE DF EF D5 20 01 /*读取 IO 状态*/
RSP: DE DF EF D5 20 01 01

读取目标节点 2001 的 IO 状态。返回状态值 IO0 为高电平，IO1~IO7 为低电平。

6. 设置 IO 状态

其功能码为 0xD6，命令长度为 7 个字节，其参数为 2 字节地址＋1 字节 I/O 状态值，bit0~bit7 位分别代表 IO0~IO7。返回值为 0x00，表示设置成功；返回其它值，表示设置失败。可设置为本地 I/O 或远程 I/O，需先将 I/O 口设置成输出状态。即：

CMD: DE DF EFD620 01 01/*设置 IO 状态*/
RSP: DE DF EFD620 01 00

将目标节点 2001 的 IO0 设置成高电平，IO1~IO7 设置成低电平。

7. 读取 AD

其功能码为 0xD7，命令长度为 7 个字节，其参数为 2 字节地址＋AD 通道号（0~3），返回值为 2 字节 AD 值，可设置本地或远程 10 位 AD，参考电压 2.47V。即：

CMD: DE DF EF D7 20 01 00/*读取 AD 值*/
RSP: DE DF EF D7 20 01 00 9E

读取本地或远程节点 2001 的 CH0 的 AD 值

8. 进入休眠

CMD: DE DF EF D8 01/*模块进入深度休眠*/

休眠命令无返回，进入休眠后不保存临时参数配置，通过复位模块或管脚 19 拉低唤醒。模块被唤醒后，所有管脚将恢复到初始状态。

9. 设置通讯模式

其功能码为 0xD9，命令长度为 5 个字节，其参数为 0x00，表示单播模式；命令参数为 0x01，表示广播模式。返回值为 0x00，表示设置成功；返回值为其它值，表示失败。即：

CMD: DE DF EF D9 00/*设置通讯模式为单播发送模式*/
RSP: DE DF EF D9 00

10. 查询节点的信号强度

CMD: DE DF EF DA 20 02/*获取模块的信号强度*/
RSP: DE DF EF DA 20 02 BA/*获取到的信号强度为 0xBA*/

获取到的信号强度是本机模块与目标模块 2002 之间的信号强度，值的范围为：0~255，值越大，信号越好。

注：所获信号强度是 LQI 链路质量指示的值，还需要对其进行计算转化为接收功率值。其计算公式为 LQI=(接收功率+95)×3，若获取到的值为 0xBA，将其转化为十进制 186，接收功率=186÷3-95=-33dBm。

11. 修改 PANID

CMD: DE DF EF DB 10 00/*设置目标节点的 PANID 为 0x1000*/
RSP: DE DF EF DB 00

固件版本 2.09 及以上版本才支持此功能。

5.2 永久参数配置协议

ZM516X 模块永久的参数配置除了可以使用配置工具进行配置外，也可以使用命令的方式进行配置。

永久的参数配置协议命令帧格式如表 5.4 所示。

表 5.4 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	字节校验

字节校验目前无效，可以是任意数值的一个字节。

永久的参数配置协议共有 7 条命令，命令标识符如表 5.5 所示。

表 5.5 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	
设置通道号	0xD2	
搜索	0xD4	
获取远程配置信息	0xD5	
修改配置	0xD6	设置成功需复位
复位	0xD9	
恢复出厂设置	0xDA	设置成功需复位
模块密码使能	0xDE	恢复出厂设置，不使能模块密码
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

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 5.6 所示。

表 5.6 配置命令响应状态

响应状态	错误码
OK	0x00
LENGTH _FAUSE	0x01
ADDRESS _FAUSE	0x02
CHECK_FAUSE	0x03
WRITE_FAUSE	0x04
OTHER_FAUSE	0x05

5.2.1 命令详细介绍

- **读取本地配置命令**

3 字节（协议标志）	1 字节	1 字节
AB BC CD	D1	校验

读取成功应答如下报文：

3 字节（协议标志）	1 字节	65 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	设备类型	固件版本

DEV_INFO 结构信息如表 5.7 所示：

运行状态：0xAA 该参数保留

固件类型：0x0001 该参数保留

表 5.7 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
DevMode	32	1	设备类型 0: 终端设备 1: 路由设备	终端设备
Chan	33	1	通道号	0x19 （CH 25）
PanID	34	2	网络 ID (PanID)	0x1001
MyAddr	36	2	本地网络地址	0x2001
MyIEEE	38	8	本地物理地址(MAC)	每个模块的具有唯一的 MAC 地址，不可修改
DstAddr	46	2	目标网络地址	0x2002
DstIEEE	48	8	目标物理地址 (保留)	0x00 00 00 00 00 00 00 00
Reserve	56	1	保留	0x00
PowerLevel	57	1	P0 模块的发射功率为：-32dBm、-20 dBm、-9 dBm、2.5 dBm； P2 模块的发射功率为：-12dBm、0 dBm、10 dBm、20dBm；对应 0x00-0x03 档位。	0x03
RetryNum	58	1	发送数据重试次数	0x05
TranTimeout	59	1	发送数据重试时间间隔(单位：10ms)	0x0A
Serial_Rate	60	1	串口波特率[1]	0x07
Serial_DataB	61	1	串口数据位[2]	0x08
Serial_StopB	62	1	串口停止位[3]	0x01
Serial_ParityB	63	1	串口校验位[4]	0x00
Reserve	64	1	发送模式： 0x00 = 单播 0x01 = 广播	0x00

【1】串口波特率：值为 1～7，对应波特率：2400、4800、9600、19200、38400、57600、115200

【2】数据位：5～8

注意：数据位如果设置为 5、6、7 位，则不可以获取配置信息。

【3】停止位：1～2

【4】校验位：0－－无校验

1－－奇校验

2－－偶校验

命令示例：读取本地配置

CMD: AB BC CD D1 05

RSP: AB BC CD D1 5A 4C 47 20 44 65 76 69 63 65 00 00 00 00 00 00 3838 38 38 38 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 07 08 01 00 00 AA 00 01 01 00

- **设置通道号**

模块可工作在 16 个物理通道上，载波频率不同，不同通道的模块彼此间物理不通，可以实现物理上划分网段的效果。

3 字节（协议标志）	1 字节	1 字节	1 字节
AB BC CD	D2	通道号(11~26)	校验

设置成功回应报文如下：

3 字节（协议标志）	1 字节	1 字节
AB BC CD	D2	响应状态

命令示例：修改通道号

CMD： AB BC CD D2 0B 11

RSP： AB BC CD D2 00

- **搜索**

模块接收到本命令后，会向本网段的通道发出广播搜索包，运行本公司固件的 ZigBee 模块（相同通道号和 PANID 的节点）会应答此广播，将自己的相关基本信息返回到搜索发起节点。

3 字节（协议标志）	1 字节	1 字节
AB BC CD	D4	校验

搜索成功回应报文如下：

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	网络号	本地网络地址	运行状态

命令示例：搜索命令

CMD： AB BC CD D4 08

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

- **获取远程配置信息**

为了获取其他节点的信息，可以通过向本机模块发送此命令。

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

注意：数据位如果设置为 5、6、7 位，则不可以获取配置信息。

远程的节点返回包含自己所有信息的数据包，回应报文如下：

3 字节（协议标志）	1 字节	65 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

命令示例：获取远程配置信息

CMD: AB BC CD D5 20 02 2B

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 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 AA 00 01 01 00

- **修改配置命令**

3 字节（协议标志）	1 字节	2 字节	65 字节	1 字节
AB BC CD	D6	网络地址	DEV_INFO 结构信息	校验

修改本机配置时，只需在命令中填本地网络地址即可。设置成功回应如下报文：

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

响应状态如表 5.6 所示。

命令示例：修改配置命令

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 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 78

RSP: AB BC CD D6 20 01 00

注：命令解析：

AB BC CD D6	/*修改配置命令标识*/
20 01	/*被修改目标模块*/
5A 4C 47 20 44 65 76 69 63 65 00 00 00 00 00 00	/*设备名称*/
38 38 38 38 38 00 00 00 00 00 00 00 00 00 00 00	/*设备密码*/
00	/*设备类型*/
19	/*通道号*/
10 01	/*网络号*/
20 01	/*本地地址*/
00 5B 28 61 00 15 8D 00	/*本地物理地址*/
20 02	/*目标地址*/
00 00 00 00 00 00 00 00	/*目标物理地址*/
00	/*保留*/

03 /*发射功率*/
05 /*重发次数*/
0A /*重试时间间隔*/
07 /*串口波特率*/
08 /*串口数据位*/
01 /*串口停止位*/
00 /*串口校验位*/
00 /*发送模式*/
78 /*校验（目前无效，可设任意一字节数值）*/

修改命令发送后，还需要再向修改前的模块地址发送一次复位命令。

注：修改命令发送后，还需要再想修改前的模块地址发送一次复位命令。

- **复位**

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

命令示例：复位

CMD: AB BC CD D9 20 01 00 01 2F /*复位帧无应答*/

- **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
AB BC CD	DA	网络地址	协议类型	校验

恢复出厂设置帧应答如下报文：

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

响应状态如表 5.6 所示。

命令示例：恢复出厂设置

CMD: AB BC CD DA 20 01 00 01 30
RSP: AB BC CD DA 20 0100 0100

- **模块密码使能**

固件版本 2.09 及以上版本支持此功能。

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，用户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。如果用户忘记了密码，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。模块密码使能的命令为：

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	DE	网络地址	R/W	密码使能	校验

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 字节如果为 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。

返回应答如下报文：

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

响应状态如表 5.6 所示。

命令示例：设置模块密码使能

```
CMD:  AB BC CD DE 20 01 01 01 14                /*  使能模块密码                */
RSP:  AB BC CD DE 20 01 01 00
```

- **模块登录**

固件版本 2.09 及以上版本支持此功能。

当模块使能了密码，用户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。模块登录的命令为：

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

该命令支持读取和设置参数，R/W 字节如果为 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。

返回应答如下报文：

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

响应状态如表 5.6 所示。

命令示例：模块登录

```
CMD:  AB BC CD DF 20 01 01 38 38 38 38 38 38 00 2B   /*  用“88888”密码登录模块   */
RSP:  AB BC CD DF 20 01 00
```

6. 快速上手

本节讲解了两个模块之间相互进行通讯的简单例子。

步骤：

1. 把两个模块的串口分别连接到电脑的串口上，参考第 4 节对两个模块进行配置：

1) 两个模块的 PANID 和通道号必须设置为一致；

2) 两个模块的目的网络地址分别为配置为对方模块的本地网络地址；

3) 同一网络内所有模块的本地地址不能相同。

配置信息如图 6.1 所示。

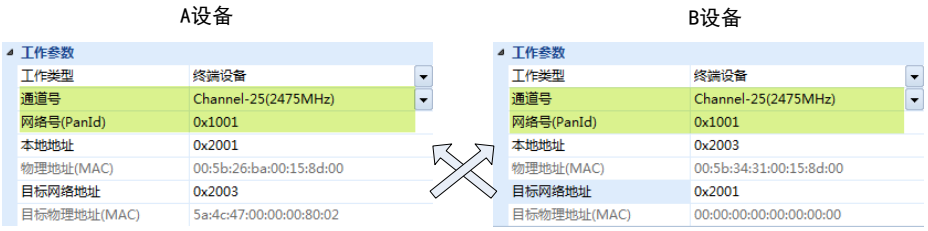

图 6.1 终端设备参数配置

2. 配置完成后关闭配置工具，使用串口调试助手打开连接两个模块的串口，设备连接上后（LINK 管脚变为低电平），两个模块即可进行透明发送数据，如图 6.2 所示。

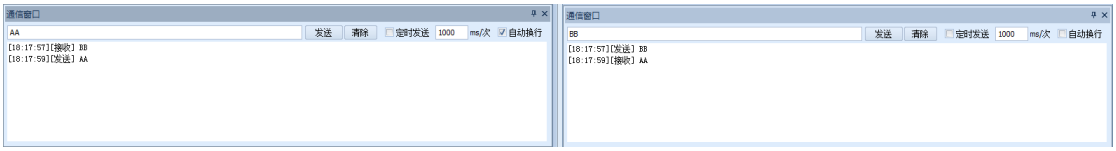

图 6.2　串口通讯测试

7. 免责声明

ZM516X ZigBee 通信模块及相关资料版权均属广州致远电子有限公司所有，其产权受国家法律绝对保护，未经本公司授权，其它公司、单位、代理商及个人不得非法使用和拷贝，否则将受到国家法律的严厉制裁。

本文档提供有关致远电子产品的信息。本文档并未授予任何知识产权的许可，并未以明示或暗示，或以禁止发言或其它方式授予任何知识产权许可。除致远电子在其产品的销售条款和条件中声明的责任之外，致远电子概不承担任何其它责任。并且，致远电子对致远电子产品的销售和／或使用不作任何明示或暗示的担保，包括对产品的特定用途适用性、适销性或对任何专利权、版权或其它知识产权的侵权责任等，均不作担保。致远电子产品并非设计用于医疗、救生或维生等用途。致远电子可能随时对产品规格及产品描述做出修改，恕不另行通知。

ZM516X ZigBee 通信模块可能包含某些设计缺陷或错误，一经发现将收入勘误表，并因此可能导致产品与已出版的规格有所差异。如客户索取，可提供最新的勘误表。

在订购产品之前，请您与当地的致远电子销售处或分销商联系，以获取最新的规格说明。本文档中提及的含有订购号的文档以及其它致远电子文献可通过访问广州致远电子有限公司的万维网站点获得，网址是：www.zlg.cn

广州致远电子有限公司保留在任何时候修订本用户手册且不需通知的权利。

销售与服务网络

广州致远电子有限公司

地址：广州市天河区车陂路黄洲工业区 7 栋 2 楼
邮编：510660
网址：www.zlg.cn

全国销售与服务电话：400-888-4005

全国服务电话：400-888-4005

销售与服务网络：

广州总公司

广州市天河区车陂路黄洲工业区 7 栋 2 楼
电话：(020)28267985　22644261

北京分公司

北京市海淀区知春路 108 号豪景大厦 A 座 19 层
电话：(010)62536178　62635573

深圳分公司

深圳市福田区深南中路 2072 号电子大厦 12 楼
电话：(0755)8364016983783155

武汉分公司

武汉市洪山区广埠屯珞瑜路 158 号 12128 室（华中电脑数码市场）
电话：(027)87168497　87168397

成都分公司

成都市一环路南二段 1 号数码科技大厦 403 室
电话：(028)85439836　85432683

上海分公司：上海

上海市北京东路 668 号科技京城东楼 12E 室
电话：(021)5386552153083451

上海分公司：南京

南京市珠江路 280 号珠江大厦 1501 室
电话：(025)68123923　68123920

上海分公司：杭州

杭州市天目山路 217 号江南电子大厦 502 室
电话：(0571)89719491　89719493

重庆分公司

重庆市九龙坡区石桥铺科园一路二号大西洋国际大厦（赛格电子市场）2705 室
电话：(023)68796438　68797619

西安办事处

西安市长安北路 54 号太平洋大厦 1201 室
电话：(029)87881295　87881296

请您用以上方式联系我们，我们会为您安排样机现场演示，感谢您对我公司产品的关注！