E18-2G4U04B 产品规格书

CC2531 ZigBee USB 无线抓包工具

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

第一章 产品概述

1.1 产品简介

E18-2G4U04B 是亿佰特设计生产的一款体积极小的 USB 接口 2.4GHz 频段的 ZigBee 协议无线抓包工具。

E18-2G4U04B 采用美国德州仪器（TI）公司原装进口 CC2531 射频芯片，芯片内部集成了 8051 单片机及无线收发器，出厂固件支持 TI Packet Sniffer 抓包软件到手即可进行抓包测试，使用 Packet Sniffer 可以快速进行协议分析，用户也可进行二次开发。

1.2 特点功能

- 支持 TI Packet Sniffer，可以快速进行协议分析；
- 理想条件下，通信距离可达 200 m；
- 最大发射功率 2.5mW，软件多级可调；
- 支持 ADC、PWM、GPIO 等外设直驱；
- 内置 32.768kHz 时钟晶体振荡器；
- 支持全球免许可 ISM 2.4GHz 频段；
- 内置低功耗 8051 内核处理；
- 丰富的资源，256KB FLASH，8KB RAM；
- 支持 2.0～3.6V/USB 供电，大于 3.3V 供电均可保证最佳性能；
- 工业级标准设计，支持-40～+85℃下长时间使用；
- 自带 PCB 板载天线，无需再外接天线。

1.3 应用场景

- 智能家居以及工业传感器等；
- 安防系统、定位系统；
- 无线遥控，无人机；
- 无线游戏遥控器；
- 医疗保健产品；
- 无线语音，无线耳机；
- 汽车行业应用。

第二章 规格参数

2.1 极限参数

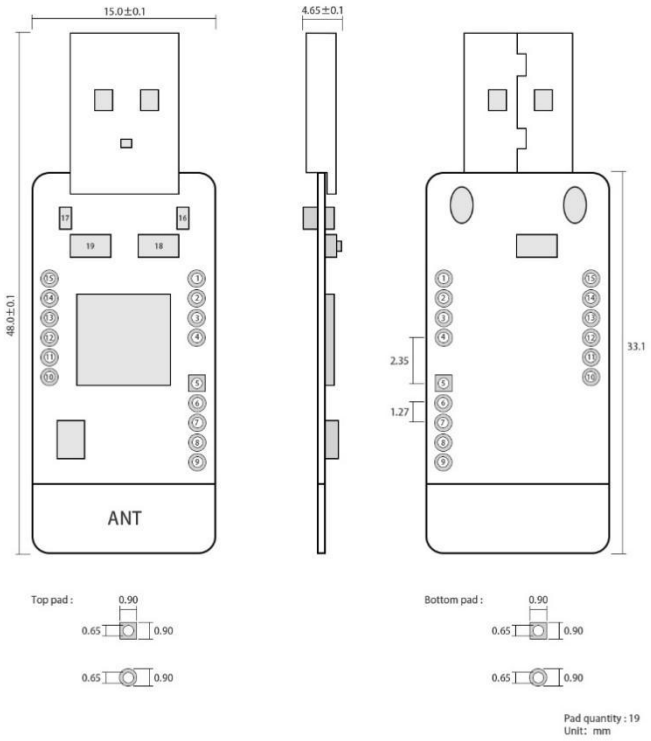
主要参数	性能		备注
	最小值	最大值	
USB 电源供电电压（V）	0	5.5	超过 5.5V 永久烧毁模块
板载电源孔供电电压（V）	0	3.6	超过 3.6V 永久烧毁模块
阻塞功率（dBm）	-	10	近距离使用烧毁概率较小
工作温度（℃）	-40	+85	工业级

2.2 工作参数

主要参数		性能			备注
		最小值	典型值	最大值	
工作电压（V）		2.7	5	5.5	USB 供电
工作电压（V）		2.0	3.3	3.6	板载电源孔供电
通信电平（V）			3.3		使用 5V TTL 有风险烧毁
工作温度（℃）		-40	-	+85	工业级设计
工作频段（GHz）		2.394	-	2.507	支持 ISM 频段
功耗	发射电流（mA）		31.5		瞬时功耗(USB 供电)
	接收电流（mA）		26		USB 供电
	休眠电流（μA）				
最大发射功率（dBm）		3.6	4.0	4.5	
接收灵敏度（dBm）		-95.5	-96.4	-97.5	空中速率为 250kbps

主要参数	描述	备注
参考距离	200m	晴朗空旷环境，高度 2.5 米，空中速率 250kbps
支持协议	ZigBee	
供电方式	USB	
接口方式	1.27mm	
IC 全称	CC2531F256RHAT/QFN40	
FLASH	256 KB	
RAM	8 KB	
内核	8051 微控制器	
外形尺寸	18*59mm	加外壳带帽
天线接口	PCB 板载天线	

第三章 机械尺寸与引脚定义

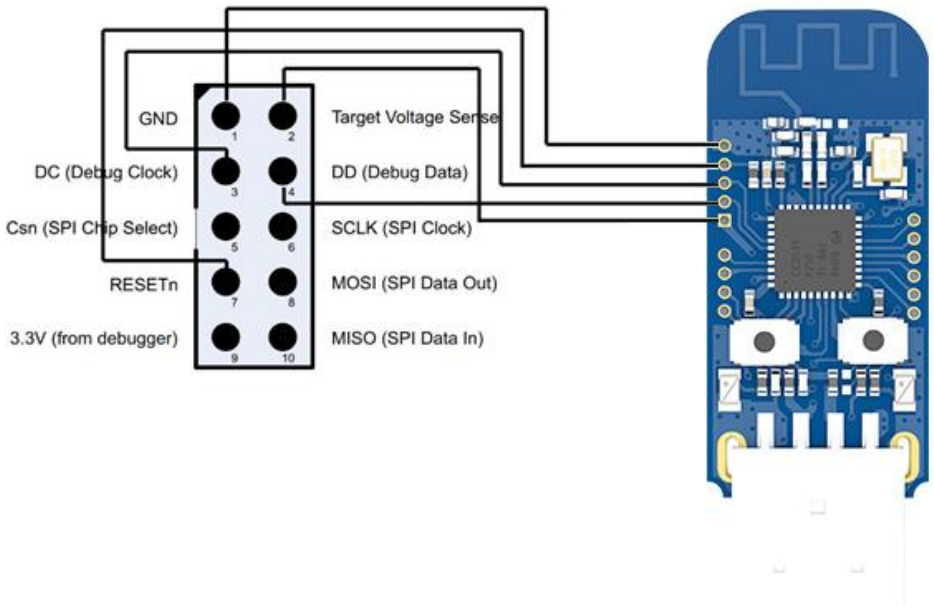


引脚序号	引脚名称	引脚方向	引脚用途
1	P1.4	输入/输出	通用 IO 口（详见 CC2531 芯片手册）
2	P1.5	输入/输出	通用 IO 口（详见 CC2531 芯片手册）
3	P1.6	输入/输出	通用 IO 口（详见 CC2531 芯片手册）
4	P1.7	输入/输出	通用 IO 口（详见 CC2531 芯片手册）
5	VCC	电源	支持电压 2.0～3.6V（尽量避免与 USB 同时供电）
6	DD	输入/输出	程序下载口 P2_1(详见 CC2531 芯片手册)
7	DC	输入/输出	程序下载口 P2_2(详见 CC2531 芯片手册)
8	RESET	输入	复位（产品内部已加复位电路）
9	GND	电源	接地
10	P0.2	输入/输出	通用 IO 口（详见 CC2531 芯片手册）
11	P0.3	输入/输出	通用 IO 口（详见 CC2531 芯片手册）
12	P0.4	输入/输出	通用 IO 口（详见 CC2531 芯片手册）
13	P0.5	输入/输出	通用 IO 口（详见 CC2531 芯片手册）
14	P0.6	输入/输出	通用 IO 口（详见 CC2531 芯片手册）
15	P0.7	输入/输出	通用 IO 口（详见 CC2531 芯片手册）
16	LED	信号指示	连接 CC2531 芯片 P1.1，高电平驱动亮
17	LED	信号指示	连接 CC2531 芯片 P0.0，低电平驱动亮
18	按键	功能按键	连接 CC2531 芯片 P1.3，低电平有效
19	按键	功能按键	连接 CC2531 芯片 P1.2，低电平有效
详细尺寸见该型号 PCB 封装文件，关于模块的引脚定义、软件驱动及通信协议详见 TI 官方《CC2531 Datasheet》			

第四章 使用方法

4.1. 烧录程序

E18-2G4U04B 无线抓包工具内置 8051 单片机，程序下载可使用 CC Debugger；



4.2. TI Packet Sniffer

出厂固件支持 TI Packet Sniffer 抓包软件到手即可进行抓包测试，使用 Packet Sniffer 可以快速进行协议分析。可点击此链接下载：http://www.ebyte.com/pdf-down.aspx?id=1093。

第五章 软件编程

推荐使用适用于无线连接的 Code Composer Studio (CCS) 集成开发环境 (IDE)。

Code Composer Studio 是一种集成开发环境 (IDE)，支持 TI 的微控制器和嵌入式处理器产品系列；Code Composer Studio 包含一整套用于开发和调试嵌入式应用的工具。它包含了用于优化的 C/C++ 编译器、源码编辑器、项目构建环境、调试器、描述器以及多种其他功能。直观的 IDE 提供了单个用户界面，可帮助您完成应用开发流程的每个步骤。熟悉的工具和界面使用户能够比以前更快地入手。Code Composer Studio 将 Eclipse 软件框架的优点和 TI 先进的嵌入式调试功能相结合，为嵌入式开发人员提供了一个引人注目、功能丰富的开发环境。

5.1 TI ZigBee FAQ 常见问题解答

① TI 的 ZigBee 协议栈不同版本的区别，如何选择合适的协议栈进行产品开发？

TI ZigBee 协议栈 Z-Stack 从最开始的 Z-Stack 0.1 到大家熟悉的 Z-Stack 2.5.1a，以及到现在 Z-Stack Home 1.2.1, Z-Stack Lghting 1.0.2, Z-Stack Energy 1.0.1, Z-Stack Mesh 1.0.0. 在协议栈的升级过程 TI 主要对协议栈做了两方面的工作，1) 根据 ZigBee Alliance 的 ZigBee Specification 进行一些新的 Feature 添加，比方说 ZigBee2007 是树形的路由，在 ZigBee Pro 中有了 Mesh 路由，并且提出了 MTO 和 Source Routing 等路由算法，所以 TI 的把相应新的功能添加到协议栈上去。当然有一部分是 Spec 中相关 bug 的修正，比方说有些描述模棱两可的；2) TI ZigBee 协议栈本身软件 bug 的修复。一个版本的协议栈相对于之前一个版本协议栈的区别，都可以在协议栈安装目录下的 Release Note 中找到。

在 Z-Stack 2.5.1a 以后，TI 的协议栈并没有继续以 Z-Stack 2.6.x 的形式直接发布，而是按照 Application Profile 的方式来发布了，原因在于 TI 希望开发者根据实际的应用选择更有针对的性的协议栈进行开发。像 Z-Stack Home 1.2.1 之类的协议栈，主要包括两部分，1）核心协议栈 Core Stack，这部分起始就是之前的 Z-Stack 2.5.1a 以后的延续版本，可以在协议栈安装目录下 Z-Stack Core Release Notes.txt 文件中找到，Version 2.6.2 。2）应用协议栈 Profile 相关，这部分主要跟实际应用相关的，Home Automation 协议栈里都是 ZigBee Home Automation Profile 相关的实现。同样 Z-Stack Lghting 1.0.2 和 Z-Stack Energy 1.0.1 也是一个 Core Stack 再加上应用上的 Profile。

1)Z-Stack Home 1.2.2a 针对智能家居相关产品的开发

2)Z-Stack Lighting 1.0.2 针对 ZLL 相关产品的开发

3)Z-Stack Energy 1.0.1 针对智能能源，Meter, In Home Display, 等相关产品的开发

4)Z-Stack Mesh 1.0.0 针对相关私有应用的产品的开发，只利用标准 ZigBee 协议相关功能，Mesh 路由等，应用层有开发者自己定义。

在 ZigBee 联盟发布 ZigBee 3.0 协议以后，最新的 ZigBee 协议栈是 Z-Stack 3.0, 目前支持的设备有 CC2530 和 CC2538。

② 产品如何进行标准 ZigBee 测试认证，需要了解哪些，需要走什么流程？

以开发标准 ZigBee Home Automation 相关产品为例。首先开发者开发产品时要按照 ZigBee Home Automation Profile Specification 中描述的产品进行开发，这个文档可以在 www.zigbee.org 下载到。在完成产品的开发后，开发着需要了解 ZigBee Home Automation Profile Test Specification, 这个文档描述了一个特定产品需要在 Test House 过的相关测试项，文档也可以在 www.zigbee.org 下载到，另外除了以上两个文档以外还有一个 PICS 文档，这个文档专门用于描述需要过认证测试产品所支持的功能，开发者根据开发产品的实际功能，和 Specification 中所要求的功能，在文档中进行打钩确认。下面是测试的流程，

1) 首先加入 ZigBee 联盟，一般可以有测试实验室帮助完成。

2) 寄送样品到测试实验室，完成 PICS 文档的填写。

3) 第一轮预测试，测试实验室对测试结果反馈，开发者修改样品代码。

4) 测试实验室对修改后的样品进行验证，然后开始正式测试。

5) 测试实验室协助开发者完成 ZigBee 联盟网上认证申请资料的准备和提交。

6) 测试实验室提交正式测试报告给 ZigBee 联盟。联盟会完成审核并发证

目前国内可以完成标准 ZigBee 测试的测试实验室有两家

1) CESI 北京 中国标准化电子研究所。

2) Element 深圳办事处(总部在英国)

详细可以参考下面的 wiki 地址，

http://processors.wiki.ti.com/index.php/ZigBee_Product_Certification_Guide

③ 设备的 64 位 MAC 地址是怎么样选取的？

在 CC2530/CC2538/CC2630 中分为两个 IEEE 地址，一个称为 Primary IEEE 地址，另外称为 Secondary 地址。Primary IEEE 地址是存放在芯片的 Information Page 里面，这个地址是 TI 向 IEEE 协会购买的，每个芯片的地址都是唯一的。并且用户只能 Read 这个值，没办法擦除/修改。在协议栈中直接通过读地址可以获得 osal_memcpy(aExtendedAddress, (uint8 *)(P_INFOPAGE+HAL_INFOP_IEEE_OSET), Z_EXTADDR_LEN)。Secondary 地址是存放在 CC2530 里的 Flash 最后一个 Page 里面，用户可以进行 Read/Write. 通过函数 HalFlashRead(HAL_FLASH_IEEE_PAGE, HAL_FLASH_IEEE_OSET, aExtendedAddress, Z_EXTADDR_LEN);。

协议栈运行是，是如何选择 Primary IEEE 地址或者 Secondary 地址作为设备的 MAC 地址的，具体在函数 zmain_ext_addr(void)操作。

1) 从 NV 中读取 IEEE 地址，如果已经存在(都不为 0xFF)，就使用该地址作为 MAC 地址了。

2) 如果 1)中没有，从 Secondary IEEE 地址存放位置读取，如果有(都不为 0xFF)，把该地址写入到 NV 中，以后就用该地址作为 MAC 地址了。

3) 如果 2)中没有，从 Primary IEEE 地址存放位置读取，如果有(都不为 0xFF)，把该地址写入到 NV 中，以后就用该地址作为 MAC 地址了

4) 如果 3)中没有，就随机产生一个 64 位的变量，写入到 NV 中，并作为 MAC 地址。

④ 如何能够禁止节点持续搜索网络，或者把发送 Beacon Request 间隔增大？

End Device 是低功耗设备，有电池供电，节点在断网以后，如何能够禁止节点持续搜索网络，或者把发送 Beacon Request 间隔增大

1)启动搜索网络 uint8 ZDApp_StartJoiningCycle(void)

停止搜索网络 uint8 ZDApp_StopJoiningCycle(void)

2) 更改发送 Beacon Request 的周期

修改变量 zgDefaultStartingScanDuration

```
// Beacon Order Values
#define BEACON_ORDER_NO_BEACONS     15
#define BEACON_ORDER_4_MINUTES      14  // 245760 milliseconds
#define BEACON_ORDER_2_MINUTES      13  // 122880 milliseconds
#define BEACON_ORDER_1_MINUTE       12  //  61440 milliseconds
#define BEACON_ORDER_31_SECONDS     11  //  30720 milliseconds
#define BEACON_ORDER_15_SECONDS     10  //  15360 MSecs
#define BEACON_ORDER_7_5_SECONDS     9  //   7680 MSecs
#define BEACON_ORDER_4_SECONDS       8  //   3840 MSecs
#define BEACON_ORDER_2_SECONDS       7  //   1920 MSecs
#define BEACON_ORDER_1_SECOND        6  //    960 MSecs
#define BEACON_ORDER_480_MSEC        5
#define BEACON_ORDER_240_MSEC        4
#define BEACON_ORDER_120_MSEC        3
#define BEACON_ORDER_60_MSEC         2
#define BEACON_ORDER_30_MSEC         1
#define BEACON_ORDER_15_MSEC         0
```

⑤ 如何让 End Device 进入低功耗状态，休眠时间是如何设定的？

在协议栈宏定义中使能 POWER_SAVING 后，然后在 f8wConfig.cfg 文件里面把-DRFD_RCVC_ALWAYS_ON=FALSE，就可以让 End Device 进入休眠状态。

关于休眠的时间是有 OSAL 操作系统的调度来决定，每次休眠时间都是按照最新会发生的一个 Event Timeout 作为休眠时间。具体在协议栈 hal_sleep 函数中有说明。

这个 timeout 主要分为两类，一类是应用层事件的 timeout，另外一类是 MAC 层事件的 timeout，

1)应用层的 timeout 的时间，是在 osal_pwrmgr_powerconserve(void)函数中，通过 osal_next_timeout();获得的。

2)MAC 层的 timeout 时间，是通过 halSleep(uint16 osal_timeout)函数里面，通过 MAC_PwrNextTimeout();来获得的。

⑥ ZigBee 3.0 协议栈有哪些新的东西？

请参考下面链接，介绍了 ZigBee 3.0 协议栈相对于之前 ZigBee Home Automation/ZigBee Light Link 所增加的东西。

http://processors.wiki.ti.com/index.php/What%27s_New_in_ZigBee_3.0

TI ZigBee 协议栈中关于终端设备的状态机切换

http://www.deyisupport.com/question_answer/wireless_connectivity/zigbee/f/104/t/104629.aspx

⑦ 关于 TI 协议栈中 OAD 和 OTA 的区别？

OAD 全称 Over the Air Download, OTA 全称 Over the Air. 这两个实现的功能都一样，都可以叫做对程序的空中升级。在早期的 ZigBee 协议标准中，并没有关于节点程序空中升级方面的标准，但是很多客户都对空中升级有需求，所以 TI 自己开发了一套关于程序空中升级的协议栈，并且命名为 OAD。后来 ZigBee 联盟看到产品对空中升级的需求越来越来，随机也指定了空中升级方面的标准，命名为 OTA，该标准也是参考了 TI 的 OAD 实现方式，做了相关的修改。所以 TI 的早期协议栈中，空中升级叫 OAD，后来的协议栈中跟随 ZigBee 联盟的空中升级协议，就叫 OTA 了。

⑧ 如果开发基于 ZigBee Mesh 网络的私有应用，应该选择哪个协议栈？

很多用户只想把 zigbee mesh 网络的功能运用在自己的系统或者产品中，并不需要完全按照 zigbee 定义的应用层规范来做，特别是一些行业性的应用。针对这样的应用需求，应该如何选择 TI 合适的协议栈进行产品开发呢？

http://www.deyisupport.com/question_answer/wireless_connectivity/zigbee/f/104/t/132197.aspx

第六章 基本操作

6.1 硬件设计

- 推荐使用直流稳压电源对该模块进行供电，电源纹波系数尽量小，模块需可靠接地；
- 请注意电源正负极的正确连接，如反接可能会导致模块永久性损坏；
- 请检查供电电源，确保在推荐供电电压之间，如超过最大值会造成模块永久性损坏；
- 请检查电源稳定性，电压不能大幅频繁波动；
- 在针对模块设计供电电路时，往往推荐保留 30%以上余量，有整机利于长期稳定地工作；
- 模块应尽量远离电源、变压器、高频走线等电磁干扰较大的部分；
- 高频数字走线、高频模拟走线、电源走线必须避开模块下方，若实在不得已需要经过模块下方，假设模块焊接在 Top Layer，在模块接触部分的 Top Layer 铺地铜（全部铺铜并良好接地），必须靠近模块数字部分并走线在 Bottom Layer；
- 假设模块焊接或放置在 Top Layer，在 Bottom Layer 或者其他层随意走线也是错误的，会在不同程度影响模块的杂散以及接收灵敏度；
- 假设模块周围有存在较大电磁干扰的器件也会极大影响模块的性能，跟据干扰的强度建议适当远离模块，若情况允许可以做适当的隔离与屏蔽；
- 假设模块周围有存在较大电磁干扰的走线（高频数字、高频模拟、电源走线）也会极大影响模块的性能，跟据干扰的强度建议适当远离模块，若情况允许可以做适当的隔离与屏蔽；
- 通信线若使用 5V 电平，必须使用电平转换电路，不建议电阻分压电路；
- 尽量远离部分物理层亦为 2.4GHz 的 TTL 协议，例如：USB3.0；
- 天线切不可安装于金属壳内部，将导致传输距离极大削弱。

6.2 软件编写

- 此模块核心为 CC2531，其驱动方式完全等同于 CC2531，用户可以完全按照 CC2531 芯片手册进行操作（详见 CC2531 手册）；
- 推荐使用适用于无线连接的 Code Composer Studio (CCS) 集成开发环境 (IDE)。
- Code Composer Studio 是一种集成开发环境 (IDE)，支持 TI 的微控制器和嵌入式处理器产品系列。Code Composer Studio 包含一整套用于开发和调试嵌入式应用的工具。它包含了用于优化的 C/C++ 编译器、源码编辑器、项目构建环境、调试器、描述器以及多种其他功能。直观的 IDE 提供了单个用户界面，可帮助您完成应用开发流程的每个步骤。熟悉的工具和界面使用户能够比以前更快地入手。Code Composer Studio 将 Eclipse 软件框架的优点和 TI 先进的嵌入式调试功能相结合，为嵌入式开发人员提供了一个引人注目、功能丰富的开发环境。
- 可在芯片空闲时重新初始化寄存器配置以获得更高的稳定性。

第七章 常见问题

7.1 传输距离不理想

- 当存在直线通信障碍时，通信距离会相应的衰减；

- 温度、湿度，同频干扰，会导致通信丢包率提高；
- 地面吸收、反射无线电波，靠近地面测试效果较差；
- 海水具有极强的吸收无线电波能力，故海边测试效果差；
- 天线附近有金属物体，或放置于金属壳内，信号衰减会非常严重；
- 功率寄存器设置错误、空中速率设置过高（空中速率越高，距离越近）；
- 室温下电源低压低于推荐值，电压越低发功率越小；
- 使用天线与模块匹配程度较差或天线本身品质问题。

7.2 模块易损坏

- 请检查供电电源，确保在推荐供电电压之间，如超过最大值会造成模块永久性损坏；
- 请检查电源稳定性，电压不能大幅频繁波动；
- 请确保安装使用过程防静电操作，高频器件静电敏感性；
- 请确保安装使用过程湿度不宜过高，部分元件为湿度敏感器件；
- 如果没有特殊需求不建议在过高、过低温度下使用。

7.3 误码率太高

- 附近有同频信号干扰，远离干扰源或者修改频率、信道避开干扰；
- 电源不理想也可能造成乱码，务必保证电源的可靠性；
- 延长线、馈线品质差或太长，也会造成误码率偏高。

第八章 相关型号

产品型号	芯片方案	载波频率 Hz	发射功率 dBm	测试距离 m	封装形式	产品尺寸 mm	天线形式
E18-MS1-PCB	CC2530	2.4G	4	200	贴片	14.1*23	PCB
E18-MS1-IPX	CC2530	2.4G	4	240	贴片	14.1*20.8	IPEX
E18-MS1PA1-PCB	CC2530	2.4G	20	800	贴片	16*27	PCB
E18-MS1PA1-IPX	CC2530	2.4G	20	1000	贴片	16*22.5	IPEX
E18-2G4M27SI	CC2530	2.4G	27	2500	贴片	16*22.5	IPEX
E18-2G4U04B	CC2531	2.4G	4	200	USB	18*59	PCB

修订历史

版本	修订日期	修订说明	维护人
1.0	2019-1-10	初始版本	Huaa
1.1	2019-3-8	错误修正	Ray
1.2	2023-1-7	错误修正	Bin

关于我们

销售热线：4000-330-990 公司电话：028-61543675
技术支持：support@cdebyte.com 官方网站：www.ebyte.com
公司地址：四川省成都市高新西区西芯大道 4 号创新中心 B333-D347

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