

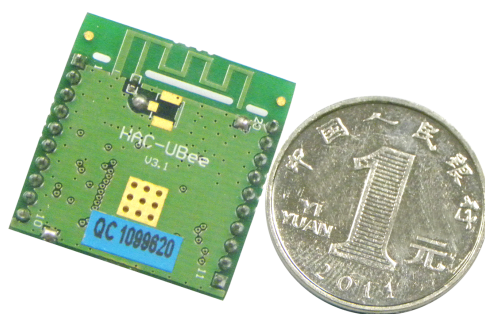
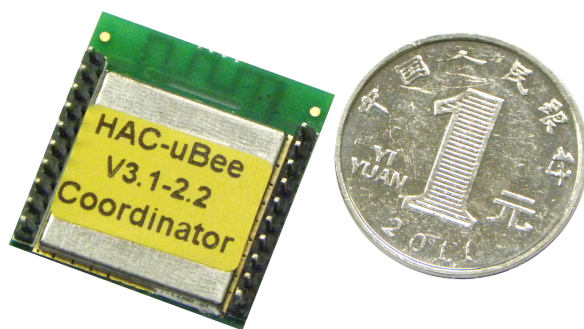


2. 4G 微功率无线数传模块 (基于 ZigBee 协议)

V3.1-2.2

HAC-UBEE

使用手册



传真: +86-755-23981007

地址: 深圳市南山区西丽路 4227 号大学城创意园 2 栋 6 楼

邮箱: koala@rf-module-china.com

网址: www.haccomm.cn www.rf-module-china.com

深 圳 市 华 奥 通 通 信 技 术 有 限 公 司

目 录

一、	HAC-UBee V3.1-2.2 微功率无线数传模块特点.....	2
二、	HAC-UBee V3.1-2.2 微功率无线数传模块的应用.....	2
三、	HAC-UBee V3.1-2.2 微功率无线数传模块的技术规格.....	3
四、	HAC-UBee V3.1-2.2 微功率无线数传模块测试开发.....	5
五、	HAC-UBee V3.1-2.2 微功率无线数传模块的工作模式.....	10
六、	辅助软件.....	35
七、	附录.....	37



一、HAC-UBee V3.1-2.2 微功率无线数传模块特点

HAC-UBee V3.1-2.2 是一款采用 ZigBee 协议栈的微功率无线数传模块，它有以下特点：

- 发射功率 2.5mW (4dBm)；接收灵敏度 -97dBm (BER=10⁻²)

- 开放频段，无需申请频点，载频频率 2.4GHz

- 高抗干扰能力和低误码率

基于 QPSK 的调制方式，采用高效前向纠错信道编码技术，提高了数据抗突发干扰和随机干扰的能力。采用直序扩频技术，有效的抗同频窄带干扰。自带 16 位 CRC 校验，能有效检错

- 空中传输速率高达 250kbps

- 视距情况下，天线置高 2 米，可靠传输距离可达 300 米

- HAC-UBee V3.1-2.2 提供 16 个信道，根据环境自动选择可靠信道通信

- HAC-UBee V3.1-2.2 提供 TTL 电平/UART 接口。波特率出厂为 38400bps，8N1 数据格式

- 功耗：接收电流≤27mA，发射电流≤40mA

- 体积小、重量轻

- 采用 SOC，外围电路少，可靠性高，故障率低

- 提供 PCB 板天线、鞭状天线、IPX 天线连接座等多种天线连接方式

- 适应 2.4GHz IEEE 802.15.4 协议和 ZigBee 应用，自动组网

二、HAC-UBee V3.1-2.2 微功率无线数传模块的应用

HAC-UBee V3.1-2.2 微功率无线数传模块适用于：

- 家庭智能控制

- 无线抄表

- 工业遥控、遥测，自动化数据采集系统

- 安防、报警

- 酒店、机房设备无线监控，门禁系统，人员定位

- 交通、路灯控制

- 物流、有源 RFID、POS 系统，无线手持终端

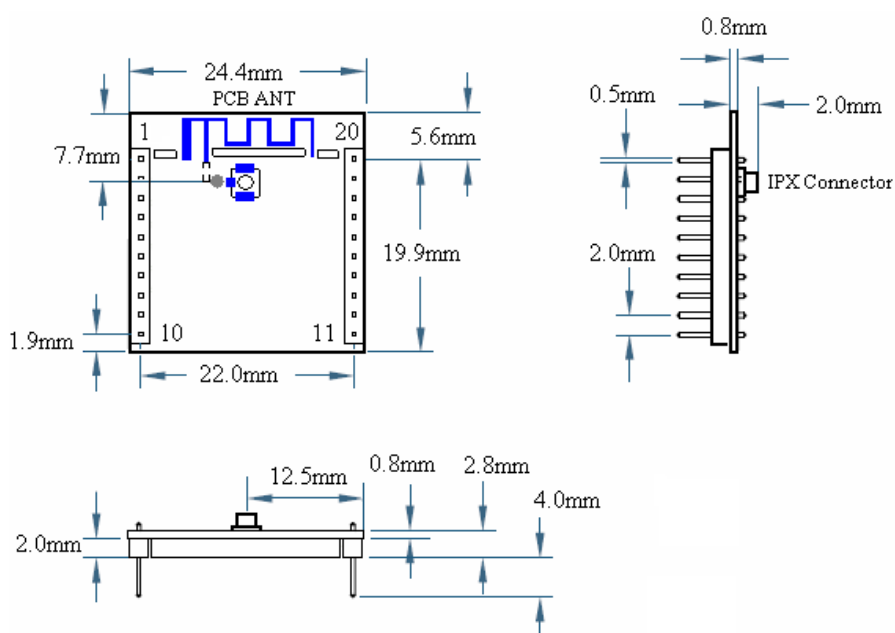
三、HAC-UBee V3.1-2.2 微功率无线数传模块的技术规格

3.1 HAC-UBee V3.1-2.2 规格参数

名称	参数			单位
	最小值	典型值	最大值	
电气性能（25℃）				
供电电压	3.0	3.3	3.6	V
接口电平	-0.3		VCC+0.3≤3.6 V	V
发射电流	36	38	40	mA
接收电流	25	26	27	mA
休眠电流		3		μ A
无线性能（25℃）				
工作频率	2.405		2.485	GHz
发射功率	3.8	4.0	4.2	dBm
接收灵敏度		-97		dBm
无线传输数率		250		Kbps
一般性能				
接口数率	1200	38400	115200	bps
工作温度	-40		80	℃
外型尺寸	25.5 X 24.4 X 4.0			mm

表 3-1

3.2 HAC-UBee V3.1-2.2 外型尺寸((25.5 × 24.4 × 4.0 mm))



3.3 HAC-UBee V3.1-2.2 管脚定义

管脚	定义	输入/输出	功能说明
1	VCC	输入	电源正，3.0~3.6V
2	TXD	输出	串行数据输出
3	RXD	输入	串行数据输入
4	DIO1	输入/输出	数字 I/O1 / 485 使能
5	RESET	输入	低电平复位
6	DIO2	输入/输出	数字 I/O2
7	DIO3	输入/输出	数字 I/O3
8	DIO4/DD	输入/输出	数字 I/O4 / 编程数据
9	DIO5/DC	输入/输出	数字 I/O5 / 编程时钟/休眠使能
10	GND		电源负，地
11	DIO6	输入/输出	数字 I/O6
12	DIO7	输入/输出	数字 I/O7
13	DIO8	输入/输出	数字 I/O8
14	DIO9	输入/输出	数字 I/O9
15	DIO10	输入/输出	数字 I/O10
16	DIO11	输入/输出	数字 I/O11
17	DIO12/ADC3	输入/输出	数字 I/O12/模拟输入 3
18	DIO13/ADC2	输入/输出	数字 I/O13/模拟输入 2
19	DIO14/ADC1	输入/输出	数字 I/O14/模拟输入 1
20	DIO15/ADC0	输入/输出	数字 I/O15/模拟输入 0

表 3-2

3.4 HAC-UBee V3.1-2.2 配件选购

1) 标准配置。

标准 HAC-UBee V3.1-2.2 版出厂自带 PCB 印制板天线，不含 IPX 天线座。



2) 选配线状天线 (Chip 天线), 型号 HAC-Antenna-CH2400。

使用线状天线需断开 PCB 天线连接, 并与线状天线的焊盘连接, 此配置不含天线座。



3) 选配馈线转接外置天线的方式。

产品外壳屏蔽较强的适合这种方式。模块上加焊 IPX 天线座, 同时需要断开 PCB 天线连接, 并将信号引到 IPX 天线座上。也可以不要 IPX 天线座, 直接焊接馈线, 这种方式连接较为牢固, 但不便于运输和装配。焊接馈线的焊盘容易在这过程中受力脱落。

A 使用双头转接馈线 KX-IPEX-10G1-SMA-F, 接外置的 10 公分可折橡胶螺旋天线 HAC-Antenna-LX2400-10-WSMA-M。



HAC-KX-IPEX-10G1-SMA-F



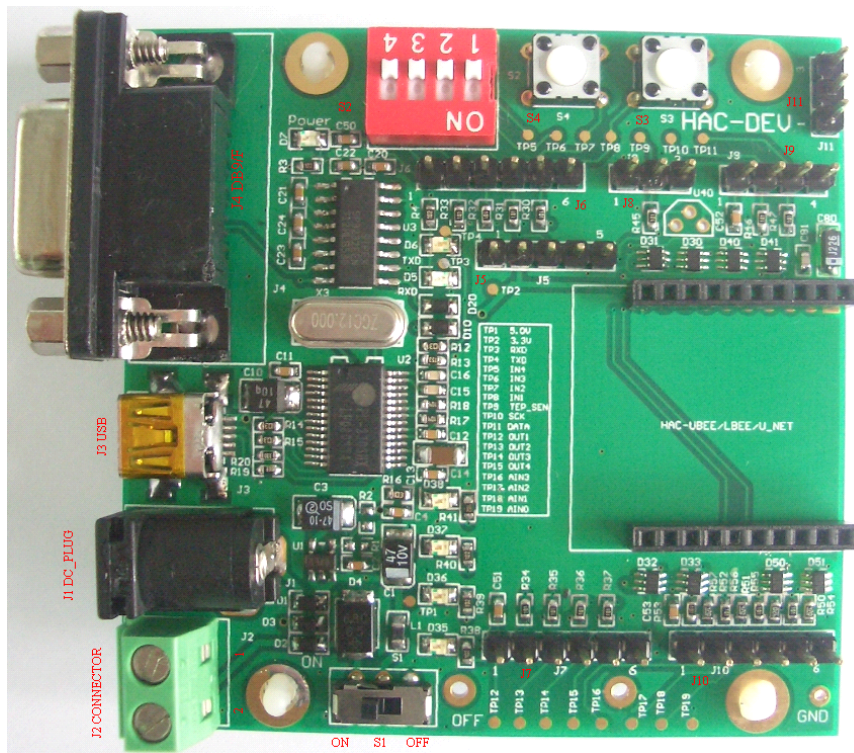
HAC-Antenna-LX2400-10-WSMA-M

B 使用型号 LX2400Z-10-KX-10G1-IPEX 的天线直接连接 HAC-UBee V3.1-2.2 模块。



四、HAC-UBee V3.1-2.2 微功率无线数传模块测试开发

4.1 开发测试板 HAC-DEV 的概述



连接器定义:

- 1) J1 (DC_PLUG) 5V 电源输入
- 2) J2 (DC_CONNECTOR) 5V 电源输入

管脚名	定义
Pin1	GND
Pin2	5V

- 3) J3 (USB_PLUG) USB 接口, USB 口转串口, 驱动程序安装见附件 2

- 4) J4 (DB9/F) RS232 数据接口

管脚名	定义
Pin2	TXD
Pin3	RXD
Pin5	GND
其它脚	无定义

- 5) J5 (Programming) CC2530F256 编程接口

管脚名	定义
Pin1	GND
Pin2	3.3V 输入



Pin3	DD
Pin4	DC
Pin5	RESET

如果有外部供电，**Pin2: 3.3V** 不能连接。

6) J6 (DA_IN) 开关电平输入

管脚名	定义
Pin1	3.3V 输出
Pin2	IN4 开关量输入第 4 路
Pin3	IN3 开关量输入第 3 路
Pin4	IN2 开关量输入第 2 路
Pin5	IN1 开关量输入第 1 路
Pin6	GND

7) J7(DA_OUT) 开关电平输出

管脚名	定义
Pin1	3.3V 输出
Pin2	OUT1 开关量输出第 1 路
Pin3	OUT2 开关量输出第 2 路
Pin4	OUT3 开关量输出第 3 路
Pin5	OUT4 开关量输出第 4 路
Pin6	GND

8) J8(DS18B20) 温度传感器 DS18B20 接口

管脚名	定义
Pin1	GND
Pin2	TEP_SEN
Pin3	GND

9) J9(SENSOR) I²C 接口，外接传感器

管脚名	定义
Pin1	3.3V
Pin2	SCK
Pin3	DATA
Pin4	GND

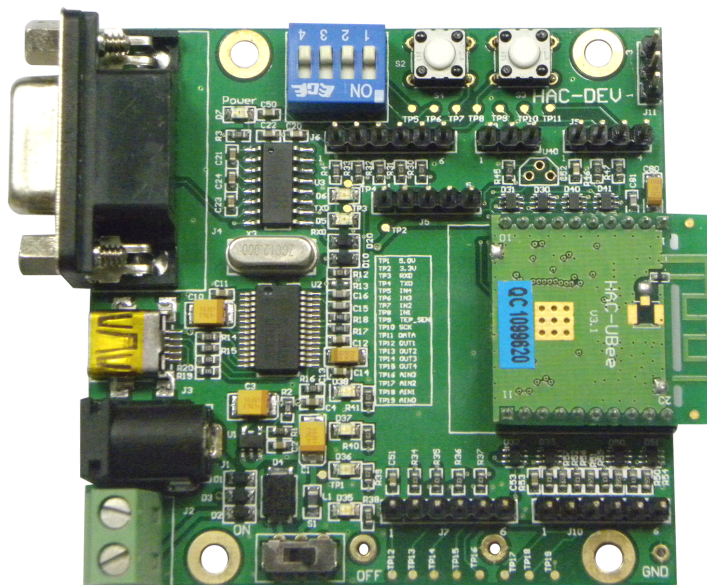
10) J10(Analog Signals IN) 4~20mA 电流信号输入

管脚名	定义
Pin1	3.3V 输出
Pin2	AIN3 电流信号输入第 3 路
Pin3	AIN2 电流信号输入第 2 路
Pin4	AIN1 电流信号输入第 1 路
Pin5	AIN0 电流信号输入第 0 路
Pin6	GND

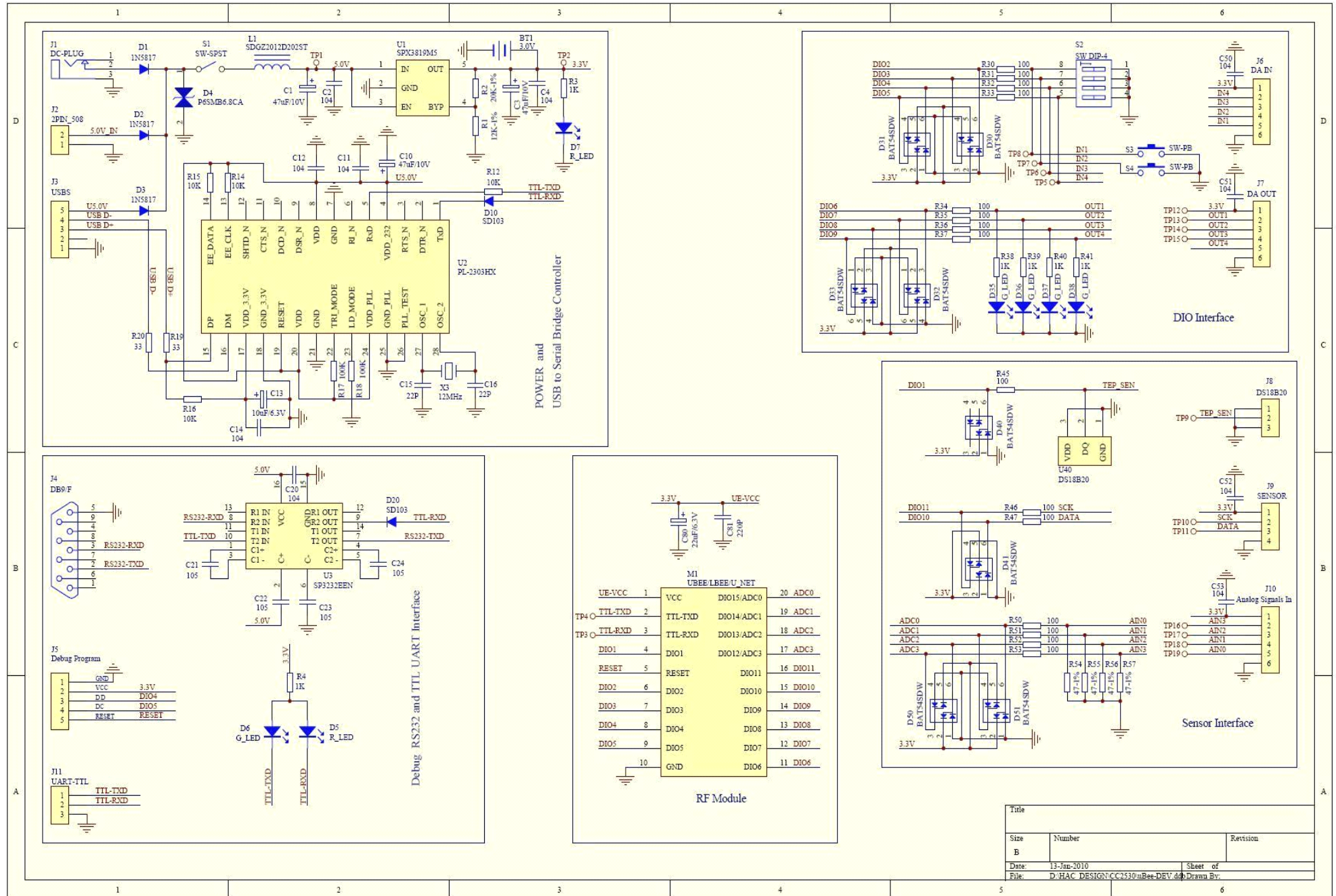
11) J11(UART_TTL) TTL 电平的串口

管脚名	定义
Pin1	TXD
Pin2	RXD
Pin3	GND

4.2 开发测试板 HAC-DEV 与 HAC-UBee V3.1-2.2 的组装示意图。



4.3 开发测试板 HAC-DEV 的原理图



五、HAC-UBee V3.1-2.2 微功率无线数传模块的工作模式

5.1 HAC-UBee V3.1-2.2 的工作模式

HAC-UBee V3.1-2.2 可以在三种模式下工作，透明、API、AT 命令。

5.1.1 透明模式

HAC-UBee V3.1-2.2 的缺省工作模式为透明工作模式，当模块按透明模式工作时，所有从模块串口的 RXD 管脚收到的数据将通过 RF 发送出去，而所有从空中接收的数据将直接发送到串口的 TXD 管脚。

从模块串口的 RXD 管脚收到的数据将保存在缓冲区里直至满足下列条件之一时才打包从空中发送出去，打包发送的条件是：

- 串口数据输入发生了停顿，没从串口收到后续数据；或：
- 从串口接收的数据已达到空中一包数据的最大载荷；

透明传输的目的地址是按 DS 命令指定 16-bit 目的地址发送。

5.1.2 API 模式

API (Application Programming Interface) 模式与透明模式相对应，API 模式要求串口上的数据通信均按一定帧格式(协议)来解释，对不符合协议的数据，模块将予以忽略。

在 API 模式下时，模块从 RXD 管脚 (pin 3)接收的数据帧包括：

- RF 空中数据发送帧；
- 命令帧(类似于 AT 命令)；

而模块从 TXD 管脚 (pin 2)发送给主机的数据帧包括：

- RF 空中数据接收帧；
- 命令返回帧；
- 其它信息帧；

注意：怎样让模块一上电就在 API 模式下工作？

设置模块进入 API 模式可使用 AT 命令；

进入 HAC-UBee V3.1-2.2 的上位机辅助软件“HAC Studio For ZigBee”的 AT Command 页面；

连续输入“+++”，并等待模块返回“OK”；

输入“ATAP 1<CR>”命令，模块返回“OK”，这是将模块置为 API 模式；

输入“ATWR<CR>”命令，模块返回“OK”，这是将设置保存，以便模块下次上电时的工作模式为 API 模式；

输入“ATCN<CR>”退出 AT 命令模式，现在，模块即在 API 模式下工作，重新上电后，它也会直接进入 API 模式。

API 模式下各种命令帧的帧格式定义见以后章节的详细叙述。

5.1.3 AT 命令模式

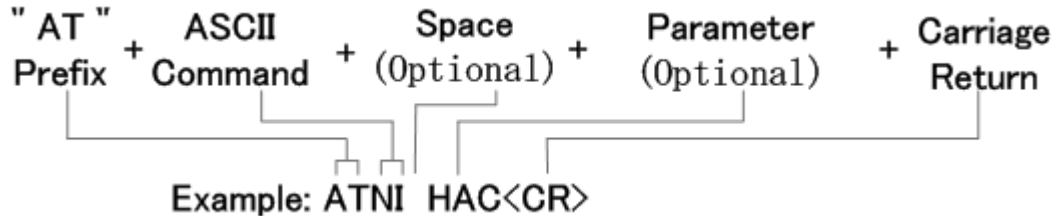
在 AT 命令模式下，可以进行修改或读取模块的参数设置，在 AT 命令模式中，命令以及命令的返回均是以可视字符出现。除了在 AT 命令模式下可以执行 AT 命令外，在 API 模式中也可以按指定的帧格式来执行 AT 命令。

注意：不能进入 AT 命令模式通常都是由于主机的串口设置与模块的串口设

置不符，模块出厂时的串口缺省设置为 38400bps (BD = 5)，8N1。

如果只是读取模块的某个参数的话，要省略 AT 命令后面的参数。

当模块收到 AT 命令后，会执行命令并返回相关信息，如果是读取参数设置，模块会返回相关参数，如果是设置相关参数，模块在成功执行命令后返回一个“OK”信息，如果执行命令出错，则会返回一个“ERROR”信息。



上面这个例子是将模块的描述串设置为“HAC”。

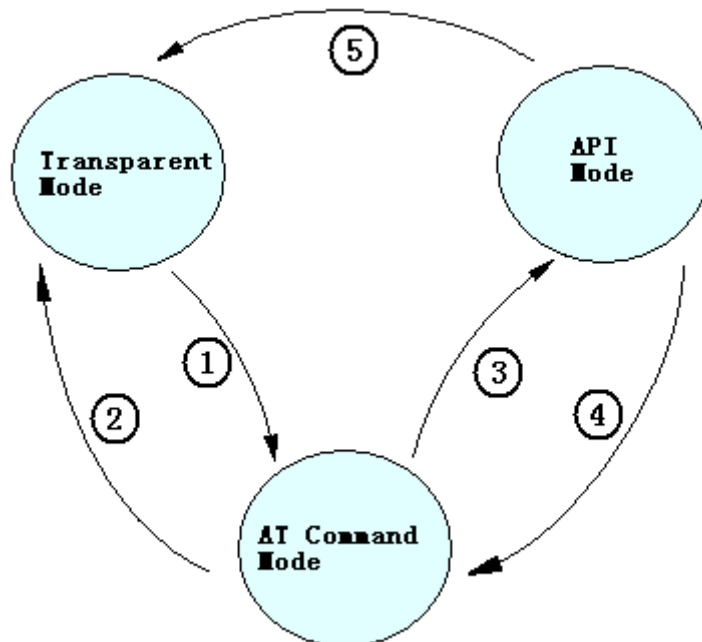
需要注意的是，一些参数在设置后会立即生效，而一些参数设置后可能要等下次上电时才能生效，还有一些参数设置后需要其它参数的配合设置才能生效，请详细阅读每一个 AT 命令的说明并特别注意“生效条件”部分。

退出 AT 命令模式的方法：

输入 ATCN 命令加回车 (0x0d) 或者 10 秒钟内无有效的命令输入。

5.1.4 如何选定模块的工作模式

HAC-UBee V3.1-2.2 的出厂设置为透明工作模式。



- 1) 在透明工作模式从串口连续输入“+++”并停顿即可转换到 AT 命令模式；
- 2) 在选择了透明工作模式 (ATAP 0) 的情况下，输入“ATCN”命令后可退出 AT 命令模式而即进入透明工作模式；或者：
在选择了透明工作模式 (ATAP 0) 的情况下，若 10 秒内串口无输入时也

将退出 AT 命令模式而进入透明工作模式；

- 3) 在选择了 API 工作模式(ATAP 1) 的情况下，输入“ATCN”命令后可退出 AT 命令模式即进入 API 工作模式；或者：
在选择了 API 工作模式(ATAP 1) 的情况下，若 10 秒内串口无输入时也将退出 AT 命令模式而进入 API 工作模式；
- 4) 在 API 模式从串口连续输入“+++”并停顿即可转换到 AT 命令模式；
- 5) 使用 API 模式下的 AT 命令设置透明工作模式(ATAP 0)，模块会立即转入透明工作模式。

5.2 AT 命令

序号	AT 命令	命令类别	命令描述	参数范围	缺省	版本要求
1	AI	Networking	网络状态。查询模块的网络状态，仅对 EndDevice 有效。	0 - 1 0 = 有网络 1 = 无网络	1	>=0x22
2	AP	Serial Interfacing	API 使能。设置/读模块的工作模式。	0 - 1 0 = 透明 1 = API	0	>=0x19
3	BD	Serial Interfacing	串口波特率。设置/读模块的串口波特率。	0 - 7 0 = 1200 1 = 2400 2 = 4800 3 = 9600 4 = 19200 5 = 38400 6 = 57600 7 = 115200	5	>=0x19
4	CH	Networking	信道。读模块的信道数(该信道数是按 802.15.4 协议定义)。	0x0B - 0x1A (Read Only)	-	>=0x19
5	CN	AT Command Mode Options	退出 AT 命令模式。	-	-	>=0x19
6	DS	Networking	16-bit 目的地址。设置/读模块的 16-bit 目的地址。当 16-bit 目的地址设为 0xFFFF 时为广播。	0x00 - 0xFFFF	0xFFFF	>=0x19
7	FR	Special	重新启动。立即执行硬件复位并重启。	-	-	>=0x19
8	HV	Diagnostics	硬件版本。读模块的硬件版本。	0x00 - 0xFFFF (Read only)	-	>=0x19
9	ID	Networking	PAN ID。设置/读 PAN (Personal Area Network) ID 的设置值。	0x00 - 0xFFFF	0x29AC	>=0x19
10	KY	Networking Secure	设置模块数据加密传输时的密钥。(数据加密传输模块需要订制)	16 字节的 Hex (Setup only)	-	>=0x21
11	MP	Networking	父节点的短地址。读取父节点的 16 位短地址。	0x00 - 0xFFFD (Read only)	-	>=0x21
12	MT	Networking	模块类型。读模块的 ZigBee 设备类型。	0 - 2 (Read only) 0-Coordinator 1-Router 2-EndDevice	-	>=0x19
13	MY	Networking	16-bit 源地址。读模块的 16-bit 源地址。	0x00-0xFFFE (Read Only)	-	>=0x19
14	ND	Networking	搜索节点的信息。读取网络中在线节点的 16 位地址、64 位高低地址、接收数据的信号强度及描述串。	0-20 个 ASCII	-	>=0x21
15	NI	Networking	节点描述串设置。设置/读取模块的描述字符串。	0-20 个 ASCII	-	>=0x21



16	NO	Networking	搜索节点选项。节点搜索时是否显示本节点信息。	0-1 0-不显示 1-显示	0	>=0x21
17	NT	Networking	节点搜索的时间限制设置。	0x01 - 0xFC 单位: 100 毫秒	0x19	>=0x21
18	PI	Networking	PAN ID。读模块实际工作的 PAN ID。	0x00 - 0xFFFE (Read only)	-	>=0x19
19	PL	RF Interfacing	功率级别。设置/读取模块空中发送数据的功率级别。	0x00-0x04	0x04	>=0x19
20	PT	Diagnostics	开关量。设置/读取模块第 6 管脚的开关量。	0 - 1	1	>=0x22
21	RE	Special	恢复缺省设置。将模块的参数恢复到出厂时的缺省设置。	-	-	>=0x19
22	RN	Networking	重置网络。下次上电时按非易失内存中的指定设置初始化网络参数,并重新搜索网络。注意:重置网络并重新搜索网络后,自己的短地址(16bit Address)、信道等可能发生改变。	0 - 1 0 = Disabled 1 = Enabled	0	>=0x19
23	RR	Networking	空中发送失败时重试次数设置。	3 - 6	3	>=0x21
24	S1	Diagnostics	采集电压值。用于采集端口的电压值,对应模块的第 20 管脚。	0x00 -0xFFFF (Read only)	-	>=0x22
25	S2	Diagnostics	采集电压值。用于采集端口的电压值,对应模块的第 19 管脚。	0x00 -0xFFFF (Read only)	-	>=0x22
26	S3	Diagnostics	采集电压值。用于采集端口的电压值,对应模块的第 18 管脚。	0x00 -0xFFFF (Read only)	-	>=0x22
27	S4	Diagnostics	采集电压值。用于采集端口的电压值,对应模块的第 17 管脚。	0x00 -0xFFFF (Read only)	-	>=0x22
28	SC	Networking	信道搜索设置。设置/读取模块加入网络时要搜索的信道。	0x01 - 0xFFFF	0x03	>=0x21
29	SH	Networking	IEEE 64-bit 地址高 32bit。读模块的 IEEE 64-bit 地址高 32bit。	0x00- 0xFFFFFFFF	-	>=0x19
30	SL	Networking	IEEE 64-bit 地址低 32bit。读模块的 IEEE 64-bit 地址低 32bit。	0x00- 0xFFFFFFFF	-	>=0x19
31	SM	Sleep (Low Power)	休眠状态。设置/读模块的休眠模式。(仅对 EndDevice 有效)	0-1 0 = Disabled 1 = Enabled	0	>=0x20
32	SP	Sleep (Low Power)	Coordinator、Router 替其子节点 EndDevice 保存数据的时间限制或 EndDevice 定期到其父节点处获取数据的周期。(对 Coordinator、Router 及 EndDevice 均有效)	0x01 - 0xFFFF 单位: 10 毫秒	0x12C	>=0x20
33	ST	Sleep (Low Power)	处于休眠模式的 EndDevice 每次唤醒后,保持工作的时间。此值必须不超过 SP 所设置值的 1/2。(仅对 EndDevice 有效)	0x01 - 0xFFFF 单位: 毫秒	0x32	>=0x21
34	VR	Diagnostics	软件版本。读模块的软件版本。	0x00 - 0xFF (Read only)	-	>=0x19
35	WR	Special	写参数。将参数写入到模块的非易失内存,这样即便模块重启或掉电后重新上电,参数仍然有效。	-	-	>=0x19

5.2.1 AI

AI 用于查询模块 EndDevice 的网络状态,该命令仅对 EndDevice 有效。若返回值为 0,表示 EndDevice 有网络,即找到父节点;若返回值为 1,表示 EndDevice 无网络,即找不到父节点。EndDevice 入网搜索需要几百毫秒到几秒的时间不等,需要使用 AI 命令多次查看才能确定其状态结果;另外其父节点也是动态变化的,即 EndDevice 每次入网后的父节点可能不一样。

Command	ATAI	
Parameter	Range	0 - 1 0 - 有网络 1 - 无网络
	Default Value	1
最低软件版本要求: 0x22		

5.2.2 AP

AP 用于设置或读取模块的工作模式。若设置参数为 0，表明在模块退出 AT 命令模式后将进入透明工作模式，而若设置参数为 1，则表明模块在退出 AT 命令模式后将进入 API 模式。

Command	ATAP (API Enable)	
Parameter	Range	0-1
	Default Value	0
	Value	0: 透明模式 1: API 模式
生效条件	退出 AT 命令模式后立即生效	
最低软件版本要求: 0x19		

设置模块工作模式的举例：

从串口连续输入“+++”并停顿换到 AT 命令模式；

用 ATAP 命令设置希望的工作模式，如 ATAP 0<CR>或 ATAP 1<CR>；

如果希望下次模块上电启动时设置仍然生效，则用 ATWR<CR>命令写入到非易失内存；

输入“ATCN<CR>”命令后退出 AT 命令模式，模块将进入设置的工作模式。

5.2.2 BD

BD 命令用于设置或读取模块串口的波特率。参数的有效范围为 0-7，分别对应了表中不同的波特率。模块的空中数据传输速率(固定为 250kbps)并不受此参数影响。建议用户不要选择过小的串口波特率，否则有可能会造成串口数据通信的溢出。只提供 AT 命令更改模块串口波特率，不提供 API 模式下更改模块串口波特率的命令。

Command	ATBD (Interface Data Rate)	
Parameter	Range	0-7
	Default Value	5
	Value	0 = 1200 1 = 2400 2 = 4800 3 = 9600 4 = 19200 5 = 38400 6 = 57600 7 = 115200



生效条件	使用 WR 命令保存设置，模块下一次上电时生效
最低软件版本要求：0x19	

修改模块串口波特率的举例：

从串口连续输入“+++”并停顿换到 AT 命令模式；

用 ATBD 命令设置希望的串口波特率，如 ATBD 6<CR>;

用 ATWR 命令写入到非易失内存，即 ATWR<CR>;

输入“ATFR<CR>”命令，模块立即重新启动。

5.2.3 CH

CH 命令用于读取模块的无线工作信道。HAC-UBee V3.1-2.2 可供选择的信道共 16 个(0x0B-0x1A)，同一个网络中的所有模块必须在同一个信道上工作，而不同网络的模块设置在不同的信道上也可以避免其相互干扰。模块的信道数符合 802.15.4 标准。中心频点 = $2405 + (CH - 11d) * 5 \text{ MHz}$ (d = decimal)。

Command	ATCH (Channel)	
Parameter	Range	0x0B - 0x1A
	Default Value	-
最低软件版本要求：0x19		

读取模块信道的举例：

从串口连续输入“+++”并停顿换到 AT 命令模式；

用 ATCH 命令读取模块的信道，如 ATCH<CR>;

输入“ATCN<CR>”命令，模块退出 AT 命令模式。

5.2.4 CN

CN 命令用于使模块立即退出 AT 命令模式。

Command	ATCN(Exit Command Mode)
Parameter	None
生效条件	立即生效
最低软件版本要求：0x19	

5.2.5 DS

DS 用于设置或读取模块 16-bit 目的地址，16-bit 地址又称为短地址。只有在透明模式下，这个设置才起作用。当 16-bit 目的地址为 0xFFFF 时，并且模块工作在透明模式下，模块将以广播方式发送空中数据。

Command	ATDS (Short Destination Address/ 16bit Destination Address)	
Parameter	Range	0x00 - 0xFFFF
	Default Value	0xFFFF
生效条件	立即生效	
最低软件版本要求：0x19		



修改模块 16-bit 目的地址的举例：

从串口连续输入 “+++” 并停顿换到 AT 命令模式；

用 ATDS 命令设置希望的目的短地址，如 ATDS FFFF<CR>；

如果希望下次模块上电启动时设置仍然生效，则用 ATWR<CR>命令写入到非易失内存；

输入 “ATCN<CR>” 命令后退出 AT 命令模式。

5.2.6 FR

FR 命令用于将模块重新启动，当模块收到 FR 命令后，模块将不返回 “OK” 而直接模拟断电并立即重新启动。

Command	ATFR(Software Reset)
Parameter	None
生效条件	立即生效
最低软件版本要求：0x19	

使模块重启的举例：

从串口连续输入 “+++” 并停顿换到 AT 命令模式；

用 ATFR 命令使模块重启，即 ATFR<CR>。

5.2.7 HV

HV 命令用于读取模块的硬件版本。

Command	ATHV(Hardware Version)	
Parameter	Range	0-0xFFFF [Read-only]
最低软件版本要求：0x19		

5.2.8 ID

ID 命令用于设置或读取模块的 PAN (Personal Area Network) ID 设置值。只有在模块的 PAN ID 相同的情况下，模块间才能互相通信。

要使设置的 PAN ID 生效，必须在设置 PAN ID 的同时要使用 RN 命令，将模块设置为下一次启动时重置网络，然后将这二个设置均写入到模块的非易失内存中去，这样，模块在下一次上电启动后，它的新 PAN ID 才能生效。

Command	ATID (PAN ID)	
Parameter	Range	0x00 - 0xFFFF
	Default Value	0x29AC
生效条件	RN=1，使用 WR 命令保存设置，模块下一次上电时生效	
最低软件版本要求：0x19		

在一个网络中的所有模块的 PAN ID 必须相同，如果要为一个模块指定其 PAN ID，可将其 PAN ID 设置成 0x00-0xFFFFE 中的某个值，若将模块的 PAN ID 设置成 0xFFFF，则视模块类型的不同而有不同的结果。若是 Coordinator 的 PAN ID 设置成 0xFFFF，那么，Coordinator 在启动时，会从 0x00-0xFFFFE 中随机选择一个

值作为其 PAN ID，而如果是将 Router 或 EndDevice 的 PAN ID 设置成 0xFFFF，则 Router 或 EndDevice 在上电启动时，将搜索周边 ZigBee 网络的 PAN ID，并将自己的 PAN ID 赋为该值后试图加入到这个 ZigBee 网络，当周边有多个 ZigBee 网络时，它将选择 RSSI 值最好的那个网络加入。

当将模块的 PAN ID 设置成 0xFFFF 时，模块加入网络后的实际 PAN ID 值，可由 ATPI 命令读出，当为模块指定 PAN ID 值 (0x00-0xFFFE) 时，用 ATPI 命令读出的 PAN ID 值与用 ATID 读出的 PAN ID 值相同。

修改模块 PAN ID 的举例：

从串口连续输入 “+++” 并停顿换到 AT 命令模式；

用 ATID 命令设置希望的 PAN ID，如 ATID 12AB<CR>;

用 ATRN 命令设置下次启动时重置网络，即 ATRN 1<CR>;

用 ATWR 命令写入到非易失内存，即 ATWR<CR>;

输入 “ATFR<CR>” 命令，模块立即重新启动。

5.2.9 KY

KY 命令用于设置数据加密传输模块的密钥值，该密钥值只能设置而不能读取，为 16 字节定长的 16 进制值 (注：数据加密传输是指模块在空中数据传输时采用 IEEE 标准 AES 加密算法进行数据传输)。重置网络 (ATRN=1) 后才生效，即使使用 ATRE 命令将模块恢复为出厂设置，密码仍然有效。

Command	ATKY	
Parameter	Range	16 字节定长的 16 进制值
生效条件	ATRN=1，使用 WR 命令保存设置，模块下一次上电时生效	
最低软件版本要求：0x21		

修改密码的举例：

从串口连续输入 “+++” 并停顿换到 AT 命令模式；

用 ATKY 设置希望的密码，如：ATKY 01234567890123456789012345678901<CR>;

用 ATRN 1 设置下次启动时重置网络，如：ATRN 1<CR>;

用 ATWR 命令写入到非易失内存，即 ATWR<CR>;

输入 “ATCN<CR>” 命令退出 AT 命令模式。

5.2.10 MP

MP 命令用来读取模块的父节点 16 bit 地址。

Command	ATMP	
Parameter	Range	0x00 - 0xFFFF[Read-only]
最低软件版本要求：0x21		

5.2.11 MT

MT 命令用于读取模块的 ZigBee 节点类型。HAC-UBee V3.1-2.2 在出厂时已确定了其类型，用户无法更改。

Command	ATMT (类型)
---------	-----------

Parameter	Range	0-2
	Value	0 = Coordinator 1 = Router 2 = EndDevice
最低软件版本要求: 0x19		

5.2.12 MY

MY 命令用于读取模块自己的 16-bit(源)地址。模块的 16-bit 源地址是在模块加入一个 ZigBee 网络时由 ZigBee 网络赋予的, 如果模块的 16-bit (源)地址为 0xFFFE 则说明它还没有加入一个 ZigBee 网络, 如果它的 16-bit (源)地址小于 0xFFFE, 则说明它已加入一个 ZigBee 网络。

关于 16-bit 地址, 参考附录“ZigBee 简介”部分。

Command	ATMY (16-bit Source Address)	
Parameter	Range	0x00 - 0xFFFE
最低软件版本要求: 0x19		

5.2.13 ND

ND 命令用于搜索网络内其它在线节点的信息, 这些信息包括节点的 16 bit 地址、64 bit 地址的高 32 bit、64 bit 地址的低 32 bit、接收到节点数据的信号强度及节点描述字符串。

当 ND 命令不带参数时, 用来搜索网络内所有在线节点的信息。

当 ND 命令带参数时, 其参数为节点描述字符串, 此时用来搜索网络内与该节点描述字符串完全相匹配的在线节点信息。

Command	ATND(Node Discover)	
Parameter	Range	0-20 个 ASCII
最低软件版本要求: 0x21		

搜索节点信息的举例:

从串口连续输入“+++”并停顿换到 AT 命令模式;

用 ATND 命令搜索指定节点, 如描述字符串为“Switch”的节点,

输入 ATND Switch<CR>;

输入“ATCN<CR>”命令退出 AT 命令模式。

5.2.14 NI

NI 命令用于读取或设置模块的描述字符串。模块的描述字符串必须是可显示的 ASCII 字符, 而且, 一个字符串不能以空格开始, 模块的描述字符串必须小于或等于 20 个字符, 当超过 20 时, 则取前 20 个字符为有效值。

Command	ATNI(Node Identifier)	
Parameter	Range	0-20 个 ASCII
生效条件	立即生效	

最低软件版本要求: 0x21

修改模块描述字符串的举例:

从串口连续输入 “+++” 并停顿换到 AT 命令模式;

用 ATNI 命令设置希望的描述字符串, 如 ATNI HAC UBee V3.1-2.2<CR>;

如果希望模块下次上电时设置仍然生效, 则用 ATWR 命令写入到非易失内存, 即 ATWR<CR>;

输入 “ATCN<CR>” 命令退出 AT 命令模式。

5.2.15 NO

NO 命令用来读取或设置搜索节点选项。当模块执行 ND 命令来搜索节点时, 根据 NO 命令的值来确定是否显示自己的相关信息。当 NO 的参数为 0 时, 模块不显示自己的信息; 当 NO 的参数为 1 时, 模块显示自己的信息。

Command	ATNO(Node Discover Options)	
Parameter	Range	0-1
	Default Value	0
	Value	0 = 不显示 1 = 显示
生效条件	立即生效	
最低软件版本要求: 0x21		

修改模块搜索节点选项的举例:

从串口连续输入 “+++” 并停顿换到 AT 命令模式;

用 ATNO 命令设置希望的选项, 如 ATNO 0<CR>或 ATNO 1<CR>;

如果希望模块下次上电时设置仍然生效, 则用 ATWR 命令写入到非易失内存, 即 ATWR<CR>;

输入 “ATCN<CR>” 命令退出 AT 命令模式。

5.2.16 NT

NT 命令用于读取或设置搜索网络节点时的时间限制, 其单位为 100mS。当 HAC-UBee V3.1-2.2 模块用 ND 命令进行网络节点搜索时, 它将最多只等待按 NT 命令设置的时间, 超过该时间后, 网络中其它节点的返回将被忽略。

Command	ATNT(Node Discover Time)	
Parameter	Range	0x01 - 0xFC [*100 msec]
	Default Value	0x19
生效条件	立即生效	
最低软件版本要求: 0x21		

修改模块网络节点搜索时间限制的举例:

从串口连续输入 “+++” 并停顿换到 AT 命令模式;

用 ATNT 命令设置希望的时间值, 如 ATNT 1A<CR>;

如果希望模块下次上电时设置仍然生效, 则用 ATWR 命令写入到非易失内



存，即 ATWR<CR>;

输入“ATCN<CR>”命令退出 AT 命令模式。

5.2.17 PI

PI 命令用于读取模块工作的实际 PAN ID。仅在模块的 PAN ID 设置值为 0xFFFF 时，其加入网络后的 PAN ID 才可能会与用“ATID”命令读出的 PAN ID 不同，关于这一点，请阅读“ATID”命令部分。

Command	ATPI (PAN ID)	
Parameter	Range	0x00 - 0xFFFE
最低软件版本要求: 0x19		

5.2.18 PL

PL 命令用于设置或读取模块的空中数据发送的功率级别，参数 0-4 的发射功率为逐级增大，参数为 0 时，其发射功率为最小，而参数为 4 时，其发射功率最大。

当设置参数不为 4 时，将影响模块的通信效果，建议用户尽量不要更改此参数。

Command	ATPL(Power Level)	
Parameter	Range	0-4
	Default Value	4
	Value	0 = Min Power 4 = Max Power
生效条件	使用 WR 命令保存设置，模块下一次上电时生效	
最低软件版本要求：0x19		

修改模块发射功率级别的举例：

从串口连续输入“+++”并停顿换到 AT 命令模式；

用 ATPL 命令设置希望的功率级别，如 ATPL 4<CR>;

用 ATWR 命令写入到非易失内存，即 ATWR<CR>;

输入“ATFR<CR>”命令，模块立即重新启动。

5.2.19 PT

PT 命令用于设置或读取模块第 6 管脚的开关量。模块的第 6 管脚与测试板 HAC-DEV 上的 J6-5 对应。

Command	ATPT	
Parameter	Range	0-1
	Default Value	1
生效条件	立即生效	
最低软件版本要求：0x22		

修改第 6 管脚开关量的举例：

从串口连续输入 “+++” 并停顿换到 AT 命令模式；

用 ATPT 设置希望的值，如：ATPT 1<CR>；

如果希望模块下次上电时设置仍然生效，则用 ATWR 命令写入到非易失内存，即 ATWR<CR>；

输入 “ATCN<CR>” 命令退出 AT 命令模式。

5.2.20 RE

RE 命令用于恢复模块的出厂缺省设置。当模块收到 RE 命令后，将立即把所有可设置参数恢复为出厂缺省设置，并将这些参数写入非易失内存，然后使模块重新启动。

此命令的执行会造成模块丢失网络，并可能造成模块的 PAN ID、16bit 地址等发生改变。

Command	ATRE(Restored defaults)
Parameter	None
生效条件	立即生效
最低软件版本要求：0x19	

使模块恢复出厂设置的举例：

从串口连续输入 “+++” 并停顿换到 AT 命令模式；

用 ATRE 命令恢复出厂设置，即 ATRE<CR>。

5.2.21 RN

RN 命令用于读取或设置模块在下次启动时是否重置网络，如果设置了下次启动时重置网络，则模块在下次启动时，将重新搜索 ZigBee 网络并寻求加入。这意味着，如果模块已加入了一个 ZigBee 网络的话，它将先失去这个网络，在它重启后，它的 PAN ID、信道、16-bit 源地址等都有可能发生改变。

Command	ATRN(Retries)	
Parameter	Range	0-1
	Default Value	0
	Value	0 = Disable 1 = Enable
生效条件	使用 WR 命令保存设置，模块下一次上电时生效	
最低软件版本要求：0x19		

设置模块下次启动时重置网络的举例：

从串口连续输入 “+++” 并停顿换到 AT 命令模式；

用 ATRN^{Retrieves} 命令设置下次启动时重置网络，如 ATRN 1<CR>；

用 ATWR 命令写入到非易失内存，即 ATWR<CR>；

输入 “ATFR<CR>” 命令，模块立即重新启动。

5.2.22 RR

RR 命令用来设置或读取模块在发送空中数据失败后所重发的次数。

Command	ATRR(Retries)	
Parameter	Range	3-6
	Default Value	3
生效条件	立即生效	
最低软件版本要求：0x21		

修改重发次数的举例:

从串口连续输入“+++”并停顿换到 AT 命令模式;

用 ATRR 设置希望的重发次数, 如: ATRR 4<CR>;

如果希望模块下次上电时设置仍然生效, 则用 ATWR 命令写入到非易失内存, 即 ATWR<CR>;

输入“ATCN<CR>”命令退出 AT 命令模式。

5.2.23 S1

S1 命令用来采集模块第 20 管脚的电压值, 返回电压值为 16 进制数, 计算公式为: (X 除以 8192) 乘以 3.3, X 为返回值; 例如, 若返回值为 0x1FE8, 则其 10 进制值为 8168, 其对应的电压为 (8168/8192)*3.3, 即为 3.29(V); 模块的第 20 管脚, 与测试板 HAC-DEV 上的 J10-5 对应。

Command	ATS1	
Parameter	Range	0x00 - 0xFFFF[Read-only]
最低软件版本要求: 0x22		

5.2.24 S2

S2 命令用来采集模块第 19 管脚的电压值, 返回电压值为 16 进制数, 计算公式为: (X 除以 8192) 乘以 3.3, X 为返回值。模块的第 19 管脚, 与测试板 HAC-DEV 上的 J10-4 对应。

Command	ATS2	
Parameter	Range	0x00 - 0xFFFF[Read-only]
最低软件版本要求: 0x22		

5.2.25 S3

S3 命令用来采集模块第 18 管脚的电压值, 返回电压值为 16 进制数, 计算公式为: (X 除以 8192) 乘以 3.3, X 为返回值。模块的第 18 管脚, 与测试板 HAC-DEV 上的 J10-3 对应。

Command	ATS3	
Parameter	Range	0x00 - 0xFFFF[Read-only]
最低软件版本要求: 0x22		



5.2.26 S4

S4 命令用来采集模块第 17 管脚的电压值，返回电压值为 16 进制数，计算公式为：(X 除以 8192) 乘以 3.3，X 为返回值。模块的第 17 管脚，与测试板 HAC-DEV 上的 J10-2 对应。

Command	ATS4	
Parameter	Range	0x00 - 0xFFFF[Read-only]
最低软件版本要求：0x22		

5.2.27 SC

SC 命令用于设置或读取模块所要搜索的信道。模块根据 SC 命令设定的值来选择工作信道。SC 设置的参数为两个字节，若两字节中的某一位为二进制数 1，表明要在该位对应的信道上搜索（每一位所对应的信道参照下表）；如果设置的值中含两位二进制数 1 以上，则采取“或”的方式来搜索信道，对于 Coordinator，会从所设置的多个信道中选择其中一个工作；对于 Router 和 EndDevice，则搜索所设置的多个信道并试图加入网络，直至加入网络为止。

要使设置的参数生效，必须在设置搜索信道的同时要使用 RN 命令，将模块设置为下一次启动时重置网络，然后将这二个设置均写入到模块的非易失内存中去，这样，模块在下一次上电启动后，它才会在根据设置值选择新的信道工作。

Command	ATSC(Scan Channels)				
Parameter	Range	0x01 - 0xFFFF			
	Default Value	0x03			
	Value	bit0 - 0x0B	bit4 - 0x0F	bit8 - 0x13	bit12 - 0x17
		bit1 - 0x0C	bit5 - 0x10	bit9 - 0x14	bit13 - 0x18
		bit2 - 0x0D	bit6 - 0x11	bit10 - 0x15	bit14 - 0x19
bit3 - 0x0E		bit7 - 0x12	bit11 - 0x16	bit15 - 0x1A	
生效条件	RN=1，使用 WR 命令保存设置，模块下一次上电时生效				
最低软件版本要求：0x21					

修改模块搜索信道的举例：

- 从串口连续输入“+++”并停顿换到 AT 命令模式；
- 用 ATSC 命令设置希望的值，如 ATSC 2<CR>; (0x0C 信道)
- 用 ATRN 命令设置下次启动时重置网络，即 ATRN 1<CR>;
- 用 ATWR 命令写入到非易失内存，即 ATWR<CR>;
- 输入“ATFR<CR>”命令，模块立即重新启动。

5.2.28 SH

SH 命令用于设置或读取模块的 IEEE 64-bit 地址的高 32-bit。

注意：每个模块出厂时的 64 bit 地址是由模块所使用的芯片厂商提供的，

芯片厂商保证了 64 bit 地址的全球唯一性。在一个 ZigBee 网络中，每个模块的 64-bit 地址必须是唯一的，否则会造成通信混乱，因此，不建议用户对 64-bit 地址进行更改。

将 64-bit 地址的高 32-bit 和低 32-bit 均设置成 0xFFFFFFFF，可以将 64-bit 地址 (IEEE 64-bit 地址或 64-bit ID) 恢复到出厂时的设置。

要使设置的 64-bit 地址生效，必须在设置 64-bit 地址的同时要使用 RN 命令，将模块设置为下一次启动时重置网络，然后将这二个设置均写入到模块的非易失内存中去，这样，模块在下一次上电启动后，它的新 64-bit 地址才生效。

Command	ATSH(Serial Number High)	
Parameter	Range	0-0xFFFFFFFF
	Default Value	-
生效条件	RN=1，使用 WR 命令保存设置，模块下一次上电时生效	
最低软件版本要求：0x19		

5.2.29 SL

SL 命令用于设置或读取模块的 IEEE 64-bit 地址的低 32-bit。

Command	ATSL(Serial Number Low)	
Parameter	Range	0-0xFFFFFFFF
	Default Value	-
生效条件	RN=1，使用 WR 命令保存设置，模块下一次上电时生效	
最低软件版本要求：0x19		

5.2.30 SM

SM 命令用于设置或读取模块的休眠模式，该设置仅对 EndDevice 有效，参数为 0 时，不允许模块休眠，参数为 1 时，允许模块在加入网络后进入休眠状态。

当模块处于无 ZigBee 网络状态时，由于模块需要不断寻找 ZigBee 网络加入，它并不进入休眠状态。

EndDevice 进入休眠状态有三个前提条件，第一，EndDevice 已加入到 ZigBee 网络；第二，SM 参数设置为 1，即休眠允许；第三，模块的休眠控制管脚为休眠允许，即管脚 9 为高电平，当这三个条件同时都满足时，EndDevice 才进入休眠状态。

Command	ATSM(Sleep Mode)	
Parameter	Range	0-1
	Default Value	0
	Value	0 = Disable 1 = Enable
生效条件	立即生效	



最低软件版本要求: 0x20

修改模块休眠模式的举例:

从串口连续输入“+++”并停顿换到 AT 命令模式;

用 ATSM 命令设置休眠模式, 如 ATSM 1<CR>;

如果希望模块下次上电时设置仍然生效, 则用 ATWR 命令写入到非易失内存, 即 ATWR<CR>;

输入“ATCN<CR>”命令退出 AT 命令模式。

5.2.31 SP

SP 命令用于设置或读取模块 Coordinator、Route 替其子节点 EndDevice 保存数据的时间限制, 也用于设置或读取 EndDevice 定期到其父节点处获取数据的周期。该命令对 Coordinator、Router 和 EndDevice 都有效, 而且 EndDevice 所设置的休眠周期值应与其父节点 (Coordinator 或 Router) 的值相等, 因为 EndDevice 在休眠期间, 是接收不到空中数据的, 其父节点会替 EndDevice 保存所有发给 EndDevice 的数据, 保存数据的时间长度则根据 SP 命令设置的值来确定。EndDevice 每次唤醒时从其父节点处取数据, 如果超过了保存时间, EndDevice 还不来取数据, 其父节点会将数据清除, 所以 EndDevice 与其父节点所设置的 SP 值应该相等。

Command	ATSP (Cyclic Sleep Period)	
Parameter	Range	0x01 - 0xFFFF [*10 msec]
	Default Value	0x12C
生效条件	使用 WR 命令保存设置，模块下一次上电时生效	
最低软件版本要求：0x20		

修改模块的 SP 值举例:

从串口连续输入“+++”并停顿换到 AT 命令模式;

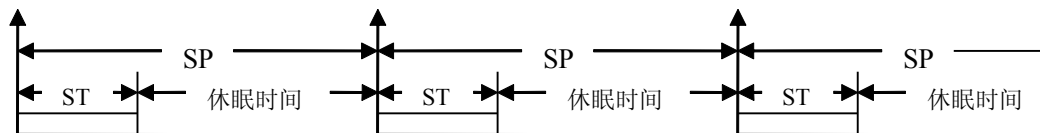
用 ATSP 命令设置希望的值, 如 ATSP 1F4<CR>;

用 ATWR 命令保存设置, 即 ATWR<CR>;

用“ATFR<CR>”命令重启模块。

5.2.32 ST

ST 命令用于设置或读取模块 EndDevice 在休眠唤醒后, 保持工作的时间。ST 所设置的值必须不超过 SP 所设置值的 1/2, 否则休眠时间周期会出现混乱。该命令仅对 EndDevice 有效。处于休眠模式的 EndDevice, 当定期唤醒时间 (SP 命令设置) 到来时, 模块自动唤醒并保持一段工作时间 (ST 命令设置), 工作时间过后再次进入休眠状态, 直至下一个唤醒时间到来时再次唤醒, 如此周期性地运作。那么模块实际的休眠时间为 (SP*10-ST), SP 单位为 10 毫秒。图示如下:



Command	ATST (Time before Sleep)	
Parameter	Range	0x01 - 0xFFFF [*1msec]
	Default Value	0x32
生效条件	立即生效	
最低软件版本要求：0x21		

修改模块唤醒后的工作时间的举例:

从串口连续输入“+++”并停顿换到 AT 命令模式;

用 ATST 命令设置希望的工作时间值, 如 ATST 64<CR>;

如果希望模块下次上电时设置仍然生效, 则用 ATWR 命令写入到非易失内存, 即 ATWR<CR>;

输入“ATCN<CR>”命令退出 AT 命令模式。

5.2.33 VR

VR 命令用于读取模块的软件版本。一些 AT 命令可能会在特定的版本上实现。

Command	ATVR (Firmware Version)	
Parameter	Range	0x00 - 0xFF[Read-only]
	Default Value	
最低软件版本要求: 0x19		

5.2.34 WR

WR 命令将当前的全部可设置项写入到模块的非易失内存中去。

模块在上电启动时, 会从非易失内存中读出参数, 而一些参数在设置后, 如果不写入非易失内存中的话, 模块下次重新上电启动后, 设置就不再有效, 因此, 用 WR 命令写入到非易失内存, 可保证这些设置即便在模块断电, 下次上电后仍然有效。

注意: 每个参数的生效条件可能会不同, 即使将其写入到非易失内存中, 下次上电也并不意味着生效, 请详细阅读各个命令说明的生效条件部分。

Command	ATWR (Write)
Parameter	None
最低软件版本要求: 0x19	

5.3 API 工作模式

当模块的工作模式为透明模式时, 所有来自 RXD 管脚的数据将在打包后通过空

中发射出去，而所有从空中接收的数据都将发送到 TXD 管脚，模块并不向这些数据中添加任何信息。

透明模式是有下列局限的：

- 要么只能发送广播，要么只能将数据发送到一个指定的模块，当需要将数据发送到不同的模块时，它将不易实现；
- 当接收到多个其它模块的空中数据时，无法判别源模块是谁，即无法判别这些数据最初来自于哪一个模块。

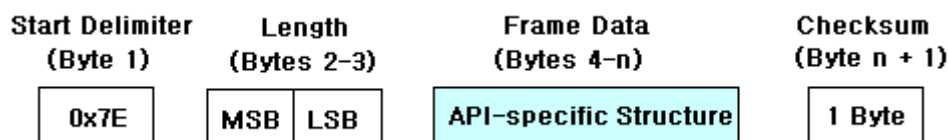
作为透明模式的一种补充，API 模式（Application Programming Interface）将没有透明模式的上述局限。API 模式要求串口上的数据通信均按一定协议来解释，对不符合协议的数据，模块将予以忽略。

5.3.1 API 帧结构

API 模式可以在 AT 命令模式下用 AP 命令来实现。当 AP 命令的参数为 0 时，为透明模式，当 AP 的参数为 1 时，为 API 模式。

API 模式（AP 参数 = 1）

在 API 模式（AP=1）下，串口数据的帧结构定义如下：



串口数据的每个帧均由 4 个字段组成，分别是 Start Delimiter、Length、Frame Data 和 Checksum。

Start Delimiter

Start Delimiter 是帧头标志，API 模式的帧头固定为 0x7E。

Length

Length 是有效数据长度，是 Frame Data 字段的长度，MSB=高字节，LSB=低字节。

Frame Data

Frame Data 是有效数据字段。

Checksum

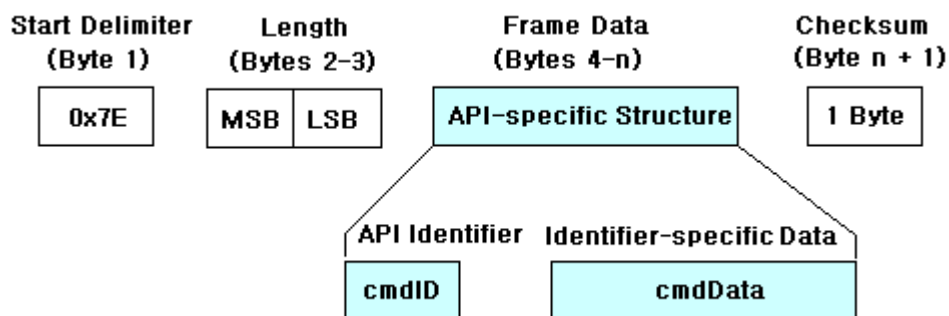
Checksum 为校验和，它用于校验整个数据帧的正确性。

校验和的计算：不包括帧头和长度（1-3 字节）在内，将“Frame Data”字段的内容逐个相加并只保留一个字节的和，再用 0xFF 减去这个和即可。

校验：不包括帧头和长度（1-3 字节）在内，将“Frame Data”字段的内容逐个相加并只保留一个字节的和，然后再加上 Checksum 的值，如果相加的结果等于 0xFF 则说明校验正确。

5.3.2 帧结构定义

API 模式下串口的帧结构及“Frame Data”字段的定义如下：

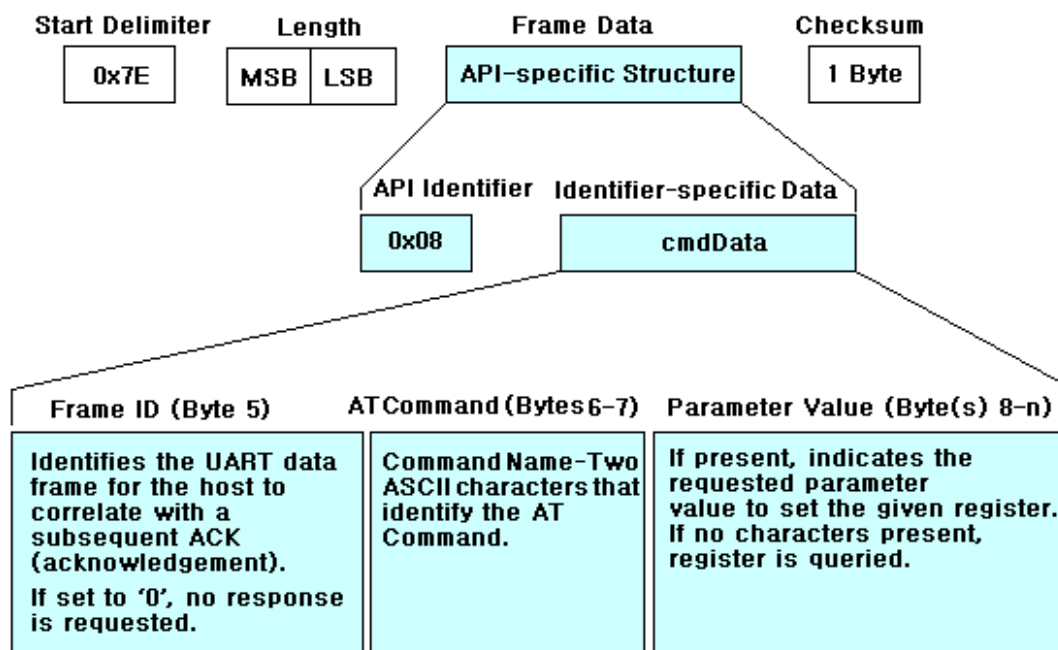


“cmdID” 字段(API-identifier) 是用于标示该数据帧执行何种 API 命令的命令码。下面各节将介绍几个不同的 API 命令，需要注意的是，对多于一个字节组成的字段(比如 “Length” 字段)，其高字节在前。

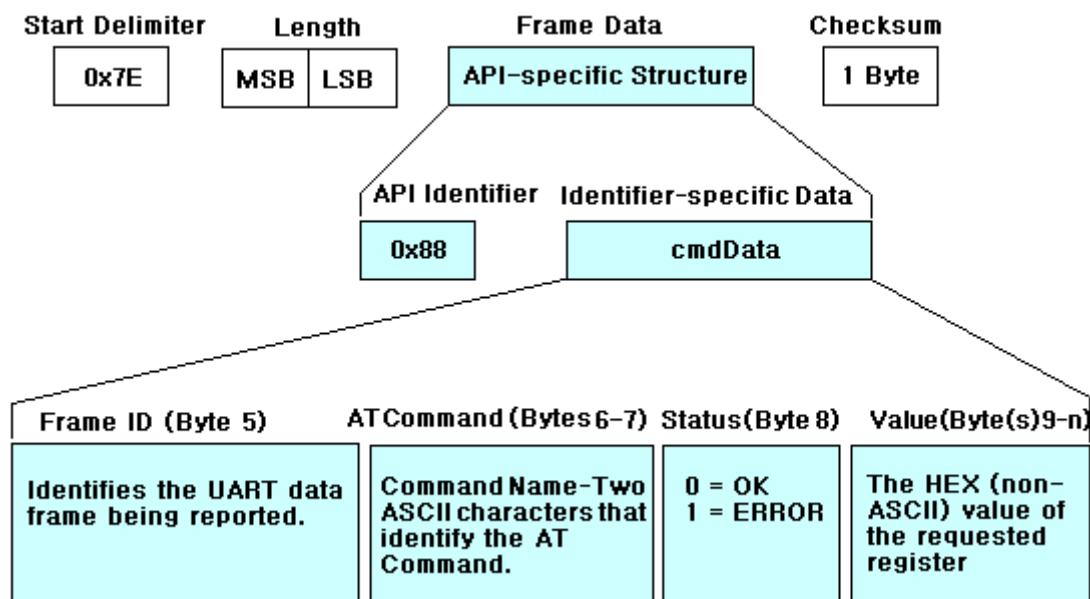
(API模式下) 本地AT命令

在 API 工作模式下，也可以执行 AT 命令，比如用一个 AT 命令读模块的参数或用一个 AT 命令设置一个参数等，与在 AT 命令模式下执行 AT 命令一样，在 API 模式下用 AT 命令设置一个参数后，这个参数是否立即生效或下次重启时生效等，依每个不同的 AT 命令而不同，而用 AT 命令读参数则会立即返回参数结果。

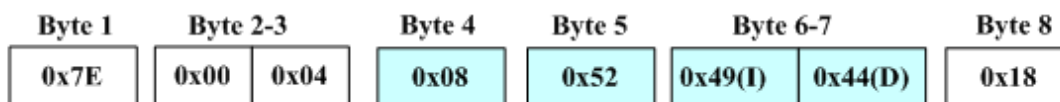
(API 模式下)本地 AT 命令请求的命令码为：0x08，帧结构如下图：



(API 模式下)本地 AT 命令返回的命令码为：0x88，帧结构如下图：

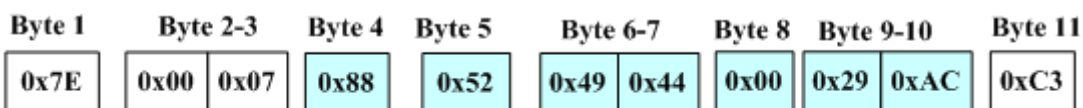


举例：API 模式下用 ID 命令读取模块的 PAN (Personal Area Network) ID，读取 ID 命令请求的数据帧如下图：



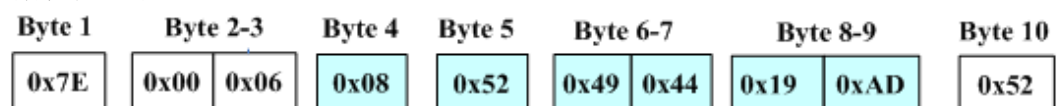
StartDelimiter Length* API Identifier Frame ID ** AT Command Checksum

读取 ID 命令返回的数据帧如下图：



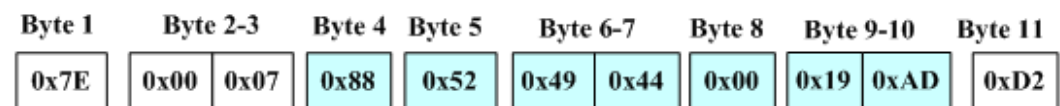
StartDelimiter Length* API Identifier Frame ID ** AT Command Status Value Checksum

API 模式下用 ID 命令设置模块的 PAN ID 为：0x19AD，设置 ID 命令请求的数据帧如下图：



StartDelimiter Length* API Identifier Frame ID ** AT Command Status Value Checksum

设置 ID 命令返回的数据帧如下图：



StartDelimiter Length* API Identifier Frame ID ** AT Command Status Value Checksum

(API 模式下) 远程 AT 命令

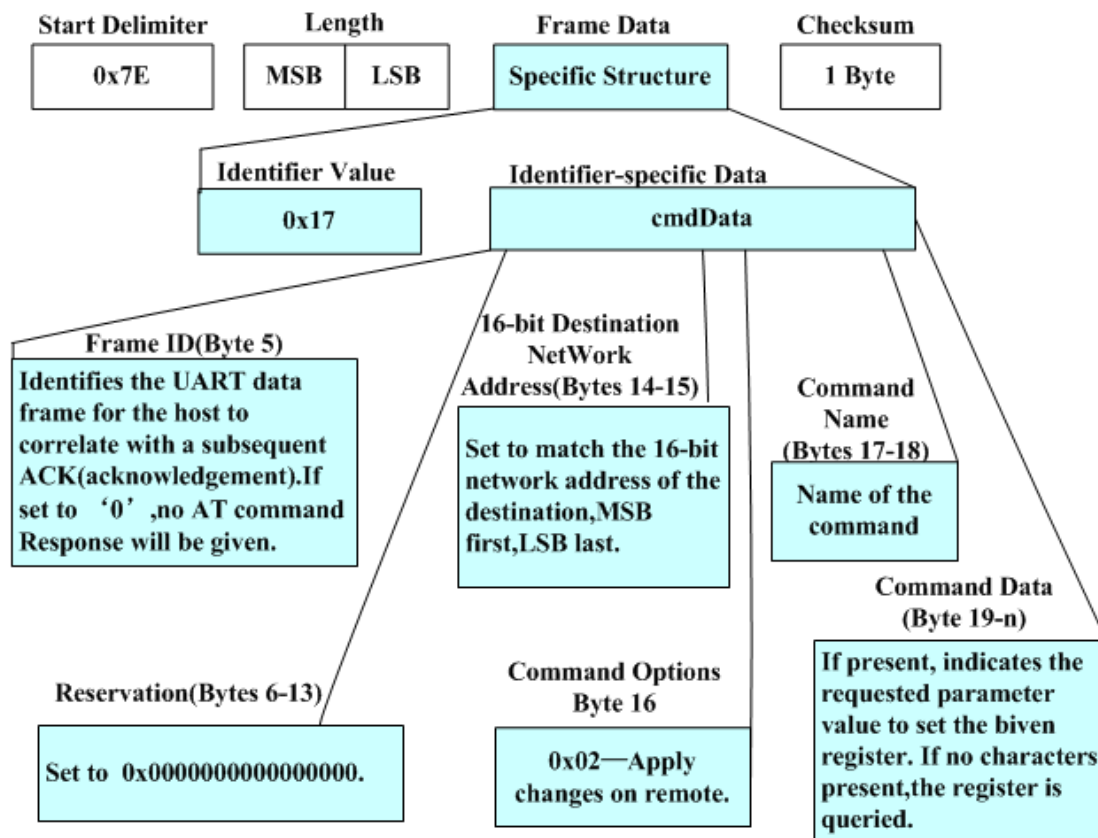
远程 AT 命令用于读取 ZigBee 网络中的一个远程目的节点参数设置或者更改这个远程目的节点参数设置等。

远程 AT 命令是工作在 API 模式下的，即通信数据需按照 API 的帧结构来定义，与在 AT 命令模式下执行 AT 命令一样，在 API 模式下用远程 AT 命令设置指

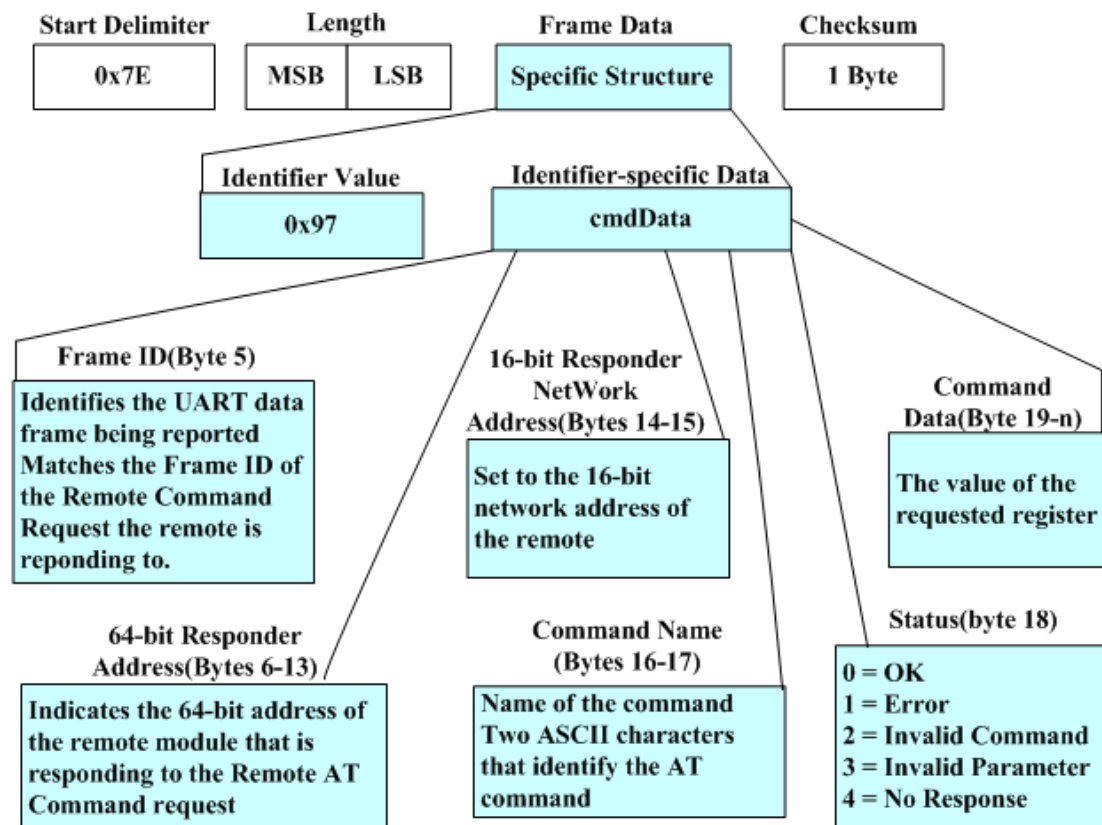
定模块的一个参数后，这个参数是否立即生效或下次重启时生效等，依每个不同的远程 AT 命令而不同。

要读取或更改这个远程节点的设置，必须知道这个目的节点的短地址，且这个目的节点必须上电在网(在线)。用远程 AT 命令读参数会立即返回参数结果，当用远程 AT 命令读网络中远程节点的参数时，输入命令中无需 AT 命令的参数。

(API 模式下)远程 AT 命令请求的命令码为：0x17，帧结构如下图：



(API 模式下)远程 AT 命令返回的命令码为：0x97，帧结构如下图：



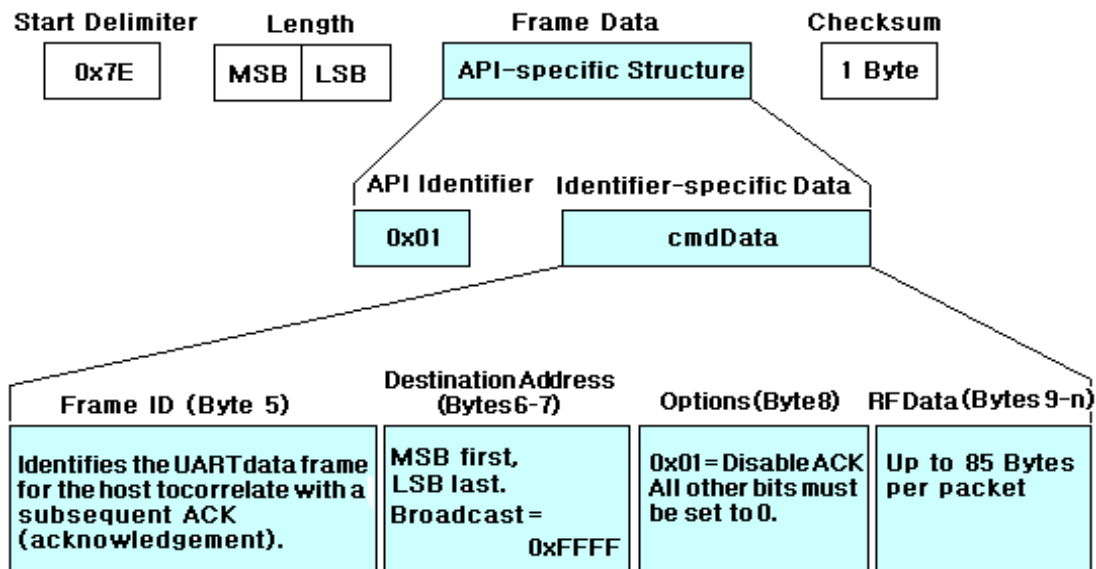
远程AT命令

序号	AT 命令	命令描述	其它说明
1	AP	远程节点工作模式	查询、设置
2	BD	远程节点串口波特率	查询、设置
3	CH	远程节点工作信道	查询
4	DS	远程节点 16-bit 目的地址	查询、设置
5	FR	远程节点系统重新启动	执行
6	HV	远程节点硬件版本	查询
7	ID	远程节点设置的 PAN ID	查询、设置
8	MP	远程节点的父节点的 16 bit 地址	查询
9	MT	远程节点设备类型	查询
10	MY	远程节点 16-bit 源地址	查询
11	NI	远程节点描述串	查询、设置
12	PI	远程节点实际的 PANID	查询
13	PL	远程节点功率级别	查询、设置
14	PT	远程节点第 6 管脚的开关量	查询、设置
15	RE	远程节点恢复出厂设置	执行
16	RN	远程节点下次启动时重置网络	查询、设置
17	RR	远程节点空中发送失败时重试次数	查询、设置
18	S1	远程节点第 20 管脚的电压值	查询
19	S2	远程节点第 19 管脚的电压值	查询
20	S3	远程节点第 18 管脚的电压值	查询
21	S4	远程节点第 17 管脚的电压值	查询
22	SC	远程节点的搜索信道	查询、设置
23	SH	远程节点 IEEE 64-bit 地址高 32bit	查询
24	SL	远程节点 IEEE 64-bit 地址低 32bit	查询
25	SM	远程节点休眠模式(仅对 EndDevice 有效)	查询、设置
26	SP	远程节点保存、获取数据周期	查询、设置
27	ST	远程节点休眠唤醒后工作的时间 (仅对 EndDevice 有效)	查询、设置
28	VR	远程节点软件版本	查询
29	WR	远程节点写设置	执行

(API 模式下)16-bit 地址的数据收发

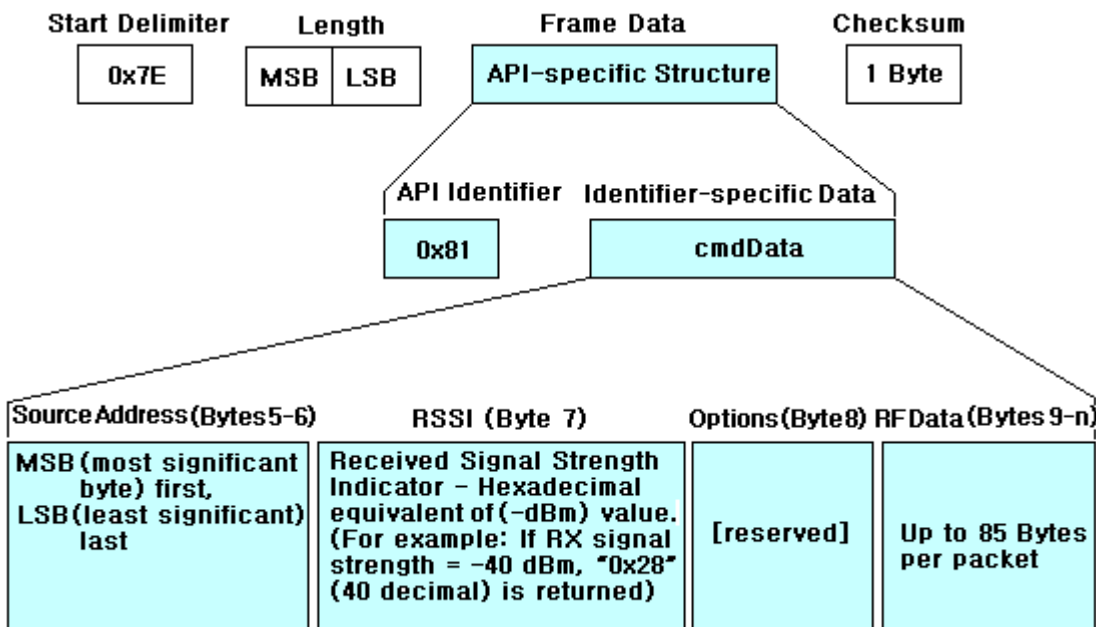
模块在收到命令码为 0x01 的数据发送请求帧后，将会把数据帧中的“RF Data”字段的内容，发送到“Destination Address”指定的 16-bit 目的地址。

(API 模式下)按 16-bit 地址发送数据的命令码为：0x01，帧结构如下图：



当模块收到空中数据后，将按照以下的帧结构定义将数据打包后发送到串口。

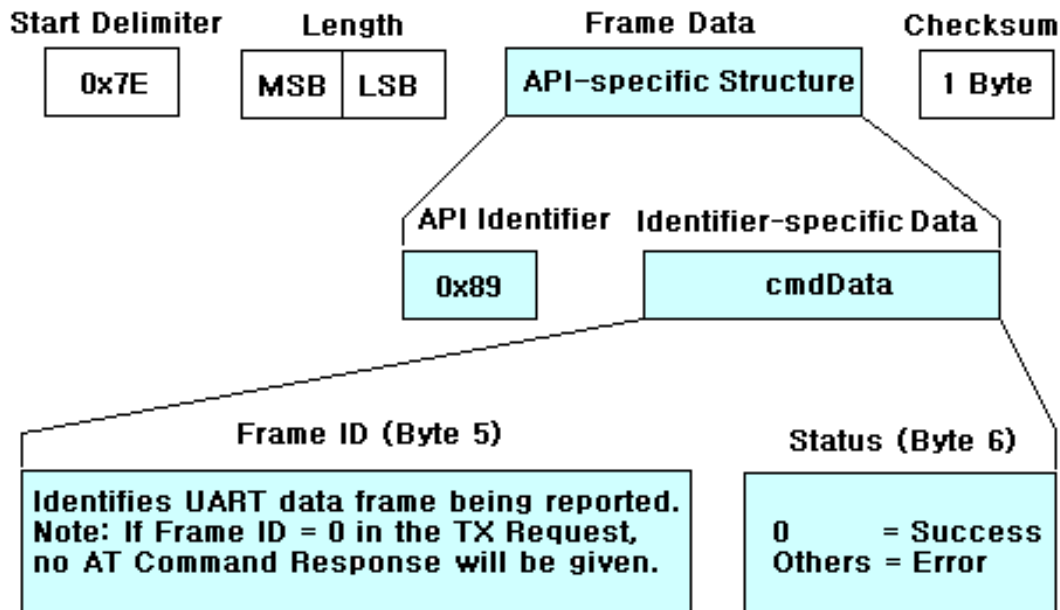
(API 模式下)按 16-bit 地址接收数据的命令码为：0x81，帧结构如下图：



(API 模式下)数据发送状态

当模块完成一个数据发送的 API 命令(命令码 0x01)后，如果未禁止 ACK，无论是否成功发送，那么模块都将返回一个发送状态帧。

(API 模式下)数据发送状态的命令码为：0x89，帧结构如下图：



5.4 常见问题

5.4.1 如何发送广播？

当一个模块发出广播数据时，同一个 PAN ID 网络中的其它所有模块（信道也必须相同）都将收到此广播数据。

透明模式下的广播

在透明模式下，将 16bit Dest Address 设置为 0xFFFF，设置命令为 ATDS，这样，在透明模式下，从模块串口输入的所有数据，将以广播的方式发送。

API 模式下的广播

在 API 模式下，只需将 16bit 的目的地址设置为 0xFFFF，这样，在 API 模式下，数据将以广播的方式发送。

5.4.2 如何在透明模式下将数据发送到一个指定模块？

当一个模块处于透明模式时，除了可以发送广播数据外，也可以将数据发送到一个指定模块，方法是：

从串口连续输入“+++”并停顿换到 AT 命令模式；

用 ATAP 命令设置透明工作模式，即 ATAP 0<CR>;

用 ATDS 命令设置希望的目的短地址，如 ATDS 1A93<CR>;

用 ATWR 命令写入到非易失内存，即 ATWR<CR>;

输入“ATCN<CR>”命令后退出 AT 命令模式。

5.4.3 怎样知道一个模块是否已加入网络？

可以通过读模块的短地址 (Short Address or 16bit Address, AT 命令为 ATMY) 来确定这个模块是否已加入网络，如果它的短地址为 0xFFFFE 则它还没有加入网

络，如果它的短地址小于 0xFFFFE 则说明其已加入了一个 ZigBee 网络。

需要注意的是，Coordinator 是永远都在网的，而一个模块如果加入了一个 ZigBee 网络，除非使用 ATRN 命令使其重新初始化网络，那么它将一直在网，即便掉电后重新上电，其也是在网状态，其短地址也一般不会变化。

5.4.4 怎样让模块一上电就在 API 模式下工作？

设置模块进入 API 模式可使用 AT 命令；

进入上位机软件“HAC Studio For ZigBee”的 AT Command 页面；

连续输入“+++”，并等待模块返回“OK”；

输入“ATAP 1<CR>”命令，模块返回“OK”，这是将模块置为 API 模式；

输入“ATWR<CR>”命令，模块返回“OK”，这是将设置保存，以便模块下次上电时的工作模式为 API 模式；

输入“ATCN<CR>”退出 AT 命令模式，现在，模块即在 API 模式下工作，重新上电后，它也会直接进入 API 模式。

5.4.5 怎样更改模块的串口波特率？

更改模块的串口波特率可使用 AT 命令中的命令 ATBD，其参数为 0—7，以将波特率改为 38400bps（对应的参数为 5）为例；

进入上位机软件 HAC Studio For ZigBee 的 AT Command 页面；

连续输入“+++”，并等待模块返回“OK”；

输入“ATBD 5<CR>”命令，模块返回“OK”，这是将串口波特率置为 38400；

输入“ATWR<CR>”命令，模块返回“OK”，这是将设置保存，以便模块下次上电时的串口波特率为 38400 bps；

输入“ATFR<CR>”命令，这是让模块重新启动，重新启动后，模块串口将在 38400bps 下工作。

注意：上位机软件 HAC Studio For ZigBee 的串口波特率设置必须与模块的串口波特率设置一致才能与模块进行正常通信，在模块更改了波特率后，上位机软件 HAC Studio For ZigBee 也要调整自己串口的波特率设置。

5.4.6 EndDevice 的休眠与休眠控制

EndDevice 进入休眠状态有三个前提条件，第一，EndDevice 已加入到 ZigBee 网络；第二，SM 参数设置为 1，即休眠允许；第三，模块的休眠控制管脚为休眠允许，即管脚 9 为高电平，当这三个条件同时都满足时，EndDevice 才进入休眠状态。

当模块进入休眠后，它将收不到空中数据，也收不到串口数据，其休眠时间的长短与休眠周期 SP 的设置有关，缺省的休眠周期为 0x12C，单位为 10mS，因此，EndDevice 将每 3000mS 唤醒一次，唤醒后，到其父节点那里去提取其它节点发给自己的空中数据。需要注意的是，即使 EndDevice 不休眠，EndDevice 也是按此周期时间去父节点那里提取其它节点发给自己的空中数据。

若想不定期唤醒模块，向模块发送串口数据是不可行的，因为向模块发送串口数据时，模块完全有可能在休眠，因此，唤醒模块的可靠方式是通过休眠控制管脚来唤醒它，只需要将 EndDevice 的管脚 9 置为低电平即可，只要其保持低电平，EndDevice 将持续处于工作状态而不休眠。模块的管脚 9 与测试板的 Switch 的 4 脚相连，因此，当 EndDevice 插在测试板上时，当 Switch 的 4 处于 OFF 时允许休眠，当 Switch 的 4 处于 ON 时不允许进入休眠。

另需要注意的是，当模块上电后，需要始终工作在 ZigBee 网络环境中才能省电，当模块处于无 ZigBee 网络状态时，由于模块需要不断寻找 ZigBee 网络加入，它并不进入休眠状态，这也意味着并不省电。

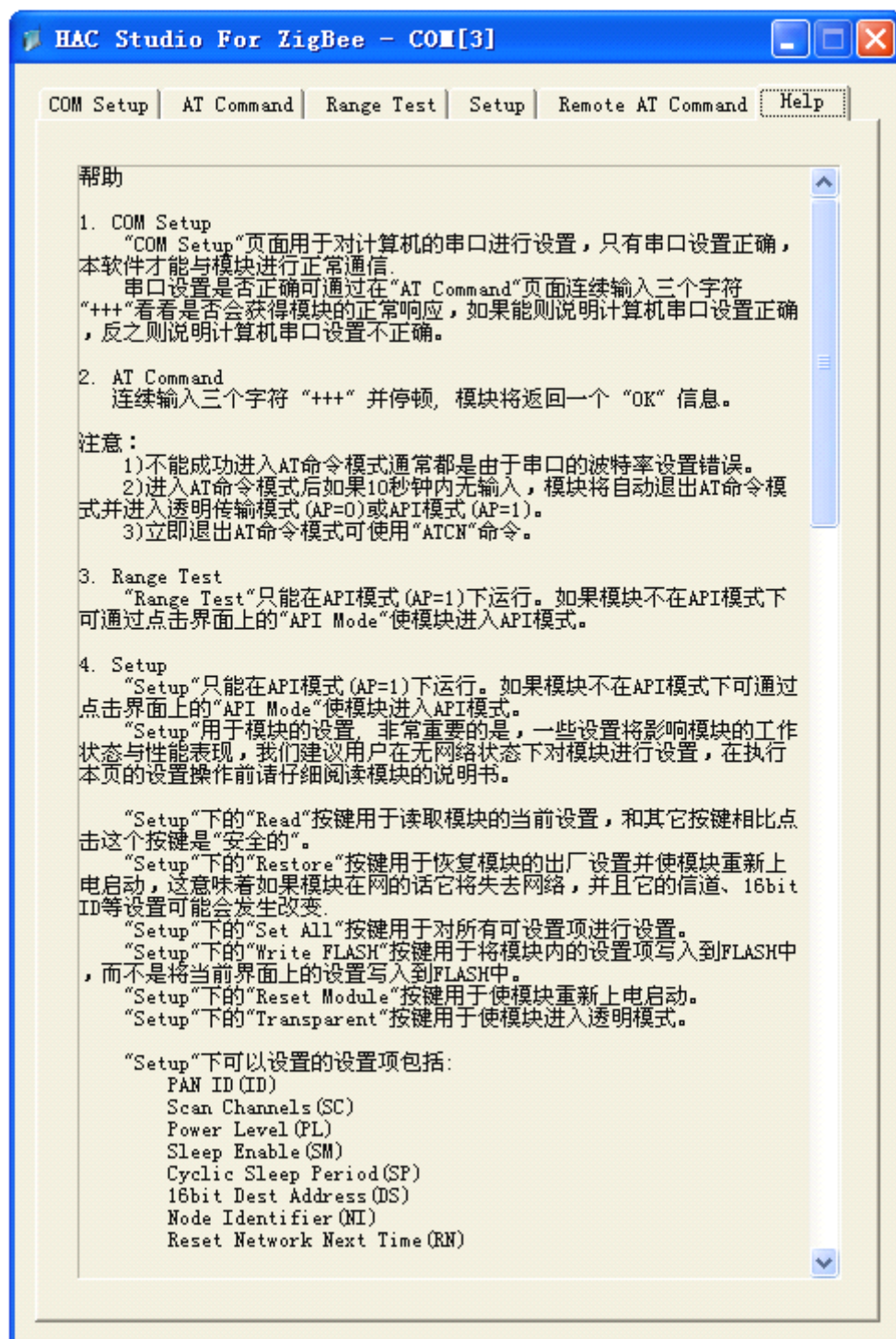
5.4.7 HAC-UBee V3.1-2.2 模块空中数据发送的净载荷

HAC-UBee V3.1-2.2 模块空中数据发送的净载荷取决于模块的当前运行状态、系统可分配资源等因素，但至少不少于 80 字节，若模块的空中数据传输为非加密模式，则其净载荷要大于 80 字节(注：空中数据数据传输为加密模式的模块需要订制)。

六、辅助软件

我们提供了一款上位机软件“HAC Studio For ZigBee V2.2”辅助 HAC-UBee V3.1-2.2 的评估、测试与设置，软件共分六个部分。

- “COM Setup” 页用于设置计算机串口，只有当计算机串口设置正确的情况下，辅助软件才能与模块进行正常通信。
- “AT Command” 页用于显示输入 AT 命令和执行结果。
- “Range Test” 页用于模块的通信测试，仅在 API 模式 (AP=1) 下正确运行。
- “Setup” 页用于模块的设置。非常重要的一点是，一些设置将影响模块的工作状态与性能表现，我们建议用户在无网络状态下对模块进行设置，“Setup” 页只能在 API 模式 (AP=1) 下运行。
- “Remote AT Command” 页用于操作远程 AT 命令，仅在 API 模式 (AP=1) 下正确运行。
- “Help” 是软件的帮助部分，建议用户在使用这个软件前，先仔细阅读软件中的“Help”部分。



七、附录

附件 1:

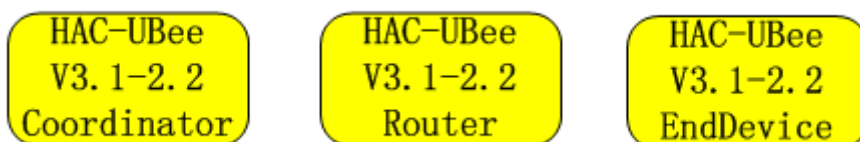
ZigBee 简介

1. 什么是 ZigBee

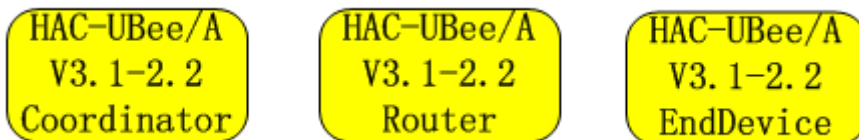
ZigBee 联盟是一个基于全球开放标准，倡导可靠、具有成本效益、低能耗的无线通信解决方案的全球企业联盟。而 ZigBee 是由 ZigBee 联盟推出的一种短距离、低功耗、低成本的无线通信技术。国际知名公司如 TI、Motorola、SIEMENS、PHILIPS 均是 ZigBee 联盟的一员。

2. ZigBee 的模块类别

我公司提供的 ZigBee 模块采用 TI 公司的 ZigBee 协议栈，按模块在网络中的作用不同，可分为三种，一种为协调器(Coordinator)，一种为路由器(Router)，另一种为终端设备(EndDevice)这三种模块的外观与接口均相同，它们可通过标签来区别，也可以通过我公司提供的上位机软件读出。



图一 非加密模块标签



图二 加密模块标签

3. ZigBee 网络

一个 ZigBee 网络中有且只能有一个协调器，协调器用于网络的组建，只有在协调器上电数秒后网络才能启动，协调器为网络的第一个节点，随后，路由器可以与协调器连接并加入到网络中来，同时，加入到网络的路由器还允许其它路由器通过连接自己加入到网络，网络中的任意二个节点可以进行点对点通讯，同时，网络中的任一节点也可以向网络中的其它所有节点进行广播。

一个模块能否加入网络取决于在其通讯距离内是否有已加入网络的节点，如果网络中与自己最近的节点的距离大于模块的通讯距离(参见模块的技术指标)，那么这个节点将脱网而无法与网络中的任一节点通讯。

ZigBee 网络的组建是在模块上电后自动完成的，用户无需操控。模块上电的先后顺序似乎并不特别重要，但只有在协调器上电后，ZigBee 网络才开始组建，一旦有路由器加入到网络，即使协调器断电，这个网络仍可正常工作，但对于数据加密传输的模块，其加入网络时，协调器必须在线。

协调器上电组建网络需要搜索最合适的信道，而路由器要加入网络同样需要搜索信道、寻找网络、进行连接等，这些过程需要约几秒到几十秒的时间不等。对协调器与路由器而言，一旦模块加入网络后，它会将其网络状态记录到非易失内存中，包括其 PAN ID、信道、16-bit 地址等，除非重新初始化其网络，那么，这个模块将始终处于在网的状态。

一个网络中的所有模块，均具有相同的 PAN ID 和信道。

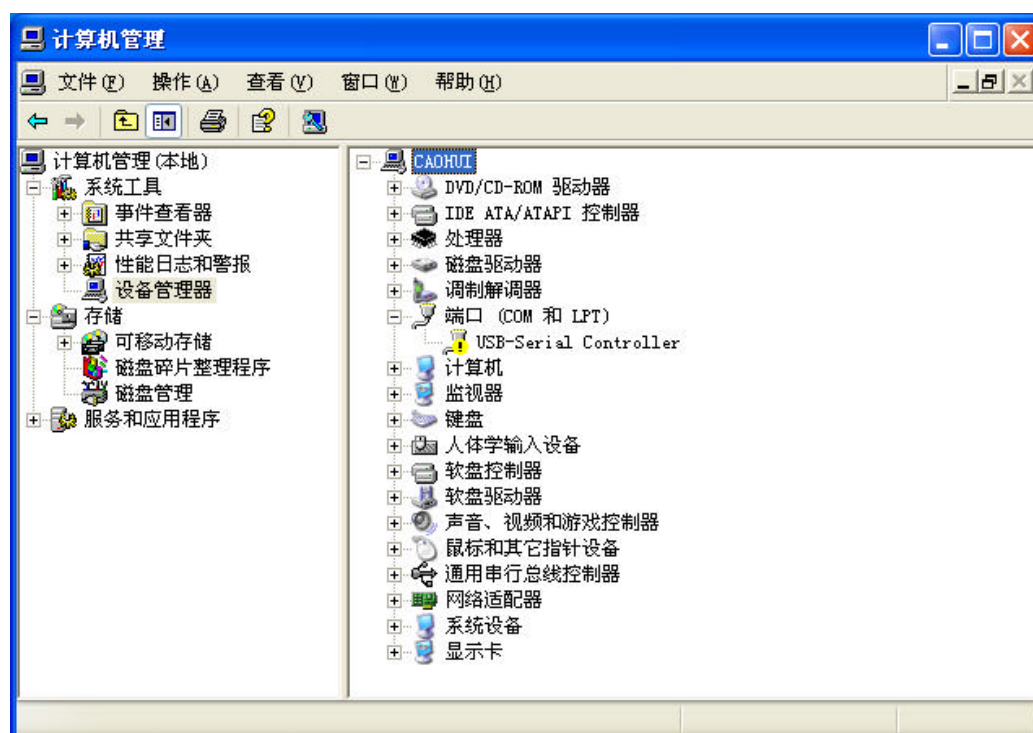
4. 模块的 64-bit 地址与 16-bit 地址

64 bit 地址，又称 IEEE 地址、64-bit ID 或 Serial Number，每个模块出厂时的 64 bit 地址是由模块所使用的芯片厂商提供的，芯片厂商保证了 64 bit 地址的全球唯一性。而模块的 16-bit 地址又称短地址或 16-bit ID，是在模块加入到 ZigBee 网络后获得的，在模块加入到一个 ZigBee 网络之前，它的 16-bit 地址为 0xFFFE，这个 16-bit 地址是无意义的，一旦模块加入到 ZigBee 网络后，它将获得一个小于 0xFFFE 的 16bit 地址，在这个网络中，这个 16-bit 地址是唯一的，除非你重置网络，否则这个 16-bit 地址将一直属于这个模块，即便这个模块掉电后重新上电，它的这个 16-bit 地址一般也不会改变。

Coordinator 的 16-bit 地址在网络中是固定的，它的 16-bit 地址总是 0x0000。

附件2:

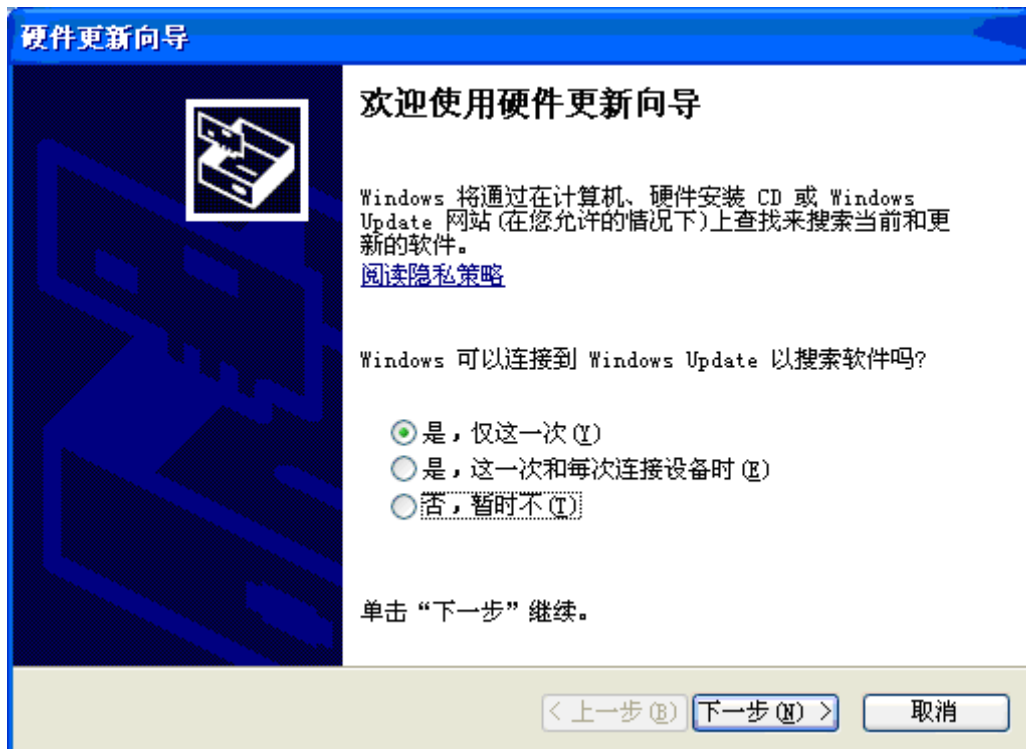
1. 把USB转串口线的一端与HAC-DEV相连，另一端插入电脑的USB口相连，打开 → 设备管理器；



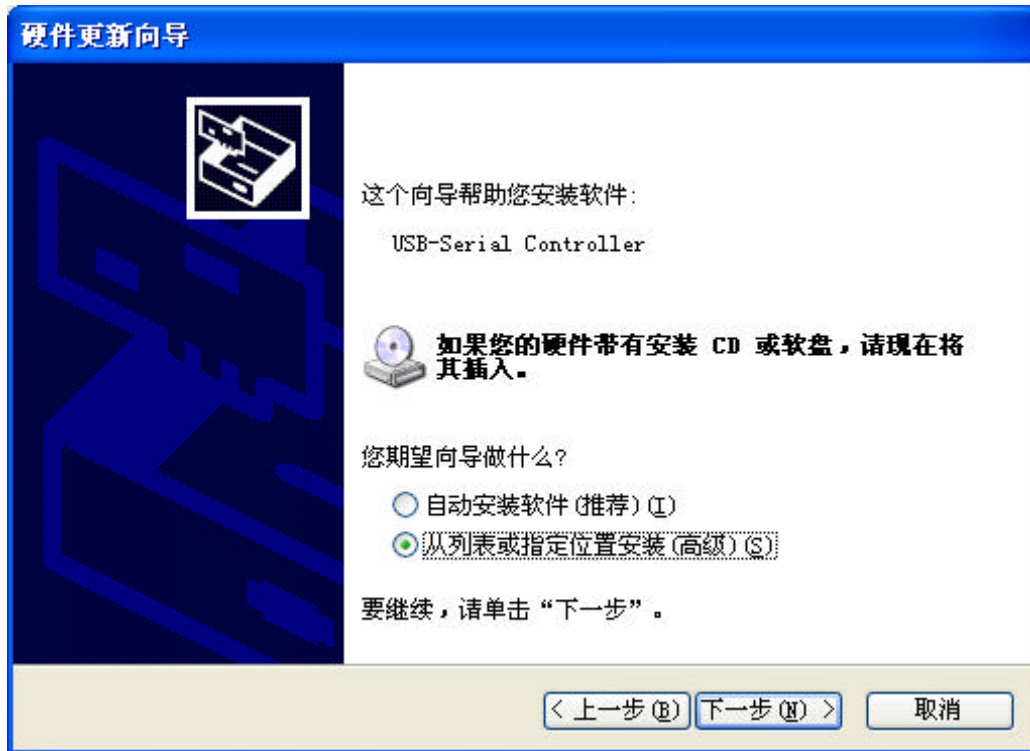
2. 点击USB-Series Controller;



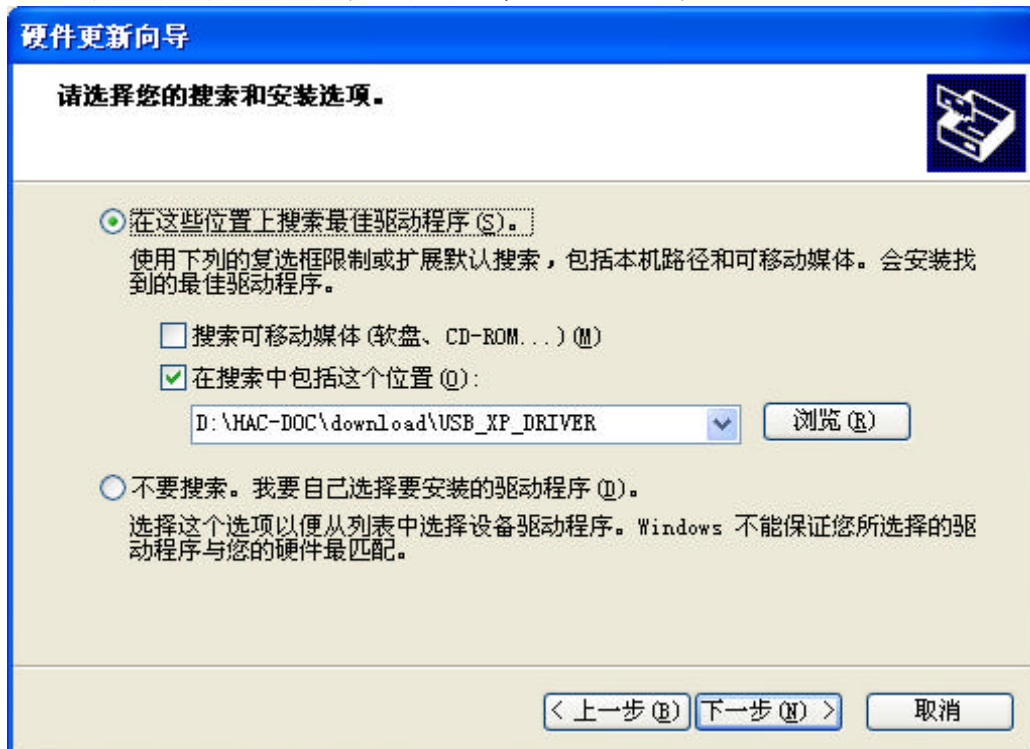
3. 点击重新安装驱动程序:



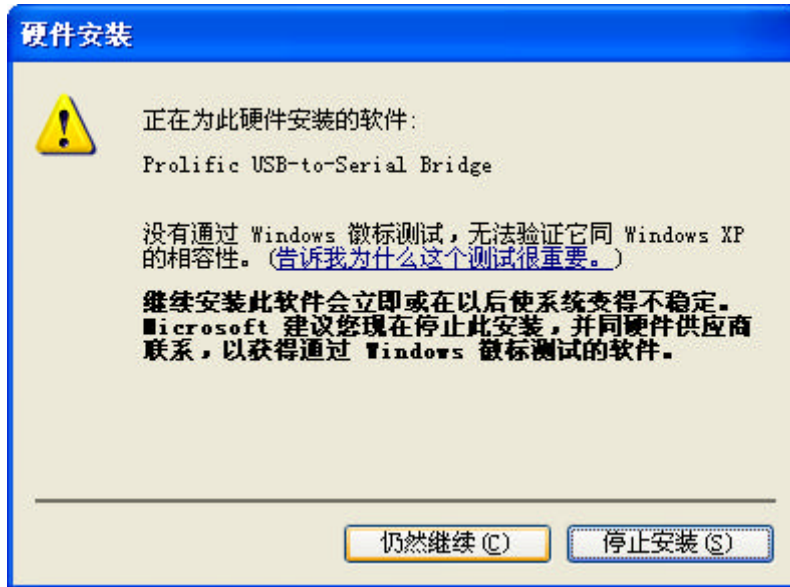
4. 选择“是，仅这一次”，点击“下一步”；



5. 选择“从列表或指定位置安装”, 点击“下一步”;



6. 点击“在搜索中包括这个位置”, 浏览到驱动程序保存的位置, 点击“下一步”;

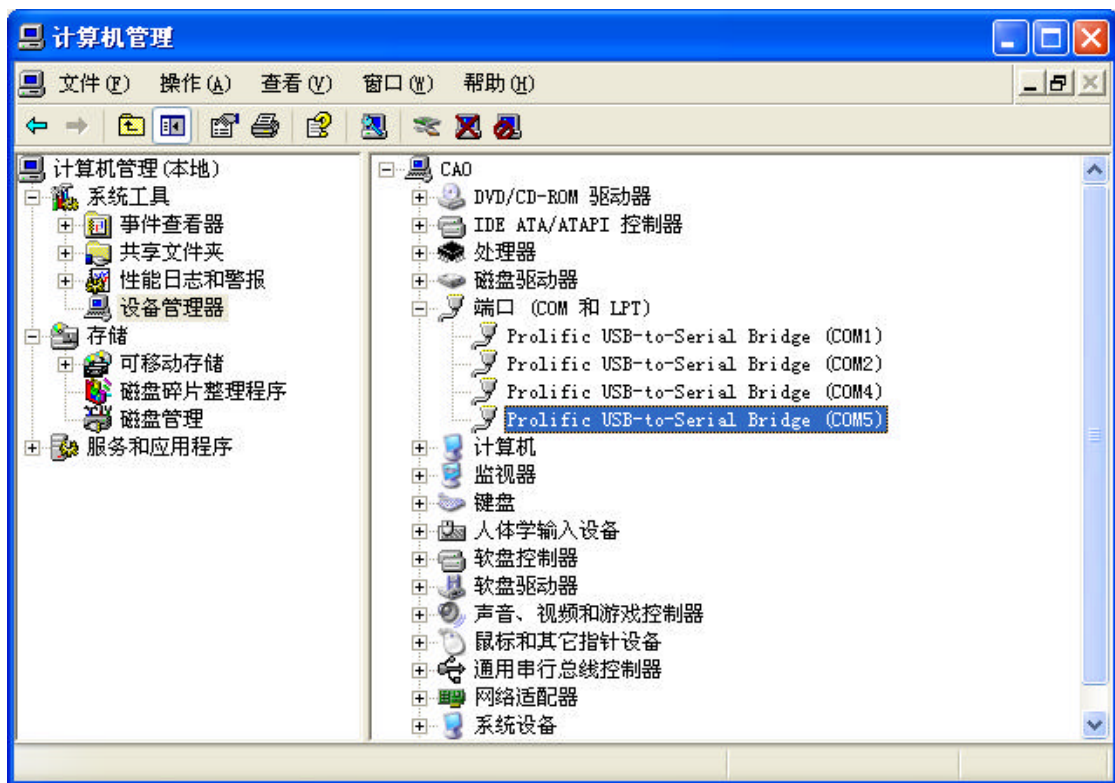


7. 点击“仍然继续”；



8. 安装完成。

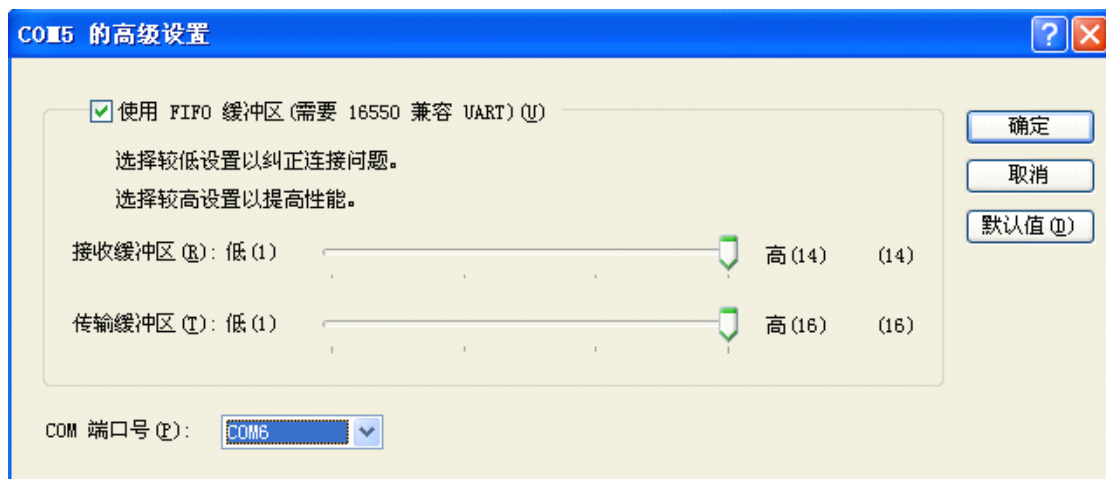
9. 串口的设置, 在“设备管理器”的“端口 (COM 和LPT)”中找到“Prolific USB_to_series Bridge(COM)”双击；



10. 点击“端口设置”中的“高级”；



11. 设置与HAC-DEV用到的串口（如COM6），点击确定键；



此时串口设置完成，用户可以在上位软件中打开 COM6 与无线模块进行数据传输。上位机软件中打开串口的波特率、校验位等要与无线模块的设置相一致。