
HAC-EmBee-A11D

HAC-EmBee-A11N

2.4G 低功耗无线数传模块

(ZigBee)

用户手册

V 2.02.2 2013/10/25



深圳市华奥通通信技术有限公司

SHENZHEN HAC TELECOM TECHNOLOGY CO., LTD

地址：深圳市南山区西丽路 4227 号大学城创意园 2 栋 6 楼

电话：+86-755-23981078

传真：+86-755-23981007

邮件：webmaster@rf-module-china.com

网址：<http://www.rf-module-china.com>

➤ 高性能

- ◇ 20dbm 可视距离 2.8km
- ◇ 7dbm 可视距离 850m

➤ 低功耗

- ◇ 20dbm 发射电流 145mA，接收电流 38mA，休眠电流 3uA
- ◇ 7dbm 发射电流 42mA，接收电流 29mA，休眠电流 3uA

➤ MESH 网络

- ◇ 自动组网，自动路由，自动愈合
- ◇ 点对点，点对多点传输
- ◇ 最多高达 16 跳传输

➤ 使用简单

- ◇ AT 命令
- ◇ API 命令
- ◇ API 远程 AT 命令
- ◇ 透明传输

➤ 符合标准

- ◇ Zigbee 2007 Pro
- ◇ All Profile

➤ 高可靠性

- ◇ DSSS O-QPSK 调制方式
- ◇ CSMA-CA 自动退避机制
- ◇ 重发与应答机制

➤ 高安全性

- ◇ 网络层 AES 加密
- ◇ 应用层 AES 加密

目录

1 EmBee 模块	6
1.1 EmBee 模块尺寸及管脚顺序	6
1.2 模块管脚分布	7
1.3 模块性能参数	8
1.3.1 HAC-EmBee-A11N 参数	8
1.3.2 HAC-EmBee-A11D 参数	9
2 EmBee 模块操作	10
2.1 UART 串口介绍	10
2.2 通信协议	10
2.2.1 透明传输模式	10
2.2.2 API 传输模式	11
2.3 AT 命令模式	11
2.3.1 进入 AT 命令模式	12
2.3.2 发送 AT 命令	12
2.3.3 AT 命令响应	12
2.3.4 退出 AT 命令模式	13
2.4 回环功能	13
2.4.1 透传模式的回环	13
2.4.2 API 模式的回环	13
3 API 操作	14
3.1 API 帧格式	14
3.2 API 帧	15
3.2.1 AT 命令帧（立即生效）	15
3.2.2 AT 命令帧（不立即生效）	16
3.2.3 AT 命令响应帧	17



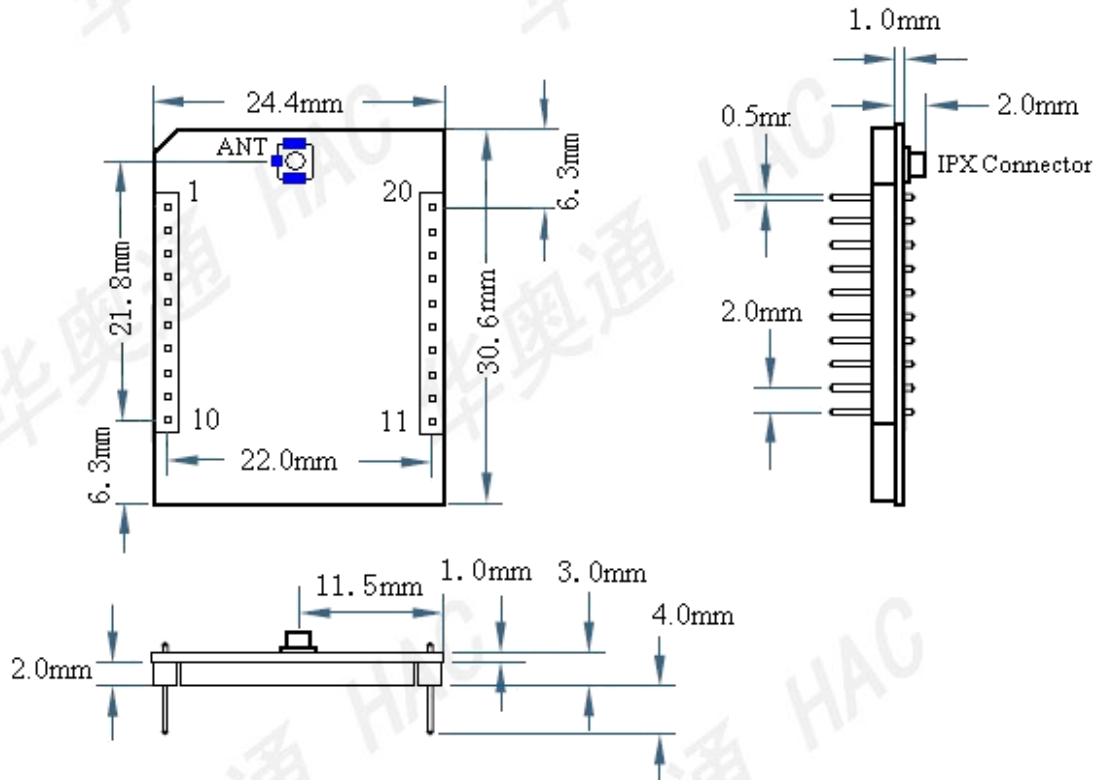
3.2.4	传输请求帧	18
3.2.5	应用层可选的传输请求帧	19
3.2.6	传输状态帧	21
3.2.1	数据接收指示帧 (A0=0)	22
3.2.2	数据接收指示帧 (A0=1)	23
3.2.3	I/O 接收指示	24
3.2.4	节点发现指示	26
3.2.5	模块状态指示帧	28
3.2.6	远端 AT 命令请求帧	29
3.2.7	远端 AT 命令响应帧	30
4	AT 命令	32
4.1	地址命令	32
4.2	网络命令	34
4.3	射频参数命令	36
4.4	串口参数命令	37
4.5	I/O 参数命令	38
4.6	诊断参数命令	41
4.7	AT 命令参数	42
4.8	休眠命令	42
4.9	命令执行	43
5	数字 I/O 和模拟 I/O	45
5.1	本地 I/O	45
5.1.1	AT 命令模式下读取本地 I/O 电平值和采样值	45
5.1.1	AT 命令模式下配置本地 I/O	46
5.1.2	API 模式下配置本地 I/O	47
5.2	远端 I/O	47
5.2.1	API 模式下配置远端 I/O	47

6 EmBee ZigBee 网络	48
6.1 协调器.....	48
6.2 路由器.....	49
6.3 终端设备.....	49
6.3.1 子节点与父节点关系.....	50
6.3.2 子节点容量.....	50
6.4 子节点工作过程.....	51
6.5 父节点工作过程.....	51

1 EmBee 模块

1.1 EmBee 模块尺寸及管脚顺序

EmBee 模块的外形结构如下：



管脚顺序从 PIN1 开始，逆时针依次至 PIN20。

1.2 模块管脚分布

针脚	命名	方向	默认状态	说明
1	VCC			电源
2	DOUT	双向	输出	UART 数据输出
3	DIN	双向	输入	UART 数据输入
4	DI012(目前未开放)	双向	输入	GPIO
5	RESET	输入		模块复位
6	DI010(目前未开放)	双向	输入	GPIO
7	DI011(目前未开放)	双向	输入	GPIO
8	保留		禁用	不要连接
9	SLEEP_RQ / DI08	双向	输入	休眠控制/GPIO
10	GND			地
11	DI04	双向	输入	GPIO
12	CTS / DI07	双向	输出	UART 流控 CTS/GPIO
13	ON_SLEEP / DI09	双向	输出	休眠指示/GPIO
14	DI020(目前未开放)	输入	输入	GPIO
15	DI05(目前未开放)	双向	输入	GPIO
16	RTS / DI06	双向	输入	UART 流控 CTS/GPIO
17	AD3 / DI03	双向	输入	模拟输入 3/GPIO
18	AD2 / DI02	双向	输入	模拟输入 2/GPIO
19	AD1 / DI01	双向	输入	模拟输入 1/GPIO
20	AD0 / DI00	双向	输入	模拟输入 0/GPIO

1.3 模块性能参数

1.3.1 HAC-EmBee-A11N 参数

名称	HAC-EmBee-A11N 参数			单位
	最小值	典型值	最大值	
电气性能 (25℃)				
供电电压	2.2	3.3	3.6	V
接口电平	-0.3		$VCC+0.3 \leq 3.6$	V
发射电流	40	42	45	mA
接收电流	28	29	32	mA
休眠电流		0.9	3	uA
无线性能 (25℃)				
工作频率	2.405		2.485	GHz
发射功率	6	6.5	7	dBm
接收灵敏度		-102		dBm
无线传输速率		250		kbps
一般性能				
接口速率	1200	9600	115200	bps
工作温度	-40		80	℃
可视传输距离		850		m

1.3.2 HAC-EmBee-A11D 参数

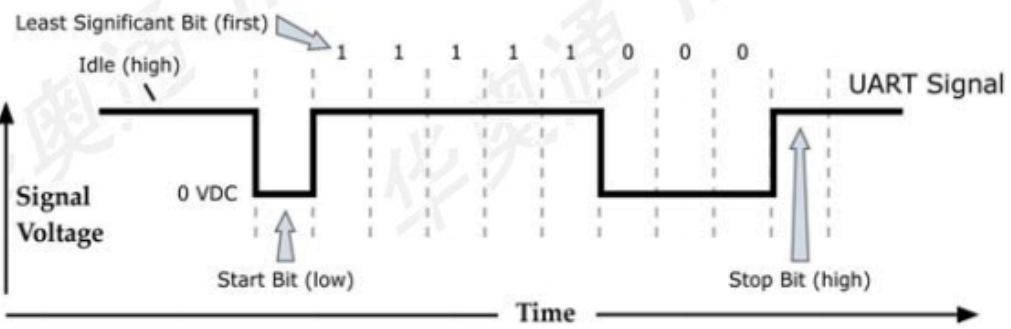
名称	HAC-EmBee-A11D 参数			单位
	最小值	典型值	最大值	
电气性能 (25℃)				
供电电压	3.0	3.3	3.6	V
接口电平	-0.3		VCC+0.3≤3.6	V
发射电流	140	145	150	mA
接收电流	35	38	42	mA
休眠电流		1.2	3	μA
无线性能 (25℃)				
工作频率	2.405		2.485	GHz
发射功率	19	20	21	dBm
接收灵敏度		-107		dBm
无线传输数率		250		kbps
一般性能				
接口数率	1200	9600	115200	bps
工作温度	-40		80	℃
可视传输距离		2800		m

2 EmBee 模块操作

2.1 UART 串口介绍

EmBee 模块是通过 UART 串口来控制，见硬件管脚说明，TX 脚当没有数据发送，处于空闲状态时，应为高电平。

每个字节数据由起始位（低），8 位为数据位（低位先发）和停止位（高）组成。下图是“0x1F”字节的传输波形图。



在实际操作过程中，要注意外部控制器和 EmBee 模块的 UART 通信口要设置相同的波特率、奇偶校验和停止位。EmBee 模块的波特率可以通过 DB 命令来设置（其默认波特率为 9600），奇偶校验可以通过 NB 命令来设置（其默认是采用无奇偶校验），停止位可以通过 SB 命令设置（其默认采用 1 位停止位）。

2.2 通信协议

EmBee 模块支持透明传输模式和 API 模式。

2.2.1 透明传输模式

透明传输模式下，EmBee 模块不对 UART 口的数据采取任何处理。即把从 UART_RX 口接收到的任何数据都通过 RF 向空中发射出去，而通过 RF 从空中接收到的数据也直接从 UART_TX 口输出。

透明传输模式通过 AT 命令来设置，设置 AP=0，并退出 AT 命令模式，则处

于透明传输模式。注意与下面的 API 模式区别，API 模式要求 AP=1。

透明传输模式下，当 EmBee 模块从 UART_RX 口接收到数据，满足下面条件之一，就把数据通过 RF 发射出去：

在一定的时间内，UART_RX 口没有接收到数据。该时间可以通过 R0 命令设置。

已经收到了一个 RF 数据包的最大数量的字节。

2.2.2 API 传输模式

当 EmBee 模块工作在 API 模式下，其 UART 口以帧的格式进行接收或发送数据。可以通过 AT 命令来设置 API 传输模式，设置 AP=1，并退出 AT 命令模式，则进入 API 模式。在该模式下用户可以与网络层的一些参数进行交互。

UART 口接收的帧（也就是用户通过 UART 口发送给 EmBee 模块的帧）有：

- (1) RF 发射的数据帧；
- (2) 命令帧（相当于 AT 命令）；

UART 口发送的帧（也就是用户通过 UART 口接收到的 EmBee 模块的帧）有：

- (1) RF 接收到的数据帧；
- (2) 命令响应帧；
- (3) 事件通知帧：如复位类型，加入网络，离开网络等；

在 API 模式下，用户可以在发送的数据帧中加入目的地址以及数据载荷的信息，这样就不需要用命令来设置这些参数。同样，用户接收到的数据帧中也包含了状态信息，源地址，数据载荷信息，处理起来更加方便。

2.3 AT 命令模式

在有些情况下，必须使用 AT 命令进行操作，例如从透明传输模式转变为 API 模式。AT 命令用来读取或设置 EmBee 模块的参数。在 AT 命令模式下，从 EmBee

模块的 UART_RX 口接收到的字符被解释为命令。

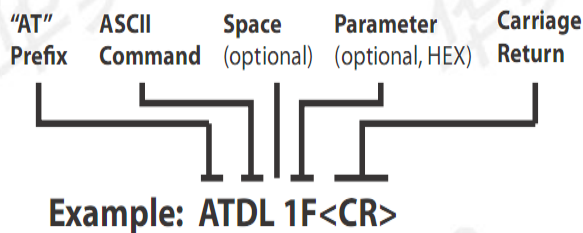
AT 命令操作步骤如下：

2.3.1 进入 AT 命令模式

连续输入 3 个 “+” 字符，即 “+++”，则进入 AT 命令模式。输入时要注意 “+” 字符之间的时间间隔，默认情况下，不要超过 1 秒（见 GT 命令）。一旦进入 AT 命令模式，EmBee 模块启动一个超时定时器，当该时间内（见 CT 命令），若无有效的 AT 命令输入，则自动退出 AT 命令模式。每当一个有效的 AT 命令输入时，该定时器重新计时。

2.3.2 发送 AT 命令

AT 命令按照如下格式进行发送。



AT 命令若是没带参数，则是读取该命令参数值；若带有参数值，则是设置该命令参数值。在上述例子中，是设置 DL 的值为 0x1F。注意，参数只采用 16 进行格式。

另外要注意的是：当改变参数值时，为了复位后，能保持该改变后的值，则改变参数值后要使用 ATWR 命令，即把该值存储到 flash 中，不会因掉电而丢失。

2.3.3 AT 命令响应

当 EmBee 模块接收到 AT 命令后，会解析并执行该命令，若成功执行，则会通过 UART_TX 口输出 “OK”，若是设置的参数范围不正确，则输出 “INVALID_PARAM, ERROR”，若是只读的命令，附带了参数，或者命令执行错误，则会输出 “ERROR”。

2.3.4 退出 AT 命令模式

有如下方法可以退出 AT 命令模式：

发送 ATCN 命令；

在 CT 所规定的时间内没有接收到有效的 AT 命令。

2.4 回环功能

回环功能可以用于测试网络中两个节点之间数据传输的成功率。在回环测试模式下，任何收到的数据将被发送回发送模块端。透明传输模式和 API 数据传输模式都支持回环测试模式。

2.4.1 透传模式的回环

模块的 CI 值设为 0x12，SE 和 DE 值都设为 0xE8，DH 和 HL 设为接收端模块的 64 位地址。当退出 AT 模式时，接收模块收到任何数据都将发送回发送端模块，这样便于测试通信数据的成功率等网络测试。

2.4.2 API 模式的回环

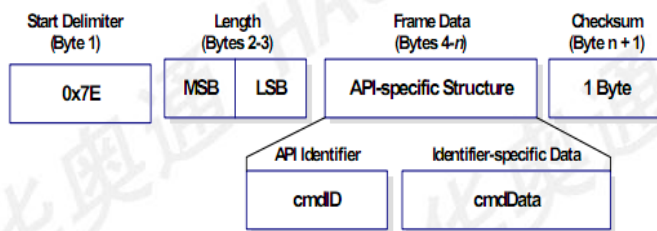
API 模式下，要使用应用层可选址的 API 传输（帧类型 0x91），才支持回环功能。模式的 CI 值为 0x12，SE 和 DE 的值设为 0xE8。当接收端模块接收到数据时，会传回发送端。

3 API 操作

API 是通过帧的格式进行数据的收发。API 模式将指明命令，命令响应以及状态信息是如何通过 EmBee 模块的 UART 口进行交互。

3.1 API 帧格式

当 AP=1，并退出 AT 命令模式时，就可以进入 API 模式，API 帧格式如下：



0x7E: 为帧开始标志。

长度域: 占 2 个字节，帧数据 (Frame Data) 内容所占的字节，不包括 0x7E，长度域本身和校验字节。

帧数据: 不同类型的帧有不同的格式，下面将详细列出。

校验: 帧数据 (Frame Data) 内容所占的字节 (不包括 0x7E，长度域本身) 相加，得到一个数，取最后一个字节，再用 0xFF 减去这个字节，则得到校验码。验证时，只要把帧数据 (Frame Data) 内容所占的字节和校验码相加，得到的数字的最后一个字节是 0xFF，则校验正确。

注意: 上述各域中，若是占有多个字节，则将按大端格式进行发送。

任何帧都以 0x7E 开头，0x7E 之前的数据 EmBee 模块简单的把它丢掉，不做任何处理。如果 EmBee 模块收到该数据帧不正确，例如，字节长度不对，或者校验不对，则也不做任何处理。

3.2 API 帧

在上节中讲到不同的帧类型有不同的帧数据结构，下面详细介绍 EmBee 模块中各种帧结构。

3.2.1 AT 命令帧（立即生效）

该 API 帧的作用相当于 AT 命令模式下的 AT 命令，用于设置或查询本地模块的命令参数。通过该 API 帧设置 AT 命令，一旦命令参数改变，立即生效。该 API 帧的结构如下：

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x08	1
帧序列号	1
AT 命令	2
命令参数（可选）	可变
校验	1

帧开始标识： 0x7E；

长度： 不包括帧开始标识符、长度域和校验；

帧类型： AT 命令帧的帧类型为 0x08；

帧序列号： 该序列号为用户在多帧情况下，标识该 API 帧是第几帧，以便识别。若该序列号为 0，则 EmBee 模块不予响应。

AT 命令： 我们目前所有的 AT 命令为两个字符，例如：“DL”，“ID”等。为 AT 命令字母的 ASCII 值。

命令参数： 若带参数，则表示设置参数；若不带参数，则表示读取参数。

校验： API 帧所有的字节（但不包括帧开始标识 0x7E，长度域本身）相加，

得到一个数，取最后一个字节，再用 0xFF 减去这个字节，则得到校验内容。

3.2.2 AT 命令帧（不立即生效）

该 API 帧也可以查询或设置 AT 命令参数。与 AT 命令帧（立即生效）的 API 帧相比，该帧所设置的参数不能立即生效，若想让所设置的参数生效，则必须使用该值发送 AC 命令，或者发送一个帧类型为 0x08 的 API 帧。该 API 帧的结构如下：

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x09	1
帧序列号	1
AT 命令	2
命令参数（可选）	可变
校验	1

帧开始标识： 0x7E；

长度： 不包括帧开始标识符、长度域和校验；

帧类型： AT 命令帧的帧类型为 0x09；

帧序列号： 该序列号为用户在多帧情况下，标识该 API 帧是第几帧，以便识别。若该序列号为 0，则 EmBee 模块不予响应。

AT 命令： 我们目前所有的 AT 命令为两个字符，例如：“DL”，“ID”等。为 AT 命令字母的 ASCII 值。

命令参数： 若带参数，则表示设置参数；若不带参数，则表示读取参数。

校验： API 帧所有的字节（但不包括帧开始标识 0x7E，长度域本身）相加，得到一个数取最后一个字节，再用 0xFF 减去这个字节，则得到校验内容。

3.2.3 AT 命令响应帧

当用户正确输入 AT 命令帧时，EmBee 模块会输出 AT 命令响应帧。有的命令会输出多帧，如 ND 命令。该 API 帧的结构如下：

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x88	1
帧应答序列号	1
AT 命令	2
命令状态	1
命令参数（可选）	可变
校验	1

帧开始标识： 0x7E；

长度： 不包括帧开始标识符、长度域和校验；

帧类型： AT 命令响应帧的帧类型为 0x88；

帧应答序列号： 该序列号为 AT 命令帧中的序列号；若 AT 命令帧中该序列号为 0，EmBee 模块则不进行响应。

AT 命令： 我们目前所有的 AT 命令为两个字符，例如：“DL”，“ID”等。为 AT 命令字母的 ASCII 值。

参数： 若 AT 命令帧是查询命令，则带命令参数；若是设置命令，则不带命令参数。

校验： API 帧所有的字节（但不包括帧开始标识 0x7E，长度域本身）相加，得到一个数，取最后一个字节，再用 0xFF 减去这个字节，则得到校验内容。

3.2.4 传输请求帧

EmBee 模块接收到一个传输请求帧后，会数据作为 RF 数据包发送到指定的目的地址。当 64 位目的地址设为 0x000000000000FFFF 时，为广播。当 64 位目的地址设为全 0，16 位目的地址设为 0xFFFE 时，或者 64 位目的地址为协调器的 64 位 MAC 地址，16 位目的地址为 0x0000 时，则往协调器发送数据。其他情形下，64 位目的地址一定要填写，16 位目的地址，填写 0xFFFE 即可。

其帧结构如下：

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x10	1
帧应答 序列号	1
64 位目的地址	8
16 位目的网络地址	2
广播跳数	1
传输条件选择	1
数据	可变
校验	1

帧开始标识： 0x7E；

长度： 不包括帧开始标识符、长度域和校验；

帧类型： 该帧类型为 0x10；

帧序列号： 该序列号为用户在多帧情况下，标识该传输请求帧是第几帧，以便识别。若该序列号为 0，则 EmBee 模块不予响应。

64 位目的地址： 目的设备的 MAC 地址，64 位。若该目的地址为 0x0000000000000000，则把数据发往网络中的协调器。若该目的地址为

0x000000000000FFFF，则该地址为广播地址，对该数据进行广播。

16 位目的地址：目的设备的网络地址，该地址为 16 位。若是不知道该地址，或者 64 位目的地址为广播地址，则设为 0xFFFE。

广播跳数：该功能目前暂没开放。使用协议栈所规定的最大跳数。

传输条件选择：该功能目前暂没开放。

数据：用户将要发往目的设备的数据。

校验：API 帧所有的字节（但不包括帧开始标识 0x7E，长度域本身）相加，得到一个数，取最后一个字节，再用 0xFF 减去这个字节，则得到校验内容。

3.2.5 应用层可选的传输请求帧

该帧与传输请求帧相比，还可以通过端点标识号（endpoint）、簇标识号（cluster ID）和应用规范标识号（profile ID）来把数据传输到某个指定的应用层部分。该帧将引起对应的应用层（通过端点标识号（endpoint）、簇标识号（cluster ID）和应用规范标识号（profile ID）来区分）直接进行数据发送。

当 64 位目的地址设为 0x000000000000FFFF 时，为广播。当 64 位目的地址设为全 0，16 位目的地址设为 0xFFFE 时，或者 64 位目的地址为协调器的 64 位 MAC 地址，16 位目的地址为 0x0000 时，则往协调器发送数据。其他情形下，64 位目的地址一定要填写，16 位目的地址，填写 0xFFFE 即可。

其帧结构如下：

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x11	1
帧应答序列号	1
64 位目的地址	8
16 位目的网络地址	2
源端点标识号	1

目的端点标识号	1
簇标识号	2
应用规范标识号	2
广播跳数	1
传输条件选择	1
数据	可变
校验	1

帧开始标识: 0x7E;

长度: 不包括帧开始标识符、长度域和校验;

帧类型: 该帧类型为 0x11;

帧序列号: 该序列号为用户在多帧情况下, 标识该传输请求帧是第几帧, 以便识别。若该序列号为 0, 则 EmBee 模块不予响应。

64 位目的地址: 目的设备的 MAC 地址, 64 位。若该目的地址为 0x0000000000000000, 则把数据发往网络中的协调器。若该目的地址为 0x000000000000FFFF, 则该地址为广播地址, 对该数据进行广播。

16 位目的地址: 目的设备的网络地址, 该地址为 16 位。若是不知道该地址, 或者 64 位目的地址为广播地址, 则设为 0xFFFE。

源端点标识号: 该 API 帧的源端点序号。

目的端点标识号: 该 API 帧的目的端点序号。

簇标识号: 传输所使用的簇 ID 号。

应用规范标识号: 传输所使用的应用规范 ID 号。

广播跳数: 该功能目前暂没开放。使用协议栈所规定的最大跳数。

传输条件选择: 该功能目前暂没开放。

数据: 用户将要发往目的设备的数据。

校验: API 帧所有的字节 (但不包括帧开始标识 0x7E, 长度域本身) 相加, 得到一个数, 取最后一个字节, 再用 0xFF 减去这个字节, 则得到校验内容。

3.2.6 传输状态帧

EmBee 模块当完成发送请求后，会从 UART_TX 口发送出一个传输状态帧，以指示该请求是否完成或者失败原因。其帧格式如下：

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x8B	1
帧应答 序列号	1
16 位目的网络地址	2
重传次数	1
传输状态	1
寻找状态	1
校验	1

帧开始标识： 0x7E；

长度： 不包括帧开始标识符、长度域和校验；

帧类型： 该帧类型为 0x8B；

帧应答序列号： 该序列号为传输请求帧中的序列号；若传输请求帧中该序列号为 0，则 EmBee 模块不进行响应。

16 位目的地址： 目的设备的网络地址，该地址为 16 位。若传输请求为单播，则该地址为目的设备的网络地址；若是广播，这该地址为 0xFFFF；

广播跳数： 该功能目前暂未开放。使用协议栈所规定的最大跳数。

重传次数： 暂时不提供该信息。

传输状态： 0x00---成功发送请求；

0x25---路由没有发现；

寻找状态： 0x00---不需要寻找；

0x01---地址寻找;

0x02---路由寻找

校验: API 帧所有的字节 (但不包括帧开始标识 0x7E, 长度域本身) 相加, 得到一个数, 取最后一个字节, 再用 0xFF 减去这个字节, 则得到校验内容。

3.2.1 数据接收指示帧 (A0=0)

在 API 模式下, 当 EmBee 模块接收到 RF 空中数据时, 它将用帧的格式从 UART 口输出数据。其帧格式如下:

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x90	1
64 位源地址	8
16 位源网络地址	2
接收状况	1
接收的数据	可变
校验	1

帧开始标识: 0x7E;

长度: 不包括帧开始标识符、长度域和校验;

帧类型: 该帧类型为 0x90;

64 位源地址: 发送该数据的 EmBee 模块的 MAC 地址, 若是 0xFFFFFFFFFFFFFFFF, 则表示该地址未知。

16 位源地址: 发送该数据的 EmBee 模块的网络地址, 该地址为 16 位。

接收状况: 该信息没有开放。

接收的数据: 数据载荷。

校验: API 帧所有的字节 (但不包括帧开始标识 0x7E, 长度域本身) 相加,

得到一个数，取最后一个字节，再用 0xFF 减去这个字节，则得到校验内容。

3.2.2 数据接收指示帧 (A0=1)

当命令 A0=1，EmBee 模块接收到 RF 空中数据时，将按以下格式从串口输出数据。帧格式如下：

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x91	1
帧应答 序列号	1
64 位目的地址	8
16 位目的网络地址	2
源端点标识号	1
目的端点标识号	1
簇标识号	2
应用规范标识号	2
广播跳数	1
传输条件选择	1
数据	可变
校验	1

帧开始标识： 0x7E；

长度： 不包括帧开始标识符、长度域和校验；

帧类型： 该帧类型为 0x91；

帧序列号： 该序列号为用户在多帧情况下，标识该传输请求帧是第几帧，以便识别。若该序列号为 0，则 EmBee 模块不予响应。

64 位目的地址： 发送端设备的 MAC 地址，64 位。

16 位目的地址：发送端设备的网络地址，该地址为 16 位。

源端点标识号：该数据传输所使用的源端点序号。

目的端点标识号：该数据传输所使用的目的端点序号。

簇标识号：该数据传输所使用的簇 ID 号。

应用规范标识号：该数据传输所使用的应用规范 ID 号。

广播跳数：该功能目前暂没开放。使用协议栈所规定的最大跳数。

传输条件选择：该功能目前暂没开放。

数据：用户将要发往目的设备的数据。

校验：API 帧所有的字节（但不包括帧开始标识 0x7E，长度域本身）相加，得到一个数，取最后一个字节，再用 0xFF 减去这个字节，则得到校验内容。

3.2.3 I/O 接收指示

当模块接收到一包 I/O 检测数据包时，并且命令 A0=0，处于 API 模式下，将会通过串口按以下帧格式输出 I/O 检测数据。该帧结构如下：

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x92	1
帧应答 序列号	1
64 位目的地址	8
16 位目的网络地址	2
接收状况	1
I/O 个数	1
数字管脚有效位	2
模拟管脚有效位	2
数字管脚高低电平值	可变

模拟管脚 AD 采样值	可变
校验	2

帧开始标识: 0x7E;

长度: 不包括帧开始标识符、长度域和校验;

帧类型: 该帧类型为 0x92;

帧序列号: 该序列号为用户在多帧情况下, 标识该传输请求帧是第几帧, 以便识别。若该序列号为 0, 则 EmBee 模块不予响应。

64 位目的地址: 发送端设备的 MAC 地址, 64 位。

16 位目的地址: 发送端设备的网络地址, 该地址为 16 位。

接收状况: 该信息没有开放。

I/O 个数: 检测的 I/O 管脚的总个数, 包括数字 I/O 和模拟 I/O。

数字管脚有效位: 按比特位指出对应的数字管脚是否被检测, 若对应的位为 1, 表示该 I/O 管脚的检测值有效; 若为 0, 则表示该 I/O 管脚的检测功能禁止, 检测值无效。该域占 2 字节, 共 16 位, 其对应的数字 I/O 管脚如下:

BIT15	BIT14	BIT13	BIT12	BIT11	BIT10	BIT9	BIT8

BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
			DI04	DI03	DI02	DI01	DI00

模拟管脚有效位: 按比特位指出对应的模拟管脚是否被检测, 若对应的位为 1, 表示该模拟管脚检测使能, 将给出 2 字节的该管脚的 AD 检测值; 若为 0, 则表示该模拟管脚的检测功能禁止, 数据包中将不给出该管脚的 AD 检测值。该域占 1 字节, 共 8 位, 其对应的模拟管脚如下:

BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
				AD3	AD2	AD1	AD0

数字管脚高低电平值：该域占用的字节数与**数字管脚有效位**域有关。若**数字管脚有效位**域所有位都为 0（即值为 0x0000），则略去该域。若不全为 0，则该域是按比特位的方式给出对应数字管脚的电平是高（1）还是低（0），占 2 个字节，其数字管脚对应关系与**数字管脚有效位**域中的对应一致。在**数字管脚有效位**域中，若对应管脚的位为 1，则表示该管脚的高低电平值是有效的；若是该数字管脚被禁能，则其值为 0。

模拟管脚 AD 采样值：该域占用的字节数与**模拟管脚有效位**域有关。若**模拟管脚有效位**域所有位都为 0（即值为 0x00），则略去该域。若不全为 0，其中为 1 的位，表示对应的模拟管脚使能 AD 检测。该模拟管脚的 AD 检测值，用 2 个字节来表示；其中为 0 的位，表示该模拟管脚没有 AD 采样，也将不给出该管脚的 AD 采样值，略去该 2 字节数据。模拟 AD 采样值在数据包中按照 AD0, AD1, AD2, AD3, 顺序排列。**采样电压**=(AD 采样值×1200)/1024mV;

校验：API 帧所有的字节（但不包括帧开始标识 0x7E，长度域本身）相加，得到一个数，取最后一个字节，再用 0xFF 减去这个字节，则得到校验内容。

3.2.4 节点发现指示

当模块收到网络中其他模块（例如该模块 JN=1）标识本模块已入网等消息帧时，会从串口输出该数据信息。有点类似使用了 ND 命令。该帧结构如下：

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x95	1
64 位源地址	8

16 位源网络地址	2
接收状况	1
16 位源网络地址	2
64 位源地址	8
NI 标识字符串	可变
16 位父节点地址	2
设备类型	1
触发源事件	1
应用规范 ID	2
制造商 ID	2
校验	1

帧开始标识: 0x7E;

长度: 不包括帧开始标识符、长度域和校验;

帧类型: 该帧类型为 0x95;

64 位源地址: 发送端设备的 MAC 地址, 64 位。

16 位源网络地址: 发送端设备的网络地址, 该地址为 16 位。

接收状况: 该信息没有开放。

16 位源网络地址: 发送端设备的网络地址, 该地址为 16 位。

64 位源地址: 发送端设备的 MAC 地址, 64 位。

NI 标识字符串: 发送端设备的标识字符串, 即发送端设备 NI 命令的内容。

16 位父节点地址: 发送端设备的父节点的 16 位网络地址, 若该节点无父节点, 则 0xFFFE。

设备类型: 发送端节点的设备类型。

0—协调器;

1—路由器;

2—终端设备;

应用规范 ID: 应用规范的标识号, 占 2 个字节;

制造商 ID: EmBee 的制造商 ID。

校验: API 帧所有的字节（但不包括帧开始标识 0x7E，长度域本身）相加，得到一个数，取最后一个字节，再用 0xFF 减去这个字节，则得到校验内容。

3.2.5 模块状态指示帧

EmBee 模块在发生下面事件时，会从 UART 口输出状态指示帧，以告知用户发生了该事件。其帧结构如下：

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x8A	1
事件	1
校验	1

帧开始标识: 0x7E;

长度: 不包括帧开始标识符、长度域和校验;

帧类型: 该帧类型为 0x8A;

事件: 0---硬件复位;

1---看门狗复位;

2---路由器或终端设备加入网络;

3---离开网络;

4---协调器建立网络;

校验: API 帧所有的字节（但不包括帧开始标识 0x7E，长度域本身）相加，得到一个数，取最后一个字节，再用 0xFF 减去这个字节，则得到校验内容。

3.2.6 远端 AT 命令请求帧

与 AT 命令帧不同的是，远端 AT 命令请求帧查询（或设置）的是远端的模块参数，而不是本地模块的参数。当命令选项为 0 时，为了使得设置的参数生效，命令参数设置完后，需要再发送远端 AC 命令。远端 AT 命令请求帧的帧结构如下：

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x17	1
帧序列号	1
64 位目的地址	8
16 位目的网络地址	2
命令选项	1
AT 命令	2
命令参数（可选）	可变
校验	1

帧开始标识：0x7E；

长度：不包括帧开始标识符、长度域和校验；

帧类型：AT 命令帧的帧类型为 0x17；

帧序列号：该序列号为用户在多帧情况下，标识该远端 AT 命令请求帧是第几帧，以便识别。若该序列号为 0，则 EmBee 模块不予响应。

64 位目的地址：目的设备的 MAC 地址，64 位。若该目的地址为 0x0000000000000000，则把数据发往网络中的协调器。若该目的地址为 0x000000000000FFFF，则该地址为广播地址，对该数据进行广播。

16 位目的地址：目的设备的网络地址，该地址为 16 位。若是不知道该地址，或者 64 位目的地址为广播地址，则设为 0xFFFE。

命令选项： 0 — 设置的命令参数不会立即生效，需要再使用远端 AC 命令。

2 — 设置的命令参数**立即生效**，不需要再使用远端 AC 命令。

AT 命令： 我们目前所有的 AT 命令为两个字符，例如：“DL”，“ID”等。
为 AT 命令字母的 ASCII 值。

命令参数： 若带参数，则表示设置参数；若不带参数，则表示读取参数。

校验： API 帧所有的字节（但不包括帧开始标识 0x7E，长度域本身）相加，得到一个数，取最后一个字节，再用 0xFF 减去这个字节，则得到校验内容。

3.2.7 远端 AT 命令响应帧

当 EmBee 从空中接收到远端 AT 命令响应数据时，会从 UART 口，以远端 AT 命令响应帧的格式输入该数据。其帧格式如下：

域	字节
帧开始标识 0x7E	1
长度	2
帧类型 0x97	1
帧序列号	1
64 位目的地址	8
16 位目的网络地址	2
AT 命令	2
命令状态	1
数据	可变
校验	1

帧开始标识： 0x7E；

长度： 不包括帧开始标识符、长度域和校验；

帧类型： AT 命令帧的帧类型为 0x97；

帧序列号： 该序列号远端 AT 命令请求帧的序列号，以使用户识别是哪个请

求的响应。

64 位源地址：源设备的 MAC 地址，64 位。

16 位源地址：源设备的网络地址，该地址为 16 位。若是不知道该地址，或者 64 位源地址为广播地址，则设为 0xFFFE。

AT 命令：我们目前所有的 AT 命令为两个字符，例如：“DL”，“ID”等。为 AT 命令字母的 ASCII 值。

命令状态：0---正确；

1---错误；

2---无效的命令；

3---无效的参数；

数据：若远端 AT 命令请求帧为设置参数，则不带数据；若远端 AT 命令请求帧为读取参数，则该数据为命令参数。

校验：API 帧所有的字节（但不包括帧开始标识 0x7E，长度域本身）相加，得到一个数，取最后一个字节，再用 0xFF 减去这个字节，则得到校验内容。

4 AT 命令

EmBee 模块目前已实现的 AT 命令将分类进行介绍。在以后的版本中还将增加新的 AT 命令。

4.1 地址命令

AT 命令	命令描述	参数范围	默认值
DH	设置或读取目的地址的高 32 位。 与 DL 起组成数据传输的 64 位目的地址。当 DH 和 DL 为 0x0000000000000000FFFF 时,为广播地址; 当 DH 和 DL 为 0x00000000000000000000 时,为协调器地址;	0-0xFFFFFFFF	0
DL	设置或读取目的地址的低 32 位。 与 DH 一起组成数据传输的 64 位目的地址。当 DH 和 DL 为 0x0000000000000000FFFF 时,为广播地址; 当 DH 和 DL 为 0x00000000000000000000 时,为协调器地址;	0-0xFFFFFFFF	0xFFFF
MY	读取该模块的 16 位网络地址。 0xFFFFE 表示该模块还没有加入网络。	0-0xFFFFE 只读	0xFFFFE
MP	读取终端设备的 16 位父节点网络地址。值 0xFFFFE 表示该节点没有父节点,只有终端设备才有父节点。	0-0xFFFFE 只读	0xFFFFE

NC	允许终端设备加入的个数。每当一个终端设备加入,该值会减 1,当该值为 0 时,表示不能再加入终端设备。	0-0x14 只读	0x14
SH	读取模块 64 位 MAC 地址的高 32 位。	0-0xFFFFFFFF 只读	固定值
SL	读取模块 64 位 MAC 地址的低 32 位。	0-0xFFFFFFFF 只读	固定值
NI	节点标识符。是一个字符串,该字符必须为可打印的 ASCII 字符。最长不能超过 20 个字符。	不超过 20 个字符的字符串	0x20
SE	应用层的源端点号。该值将用于控制数据传输中的源端点。该命令只有在透明传输模式下才生效。	0-0xFF	0xE8
DE	应用层的目的端点号。该值将用于控制数据传输中的目的端点。该命令只有在透明传输模式下才生效。	0-0xFF	0xE8
CI	应用层的簇 ID 值。该值将用于控制数据传输。该命令只有在透明传输模式下才生效。	0-0xFFFF	0-0x11
NP	可发送的最大字节数。EmBee 模块可以在空中发射的最大字节数。 注:如果目的节点是 Enddevice,而且 SP 设置的时间较长,不建议一次发送超过 84 字节的数据	0-0xFFFF 只读	

	包。		
DD	设备类型标识。该值用于区分不同的 EmBee 设备。	0-0xFFFFFFFF	0X30000

4.2 网络命令

AT 命令	命令描述	参数范围	默认值
CH	读取工作信道。模块正在使用的信道,采用 802.15.4 中定义的信道号进行表示。0 表示模块还没有加入网络。	0, 0x0B-0x19。 只读	
CE	协调器使能。设置该设备是否是一个协调器。	0-非协调器 1-协调器	0
ID	扩展网络 ID 值设置, 该值为 64 位。如果为 0, 协调器将选择一个随机的扩展网络 ID; 路由器和终端设备将加入任意扩展网络 ID 的可加入的网络。	0- 0xFFFFFFFF FFFFFFFF	0
OP	已获得的扩展网络 ID。该值为模块在网络中的扩展网络 ID。如果 ID 命令值大于 0, 则 OP 与 ID 命令值相等。	0x01- 0xFFFFFFFF FFFFFFFF 只读	
OI	已获得的 16 位网络 ID。该值为模块在网络中分配得到的网络 ID。	0-0xFFFF 只读	
NT	节点查询时间。当执行 ND 命令时, NT 值会一起被广播。其他收到该广播数据的节点将会随机延时一段小于 NT 的时间,再发送响	0x20-0xFF (×100ms)	0x3C

	应，以免造成网络堵塞。		
NO	<p>网络发现选项。该值采用位选址的方式进行选择相应的选项。该命令决定当收到 ND 响应，或者 API 节点发现指示帧时，输出哪些可选项。</p> <p>0x01=从串口输出 ND 响应，或者 API 节点发现指示帧时，会附上 DD 值。</p> <p>0x02=当使用 ND 命令时，只输出 ND 响应。</p>	0-0x03[位选址]	0
SC	<p>信道设置。协调器建立网络，或路由器（终端设备）加入网络时，将只扫描这些信道。</p> <p>该值采用位定义的方式进行选择，某位为 1，则该位对应的信道被选择。</p> <p>0 (0x0B) 1 (0x0C) 2 (0x0D) 3 (0x0E) 4 (0x0F) 5 (0x10) 6 (0x11) 7 (0x12) 8 (0x13) 9 (0x14) 10 (0x15) 11 (0x16) 12 (0x17) 13 (0x18) 14 (0x19) 15 (0x1A)</p>	1-0x7FFF (第 15 位所对应的信道不能使用)	0x7FFF
SD	<p>扫描持续时间指数。</p> <p>协调器—为了建立网络在每个信道上进行活动扫描和能量扫描所持续的时间。</p>	0-7	3

	路由器/终端设备—在加入网络时，为了寻找可以加入的节点，在每个信道上进行活动扫描的持续时间。 扫描持续时间 = 信道总数 × (2 ^{SD}) × 15.36 ms 其中，信道总数由 SC 参数决定。		
ZS	ZigBee 协议栈应用规范。加入同一个网络的设备该参数值必须一致。	0-2	0
NJ	允许其他模块加入的时间。设置该值不会引起模块重启。每当 NJ 值更新，或者模块重启，该值重新计数，时间到，则不允许其他模块加入。 NJ = 0xFF，表示该节点一直允许其他模块节点加入。	0-0xFF (×1 sec)	0xFF
JN	已加入网指示。如果使能，模块当加入网络或上电（并且加入网络）时，会广播一个已加入网络指示帧。如果网络规模大，应该禁止该功能，以免引起广播风暴。	0-1	0

4.3 射频参数命令

AT 命令	命令描述	参数范围	默认值
PL	功率等级。射频模块发射时的功率等级。	EmBee-K11N: 0=-1 dBm	4

		1=1 dBm 2=3 dBm 3=5 dBm 4=7 dBm EmBee-K11D: 0=12 dBm 1=14 dBm 2=16 dBm 3=18dBm 4=20 dBm	
PM	功率模式。使用 boost 模式会使得输出功率增加 3dB，灵敏度也会提高 2dB。	0-1 0=boost 模式 禁能 1=boost 模式 使能	1
DB	接收信号强度 (RSSI) 值。该数据只反映最新接收到的一包数据的 RSSI 值。	0-0Xff 只读	

4.4 串口参数命令

AT 命令	命令描述	参数范围	默认值
AP	API 使能。设置是否使用 API 模式。	0-API 禁能 1-API 使能	0
AO	API 模式。配置 API 选项。选择用不同的帧格式把接收到的空	默认的 API 指示使能。	0

	中数据从串口输出。	应用层可选址的 API 指示。 (参考帧类型为 0x91 的 API 帧)	
BD	UART 口波特率设置。	0-1200bps 1-2400 2-4800 3-9600 4-19200 5-38400 6-57600 7-115200	3
NB	UART 口的奇偶校验位设置。	0-无奇偶校验 1-偶校验 2-奇校验	0
SB	UART 口的停止位设置。	0-1 位 1-2 位	0
RO	该时间设置在透明传输模式下，字符间时间间隔达多长，模块将把从 UART 口接收到的数据进行发射，没有达到该时间又收到数据，则把它先缓存起来。单位为 1 个字符的持续时间。RO=0 表示接收到数据马上就发送。	0-0xFF	5

4.5 I/O 参数命令

AT 命令	命令描述	参数范围	默认值
-------	------	------	-----

D0	I/O 管脚功能。	0-未使用; 3-数字输入; 4-数字输出, 低。 5-数字输出, 高。	0
D1	I/O 管脚功能。	0-未使用; 3-数字输入; 4-数字输出, 低。 5-数字输出, 高。	0
D2	I/O 管脚功能。	0-未使用; 3-数字输入; 4-数字输出, 低。 5-数字输出, 高。	0
D3	I/O 管脚功能。	0-未使用; 3-数字输入; 4-数字输出, 低。 5-数字输出, 高。	0
D4	I/O 管脚功能。	0-未使用; 3-数字输入; 4-数字输出, 低。	0

		5-数字输出，高。	
D8	DI08 管脚功能设置。目前该管脚只有一个功能，即唤醒终端节点模块。	1-作为终端模块唤醒管脚。	1
PR	<p>上拉/下拉使能。配置 I/O 管脚内部电阻是否上拉、下拉。该值采用比特位定义的方式，1 表示使能上拉、下拉；0 表示内部电阻没有使用。比特位定义如下：</p> <ul style="list-style-type: none"> 0- DI04 1- AD3/DI03 2- AD2/DI03 3- AD1/DI01 4- AD0/DI00 5- RTS/DI06 6- SLEEP_RQ/DI08 7- DIN 8- DI05 9- ON_SLEEP/DI09 10- DI012 11- DI010 12- DI011 13- CTS/DI07 14- DOUT 	0-7FFF	0x1FFF
PD	上拉、下拉设置。PR 命令中被使能的管脚，若 PD 命令中对应的位为 1，则内部电阻上拉，若为	0-7FFF	0x1FBF

	0, 则内部电阻下拉。		
%V	读取 Vcc 脚的供电电压。单位为 mV。	0-0xFFFF 只读	

4.6 诊断参数命令

AT 命令	命令描述	参数范围	默认值
VR	软件版本号。	0-0xFFFF 只读	
VL	读取模块的名称, 类型, 协议栈版本号。	可打印的 ASCII 字符串。 只读	
HV	读取硬件版本号。	0-0xFFFF 只读	
AI	读取网络建立或加入网络的状态信息。	0x00- (协调器) 成功建立或 (路由器或终端设备) 加入网络; 0x21- 扫描没有发现网络; 0x22- 扫描没有发现符合 SC 参数和 ID 参数的网络; 0x23- 发现了协调器或路由器, 但是他们	

		不允许加入。 0x2C- 离开网络失败。 只读	
--	--	-------------------------------	--

4.7 AT 命令参数

AT 命令	命令描述	参数范围	默认值
CT	AT 命令超时时间。模块连续该时间内没有收到有效的 AT 命令，将自动退出 AT 命令模式。	2-0x028F (× 100ms)	0x64
CN	退出 AT 命令模式。执行该命令将立即退出 AT 命令模式。	---	---
GT	进入 AT 命令的“+”字符之间的最大时间间隔。	1-0x0CE4 (× 1ms)	0x3E8

4.8 休眠命令

AT 命令	命令描述	参数范围	默认值
SM	休眠模式。协调器和路由器该值要为 0，终端设备要为 5。	0-禁能休眠 5- 周期性休眠，但是可以通过管脚强制唤醒。	0
SP	休眠周期。该值定义每一次终端设备休眠的时间。对父节点而言，该值决定父节点能为其子节点保存多久的信息。	0x20-0xAF0 (× 10ms)	0x20
ST	接收到数据情况下，经过多长时间	1-0xFFFFE	0x1388

	间进入休眠。终端设备每接收到空中数据后，会启动定时器计时，当超过 ST 定义的时间还没收到数据，将又进入休眠。	(× 1ms)	(5s)
SI	执行该命令，终端设备马上进入休眠。	---	---
\$S	路由器（或协调器）是否允许休眠。该命令只针对路由器（或协调器）。如果为 1，且 DI08 引脚为高电平，则路由器（或者协调器）会进入休眠。DI08 为低电平，唤醒模块。	0-禁能路由器（或协调器） 休眠功能 1-使能路由器（或协调器） 休眠功能。	0

4.9 命令执行

AT 命令	命令描述	参数范围	默认值
AC	该命令使改变的参数立刻生效。 例如：改变 BD 参数的值，便不会立刻改变 UART 口的波特率。 当执行 AC 命令后，该波特率便生效。之后就要改变波特率才能通信。	---	---
WR	把参数值保存到 flash 中，掉电后还能继续保持。	---	---
RE	恢复默认值。模块的参数将改变成默认值。	---	---
FR	软件复位。执行该命令后，模块 2 秒钟之后将执行软件复位。	---	---

NR	网络复位。执行该命令后模块的网络层复位。	---	---
ND	寻找网络所有节点。执行该命令后，模块将广播发现网络节点数据帧，然后从 UART 口输出所有节点的响应。每个节点的响应按如下格式输出： MY<CR> SH<CR> SL<CR> NI<CR> Parent_network_address<CR> Device_type<CR> Status<CR> Profile ID<CR> Manufacture_ID<CR> <CR>	---	---
IS	强制读取 I/O 管脚。包括设置成输入状态的数字管脚的高低电平和输入模拟状态的管脚的 AD 采样值。 详见 <u>AT 命令模式下读取本地 I/O 电平值和采样值</u>	---	---

5 数字 I/O 和模拟 I/O

5.1 本地 I/O

5.1.1 AT 命令模式下读取本地 I/O 电平值和采样值

AT 命令模式下，用 ATIS 命令可以读取 I/O 口状态。从串口输出的 I/O 采样数据按如下域的转换成字符串形式输出：

域	长度
采样设置	1
数字管脚有效位	2
模拟管脚有效位	2
数字管脚高低电平值	可变
模拟管脚 AD 采样值	可变
校验	2

注意：以上述各域转换为 **16 进制的字符串**的形式输出，且各域输出结尾还包含**回车符<CR>**。若是占有多个字节，则将按**大端格式**转换为字符串。

数字管脚有效位：按比特位指出对应的数字管脚是否被检测，若对应的位为 1，表示该 I/O 管脚的检测值有效；若为 0，则表示该 I/O 管脚的检测功能禁止，检测值无效。该域占 2 字节，共 16 位，其对应的数字 I/O 管脚如下：

BIT15	BIT14	BIT13	BIT12	BIT11	BIT10	BIT9	BIT8

BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
			DI04	DI03	DI02	DI01	DI00

模拟管脚有效位：按比特位指出对应的模拟管脚是否被检测，若对应的位为 1，表示该模拟管脚检测使能，将给出 2 字节的该管脚的 AD 检测值；若为 0，则表示该模拟管脚的检测功能禁止，数据包中将不给出该管脚的 AD 检测值。该域占 1 字节，共 8 位，其对应的模拟管脚如下：

BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
				AD3	AD2	AD1	AD0

数字管脚高低电平值：该域占用的字节数与**数字管脚有效位**域有关。若**数字管脚有效位**域所有位都为 0（即值为 0x0000），则略去该域。若不全为 0，则该域是按比特位的方式给出对应数字管脚的电平是高（1）还是低（0），占 2 个字节，其数字管脚对应关系与**数字管脚有效位**域中的对应一致。在**数字管脚有效位**域中，若对应管脚的位为 1，则表示该管脚的高低电平值是有效的；若是该数字管脚被禁能，则其值为 0。

模拟管脚 AD 采样值：该域占用的字节数与**模拟管脚有效位**域有关。若**模拟管脚有效位**域所有位都为 0（即值为 0x00），则略去该域。若不全为 0，其中为 1 的位，表示对应的模拟管脚使能 AD 检测。该模拟管脚的 AD 检测值，用 2 个字节来表示；其中为 0 的位，表示该模拟管脚没有 AD 采样，也将不给出该管脚的 AD 采样值，略去该 2 字节数据。模拟 AD 采样值在数据包中按照 AD0, AD1, AD2, AD3, 顺序排列。 $采样电压 = (AD 采样值 \times 1200) / 1024mV$;

5.1.1 AT 命令模式下配置本地 I/O

AT 命令模式下，用 ATDx（x 为 IO 口标识序号）命令可以配置本地 I/O 口状态。详见 I/O 参数命令

5.1.2 API 模式下配置本地 I/O

API 模式下，用 AT 命令帧可以配置本地 I/O 口状态。详见 AT 命令帧（立即生效）和 AT 命令帧（不立即生效）。

5.2 远端 I/O

5.2.1 API 模式下配置远端 I/O

API 模式下，用远端 AT 命令请求帧可以配置本地 I/O 口状态。详见 远端 AT 命令请求帧。

6 EmBee ZigBee 网络

ZigBee 是的物理层和 MAC 层是基于 IEEE802.15.4, ZigBee 联盟在 802.15.4 之上定义了网络层和应用层。EmBee 模块完全兼容这些层。在 EmBee 模块组成的 ZigBee 网络中, 每个模块根据配置, 可以成为协调器或者路由器或者终端设备。下面分别对模块的这些类型进行介绍。

6.1 协调器

协调器负责选择一个信道和 PAN ID 来建立网络, 而且协调器是这三种设备类型中唯一能创建网络的设备, 所以每个网络都要有一个协调器。当协调器创建完网络, 它允许新的设备加入, 也可以路由数据包, 与网络中的其他类型模块进行通信。

协调器选择信道是通过在不同的信道上进行扫描实现的, 当该信道上扫描到的电平大于某个值, 就认为该信道已被其他网络占用, 它不能再使用该信道了, 直到选择到一个没有被占用的信道。用户也可以让协调器只工作在指定的信道上, 用 SC 命令进行设置。

协调器选择 PAN ID 是通过网络扫描来实现的。当协调器完成信道扫描后, 在可用的信道上广播信标请求, 收到该信标请求的其他网络中的协调器和路由器会给该协调器发送信标响应, 该信标响应帧中包含了响应节点所在网络的 16 位 PAN ID 和 64 位的扩展 PAN ID。

当协调器完成了信道扫描和网络扫描后, 选择一个可用信道和网络 ID 来创建网络。网络是否创建成功, 可以通过 AI 命令来获知, 当 AI 返回 0, 表示网络已创建。用户也可以指定协调器的 64 位扩展 PAN ID, 通过 ID 命令来实现。

值得注意的是: 无论 SC 的值或者 ID 的值该变, 都会引起该协调器离开网络, 重新创建一个新的网络。

当协调器成功创建了网络, 此时网络中只有协调器 1 个节点。该协调器允许其他模块加入到这个节点, 从而加入到该网络。当用户不希望其他模块再加入时, 可以通过设置 NJ 命令来实现。

6.2 路由器

路由器在成为网络中的一个节点前，必须通过发现网络和加入网络来完成。当加入网络后，路由器可以让其他模块也加入它，从而加入网络。也可以路由数据包，和网络中的其他节点进行通信。

路由器发现网络是通过网络扫描来完成的，与协调器的网络扫描大致相同。当路由器在其指定的信道列表的信道上发出一个信标请求帧时，其附近网络的协调器或路由器会给该路由器发送一个信标响应。信标响应带有响应节点所在网络的 PAN ID，和是否允许其他模块加入的信息。路由器从中选择一个合适的网络加入，选择的条件是 PAN ID 与 ID 命令相同（当 ID=0 时，不需要该条件）并且网络允许其他节点加入。若该信道不满足条件，继续从信道列表中的下一个信道继续进行网络扫描。

用户可以设置 SC 命令的值，指定路由器只能在某些信道上进行扫描；也可以设置 ID 值，指定路由器只能加入到指定 PAN ID 的网络。当路由器成功加入网络后，会从加入的节点获得该一个 16 位的网络地址，用于在网络中通信，该值可以通过 MY 命令进行查询。

路由器是否成功加入网络，可以通过 AI 命令查询，当 AI 返回值为 0 时，表明路由器已成功加入网络。

同样，当 SC 的值和 ID 的值改变时，都会引起路由器离开目前的网络和加入新的网络（存在的话）。

6.3 终端设备

同路由器一样，当终端设备成为网络中的一个节点之前，它也需要扫描网络和加入网络。当终端设备加入网络后，它可和网络中的其他节点进行通信。因为终端设备可以采用电池供电，在功耗方面有严格要求，所以其不能路由数据包，也不允许其他节点加入它。

终端设备的网络扫描与路由器的网络扫描类似，但是其判断某个节点是否允许加入的标准是：

- (1) 若其 ID 命令不为 0，则 PAN ID 要与 ID 值相等；

(2) 该节点是否允许其他节点加入；

(3) 该节点是否还能容纳得了子节点。若该节点的 NC 命令值不为 0，则表明还可以容纳其他子节点。

当终端设备加入网络时，也会从其父节点处获得 16 位网络地址，用于网络中通信，该值可以通过 MY 命令查看。终端设备是否成功加入网络，可以通过 AI 命令查询，当 AI 返回值为 0 时，表明终端设备已成功加入网络。

同样，当 SC 的值和 ID 的值改变时，都会引起终端设备离开目前的网络和加入新的网络（存在的话）。

6.3.1 子节点与父节点关系

终端设备的省电是通过周期地休眠来实现的，这样，当终端设备有发往它的数据包到来时，它还可能在休眠。这时，终端设备加入的那个模块（父节点）为其保存该数据包，直到终端设备醒来，然后递交给终端设备。这样终端设备和其加入的节点模块，就构成了父子关系。

6.3.2 子节点容量

路由器和协调器有一张子节点表，用于维护加入其的子节点。该表的大小决定了其能容纳子节点能力。若路由器（或协调器）的子节点表没有满，还有剩余空间，则可以再允许其他子节点加入。

路由器（或协调器）还可以容纳多少个子节点，可以通过 NC 命令查询。NC 的初始值是 20 (0x14)，每当一个子节点加入后，该值会减 1，直到为 0，就不再允许其他子节点加入。所以用户在设计网络时，需要满足该约束关系：即要有足够的路由器去容纳终端设备。

终端设备

在协调器、路由器和终端设备中，终端设备工作原理和操作最为复杂。这里单独对其进行描述。

当终端设备加入网络，其加入的节点就是其父节点。

终端设备为了省电需要周期地休眠，在休眠期间，它不会接收空中数据，是通过其父节点为其保存，然后再等子节点醒来，发送给子节点。下面介绍父子关

系的一对父子节点是如何工作。

6.4 子节点工作过程

终端设备进行周期性休眠，当其醒来，会向其父节点发送消息请求帧，当父节点接收到该消息请求后，会查找是否缓存这该子节点的数据，然后向该子节点发送一个应答帧，告诉是否有它的数据。如果子节点收到父节点的应答后，发现没有它的数据，它立即进入休眠。知道休眠周期到来，它再次向父节点发送消息请求帧。该休眠周期可以通过 SP 命令设置。

如果子节点收到父节点的应答后发现它有数据，则准备接收数据，不会马上进入休眠。当每接收到一包数据后，会启动计时器，并每隔 100ms 会向其父节点查询是否有数据需要接收。直到计时器超时，达到 ST 命令所设置的时间，则进入休眠。若用户知道其想要的数据已经接收完毕，也可以给终端设备发送一个 SI 命令，则终端设备不会等到计时器超时而立即进入休眠。

如果终端设备要发送数据给网络中的其他模块，它只能先把数据发送给其父节点。然后执行一些路由查询，目的地址发现等工作，再把数据传输出去。最后再向终端设备报告发送状态。

终端设备在休眠中也可以通过 DI08 管脚强制唤醒。

6.5 父节点工作过程

如果父节点接收到其子节点的数据，它将把该数据缓存起来。等到子节点醒来，发送一个消息请求帧，再把数据发送给子节点。

若是该子节点超过一定时间没有来请求数据，父节点就会把该数据删除，不再为子节点保留。该时间为 $SP \times 1.2$ ，用户可以通过 SP 命令设置。一般情况下，网络中各节点的 SP 值要统一。