**MTK平台 FAQ**

[1、 射频相关 3](#_Toc10022060)

[2、 网络相关 5](#_Toc10022061)

[2.1、single / multitone tone 5](#_Toc10022062)

[2.2、使用域名建立UDP（DNS解析） 5](#_Toc10022063)

[2.3、UDP数据传输问题 6](#_Toc10022064)

[2.4、入网失败 6](#_Toc10022065)

[2.5、网络状态指示灯 7](#_Toc10022066)

[2.6、配置APN 7](#_Toc10022067)

[3、不常用指令功能 7](#_Toc10022068)

[4、OPEN-CPU 8](#_Toc10022069)

[4.1、资源 8](#_Toc10022070)

[4.2、主要外设资源 9](#_Toc10022071)

[4.3 、SDK结构 10](#_Toc10022072)

[5、功耗相关 11](#_Toc10022073)

[6、PSM相关 12](#_Toc10022074)

[6.1、进入不了PSM 14](#_Toc10022075)

[6.2、查询无法进入PSM 14](#_Toc10022076)

[6.3、快速进入PSM 16](#_Toc10022077)

[7、升级 17](#_Toc10022078)

[7.1、普通升级-模块 17](#_Toc10022079)

[7.2、普通升级-MCU 17](#_Toc10022080)

[7.3、OPEN版本升级标准版本常见问题 18](#_Toc10022081)

[7.4、 DFOTA升级 18](#_Toc10022082)

[8、log相关的问题 19](#_Toc10022083)

[8.1、BC26串口及USB口说明： 19](#_Toc10022084)

[8.2、OPEN下EVB和客户自己的板子抓取log 24](#_Toc10022085)

[8.3、Log分析 26](#_Toc10022086)

[**8.3.1、AP侧无法进入DeepSleep** 27](#_Toc10022087)

[9、实验室&入库相关 27](#_Toc10022088)

[9.1、泰尔实验室测试相关 27](#_Toc10022089)

[**9.1.1：协议测试问题** 27](#_Toc10022090)

[**9.1.2：卡接口测试问题** 28](#_Toc10022091)

[9.2、DM入库相关 29](#_Toc10022092)

[9.3、NV入库相关 30](#_Toc10022093)

[10、连接态、IDLE、PSM态 30](#_Toc10022094)

[11、常见其他问题 31](#_Toc10022095)

[11.1、BAND相关 31](#_Toc10022096)

[11.2、QBAND查询 31](#_Toc10022097)

[11.3、RAI功能 32](#_Toc10022098)

[11.4、SIM卡相关 32](#_Toc10022099)

[12、版本问题 32](#_Toc10022100)

[13、协议相关的问题 34](#_Toc10022101)

[**13.1、MQTT协议** 34](#_Toc10022102)

[**13.2、Coap协议** 34](#_Toc10022103)

[**13.3、LWM2M协议** 34](#_Toc10022104)

[BC20 相关问题 34](#_Toc10022105)

[1、 版本问题 35](#_Toc10022106)

[1.1、老版本和新版本的UART区别 36](#_Toc10022107)

[1.2、升级相关的问题 37](#_Toc10022108)

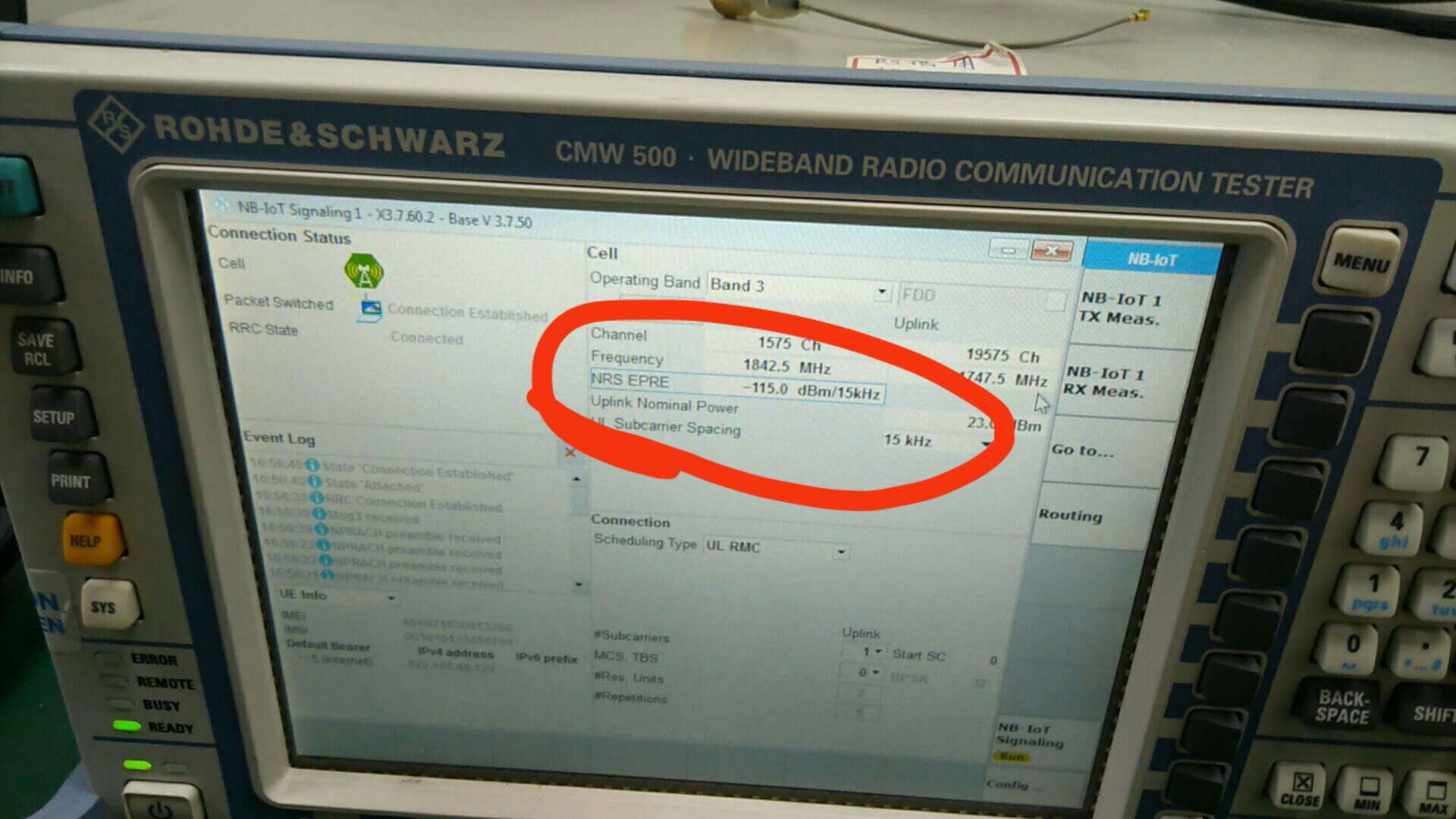
[1.3、Log相关 38](#_Toc10022109)

1. **射频相关**

测试CMW500锁MTK 的BAND指令：AT\*MBSC=1,8锁BAND

在测试传导值偏低的时候可以通过修改NRS EPRE的值，把这个值改小一点，默认是-85dB/15KHz,一般可以改到-115dB/KHz左右。

CSQ查询为0，0 且使用AT+QBAND?指令查询BAND只能返回OK 并不能返回具体的BAND信息。使用MTK的内部指令配置一下BAND的信息，并且软重启一下就可以了 AT\*MBSC=1,5（设置为BAND5）。



* 1. **功率相关**

客户如果自己想测试模块的发射功率，最经济的方法是使用频谱仪，配合强发命令来使模块发出功率。

注意：使用频谱仪只能测试模块的发射功率，不能测试接收灵敏度。且线损要补偿合理。

**1.2、射频天线相关**

同一个模块类型中PA不一样会导致天线存在差异，不同的PA需要调整不同的天线，尤其是BC26NB和BC26NC，天线是不可以混用的。

我们平时说的PA就是功率放大器。

**天线阻抗设计**

我们的模块的RF线需要走50欧姆的阻抗匹配，在使用我们推荐的阻抗工具时需要注意，工具中的H并不是指板子的厚度，而是表层到参考层的距离，另外阻抗是根据叠层结构算的。

**1.3、频率、频段、频点**

频率

频段

频点

1. **网络相关**

**2.1、single / multitone tone**



用single tone还是multitone是基站调度决定的，至于multitone的耗流我们是在仪器下测试出来的。

**能否通过指令查出目前是哪种方式？**

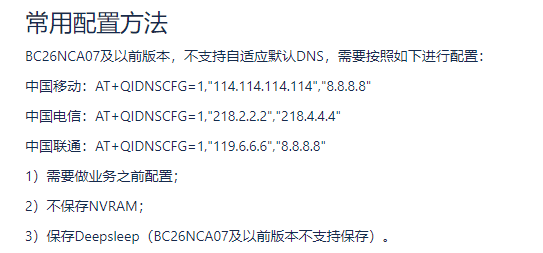
**2.2、使用域名建立UDP（DNS解析）**

使用UDP通信时，模块支持用域名（非IP地址）创建socket，目前由于网络的限制仅仅PCO模式，但是3GPP标准使用的是EPCO,我们模块内部默认是打开EPCO模式的，所以客户在测试时会存在概率性的失败的现象。使用指令AT+QCFG="epco",0 // 关闭ePCO，使能PCO，后面注网可以使用网络下发的DNS Server。该指令仅仅A06以后的版本才支持。

如果在建立TCP连接时，域名解析时间比较长可以用指令AT+QIDNSCFG=1,"114.114.114.114"（A06版本上新增的命令）先配置一个DNS,这样会加快域名解析的速度。我们模块内部默认了一个电信的DNS，用这个解析时间比较长，尤其是用移动卡时间会更久。

另外电信的卡如果走UDP协议，必须要找运营商开通IP定向服务，否则无法使用，移动的卡没有这个限制。

当用户使用移动卡域名解析失败的时候可以直接先让用户配置DNS为8.8.8.8可以不先关闭EPCO。



**2.3、UDP数据传输问题**

在使用UDP传输数据时，在不复位不重启的情况下，模块只要OPEN一次就可以了，下次直接发送数据就可以了！

**2.4、入网失败**

在设备已经附着上了网络以后，要能获取到网络下发的IP地址后才可以做数据业务。下发了IP地址，只要不去激活（或设备重启），IP会一直存在，即使进入PSM模式退出后还是这个IP地址。

经常遇到查询CEREG的返回状态是0，2正在找网的状态，但是就是一直附着不上网络。

1. 排查，先锁定相关的BAND查看能否注册上网络，（可以尝试采用MTK的内部指令查看一下）
2. 有些客户在使用FLASH\_TOOL工具进行升级固件的时候，习惯性的先format一下，这会导致模块射频参数的丢失，从而会引起模块注册不上网络。
3. 还有就是用非NB的卡去注册网络，模块会显示一直在找网中。
4. A06的固件版本在使用新的电信卡注网的时候发现一直注册不上网络，但是用A03的版本就可以注册上。这是因为电信卡RPLMN 配置错误导致的。这个问题已经在正式归档的A07的版本上修复了。

**2.5、网络状态指示灯**

BC26在A06的版本上已经支持网络状态指示的功能了，开机后需要执行一下AT+QLEDMODE=1 命令,掉电保存！

**2.6、配置APN**

使用AT+QCGDEFCONT="IP", ,配置APN为空，然后再用AT+CGDCONT?查询卡的APN。

AT+QCGDEFCONT指令可以配置默认的APN，当使AT+CGDCONT(配置非默认APN)配置不成功时可以使用这个指令来配置APN.

在国外需要用这个指令来配置APN，在不更换运营商卡的情况下，APN只需要配置一次就可以了，更换了运营商后APN要重新配置。

物联网卡续费需要用CCID和MISIDN两个号码。

**2.7、为什么NB不支持高速移动的场景**

由于速度快，可能你发下一个数据的时候，已经移动到另外一个小区的覆盖范围了，但是终端由于上次发送的数据维持了RRC连接（默认20S释放），这时不会与新的小区进行同步，从而无法从新的小区上获取数据，也就不能收发数据。

RRC的释放时间是不是移动20S、电信10S ，收不到基站的释放信息内部超时时间300S（MTK的机制）。海思是255S。

**GSM & LTE**

GSM和LTE支持在连接态下切换，NB不支持连接下切换，只能在IDLE态下进行重选。

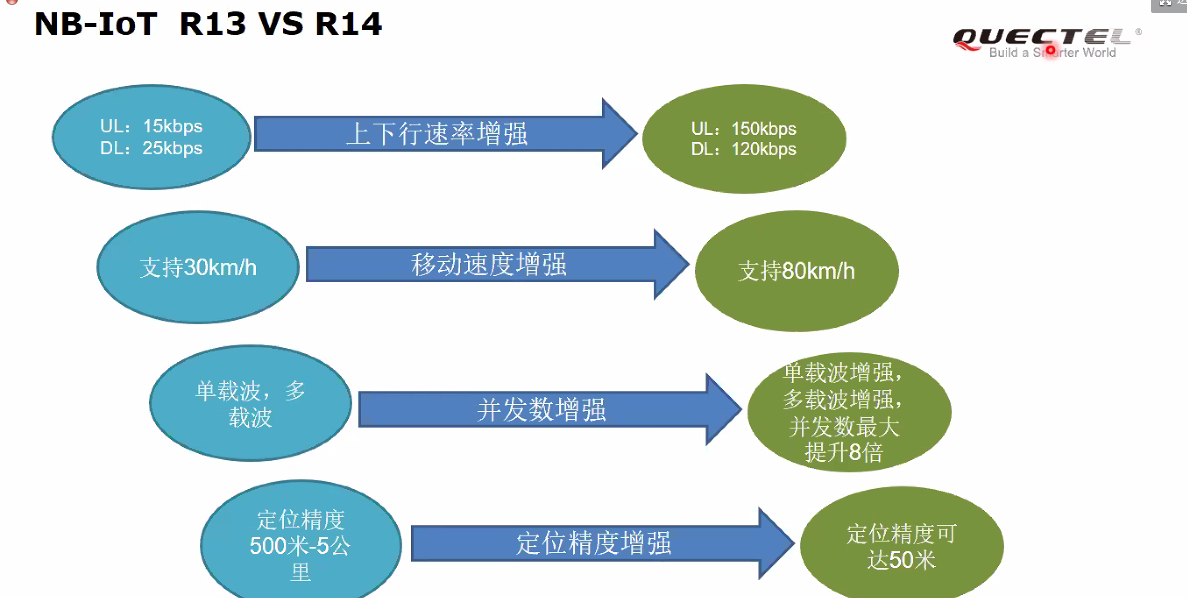
**2.8、领小区重选**

邻小区信号一直比较好，但模组就是重选不过去怎么回事？

重选是需要时间的，判定重选条件也需要时间。模组只能在IDLE态做这些测量，判断和比较。换句话说T3324时间要足够长，或者关闭PSM功能，这样从连接态退出来就能在IDLE态持续待一段时间，从而完成重选。

**2.9、R13&R14**

R13对比R14，目前MTK的固件版本还不支持R14



R14主要的优势在于数据上下行的速率提升以及支持基站的功能。

**3、不常用指令功能**

AT+QENG=0 获取基站Cell id信息，以及信号相关的信息，在最新的固件和文档中，在连接态和IDLE态下都可以正常的获取到信号相关的信息。

AT+CPSMS查询的是用户设置的时间，如果没有设置就是默认3小时。

AT+CEREG=5是网络下发的时间，最终还是以运营商下发时间为准。

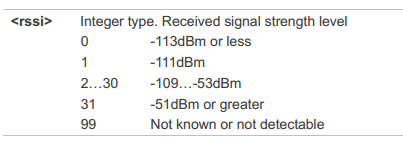
**3.1、AT+IPR:**

关于波特率：BC26在115200以下的波特率可以实现自动同步，使用AT+IPR=bound 以后就固定了波特率，使用AT+IPR=0后可以实现波特率的自适应，开启自适应后要重启一下，完成自适应。

如果自适应波特率没有成功，则模块不会自动上报URC信息，必须要自适应成功后才会上报URC信息。

**3.2、AT+CSQ:**

AT+CSQ指令获取的就是RSSI的值，这个值只是在里面做了一定的处理。如下图：



另外为什么的CSQ查询的值信号很好，但发送数据总是失败？

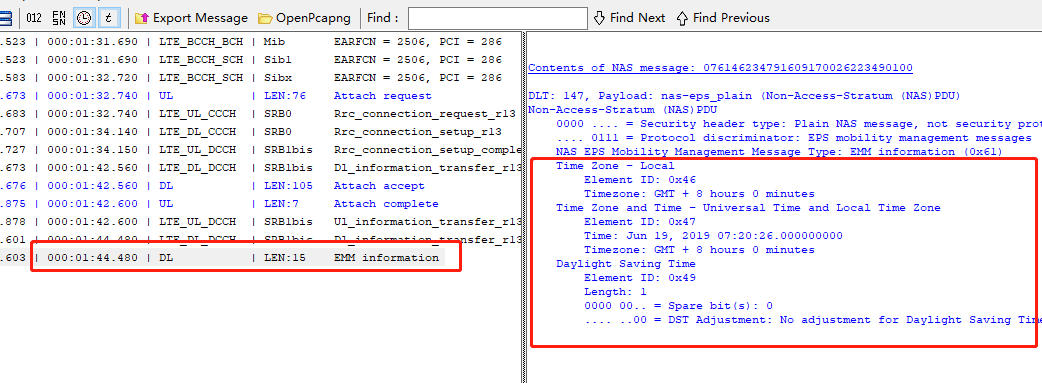
AT+CSQ查询的值是**RSSI**，这是一个频率上的总的电平值，其中不仅包含有用信号，也包含无用的干扰、噪声。

因此该值大，不一定信号就好。

信号的好坏可以通过AT+QENG=0查询。

**3.3、AT+CCLK 获取不到网络时间&授时相关**

1、模块入网成功后一直获取不到网络时间，这个时候可以通过Log 查看网络有没有下发时间给模块，具体是在EMM information里面查看，如下图所示：



AT+CCLK获取本地时间的误差

每48小时的误差在1-2S。



2、客户需要获取比较实时的网络时间，可以通过AT+QNTP的指令来自行配置服务器，来获取时间。

**3.4 AT+CFUN=0 那么久要干啥**

AT+CFUN=0 的执行过程最长要85S，这个不过不是我们之前理解的仅仅是关闭射频的电源开关。

AT+CFUN=0的过程实际上是一个和网络交互的过程。

当执行了AT+CFUN=0后，终端发起Detach Request，网络收到模块的请求后会释放RRC，模块收到网络释放的RRC后才会关闭射频，而以上的这些操作受网络的影响比较大，所以执行CFUN指令后需要等待的时间由快有慢。

**3.5、AT+QSPCHSC 新旧算法（扰码）**

BC26上默认是关闭的，可以用指令切换新旧算法，目前国内的基站默认关闭扰码。

**3.6、AT+QGACT 激活PDN**

适用于多路PDN应用，在注网成功以后执行。

**3.7、AT+CGATT**

该指令配置成1，触发模块去找网，但是AT+CGATT?查询的结果是网络是否已经注册上了，比CEREG的返回信息要少点。国内默认的CGATT=1,客户不需要去配置，也不需要去查询，注网成功与否查看CEREG的返回状态，能否做业务查看是否分配了IP地址。

**4、OPEN-CPU**

**4.1、资源**

32-bit ARM® Cortex®-M4 RISC 78MHz with FPU and MPU

RTOS

* + Code Region: 200KB space for APP image bin
  + RAM: 100KB static memory and 300KB dynamic memory
  + User File System Space: Not supported.
* 安全备份区

目前开放2个block（共计4KB空间）用于客户保存掉电或进入PSM不能丢失数据

**注:**如果客户需要更大的falsh空间来保存掉电不丢失数据，建议客户可以通过我们提供的I2C或者SPI自己外扩资源。

**4.2、主要外设资源**

GPIO:共计13个GPIO口

EINT：共计4个

I2C：一个，可以用GPIO口来模拟IIC

SPI：一个硬件SPI接口

PWM：提供4路PWM ,但同时只能使用一个。

ADC: 采集电压范围0-1.4V

NB模块内部自带硬件看门狗，所以用户可以不用外接看门狗。当程序出现卡住的现象以后，模块会在30S后重启。

异常重启：比如指针错误，数据越界都会直接dump，如果没有接GKI 工具，会直接重启。

**4.3 、SDK结构**

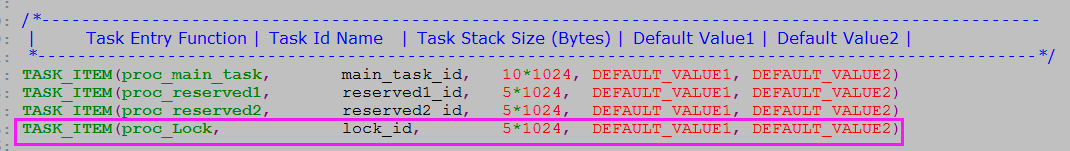


* **注意**
* 客户可以自己增加新的文件夹，但是为了后面移植我司最新的SDK方便，尽量不要更改我们已有的目录结构，用户代码尽量增加在custom文件夹或者单独创建文件夹。

**4.4、如何新增一个TASK**

在\custom\config\ custom\_task\_cfg.h中增加

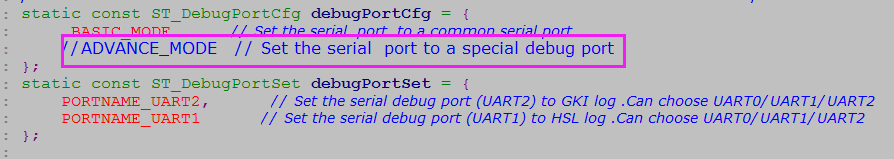
注：默认的三个任务（proc\_main\_task,proc\_reserved1,proc\_reserved2），建议客户不更改，顺序也不移动，因为我们用户库(app\_start.lib)中会用到这三个任务，如果更改会影响代码运行。如果客户需要新增task，可以在后面按照格式增加。



* **如何配置debug口模式**

在\custom\config\custom\_sys\_cfg.c中

注：根据实际的PCB预留串口，选择合适的引脚来抓取log

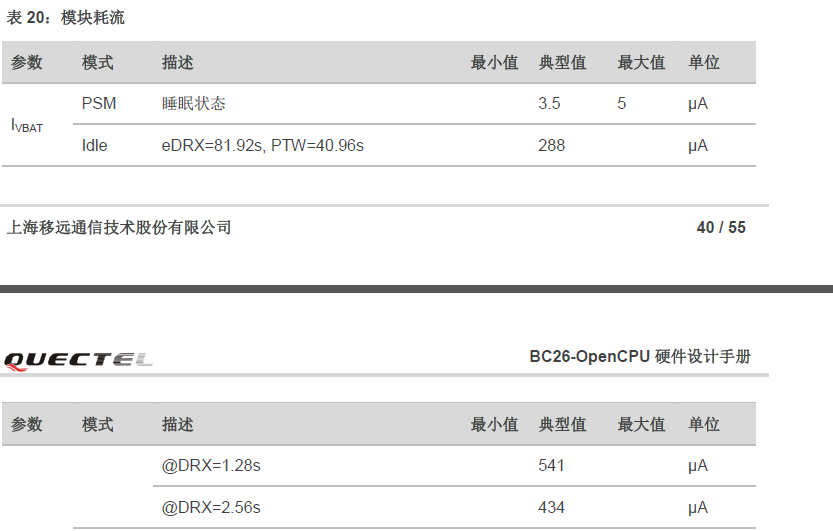


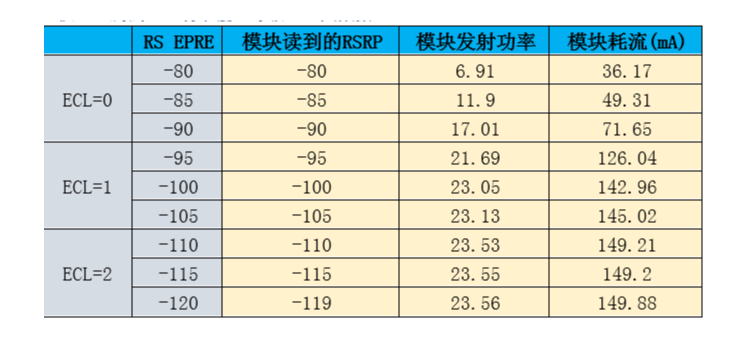
**5、功耗相关**

**5.1开机电流**

BC26模块在开机时有一个700mA的瞬间电流，但是持续时间比较短，只有200us，所以电源在设计时要考虑到瞬间电流的影响，否则会出现开机失败的现象。一般电源在设计时要求能够提供最大500mA的电流。

**5.2、不同的ECL下的模块耗流。**





**5.3、无网下的搜网流程**

**5.4、快速进入低功耗**

在A08版本之前的版本，当模块上报了ENTER\_PSM的URC之后，只表示网络测进入了PSM模式，AP测还没有进入低功耗模式，在A08的版本上，在做完业务之后可以执行AT+QSCLK=1的指令来释放所有的AP测。当网络测进入PSM后，模块就进入低功耗模式了。

指令一直独有，在新的版本上实现的功能不一样了。

且A08的版本支持AP测和网络测分别上报URC。

**6、PSM相关**

目前我们对外所说的模组进入PSM状态需要两个条件（AP侧进（模块端）入PSM、modem侧（网络端）进入PSM）。

AP侧进入PSM的条件：当前系统创建的所有task都进入idle模式，没有业务需要处理 （模块进入PSM）。

Mode侧进入PSM的条件：T3324超时，会上报URC(“+QNBIOTEVENT: PSM”,QNBIOTEVENT=1,默认为0不打开) (网络进入PSM)。

低功耗=deepsleep(模块的低功耗)+PSM（网络侧的低功耗）。

注意：

1. RTC、PSM\_EINT唤醒模组，其实只是AP侧从PSM退出，modem侧还是处于PSM状态，需要上发数据才会退出modem侧PSM。

2、执行Ql\_SleepEnable/Ql\_SleepDisable功能和  
AT+SM=LOCK/UNLOCK效果一样。

3、执行Ql\_SleepDisable模组不会进入深度睡眠和轻度睡眠，客户调试时可以先关闭。

4、频繁的发送AT、timer、eint、rtc触发都会影响模组AP侧进入PSM。

5、当收到URC enter PSM后，由于powerkey一直拉低进入不了deep sleep。测试功耗5mA。相反，如果进入deep sleep，按powerkey唤醒，这时候modem还是在PSM状态，应该也是5mA。

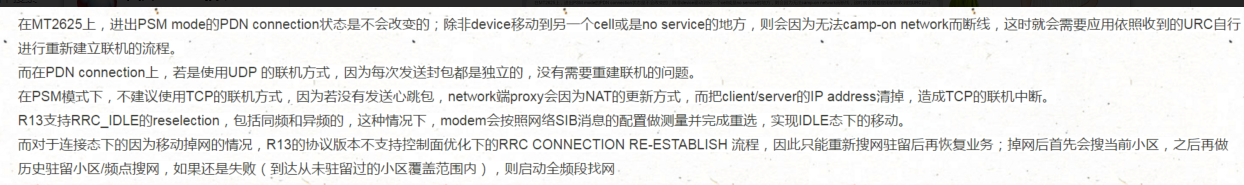
6、当开机直接CFUN=0并返回OK时，模块在10S后（指令的超时时间）会进入DEEPSLEEP模式，此时模块的串口不通。

当使用指令 AT+SM=LOCK住模块后，此时只要模块入网成功，网络侧一样会进入PSM模式，只是模块本身不会进入Deepsleep模式。

当网络侧进入PSM后此时模块没有进入DeepSleep 模式，关闭射频后模块会立马退出PSM模式。

7、当模块进入DeepSleep模式以后，使用PSM\_EINT按键唤醒模块，如果此时模块不做任何的处理，模块会很快在次进入DeepSleep模式。

目前BC26实现了TCP、UDP的RAI功能，但是使用TCP的RAI功能时只能实现Mode侧进入PSM 状态（网络侧有URC上报进入PSM），但是AP侧无法进入Deepsleep 所以此时的串口仍然是通的，必须把TCP连接close以后才能进入deepsleep模式。



所以目前MQTT和TCP协议都不适合PSM模式。经过实际测试LWM2M协议也是可以使用RAI的功能快速释放RRC连接。

**6.1、进入不了PSM**

客户的设备AP侧进入不了Deepsleep解决方法

查看是不是锁了AT+SM=LOCK

运行AT+QRELLOCK释放所有的任务

检查硬件上的Powerkey按键是否一直被拉低

如果用户执行AT+SM=LOCK,FOREVER这个命令，这个结果会保存到Flash里面，且重新烧写固件也覆盖不了。可以用AT+SM=UNLOCK,FOREVER解锁下测试下。

AT+CPSMS=0 该指令会导致模块在入网的时候不向网络发起T3324定时器的值，导致在Log里面看起来像卡没有开通PSM.

**6.2、查询无法进入PSM**

通过发送AT+SM=STATUS指令，会调用sleep\_management\_get\_lock\_sleep\_handle\_list()函数

这个函数里面的log列举了当前lock sleep的所有handle

对于handle所代表的具体内容，其中0~18的handle可通过查看代码中sleep\_management\_lock\_request\_t这个枚举来确认，18以上的handle内容在log中会有显示

1.7.0基线的枚举内容如下：

SLEEP\_LOCK\_DMA = 0,

SLEEP\_LOCK\_SPI\_MASTER = 1,

SLEEP\_LOCK\_SPI\_SLAVE = 2,

SLEEP\_LOCK\_UART0 = 3,

SLEEP\_LOCK\_UART1 = 4,

SLEEP\_LOCK\_UART2 = 5,

SLEEP\_LOCK\_UART3 = 6,

SLEEP\_LOCK\_I2C0 = 7,

SLEEP\_LOCK\_I2C1 = 8,

SLEEP\_LOCK\_I2C2 = 9,

SLEEP\_LOCK\_I2S0 = 10,

SLEEP\_LOCK\_I2S1 = 11,

SLEEP\_LOCK\_I2S0\_AHB = 12,

SLEEP\_LOCK\_I2S1\_AHB = 13,

SLEEP\_LOCK\_SDIO\_MST = 14,

SLEEP\_LOCK\_SDIO\_SLV = 15,

SLEEP\_LOCK\_ULS = 16,

SLEEP\_LOCK\_ADC = 17,

SLEEP\_LOCK\_TRNG = 18,

SLEEP\_LOCK\_USER\_START\_ID = 19,

SLEEP\_LOCK\_INVALID\_ID = 0xFF

1.1.2基线的枚举内容如下：

SLEEP\_LOCK\_DMA = 0,

SLEEP\_LOCK\_SPI\_MASTER = 1,

SLEEP\_LOCK\_SPI\_SLAVE = 2,

SLEEP\_LOCK\_UART0 = 3,

SLEEP\_LOCK\_UART1 = 4,

SLEEP\_LOCK\_UART2 = 5,

SLEEP\_LOCK\_UART3 = 6,

SLEEP\_LOCK\_I2C0 = 7,

SLEEP\_LOCK\_I2C1 = 8,

SLEEP\_LOCK\_I2C2 = 9,

SLEEP\_LOCK\_I2S0 = 10,

SLEEP\_LOCK\_I2S1 = 11,

SLEEP\_LOCK\_I2S0\_AHB = 12,

SLEEP\_LOCK\_I2S1\_AHB = 13,

SLEEP\_LOCK\_SDIO\_MST = 14,

SLEEP\_LOCK\_SDIO\_SLV = 15,

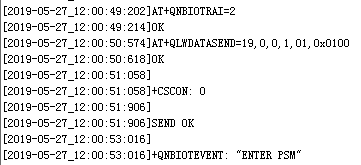
SLEEP\_LOCK\_ULS = 16,

SLEEP\_LOCK\_USER\_START\_ID = 17,

SLEEP\_LOCK\_INVALID\_ID = 0xFF

**6.3、快速进入PSM**

1、RAI



RAI的功能不适合TCP封装的协议（有挥手的过程），RAI只是释放数据发送后的第一条数据，协议底层的握手会再次建立RRC。

因此不适合TCP、MQTT等协议。

支持UDP、LWM2M协议。

2、配置T3324定时器缩短IDLE。

通过AT+CPSMS指令来缩短3324定时器的值，缩短IDLE态的时间，来快速进入PSM。配置该命令之前要先关闭CFUN。

例：AT+CPSMS=1,,,"00000100","00000000" （T3324定时器）

在IDLE态下停留0S之后进入PSM。

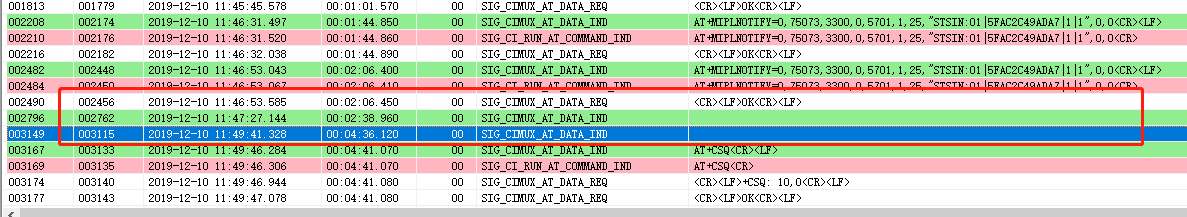
AT+CEDRXS =0这个关闭eDRX的命令可以忽略。

以上指令均掉电保存。

关于3412以及3324定时器值的计算：

**6.4、发送指令无响应**

当出现给模块发送指令，模块没有回应的情况，连续发送才有反应的时候，模块进入了轻休眠模式，目前推荐客户流程是开机、从PSM中唤醒、复位之后，先锁一下（AT+QSCLK=0），防止模块进入轻休眠，业务结束之后在解除锁定（AT+QSCLK=1）。



AT+QSCLK=0 //不能light sleep或者deep sleep

AT+QSCLK=1 //能进入light sleep 或deep sleep

AT+QSCLK=2 //能进入deep sleep 但不能进入light sleep

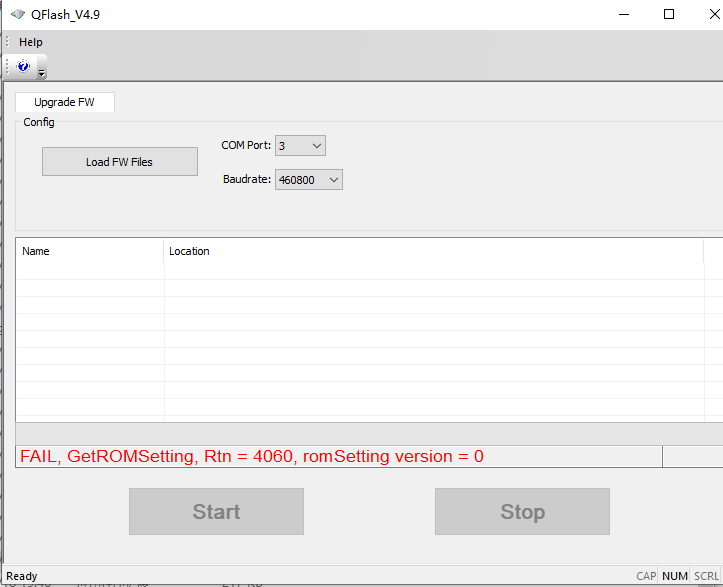
AT+SM=status //查看当前有哪些handle lock住了系统，导致无法进入sleep

**7、升级**

**7.1、普通升级-模块**

目前客户可以通过FTP/HTTP服务来升级。需要客户自己搭建FTP/HTTP服务器。客户需要把要升级的APP.BIN发给我们来做成固件包，然后放到客户的服务器上通过指令来升级。（后期会开放固件包的升级工具和方法）。

当客户升级SDK包文件时，把编译好的GCC文件单独拿出来给客户的时候出现添加文件失败的现象：



此时需要在文件名字中包含BC26、BC66等特殊关键字才可以正常添加。

A06版本支持电信IOT平台升级，COAP方式，内核和APP都可以升级，以差分包的形式升级。电信平台也是支持给MCU升级。

A04版本只支持HTTP升级。

**7.2、普通升级-MCU**

目前可以实现模块给MCU升级，通过电信平台，升级方式分为两种：

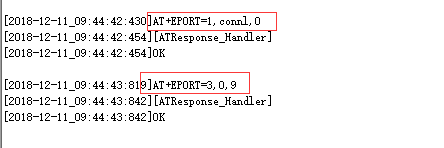
标准模块下需要通过模块将升级程序下载的客户MCU的内存中，或者外挂的EEPROM中。MCU支持主动升级。

OPEN下可以将MCU程序下载到模块中，扩充模块BUFFER的方式，最大300KB，之后升级外部MCU。

**7.3、OPEN版本升级标准版本常见问题**

**BC26 OPEN刷回标准步骤**

1. 刷入OPEN 05版本中的APP（SDK中，不是固件）。
2. 刷好后复位用AT指令测试一下，发送指令：AT+EPORT=1,connl,0配置UART0为AT口。
3. 发送指令：AT+EPORT=3,0,9，配置UART0口的波特率为115200。



1. 刷入OPEN 05版本（刷的是固件，不是APP），注意在烧录之前不能复位键，否则程序会运行，改变之前的配置。会把AT口切回到UART3口。
2. 烧录成功就可以用UART0发送数据了，此时可以刷入别的低版本的标准固件了。

**7.4、 DFOTA升级**

BC26目前支持在线制作OPEN-CPU的APP差分包，目前还不支持固件的制作，固件的制作仍然需要通过公司来实现。

BC26A03的固件版本通过DFOTA升级到A06的版本，需要中间过渡一下，因为这个两个版本的基线不一样，不能直接升级，目前我们内部自己编造了一个中间过渡版本给客户过渡。



如果用户弄乱的AT口，不知道哪个是AT口，发送AT指令模块又无法响应，只能对模块进行升级操作。此时可以用一下方法拯救模块。

1、首先将OPEN版本升级为A06的版本

2、烧入APP中的Flash文件。此时的AT口应该是可以发送数据了。

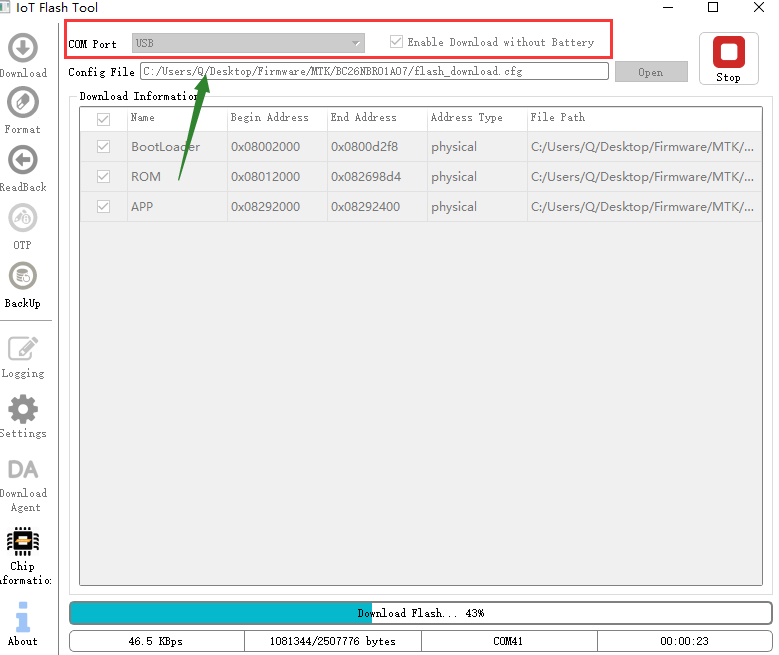
3、使用指令配置AT口：AT+EPORT=1,connl,0，配置一下UART0为AT口。AT+EPORT=3,0,9，配置UART0口的波特率为115200。

4、烧入标准版本的固件就可以了。

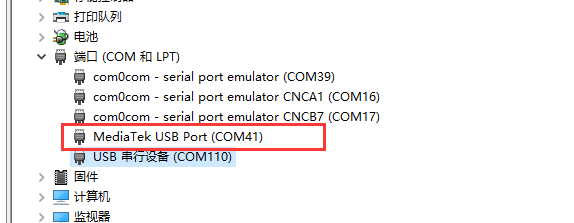
**7.5、 USB升级**

BC26可以通过USB口来下载固件和SDK，下载固件和SDK时需要将USM\_MODE拉低。

打开升级工具，选择USB口升级，之后选择对应的固件，点击开始。



然后复位一下模块，此时会发现之间的两个串口变成了USB口。



等待下载完成即可。复位模块后USB会变成之前的两个串口。

如果将USB\_MODE拉低，影响到正常的POWERKEY开机，开机时间要2S以上，是否会影响到主串口升级？

USB\_MODE拉低后模块会进入下载模式，此时模块需要监测是否有固件下载的过程，所以此时开机时间会比较长。

VBUS\_3.3V供电后会影响到AT指令的响应？

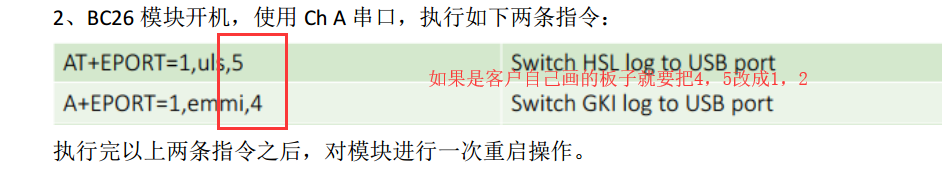
单独给VBUS\_3.3V供电后会导致AT口不通，需要同时接上DM/DP口才可以正常使用AT口，切记。

**8、log相关的问题**

**8.1、BC26串口及USB口说明：**

客户用我们的EVB板抓取log，可以直接参考我们的EVB log指导手册。

如果客户自己画的板子抓取log 的话需要将两个DBG口引出来，且主串口也要引出来。要做如下修改：



如果不需要抓取Log只需要将硬件去掉就行了，不需要进行端口相关的配置。

BC26有三个串口,分别是：



1、主串口（UART0---CHA）：AT口用于通信

2、CHB --- UART2 --- DEBUG口-----HSL log----usl

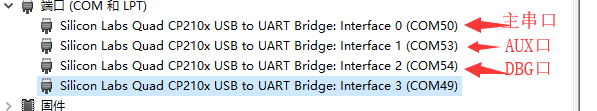
3、UART1---AUX口------GKI log----emmi

4、两个USB口：

MTK USB modem port ---- 配合GENIE LOG工具用于抓取GKI LOG

MTK USB debug port ---- 配合GENIE LOG工具用于抓取HSL LOG

1. 最新的TE-B V2.1的EVB板将主串口、AUX口和DBG口全部引出到USB上，也就是说只要配置一下抓Log的口，log可以直接从USB转换芯片上出来。具体的对应关系如下图：



注：BC26和BC20的串口对应关系不一样，BC26 的主串口是Interface 0,而BC20的主串口是Interface 1.且BC20的开机信息是从DBG口输出，并不是从主串口输出，这点需要注意。

UART3口和UART0口都可以做为主串口吗？二者有什么区别。

NOTE:

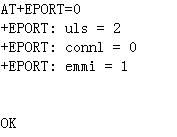
1.目前BC26/BC66 TE-B上辅助串口并未引出，其实际对应的是UART1

2.如果USB口一直插着（可以不通信）系统会一直处于唤醒状态，类似于AT口下发了AT+SM=LOCK命令

1. AT+EPORT命令说明

该条AT命令用于配置制定端口的功能和属性，属于内部调试命令，不建议给客户使用

1. AT+EPORT=0用于查询当前功能口的使用情况



uls: HSL LOG功能输出口

connl: AT通信口

emmi: GKI LOG功能输出口

0 : UART0

1: UART1

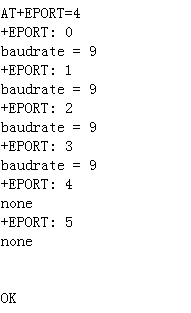
2: UART2

3: UART3

4: USB

5: USB

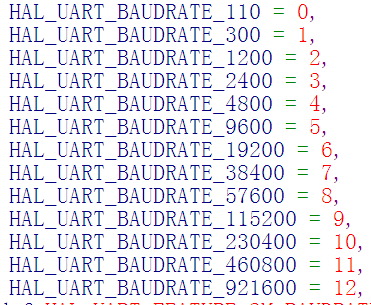
1. AT+EPORT=4用于查询当前功能口的波特率设置



USB口(4/5)对应的波特率为921600，不可以切换

UART口(0/1/2/3)对应的波特率为115200，可以切换

常见波特率对应如下：



1. AT+EPORT=1,owner,port\_id用于重新配置指定端口的功能，重启生效

owner： uls,emmi,connl

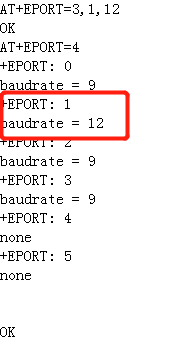
port\_id: 0/1/2/3/4/5



1. AT+EPORT=3,port\_id,baudrate用于重新配置指定端口的波特率，重启生效

port\_id: 0/1/2/3

baudrate：参考第二条中的波特率枚举



端口配置说明：

一般情况下，connl我们不会去配置，默认主串口UART0进行AT通信，但是支持在其他口进行AT通信

配置较多的主要是uls/emmi口，用于抓取底层log，分别对应HSL log(uls)和GKI log(emmi)，关于如何通过genie log抓取日志本文档不包括，在其他文档体现

默认的TE-B由于辅助串口没有引出来，主串口用于通信，所以如果用串口来抓LOG，同一时间只能抓一组(GKI OR HSL),如果用USB口就可以同时抓两种LOG。

需要注意的是如果USB有电，模组就不会进休眠，如果涉及到功耗CASE，不要用USB抓LOG，改用串口抓LOG。

NOTE:

目前TE-B不要配置connl串口为1/3（AT+EPORT=1,connl,1/ AT+EPORT=1,connl,3），因为UART1，UART3没有引出，如果误配置成1/3口，要么通过把UART1/3引出来切换原始配置，要么重新格式化FLASH（谨慎操作，因为会把射频参数和IMEI号全部擦除）

配置端口的时候，不要将两个功能同时映射到同一个port口，这样程序可能会出现异常，要保证功能口对应的port口唯一.

**8.2、OPEN下EVB和客户自己的板子抓取log**

1、EVB上默认的是将USB口引出来抓取Log，USB的引脚在模块的底部，一般的客户自己画板子的时候不会将USB口引出来，所以客户一般不用USB口抓取Log,但是我们的EVB上只引出了USB口，并没有AUX和DBG口，所以只能用USB口来抓取log.

抓取Log之前先确认一下口是否配置正确。

AT+EPORT=0

+EPORT: uls = 5

+EPORT: emmi = 4 4和5代表着抓取log的口为USB口。

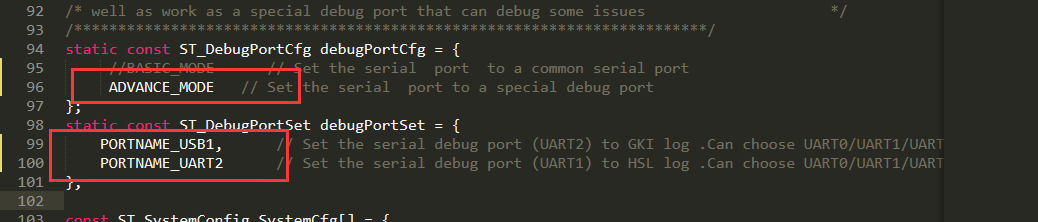
如果查询结果不是这个USB口则无法抓取Log。需要配置为USB口。

具体的代码配置见下图。

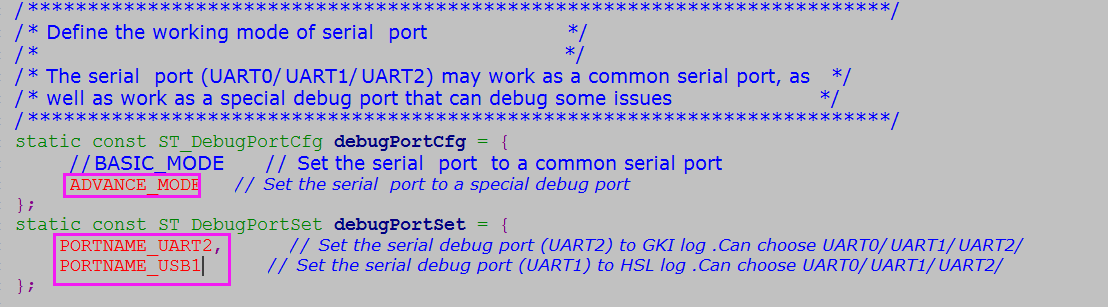


上图为OPEN下代码修改抓取Log口的配置，当然也可以通过指令来修改口的配置，但是一般不轻易给客户修改，改错了改回来很麻烦。另外通过指令的方式修改后不能让程序运行否则会把修改的结果覆盖掉。

SDK1.4的代码中可以通过配置以下代码来修改log的输出。



这样配置是不是用USB1抓GKI 用UART2抓HSL



使用UART2抓GKI LOG 使用USB1抓HSL log，客户的HSL没有引出来，可以不抓，但是配置还是需要的

2、客户画的板子，没有连接USB，只把辅助串口和DBG口引出来了如何抓取Log。

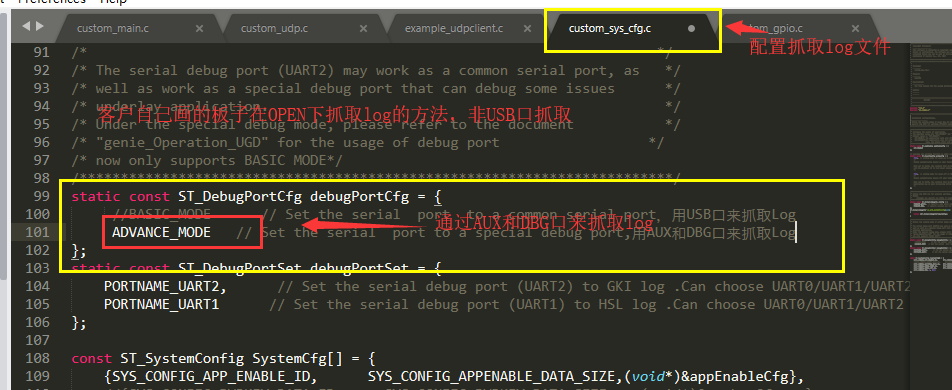
这时需要两个USB转1.8V的串口线，分别接在AUX口和DBG口上，应为要同时抓取GKI 和HSL两个Log。

同样用AT指令查询下串口是否正确。

UART1----AUX口-----1------ uls-----HSL

UART2----DBG口-----2------ emmi------GKI

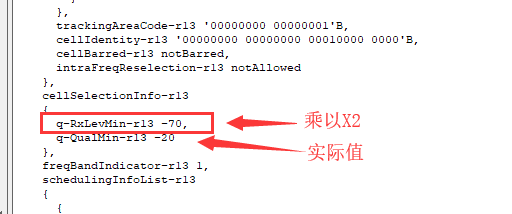
如果查出uls和emmi 分别对应着这两个口，则表示配置正确，否则需要通过指令来修改或者通过程序来修改。下图为通过代码来修改的方法。



也可以通过指令的方式来修改，但是修改后不能让程序运行，否则会被覆盖。

**8.3、Log分析**

RSRP和RSRQ的参考值网络会在SIB消息中下发，作为参考值。这个值越大说明网络环境越好。



**8.3.1、AP侧无法进入DeepSleep**

抓取log之前先执行AT+SM=STATUS，这样会把LOCK住的任务抓取到，之后在抓log.

**9、实验室&入库相关**

入网认证资料



**9.1、泰尔实验室测试相关**

**9.1.1：协议测试问题**

要求打开IPV4V6的功能。

AT+QCGDefCONT="IPV4V6","CMNET"

使用该命令配置为IPV4V6，配置返回OK后，使用AT+CGDCONT?

查询是否配置成功。

对于QCGDEFCONT这个命令，该命令用于配置默认PDN的APN和PDN\_TYPE. 对应的CID为1. 不要用AT+CGDCONT来配置默认PDN的信息，对于其他路的PDN激活，可以使用CGCONT和CGACT来配置激活，MTK平台默认同时支持三路承载。

**9.1.2：卡接口测试问题**

1、实验室要求paging消息之后模组再rrc request，但是会出现直接request的现象。原因：MTK平台attach结束后会主动发起一包上行数据(ICMP ping包，ESM DATA TRANSFER ，由于开启自动PDN激活机制引起的)，而星河亮点的SP8315对此条信令不做响应，导致测试进程中断，最终超时用例失败。

执行下面指令后，终端不再主动发起ESM DATA TRANSFER。

解决方法可以通过指令

AT+ENVDM=1,tel\_conn\_mgr,default\_pdn\_flag,1,00

来配置一下，配置成功后重启一下。

但是当模块有上下行数据时需要打开

AT+ENVDM=1,tel\_conn\_mgr,default\_pdn\_flag,1,01

否则会导致其他测试项失败。

可用指令查询当前的配置

AT+ENVDM=0,tel\_conn\_mgr,default\_pdn\_flag

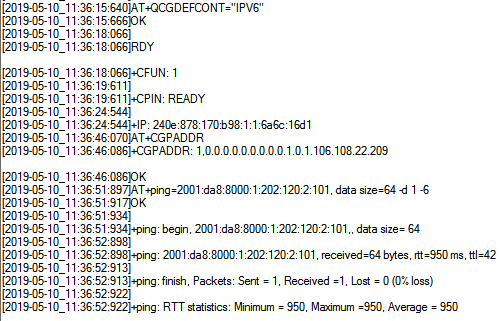
2、开始测试前建议执行AT+QSCLK=0或AT+SM=Lock关闭睡眠，以免测试中进入休眠导致测试失败。

3、要执行AT+COPS=0设置自动搜网，手动搜网会导致用例失败

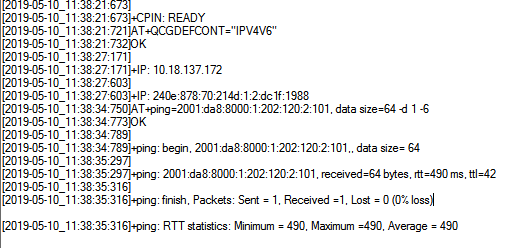
其他的一些问题，有时候复测一下就可以通过。

**9.1.3：IPV4IPV6测试问题**

1)测试单栈IPV6步骤：



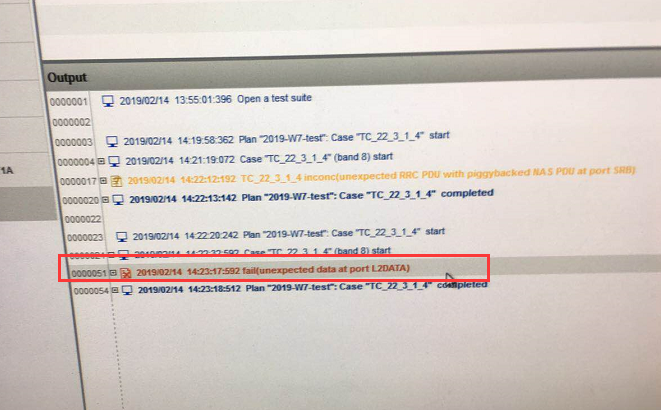
2)测试双栈IPV4V6步骤：



**9.2、DM入库相关**

9.2.1、协议一致性问题

测试项22.3.14 L2 data fail，对应3GPP中的36523-1。这个是因为星河仪器升级，MTK那边没有做对应的升级导致测试失败，已经找MTK拿到对应的基线版本。目前使用对应基线的测试版本可以测试通过，版本见入网认证文件夹。



另外协议一致性测试 GCF 22.3.1.4 需要注意测试仪器的版本

如果仪表版本1.8.0.0A或以上版本，需要使用A06版本测试，归档的A06版本会包含对升级后的仪器版本的测试支持。

**9.3、NV入库相关**

**10、连接态、IDLE、PSM态**

10.1 TAU时间

TAU周期可以理解成三个状态的总和，包括连接态（数据传输态）、IDLE态（空闲态）、PSM态。

TAU的周期不会应为这个三个状态出现的次数改变而改变，也就是说在TAU周期中可以多次从PSM中出来在进入，但是从PSM中出来的动作不是网络侧发起的，必须是模块或者外部状态的改变而引起的。

从PSM中唤醒后，如果连接的是电信的IOT平台，此时模块会去主动注册平台，并Update一下，把平台上缓存的下行数据带下来。

平台目前的自注册时间改不了，默认的是86400S，且这个时间到了以后模块也会默认的注册一下平台（否则平台会显示离线），注册的时候也会Updata一下，且把平台上缓存的数据带下来。

一个eDRX下面有一个PTW，这个时间可以由指令来配置。但是必须是DRX的整数倍。

**11、常见其他问题**

**11.2、QBAND查询**

MTK平台的模块在没有注册上网络之前查询QBAND返回的结果是OK也不会报错也不会返回具体的BAND信息，只有在注册上网络以后才会返回具体的BAND信息。CSQ在没有注册上网络之前一直是0，0.

**11.1、BAND相关**

BAND设置不成功，查询BAND只返回OK，并不会返回具体的BAND信息。但是也注册不上网络，CEREG? 一直返回0，2。

在没有注册上网络之前是查询不到BAND的信息的，只会返回OK。只有在注册上网络以后才会查询到BAND的具体值。

此时可以使用MTK内部指令设置一下AT\*MBSC=1,8，之后再查询AT+QBAND?查询到结果以后就可以注册上网络了。

可以通过查询SIM卡的号段确认是哪个运营商，之后来锁BAND 加速入网。

**11.3、RAI功能**

客户在使用TCP/UDP功能上传数据时，希望发送完数据后立马进入IDLE状态。

TCP不适合使用RAI的功能，RAI释放的是最后一次数据的连接，会释放握手挥手的过程。另外TCP底层的协议会保持连接态不会立刻进入IDLE态，（AP侧不会进入Deepsleep）,所以串口是通的，只有closed TCP连接后才能进入。

可以在每次发UDP送数据之前执行指令AT+QNBIOTRAI=1，这样在数据发送完成后模块会立马进入IDLE状态。

该指令需要在每次发送数据之前都要执行一下！

LWM2M协议支持RAI的功能。

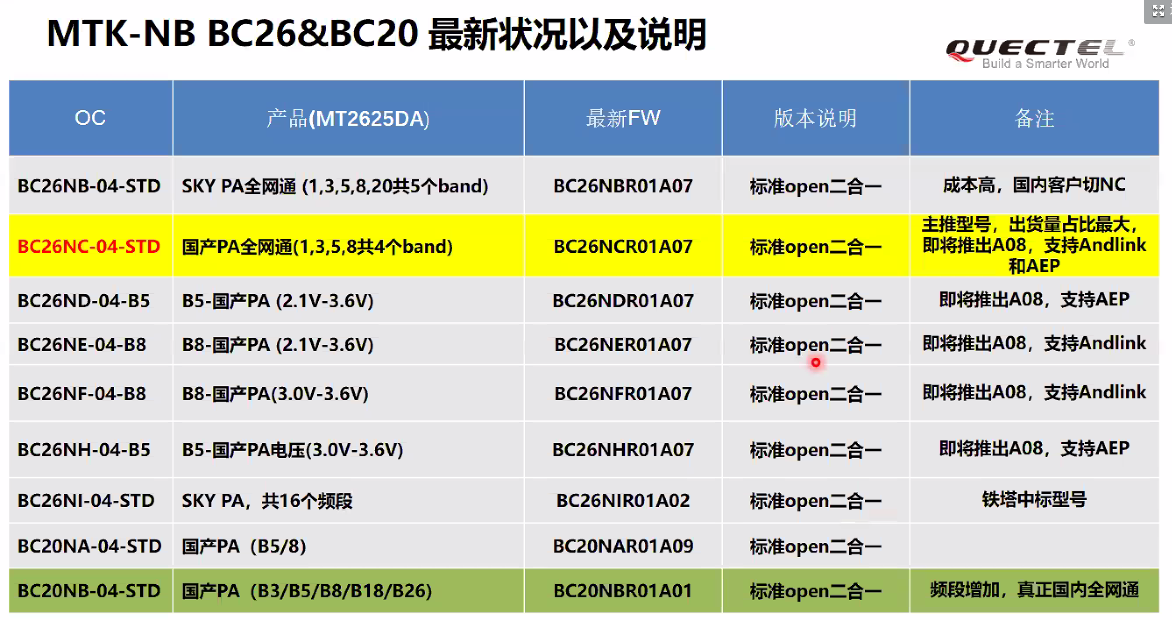
**11.4、SIM卡相关**

目前硬件设计手册上标注的是1.8V的SIM卡，我们的模块也是支持3V的SIM卡的，但是需要VBAT的电压大于3V才可以。

读取NB卡的卡号指令AT+cnum 就可以返回NB卡的卡号，所有版本都支持。如果卡里面没有写入这个号，就查询不到，返回error。

关于eSIM（模块内部贴片卡）,MTK支持内部贴片，但是需要定制OC ，价格不一样，且对尺寸（2x2）和起订量有要求，具体需要销售沟通。

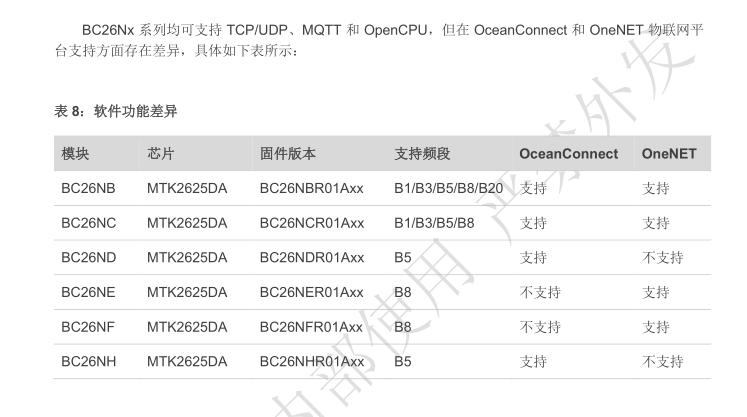
**12、版本问题**

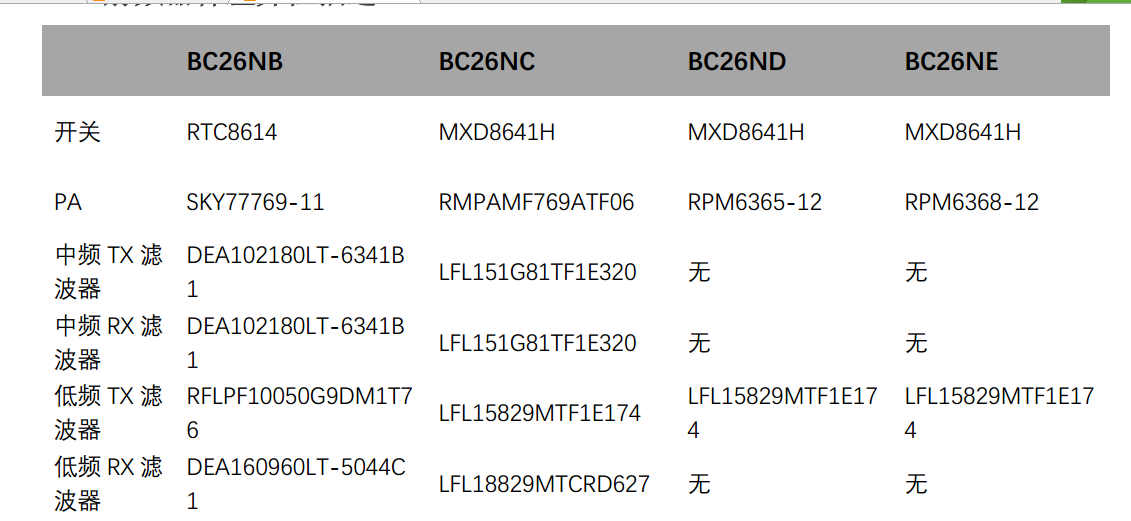


单频模块

NB、NC、ND、NE、NF版本，这几个版本的引脚是完全兼容的。

模块的PA区别：





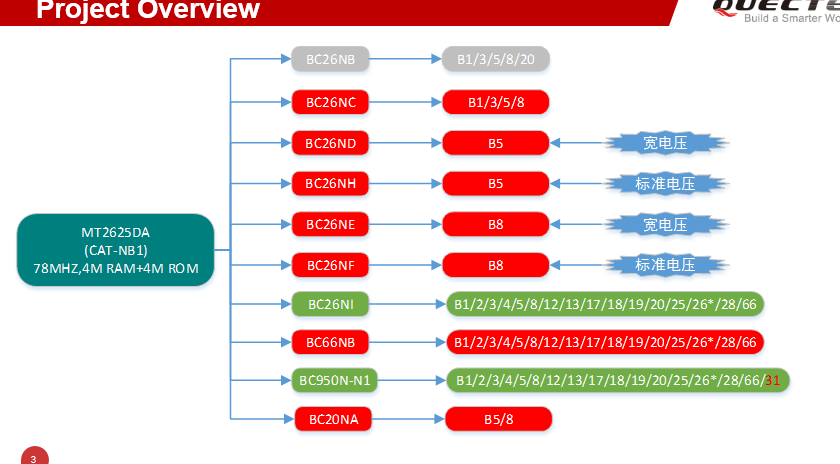


NC&ND 为BAND5的模块，固件版本相同，区别在与供电电压不一样

NE&NF 为BAND8的模块，固件版本相同，区别在与供电电压不一样

BC26和BC66是有区别的

BC26的TX、RX和BC66是相反的，另外66主要是国外的认证，没有国内运营商的认证。



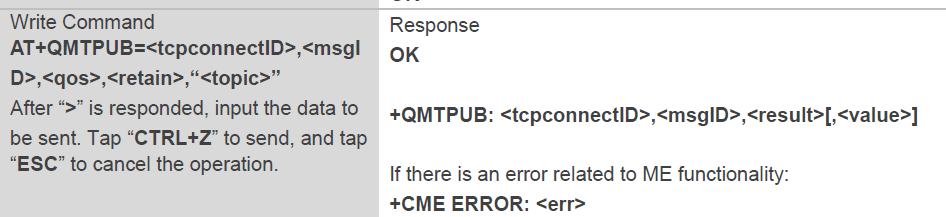
**13、协议相关的问题**

**13.1、MQTT协议**

1、BC26 可以同时支持两路MQTT协议，根据ID来区分，不是Topic。

目前BC26NC的A07版本已经支持JSON的数据格式了，数据要用双引号括起来，只要数据的首尾有双引号即可，中间有特殊字符没有影响。

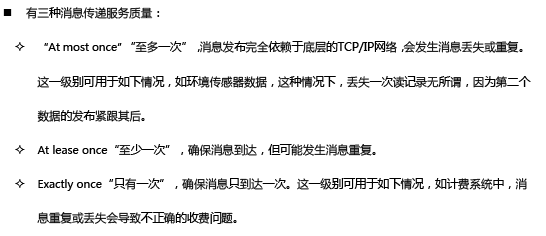
2、BC26在采用MQTTQ进行数据传输的时候，遇到逗号或者双引号会截断，平台上只能收到之前的数据，此时可以采用数据模式进行传输。



3、MQTT协议底层默认有120S的心跳包（也可以用指令也配置，但是不建议配置太长，太长会导致连接断开）。来维持长连接，当数据发送完毕后，心跳包的时间会重新计时。

4、BC66 已经支持MQTTS 了从A10的版本开始的。

1. Qos可以理解为几个传输等级（服务质量）



**13.2、Coap协议**

BC26 Coap协议目前只有调试版本可以给客户使用。

**13.3、LWM2M协议**

我们BC26上的LWM2M协议不是标准的LWM2M协议，BC66上的是标准的LWM2M协议。

目前BC26上只是实现了19/0/0和19/1/0这两个功能，其余的没有。

LWM2M也是支持JSON的数据格式的。

**13.4、TCP协议**

TCP目前也是支持JSON数据格式的。要注意数据的长度，长度不包括首尾的双引号，其他的都包括。

**13.4.1、TCP Socket相关**

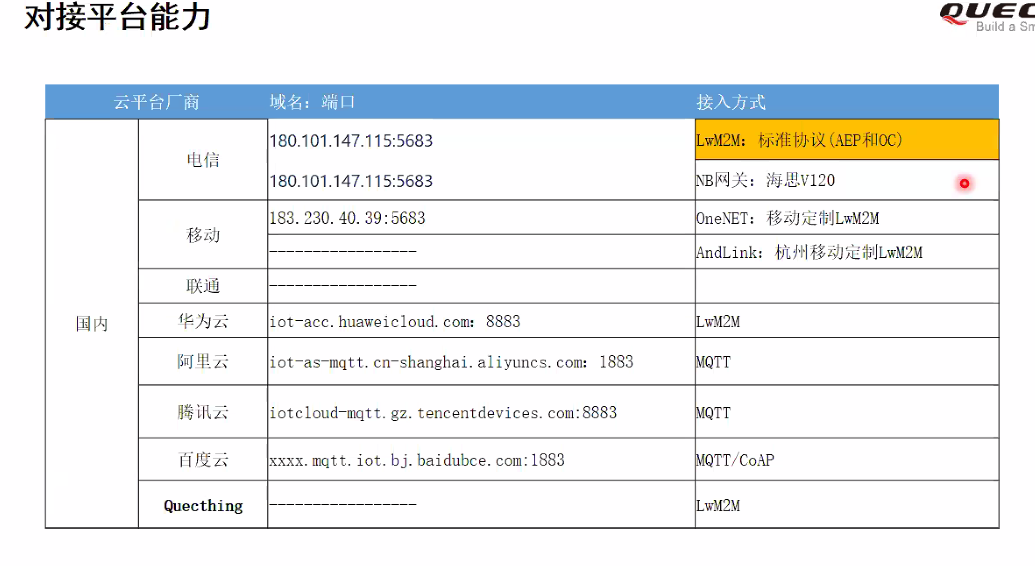
TCP 协议从PSM唤醒后socket是存在的（UDP没有SOCKET的概念），重启之后不存在，CFUN切换之后需要重新建立Socket ,但是UDP不需要重新建立，可以直接发送数据。

Socket 反复创建需要先将之前的Socket 关闭，之后等待120S后才能重新建立。

所谓的透传模式，在BC26上就是数据模式。

**14、网络平台问题**

平台对接能力和对应的协议



**14.1 电信IOT平台**

Lifetime :模块注册上电信IOT平台后，默认会在24x0.8=19.2小时向IOT平台发送一个心跳包，维持设备在平台上的在线状态。

**14.2 OC平台注意事项**

1、OC平台对接数据失败后，建议走一轮异常处理机制（closed+delete），如果失败后建议重启。

2、SEND OK 是平台测回复的。

3、CON 数据快速释放需要配置重传间隔（3-4S）.

4、前四条指令不需要重复配置，只有在重启或者delete之后才会要配置。

5、lifetime在NCA08的版本可以关闭。NC的版本UPDATA OK 之后会Lifetime会清零，NB不会清零。

6、NB lifetime 自动唤醒后要等3mins才会进入Deepsleep（NC上目前不存在这个问题）。

7、固定波特率后判断是不是异常重启：RDY。

8、建议整个业务之前先锁住AP侧，整个业务结束后释放（AT+QSCLK=0），休眠唤醒+重启都要锁一下。

9、域名先解析出IP，在用IP去连。

10、入网成功=CEREG+IP。

11、lifetime 时间配置指令：AT+QLWCFG="lifetime",timeis。

**14.3电信平台FOTA注意事项**

1、Bin 文件直接压缩，不需要放到文件夹中。

2、上报5，0，3之后锁一下AP侧。

3、固件包下载过程中可以正常响应AT命令。

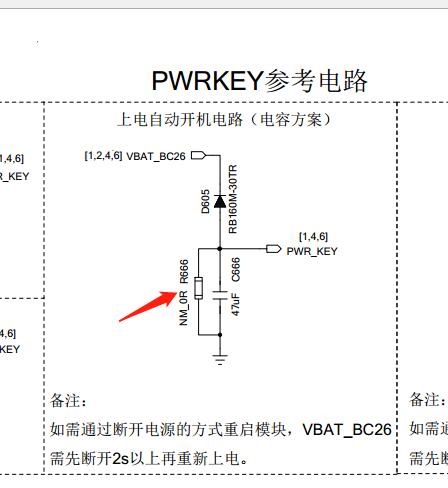
4、升级过程断电后开机会继续升级。

**14.4、阿里云平台**

阿里平台：  
支持MQTT 的 PUB、SUB、PING、PONG、CONNECT、DISCONNECT和UNSUB等报文。  
支持clean session。  
不支持will、retain msg。  
不支持QoS2。  
基于原生的MQTT Topic上支持RRPC同步模式，服务器可以同步调用设备并获取设备回执结果

**15、硬件相关问题**

**15.1、开机相关**



上电自动开机电路，电阻悬空不贴，用在不考虑功耗，直接拉低的情况下使用的。目前只贴电容，用电容的自放电实现开机。

**BC20 相关问题**

1. **版本问题**

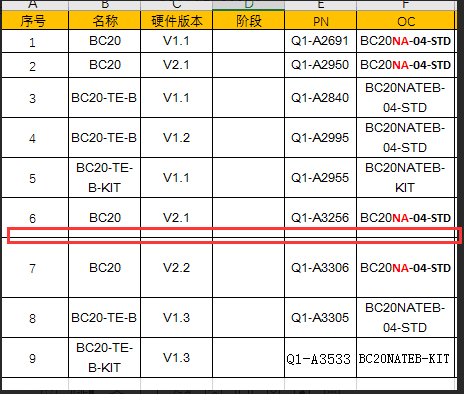
BC20=BC26+和芯星通的GNSS。

目前的BC20 仅支持BAND5 和8，并不支持BAND3.

BC20从归档的A03开始都有加密功能，所以从A02的版本升级到A03之后的版本需要我们从工厂来升级，加入加密文件（不对外）。

BC20早期生产过V1.1和V2.1的两批初版模块，（版本是BC20A02，无Flash加密），A03/A04只要是归档生产的，都具有Flash加密；但是早期这些拿到A02的初级版本，功能不全，想要升级到A03，所以，后面单独出了A03的beta1030（无flash加密的），不然客户从A02升级到A03，模组的AT口不通（带Flash加密的版本，产线会做解密处理）。升级回去原版本可以继续使用。

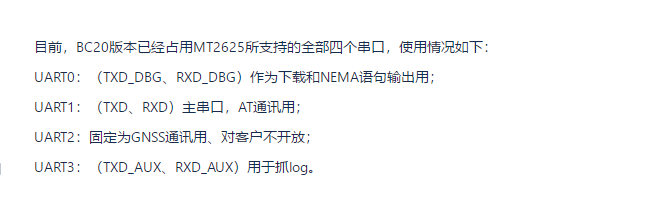
早期的版本GPS信息只能通过AT指令来读取，后续的版本GPS信息可以通过AT指令和串口输出。区别在于PN的区别。

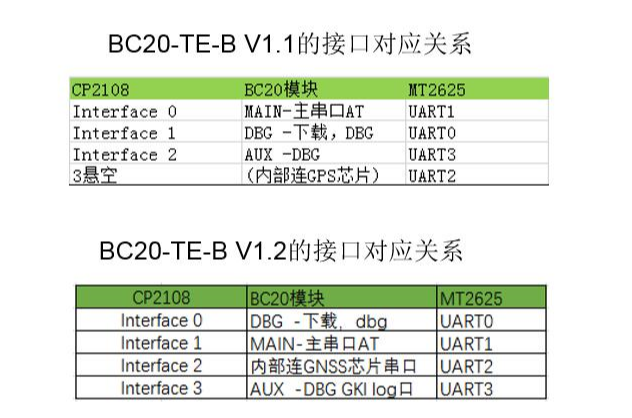


红线之上的模块GPS信息只能通过AT命令来读取。

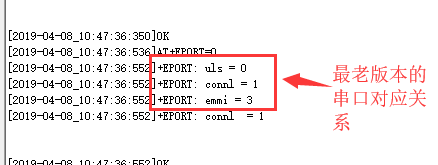
红线之下的模块GPS信息可以通过串口输出。

* 1. **老版本和新版本的UART区别**





最老版本的BC20对应关系。



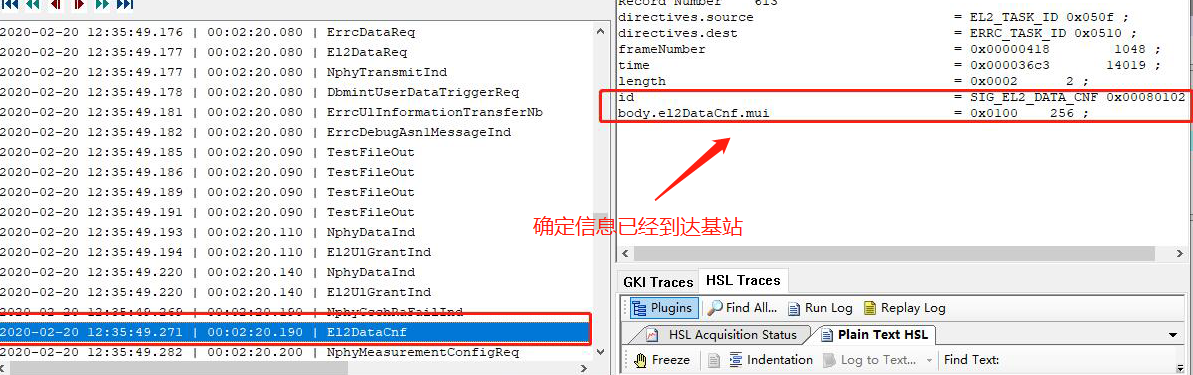
**1.2、升级相关的问题**

BC20目前使用DBG口升级固件。

**1.3、Log相关**

1、目前BC20只可以使用串口3抓GKI对应模块上的AUX口，HSL抓不了。要抓取HSL log需要使用USB口来抓取，模块上的DBG口抓取不了。

2、如何确认模块发送出去的信息已经到了基站：

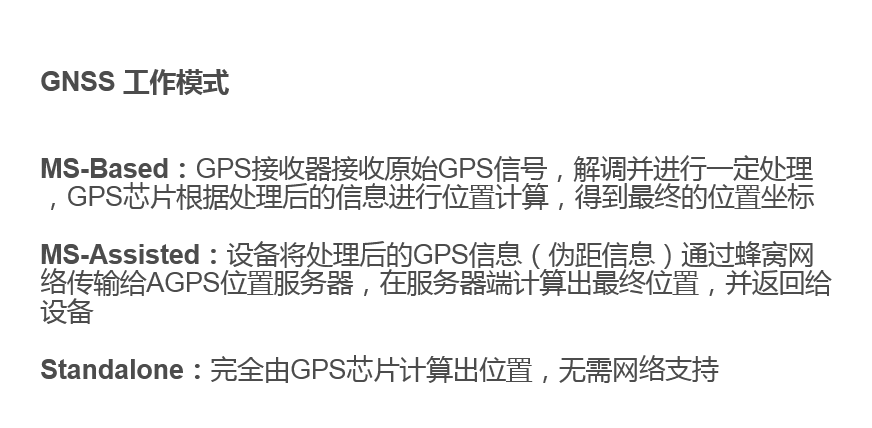


1. **GNSS 定位相关**

使用AGPS的功能，首先注网成功后发AT+QGNSSAGPS=1 打开GNSS,返回OK后用指令查询AT+QGNSSAGPS? 。AGPS需要从服务器上下载星历,这个下载的时间和网络环境有关。

AT+QGNSSAGPS?指令返回1后表示星历下载成功。

星历信息会在2小时内有效，断电或者模块进入PSM后，在起来星历信息依然有效。



plane mode： 用户面和控制面