**海思常见问题汇总**

[1、无法进入PSM状态的问题 2](#_Toc536475639)

[1.1、BC35-G模组，无法进入PSM？ 2](#_Toc536475640)

[1.2、150 \_ONT的版本自动唤醒问题？ 3](#_Toc536475641)

[2、APN相关 4](#_Toc536475642)

[3、URC状态上报 5](#_Toc536475643)

[4、在COAP下的513问题（海思120平台） 5](#_Toc536475644)

[**4.1：为什么会有513错误？** 5](#_Toc536475645)

[**4.2：如何解决513错误？** 5](#_Toc536475646)

[5、523的错误的原因 7](#_Toc536475647)

[6、IP相关 7](#_Toc536475648)

[7、重要的AT指令 8](#_Toc536475649)

[8、150平台问题汇总 8](#_Toc536475650)

[**8.1网络指示灯** 8](#_Toc536475651)

[**8.2新增的三大功能** 9](#_Toc536475652)

[**8.2.1：ROHC技术（数据头压缩技术）** 9](#_Toc536475653)

[**8.2.2：NIDD（非IP数据）** 9](#_Toc536475654)

[**8.2.3：OTDOA、E-CID（基站定位技术）** 9](#_Toc536475655)

[9、自注册相关 10](#_Toc536475656)

[10、海思RAI数据发送标记位 13](#_Toc536475657)

[**10.1：发送UDP数据待标志位** 13](#_Toc536475658)

[**10.2：发送COAP 数据到IOT平台（NON/CON数据）** 14](#_Toc536475659)

[11、海思平台协议支持表 15](#_Toc536475660)

[12、海思硬件相关 15](#_Toc536475661)

[**12.1：150替代120功耗上升问题** 15](#_Toc536475662)

[**12.2：150替代120功耗上升问题** 15](#_Toc536475663)

[13、海思LOG分析 15](#_Toc536475664)

[14、注网问题 19](#_Toc536475665)

[**14.1：注网流程** 19](#_Toc536475666)

[**14.2：注网被拒常见原因** 20](#_Toc536475667)

[15、MCU常见问题 21](#_Toc536475668)

[16、入库、入网以及认证相关 21](#_Toc536475669)

[**16.1 传导&OTA测试** 21](#_Toc536475670)

[17、功耗相关 23](#_Toc536475671)

[17.1、海思150&MTK不同电压下的功耗对比 23](#_Toc536475672)

[18、透传与非透传 24](#_Toc536475673)

[19、各大平台相关的问题 25](#_Toc536475674)

[19.1：电信平台绑定不成功 25](#_Toc536475675)

[19.2 南向、北向 25](#_Toc536475676)

[20、TAU 、PSM时间 26](#_Toc536475677)

[21、SIM卡相关问题 27](#_Toc536475678)

[22、升级相关的问题 27](#_Toc536475679)

[23、高低温相关的问题 27](#_Toc536475680)

[23、其他问题 28](#_Toc536475681)

# 1、无法进入PSM状态的问题

**1.1、BC35-G模组，无法进入PSM？**

软件版本BC35GJBR01A01\_ONT无法进入休眠模式。

A:通过AT+QSREGENABLE?（内部指令）指令查询，返回+QSREGENABLE:1的话表明自注册是开的，卡一直在注网，导致无法进入PSM，通过AT+QSREGENABLE=0，修改后，模组可以正常进入PSM。

B：150模组在不对接IOT平台的时候，模组的自注册的功能是关闭的，就不会存在1小时唤醒一次的情况了！

**1.2、150 \_ONT的版本自动唤醒问题？**

150\_ONT版本存在模块进入PSM后会自动唤醒的现象，这个是移动DM库的要求，要求模块定期的向移动的网络上报信息（该信息是模组底层上报的）查看模块是否使用的是移动的卡以及上报一些信息。

A01的版本默认的时间是900S=15分钟。

A02的版本默认的时间是86400S=24H。

这个时间可以通过指令来配置修改，但是不能关闭，关闭后会导致不能做移动DM入库。

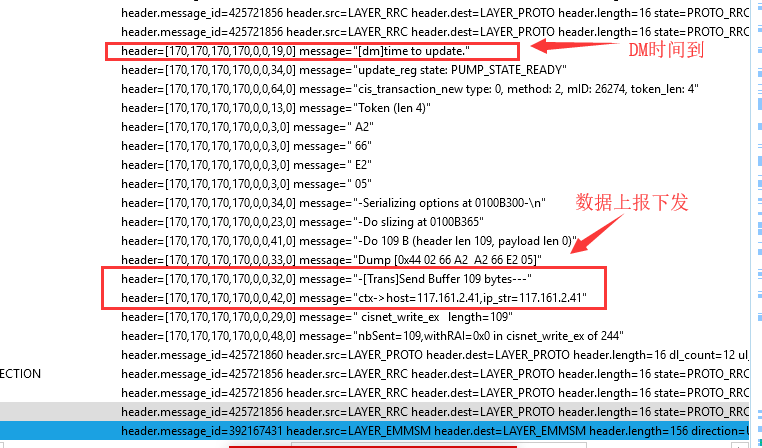
AT+DMPCONFIG=1,117.161.2.41,5683,3000（该指令需要重启生效）

AT+DMPCONFIG?查询命令。

1：表示配置DM IP地址和更新时间。

这个唤醒的原因是：模块需要定期的向移动的服务器（非平台服务器）上报信息导致。

LOG中的提示：



**13.波特率会影响进入PSM**

目前海思的所有模块在通信波特率高于115200以上均进入不了PSM状态。

**1.4、PSM串口唤醒**

海思的串口唤醒可以用指令唤醒，与网络无关的指令只能瞬间唤醒模块，返回OK后会立刻进入PSM，且指令返回的值并不是真实的值，真正唤醒模块的方法是发送一包上行数据。

# 2、APN相关

1、150平台使用AT+CGCONTRDP指令可以读取卡的APN (得b300SP5后的版本才支持)，并不是进入PSM的卡APN。

2、120模组的APN是网络下发的，150的APN是需要设置的，不设置就为空，可以入网。

# 3、URC状态上报

**1、**上报PSM状态信息AT+NPSMR=1，1

+NPSMR:0或1

2、AT+CSCON=1 打开模组状态上报功能，返回1表示模组在连接态，返回0表示模组在IDLE态。开机后要打开模组才会主动上报。

# 4、在COAP下的513问题（海思120平台）

**4.1：为什么会有513错误？**

答：513错误是模组在发送第一包数据的时候跟平台建立TUP连接超时导致的，在建立连接时核心网只给了4S的时间来建立TUP连接，一旦在4S的时间内连接失败就会报513错误，同时这包数据丢失。

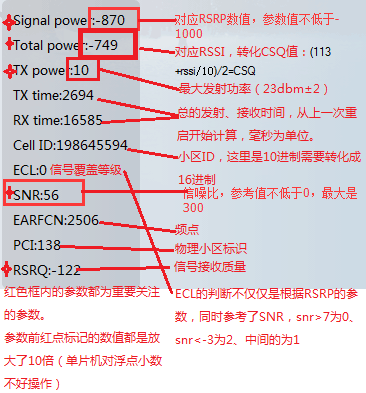
**4.2：如何解决513错误？**

答：可以通过一下3种方式来解决513ERROR

1、在第一次数据发送失败以后，模组底层会发起4次重新连接，所以要在10-20S内在发送一包数据给基站确认连接。

2、优化网络：模组和基站在4S内建立不了连接，很大一部分原因是因为网络环境不好，如何查看网络环境？

A：通过AT+NUESTATAS 指令来查看其中的ECL、SNR和RSRQ这三个参数。如果这三个参数不在正常的范围内，就要找运营商的网优来优化一下网络。



参数说明：（所有的数值都要除以10，浮点数单片机不好操作）

Signer power:对应的RSRP的数值，参数的值不低于-1000。

Total power:对应RSSI,转化CSQ值（113+RSSI/10）/2=CSQ。

TX power: 最大发射功率（23Db±2），在此功率下网络不好。

ECL:信号覆盖等级，SNR值大于7则ECL=0，SNR小于-3则ECL=2,在-3到7之间则ECL=1。 ECL的值围为0 时，功耗最低，此时的信号最好。

SNR:信噪比，参考值不低于0，最大300.（当这个值在同一个地点不同时间，变化太大的时候，说明不正常）。

RSRQ:信号接收质量，在-100以内。

3、在第一次配置NCDP时需要软重启一下。

# 5、常见错误码以及原因

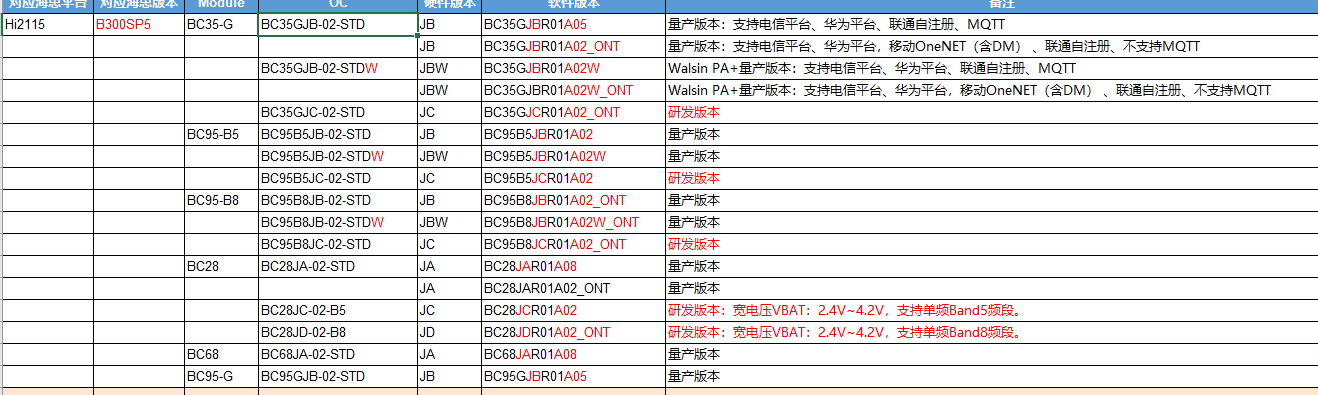
**5.1、523的错误的原因**

A、频偏，MCU和模块通信的波特率发生了偏移，尤其是在用户使用内部晶振的时候，在高低温下很容易出现这个问题，需要用户更换为外部晶振。

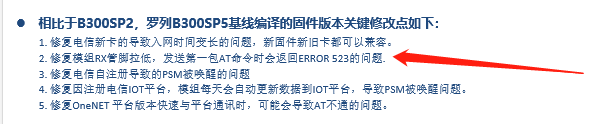
B、150之前的版本会出现523错误。

解决：已经在B300SP5版本中解决。

对应移远的版本：



相比之前的版本修复问题如下：



C、连续523错误

发送指令时连续出现523的错误，需要用户排查一下串口的电平是否超过模块电平,另外MCU的波特率也会导致发送AT指令时一直报523错误。

**5.2 发送CON数据报159错误**

发送的CON数据要等到ACK后才能发送下一包数据。否则就会报159的错误。这个最大等待时间是165S。

# 6、IP相关

海思120平台不支持IPV4 150平台增加了对IPV6的支持。

# 7、重要的AT指令

**7.1、海思150平台AT+CGDCONT?**

[2018-11-29\_19:59:46:039]AT+CGDCONT?

[2018-11-29\_19:59:46:057]+CGDCONT:0,"NONIP","cmnbiot",,0,0,,,,,0

[2018-11-29\_19:59:46:096]OK

模组没有配置IP导致一直没有办法注网。

通过固件升级仍然无法修改这个参数，原因未知。

AT+CGDCONT=0,"IPV4V6",,,0,0,,,,,0

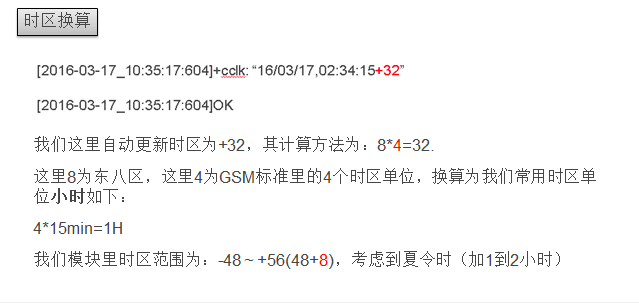
配置APN为AT+CGDCONT=0,"IPV4V6",,,0,0,,,,,0 APN为空的话网络会自动下发。

**7.2、AT+CFUN**

执行AT+CFUN=0或1的操作时需要等待模块返回OK 后才可以执行其他指令，最大超时时间为85S。在这85S内模块需要和网络完成交互。具体交互信息如下：

7.3、AT+CCLK

+CCLK:18/06/21,11:39:20+32    
这个32的含义是啥意思，是代表0时区的含义还是啥？ 那+00代表的是？



另外CCLK是在附着网络的时候同步的基站时间（是24301，EMM INFO 带过来的），之后是模块的内部定时器在工作，每24小时累计误差约10S左右。

# 8、150平台问题汇总

**8.1网络指示灯**

BC35GJBR01A04的固件版本网络指示灯式可以用的了。

BC28JAR01A08也是支持的了。

海思150平台已经支持了。

需要先执行AT+QLDEMODE=1 打开网络指示灯的功能。





根据LED灯的闪烁来判断网络的连接状态。

**8.2新增的三大功能**

**8.2.1：ROHC技术（数据头压缩技术）**

头压缩，数据发送方根据算法对数据头进行压缩，接收方在做一个解压缩。减少头部以减少带宽，仅支持UDP和IP压缩。（特别是在小包数据发送的时候可以节省带宽）。

**8.2.2：NIDD（非IP数据）**

数据传输时把IP的封装去掉，前提是需要在HSS时为终端设备进行NON-IP的PDN签约，以便建立NON-IP类型的PDN。

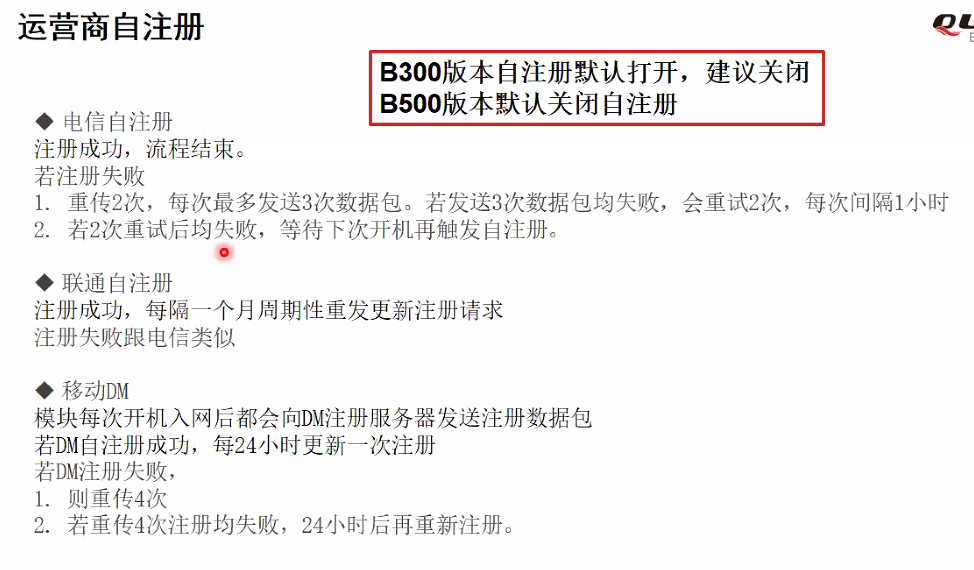
**8.2.3：OTDOA、E-CID（基站定位技术）**

通过模组的数据到基站的时间差来大致判断模组的位置，此方法的前提是必须有三个基站能接到模组的上传信息，模组上报的时间差通过网络传输到定位服务器上，由定位服务器计算出模组的大致位置，用户通过访问定位服务器来获取模组的位置信息。

目前：BC35-G不支持AT命令模式获取位置信息， 支持运营商服务器获取。模组已经支持了R14特性，只是现在没有网络侧的支持， 没有进行大批量的实际大量商用。

# 9、自注册相关

9.1、运营商自注册



1、自注册：和运营商有关系，默认是打开的（ B500的版本上默认关闭），这个自注册是和运营商的服务器连接（非平台）。这个自注册是为了入运营商的库，所以默认是打开的，不建议关闭，用户非要关闭的话后果自负。

由自注册失败（这个失败是已经附着上了网络，但是连接运营商的服务器失败）导致的模块从PSM里面唤醒。常见的自注册失败的原因是：域名解析失败、网络环境差。

域名解析失败（DNS）:域名解析失败后，模块会尝试8分钟的自注册，超过时间后就会放弃。域名解析只有移动电信才有，联通没有域名解析，直接给IP地址。Log 里面的error 202就是域名解析失败的关键字。

1.2、打开、关闭模组的自注册功能（电信、联通）

AT+QSREGENABLE=0是关闭

AT+QSREGENABLE=1是打开

AT+DMPCONFIG=0,0    关闭移动自注册

此指令是内部指令。

当网络环境差导致自注册失败以后，模组会有重新注册的机制，也可以通过AT+QLWSREGIND=0能触发注。

9.2、自动注册平台

是指模组往电信IOT平台上的自动注册，目的是为了节约指令流程，方便用户。

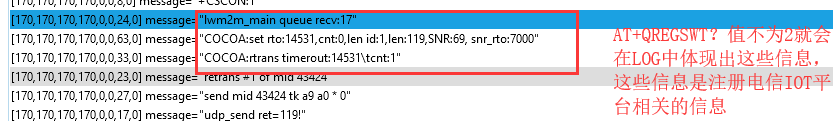
自动注册平台条件：入网成功+平台配置IMEI+NCDP+开启自注册功能。如果没有配置NCDP服务器，则无法自动连接OC平台，但是模块底层会尝试去连接。

只要电信平台的自注册功能打开，并且成功入网后，每隔一个小时模块会自动的去激活网络，重新尝试OC平台的连接（尽管没有NCDP地址）。

自动注册会定期的唤醒模组往平台上发送数据，以检测使用的是不是电信的卡。

在注册移动oneNET平台的时候需要查询一下AT+QREGSWT？是否为2，如果不是要设置成2，否则在注册oneNET平台的时候会注册电信平台。

只要不用IOT平台就关闭自注册。AT+QREGSWT=2



（机卡绑定：一张卡对应一个模块，卡只能在这个模块上使用，在别的模块上注册不上网络，需要找运营商解卡。）

后期如果有客户需要使用我司的海思150平台进行入网许可认证，建议客户测试之前把电信iot自动注册，电信自注册关闭，如果时onenet版本还需要把DM关闭。否则认证测试的时候，在SIM卡测试时，会多了一些额外的信令，导致测试不会通过

AT+QTEST=2,5,0-----关闭电信自注册

AT+DMPCONFIG=0,0 ----关闭DM

AT+QREGSWT=2------关闭电信iot自动注册

2、客户如果采用UDP模式不关闭自注册会有啥影响没？

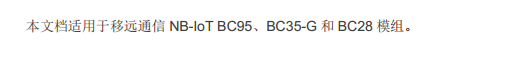
不关闭华为平台的注册功能会有两个影响：

1. 会导致模组异常的退出PSM状态
2. 新模组上线后一个小时后会自动重启； 上电过一次后，后续每隔一个月重启一次
3. AT+QSREGENABLE=0是关闭自注册指令
4. 150模组在电信IOT平台上的活动时间是固定的（86400S），无法修改，时间到了会自动Updata。
5. 上电开机后的第一段乱码是正常的，是Bootloader打印的，无法取消，建议客户在开机的时候匹配NEUL OK关键字，他的一些字符做忽略处理。
6. 最新的版本有at+qchipinfo指令可以查询模组电压和温度。

# 10、海思RAI数据发送标记位

基站通过判断标志位的类型来下发Releses 来让模组进入PSM。

120和150平台发送CON数据时，模组会收到平台的下行数据，告知模组平台有没有收到模组的上报数据。具体说明如下：



**10.1：发送UDP数据待标志位**

AT+NSOSTF=<socket>,<remote\_addr>,<remote\_port>,<flag>,<length>,<data>

Flag: 0x200 RRC 连接释放指示： 上行数据发送完成后， 指示核心网立即释放连接进入IDLE后进入PSM  
 0x400 RRC 连接释放指示： 上行数据发送完成并收到下行数据回复后， 指示核心网立即释放连接进入IDLE后进入PSM.

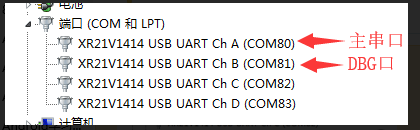
**10.2：发送COAP 数据到IOT平台（NON/CON数据）**

AT+QLWULDATAEX=<length>,<data>,<mode>

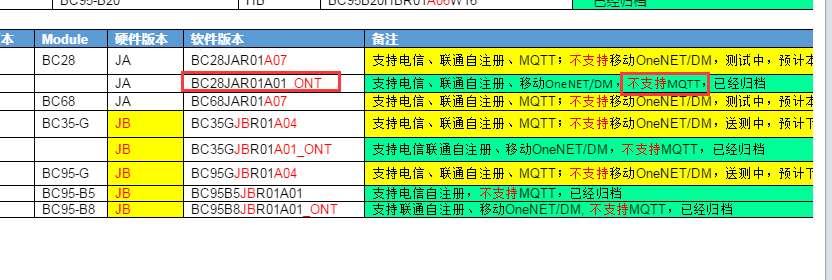
Mode: 0x0000：发送 NON 数据(核心网不回复)  
0x0100： 发送 CON 数据(核心网收到数据后回复一个ACK给模组，释放RRC)  
0x0001： 发送 NON 数据，带 RELEASE 标记（模组发送数据到平台，平台收到数据后，核心网释放RRC）。  
0x0101： 发送 CON 数据，带 RELEASE\_AFTER\_REPLY 标记（模组发送数据，核心网收到数据，并通知平台回复模组，平台回复模组的信息经过核心网后，核心网同时下发一个信息给模组释放RRC，进入IDLE态）。

注：RAI 的功能目前还不支持TCP协议。s

6、150测试板映射出来的4个口。C、D口暂时没有用上。

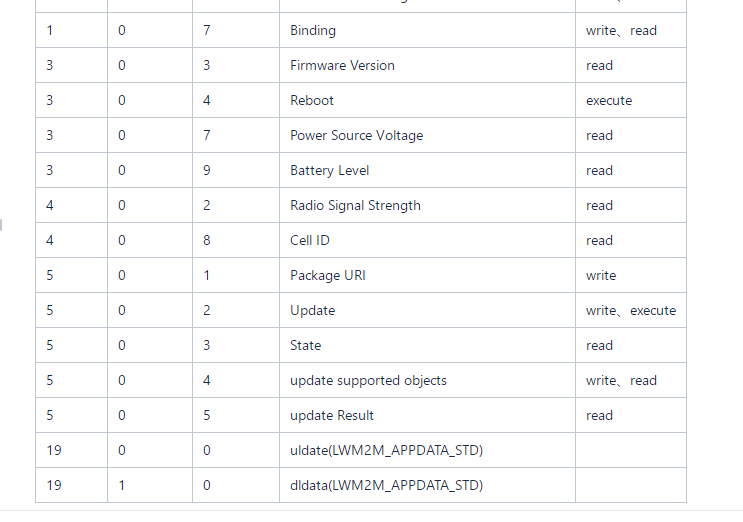


# 11、海思平台协议支持表



**11.1 :LWM2M协议支持OBJ**





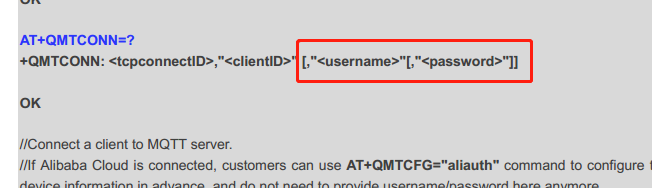
**11.2、MQTT协议**

1、在使用MQTT发送数据的时候会出现遇到特殊字符后数据截断的情况，目前新出的固件已经修复了该问题，可以用如下指令进行数据发送测试。

2、在使用MQTT协议连接平台的时候，一个小时左右会出现断开的现象（用的是移动的卡），此时需要关闭电信平台的自注册的功能**.** AT+QREGSWT=2关闭自注册。

原因：模块打开自动注册的功能，但是没有配置NCDP地址，这个时候模块会每隔一个小时去激活网络，然后重连。

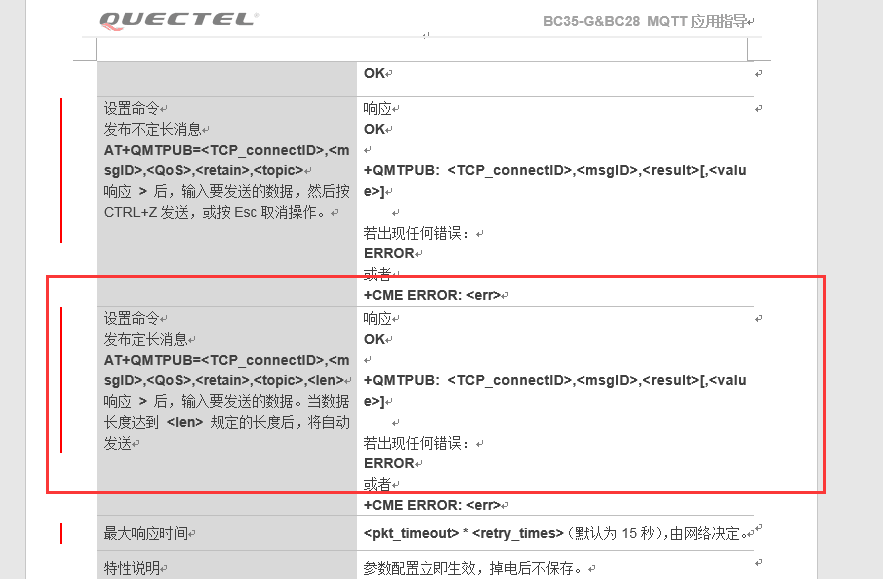
1. 对接阿里云的用户明和密码



这个两个参数有对接平台的三元组合成而来，从平台获取三元组信息，输入到模块中，模块自动算出用户名和密码。

类似于以下小工具计算而来。



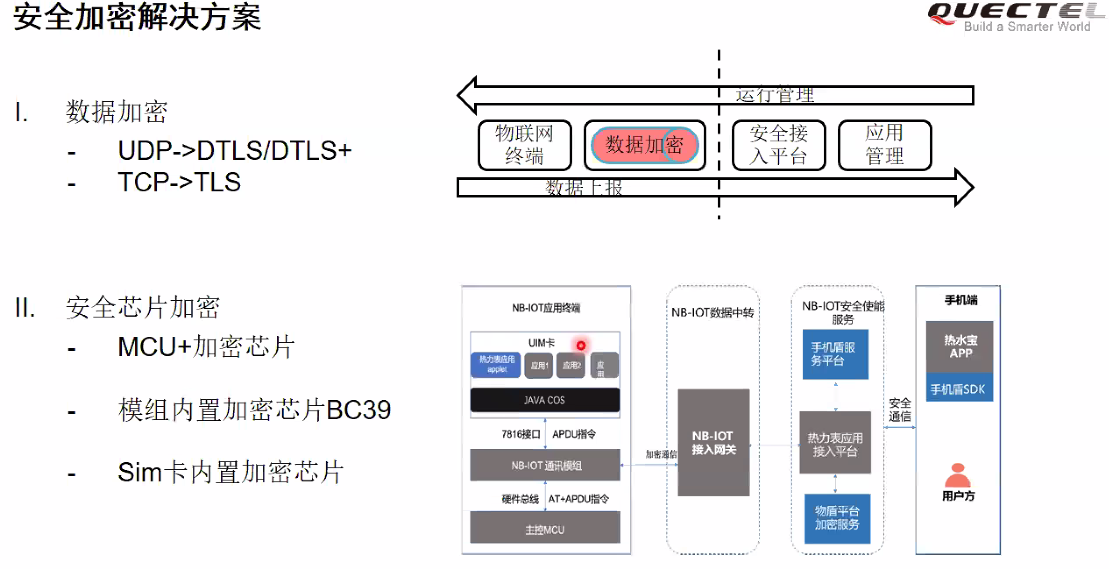


# 12、海思硬件相关

**12.1：150替代120功耗上升问题**

**12.2：加密相关**

软件上支持加密跟着协议走，硬件加密模块暂时还没有出来。

****

**12.3：看门狗**

模块内部，内置硬件看门狗，30S复位一次，标准和OPEN都不提供接口给客户。

# 13、海思LOG分析

整个入网流程：

模组上电===》识别SIM卡===》PLMN选择===》扫频点===》小区搜索===》小区选择===》发起小区附着请求===》RRC建立请求===》随机接入===》RRC建链完成===》入网附着完成

模块上电信息：关键字：Reboot

频点搜索：关键字FREQ

海思模组扫频会先按照设置band的先后顺序进行扫对应band下的所有频点。如果客户使用的运营商SIM卡支持的band设置顺序在后面，就会导致入网时间长的问题。

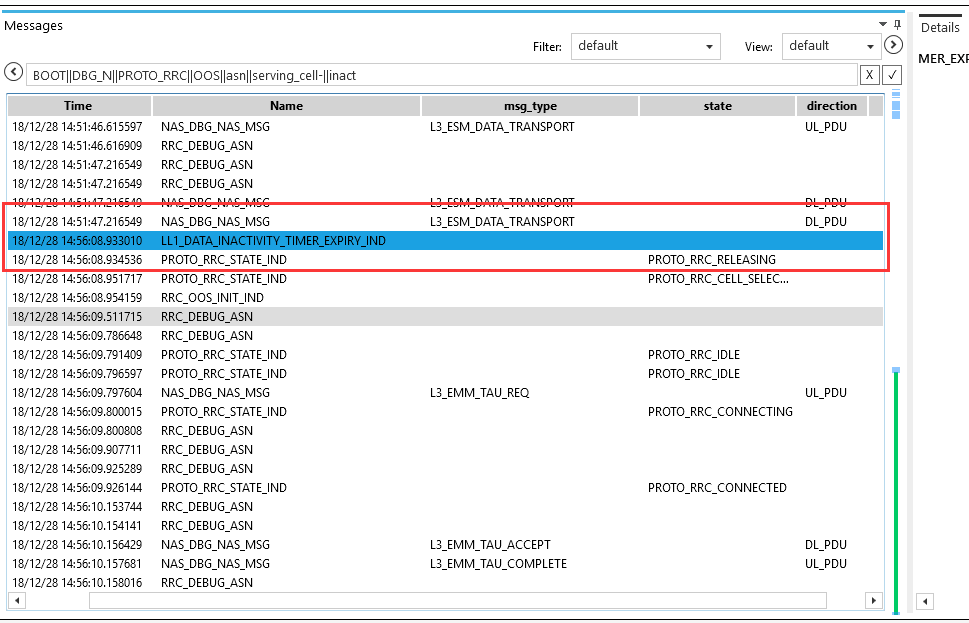
模组搜频会有快搜和慢搜机制。

快搜可以理解为模组会优先找之前入网过的频点和小区，如果没找到或者之前的频点和小区信号质量差，模组会进入慢搜的过程，导致入网时间加长。

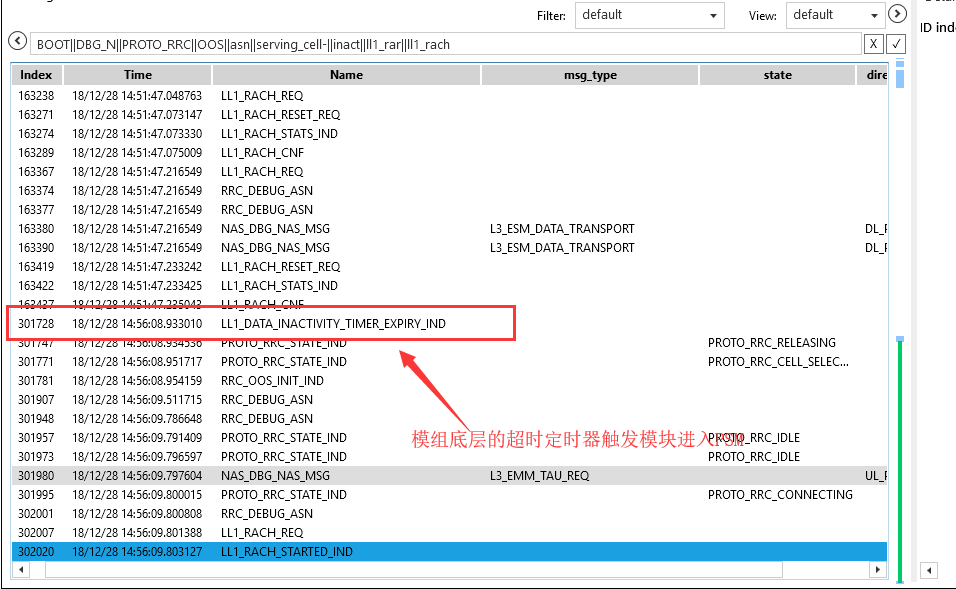
扫频：先找上一次入网时候保存的频点（为了加速入网）类似于从PSM出来后，之前保存的频点没有搜到或者频点下没有合适的小区在去搜索其他的频点（这会增加入网的时间）。

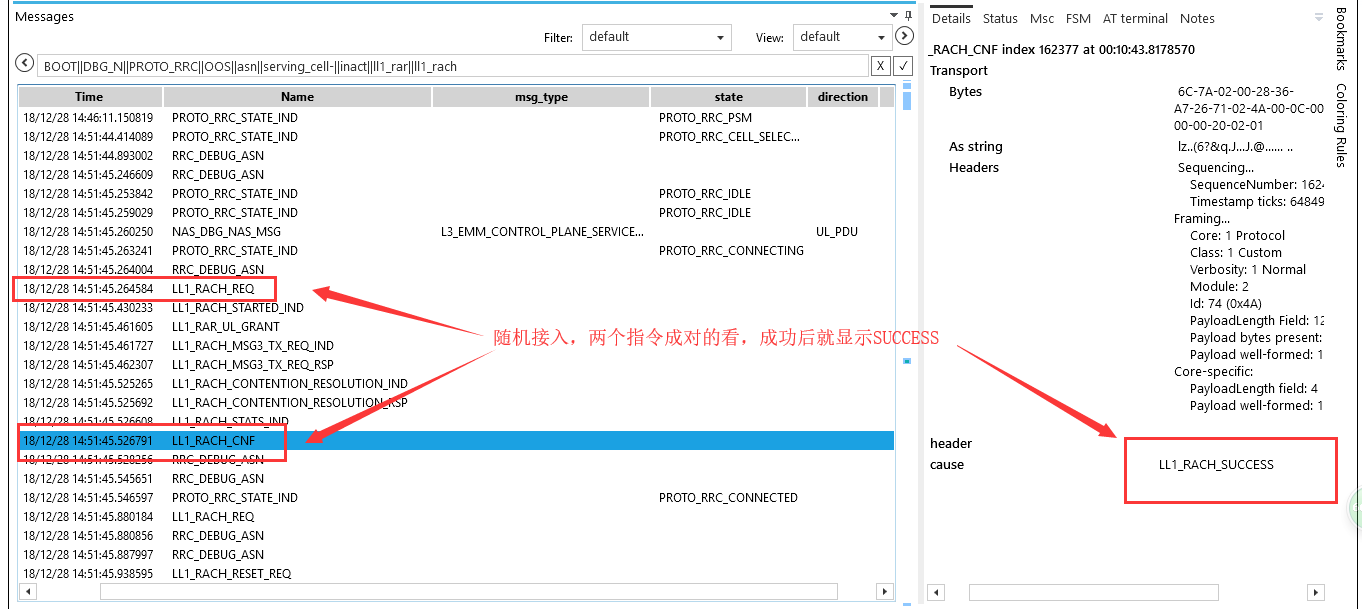
**LOG里面看进入PSM时间过长的原因分析：**

**模组发送完数据以后，正常情况下会收到基站下发的RRC\_RELEASING信息，模组接收到这个信息后回进入PSM，如果基站没有下发这个信息，或者是模组没有收到这个信息，模组底层会启动一个定时器，启动的时间是CONNECT 时间到了以后就启动，这个定时器超时以后也会进入PSM，定时器的时间为250多秒。**



**Inact 关键字：过滤出RRC\_RELEASING释放信息是由模组内部的定时器超时释放的。**







RRC流程

关键字 ：proto\_rrc 查询模组处于哪个连接状态。

PROTO\_RRC\_CONNECTED （此状态下模组和核心网由数据交互，此时的功耗也是最高的）.

PROTO\_RRC\_RELEASING (此状态是从连接态转向IDLE态的标记)

PROTO\_RRC\_CONNECTED PROTO\_RRC\_RELEASING

无数据交互时：移动：20S从连接态转为IDLE。

电信：35S（目前实测）。

L3\_EMM\_TAU\_REQ ：流程

L3\_ESM\_DATA\_TRANSPORT ：表示此时正在发送数据

模块上电开机或者掉电重启后，会首先在IDLE态下做短暂的停留（搜索到合适的频点），之后会转入到连接态。

Backoff 网络让模块等待的关键字。

**13.1、上下行数据流程分析**

数据过滤关键字：proto\_data。此关键字可以过滤出和网络交互的上行数据。

上行数据过滤流程：

**步骤1：关键字PDCP\_DATA\_REQ||****PDCP\_DATA\_CNF。**

**PDCP\_DATA\_REQ：**过滤RRC层发送上行PDCP PDU至PDCP UL层的消息。

参数：  
pdu: PDCP PDU 的指针  
pdu\_len: PDCP PDU 的长度  
rb\_id:承载，有以下两种

L2\_SRB1： SRB1，使用 AM 模式进行传输， 进入 CONNECTED 连接态后均采用该方式进行上行传输。  
L2\_SRB0：SRB0，使用 TM模式进行传输，只有在 IDLE空闲态下发送 RRC\_CONNECT\_REQ文档名称文档密级才会使用该方式进行上行传输。  
proc\_id： process id， 在 PDCP\_UL\_DATA\_CNF 中有相同字段，用于其指示上行传输成功的 PDCP PDU。

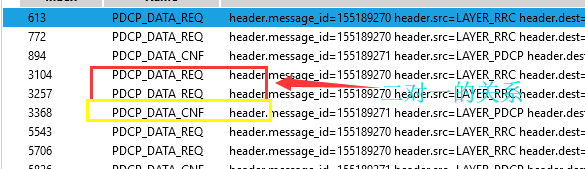
**PDCP\_DATA\_CNF：**过滤PDCP UL发送至RRC层指示对应的PDCP PDU发送状态。

参数：

status: PDCP PDU 发送状态  
PDCP\_TX\_SUCCESS： 发送成功  
PDCP\_MAX\_RLC\_RETRX\_ERR： 重传超过最大次数后失败  
PDCP\_RACH\_FAILURE： 重同步随机接入失败导致的传输失败  
proc\_id: PDCP PDU 的 process id，与PDCP\_DATA\_REQ 中的 proc\_id 相对应  
rb\_id:承载， 有以下两种  
L2\_SRB1： SRB1，使用 AM 模式进行传输， 进入 CONNECTED 连接态后均采用该方式进行上行传输。  
L2\_SRB0：SRB0，使用 TM模式进行传输，只有在 IDLE空闲态下发送 RRC\_CONNECT\_REQ才会使用该方式进行上行传输。  
proc\_id： process id， 在 PDCP\_DATA\_CNF 中有相同字段，用于其指示上行传输成功的 PDCP PDU。

观察每一个PDCP\_DATA\_REQ是否都有一个与之对应的PDCP\_DATA\_CNF。

如果都是一一对应的关系，则说明上层发往L2的上行数据包都发送成功。如果不是对应的关系则说明PDCP\_DATA\_REQ对应的上行数据包没有发送成功。如一对多的关系：



则进入步骤2的查询。

**步骤2：过滤关键字**

MAC\_UL\_UPDATE\_BUFFER\_SIZE\_REQ||RLC\_UL\_STATUS\_IND

**MAC\_UL\_UPDATE\_BUFFER\_SIZE\_REQ：** RLC层更新RLC BUFFER状态  
包含参数：  
total\_len:上行待传输的数据的总字节数；  
sr\_len:上行待传输的状态报告的字节数；  
total\_retx\_len:待上行重传数据的总字节数；  
retx\_bs\_p： 待上行重传的各个 RLC PDU 的长度数组；  
retx\_bs\_num： 待上行重传的 RLC PDU 的个数；  
tx\_header\_len:在包含所有的上行新传数据情况下的 RLC PDU header 的长度；  
tx\_len:待新传的上行数据长度

**RLC\_UL\_STATUS\_IND：**RLC DL接收到指示上行数据的RLC SR状态报告后转发给RLC UL， RLC UL根据其中信息释放RLC PDU， 并指示PDCP UL发送结果。

包含参数：  
ack\_sn: ACK SN 表示所以小于该值的 SN RLC PDU， 除了下面 nack\_sn 之外的 RLC PDU 都确认被接收到了；  
nack\_sn: NACK SN 表示未被成功接收到的 SN；  
so\_start:未成功接收的 SN 中丢失分片的起始字节；  
so\_end: 未成功接收的 SN 中丢失分片的结束字节；  
nelem\_filled: nack element 的数量，表示 RLC 丢包的数量。

通过过滤上面两个关键字后：  
观察 MAC\_UL\_UPDATE\_BUFFER\_SIZE\_REQ 中的数据是否都已经成功发送，并观察接下来的 RLC\_UL\_STATUS\_IND 是否指示 BTS 都已经接收成功。

正常期望：  
MAC\_UL\_UPDATE\_BUFFER\_SIZE\_REQ 中的 total\_len 是逐渐减少为 0，直至total\_len 为 0 为止，接下来的有 RLC\_UL\_STATUS\_IND，并且当中 nelem\_filled 应该为 0 则说明已发送的上行数据均被 BTS 确认接收成功。

异常：  
1. 最后MAC\_UL\_UPDATE\_BUFFER\_SIZE\_REQ中total\_len始终不为0，并没有逐渐减少，则继续步骤3；  
2. MAC\_UL\_UPDATE\_BUFFER\_SIZE\_REQ中total\_len最终减为0，并且后续也有RLC\_UL\_STATUS\_IND\_INFO，但是发现其中的nelem\_filled，则继续步骤4；  
3. MAC\_UL\_UPDATE\_BUFFER\_SIZE\_REQ中total\_len最终减为0，但是后续没有发现RLC\_UL\_STATUS\_IND\_INFO，则继续步骤5；

**13.2、查看网络信号**

**过滤关键字：LL1\_NRS**

当 RSRP 大于-100 且 RSRQ 大于-9， 表示信号质量较好。  
当 RSRP 小 于 -115 或 RSRQ 小 于 -15 ， 表 示 网 络 信 号 质 量 较 差

SNR:信噪比，参考值不低于0，最大300.

其中 rsrp、rsrq、snr 是本次的测量值。  
filtered\_rsrp、filtered\_rsrq、filtered\_nrs\_snr 是取最近 4 次的平均值更准确。但是它们只在cell\_select 之后才有效， cell\_select 之前这些值为 0。

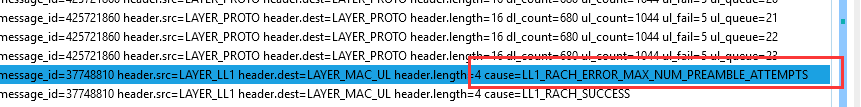
**13.3、随机接入**

过滤关键字：LL1\_RACH

通过查看LL1\_RACH\_CNF的状态也就是后面的Case 是不是成功的。如果是成功的则是下面的提示：



失败则为下面的提示：



# 14、注网问题

**14.1：注网流程**

1、用户应首先查询能否读取的SIM卡号，如果读取不到SIM卡号的话CFUN的值为0.另外当CFUN=0的话也是读取不到SIM卡号的（当模组进入PSM后，把SIM卡拔掉还是可以读取的SIM卡号的，设备查询还是在入网的状态）。

2、当能获取到SIM卡后，查询BAND的值，不对需要重新设置，设置完成后查询设置的是否正确。然后查询CFUN 的值是否为1，不为1设置为1。设置完成后查询一下，是否设置成功。

3、查询一下CSQ的值（信号质量强度），一般能获取到SIM卡，且CFUN查询的值为1以后CSQ的值就应该有了（CSQ都为99，需要查询SIM卡，CFUN的值以及卡是否为NB卡等）

4、查询CEREG的值是否为0，1（已经注册上网络），如果为0,0则需要设置一下CGATT=1。也可以先查询CGATT的值是否为1，如果不是可以手动设置为1。若为0,2则说明模块正在找网。需要等待。

如果在CEREG=0,2的情况下长时间注册不上网络，则很有可能是入网被拒了，需要查询一下网络和客户的SIM卡是否正确。

5、在香港的虚拟网络下NB注册网络需要单独配置APN否则CSQ一直为99，99

6、CSQ都为0，0状态，CEREG返回0，2：

**14.2：注网被拒常见原因**

1、RRC被拒，很有可能是网络问题

2、设备能读取到SIM卡号，且CFUN的值为1，且BAND设置也是正确的，但是模块一直在找网中，卡一开始在模块上是可以正常注网的，但是换了一个模块后就无法注网了。很有可能的原因是SIM卡开通了机卡绑定功能，一张卡只能在一个模块上使用，没有办法交叉使用SIM卡。

**14.3：Back-off机制**

当网络侧出现拥塞时，会通过下发 Back-off 定时器，以限制一段时间内终端的接入。

  该定时器有三个来源： 核心网通过 ATTACH REJECT、 TAU REJECT、 SERVICE REJECT 等消息下发；基站侧通过 Extended wait time 下发；网络侧 REJECT， 却不带定时器值时，终端选取 15-30min 的随机值。  
  协议要求终端起 Back-off 定时器后，在超时前执行了 AT+CFUN=0，则会将 Backoff 定时器剩余值存储到 KV 中； 重启终端时会根据 KV 中 Back-off 定时器剩余值重新启动该定时器，定时器超时后， 终端就可正常入网。  
  需要注意的是， 终端再次下电前一定需要先执行 AT+CFUN=0 后再下电，才可将KV 中该 Back-off 定时器剩余值更新，否则再次重启后，模组依然会按照 KV 中的Back-off 定时器值启动该定时器， 超时后才能正常入网。

**14.4、无网情况下的搜网机制**

Start search network （所有频点所搜完毕）------   deep sleep(10min) --------- search network---- deepsleep(20min) ………40min………80min…….……   24H ……24H ……24H ……24H ……24H ……

Deepsleep 下的耗流也是uA级别的。

# 15、MCU常见问题

上报信息中建议包含字段：Signal , RSRP 信号强度、SNR信号质量、PCI 物理小区标识、Battery 电池电量

模块串口的RTS 和CTS 默认是不支持的

# 16、入库、入网以及认证相关

**16.1 传导&OTA测试**

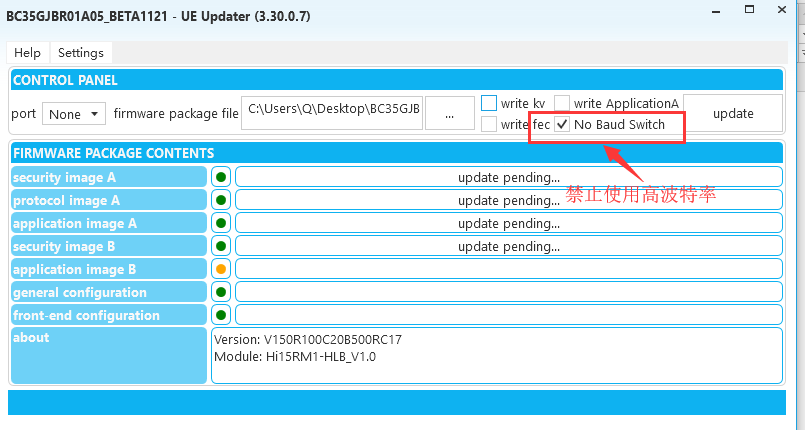
1、V150模块支持功率等级class3

2、CP功能 V120和V150都支持

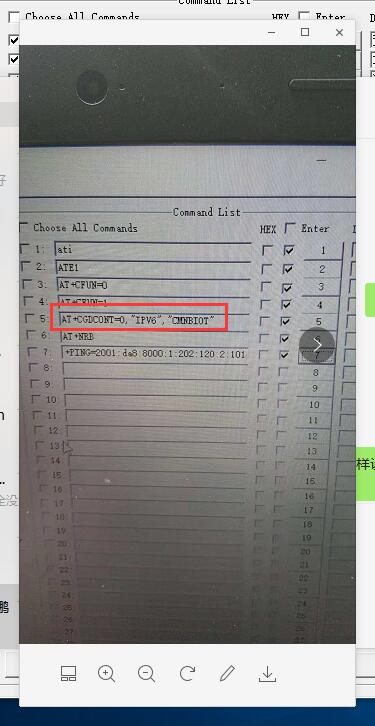
3、用户面的问题



可以通过升级海思B500的固件来解决，目前我这边只有BC28和BC35-G的BETA版本，该版本只针对入库的这两项。升级需要使用专门的升级工具。



4、IP 一致性的问题：



IP 一致性的问题 ，在测试前添加

AT+CGDCONT=0.”IPV6”,”CMNBIOT”

1. 入网问题

16.2、IPV6测试认证：

1. 目前测试仪表可能是安利，也可能是Anite,这两个仪表APN不同，需要跟实验室工程师确认用哪个，设置方法at+cgdcont=1,”IPV4V6”,”APN name”。用at+cgdcont?查询APN是否设置成功，如果发现有其他路的APN，请使用at+cgdcont=2 at+cgdcont=3这样的命令删除掉。
2. 测试时请使用NDIS方式拨号，在电脑上打开dos窗口使用ipconfig /all查询是否获得IP地址，实验室工程师会检查。之后使用ping -6来ping IPV6的地址和域名，使用ping -4来ping IPV4的地址和域名。
3. 如果有信号差或者注册不上的情况，请连接射频线的时候尽量用最少的转接线，减少线损。

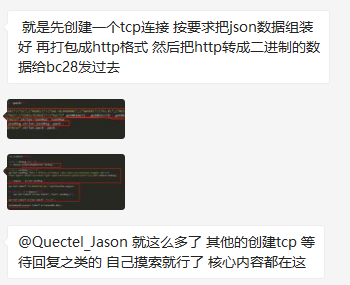
16.3、电信终端入库

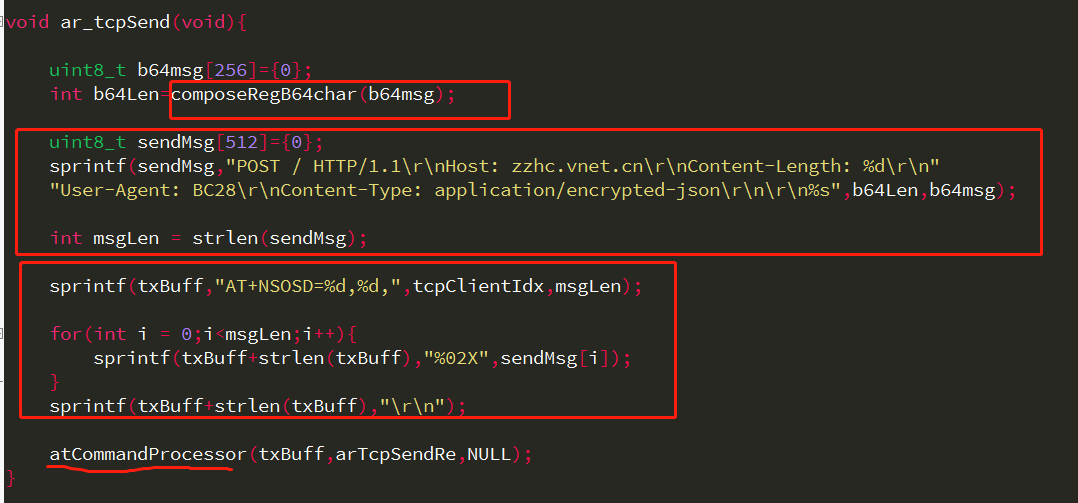
1、首先用域名解析把电信白皮书上的域名解析成IP

2、按照电信入库的数据格式把数据组成他们要求的格式

3、用我们的COAP协议发送数据到解析出来的IP+5683的端口上。

http 数据格式上传：





16.4、机卡一致性

机卡一致性测试：

设置成 单band

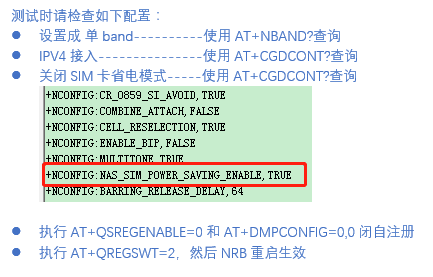
---使用AT+NBAND?查询

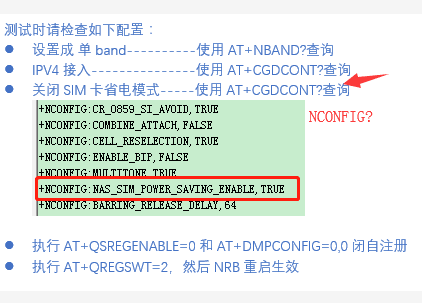
IPV4接入

---使用AT+CGDCONT?查询 （配置成IPV4V6）

关闭SIM卡省电模式

---使用AT+NCONFIG?查询





# 17、功耗相关

17.1、海思150&MTK不同电压下的功耗对比



17.2、使用TCP协议进入PSM后功耗偏大问题

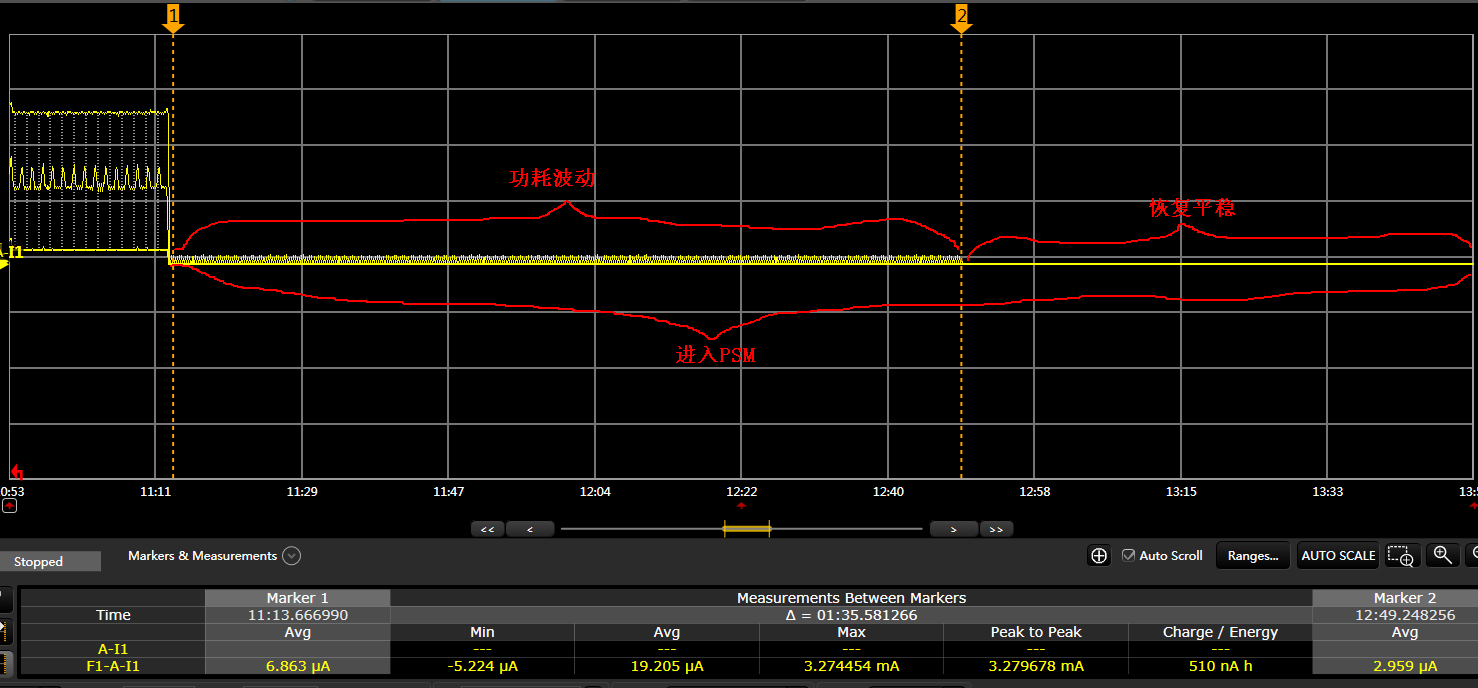
  客户反馈在使用我们海思模组的时候，用tcp功能，当进入psm后，功耗不稳定，经过研发分析结论如下，该问题暂时还不能解决。

   或者说服客户用udp协议，udp不会出现这个问题。

    模组进入PSM后， TCP底层是有一个定时器在工作，这个是协议栈的定时器，不能去除，所以当定时器超时时会导致功耗会有一点上升。

当TCP数据发送完毕关闭socket，TCP链路有一个120s的保护时间，所以从功耗上看，当关闭socket进入PSM后会有一段时间的波动，之后功耗恢复平稳。

使用客户模组验证结果如下：



# 18、透传与非透传

透传是将数据与命令不区分的发送出，

非透传是区分数据和命令的

透传与非透传的切换是：0X1A或者键盘上的Ctrl+z.

输入“+++”退出数据数模式，如果返回OK则表示进入命令模式。

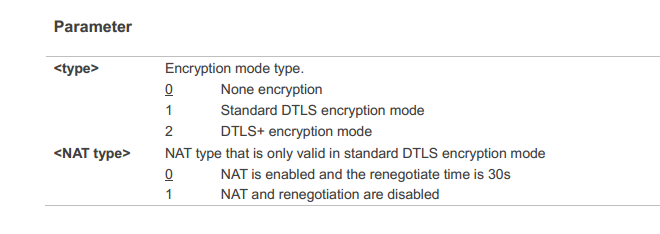
# 19、各大平台相关的问题

**19.1：电信平台绑定不成功**

1、尝试删除设备重新在平台上注册一下

2、150的版本会返回513的错误，可以尝试把平台上的设备删除重新注册一下。

3、模块开启了DTLS加密，但是平台上并没有开启加密，通过AT指令查看模块的加密是否被打开了：AT+QSECSWT? 默认的是0，1关闭DTLS加密。



**19.2 :南向、北向**

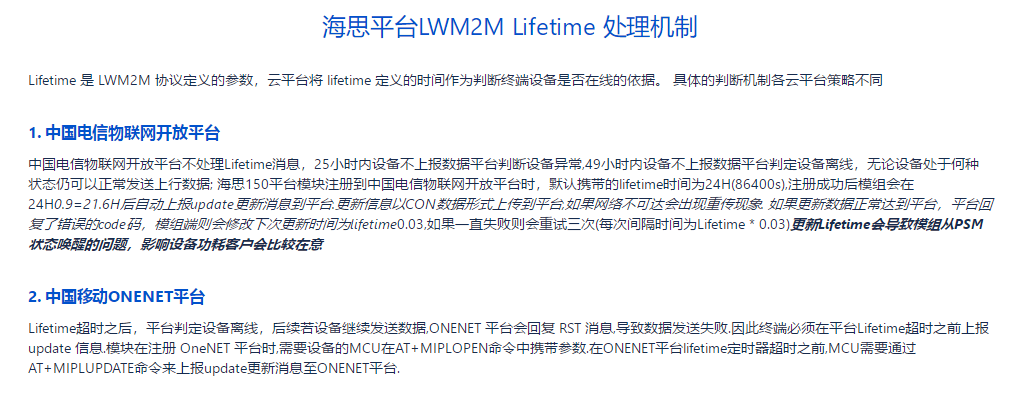
南向：应用服务器到平台到模组

北向：模组往平台往应用服务器

模组是在最底层的，依次的顺序为：

模组、基站、核心网、平台、服务器（由底向上）

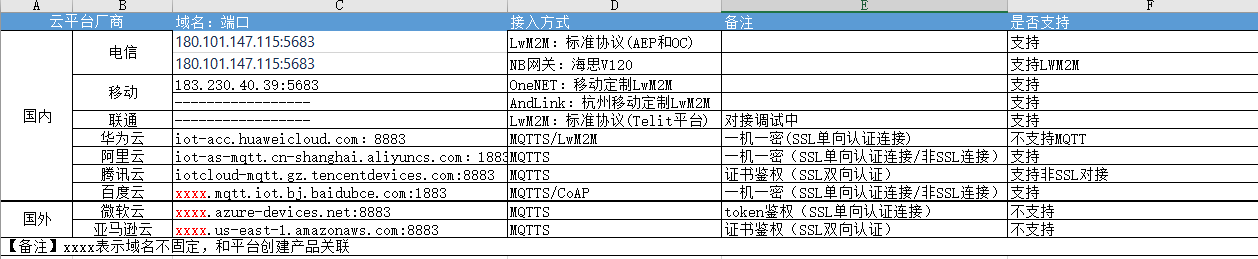
**19.3：平台的lifetime**



电信平台的lifetime机制目前已经支持客户自动配置，且自动更新的时间为：配置时间X 0.9。且数据发送到平台后该时间会重新清零，重新计时。

移动平台的lifetime的是更新只能通过数据或者AT命令来更新。

19.4：各大运营商平台的支持情况汇总



**19.5 :Andlink 平台**

目前海思支持Andlink平台的模块只有BC28JD的宽压版本单BAND8模块，需要特定的固件来自持，固件名\_ADL。已经归档。（2020-03-04）.

**19.6、移动NET平台**

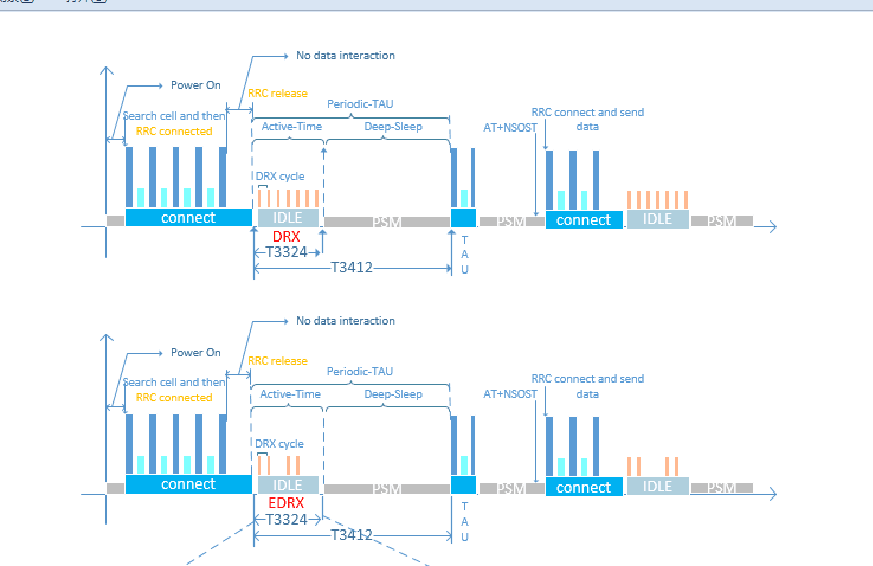
平台上开启了自动订阅，但是接受不到下发的MIPLDISCOVER信息。

平台上的自动发现资源开关也是要打开的。



之后就可以自动接受到MIPLDISCOVER信息了。

# 20、TAU 、PSM时间



TAU的时间是固定的，即使在PSM状态下模组唤醒了并完成了业务，此时模组再次进入PSM模式，但是TAU时间不会停止记时，时间到了后还是会从PSM中唤醒。并不是说TAU的时间不可配置。

海思的可以利用串口发送数据来唤醒模组。

MTK是通过PWKEY或者PSM\_INT按键来唤醒模块，MTK的进入PSM后串口是不通的，所以没有办法通过串口发送数据来唤醒模组。

# 21、SIM卡相关问题

NB 的SIM卡不支持热插拔。

读取不到SIM卡号，返回524错误，开机CFUN=0等这些情况，大概率的是由于：自动找网被关闭了。

**21.1、CCID**

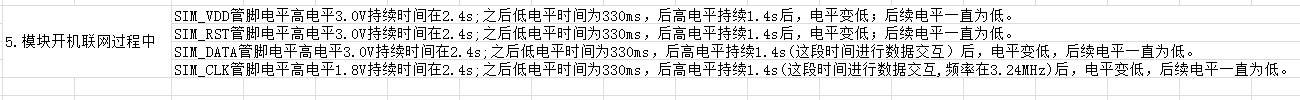
用指令读取ICCID的号和卡上显示的不一样（卡上最后一位是字母，实际读出来的是数字），运营商对卡商的要求。最终以读出来的数字为准。

**21.2、模块内部的eSIM**

需要定制OC，SIM卡尺寸5X6。具体的价格需要销售找项目经理去谈。



**21.3、BC95&BC28 SIM卡电平变化**



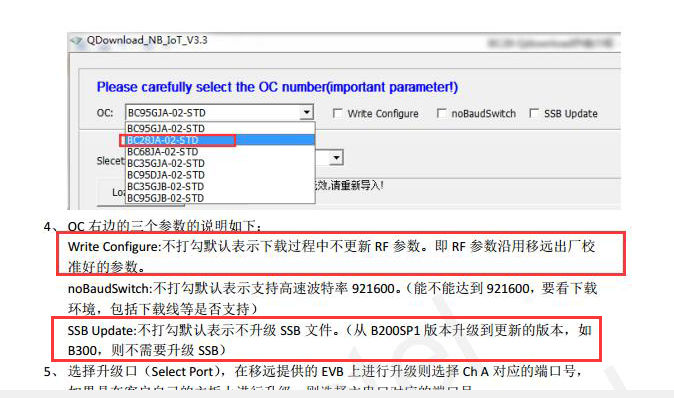
# 22、升级相关的问题

1、DFOTA升级失败

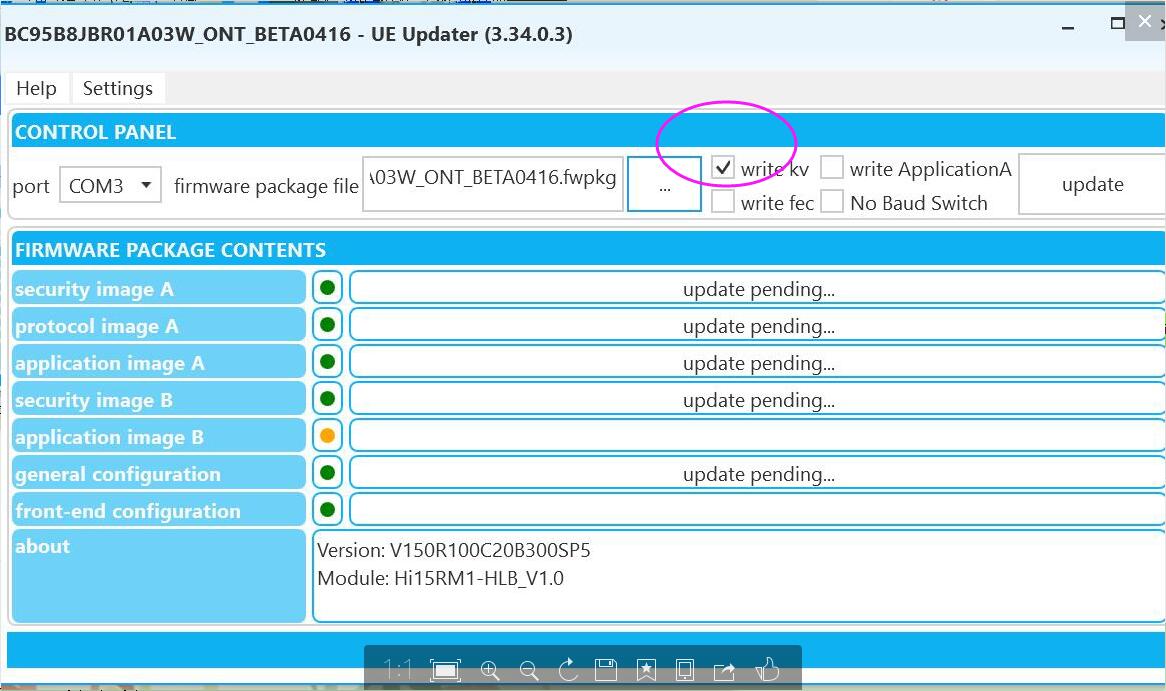
客户在DFOTA升级失败是因为填写了一些其他的描述，一般非必填项都不填。

2、目前海思120平台的BC单频模块对接oneNET平台需要专门的固件版本的支持，且仅仅是B8的模组支持，B5的模组不支持使用oneNET的固件版本。

3、BC28JAR01A02的固件往更高的固件升级需要用专门的工具添加SSB文件。否则升级会失败。



* 1. 跨基线升级



如果失败就把no band switch也勾上

# 23、高低温相关的问题

客户在做低温试验时出现了模块发送数据失败的现象（前20分钟左右的时间正常），从低温恢复到常温后又恢复正常（中间未做任何处理）。

出现这样的问题首先要和客户确认设备的MCU是使用的内部晶振还是外部晶振，内部晶振很有可能引起这个问题，更换为外部晶振后可以解决这个问题。

另外还有可能是低温下SIM卡导致的。

# 24、IMEI号相关

IMEI=8 TAC+7 SN

**25、lifetime 问题**

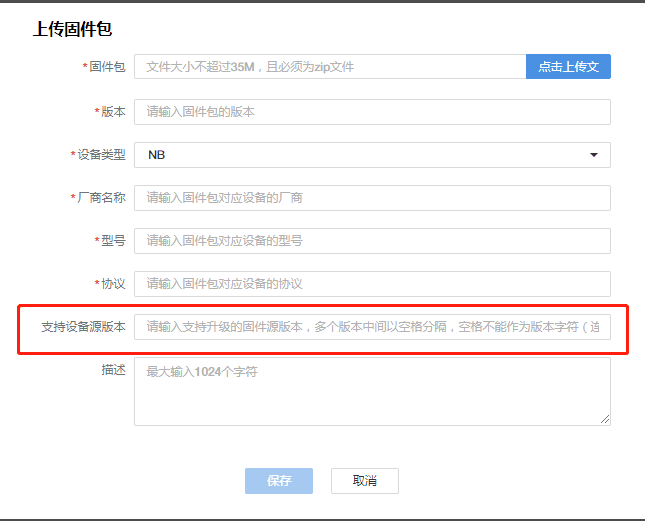
Lifetime 参数是 LwM2M 协议定义的参数。 云平台可以将 lifetime 的时间作为判断终端设备是否在线依据。具体的判断机制各云平台策略不同：  
1) 中国电信物联网开放平台: lifetime 定时器超时之后，电信平台判断设备异常， 但此时设备仍可以正常发送上行数据。  
2) 中国移动 OneNET 平台：lifetime 定时器超时之后，移动平台判定设备离线，后续若设备继续发送数据，OneNET 平台会复位模组的连接。导致数据发送失败。因此，终端必须在平台 lifetime定时器超时之前上报 update 信息，更新 lifetime 定时器。

**针对不同的云平台，模组的机制为：**  
1) 对于中国电信物联网开放平台: V150R100C20B300SP5(通过 AT+CGMR 命令查询)基线版本之前的模组注册上中国电信物联网开放平台时，默认携带的 lifetime 时间为 24H. 模组会在24H\*0.9=21.6H 的时候自动上报 update更新消息至电信物联网开放平台。

V150R100C20B300SP5基线版本及之后的版本，模组新增了 AT+QCFG="LWM2M/Lifetime"命令， 该命令可以配置lifetime 的参数。  
2) 针对中国移动 OneNET 平台: 模组在注册 OneNET 平台时，需要设备的 MCU 在 AT+MIPLOPEN 命令中携带 lifetime 参数。 在 OneNET 平台 lifetime 定时器超时之前， 设备的 MCU 需要通过  
AT+MIPLUPDATE 命令来上报 update 更新消息至 OneNET 平台。

# 25、其他问题

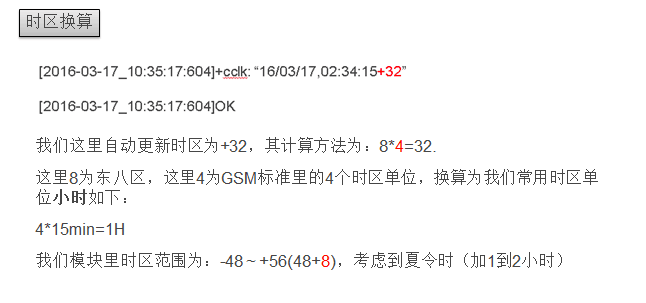
23.1：单模的模组也可以设置成其他的BAND不会报错，但是注册不上网络。例如BC98B8模块可以通过AT+NBAND=5设置成BAND5，查询出来也是BAND5，但是此时模块会一直在找网中，附着不上网络。



其他问题

1、固件版本带W和不带W的区别是PA芯片（射频）的不同，射频参数不一样，所以这两个版本不能互升。

9、时间+时区的换算



10、150目前还不支持MQTT with SSL

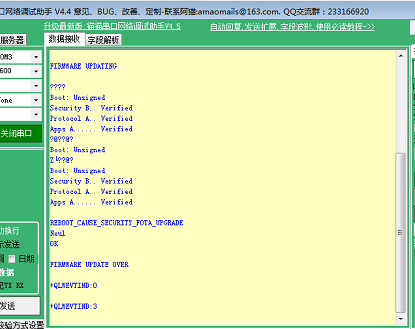
11、DFOTA升级问题

DFOTA升级时，对差分包进行数字签名时要注意差分包中的bin文件个数，如果有两个Bin文件，很容易导致上传差分包失败，可以把差分包解压出来单个加密上传。

ONENET 平台的FOTA包 直接就是 .bin

电信平台的FOTA包 都是 zip 进行签名的

15、实网下的功率测试是没有办法测试的，因为实网下模组走的是信令模式，模组的发射功率是收基站调度和控制的，所以没有办法通过模块来控制模组的发射功率。要测试模组的发射功率只有连接仪器下用非信令模式来强发测试。



更新到11-9日的记录。

你@hardy  他也抓瞎，C:\Users\Q\AppData\Local\Temp\X@8}U9MLE}EBUE273)]9PGF.gif  
江西FAE-彭家 2018/12/26 17:27:23  
  
1. V150模块支持功率等级class3  
17:31:50  
江西FAE-彭家 2018/12/26 17:31:50  
  
2.CP功能 V120和V150都支持  
江西FAE-彭家 2018/12/26 17:32:50  
  
V120不支持UP功能，V150后续支持UP（预计时间在2019年，hayden给的回复）  
  
FAE-胡永兴 2018/12/26 17:33:02  
  
C:\Users\Q\AppData\Local\Temp\G@YVKCPZR)X}3UKB(_VF`LW.gif  
  
FAE-胡永兴 2018/12/26 17:33:15  
  
谢谢！  
江西FAE-彭家 2018/12/26 17:33:18  
  
V120模块也支持class3    
江西FAE-彭家 2018/12/26 17:33:24  
  
不支持class6  
江西FAE-彭家 2018/12/26 17:33:37  
  
永兴，你把那个差异文档看一下