##### Q: 当配置多路APN后，执行AT+CGATT=1，激活的是哪一路APN?

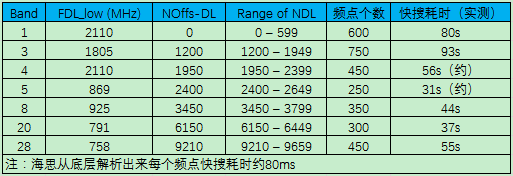
A: 通过AT+CGDCONT命令配置多路APN时，使用AT+CGATT=1，激活的是第一次配置APN的那一路， 所以就如截图结果，默认只有cid=0这一路，当多路PDN时，第一次配置的是cid=1，所以使用AT+CGATT=1激活的就是cid=1这一路。

##### Q：在信号不好的情况下， 从收到+QLWULDATASTATUS:4到进入PSM，模块经过了哪几个阶段，每个阶段受信号影响会产生什么结果。每个阶段有没有最大超时时间，或者哪个阶段会导致模块进入不了PSM，功耗会多少？

A：在信号比较好的情况下，模组发送CON类型的数据带快速释放的标志位。 平台回复ACK消息后，模组收到ACK后，提示+QLWULDATASTATUS:4 此时基站会快速释放连接。待active time超时后，模组进去PSM状态。 如果信号较差的情况。模组上行消息发送后，没有收到ACK， 模组会进行CON数据的重发， 3次或者4次。 重发次数与信号的质量有关。 重发最大超时时间不超过165s. 此时模组是处于active状态。 平均功耗约为80~90mA左右(受信号质量影响较大)。

##### Q：全频段模组，在搜网上是怎样的策略。比如设置NBAND=8，3，5，比如一个频段B8扫完频点需要多长时间。使用的是电信卡，这时模组入网，要多久时间的。在等待模组入网超时的时间上，设置多少比较合理？

A：模组搜网的时长与所在BAND的频点个数有关。 band8有350个频点， 全部快速搜网大约需要40s的时间。  根据我们的《Quectel\_BC95&BC35-G&BC28\_应用设计指导\_V1.1.pdf》指导， 推荐的超时时间是300s.



##### Q：如果模块处于进入不了PSM的状态，执行重启模块再执行CFUN=0，这时模块的功耗和进入PSM的功耗相当？

A：是的！模组在CFUN=0的时候功耗与PSM状态的功耗是一样的。

##### Q：在模组上电入网，信号不好情况下，有没有可能导致进入不了PSM，或者超时时间很长。

A：目前为止，没有发现模组进不了PSM的情况。 但是在信号差的时候，有数据的重发，这个会导致模组会延迟进入PSM。

##### Q：AT+NUESTATS报告的接收信号的电平用dB表示，dB是一个相对测量单位。应该是dBm吗?如果不是—我们如何将其转换为dBm?

AT+NUESTATS  
Signal power:-842 -->RSRP： -84.2dBm  
Total power:-780 -->RSSI: -78.0dbm  
TX power:100 -->tx Poewr: 10dBm  
TX time:859 -> 859 ms  
RX time:26543 -> 26543 ms  
Cell ID:137262770  
ECL:0  
SNR:226 -->22.6dB  
EARFCN:3734  
PCI:105  
RSRQ:-108  
OPERATOR MODE:4  
CURRENT BAND:8

##### Q：AT+NUESTATS报告的“信号功率”和“总功率”有什么区别?BC95使用哪一个来确定覆盖率水平?

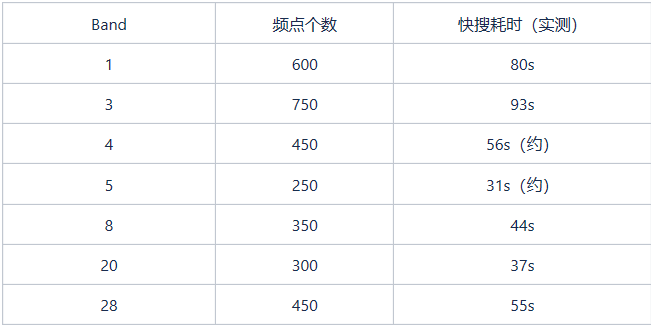
A：Signal power-> RSRP Total power->RSSI;覆盖水平取决于基站发送的RSRP阈值和模块的信噪比。

##### Q：AT+NUESTATS如何计算TX\RX中报告的时间?每个通信事件的值是向上舍入还是向下舍入到毫秒?它们是否包括服务操作，例如RACH的TX\RX ?

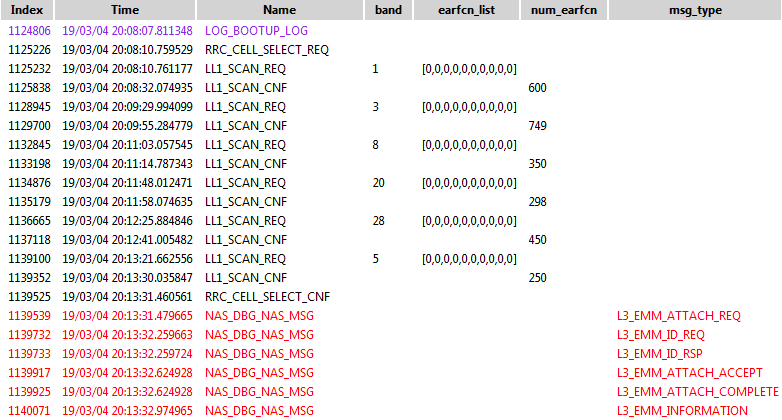
A：这个时间是指RF和PA在ms中传输和接收的累计时间。这个时间包含了所有与空中接口相关的传输和接收。

##### Q：模组按照band顺序搜网，每个band需要搜多久？

A：若模组配置为全band（1,3,8,20,28,5），没有保存先验频点，模组会按照band顺序进行搜索，首先进行一轮快搜，搜索每个band的时间跟band下的频点多少有关，可参看如下测试数据：



实测log：



##### Q：目前短信支持 的编码和解码 方式分别是什么？

A：7位8位16位都支持

##### Q：模组入网被拒，收到ATTACH\_REJECT（Cause: Requested service option not subscribed (33)），一般什么原因导致？

A：这个非UE问题，核心网侧分析可能有以下几个原因 ：

  1、 Non-IP数据传输 License关闭了  
  2、 ADD NONIPSUBCTRL。没有配置对应的APNNI信息  
  3、 请求的APN没有签约  
  4、 接入的用户类型不是NB

如果不是以上原因导致，需要继续定位的话需要核心网抓跟踪来定位。

##### Q：葡萄牙运营商测试：模组在PSM下，T3412到期时，从PSM唤醒，TAC改变，触发周期TAU被拒

A：之前海思的机制是在这个场景下模组会触发周期TAU，但国外运营商反馈跟据协议，此时模组应该触发正常的TAU。海思已在 V150R100C20B500SP1RC40修改。

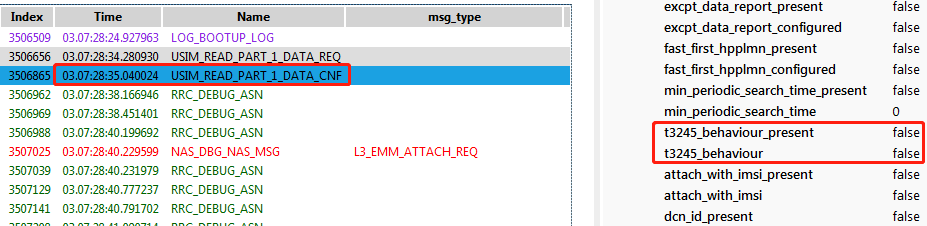
##### Q：三川水表客户，BC35G在RSRP小于-120时入网失败，而BC95HB可以入网成功

A：120的解决方案发布的比较早，前期的网络参数、配置等都还未调优，所以120上面在计算S准则时加了个优化策略：（q\_rx\_lev\_min <-100）&&（q\_rx\_lev\_min >= -130） 时，srxlev +=50； （q\_rx\_lev\_min <-130）时，srxlev +=100；

而150是发布时现网参数等已经比较稳定了，所以150上是符合标准的实现。

##### Q：韩国KT认证，要求注册被拒后未触发T3245定时器。

A：根据协议，T3425定时器是SIM卡里的，如果不支持就出发T3247，需确认是否使用了支持T3425的SIM卡。



#### 背景搜的机制？

Q：背景搜会在什么时机启动，是开机启动后立即启动还是要有什么条件触发？

A：卡里面的GUTI值中带的RPLMN是4.5.9，卡里面的hplmn是4.117.88，所以是由于走了漫游，就启动了背景搜。等附着之后，在2分钟后开始第一次的HPLMN搜索，再一次是2小时后，一直叠加这样子，最后一天一次吧。

如果像log中搜索过程被打断，那就会启动间隔1分钟的定期器再去尝试。这个功能是协议定的功能，所以关不了。

Q：卡里面的hplmn是4.117.88-----这个是从哪条LOG信息里看？  
A：可以通过RRC\_SIM\_DATA\_REQ，看details里面ehplmn\_list中的就是卡里相关的。B500版本对这个流程有优化，目前是PSM优先级较高，会打断背景搜；B500优化后会背景搜结束后再进PSM。

##### Q：现在V150平台的KV总共存储空间是8K，Open版本需要获取剩余的KV空间大小，用什么方法获取剩余KV空间大小？

A：目前没有这样的接口，机制就是写满了擦除循环写入。

##### Q：拥塞控制 Back-off 定时器功能说明(Backoff 机制)

A：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。

##### Q：RACH失败，为什么要将MAC 层buffer中的数据丢弃？有3GPP的协议规定吗？

A：目前我们的策略就是两次尝试发数失败之后就会把这次的数据丢掉，协议中应该是没有对这个有相关说明。

##### Q： V120支持SMS, 是LTE里SMS over SGs吗？

A： 1都支持，SMS over SGs对应的是ue联合附着；如果核心网支持S3口 ，UE就可以 用EPS附着发送

##### Q： TAU req字段Additional update type中，SAF位在什么情况下会被置位成1？

A：当前有数据在tau后要发送或者是之前有paging要触发建链就会为1

##### Q: 模块入网发起附着ATTACH REQ和 去附着DEATTACH的超时时间是多少？ 即失败后多久发起重试？

A: attach 10s超时 5次， detach 15s超时，5次。

##### Q: AT+CCLK获取的时间，是从NAS层核心网下发的， 这个是基于NITZ(3GPP TS 22.042)的协议的吗？

A: 是24301，EMM INFO 带过来的。

##### Q: UICC\_DBG\_PPS\_CNF中的len长度有取值范围吗？ 是不是只要这个值是0， 我就可以认为该SIM卡的PPS流程存在异常？

A: 一般跟UICC\_DBG\_PPS\_REQ的长度一致，0肯定是异常。

##### Q: 从日志中该如何确认模组在入网的时候和基站协商的子载波类型？（3.75K或者15K）

A: DSP\_NPUSCH\_REQ中的subcarrier\_spacing。（DSP消息暂不开放的）

##### Q: R14的定位的一些经纬度信息是基站侧听过SI消息发给模组的吗？

A: 有一整套东西，原理就是，核心网(基站) 说，帮我做一次测量，按照格式返回。芯片接到命令后，就去测量，把值给核心网（基站）核心网知道了测量，他又知道测量到的小区具体位置，然后得到一个位置发给UE。

##### Q：有国外客户测试，模组处于connect状态时，服务器端连续下发10包，512字节的数据，在115200波特率时模组可以正常接收到，但是在9600波特率时只能接收4包

A： 发包速率快，波特率速率无法匹配，请降低发包速率

##### Q：B180版本与B200版本互相升级（平滑升级）导致Flash被擦除

A：升级ssb.bin就会擦除，不会保留KV。

#### TCP功能的一些问题答疑

Q：模组入网后，创建TCP连接，待模组进入IDLE态后，TCP链路底层是如何维护的？  
A：TCP链路依旧保持，但是如果IP地址丢失后TCP socket会自动关闭。

Q：模组入网后，创建TCP连接， 待模组进入PSM态后，TCP链路底层是如何维护的？  
A：TCP链路依旧保持，保持多久视服务器的keepalive时间而定，如果进入PSM后，服务器发送keepalive探测包，模组是收不到的，此时服务器会RST模组。模组唤醒后发送数据会收到RST，自动关闭TCP连接

Q：connect状态下发送数据，若第一次数据发送失败，TCP协议栈是如何进行重传的，重传几次？ 每次重传间隔是多少？  
A：这里的发送失败如果是指NSOSD命令直接返回错误的话，这包数据就会丢失，需要重发；如果是协议核发出，但是服务器没有收到，或是服务器下发对应的ACK没有收到，那么会发生重传数据重传共计12次，间隔为3 6 12 24 48 98 192 386 386 386 386s。TCP建连SYN重传6次。

Q：使用TCP功能的时候，功耗会增加吗？ 如果增加，增加了多少？  
A：使用TCP和UDP一样，如果不打开TCP keepalive，功耗几乎不受影响（重传次数不多的情况）

Q：模组的TCP有keepalive定时器吗？ 如果有keepalive是怎么工作的？  
A：目前keepalive未打开，后续可能会提供设置的接口。（LWIP中keepalive间隔默认为2小时）

Q：TCP链路被异常关闭，TCP socket closed by err-13的可能原因？

A：1.TCP socket closed by err-13表示的就是网络链接出现异常中断的意思，它只是反馈当前网络的一种状态，具体网络断开原因需要多方面进行排查，单UE端无法做到精准定位；

  2.具体导致网络中断的原因有很多，比较典型的如下：  
   2.1 终端发送去附着命令（脱网）  
   2.2 终端发送关机命令（关机）  
   2.3 应用服务关闭链接的监听（网络异常导致链接断开 ：可能是应用服务器设置，也可能是网络异常导致，这个需要应用服务器端排查）

Q：在测试TCP功能中，发现，发送和接收操作几次之后，连接会异常断开  
A：从日志分析，发数时发现socket已经被重置，出现错误 Socket 1 had closed by err -14,此问题是服务器端主动发的重置要求导致，排查服务器端为什么 要发送 socket 重置

Q：创建一个socket然后发送TCP数据，随后关闭这个socke，再用同样的端口号创建，创建失败

A：在TCP/IP协议中，正常close socket之后，为了保证服务端能正常收到客户端的最后一个ACK，让服务端的状态能正常变迁到CLOSED状态，设置了一个TIME\_WAIT定时器(2\*TCP\_MSL)，计时时间为120s，所以正常四次挥手关闭的socket资源会被保护2分钟。

Q：关于海思Hi2115芯片不支持TCP Server功能的说明

A：关于TCP Server功能主要有以下风险

* 1. TCP SERVER功能可能会极大扩大终端产品的攻击面（DDOS,信息泄漏，执行恶意代码等）；
  2. 从整个产品来说，按照华为红线要求，需要提供认证机制（识别客户端是否合法），但是客户端认证部署在应用层，如果客户不部署引入的风险不可控。

鉴于以上安全风险，海思对所有模组客户发布的版本都不支持TCP server功能。

##### Q：短信的发送问题，发送的方式与3GPP 27005协议中的命令不一致，编辑好短信内容后，以Ctrl+Z结尾就能直接来发送短信，或者以十六进制数据1A结尾也能直接发送短信。但是当前Hi2110的实现与协议不一致

A：这个是按照协议实现的，1A就是Ctrl+Z的ASCII码。 对于UE来说只会识别1A结束的PDU码流，这个码流是直接添加1A还是通过Ctrl+Z的方式添加上去，UE不关注，这个应用层或工具保证Ctrl+Z能自动补充1A的字符到PDU后就可以了。

#### AT+NUESTATS命令查询的信息问题答疑

Q：PCI变了，为什么cellid没有变？   
A：更新pci, rrc更新cell id,现在有个现象：小区的的PCI被LL1更新了，但是RRC还没来得及更新cell id，就会造成 pci跟cell id对应不上的情况

Q：PCI变了，TXpower为-32768， 发送数据后恢复

A：是因为OOS（9:06:54）后cellid,pci，txpower被reset，LL1进行小区测量更新了PCI（9:07:00），RRC 小区选择更新了cell id（9:06:59）

tx power 没有被更新直到发送数据后更新,这个问题和海涛确认过由于从OOS到发送数据之间没有进行TX行为，所以没有更新，是正常现象。

##### Q：BC95G测试，在EPCO中没有携带Reliable Data Service

A：目前不支持此功能。

##### Q：模组附着网络被拒后cereg的值查询仍然为2， 期望值应该为3.

A：收到ATTACH\_REJECT 紧接着启动 T3402（12分钟），启动了T3402就说明UE有意识的要尝试附着，并在超时（12分钟后）就会发起附着请求。这个时候cereg应该是2。有关cereg为3的情况，例如：当被入网被拒的原因值是 EPS services not allowed (不允许操作EPS业务时)。cereg有可能会为3，以下三种被拒的原因值也会使cereg的状态可能为3.

* Cause #3 – Illegal UE
* Cause #6 – Illegal ME
* Cause #8 – EPS services and non-EPS services not allowed

##### Q：欧洲客户V120模组异常重启—REBOOT\_CAUSE\_PROTOCOL\_MONITOR\_REBOOT\_RE

A：有数据一小时没有发送出去会触发这个重启，PDH\_MONITOR定时器是为了防止协议核底层无保护的进行尝试驻留操作而做的保护定时器，每次在PDH模块收到数据时，会重启定时器，在队列为空时会停掉该定时器；定时器超时时，会重启整个系统。

##### Q：AT+QLWULDATAEX=3,AA34BB,0x0001命令携带release辅助RAI标志的数据在发送NON数据时无效，模块发送完数据无法立即release

A：发送NON数据携带RAI标志是会立即释放RRC链接，模组会从connect态 --> idle态 --> psm态，而模组从idle态进入psm态的时间是在核心网配置的；之所以接入不通运营商网络，有的会立即进入PSM态，下行数据不会从新唤醒模组，而有的没有立即进入PSM态，一旦有下行数据就会让模组重新唤醒，这都取决于核心网设置的。

* RDK的实现跟3GPP协议规定是一致的，只要上报NON数据携带RA标识，RRC链接是应该立即释放的，但是下行数据不是一定能唤醒模组的，这取决于模组是否进入PSM态，如果进入PSM态下行数据就不能唤醒模组；
* 模组日志中通过观察A核日志是否有+CSCON：1 --> +CSCON：0的状态变化来确定是否释放RRC链接。通过过滤asn,psm关键字可以观察模组是否立即进入psm态；

##### Q：模组在思科的核心网下接入，模组一直不停附着与去附着循环

A：是核心网的流程不对，发送EMM Information需要在建立EMM上下文之后，即ATTACH完成后，参考协议24.301-5.4.5

#### 小区重选

Q：如果模组搜到了小区A， 但已知无法获取A小区的MIB消息，接下来芯片的策略是什么？ 是重新扫频点 还是重新搜小区？  
A：根据协议，UE会bar掉A小区5分钟，然后如果该频点上有其他的小区，那UE会先尝试驻留其他小区，如果都驻留不了，UE会重新扫频。

Q：芯片进入idle态后会立即测量临近小区吗？ 测量临近小区需要什么特殊的触发条件吗？  
A：UE进入IDLE态后不会立即侦测邻区，只会测量主服务小区，当主服务小区的RSRP低于sib3、sib5中配置的同频和异频邻区测量门限之后，UE才会启动侦测邻区。

Q：锁定频点，不锁定PCI：此情况是否能发起重选？同频和异频都能重选吗？

A：可以触发重选，包括同频和异频

Q：锁定频点，锁定PCI：此情况是否能发起重选？同频和异频都能重选吗？

A：不可以触发重选，包括同频和异频

##### Q：使用AT+MLWULDATAEX命令发送CON数据，若信号很差，发送超时的时间是多少？

A：150模组每次重传的时间大于4秒，小于126秒，具体时间是通过算法实现，根据信号强度等相关因素计算的，总时间165秒以内，安全模式：400秒以内；

  120B657SP5版本重传时间（random为1到5的随机数）：第一包发送失败==>(10+<random>) 秒，重传1 ==>(10+<random>) 秒，重传2 ==>2\*(10+<random>) 秒；重传3 ==>3\*(10+<random>) 秒，重传4 ==>4\*(10+<random>) 秒，

  总时间165秒以内，安全模式：400秒以内。

##### Q：客户在沃达丰运营商下测试BC95模组，新的SIM卡第一次开机入网正常，断电后再次上电，入网出现SIM鉴权失败

A：这个错误原因是 Synch failure，可能是突然断电SIM卡没来得及存储相关信息，和核心网信息没对齐，请客户软重启后再尝试几次。和模组固件没有关系，就是SIM卡中的信息和核心网鉴权请求带下来的信息同步出现问题。

##### Q：V150模组，B300版本，模组发起联合附着成功后，在执行AT+CGATT=0去附着的动作，仅去附着了eps only.

A：按照协议NB是不应该支持联合附着的。非bug，代码实现上就没有去实现CS的去附着，主要是基于这个是兼容设计，后续运营商的核心网支持了非联合附着，会考虑将联合附着移除。

#### DFOTA

Q：[DFOTA]UPdating过程中，模块自动重启，上报了3条BOOT 的消息？

A： 3次重启是正常。下载完成后会先第一次重启，进入小核校验并升级大核；大核升级完成后会第二次重启，进入大核升级小核；小核升级完成后所有核都升级完成 会第三次重启，退出升级流程。

##### Q：模组支持的UDP功能，在模组接收到服务器的UDP消息时，会去检查UDP协议包中的check sum域吗？

A： 我们发上去的不会计算check sum，收到的会校验check sum

##### Q：SIM卡检测机制

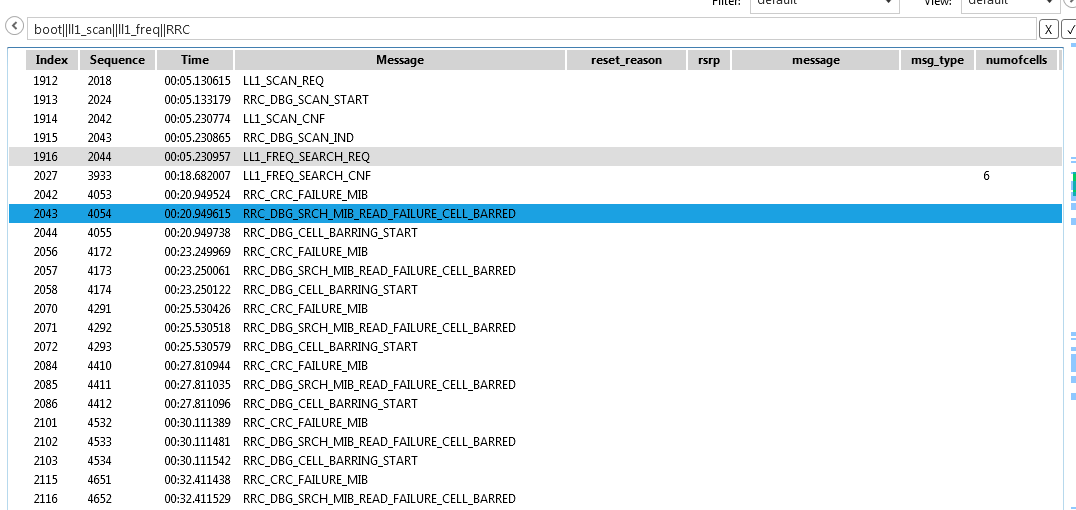
A：我们的SIM卡检查机制，在UE需要做业务的时候，会进行SIM卡的在位检查，在刚进IDLE入状态的时候，30s之内可以检查到SIM是否在位，超过30s之后，就不会进行检查，再次发送数据，会触发检查。

##### Q：模组进入PSM状态后， 约3分18秒，模组功耗会变大，然后无法恢复或者很久才能恢复到deep sleep的功耗状态

A：log的最后由于ESM PTI TIMER（procedure Transaction Identity）定时器超时,此定时器一次性超时，不会周期性启动。只会产生一点点毛刺对功耗影响不大。

##### Q： 通过慢搜流程搜到小区后，但是无法读取到小区的MIB消息。 接下来UE行为会怎样？

A:UE 读取小区的系统消息，如果解析失败，UE会将该小区barred，然后去读另外的小区。



##### Q：OneNET下行请求重发间隔是多少？

A：默认情况下，平台在第一包发送之后5~7s内没有收到回复就会发送第二包，再等待2\*（5~7）s若没有收到回复再发送第三包，再等待4\*（5~7）s若没有收到回复则判断超时。

##### Q：目前版本是否支持TLS和DTLS

A：目前版本不支持TLS（这个是基于TCP的），可以支持DTLS。

##### Q：NAS层重传机制，重传间隔多少？

A：从B500SP2基线版本将NAS层重传从2次修改为30次；底层上报失败则马上进行重传，没有间隔时间。NAS以下各层的传输超时时间及重传按照协议实现。NAS层还有个5min钟的保护定时器，如果数据5min内传输失败则主动Release。

#### Q：模组PSM状态被唤醒(PSM唤醒PSM)

A：模组处于PSM状态时，可以直接被AT串口或者模组内部定时器直接唤醒，并发送数据到网络。模组PSM状态被唤醒有如下情况：

 ·终端的MCU有上行数据发送，通过AT串口发送数据给模组。  
 ·3GPP协议的跟踪区域更新(TAU)上报。包括：周期性更新，区域码变化更新，链路异常更新。  
 ·终端的MCU发送CON类型的数据时，因长时间没有收到云平台的ACK应答，CON数据重传导致的PSM唤醒。  
 ·因使用了LwM2M协议，需要上报update消息来更新lifetime时间导致的PSM唤醒。  
 ·因运营商的自注册功能，若第一次自注册失败，模组会重发自注册信息导致的PSM唤醒。  
 ·模组进入无网状态，PLMN\_SEARCH定时器超时后搜网，会从PSM唤醒。