M5311 AT 使用流程示例

NB-IoT 系列

版 本：V1.3

日 期：2018-9-18

中移物联网有限公司

iot.10086.cn

重要声明

版权声明

商标声明

中移物联网有限公司和中移物联网有限公司的产品是中移物联网有限公司专有。在提及其他公司及其产品时将使用各自公司所拥有的商标，这种使用的目的仅限于引用。

不作保证声明

中移物联网有限公司不对此文档中的任何内容作任何明示或暗示的陈述或保证，而且不对特定目的的适销性及适用性或者任何间接、特殊或连带的损失承担任何责任。

保密声明

本文档（包括任何附件）包含的信息是保密信息。接收人了解其获得的本文档是保密的，除用于规定的目的外不得用于任何目的，也不得将本文档泄露给任何第三方。

关于文档

修订记录

版本	日期	作者	描述
1.0	2018.4.12	曾定立	首次创建
1.1	2018.5.16	曾定立	增加 1.4 睡眠状态指示
1.2	2018.6.1	孟 桃	HTTP 协议 AT 指令变更
1.3	2018.9.18	曾定立	睡眠模式变更、TLS 变更、新增 NB 网络配置、硬件相关指令、Genie Log 使用

注：文档中涉及的相关指令参数意义详见中移物联网公司《M5311 AT Command Interface Specification》文档

目录

1. 睡眠模式

M5311 包括两种睡眠模式：①深度睡眠；②浅睡眠。

深度睡眠：PSM 模式，外设断电、AT 命令任务终止、uart 无响应，触发 WAKEUP_IN 下降沿可唤醒深度睡眠。

浅睡眠：关闭部分外设功能，串口无响应，串口输入”AT”可唤醒浅睡眠。

1.1.深度睡眠

1.1.1.进入深睡眠模式

模组在以下四种情况下，若在条件成立前 10s 内无 AT 命令输入[1]，会进入深度睡眠模式：
① 在飞行模式（AT+CFUN=0）下，模组在 10s 后进入深度睡眠；
② 在 TCP 断开连接前提下，附着上网络并同步进入 PSM 模式后，模组进入深度睡眠；
③ 在 TCP 断开连接前提下，若 eDRX 有效周期大于 81.92s，并同步进入 eDRX 模式，模组进入深度睡眠；
④ 在模组驻网失败（AT+CEREG?返回+CEREG: 0,0）后，模组进入深度睡眠模式。

1.1.2.深睡眠唤醒

进入深度睡眠后 AT 命令不会做应答，且输入 AT 命令无法唤醒模组，深度睡眠可以通过以下方式唤醒，唤醒时间默认为 10s(可通过 AT*WAKETIME 指令配置唤醒时长)，期间发送 AT 有响应：
①触发 WAKEUP_IN 下降沿；

1.2.浅睡眠

1.2.1. 进入浅睡眠模式

模组在以下情况下，若在条件成立前 10s 内无 AT 命令输入[1]，会进入到浅睡眠模式：
① 进入空闲态后，模组立即进入浅睡眠模式；

[1] 若在模组睡眠前，输入 AT 命令，若此时即使满足睡眠条件，模组仍然会维持 10s 的唤醒状态；若持续输入间隔小于 10s 的 AT 命令，模组在发送 AT 命令期间将持续维持唤醒，直到最后一条 AT 命令输入完成后 10s，模组才能在满足睡眠条件下进入睡眠；若要实现发送完最后一条 AT 命令立即进入深/浅睡眠，可输入 AT*ENTERSLEEP。

② 若保持 TCP 连接，附着上网络并同步进入 PSM 模式后，模组只会进入浅睡眠，而不会进入深睡眠；
③ 若保持 TCP 连接，若 eDRX 有效周期大于 81.92s，并同步进入 eDRX 模式，模组只会进入浅睡眠，而不会进入深睡眠；

1.1.2.浅睡眠唤醒

进入浅睡眠以后，可以通过以下方式唤醒，唤醒时间默认为 10s，期间发送 AT 有响应：
① 输入”AT”唤醒[2]：输入的首个 AT 只做唤醒中断，而不做响应，第二个 AT 才会响应。CMIOT 规定只可以输入 AT 唤醒浅睡眠，并待第二个 AT 响应返回 OK，方可输入其他 AT 命令进行操作，规定用法如下：

```
                    //模组处于浅睡眠状态
AT                  //输入AT唤醒浅睡眠
                    //首条AT只做中断唤醒，不会响应返回OK或者error

AT                  //输入第二条AT确认浅睡眠是否唤醒
OK                  //返回OK，浅睡眠已唤醒，可以进行其他操作

AT+SWVER
M5311-MLVH0S01
OK
```

② 触发 WAKEUP_IN 下降沿(可通过 AT*WAKETIME 指令配置唤醒时长)；

1.3.开关睡眠

1.3.1.关闭睡眠

关闭睡眠以后，模组将维持在唤醒状态。
例如：

```
AT+SM=LOCK              //关闭睡眠，模组维持唤醒状态，输入AT命令有响应
                        //仅生效一次，重启或深睡眠唤醒后该设置失效
OK
AT+SM=LOCK_FOREVER      //永久关闭睡眠，模组维持唤醒状态，输入AT命令有响应
                        //重启模组后该设置依然生效
OK
```

[2] 浅睡眠唤醒只能通过输入“AT\r\n”字符来唤醒，不能通过输入其余指令唤醒。

1.3.2.打开睡眠

例如：

```
AT+SM=UNLOCK                    //打开睡眠，模组会进入相应的深睡眠或浅睡眠模式
                                //仅生效一次，重启或深睡眠唤醒后该设置失效
OK
AT+SM=UNLOCK _FOREVER           //永久打开睡眠，模组会进入相应的深睡眠或浅睡眠模式
                                //重启模组后该设置依然生效
OK
```

1.4.睡眠状态指示

1.4.1.深度睡眠唤醒状态指示

判断模组是否处于深睡眠状态有两种方法：①通过 WAKEUP_OUT 输出电平判断；②通过 URC 上报消息判断。两种方法均默认关闭，需要输入相关 AT 命令进行设置。

① 通过 WAKEUP_OUT 输出电平判断

使能 WAKEUP_OUT 引脚功能：

```
AT+CMSYSCTRL=1,1                //使能WAKEUP_OUT引脚
OK
```

WAKEUP_OUT 输入电平与深睡眠状态对应关系如下：

WAKEUP_OUT	睡眠状态
高电平(LED 亮)	唤醒状态
低电平(LED 灭)	深睡眠

② 通过 URC 上报消息判断

例如：

```
AT*MATWAKEUP=1                  //使能深度睡眠唤醒提示功能
OK
AT*SLEEP=1                      //使能进入深度睡眠提示功能
OK

*GOTOSLEEP                      //进入深度睡眠模式

*MATWAKEUP                      //深度睡眠被唤醒
```

1.4.2.浅睡眠唤醒状态指示

判断模组是否处于浅睡眠只能通过 STATUS 输出电平进行判断，暂无 URC 上报功能。STATUS 默认关闭，需要输入相关 AT 命令进行设置。

通过 STATE 输出电平判断

使能 STATE 引脚浅睡眠指示功能：

```
AT+CMSYSCTRL=0,1                    //使能STATUS引脚，并设置为浅睡眠指示功能
OK
```

STATUS 输入电平与浅睡眠状态对应关系如下：

STATUS	睡眠状态
高电平(LED 亮)	浅睡眠
低电平(LED 灭)	唤醒状态

1.5.睡眠相关设置

（1）WAKEUP_IN 唤醒时长设置

WAKEUP_IN 下降沿可唤醒深/浅睡眠，默认唤醒时长为 10s，若无网络相关业务发生且无其余 AT 指令输入，10s 后模组将重新进入睡眠，可通过 AT*WAKETIME 来进行配置该唤醒时长。

注：若 WAKEUP_IN 下降沿唤醒睡眠后，做了网络相关业务，将更新 T3324 及 T3412 定时器，模组需同步 T3324 定时器才能进入深度睡眠。

例如：

```
AT*WAKETIME=5                       //设置WAKEUP_IN中断唤醒时长为5s
OK
```

（2）符合睡眠条件下，快速进入睡眠

以下两种情况，可通过发送 AT*ENTERSLEEP 命令实现快速接入深/浅睡眠模式

① 由于发送 AT 命令会维持模组唤醒 10s，若在符合 1.1.1 及 1.2.1 所述条件下，10s 内有 AT 命令发出，会造成模组推迟进入深/浅睡眠，此时可通过 AT*ENTERSLEEP 快速进入睡眠。

例如：

```
AT*SLEEP=1                          //使能进入深度睡眠提示功能
OK

AT                                  //T3324即将到期时输入AT，将维持唤醒10s
OK

AT*ENTERSLEEP                       //立即进入深睡眠
OK
```

*GOTOSLEEP //进入深度睡眠模式

② 若在符合 1.1.1 及 1.2.1 所述条件下，WAKEUP_IN 唤醒深/浅睡眠后，将维持唤醒相应的时长，唤醒期间若无业务发送及 TAU 到期，此时可通过 AT*ENTERSLEEP 快速进入睡眠。

AT*MATWAKEUP=1 //使能深度睡眠唤醒提示功能

OK

AT*SLEEP=1 //使能进入深度睡眠提示功能

OK

*GOTOSLEEP //进入深度睡眠模式

*MATWAKEUP //WAKEUP_IN唤醒

AT*ENTERSLEEP //立即进入深睡眠

OK

*GOTOSLEEP //进入深度睡眠模式

2. 驻网流程及 NB 网络配置

2.1 驻网流程

注意：每个 AT 命令之间应该留有一定时间间隔

（1）开机启动

*ATREADY: 1 //AT 命令通道准备完成

+CFUN: 1

+CPIN: READY //SIM 卡识别成功

AT //开机之后循环发送 AT 直到返回 OK，证明模块初始化正常

OK

（2）驻网流程

AT+COPS=1,2,"46000" //手动选择移动运营商，此步可省略

OK

AT+CSCON=1 //打开信号提示自动上报，可省略

OK

AT+CEREG=1 //打开注册信息自动上报，可省略

OK

+CSCON:1 //自动上报的网络信号提示——已连接

+CEREG:1 //自动上报的网络注册信息——1-本地网络已注册入网，5-漫游已注册，其

```
                                        //它情况为注册异常，详细请参考 AT 命令手册
                                        //如果未使能自动上报，则用户需要使用 AT+CEREG?查询注册状态
AT+CGACT?
+CGACT: 1,1                             //+CGACT: <cid>,<state> PDP 连接状态——< state > 1-cid 对应定义的 PDP
                                        //地址已激活，< state > 0-cid 对应定义的 PDP 地址去激活
OK

AT+EGACT=1,1,"","",""                   //激活PDN，默认自动激活PDN，此步骤可省略
+EGACT:1,1,1,1                          //PDN 连接成功
OK

AT+CGDCONT?
+CGDCONT: 1,"IP","cmiot","",0,0,0,,,,,,0,,0
                                        //查询当前 APN，此步骤可省略
OK

AT+CGPADDR=1
+CGPADDR: 1,"10.64.118.25"              //查询 PDP 地址，此步骤可省略
OK
```

注：需要确认入网状态为已注册才能进行后续数据收发操作，如果不使用自动上报功能，可使用AT+CEREG?命令主动查询当前附着状态直到变为已附着，用 AT+CGACT?命令查询 PDP 上下文激活状态，目前测试开机注册时间范围为 10s-180s

2.2 NB 网络配置

2.2.1 PDN 激活与去激活

（1）自动激活

默认在驻网时自动激活 PDN/PDP context，若无特殊情况再次激活，开机驻网成功后将返回：

+IP: 10.132.37.162

则证明默认的 PDN 已连接完成。

（2）建立 PDN 连接方法

AT+CGDATA：DATA 模式

AT+EGACT：Command 模式.

(M5311 不支持使用 AT+CGACT=1,1 方式激活 PDN)

（3）PDN 去激活

① 只有一条 PDN 连接

无法做到去激活 PDN，而保持 UE Attach，只能通过 Deattach 实现：

AT+CGATT=0

AT+CFUN=0

② 有多条 PDN 连接

AT+CGACT=0,<cid>　　//去激活<cid>对应的 PDP，适用于所有情况

AT+EGACT=0,<cid>　　//去激活<cid>对应的 PDP，仅适用于 AT+EGACT 方式激活的方式，对于驻网默认自动激活的 PDN，此方法不适用

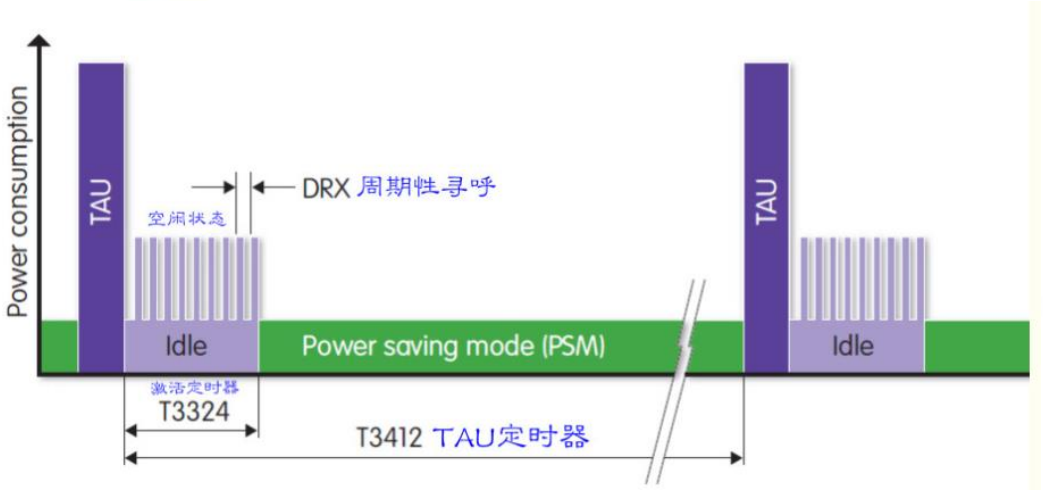
2.2.2 PSM/eDRX 模式配置与查询

（1）PSM/eDRX 设置

AT+CPSMS=1,,,"00101111","00100010"　　//设置 T3412 为 15hr，T3324 为 2min，编码参考 *GPRS timer 2/3*

AT+CEDRXS=1,5,"0011"　　//设置 eDRX 寻呼周期为 40.96

M5311 的 T3412 计时器从进入 Idle 态开始计时。流程图如下：



（2）PSM/eDRX Accept 查询

①PSM Accept 查询

AT+CEREG=5

AT+CEREG?

+CEREG: 1,"2A2A","0DDB0FBD",9,"00",0,0,"00100010","00101111"

　　//参考 AT 手册，最后两个参数分别代表 T3324 和 extended periodic TAU value (T3412)

若 TAU 没有达到 extended periodic TAU 范围，可以使用以下 AT 命令读取 T3412 的值，单位为 s：

AT+TAUAC?

+TAUAC: 10800　　//T3412 为 10800s

② eDRX Accept 查询

AT+CEDRXRDP

+CEDRXRDP: 5,"0011","0011","0001"　　//寻呼周期为 40.96s，时间窗为 5.12s

2.3 锁定 BAND/EARFCN

2.3.1 锁 BAND

（1）M5311 支持的 BAND

软件支持的 BAND：1,3,5,8,28

通过校准的 BAND：3,5,8

（2）M5311 搜网规则

根据所识别到 SIM 卡来优先搜索 BAND 的顺序，例如：识别到移动卡，则优先搜索 B8 然后是 B1,3,5…

（3）锁定 BAND

M5311-MLVH0S00 版本不支持锁 BAND，M5311-MLVH0S01 及之后版本支持锁 BAND。

通过 AT*CMBAND 来进行设置，重启后设置生效。

例如：

AT*CMBAND=8　　// Lock UE to B8

AT+CMRB　　//takes effect after rebooting

AT*CMBAND?

*MBAND: 8　　//Currently selected band 8

OK

AT*CMBAND=0　　//恢复默认值：B1,3,5,8,28

AT*CMBAND?

*CMBAND: 1,3,5,8,28

OK

2.3.2 锁 EARFCN/Cell

例如：

AT*MFRCLLCK=1,3736,3　　// Lock to EARFCN 3736

AT*MFRCLLCK=1,3736,3,192　　// Lock to EARFCN 3736, PCI 192

设置后立即生效，掉电不保存。

3. UDP/TCP 数据收发

3.1.创建 UDP/TCP Socket

3.1.1.创建 UDP Socket

AT+IPSTART=<sockid>,<type>,<addr>,<port>[,<cid>[,<domian>[,<protocol>]]]
例如：

```
AT+IPSTART=0,"UDP","47.93.217.230",2008   //创建编号为0的UDP socket，对端地址为47.93.217.230、端口为2008
                                          //socket编号范围为0-4
OK                                        //创建UDP成功
```

3.1.2.创建 TCP Socket

AT+IPSTART=<sockid>,<type>,<addr>,<port>[,<cid>[,<domian>[,<protocol>]]]
例如：

```
AT+IPSTART=0,"TCP","47.93.217.230",2008   //创建编号为0的TCP socket，对端地址为47.93.217.230、端口为2008
                                          //socket编号范围为0-4
OK                                        //创建TCP成功
```

3.2.绑定本地端口

AT+IPLPORT=<socket_id>,<local_port>
例如：

```
AT+IPLPORT =0,36000                       //绑定编号为0的socket到本地36000端口
OK                                        //绑定端口成功
```

注：该步骤可省略，系统分配随机端口

3.3.发送 UDP/TCP 数据

发送UDP数据：
AT+IPSEND=<socket_id>,[<data_len>],<data>[,<addr>,<port>[,<pri_flag>]]
注：若<addr>,<port>省略，则默认使用AT+IPSTART指定的地址和端口；若配置<addr>,<port>，该条指令将往所配置的地址和端口发送数据，该地址仅对此命令生效一次。

发送TCP数据：
AT+IPSEND=<socket_id>,[<data_len>],<data>[,<pri_flag>]

例如：

```
AT+IPSEND=0,0,"this is normal string"        //<data_len>为 0 或空缺表示发送 string 类型，自动计算<data>长度
+IPSEND: 0,21                                //第0号Socket成功发送21 Bytes数据
OK
AT+IPSEND=0,2,"3132"                         //<data_len>大于0表示发送hex，<data_len>为实际发送的hex字节数
+IPSEND: 0,2
OK
AT+IPSEND=0,0,"1233","183.230.40.150",36000,1
                                             //发送4 Bytes数据到指定地址，设置IPTOS优先级为lowdelay
                                             // IPSEND仅UDP能指定IP地址/端口
OK
AT+IPSEND=0,0,"1233",1
                                             //发送4 Bytes TCP数据，并设置IPTOS优先级为lowdelay
OK
```

注：AT+IPSEND 中 TCP 与 UDP 指令有所区别，UDP 模式下第四、第五个参数为<addr>,<port>，仅在 UDP 模式下可以配置；TCP 模式第四个参数为整形的<pri_flag>，输入其他类型数据返回 error。

3.4.接收 UDP/TCP 数据

M5311 可通过 AT+IPRCFG 设置多种数据接收模式：

AT+IPRCFG=<auto_receive>[,<mode>[,<hex>]]

例如：

（1）自动输出接收数据模式

```
AT+IPRCFG=1,0,0                  //自动输出 string 类型，格式：+IPRD: <socket_id>,<data_len>,<data>
OK
+IPRD: 0,15,hello, CMCC IOT      //自动接收输出 15 字节

AT+IPRCFG=1,1,0                  //自动输出 string 类型，格式：<data>
OK
hello, CMCC IOT                  //自动接收输出 15 字节

AT+IPRCFG=1,2,1                  //自动输出 hex 类型，格式：+IPRD:
                                 //<socket_id>,<remote_addr>,<remote_port>,<data_len>,<data>
OK
+IPRD: 0,"47.93.217.230",2008,15,68656C6C6F2C20434D434320494F54
```

（2）手动接收模式

```
AT+IPRCFG=0,0,0                  //手动输出 string 类型，格式：+IPRD: <socket_id>,<data_len>,<data>
OK
```

```
+IPNMI: 0,15                    //编号 0 的 socket 接收到 15 字节数据 string 类型
AT+IPRD=0,15                    //读出 socket 0 接收到的 15 字节
+IPRD: 0,15,hello, CMCC IOT
OK

AT+IPRCFG=0,1,0                 //手动输出 string 类型，格式：<data>
OK
+IPNMI: 0,15                    //编号 0 的 socket 接收到 15 字节 string 类型数据
AT+IPRD=0,15                    //读出 socket 0 接收到的 15 字节
hello, CMCC IOT
OK

AT+IPRCFG=0,2,1                 //手动输出 hex 类型，格式：+IPRD:
                                //<socket_id>,<remote_addr>,<remote_port>,<data_len>,<data>
OK
+IPNMI: 0,15                    //编号 0 的 socket 接收到 15 字节数据 hex 类型
AT+IPRD=0,15                    //读出 socket 0 接收到的 15 字节
+IPRD: 0,"47.93.217.230",2008,15,68656C6C6F2C20434D434320494F54
OK
```

注：本示例的测试服务器为中移物联网公司内部测试服务器。

3.5.关闭 UDP/TCP

```
AT+IPCLOSE =<socket>            //<socket>为 AT+IPSTART 所指定的<sockid>
OK
```

4. MQTT 数据发送

4.1. 通用流程

MQTT 是一个通用的数据传输协议，因此可以连接自己搭建的 MQTT 服务器或其它支持 MQTT 协议的云平台，先介绍基本的流程用于连接私有的 MQTT 服务器

4.1.1. MQTT client 参数配置

AT+MQTTCFG=<server>,<port>,<id>,<keepAlive>,<user>,<passwd>,<clean>,<encrypt>
例如：AT+MQTTCFG=120.76.28.207,36001,20142946,60,75829,XXXXOOOOAAAA,1,0
若采用 TLS 加密传输，encrypt 设置为 1，加密功能的使用在 4.3 中介绍

4.1.2. 连接-订阅-推送-取消订阅

连接

AT+MQTTOPEN=<usrFlag>,<pwdFlag>,<willFlag>,<willRetain>,<willQos>,<will-topic>,<will-mesg>

例如： AT+MQTTOPEN=1,1,0 //不带 willmsg
或者 AT+MQTTOPEN=1,1,1,1,1,mywill,bye //带上 willmsg

订阅

AT+MQTTSUB=<topic>,<Qos>[,<index>]

例如：AT+MQTTSUB=light,1,0
AT+MQTTSUB?可查询已经订阅的主题列表

推送

AT+MQTTPUB=<topic>,<Qos>,<retained>,<dup>,<message_len>,<message>

例如：

AT+MQTTPUB=pyr,1,0,0,3,7E7A7A (HEX)

或者

AT+MQTTPUB=pyr,1,0,0,0,abcdef (TEXT)

其中，HEX 形式发送需指令 message_len 的长度

取消订阅

AT+MQTTUNSUB=<topic>

例如：

AT+MQTTUNSUB=light

4.1.3. 断开连接-销毁参数配置

断开连接 AT+MQTTDISC

释放资源 AT+MQTTDEL

4.2. 连接云平台

目前支持对 Onenet 平台和 Aliyuniot 平台的简单接入，

接入 Onenet 时：
AT+MQTTCFG=<server>,<port>,<id>,<keepAlive>,<user>,<passwd>,<clean>,<encrypt>
Server 为 183.230.40.39，port 为 6002，id 填写待接入的设备 ID 号，user 填产品 ID 号，passwd 填写 APIkey

例如：
AT+MQTTCFG=183.230.40.39,6002,4069959,15,75829,IIOu0oFUg1guk20ornTK1uzAcnM=,1,0

后续操作同 4.1 章节

接入 aliyuniot 时：
AT+MQTTALICFG=<server>,<port>,<id>,<keepAlive>,<user>,<passwd>,<clean>,<encrypt>
配置时注意加上 ALI
Server :<${productKey}.iot-as-mqtt.cn-shanghai.aliyuncs.com>
Port:1883 id 填写 devicename，keepalive 值在 60 与 300 之间，user 填写 productKey，passwd 处填写 deviceSecret，配置完成后，其它操作同章节 4.1

4.3. MQTT-TLS 加密传输

使用加密传输时将配置中的 encrypt 设置为 1，目前仅与私有 MQTT 服务器 mosquitto 进行过调试。
第一次使用时，需要将 CA 证书写入 NV 中再进行连接，写入方式
AT*MNVMW=0,"cmmqtt","ca",0,ca_len,"your CA"
若服务器端开启了双向认证，还需写入 client_ca 和 client_key
AT*MNVMW=0,"cmmqtt","client_ca",0,clientca_len,"your client CA"
AT*MNVMW=0,"cmmqtt","client_key",0,clientkey_len,"your client key"
写入和配置完成后其它操作同章节 4.1

5. TLS 数据收发

5.1. TLS 参数设置

AT+TLSCFG=<tid>,<type>,<value>[,<type>,<value>[,<type>,<value>[…]]]

5.1.1.证书认证模式配置

TLS 安全传输方式主要包括以下三种情况：

（1）忽略服务器证书

该模式下可以忽略服务器证书，直接添加为信任，因此无需再配置服务器根证书。

例如：

```
AT+TLSCFG=1,1,”182.150.27.42”,2,50090,3,0,4,0,5,2
                        //设置服务器IP, Port，第7、8个参数（4,0），0代表忽略服务器证书，将其添加为信任证书
OK                      //TLS参数配置成功
```

（2）验证服务器证书

该模式下必须验证服务器证书，需配置正确的服务器根证书做校验。

例如：

```
AT+TLSCFG=1,1,”182.150.27.42”,2,50090,3,0,4,2,5,2
                        //设置服务器IP, Port，第7、8个参数（4,2），2代表必须服务器证书，需输入正确的服务器
                        //根证书
OK                      //TLS参数配置成功
```

（3）自动选择验证服务器证书

该模式下服务器证书为可选，若配置了服务器证书，则做相应的证书校验，若没有配置服务器证书，则忽略证书校验，直接添加服务器为信任。

```
AT+TLSCFG=1,1,”182.150.27.42”,2,50090,3,0,4,1,5,2
                        //设置服务器IP, Port，第7、8个参数（4,1），1代表必须服务器可选
OK                      //TLS参数配置成功
```

5.1.2.证书配置

1.仅加密传输，不认证合法性

5.1.1 节所述模式(1)和(3)，可以忽略证书配置，直接建立连接。

2.单向认证

①仅认证服务器合法性

仅认证服务器证书是否合法，可选 5.1.1 所述模式(2)或(3)，再配置服务器证书

例如：

```
AT+TLSCFG=1,6,1344,1,"-----BEGIN CERTIFICATE-----\r\n
```

```
MIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER\r\n
MA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN\r\n
MTEwMjEyMTQ0NDAwWhcNMjEwMjEyMTQ0NDAwWjA7MQswCQYDVQQGEwJOTDERMA8G\r\n
A1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA0G\r\n
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx\r\n
mdTs6st8GFgIlKXsm8WL3xoemTiZhx57wI053zhdcHgH057Zk+i5clHFzqMwUqny\r\n
50BwFMtEonILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEkHHxvYPZP9al4jwqj+8n\r\n
YMPGn8u67GB9t+aEMr5P+1"
OK                          //第4个参数为1代表还需继续输入证书
AT+TLSCFG=1,6,1344,1,"gmIgNb1LTV+/Xjli5wwOQuvfwu7uJBVcA0Ln0kcmnL\r\n
R7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+E1ixVA0hmnM3oTDPb5Lc9un8rNsu\r\n
KNF+AksjoBXyOGVkCeoMbo4bF6BxyLObyavpw/LPh5aPgAIynplYb6LVAgMBAAGj\r\n
gZUwgZIwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUtFrkpbPe0lL2udWmlQ/rPrzH\r\n
/f8wYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNV\r\n
BAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVz\r\n
dCBDQYIBADANBgkqhkiG9w0BAQUFAAOCAQEAuP1U2ABUkIslsCfdlc2i94QHHYeJ\r\n
SsR4EdgHtdciUI5I62J"
OK                          //第4个参数为1代表还需继续输入证书
AT+TLSCFG=1,6,1344,0,"6Mom+Y0dT/7a+8S6MVMCZP6C5NyNyXw1GWY/YR82XTJ8H\r\n
DBJiCTok5DbZ6SzaONBzdWHXwWwmi5vg1dxn7YxrM9d0IjxM27WNKs4sDQhZBQkF\r\n
pjmfs2cb4oPl4Y9T9meTx/lvdkRYEug61Jfn6cA+qHpyPYdTH+UshITnmp5/Ztkf\r\n
m/UTSLBNFNHesiTZeH31NcxYGdHSme9Nc/gfidRa0FLOCfWxRlFqAI47zG9jAQCZ\r\n
7Z2mCGDNMhjQc+BYcdnl0lPXjdDK6V0qCg1dVewhUBcW5gZKzV7e9+DpVA==\r\n
-----END CERTIFICATE-----"
OK                          //第4个参数为0代表证书配置完成
```

②仅认证客户端合法性

此模式是服务器需要验证客户端是否合法，可选 5.1.1 所述模式(1)或(3)，再配置客户端证书和私钥。

配置方法如下：

```
AT+TLSCFG=1,7,<size>,<more>,<certificate>          //<size>为证书长度，<more>代表是否分包输入
                                                   //<certificate>为客户端证书,方法与服务证书配置一致
OK
AT+TLSCFG=1,8,<size>,<more>,<private_key>          //<size>为私钥长度，<more>代表是否分包输入
                                                   //<private_key>为客户端私钥,方法与服务证书配置一致
OK
```

3.双向认证

客户端与服务器需互相认证是否合法，可选 5.1.1 所述模式(2)或(3)，再配置服务器证书、客户端证书和私钥。

配置方法如下：

AT+TLSCFG=1,6,<size>,<more>,<certificate> //<size>为证书长度，<more>代表是否分包输入
////<certificate>为客户端证书

OK

AT+TLSCFG=1,7,<size>,<more>,<certificate> //<certificate>为客户端证书,方法与服务证书配置一致

OK

AT+TLSCFG=1,8,<size>,<more>,<private_key> //<private_key>为客户端私钥,方法与服务证书配置一致

OK

5.2. 建立 TLS 连接

AT+TLSCONN=<tid>,<cid>,<time>

例如：

AT+TLSCONN=1,1,60 //建立TLS连接，设置超时参数为60s

OK

+TLSCONN:1,1 //TLS连接建立

注：返回+TLSCONN:1,1 说明 TLS 连接建立，若返回其他数值，说明 TLS 连接建立失败，错误码参见《M5311 AT Command Interface Specification》文档 5.9.2 节。

5.3. 发送 TLS 数据

AT+TLSSEND=<tid>,<data_len>[,<encoded_method>]

例如：

AT+TLSSEND=1,75,"GET https://182.150.27.42/test.html HTTP/1.1\r\nHost: 182.150.27.42\r\n\r\n"
//向服务器发送数据，数据格式默认为string格式，数据内容格式参考HTTP请求格式

OK

+ETLSEND:1,69 //返回数据发送结果，第2个参数为大于0的数值代表实际发送了多少字节，
//为-1则代表发送失败

5.4. 接收 TLS 数据

AT+TLSRECV=<tid>,<max_len>[,<encoded_method>]

例如：

+TLSNMI: 1,645 //提示接收645Byte数据

AT+TLSRECV=1,645,801 //接收645Byte TLS数据，并编码为string类型

OK

+TLSRECV:1,647,"HTTP/1.1 200 OK\r\nDate: Tue, 18 Sep 2018 03:37:44 GMT\r\nServer: Apache/2.4.27 (Win32) OpenSSL/1.0.2l\r\nLast-Modified: Mon, 27 Nov 2017 01:57:39 GMT\r\nETag: "15c-55eed3a259fdb"\r\nAccept-Ranges: bytes\r\nContent-Length: 348\r\nContent-Type: text/html\r\n\r\n<!doctype html public "-//W3C//DTD HTML 4.0 Transitional//EN">\r\n<html>\r\n\t<head>\r\n\t\t<title> Test </title>\r\n\t</head>\r\n\t<body>\r\n\t\t<H1>This is an example page for testing.</H1>\r\n\t\t<H2>This is an example page for testing.</H2>\r\n\t\t<H3>This is an example page for testing.</H3>\r\n\t\t\tThis is an example page for testing.\r\n\t</body>\t\r\n</html>"

+TLSNMI: 1,69 //提示接收69Byte数据，该数据可能为TCP消息等

AT+TLSRECV=1,69,801 //接收69Byte TLS数据

OK

+TLSRECV:1,-2 //因+TLSNMI提示为TCP 消息，TLS数据接收失败

+TLSERR: 1,-4 //返回错误码-4，提示TLS链接已断开(被服务器断开)

+TLSCLOSE:1,1 //关闭该TLS链接

5.5. 关闭 TLS 连接

AT+TLSCLOSE=<tid>

例如：

AT+TLSCLOSE=1 //向服务器发送数据，数据格式默认为string格式，数据内容格式参考HTTP请求格式

OK

+TLSCLOSE:1,1 //返回连接关闭结果，第2个参数为1代表连接已关闭，为-1代表连接关闭失败

6. HTTP/HTTPS 客户端协议

6.1. M5311 所支持的 HTTP/HTTPS 客户端协议介绍

M5311 的 HTTP/HTTPS 协议支持 HTTP 的 GET、POST、PUT、DELETE 方法，且同时支持多个 HTTP/HTTPS 实例，在 HTTPS 的使用中，需要用户在创建实例时传入将要访问服务器的 CA 根证书（或上级颁发者的证书）。

6.2.Get Texts from HTTP server

AT+HTTPCREATE="http://1i869245p2.iask.in:30686/"　　创建 http 实例
+HTTPCREATE:0　　模组返回 httpclient id:0
OK

AT+HTTPSEND=0,0,"/"　　发送 METHOD 为 0（GET）的请求包，路径为根目录“/”
OK　　模组收到命令

+HTTPCON:0,CONNECTED　　代表连接结果 CONNECTED 为成功，ERROR 为失败

+HTTPNMIH:0,0,800,Server: Microsoft-IIS/5.1　　服务器应答头
X-Powered-By: ASP.NET
Content-Type: text/html
Accept-Ranges: bytes
ETag: "0c76c133e39c71:8f6"
Content-Length: 496

服务器应答内容：
+HTTPNMIC:0,1,496,798,3c68746d6c3e0d0a0d0a3c686561643e0d0a3c6d65746120687474702d65717569763d22436f6e74656e742d5479706522200d0a636f6e74656e743d22746578742f68746d6c3b20636861727365743d676232333132223e0d0a3c6d657461206e616d653d2247454e455241544f5222200d0a636f6e74656e743d224d6963726f736f66742046726f6e74506167652046726f6e74506167652e456469746f722e446f63756d656e74220d0a3e0d0a3c7469746c653e4e6577205061676520313c2f7469746c653e0d0a3c2f686561643e0d0a0d0a3c626f64793e0d0a3c63656e7465723e20200d0a3c703e0d0a0d0a3c2f703e0d0a3c703e3c666f6e7420666163653d22cbcecce5222073697a653d2232223eb3c9b6bcd6dac9bdbfc6bcbcd3d

0cfdeb9abcbbe3c2f666f6e743e3c2f703e0d0a3c703e3c666f6e7420666163653d22cbcecce5222073697a653d2232223e266e6273703b266e6273703b203c61200d0a68726566

+HTTPNMIC:0,0,496,194,3d22687474703a2f2f7777772e7a7374656c2e636f6d223e485454503a2f2f0d0a5757572e5a5354454c2e434f4d3c2f613e3c2f666f6e743e3c2f703e200d0a3c2f63656e7465723e20200d0a3c2f626f64793e0d0a0d0a3c2f68746d6c3e0d0a

数据传输完毕后服务器主动关闭了连接，模组会有如下信息：
+HTTPERR:0,-2

6.3.POST Texts to HTTP server

假如以下是将要发送到服务器的请求头
Header: api-key:JDYiKyKfi4I4sOFWeJsI4S3Cbl0=
Content-type:NULL(default)
Content-length:10
发送内容：
Content: {"RPM":22}

那么，具体的 AT 指令如下：
AT+HTTPCREATE="http://1i869245.iask.in:30686/"
+HTTPCREATE:0
OK

If use default encode(string),the AT Command is（如果采用默认的编码格式）:
AT+HTTPHEADER=0,api-key:JDYiKyKfi4I4sOFWeJsI4S3Cbl0=\r\n,0
OK
注：
请求头里面的 host 字段模组会自动填充。
Content-type 字段如没有特殊要求，可以不填。
Content-length 字段不要额外填入，模组会根据 AT+HTTPCONTENT 命令自动判断

AT+HTTPCONTENT=0,{"RPM":22},0　　设置发送内容
OK

If use HEX encode,the AT Command is（如果采用 16 进制编码）:
AT+HTTPHEADER=0,6170692D6B65793A4A4459694B794B6669344934734F4657654A734934533343626C303D0d0a,1

OK

AT+HTTPCONTENT=0,7B2252504D223A32327D,1 同上
OK

AT+HTTPSEND=0,1," /devices/10372384/datapoints?type=3" 发送 METHOD 为 1（POST）
OK

+HTTPCON:0,CONNECTED
...

Note:*in <Header>,the "\r\n" is need,stand for a newline.if user want to input a char \r\n in defualt encode,an '\'should be add like this:*
AT+HTTPHEADER=0,api-key:JDYiKyKfi4I4sOFWeJsI4S3Cbl0=\\r\\n,0
AT+HTTPCONTENT=0,{"RPM":2\\r\\n2},0
注意：请求包里面每个字段后的换行符"\r\n"不可省略，如果用户仅仅是要发送\r\n 的字符内容，可在前面加"\"，例如：
AT+HTTPHEADER=0,api-key:JDYiKyKfi4I4sOFWeJsI4S3Cbl0=\\r\\n,0
AT+HTTPCONTENT=0,{"RPM":2\\r\\n2},0
模组会自动去掉转义字符"\"后按字符方式发送，且长度按照去掉转移字符后的长度发送。

6.4.Get a text file from an HTTPS server

AT+HTTPCREATE=https://182.150.27.42:50090/
+HTTPCREATE:0
OK

连接 HTTPS 服务器需要先配置证书，如果不配置证书，模组在连接时会跳过 TLS 的 certificate verification 的步骤，如果服务器要求必须 certificate verification 此步骤的话，不输入证书连接会失败。
传入证书的 AT 指令如下：（此服务器没有必须要求 certificate verification 此步骤）：
AT+HTTPCFG=0,1,-----BEGIN CERTIFICATE-----
\r\nMIIDhzCCAm+gAwIBAgIBADANBgkqhkiG9w0BAQUFADA7MQswCQYDVQQGEwJOTDER
\r\nMA8GA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwHhcN\
r\nMTEwMjEyMTQ0NDAwWhcNMjEwMjEyMTQ0NDAwWjA7MQswCQYDVQQGEwJOTDERM
A8G\r\nA1UEChMIUG9sYXJTU0wxGTAXBgNVBAMTEFBvbGFyU1NMIFRlc3QgQ0EwggEiMA
0G\r\nCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDA3zf8F7vglp0/ht6WMn1EpRagzSHx\r\n
mdTs6st8GFgIlKXsm8WL3xoemTiZhx57wI053zhdcHgH057Zk+i5clHFzqMwUqny\r\n50BwFMtEon

ILwuVA+T7lpg6z+exKY8C4KQB0nFc7qKUEkHHxvYPZP9al4jwqj+8n\r\nYMPGn8u67GB9t+aEMr5P+1gmIgNb1LTV+/Xjli5wwOQuvfwu7uJBVcA0Ln0kcmnL\r\nR7EUQIN9Z/SG9jGr8XmksrUuEvmEF/Bibyc+E1ixVA0hmnM3oTDPb5Lc9un8rNsu\r\nKNF+AksjoBXyOGVkCeoMbo4bF6BxyLObyavpw/LPh5aPgAIynplYb6LVAgMBAAGj\r\ngZUwgZIwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUtFrkpbPe0lL2udWmlQ/rPrzH\r\n,0
OK

AT+HTTPCFG=0,1,/f8wYwYDVR0jBFwwWoAUtFrkpbPe0lL2udWmlQ/rPrzH/f+hP6Q9MDsxCzAJBgNV\r\nBAYTAk5MMREwDwYDVQQKEwhQb2xhclNTTDEZMBcGA1UEAxMQUG9sYXJTU0wgVGVz\r\ndCBDQYIBADANBgkqhkiG9w0BAQUFAAOCAQEAuP1U2ABUkIslsCfdlc2i94QHHYeJ\r\nSsR4EdgHtdciUI5I62J6Mom+Y0dT/7a+8S6MVMCZP6C5NyNyXw1GWY/YR82XTJ8H\r\nDBJiCTok5DbZ6SzaONBzdWHXwWwmi5vg1dxn7YxrM9d0IjxM27WNKs4sDQhZBQkF\r\npjmfs2cb4oPl4Y9T9meTx/lvdkRYEug61Jfn6cA+qHpyPYdTH+UshITnmp5/Ztkf\r\nm/UTSLBNFNHesiTZeH31NcxYGdHSme9Nc/gfidRa0FLOCfWxRlFqAI47zG9jAQCZ\r\n7Z2mCGDNMhjQc+BYcdnl0lPXjdDK6V0qCg1dVewhUBcW5gZKzV7e9+DpVA==\r\n-----END CERTIFICATE-----\r\n,0
OK

当然也可以选择传入十六进制编码的证书：
or HEX encode:
AT+HTTPCFG=0,1,2D2D2D2D2D424547494E204345525449464949434154452D2D2D2D2D0D0A4D494944687A4343416D2B6741774942416749424144414E42676B71686B6947397730424151554641441374D5173774351594456514147457744A4F544445520D0A4D413847413155454368 4D4955473975 95584A5455307778475441584267 4E5642414D5445464276624746795531 4E4D4946526C6333516751304577676745694D4130470D0A4353714753496233445145424151554141344942447741776767454B416F494241514441337A6638463776676C70302F687436574D6E3145705261677A5348780D0A6D6454733673743847466749 6C4B58736D38574C33786F656D54695A6878353777493035337A6864634867483035375A6B2B6935636C48467A714D7755716E790D0A,1
OK

AT+HTTPCFG=0,1,35304277464D74456F6E494C777556412B54376C7067367A2B65784B593843344B5142306E466337714B55456B4848787659505A5039616C346A77716A2B386E0D0A594D50476E38753637474239742B61454D7235502B31676D49674E62314C54562B2F586A6C693577774F51757666777537754A42566341304C6E306B636D6E4C0D0A5237455551494E395A2F5347396A477238586D6B7372557545766D45462F42696279632B45316978564130686D6E4D336F54445062354C6339756E38724E73750D0A4B4E462B416B736A6F4258794F47566B43656F4D626F346246364278794C4F6279617670772F4C5068356150674149796E706C5962364C5641674D424141476A0D0A675A5577675A4977444159445652305442415577417745422F7A416442674E56485134454667515574467 26

B70625065306C4C327564576D6C512F7250727A480D0A2F6638775977595445652306A4246777757
6F41557446726B70625065306C4C327564576D6C512F7250727A482F662B68503651394D4473784
37A414A42674E560D0A42415954416B354D4D5245774477595445651514B4577685162327868636C
4E545444455A4D4263474131554541784D515547397359584A5455307767564756 7A0D0A,1
OK

AT+HTTPCFG=0,1,6443424451594942414441 4E42676B71686B6947397730424151554641414F434
151454175503155324142556B49736C734366646C6332693934514848596 54A0D0A5373523445646
74874646369554935493 6324A364D6F6D2B593064542F37612B3853364D564D435A503643354E79
4E795877314757592F5952383258544A38480D0A44424A6943546F6B3544625A36537A614F4E427
A645748587757776D693576673164786E375978724D396430496A784D3237574E4B7334734451685
A42516B460D0A706A6D6673326362346F506C34593954396D6554782F6C76646B5259457567363
14A666E3663412B7148707950596454482B55736849546E6D70352F5A746B660D0A6D2F5554534
C424E464E48657369545A654833314E637859476448536D65394E632F67666964526130464C4F436
65778526C4671414934377A47396A4151435A0D0A375A326D4347444E4D686A51632B425963646
E6C306C50586A64444B3656307143673164566577685542635735675A4B7A563765392B44705641
3D3D0D0A2D2D2D2D2D454E44204345525449464943415445 2D2D2D2D2D0D0A,1
OK

AT+HTTPSEND=0,0,"/"
OK

+HTTPCON:0,CONNECTED

+HTTPNMIH:0,0,800,Date: Mon, 09 Apr 2018 01:07:13 GMT
Server: Apache/2.4.27 (Win32) OpenSSL/1.0.2l
Last-Modified: Mon, 27 Nov 2017 01:57:39 GMT
ETag: "15c-55eed3a259fdb"
Accept-Ranges: bytes
Content-Length: 348
Content-Type: text/html

+HTTPNMIC:0,0,348,696,3c21646f63747970652068746d6c207075626c696320222d2f2f5733432f2f4
454442048544d4c20342e30205472616e736974696f6e616c2f2f454e223e0d0a3c68746d6c3e0d0a093c
686561643e0d0a09093c7469746c653e2054657374203c2f7469746c653e0d0a093c2f686561643e0d0a0
93c626f64793e0d0a09093c48313e5468697320697320616e206578616d706c6520706167652072 2
074657374696e672e3c2f48313e0d0a09093c48323e5468697320697320616e206578616d706c6520706
1676520666f722074657374696e672e3c2f48323e0d0a09093c48333e5468697320697320616e2065786
16d706c6520706167652066f722074657374696e672e3c2f48333e0d0a0909093c7374726f6e673e5468
69733c2f7374726f6e673e20697320616e206578616d706c6520706167652066f722074657374696e67

2e0d0a093c2f626f64793e090d0a3c2f68746d6c3e

+HTTPERR:0,-2

7 硬件相关指令

7.1 串口波特率

例如：

AT+IPR=9600

OK　　//返回 OK，立即生效

AT+IPR=0

OK　　//自适应波特率

注：自适应波特率功能非实时适应，其触发存在一定条件，且达到条件后，只会触发一次。满足以下三个条件之一，则会触发一次串口波特率的自适应功能：1.AT+IPR=0 返回 OK 后，串口将适应其接收到的第一串口消息作为固定波特率；2.模组从深/浅睡眠唤醒后，串口将适应其接收到的第一串口消息作为固定波特率；3.开机/软重启/硬重启，串口将适应其接收到的第一串口消息作为固定波特率。

7.2 流控功能

1.关闭流控，执行以下命令，立即生效，重启后保留配置

AT+IFC=0,0

AT&K0

2.打开软件流控，执行以下命令，立即生效，重启后保留配置

AT+IFC=1,1

AT&K4

3.打开硬件流控，执行以下命令，立即生效，重启后保留配置

AT+IFC=2,2

AT&K3

低电平有效

7.3 GPIO

仅开放 GPIO0-1，对应 PIN34 及 PIN35 引脚，配置方法参考 AT+GPIO

7.4 ADC

当前仅支持 ADC0
测量范围：0~1399mv
参考 AT+CMADC

7.5 LED 灯配置和指示

LED 状态灯：STATUS/WAKEUP_OUT
STATUS：可用作浅睡眠状态指示、网络状态指示
WAKEUP_OUT：深睡眠状态指示
通过 AT+CMSYSCTRL 来进行使能/配置，为节省功耗，LED 默认关闭。
STATUS 设置为浅睡眠状态：
AT+CMSYSCTRL=0,1
输出高电平（LED 亮）：浅睡眠模式
输出低电平（LED 灭）：唤醒状态

STATUS 设置为网络指示：
AT+CMSYSCTRL=0,2

EPS registration status	Description
unregistered	80ms high/800ms low
registered	80ms high/3000ms low

使能 WAKEUP_OUT
AT+CMSYSCTRL=1,1

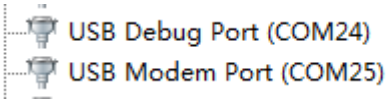
8 Genie Log 使用

Genie Log 分为两个部分：GKI 和 HSL。
GKI：包含 AP <--> Modem 信号值、程序调试输出 LOG、Modem 输出信号、RRC Decode。
HSL：包含 AP、Modem 所有输出信息，仅开放部分消息，可输出 ARFCN/RSRP/SNR 等实时数据。

8.1 连接方式

（1）USB

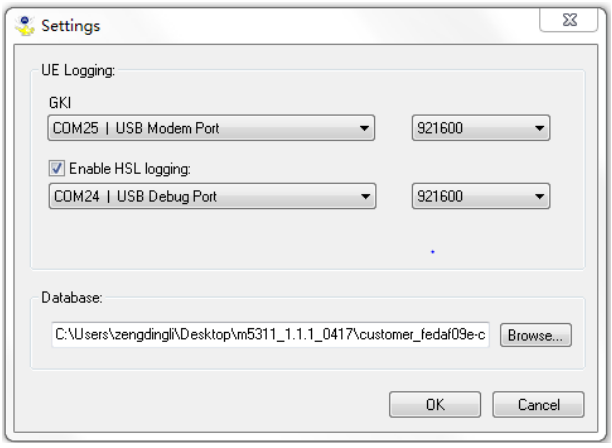
由于 USB 供电会使模组处于唤醒状态，若使用 USB 抓取 LOG，模组无法进入深/浅睡眠，因此，在测低功耗性能时，不能使用 USB 模式抓 LOG，只能通过 uart 抓取。
①安装 USB 驱动后，会虚拟出两个 COM 口，如下：



②配置 USB 作为 LOG 的输出端口，如下：

```
AT+EPORT=1,emmi,4
OK
AT+EPORT=1,uls,5
OK
```

该设置与 USB COM 口对应关系如下：
emmi（GKI）<--> USB Modem Port（COM25）
uls（HSL）<--> USB Debug Port（COM24）
重启模组，设置生效。
③ Genie Log 配置：Config—setting，如下：



波特率：USB 无需设置波特率，值可以随便设置。

Database：固件包中的.dec 文件。

（2）uart0 & uart2

①配置 uart0&uart2 作为 LOG 的输出端口，如下：

```
AT+EPORT=1,emmi,0
OK
AT+EPORT=1,uls,2
OK
```

emmi（GKI）<--> uart0

uls（HSL）<--> uart1

设置 uart0&uart2 波特率：

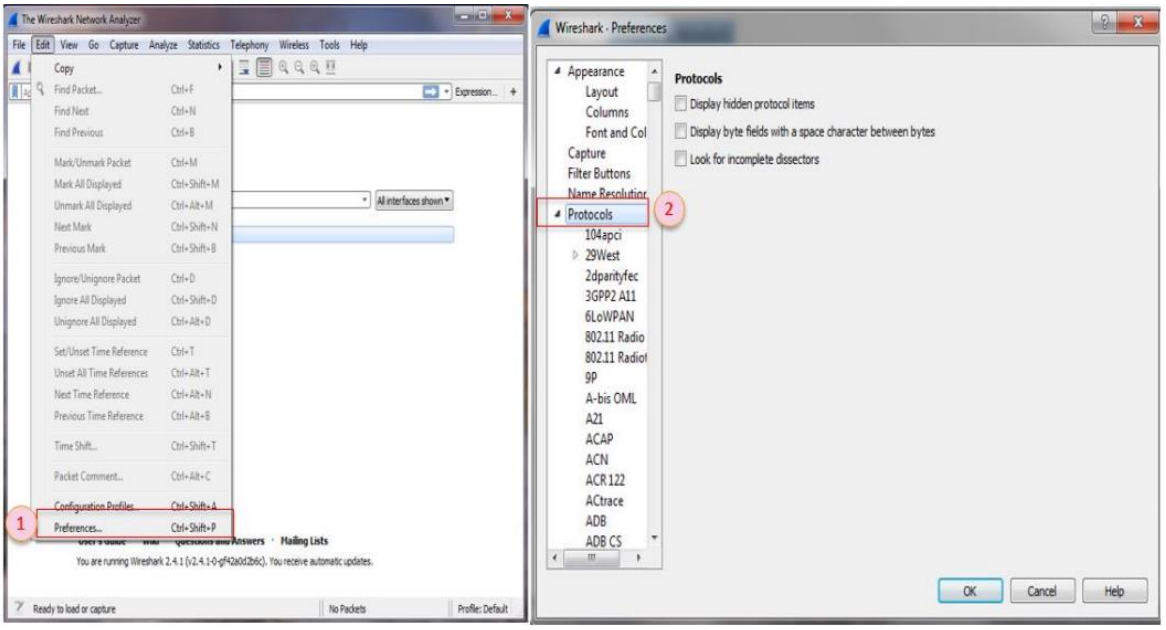
```
AT+EPORT=3,0,115200
OK
AT+EPORT=3,2,115200
OK
```

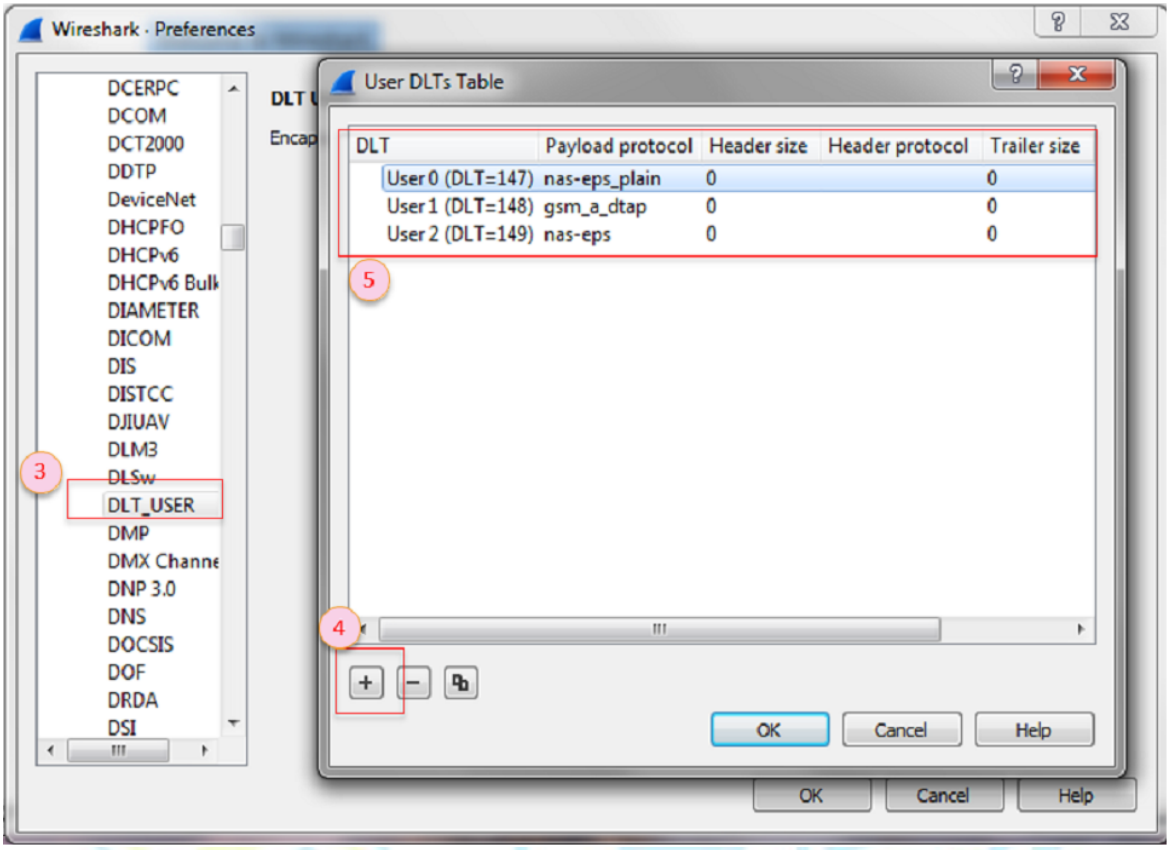
重启模组，设置生效。

②Genie Log 配置：与 USB 模式类似，但波特率必须与 AT+EPORT 所配置的值一致。

8.2 RRC Decoder

RRC Decoder 可以查看到信令流程和消息，NAS 层信令消息需要通过映射到 Wireshark 来获取，参照如下图步骤配置 Wireshark：





运行 genie log，在 RRC Decoder 可以查看到驻网信令流程。

驻网流程如下：

```
718     000:00:01.180  LTE_BCCH_BCH  Mib       EARFCN = 3736, PCI = 192
720     000:00:01.180  LTE_BCCH_SCH  Sib1      EARFCN = 3736, PCI = 192
840     000:00:05.080  LTE_BCCH_SCH  Sibx      EARFCN = 3736, PCI = 192
855     000:00:05.110  UL            LEN:96    Attach request
862     000:00:05.110  LTE_UL_CCCH   SRB0      Rrc_connection_request_r13
884     000:00:05.620  LTE_DL_CCCH   SRB0      Rrc_connection_setup_r13
891     000:00:05.620  LTE_UL_DCCH   SRB1bis   Rrc_connection_setup_complete_r13
910     000:00:05.750  LTE_DL_DCCH   SRB1bis   Dl_information_transfer_r13
912     000:00:05.750  DL            LEN:36    Authentication request
920     000:00:05.950  UL            LEN:11    Authentication response
925     000:00:05.950  LTE_UL_DCCH   SRB1bis   Ul_information_transfer_r13
936     000:00:06.290  LTE_DL_DCCH   SRB1bis   Dl_information_transfer_r13
938     000:00:06.290  DL            LEN:8     Security mode command
941     000:00:06.300  UL            LEN:13    Security mode complete
946     000:00:06.310  LTE_UL_DCCH   SRB1bis   Ul_information_transfer_r13
968     000:00:07.510  LTE_DL_DCCH   SRB1bis   Dl_information_transfer_r13
970     000:00:07.510  DL            LEN:82    Attach accept
984     000:00:07.550  UL            LEN:7     Attach complete
989     000:00:07.550  LTE_UL_DCCH   SRB1bis   Ul_information_transfer_r13
1067    000:00:08.210  LTE_DL_DCCH   SRB1bis   Dl_information_transfer_r13
1069    000:00:08.210  DL            LEN:21    EMM information
1639    000:00:28.630  LTE_DL_DCCH   SRB1bis   Rrc_connection_release_r13
```

Attach accept 消息如下：

```
DLT: 147, Payload: nas-eps_plain (Non-Access-Stratum (NAS)PDU)
Non-Access-Stratum (NAS)PDU
    0000 .... = Security header type: Plain NAS message, not security protected (0)
    .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
    NAS EPS Mobility Management Message Type: Attach accept (0x42)
    0000 .... = Spare half octet: 0
    .... 0... = Spare bit(s): 0x00
    .... .001 = Attach result: EPS only (1)
    GPRS Timer - T3412 value
        GPRS Timer: 2 min
            001. .... = Unit: value is incremented in multiples of 1 minute (1)
            ...0 0010 = Timer value: 2
    Tracking area identity list - TAI list
        Length: 6
        0... .... = Spare bit(s): 0x00
        .00. .... = Type of list: list of TACs belonging to one PLMN, with non-consecutive TAC values (0)
        ...0 0000 = Number of elements: 0 [+1 = 1 element(s)]
        Mobile Country Code (MCC): China (460)
        Mobile Network Code (MNC): China Mobile (00)
        Tracking area code(TAC): 10794
    ESM message container
        Length: 46
        ESM message container contents: 5201c101091905636d696f74066d6e63303034066d636334...
            0101 .... = EPS bearer identity: EPS bearer identity value 5 (5)
            .... 0010 = Protocol discriminator: EPS session management messages (0x2)
            Procedure transaction identity: 1
            NAS EPS session management messages: Activate default EPS bearer context request (0xc1)
            EPS quality of service
                Length: 1
                Quality of Service Class Identifier (QCI): QCI 9 (9)
            Access Point Name
                Length: 25
                APN: cmiot.mnc004.mcc460.gprs
            PDN address
                Length: 5
                0000 0... = Spare bit(s): 0x00
                PDN type: IPv4 (1)
                PDN IPv4: 100.110.177.97
            APN aggregate maximum bit rate
                Element ID: 0x5e
                Length: 4
                APN-AMBR for downlink: 8640 kbps
                APN-AMBR for uplink: 8640 kbps
                APN-AMBR for downlink (extended): 100 Mbps
                Total APN-AMBR for downlink: 100.000 Mbps
                APN-AMBR for uplink (extended): 100 Mbps
                Total APN-AMBR for uplink: 100.000 Mbps
            ESM cause
                Element ID: 0x58
                Cause: PDN type IPv4 only allowed (50)
            Control plane only indication
                1001 .... = Element ID: 0x9-
                .... 000. = Spare bit(s): 0x00
                .... ...1 = CPOI: PDN connection can be used for control plane CIoT EPS optimization only
    EPS mobile identity - GUTI
        Element ID: 0x50
        Length: 11
        .... 0... = Odd/even indication: Even number of identity digits
        .... .110 = Type of identity: GUTI (6)
        Mobile Country Code (MCC): China (460)
        Mobile Network Code (MNC): China Mobile (00)
        MME Group ID: 929
        MME Code: 110
        M-TMSI: 0xc8ee8783
    EPS network feature support
        Element ID: 0x64
        Length: 1
        1... .... = Control plane CIoT EPS optimization: Supported
```