中国移动
China Mobile

M5311
软件用户手册

NB-IoT 系列

版本：V2.3

日期：2020 年 9 月

中移物联网有限公司
One MO iot.10086.cn

服务与支持

如果您有任何关于模组产品及产品手册的评论、疑问、想法，或者任何无法从本手册中找到答案的疑问，请通过以下方式联系我们。

中移物联网有限公司

OneMO 官网：onemo10086.com

邮箱：SmartModule@cmiot.chinamobile.com

客户服务热线：400-110-0866

微信公众号：CMOneMO

文档声明

注意

本手册描述的产品及其附件特性和功能，取决于当地网络设计或网络性能，同时也取决于用户预先安装的各种软件。由于当地网络运营商、ISP，或当地网络设置等原因，可能也会造成本手册中描述的全部或部分产品及其附件特性和功能未包含在您的购买或使用范围之内。

责任限制

除非合同另有约定，中移物联网有限公司对本文档内容不做任何明示或暗示的声明或保证，并且不对特定目的适销性及适用性或者任何间接的、特殊的或连带的损失承担任何责任。

在适用法律允许的范围内，在任何情况下，中移物联网有限公司均不对用户因使用本手册内容和本手册中描述的产品而引起的任何特殊的、间接的、附带的或后果性的损坏、利润损失、数据丢失、声誉和预期的节省而负责。

因使用本手册中所述的产品而引起的中移物联网有限公司对用户的最大赔偿（除在涉及人身伤害的情况中根据适用法律规定的损害赔偿外），不应超过用户为购买此产品而支付的金额。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。公司保留随时修改本手册中任何信息的权利，无需进行提前通知且不承担任何责任。

商标声明

中国移动 China Mobile为中国移动有限公司注册商标。

本手册和本手册描述的产品中出现的其他商标、产品名称、服务名称和公司名称，均为其各自所有者的财产。

进出口法规

出口、转口或进口本手册中描述的产品（包括但不限于产品软件和技术数据），用户应遵守相关进出口法律和法规。

隐私保护

关于我们如何保护用户的个人信息等隐私情况，请查看相关隐私政策。

操作系统更新声明

操作系统仅支持官方升级；如用户自己刷非官方系统，导致安全风险和损失由用户负责。

固件包完整性风险声明

固件仅支持官方升级；如用户自己刷非官方固件，导致安全风险和损失由用户负责。

版权所有©中移物联网有限公司。保留一切权利。

关于文档

修订记录

版本	日期	作者	描述
V1.0	2018.4.12	曾定立	首次创建
V1.1	2018.5.16	曾定立	增加睡眠状态指示说明
V1.2	2018.6.1	孟桃	HTTP 协议 AT 指令变更
V1.3	2018.12.11	曾定立	– 睡眠模式变更、TLS 变更、新增 NB 网络配置、清除驻网记录、硬件相关指令、Genie Log 使用、HTTP 相关指令变更、RAI 设置； – 删除 MQTT/HTTP 指令集； – 更改 LOG 抓取方式。
V1.4	2018.12.29	曾定立	– 增加 M5311-LV 及 M5311-CM 相关差异说明； – 增加短信流程说明； – 更改文档名称《M5311 通信示例流程》为《M5311 软件用户手册》。
V1.5	2019.2.22	曾定立	增加 CCLK\CMNTP 时间同步指令说明
V1.6	2019.6.18	曾定立	– 更改 3.4 清除驻网记录说明； – 增加 6.6 节 UDP/TCP 休眠策略； – 变更 9.1 节串口波特率自适应模式说明； – 变更第 10 章 Genie log 使用。
V1.7	2019.7.19	曾定立	变更第 6 章，创建 TCP/UDP Socket 成功判断条件，发送数据说明。
V1.8	2019.8.13	曾定立	– 增加 8.1 节中 TCP RAI 使用注意说明； – 增加 8.2 节 快速释放 RRC 连接指令。
V1.9	2019.9.9	曾定立	增加 M5311-DB、M5311-CL 版本说明。
V2.0	2020.2.24	曾定立	– 增加第 10 章 DNS 业务介绍； – 增加第 11 章 IPv6 业务介绍； – 增加 AT+CMNTP 执行命令说明； – 增加 M5311-GB 版本说明。
V2.1	2020.6.17	曾定立	增加 1.2.1、1.2.2 版本说明章节。
V2.2	2020.7.6	曾定立	– 变更 AT+IPR=0 自适应波特率生效条件； – 增加 UDP 下行数据长度说明； – 增加接收 TLS 数据长度、编码说明。
V2.3	2020.9.17	曾定立	增加 3.2.2 节 PDN 异常断开处理流程

文档中涉及的相关指令参数意义详见中移物联网有限公司 *M5311 AT Command Interface Specification* 文档。

目录

1 综述

1.1 文档目的

本文档主要介绍了 M5311 模块的软件相关特性，适用于 M5311-LV、M5311-CM、M5311-DB、M5311-CL 及 M5311-GB 版本，包括模块的 AT 流程、业务流程、接口配置等。

1.2 版本说明

1.2.1 模组子型号版本说明

M5311-LV、M5311-CM、M5311-DB 及 M5311-CL 软件版本的差异见下表。

功 能	M5311-LV	M5311-CM	M5311-DB	M5311-CL	M5311-GB
频 段	BAND 3、BAND 5、BAND 8	BAND 8	BAND 5、BAND 8	BAND 8	BAND 1、BAND 3、BAND 5、BAND 8、BAND 20、BAND 28
BAND 配置	AT*CMBAND 配置或锁定 BAND	不可配置	AT*CMBAND 配置或锁定 BAND	不可配置	AT*CMBAND 配置或锁定 BAND
电信 IoT 平台	支持	不支持	支持	不支持	支持

1.2.2 软件版本说明

M5311 固件版本号可通过 AT+CGMR 指令进行查询，例如：M5311-MLVH1S04，M5311 代表模组型号，M 代表量产版本，LV 代表 M5311-LV 子型号，S04 代表当前软件版本号。

- 本文档 M5311-LV、M5311-CM、M5311-DB、M5311-CL 及 M5311-GB 各个版本间差异性，以[*]标注说明；
- 软件版本仅支持升级，不支持回退，版本回退可能会造成未知风险，切勿使用下载工具或 FOTA 对模组当前版本进行回退。例如：S04 回退到 S03，可能会存在未知风险；
- 各子型号的固件必须同模组子型号硬件匹配，若固件版本与子型号硬件不匹配，可能会造成无法驻网等问题。例如：M5311-MLVH1S04 的固件版本下载到 M5311-CM 硬件后，可能会导致 M5311-CM 无法驻网。

1.3 手册说明

本文档介绍了 M5311 模块的睡眠模式、驻网流程及 NB 网络配置、UDP/TCP 数据收发、TLS 数据收发、RAI 设置、硬件相关设置、log 工具使用。

OneNET/MQTT/HTTP 协议指令及 DM 功能参见相关说明文档，AT 指令详细说明参见 *M5311_AT_Command_Interface_Specification*。

2 睡眠模式

M5311 包括两种睡眠模式：深度睡眠和浅睡眠。

- **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。

2.1 深度睡眠

2.1.1 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，会进入深度睡眠模式：

- 在飞行模式（AT+CFUN=0）下，模组在 10s 后进入深度睡眠；
- 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；
- 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；
- 在插入 SIM 卡前提下，模组搜索完全频段，尝试驻网失败（AT+CEREG?返回+CEREG: 0,0）后，进入深度睡眠模式；若不插 SIM 卡，AT+CEREG?返回+CEREG: 0,0 模组不会进入深睡眠模式。

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。

2.1.2 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，唤醒模组后，可保持唤醒状态的默认时间长为 10s（可通过 AT*WAKETIME 指令配置唤醒时长），期间发送 AT 有响应：

- WAKEUP_IN 由高电平拉至低电平，并保持低电平一定时间，低电平持续时间参见《M5311 硬件设计手册》，WAKEUP_IN 禁止长时间拉低。

2.2 浅睡眠

2.2.1 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，会进入到浅睡眠模式：

- 进入空闲态后，模组立即进入浅睡眠模式；
- 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；
- 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；
- 若不插 SIM 卡，AT+CEREG?返回+CEREG: 0,0，模组只会进入浅睡眠，而不会进入深睡眠；
- 若 TCP 连接未关闭情况下，因信号丢失而导致驻网失败，模组会进入浅睡眠，而不会进入深睡眠。

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。

2.2.2 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：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
```

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。

（2） WAKEUP_IN 由高电平拉至低电平，并保持低电平一定时间，低电平持续时间参见《M5311 硬件设计手册》(可通过 AT*WAKETIME 指令配置唤醒时长)，WAKEUP_IN 禁止长时间拉低。

2.3 开关睡眠

2.3.1 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
```

2.3.2 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
```

2.4 睡眠状态指示

2.4.1 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。

- **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

- **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。
```

2.4.2 浅睡眠唤醒状态指示

判断模组是否处于浅睡眠只能通过 STATE 输出电平进行判断，暂无 URC 上报功能。STATE 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 STATE 引脚，并设置为浅睡眠指示功能。
OK
```

STATE 输入电平与浅睡眠状态对应关系如下：

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

2.5 睡眠相关设置

■ 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。例如：

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

- AT*WAKETIME 指令配置的唤醒时长，仅对 WAKEUP_IN 下降沿唤醒深/浅睡眠的情况生效，对于输入 AT 指令持续唤醒的 10s 是固定值，该指令对此不生效；
- 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。

■ 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 2.1.1 及 2.2.1 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。
```

3 驻网流程及 NB 网络配置

3.1 驻网流程

每个 AT 命令之间应该留有一定时间间隔，建议间隔大于 500ms。

（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: 1,1                          //自动上报的网络注册信息，+CEREG: <n>,<stat>，附着状态——
                                     <stat> 1-本地网络已注册入网，5-漫游已注册，6、7-注册网络仅支持
                                     短信，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: <cid>,<state> PDP 连接状态——< state > 1-cid 对应定义的
+CGACT: 1,1                          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?                          //查询当前 APN，此步骤可省略。
+CGDCONT: 1,"IP","cmiot","",0,0,0,,,,,,0,,0
OK
AT+CGPADDR=1                         //查询 PDP 地址，此步骤可省略。
+CGPADDR: 1,"10.64.118.25"
```

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约为 10s-180s。

3.2 NB 网络配置

3.2.1 PDN 激活方法

（1） **自动激活 PDN**

默认在驻网时自动激活默认 PDN/PDP context，开机驻网成功后将返回默认 PDN 的 IP 地址，例如：+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=<cid>,1 方式激活 PDN ）

（3） **PDN 去激活**

– 只有一条 PDN 连接

在只有一条 PDN 连接的情况，使用去附着或关闭协议栈命令请求断开网络及 PDN 去激活：

AT+CGATT=0

AT+CFUN=0

– 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。

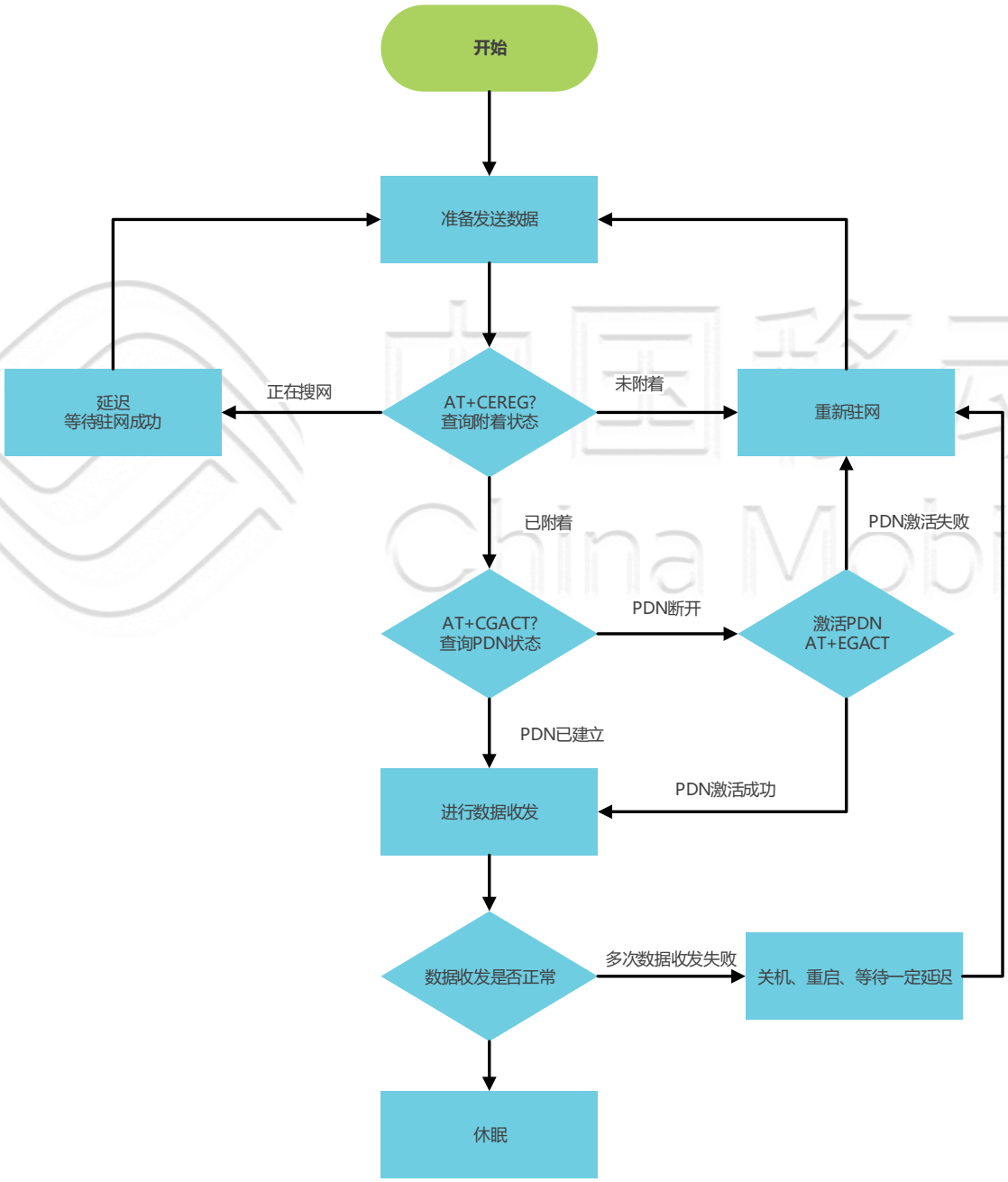
AT+EGACT=0,<cid> //去激活<cid>对应的 PDP，仅适用于 AT+EGACT 方式激活的方式，对于驻网默认自动激活的 PDN，此方法不适用。

3.2.2 PDN 异常断开处理流程

M5311 在默认配置下，开机会自动驻网，并自动激活 PDN，例如当串口输出+IP: 10.132.37.162 时，证明 PDN 已连接。

当网络发生 PDN 被隐式释放时，M5311 可自动完成重新附着、重建 PDN。但由于网络侧的原因导致 PDN 断开，例如：核心网和基站携带的 attachwithoutPDN 标志位不一致等原因造成 PDN 断开，M5311 不会自动重建 PDN，建议对网络 PDN 异常断开的情况进行判断并处理。

以下流程是对于网络、PDN 状态判断处理的例子，当网络发生 PDN 异常断开时，可通过 AT+CEREG? 和 AT+CGACT?来查询当前网络状态，若 PDN 异常断开，可通过 AT+EGACT 或重新驻网的方式来恢复网络。以下流程示例是进行网络数据业务的处理流程，仅供参考：



以下是以 AT+CEREG=0、仅激活一路 PDN 的默认状态下为示例的 PDN 状态判断 AT 指令流程：

（1） **通过 AT+EGACT 激活 PDN**

AT+CEREG?	//查询网络附着状态。
+CEREG: 0,1	//+CEREG: <n>,<stat>，<stat>为 1 表示已注册入网，5 表示漫游已注册，6、7 表示注册网络仅支持短信，其它情况为注册异常，详细请参考 AT 命令手册。
OK	
AT+CGACT?	//查询 PDP 上下文是否已激活。
+CGACT: 1,0	// +CGACT: <cid>,<state>，<cid>为 PDP 上下文标号，<state>为 PDP 上下文激活状态，0 表示未激活，1 表示已激活。PDN 已断开，需要重新驻网或重建 PDN。
OK	
AT+EGACT=1,1,"","",""	//激活 PDN，EGACT 参数请参考 AT 指令手册，此示例<apn>配置为空，可能在部分区域网络需要输入正确的 APN，若无法得知 APN 建议直接对模组进行重新驻网。
+EGACT:1	
OK	
+IP: 10.2.174.59	//串口返回+IP: 10.2.174.59 和+EGACT:1,1,1,1 代表 PDN 激活成功。
+EGACT:1,1,1,1	

（2） **通过重新驻网的方式恢复 PDN**

AT+CEREG?	//查询网络附着状态。
+CEREG: 0,1	//<stat>为 1 表示已注册入网。
OK	
AT+CGACT?	//查询 PDP 上下文是否已激活。
+CGACT: 1,0	//<state>为 0 表示未激活，PDN 已断开，需要重新驻网或重建 PDN。
OK	
AT+COLDRB	//重启模组，重新进行驻网，此外，还可以通过 AT+CGATT=0/ AT+CFUN=0 返回 OK 后，再执行 AT+CGATT=1/ AT+CFUN=1 来重新驻网。
OK	
COLD REBOOTING..	
*ATREADY: 1	
+CFUN: 1	
+CPIN: READY	
+IP: 10.36.148.31	//已完成驻网，并激活 PDN。

- M5311 禁止使用 AT+CGACT=<cid>,1 激活 PDN，若执行了 AT+CGACT=<cid>,1，AT+CGACT?判断结果将受到影响；
- 本章节所提供的示例流程仅供参考，请根据实际具体应用进行调整；
- 模组重启方式可根据具体需求，通过拉低 RESET 管脚实现硬件复位、通过 AT+COLDRB 实现冷重启、通过 AT+CMRB 实现软重启，本文 AT 流程中重启方式仅供参考，请根据实际具体应用选择重启方式。

3.2.3 PSM/eDRX 模式配置与查询[*]

（3） **PSM/eDRX 设置**

– PSM 设置

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

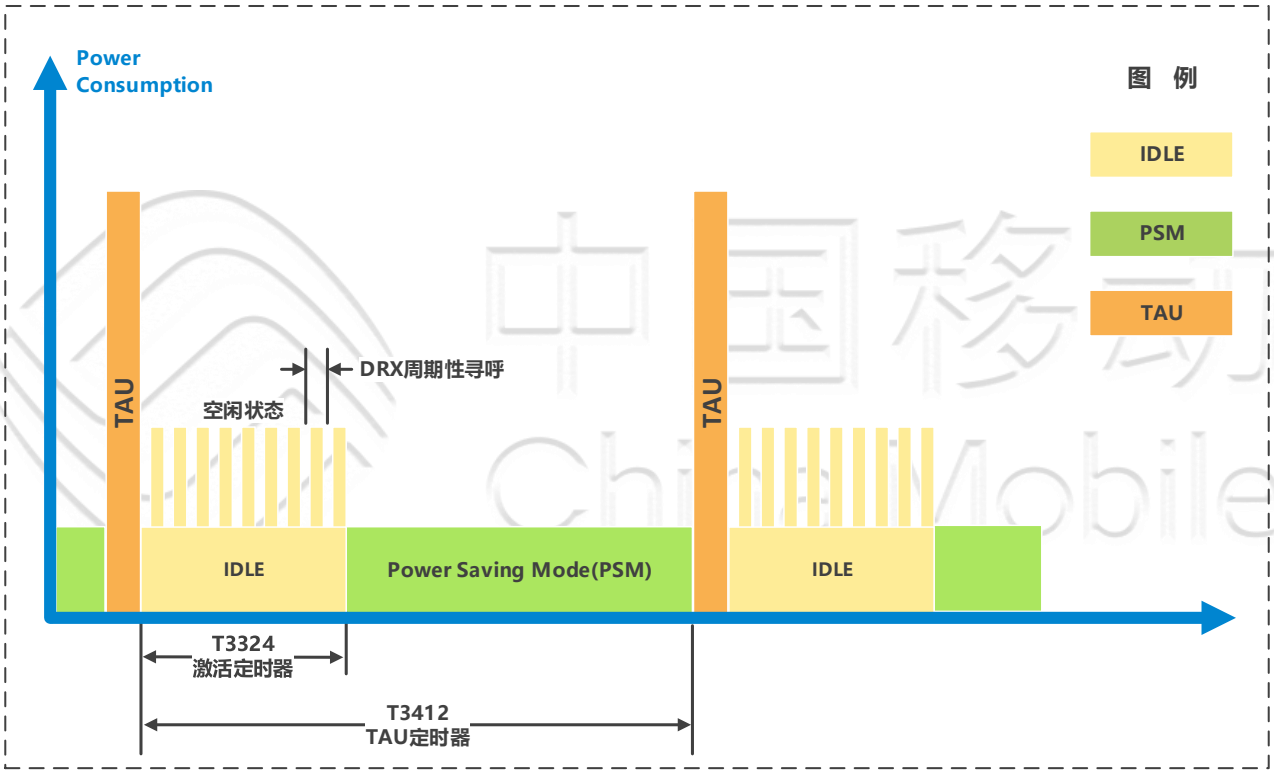
– eDRX 设置

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

– eDRX PTW 设置

AT*EDRXCFG=1,5,"0011","0001" //设置 eDRX 寻呼周期为 40.96，时间窗(PTW)为 5.12s。

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



（4） **PSM/eDRX Accept 查询**

– PSM 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 和扩展周期性计时器 TAU 值（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。

– eDRX Accept 查询

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

– M5311-LV 版本：M5311-MLVH0S01 及之前版本不支持 AT*EDRXCFG, M5311-MLVH1S02 及之后版本支持该功能；
– M5311-CM 版本：M5311-MCMH0S01 及之后版本支持 AT*EDRXCFG；
– M5311-DB、M5311-CL 及 M5311-GB 版本：均支持 AT*EDRXCFG。

3.3 锁定 BAND/EARFCN

3.3.1 锁 BAND[*]

（1） **M5311 支持的 BAND**

M5311-LV 版本支持的 BAND：3,5,8
M5311-CM\M5311-CL 版本支持的 BAND：8
M5311-DB 版本支持的 BAND：5,8
M5311-GB 版本支持的 BAND：1,3,5,8,20,28

（2） **锁定 BAND**

通过 AT*CMBAND 来进行设置，重启后设置生效。例如：

```
AT*CMBAND=8                 //锁定 BAND 为 B8。
AT+CMRB                     //重启生效。
AT*CMBAND?
*MBAND: 8                   //当前所支持的 BAND 为 B8。
OK
AT*CMBAND=0                 //恢复默认值：LV 版本为 B 3,5,8，DB 版本为 B 5,8。
AT*CMBAND?
*CMBAND: 3,5,8
OK
```

（3） **M5311 搜网顺序及配置**

- M5311-LV\M5311-DB 版本搜网规则；
  根据 SIM 卡识别国内运营商信息来优先搜索 BAND 的顺序，例如：识别到移动卡，则优先搜索 B8 然后是 B3,B5。
- M5311-CM\M5311-CL 版本搜网规则；
  只搜索 B8。
- M5311-GB 版本搜网规则；
  默认配置下，将按照 BAND 从小到大的优先顺序搜索，例如：优先搜 B1，然后是 B3、B5、B8、B20、B28。
  M5311-GB 版本可通过 AT+BANDPL 指令来配置搜网优先顺序，例如：

```
AT*CMBAND=1,3,8,28          //锁定 BAND 为 B1,3,8,28。
AT+BANDPL=8,3,28,1          //配置 BAND 优先顺序为 B8、B3、B28、B1。
AT*CMBAND=0                 //BAND 锁定恢复默认值，支持的 BAND 有：B1、B3、B5、B8、
                            B20、B28。
AT+BANDPL=8,3,28            //由于 BAND 未锁定，BANDPL 未配置的 BADN 将按照从小到大顺序
                            搜索，因此搜网优先顺序为：B8、B3、B28、B1、B5、B20。
```

- M5311-CM\M5311-CL 版本仅支持 B 8，AT*CMBAND 命令仅可查询当前模组所支持的 BAND，不支持锁 BAND 命令；
- AT+BANDPL 仅支持 M5311-GB 版本，M5311-LV\M5311-DB 版本将按照国内运营商自动选择 BAND 优先顺序，M5311-CM\M5311-CL 版本仅支持 B8；
- M5311 搜网顺序详细说明请参考《M5311_搜网过程说明》文档。

3.3.2 锁 EARFCN/Cell

例如：

AT*FRCLLCK=1,3736,2　　//锁定频点至 EARFCN 3736。
AT*FRCLLCK=1,3736,2,192　　//锁定频点至 EARFCN 3736, PCI 192。

设置后立即生效，掉电不保存。

3.4 清除驻网(PLMN, EARFCN, PCI)记录

模组在驻网成功，再去附着（AT+CFUN=0/AT+CGATT=0）成功后，便会保存该驻网记录，包括 PLMN、EARFCN、PCI 等，当模组发生再次驻网时，会优先向已记录的小区发送附着请求，若该小区无法附着或附着失败，模组才会搜索其余小区。

- 在驻网成功后，执行 AT+CFUN=0 去附着，模组会保存该驻网记录，且 AT+CFUN=1/AT+CFUN=0 切换附着和去附着流程，每次均会保存保存驻网记录；
- 在驻网成功后，执行 AT+CGATT=0 去附着，模组会保存该驻网记录，但仅首次能够生效，第二次执行 AT+CGATT=1/AT+CGATT=0 切换附着与去附着流程，将不再保存驻留频点信息等；
- 若驻网成功后，直接 RESET，模组不会保留该小区记录。

执行 AT+CLPLMN 命令可清除模组的驻网记录，例如：

```
AT+CLPLMN                    //清除驻网记录。
+CLPLMN: 0                   //返回 0，说明已成功清除记录。
OK
```

4 短信流程

模组驻网成功后，进行以下短信流程。例如：

（1） **中心号码设置**

```
AT+CSCA="13800200569"          //设置当地短信中心号码。
OK
AT+CSCA?                       //查询短信中心号码配置。
+CSCA: "8613800200569",129
OK
```

（2） **文本模式短信收发**

```
AT+CMGF=1                      //设置文本模式。
OK
AT+CMGS="1064899990000"        //发送短信到 MT 号码"1064899990000"。
> test
+CMGS: 56
OK
+CMTI: "SM",10                 //接收到一条新短消息。
AT+CMGL="REC UNREAD"           //列出未读短信成功，即收到的短信。
+CMGL: 10,"REC UNREAD","1064899990000",,"18/10/23,16:24:21+32"
60A8597DFF0C6D4B8BD577ED4FE15DF265365230FF0C56DE590D60A84E006761FF01FF01
```

（3） **PDU 模式短信收发**

```
AT+CMGF=0                      //设置 PDU 模式。
OK
AT+CMGS=19                     //PDU 模式发送短信。
> 0015660D91014698990900F00008FF044F60597D
+CMGS: 20
OK
+CMTI: "SM",11                 //接收到一条新短消息。
AT+CMGL=1                      //列出未读短信成功，即收到的短信。
+CMGL: 11,1,,56
0891683108200065F9240DA0014698990900F000088101421151952324 60A8597DFF0C6D4B8BD577ED4FE15D
F265365230FF0C56DE590D60A84E006761FF01FF01
OK
```

5 网络时间同步

M5311 支持两种方式同步网络时间：① 开机驻网成功后，自动获取网络时间，且同步到模组本地时间，通过 AT+CCLK?获取同步时间；② 通过 AT+CMNTP 指令，向指定 NTP 服务器发起 NTP 服务获取网络时间。

5.1 驻网自动同步网络时间

开机驻网成功后，模组会同步网络时间到本地时间，更新 AT+CCLK?返回结果。

AT+CCLK?

+CCLK: <time>

<time>格式为"yy/MM/dd,hh:mm:ss ± zz"，"yy/MM/dd,hh:mm:ss"表示 UTC 时间，" ± zz"表示 1/4 小时时间差，例如：北京时间 2019/2/22 14:19:15 等同于 2019/2/22 06:19:15 GMT+8 等同于 19/02/22,06:19:15+32。

例如：

```
*ATREADY: 1
+CFUN: 1
+CPIN: READY                    //开机，开始搜索网络。
AT+CCLK?
+CCLK: 00/01/01,00:00:02+32     //未附着上网络，CCLK 返回系统默认时间。
OK
+IP: 10.162.70.92               //驻网成功。
AT+CCLK?
+CCLK: 19/02/22,06:19:15+32     //同步到网络时间。
OK
```

5.2 AT+CMNTP 同步网络时间

AT+CMNTP=<server>[,<port>,[<set_rtc>,[<timeout>]]]

通过向指定服务器请求获取网络时间，<server>,<port>为服务器地址和端口号，端口号默认为 123；<set_rtc>为获取服务器网络时间后是否更新本地时钟，默认为更新；<timeout>为指令请求的最大超时时间。

例如：

```
AT+CMNTP                                  //向 cn.ntp.org.cn 服务器请求网络时间，且不更新本地时钟。
OK
+CMNTP: 0,"19/02/22,06:38:23+32"          //获取到网络时间，"19/02/22,06:38:23+32"时间格式与 AT+CCLK 指令的
                                          <time>参数格式一致。
AT+CCLK?                                  //由于 AT+CMNTP 未同步本地时钟，因此 AT+CCLK?与 AT+CMNTP
+CCLK: 19/02/22,06:37:53+32               返回结果存在一定误差。
OK
AT+CMNTP="cn.ntp.org.cn",,1,30            //向 cn.ntp.org.cn 服务器请求网络时间，且更新本地时钟。
OK
+CMNTP: 0,"19/02/22,06:50:15+32"
OK
AT+CCLK?                                  //本地时间已同步更新到 NTP 网络时间。
+CCLK: 19/02/22,06:50:16+32
OK
```

AT+CMNTP 指令需等待自动上报结果(+CMNTP: <err>[,<time>])返回后才能输入下一条 AT+CMNTP 指令，否则将返回 ERROR。

例如：

```
AT+CMNTP="cn.ntp.org.cn"
OK
AT+CMNTP="cn.ntp.org.cn"                  //上一条 CMNTP 指令未返回+CMNTP:<err>[,<time>]，再次输入
+CME ERROR: operation not allowed         CMNTP 指令将报错。
+CMNTP: 2                                 //返回第一条 CMNTP 指令自动上报结果，为请求超时。
AT+CMNTP="cn.ntp.org.cn"                  //由于上一条 CMNTP 指令已返回结果码，此时再次请求 AT+CMNTP
OK                                        指令将返回 OK。
+CMNTP: 0,"19/02/22,06:59:53+32
```

6 UDP/TCP 数据收发

6.1 创建 UDP/TCP Socket

6.1.1 创建 UDP Socket

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

由于 S03 及以后版本 AT+IPSTART 由同步阻塞方式变更为异步方式。需在创建后确认 Socket 状态。

（1）以 IP 方式创建 UDP

以 IP 方式创建 UDP，UDP Socket 创建较快，在 AT+IPSTART 返回 OK 后，可间隔 500ms 发送 AT+IPSTATUS=0 查询 UDP 状态，若为 CONNECTED 表示创建成功。

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
AT+IPSTATUS=0
+IPSTATUS:                                       //UDP Socket 创建成功。
0,"UDP","106.12.79.254",36000,"CONNECTED"
OK
```

（2）以域名方式创建 UDP

以域名方式创建 UDP，在 AT+IPSTART 返回 OK 后，由于后台任务需完成 DNS 解析，因此需间隔一定时间，发送 AT+IPSTATUS=0 查询 UDP 状态，若为 CONNECTED 表示创建成功。

例如：

```
AT+IPSTART=0,"UDP","www.iottest.work",36000      //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
AT+IPSTATUS=0                                    //间隔一定时间，例如 10-30s。
+IPSTATUS:                                       //UDP Socket 创建成功。
0,"UDP","106.12.79.254",36000,"CONNECTED"
OK
```

6.1.2 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。
OK	//Socket 编号范围为 0-4。
CONNECT OK	//TCP Socket 创建和连接成功。
AT+IPSTATUS=0	//确认 TCP Socket 创建和连接成功。
+IPSTATUS:0,"TCP","47.93.217.230",2008,"CONNECTED"	
OK	

6.2 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。
```

该步骤可省略，系统分配随机端口。

6.3 发送 UDP/TCP 数据

发送 UDP 数据：

AT+IPSEND=<socket_id>,[<data_len>],<data>[,<addr>,<port>[,<pri_flag>]]

- 若<addr>,<port>省略(其中一项或两项参数缺省)，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；
- string 格式发送数据，<data>的长度范围为：1-1440 Byte；hex 格式发送数据，<data>的长度范围为：1-720 Byte。

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	

- 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；
- S03 以前的版本 AT+IPSTART 采用域名的方式创建 Socket，由于解析 DNS，会在 AT+IPSTART 阻塞住，返回 OK 以后，Socket 创建成功，调用 AT+IPSEND 发送 UDP 数据，TCP 需等到 CONNECT OK 以后，调用 AT+IPSEND 发送 TCP 数据，否则 AT+IPSEND 返回 ERROR；
- S03 及以后的版本，域名的方式创建 Socket，不会发生阻塞，后台任务解析 DNS，UDP 需通过 AT+IPSTATUS 确认 UDP 状态为 CONNECTED，才能调用 AT+IPSEND 发送 UDP 数据，TCP 需等到 CONNECT OK 以后，才能调用 AT+IPSEND 发送 TCP 数据，否则 AT+IPSEND 返回 ERROR。

6.4 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**

在接收到+IPNMI:上报后，通过 AT+IPRD 指令读出数据。TCP Socket 可通过<data_length>参数读出指定长度数据，而对于 UDP Socket，<data_length>参数无效，将读出接收的整包数据。

AT+IPRD=<socket_id>,<data_length>

```
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。
OK
+IPRD: 0,15,hello, CMCC IOT
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。
OK
hello, CMCC IOT
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。
OK
+IPRD: 0,"47.93.217.230",2008,15,68656C6C6F2C20434D434320494F54
```

- 在手动及自动接收模式下，模组能够接收的数据长度范围是 1-1440Byte，例如：自动输出接收数据模式下，模组所能输出的数据的长度范围在 1-1440Byte，手动接收模式下，AT+IPRD 指令中<data_length>长度限制为 1-1440Byte；
- 本示例的测试服务器为中移物联网公司内部测试服务器。

6.5 关闭 UDP/TCP

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

6.6 UDP/TCP 休眠策略

6.6.1 UDP 休眠策略

创建 UDP Socket 以后，模组能够进入深\浅睡眠，模组由深睡眠或 PSM 唤醒后，无需重新创建 UDP Socket，可直接收发数据。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。
*gotosleep                                  //进入深度睡眠。
*MATWAKEUP                                  //深度睡眠被唤醒。
AT+IPSEND=0,0,"1233"                        //深度睡眠唤醒后，可直接发送 UDP 数据。
+IPSEND: 0,2
OK
```

6.6.2 TCP 休眠策略

TCP 连接建立之后，在 TCP Socket 主动或被动关闭前，模组禁止进入深度睡眠，需关闭 TCP 以后才能进入深睡眠。

7 TLS 数据收发

7.1 TLS 参数设置

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

7.1.1 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 8、9 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 8、9 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 8、9 个参数（4,1），1 代表必须服务器可选。
OK
//TLS 参数配置成功。
```

7.1.2 证书配置

（1） **仅加密传输，不认证合法性**

7.1.1 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**

– 仅认证服务器合法性；

仅认证服务器证书是否合法，可选 7.1.1 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/LPh5aPgAlynplYb6LVAgMBAAGj\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
DBJiCTok5DbZ6SzaONBzdWHXwWwmi5vg1dxn7YxrM9d0ljxM27WNKs4sDQhZBQkF\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。
```

– 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 7.1.1 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 7.1.1 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
```

7.2 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。
```

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 4.5.2 节。

7.3 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。
```

7.4 接收 TLS 数据

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

例如：

```
//TLS 默认是手动接收模式，在接收到+TLSNMI 提示后，需发送 AT+TLSRECV 读出所接收的数据。
+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\t<strong>This</strong> 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。
AT+TLSRMOD=1,1,30,802,512,1000                  //设置接收模式为自动接收, HEX 编码, 接收超时参数为 30s（防止接
                                                  收大包超时而导致接收失败），自动接收每包最大为 512Byte，接
                                                  收串口输出间隔为 1000ms。
OK
+TLSRECV: 1,1024,"485454502F312E3120...",802
.....
+TLSRECV: 1,158,"3E0D0A090...",802               //自动输出接收数据，编码格式为 HEX。
```

- <max_len>是数据编码后，实际输出的长度；
- 当<encoded_method>=801 时，将编码为 string 格式，string 格式将回车、换行符号转义为'\r'、'\n'。

7.5 关闭 TLS 连接

AT+TLSCLOSE=<tid>

例如：

```
AT+TLSCLOSE=1          //关闭<tid>=1 的 TLS 连接。
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。
```

8 RAI 设置

8.1 RAI Flag 配置

RAI 的相关设置主要用于配置模组完成数据发送或接收后，是否快速进入 idle 态，M5311 通过 AT*NBIOTRAI 可配置 RAI 模式，该指令仅生效一次，需在每次发包前设置该指令。

AT*NBIOTRAI=<rai>	
参数	
<rai>	
0	关闭 RAI
1	发送完 1 个上行包，模组立刻进入 idle 态。
2	发送 1 个上行包，且接收到 1 个下行包，模组立即进入 idle 态。
备注	
– <rai>=1 模式适用于无 ACK 的 UDP 发包方式；该模式对 TCP 包无效；对于有 ACK 的 UDP 发包方式，设置该模式，可能存在两种风险：1）模组发完 UDP 包立即进入 idle 态，而后接收到 UDP 确认包，模组将重新建立 RRC 连接，从而进入到 active 态；2）模组发完 UDP 包立即进入 idle 态，此时若进入 PSM 或 Edrx，则模组将接收不到 UDP 确认包； – <rai>=2 模式适用于有 ACK 的 UDP 发包方式，模组发送一个上行包，且接收到一个下行包以后才能立即进入 idle 态；该模式虽然可以实现发送完成 TCP 包后立即进入 idle 态，但由于 TCP 不断开连接，模组无法进入睡眠模式，因此需要在 TCP 使用结束后及时关闭连接。	
示例	
AT+CSCON=1	//打开 RRC 状态上报。
+CSCON: 1 OK	//RRC 处于连接态。
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。
AT*NBIOTRAI=1 OK	//仅生效一次，需在每次发包前输入该指令。
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 OK	//第 0 号 Socket 成功发送 21 Bytes 数据。
+CSCON: 0	//无 ACK 的 UDP 发包方式，RAI 生效，释放 RRC 连接。
AT*NBIOTRAI?	
*NBIOTRAI: 0 OK	//AT*NBIOTRAI=1 仅生效一次，使用完成后返回默认值为 0。
+CSCON: 1	//RRC 连接建立。
AT*NBIOTRAI=2 OK	

AT*NBIOTRAI=<rai>	
示例（接上页）	
AT+IPSEND=0,0,"hello cmiot"	//<data_len>为 0 或空缺表示发送 string 类型，自动计算<data>长度。
+IPSEND: 0,21 OK	//第 0 号 Socket 成功发送 21 Bytes 数据。
+IPRD: 0,"47.93.217.230",2016,13,hello custom	//收到服务器确认包。
+CSCON: 0	//满足 AT*NBIOTRAI=2 条件，RRC 立即释放。

TCP 释放需要完成四次挥手，因此无法使用 AT*NBIOTRAI 快速释放 RRC 连接。

8.2 快速释放 RRC 连接指令

AT*RAIREQ 指令可实现在 RRC 连接态下快速释放 RRC Connection，进入 idle 态，需注意的是该指令会向保留（或指定）的 IP 地址发送 UDP\ICMP 数据包，IP 包的大小为 29Byte。

（1）**发送 UDP 包到保留（或指定）的 IP 地址，快速释放 RRC 连接。**

– 发送完 1 个上行包，模组立刻进入 idle 态，例如：

AT+CSCON=1	//打开 RRC 状态上报。
+CSCON: 1	//RRC 处于连接态。
OK	
AT*RAIREQ	//发送 1Byte UDP 包（加上 IP 包头有 29Byte）到 169.254.123.123:36000（保留 IP 地址），如果发送成功，RRC Connection 将会立即释放。
OK	
+CSCON: 0	//RRC Connection 释放。
+CSCON: 1	//RRC 连接建立。
AT*RAIREQ=0,"169.254.10.1",798	//发送 1Byte UDP 包（加上 IP 包头有 29Byte）到 169.254.10.1:789，如果发送成功，RRC Connection 将会立即释放。
OK	
+CSCON: 0	//RRC Connection 释放。

（2）**发送 ICMP 包到保留（或指定）的 IP 地址，若该 IP 路由可达，则快速释放 RRC 连接。**

– 发送 1 个上行包，且接收到 1 个下行包，模组立即进入 idle 态，例如：

AT+CSCON=1	//打开 RRC 状态上报。
+CSCON: 1	//RRC 处于连接态。
OK	
AT*RAIREQ=1,"114.116.144.151"	//发送 1Byte ICMP 包（加上 IP 包头有 29Byte）到 114.116.144.151,如果该 IP 地址可达，RRC Connection 将会立即释放。
OK	
+CSCON: 0	//RRC Connection 释放。

9 硬件相关指令

9.1 串口波特率

M5311 串口波特率默认为自适应模式，为避免在自适应模式下串口波特率受到外部干扰，建议在开机后将串口波特率设置为固定值。例如：

模组开机

```
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
AT+IPR?
+IPR: 0                     //默认为自适应波特率模式。
OK
AT+IPR=9600
OK                          //返回 OK，固定波特率为 9600，立即生效，模组复位或断电重启均保存配置。
AT                          //间隔 AT+IPR=9600 输入 500ms 后输入 AT 响应 OK。
OK
```

- 指令输入 AT+IPR，波特率立即生效，由于串口完成初始化存在一定延迟，该指令输入后至少间隔 500ms 后才能输入下一条指令。
- 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。满足以下两个条件之一，则会触发一次串口波特率的自适应功能。
  - 模组开机后，在未进入深度睡眠前，执行 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，进入深度睡眠后，唤醒模组执行 AT+IPR=0 返回 OK 后将不再自适应波特率；
  - 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。

9.2 流控功能

（1） 关闭流控，执行以下任意一条命令，立即生效，重启后保留配置。

```
AT+IFC=0,0
AT&K0              //等效于 AT+IFC=0,0。
```

（2） 打开软件流控，执行以下任意一条命令，立即生效，重启后保留配置。

```
AT+IFC=1,1
AT&K4              //等效于 AT+IFC=1,1。
```

（3） 打开硬件流控，执行以下任意一条命令，立即生效，重启后保留配置。

```
AT+IFC=2,2
AT&K3              //等效于 AT+IFC=2,2，低电平有效。
```

9.3 GPIO

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

9.4 ADC

当前仅支持 ADC0，对应 Pin38 引脚。

- **测量范围：0~1399mv**
- **参考 AT+CMADC**

9.5 LED 灯配置和指示

- **LED 状态灯：**STATE/WAKEUP_OUT
- **STATE：**对应 Pin21 引脚，可用作浅睡眠状态指示、网络状态指示。
- **WAKEUP_OUT：**对应 Pin16 引脚，用作深睡眠状态指示。

通过 AT+CMSYSCTRL 来进行使能/配置，为节省功耗，LED 默认关闭。

- **STATE 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**
- **使能 WAKEUP_OUT：AT+CMSYSCTRL=1,1**
- **STATE 设置为网络指示：AT+CMSYSCTRL=0,2**

驻网状态	输出 PWM 波形
未附着	80ms 高电平/800ms 低电平
已附着	80ms 高电平/3000ms 低电平

10 DNS 业务介绍

10.1 DNS 服务器地址

DNS 服务器地址的正确性将影响 TCP\UDP、MQTT、HTTP、TLS、OneNET、PING 指令集域名解析能否成功。

■ 默认 DNS 服务器地址

若无指令配置 DNS 服务器地址，则模组在驻网成功后根据网络携带信息中自动配置 DNS 服务器地址，若网络不携带 DNS 服务器地址，则使用模组默认的 DNS 服务器地址。

模组默认的 IPv4 服务器地址为：

第一服务器地址：119.29.29.29
第二服务器地址：114.114.114.114

模组默认的 IPv6 服务器地址为：
第一服务器地址：2400:3200::1
第二服务器地址：2001:4860:4860::8888

■ 指令配置 DNS 服务器地址

若指令配置了 DNS 服务器地址，模组将以配置的 IP 作为 DNS 服务器地址。

IPv4 DNS 服务器地址配置及查询，例如：

```
AT+DNSSER="180.76.76.76",0
OK
AT+DNSSER="223.5.5.5",1
OK
AT+DNSSER?
+DNSSER: 0,180.76.76.76
+DNSSER: 1,223.5.5.5
OK
```

IPv6 DNS 服务器地址配置及查询，例如：

```
AT+DNSSERV6="2001:da8:202:10::36",0
OK
AT+DNSSERV6="2400:da00::6666",1
OK
AT+DNSSERV6?
+DNSSERV6: 0,2001:DA8:202:10::36
+DNSSERV6: 1,2400:DA00::6666
OK
```

10.2 DNS 服务请求

- IPv4 DNS 业务

```
AT+CMDNS="iot.10086.cn"
OK
+CMDNS: 183.230.40.127
```

M5311 S03 及以前版本不支持 IPv6DNS 服务器配置，M5311 S04 版本新增 AT+DNSSERV6 指令支持 IPv6 服务器地址配置。

11 IPv6 业务介绍

11.1 IPv6 入网配置

模组接入 IPv6 网络，需配置正确的 PDP 类型，M5311 默认的 PDP 类型为“IPv4v6”的双栈模式。

- **修改默认 PDP 类型，重启生效。**

```
AT*CGDEFCONT="IPV4V6",""          //更改默认 PDP 类型为“IPV4V6”的双栈模式，第二个参数填当地可使用的 APN。
OK
AT*CGDEFCONT="IPV6",""            //更改默认 PDP 类型为“IPV6”的仅支持 IPv6 的单栈模式，第二个参数填当地可
                                  使用的 APN。
OK
```

- **确认 IPv6 入网**

```
IPV4V6 双栈模式下，同时激活 IPv4 及 IPv6 PDN:
ATREADY: 1
+CFUN: 1
+CPIN: READY
+IP: 10.149.81.93                 //模组开机信息打印 IPv4 地址说明已激活 IPv4 PDN。
+IP: 2409:8900:8500:55bd:1:1:acf9:290   //模组开机信息打印 IPv6 地址说明已激活 IPv6 PDN。
IPV6 单模式下，只激活 IPv6 PDN:
ATREADY: 1
+CFUN: 1
+CPIN: READY
+IP: 2409:8900:8500:55bd:1:1:acf9:290   //模组开机信息打印 IPv6 地址说明已激活 IPv6 PDN。
若开机信息无 IP 地址返回，可通过以下方式查询确认：
AT+CEREG?
+CEREG: 0,1                       //已附着上网络。
OK
AT+CGPADDR=1
+IP: 2409:8900:8500:55bd:1:1:acf9:290   //查询到 IPv6 地址，说明已激活 IPv6 PDN。
OK
```

11.2 IPv6 数据业务

IPv6 PING 业务

AT+PING 指令支持 ping IPv6 地址及域名，需将 AT+PING <type>参数置为 1，例如：

```
AT+PING="2001:da8:8000:1:202:120:2:101",16,8000,10,1
OK
+PING: 2001:da8:8000:1:202:120:2:101,44,579
+PING: 2001:da8:8000:1:202:120:2:101,44,620
+PING: 2001:da8:8000:1:202:120:2:101,44,622
+PING: 2001:da8:8000:1:202:120:2:101,44,619
+PING: 2001:da8:8000:1:202:120:2:101,44,272
+PING: 2001:da8:8000:1:202:120:2:101,44,584
+PING: 2001:da8:8000:1:202:120:2:101,44,323
+PING: 2001:da8:8000:1:202:120:2:101,44,322
+PING: 2001:da8:8000:1:202:120:2:101,44,669
+PING: 2001:da8:8000:1:202:120:2:101,44,203
--- 2001:DA8:8000:1:202:120:2:101 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss
rtt min/avg/max = 203/481/669
AT+PING="ipv6.sjtu.edu.cn",16,8000,10,1
OK
+PING: 2001:da8:8000:1:0:0:0:80,45,318
+PING: 2001:da8:8000:1:0:0:0:80,45,526
+PING: 2001:da8:8000:1:0:0:0:80,45,302
+PING: 2001:da8:8000:1:0:0:0:80,45,591
+PING: 2001:da8:8000:1:0:0:0:80,45,678
+PING: 2001:da8:8000:1:0:0:0:80,45,646
+PING: 2001:da8:8000:1:0:0:0:80,45,594
+PING: 2001:da8:8000:1:0:0:0:80,45,673
+PING: 2001:da8:8000:1:0:0:0:80,45,670
+PING: 2001:da8:8000:1:0:0:0:80,45,540
--- 2001:DA8:8000:1::80 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss
rtt min/avg/max = 302/553/678
```

M5311 S03 及以前版本无 AT 指令支持 IPv6 数据业务，S04 版本支持 DNS 及 PING 业务。

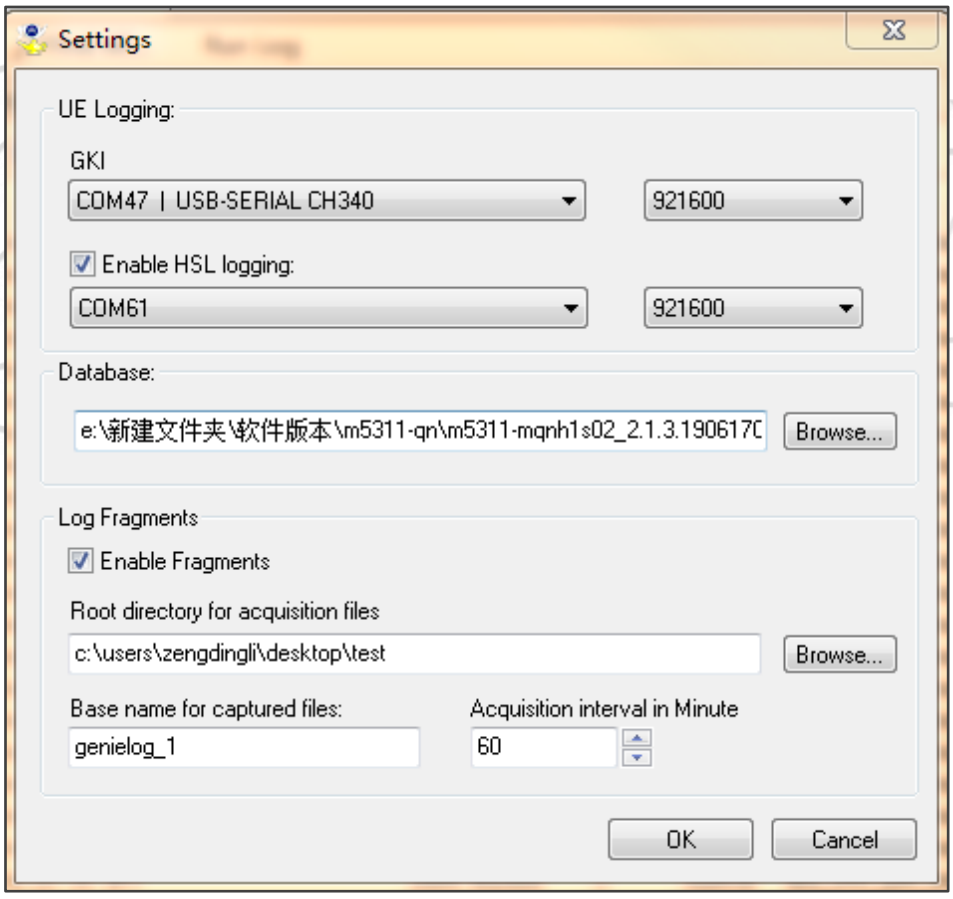
12 Genie Log 使用

- **GKI LOG：**包含 AP <--> Modem 信号值、程序调试输出 LOG、Modem 输出信号、RRC Decode。
- **HSL LOG：**包含协议栈消息等。

12.1 连接方式

12.1.1 模组休眠相关 LOG 抓取

由于 USB 供电会导致模组无法进入休眠，若需要抓取休眠相关业务的 LOG，可通过 DBG (PIN 1-2)或 UART 2 (PIN 44-45)来抓取 GKI 和 HSL LOG。



M5311 S03 及以后版本可通过复用 WAKEUP_OUT (PIN 16) 引脚为 UART 3 TX 来抓取 HSL LOG。

若使用 WAKEUP_OUT 引脚复用为 HSL LOG，请确认业务逻辑中未使用 WAKEUP_OUT，配置 WAKEUP_OUT 为 HSL LOG 后，原 AT+CMSYSCTRL 指令所配置的 WAKEUP_OUT 唤醒指示功能将失效。

以 DBG 作为 GKI LOG，WAKEUP_OUT 作为 HSL LOG 为例，指令配置如下：

（1） 配置 DBG 作为 GKI LOG 的输出端口，设置 DBG 波特率为 921600，如下
AT+LOGCFG=0,0,921600

（2） 配置 WAKEUP_OUT 复用为 UART 3 TX 并作为 HSL LOG 的输出端口，设置 UART 3 TX 波特率为 921600，如下：
AT+LOGCFG=1,3,921600

重启模组，设置生效。

（3） Genie Log 配置：选择 GKI 为 DBG 识别的 COM 口，波特率必须与 AT+LOGCFG 所配置的值一致，选择 HSL 为 UATR 3 识别的 COM 口，Database 需选择与固件版本对应的.dec 文件。

12.1.2 USB LOG 抓取

USB 方式抓取 LOG 会导致模组无法休眠，无需休眠的业务流程可通过此方式抓取 LOG。

连接 USB 到 PC 可模拟出 USB COM1 (USB Modem port)及 USB COM2 (USB Debug port)两个 port，可分别配置为 GKI 和 HSL LOG。

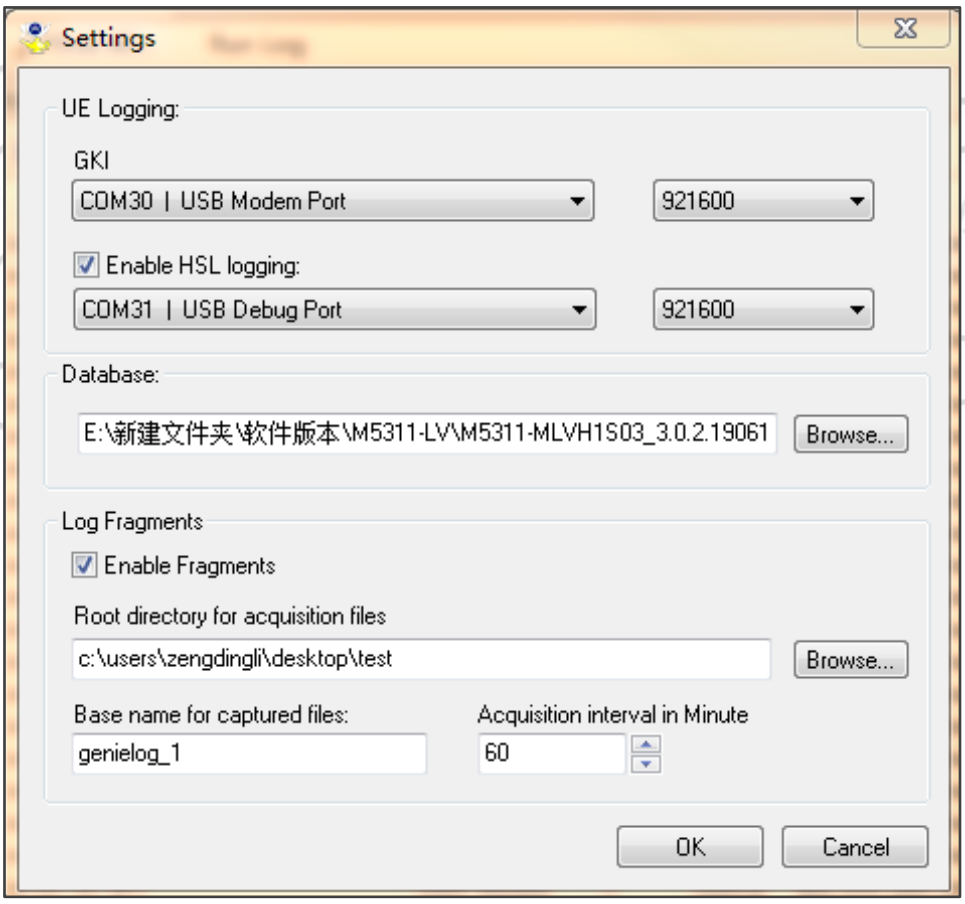
以 USB COM1 (USB Modem port)作为 GKI LOG，USB COM2 (USB Debug port)作为 HSL LOG 为例，指令配置如下：

(1) 配置 USB COM1 (USB Modem port)作为 GKI LOG 的输出端口，波特率无需配置，如下：
AT+LOGCFG=0,4

(2) 配置 USB COM2 (USB Debug port)作为 HSL LOG 的输出端口，波特率无需配置，如下：
AT+LOGCFG=1,5

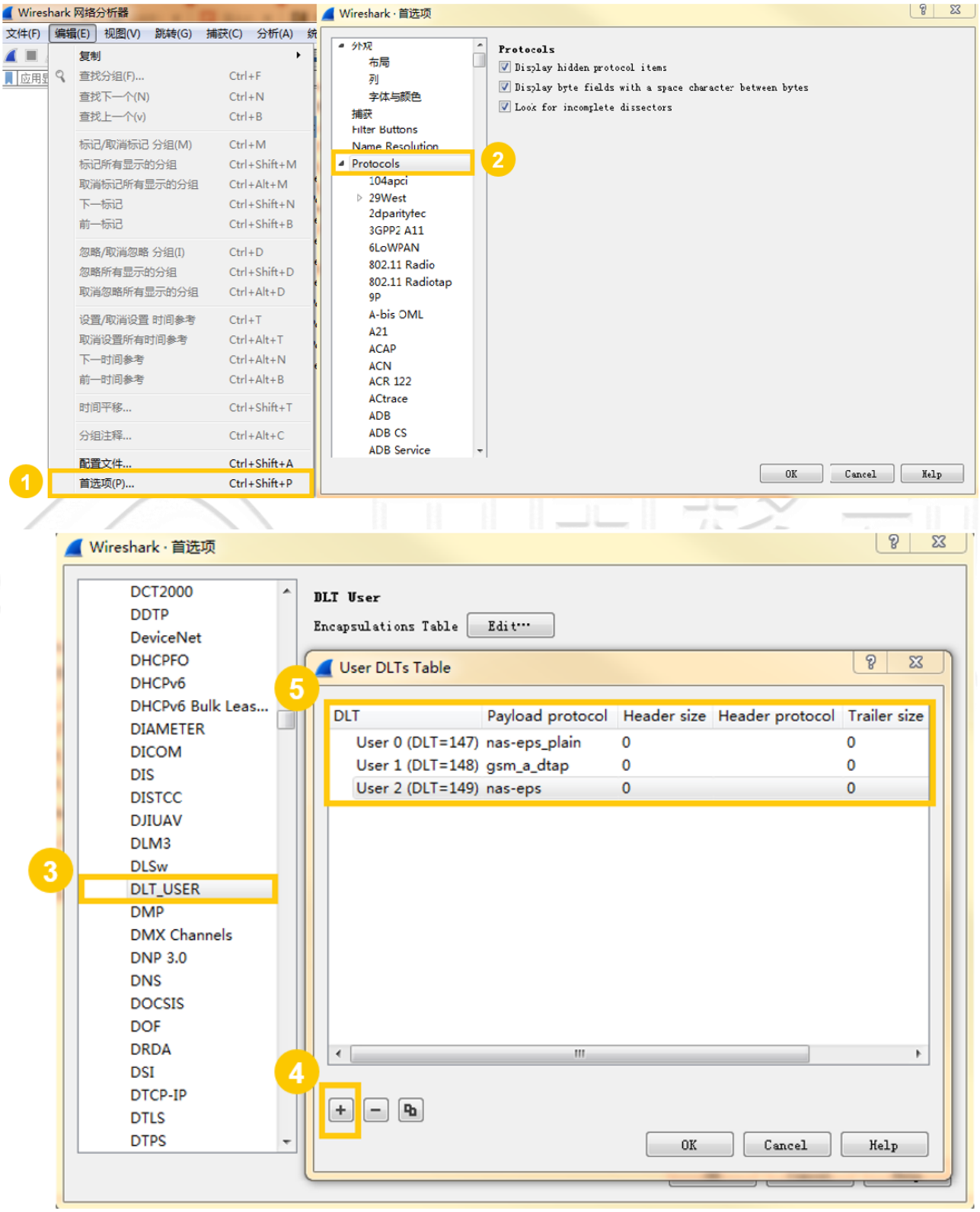
重启模组，设置生效。

(3) Genie Log 配置：选择 GKI 为 USB Modem port，波特率设置为 921600 及以上：选择 HSL 为 USB Debug port，Database 需选择与固件版本对应的.dec 文件。



12.2 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
```