

简述 NB 物联网测试方法

NB 物联网作为新技术应用于智慧城市的建设，基本业务功能测试从 2016 年 11 月中旬开始，一直持续至今，而我也很荣幸一直处于物联网测试队伍中，我也将自己接触的东西，写给大家，希望大家给出宝贵意见和建议！整个 NB 测试工作环境由终端，基站，核心网，灌包服务器，IoT 平台。



一：测试终端，测试软件和软件版本

NB 测试终端为 nierda 公司的 dongle。测试软件为串口调试工具，UElogview 和 GENEX Probe 3.18！数据分析软件为 dist 和 GENEX Assistant 3.18！软件版本为华为公司提供！

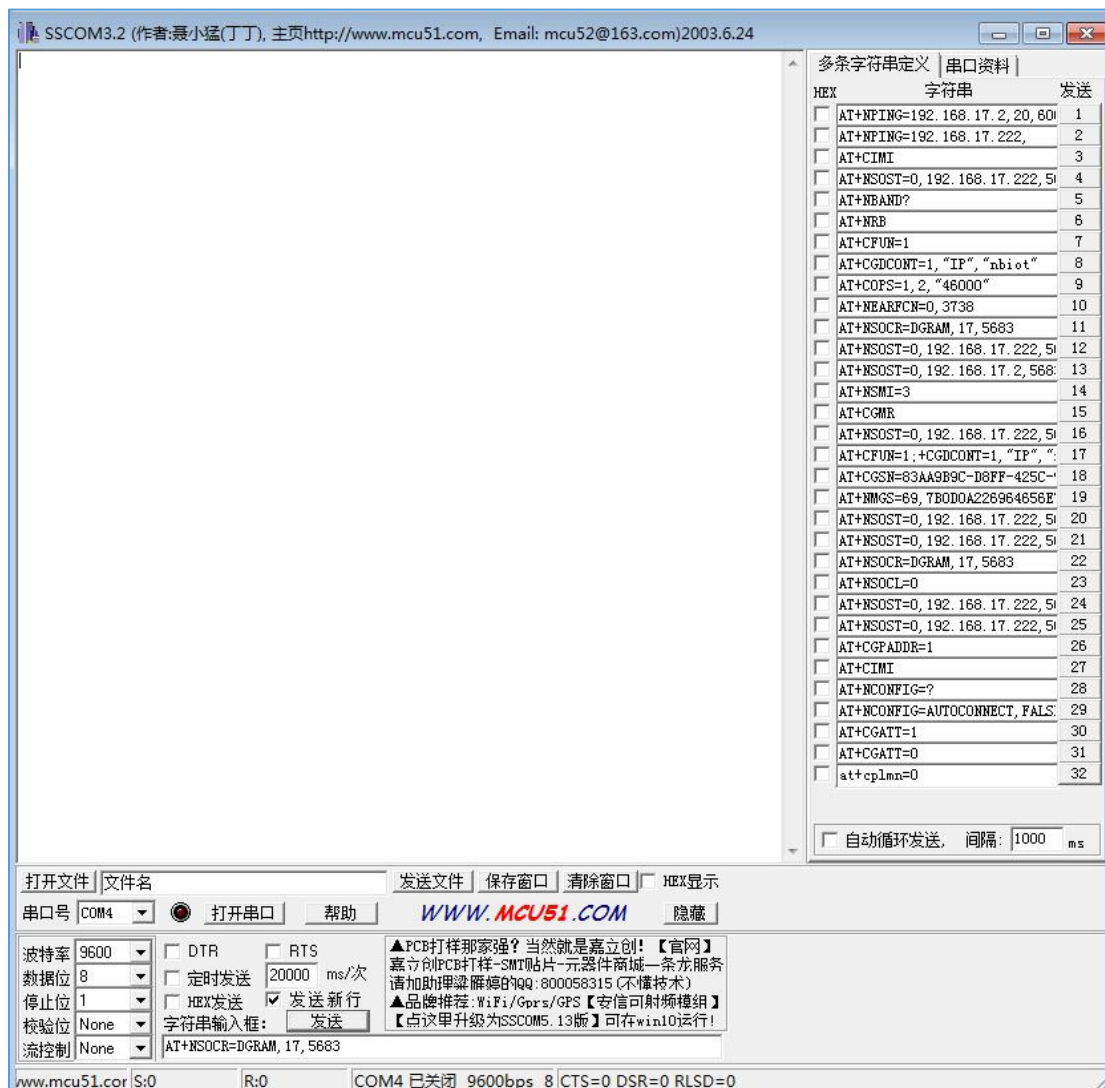
二：测试软件安装

按照提供的软件包，按照顺序安装即可，对于某些电脑装不了 UElogview，需重新安装系统。GENEX Probe 3.18 和 GENEX Assistant 3.18 安装之后，向华为公司提供 ESN 号，申请 license，更新 license 之后，软件就可以使用！

三：软件使用

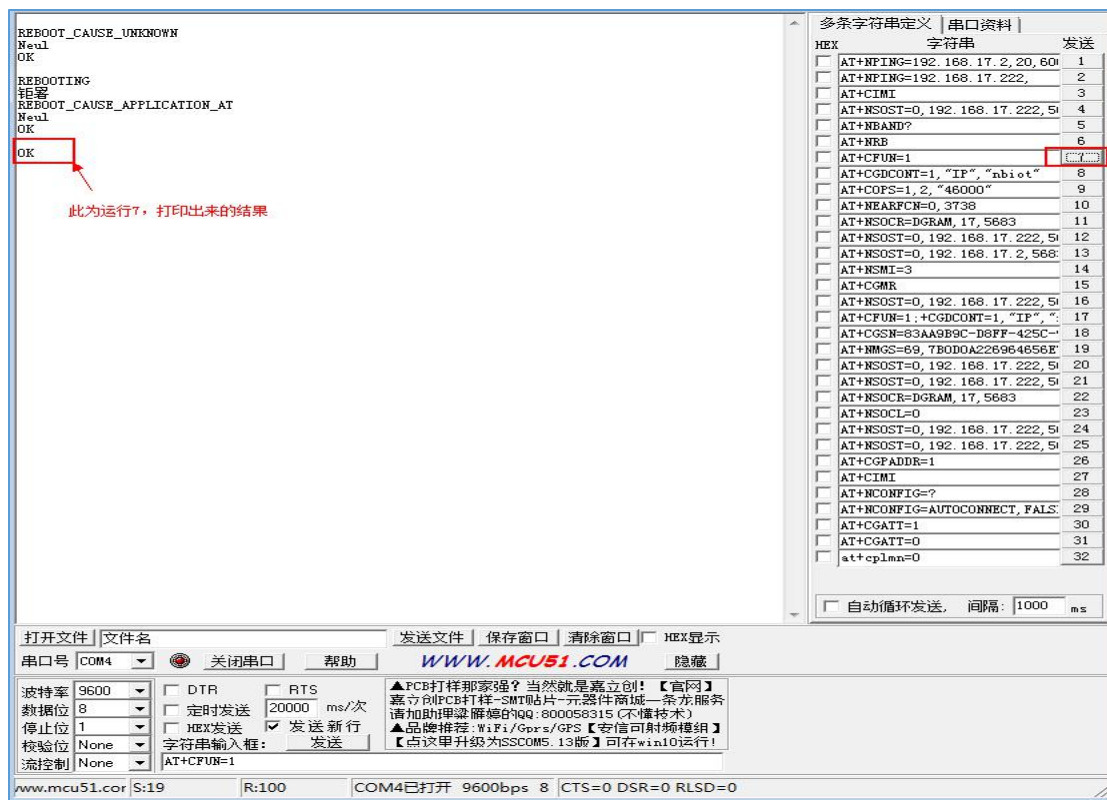
1：串口调试工具和 UElogviewr

串口调试工具为免安装版，打开工具，桌面如下！



一些开机复位锁频等指令为窗口右边。需要在打开串口工具点击[扩展]。点击最右边的发送，即视为执行此条命令。左边窗口会打印出信息！

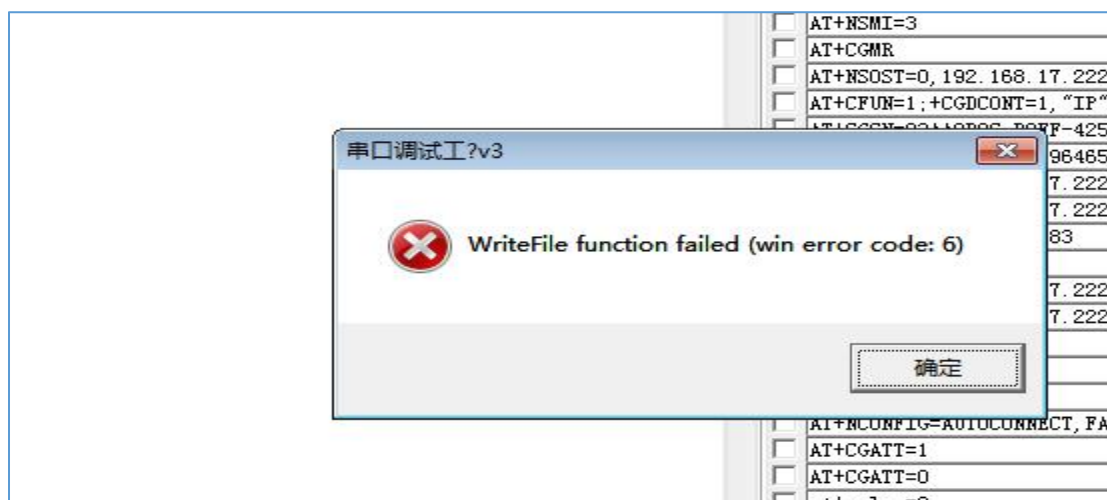




注意事项:

(1): 如果打印出现 **ERROR**，有两种可能，一种为串口指令格式错误，不符合版本和软件要求。其二为终端未正常接入，会导致一些指令出现错误，需要排查！

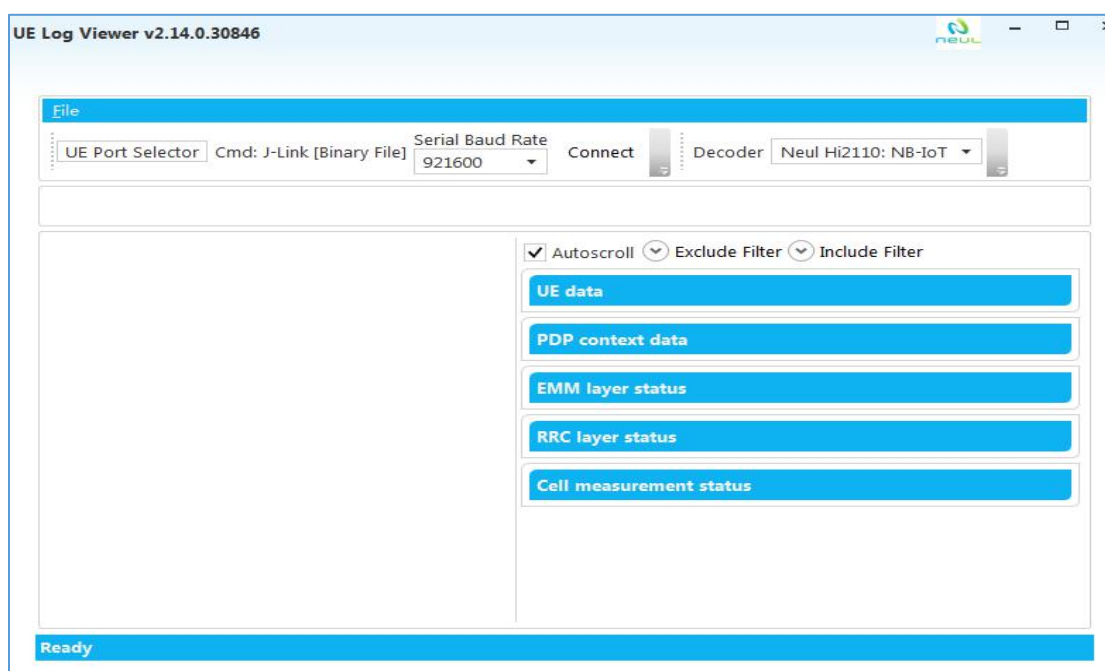
(2): 如果出现下面不正常窗口，说明[打开串口]未打开！打开这个就 OK。



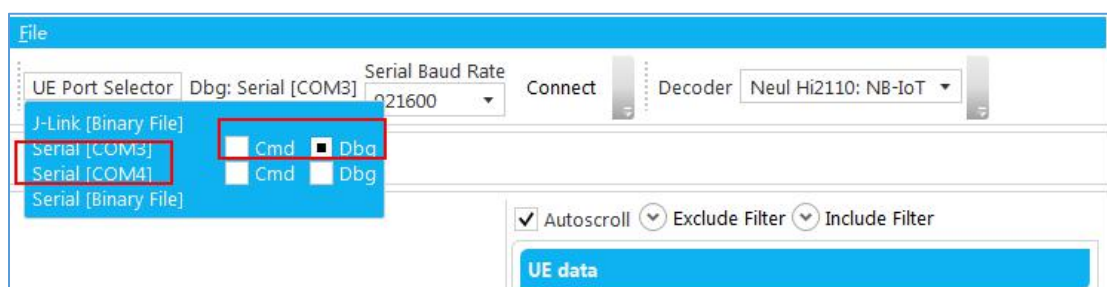


当终端插入电脑，会出现两个端口，一个是输出端口，一个是输入端口，两个端口将串口工具和 UElogviewr 串连起来。接下来介绍一下 UElogviewr 使用。

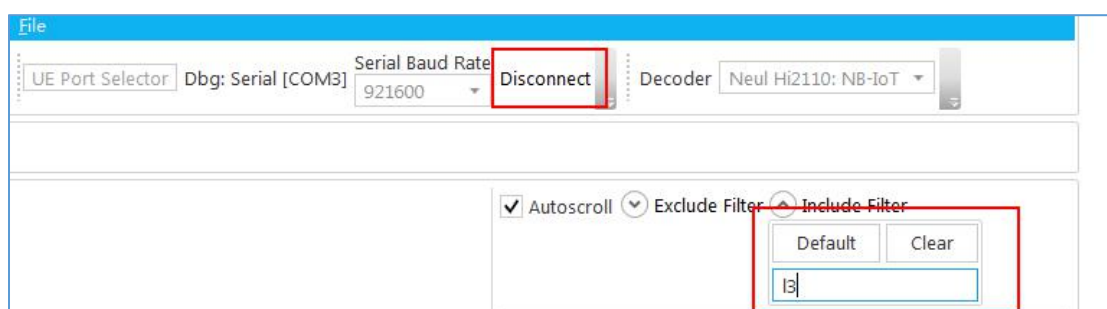
UElogviewr 窗口如下，



出现端口 3 和 4，UElogviewr 里的端口和串口工具的端口不一样，如下，点击[Cmd]之后再点击[Dbg],然后点击[Connect]，这样就使得 UElogviewr 处于记 log 状态！



如下图，就处于记 log 状态！L3 是筛选信息，若不筛选信息，终端接入 log 和做业务时，会出现大量的信令，很容易导致软件崩溃！



2: GENEX Probe 3.18 使用

整体操作流程如下：插上终端——连接终端——导入工参和图纸——制定测试计划——记录 log——运行测试计划——停止记录 log。

PROBE 作为很常见的网优测试软件，就不多做介绍。

3: 数据分析软件使用

DIST 为免安装软件，GENEX Assistant 3.18 为数据分析常用软件，不多做介绍！

四：测试介绍

1：常用 AT 命令简介

AT 命令	AT 命令解释
AT+NRB	复位
AT+CFUN=1	开机
AT+NEARFCN=0, 3738	锁频
AT+CIMI	查询 ISMI 信息
AT+CGMR	查询终端版本
AT+CGATT=1	attach
AT+CGATT=0	detach
AT+NSOCR=DGRAM, 17, 5683	创建 SOCR 端口
AT+NSOST=0, 192. 168. 17. 222, 5683, 10, 40024678921345328790	灌包命令
AT+NPING=192. 168. 17. 2, 20, 60000	ping 包命令

2：上行 UDP 灌包业务和上行 ping 包业务介绍

上行 UDP 灌包业务

AT+NSOCR=DGRAM,17,5683-----创建 SOCR 端口 5683 端口

AT+NSOST=0,192.168.17.222,5683,10,40024678921345328790-----

---UDP 灌包 10Bytes 20 个 16 进制数字表示 10Bytes

注：测试上行 UDP 灌包，当 attach 成功后，需要点击锁 SOCR 端口的 AT 命令后，再点击上行灌包的 AT 的命令，10 表示是灌包大小，后面 20 个 16 进制数字表示 10Bytes 的数据量，若业务要求灌 100,200,300,500，则命令需要做出相应的改变。

上行 ping 包业务——需要核心网加路由

AT+NPING=192.168.17.222,20,60000----- ping20Bytes

AT+NPING=192.168.17.222,200,60000----- ping200Bytes

AT+NPING=192.168.17.222,1000,60000----- ping1000Bytes

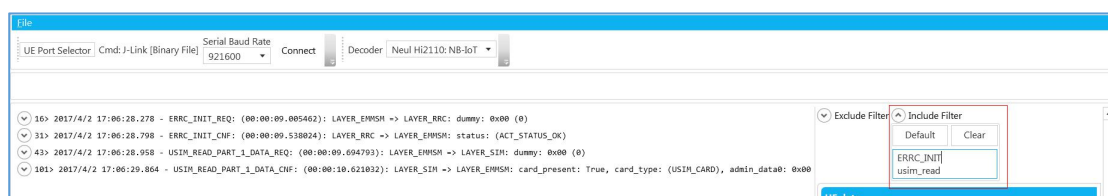
注：测试 ping 包业务时，当 attach 成功后，即可点击 ping 的 AT 命令。

3：入网接入流程

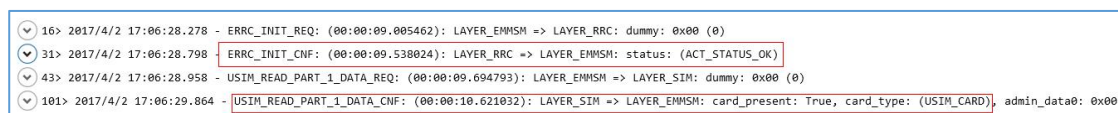
开机流程——搜网流程——建链流程——附着流程

(1) 开机流程

在 UeLogviewer 工具中输入 ERRC_INIT、usim_read 过滤日志，如下：



可以看到如下两条日志：



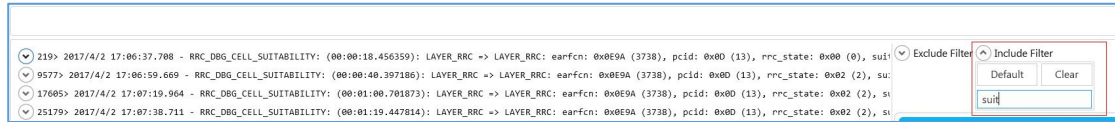
ERRC_INIT_CNF 消息中返回的状态是 ACT_STATUS_OK，表示终端开机初始化成功完成；

USIM_READ_PART_1_DATA_CNF 消息中信元 card_present 状态为 True，表示终端读 SIM 卡成功。

如果后续又 log 中出现非如上状态的消息，则表示该步骤可能存在问题，需要反馈日志进一步分析。

(2) 搜网流程

在 UeLogviewer 工具中输入 suit 进行消息过滤，如图：



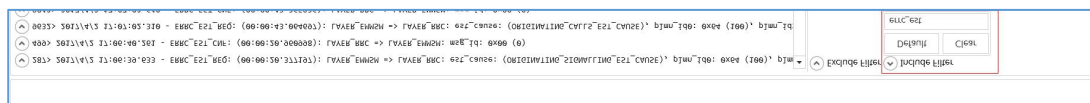
过滤出 RRC_DBG_CELL_SUITABILITY 消息，如下图：



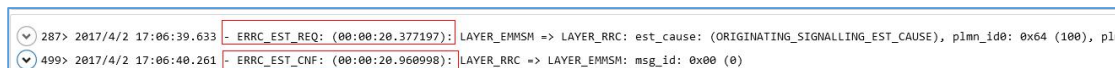
该消息中 suitable 信元应该是 True，表示搜索到合适驻留的小区，如果为 False 则表示存在问题，需要反馈日志进一步定位

(3) 建链流程

在 UeLogviewer 工具中输入 errc_est 进行消息过滤，如图：



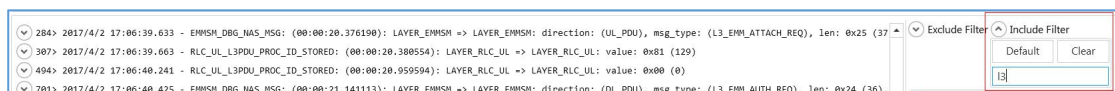
在消息框里面存在如下两条消息：



两条消息成对出现，如果发现不存在该消息或者存在 ERR_EST_REJ 消息，表面建链流程存在异常，需要反馈日志进行分析。

(4) 附着流程

在 UeLogviewer 工具中输入 I3 进行消息过滤，如图：



出现的消息流程如下：

284>	2017/4/2 17:06:39.633	-	EMMSM_DBG_NAS_MSG: (00:00:20.376190): LAYER_EMMSM => LAYER_EMMSM: direction: (UL_PDU), msg_type: (L3_EMM_ATTACH_REQ), len: 0x25 (37)
307>	2017/4/2 17:06:39.663	-	RLC_UL_L3PDU_PROC_ID_STORED: (00:00:20.380554): LAYER_RLC_UL => LAYER_RLC_UL: value: 0x81 (129)
494>	2017/4/2 17:06:40.241	-	RLC_UL_L3PDU_PROC_ID_STORED: (00:00:20.959594): LAYER_RLC_UL => LAYER_RLC_UL: value: 0x00 (0)
701>	2017/4/2 17:06:40.425	-	EMMSM_DBG_NAS_MSG: (00:00:21.141113): LAYER_EMMSM => LAYER_EMMSM: direction: (DL_PDU), msg_type: (L3_EMM_AUTH_REQ), len: 0x24 (36)
932>	2017/4/2 17:06:40.839	-	EMMSM_DBG_NAS_MSG: (00:00:21.559051): LAYER_EMMSM => LAYER_EMMSM: direction: (UL_PDU), msg_type: (L3_EMM_AUTH_RSP), len: 0x0B (11)
937>	2017/4/2 17:06:40.839	-	RLC_UL_L3PDU_PROC_ID_STORED: (00:00:21.559997): LAYER_RLC_UL => LAYER_RLC_UL: value: 0x01 (1)
1354>	2017/4/2 17:06:41.550	-	EMMSM_DBG_NAS_MSG: (00:00:22.269714): LAYER_EMMSM => LAYER_EMMSM: direction: (DL_PDU), msg_type: (L3_EMM_SECURITY_MODE_CMD), len: 0x24 (36)
1359>	2017/4/2 17:06:41.551	-	EMMSM_DBG_NAS_MSG: (00:00:22.275299): LAYER_EMMSM => LAYER_EMMSM: direction: (UL_PDU), msg_type: (L3_EMM_SECURITY_MODE_COMPLETE), len: 0x24 (36)
1364>	2017/4/2 17:06:41.551	-	RLC_UL_L3PDU_PROC_ID_STORED: (00:00:22.276558): LAYER_RLC_UL => LAYER_RLC_UL: value: 0x02 (2)
1755>	2017/4/2 17:06:41.910	-	EMMSM_DBG_NAS_MSG: (00:00:22.650482): LAYER_EMMSM => LAYER_EMMSM: direction: (DL_PDU), msg_type: (L3_EMM_ATTACH_ACCEPT), len: 0x52 (82)
1759>	2017/4/2 17:06:41.910	-	EMMSM_DBG_NAS_MSG: (00:00:22.652709): LAYER_EMMSM => LAYER_EMMSM: direction: (UL_PDU), msg_type: (L3_EMM_ATTACH_COMPLETE), len: 0x25 (37)

L3_EMM_ATTACH_REQ:表示发起附着请求

L3_EMM_AUTH_REQ: 表示发起鉴权请求

L3_EMM_AUTH_RSP: 表示鉴权成功

L3_EMM_SECURITY_MODE_CMD: 表示发起安全模式

L3_EMM_SECURITY_MODE_COMPLETE: 表示安全模式成功

L3_EMM_ATTACH_ACCEPT: 表示附着流程被接收

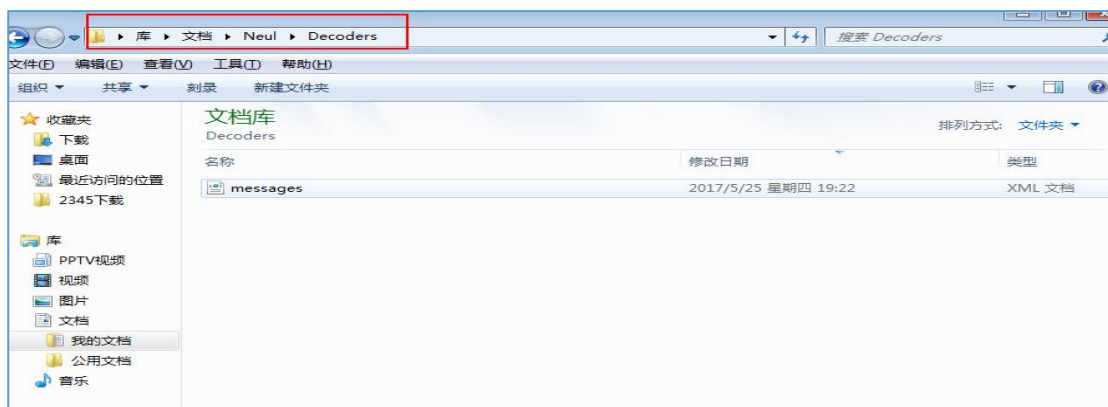
L3_EMM_ATTACH_COMPLETE: 表示附着流程成功

附着流程一定要观察到 L3_EMM_ATTACH_COMPLETE 消息，才算是成功完成附着，之后就可以进行上下行数传了，如果未观察到 L3_EMM_ATTACH_COMPLETE 消息，说明附着流程失败，需要进一步定位失败原因。

五：测试过程

1: 更换 messages

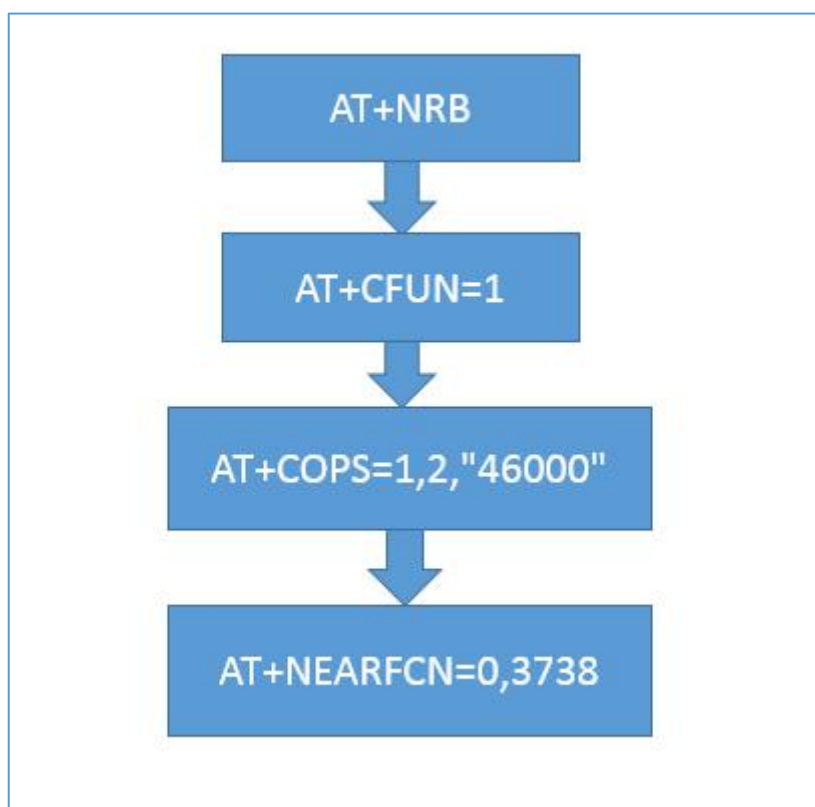
由于当前测试版本较多，不同的测试业务需要不同版本的终端，不同的测试终端需要不同的 messages。在用 UElogviewr 测试时，需要更换 messages，更换 messages 地址为



2: 连接设备

设备连接上文已简单介绍，这里就不作多余介绍了。

3: 终端入网



注：每发送一次命令，都要等串口工具出现 OK，再点击下一条命令。

执行完成后，UE 正常接入后，会出现 attach complete。

4: 观看测试信息

接入成功之后，UElogviewr 里看到如下窗口

The screenshot displays the UElogviewr interface. On the left, a log window shows various system events. On the right, there are four status panels: 'activated' (True), 'EMM layer status' (PROTO_EMM_REGISTERED), 'RRC layer status' (PROTO_RRC_CONNECTED), and 'Cell measurement status'. Red boxes and numbers 1-4 highlight specific fields: 1 points to 'IPv4 address' (0.0.0.7), 2 points to 'last_reject_cause' (EMM_CAUSE_UNKNOWN), 3 points to 'state' (PROTO_RRC_CONNECTED), and 4 points to the 'Cell measurement status' panel.

UE data	Value
dl_count	9
ul_count	13
ul_fail	0
ul_queue	0

(1):可以看到测试终端 ip，杭州目前测试终端 ip 为 192.168.20.X (x 为图中出现的数字)。

(2):当终端接入被 reject 时，可以看到被拒的原因，作简单分析。

(3):可以看到当前终端处于连接态还是空闲态！

(4):可以看到测试信息，频点，PCI，RSRP，SINR 等重要信息。

当需要灌包和 ping 包时，可以通过如下窗口看到包的个数。

UE data	
dl_count	9
ul_count	13
ul_fail	0
ul_queue	0

常见问题集:

现象 1:

日志中使用 L3 过滤日志，发现一直重复发送 L3_EMM_ATTACH_REQ 消息，但没有其他附着流程的消息，比如说 L3_EMM_ATTACH_COMPLETE 、 L3_EMM_ATTACH_ACCEPT 、 L3_EMM_SECURITY_MODE_COMPLETE 等消息。

排查方向:

- 1、检测自己的终端版本号，执行 AT+CGMR 命令查看返回值，并告知后台；
- 2、让后台检测基站版本号和 DCI_SF_REP_NUM_COMP_SWITCH 是否打开；

现象 2:

日志中使用 L3 过滤日志，发现存在 L3_EMM_ATTACH_REJ 消息，表示附着流程被核心网拒绝了。

排查方向:

需要联系核心网同事查看具体拒绝原因，常见的原因有：开卡信息异常、基站 TAC 未在核心网出做配置。

现象 3:

使用搜网流程中描述的方法，进行排查，发现 suitable 信元应该是 FALSE，表示没有发现可用的小区

排查方向:

继续排查该消息中的其他信元如果发现存在如下信息:

1、band_not_supported:True,表示终端不支持当前小区频点的 band,需要修改终端支持的 band 信息,可用执行如下命令:

AT+NRB

AT+CFUN=0

AT+NBAND=5,8

进行支持 band 信息的修改。之后执行复位并进行正常入网操作。

2、wrong_plmn: True,表示当前卡的 plmn 信息和小区携带的 plmn 信息不匹配,导致无法入网,可使用如下命令进行锁定 PLMN:

AT+COPS=1,2,"46000"

注意移动使用 46000,其他运营商需要修改到对应的运营商的 PLMN。

对于一个新技术的业务功能测试验证,遇到问题,则需要我们多点耐心,和同事及技术大牛交流学习尤为重要,在交流过程中,多听多记,下次遇到问题回想以前解决的方法!对于测试新人来说,多和老同事学习外测经验,多在测试过程中,积累经验!

六：相关简单知识

NB 技术优点：广/深覆盖——比 GSM 覆盖增加 20dB+;

低功耗——基于 AA 电池，使用寿命可超过 10 年；

低成本——终端芯片低至\$1;

大连接——连接数可达到数 10 亿；

微信扫描以下二维码，免费加入【5G 俱乐部】，还赠送整套：5G 前沿、NB-IoT、4G+ (VoLTE) 资料。

