Revision History

文件名称	**Modem 简单流程及案例分析 V1.0**		
文件编号		版本编号	V1.0
发布日期	2015-11-27	主控部门	软件二部

	意见	签名/日期
参与：王储、朱玉		2015-11-25

版本号	修改时间	修改人	修改原因	修改主要内容
V1.0	2015-11-27	王储	拟制	整理

目 录

一、SIM Status

(一) SIM Status.

A. case 1: SIM 卡热插拔压力测试不识卡

SIM 卡热插拔压力测试，多次热拔插，某次插入，不识别 SIM 卡；不识别卡后，接着拔出卡再插入，可以再次识别。

MDlog 看到的现象如下：

08:17:10:852 最后一次拔出，sim task 收到 MSG_ID_SIM_PLUG_OUT_IND，接着 08:17:12:412 有触发 insert SIM 中断（拔插间隔不足两秒），但是 sim task 没有收到 MSG_ID_SIM_PLUG_IND_IND msg，忽略了此次插入动作的处理。

2327 1166723 08:17:10:852 Hight remove SIM=%d,%d

40299 1166723 08:17:10:852 MOD_DRV_HISR MOD_SIM_2 PS_SIM_SAP MSG_ID_SIM_PLUG_OUT_IND

这种现象为 SIM 热拔插太快，需要如下复测：

1、加大 SIM EINT debounce time 为 100；

2、保持热拔插间隔标准：拔卡后，请至少等待 2S，让 SIM 安全下电，sim state 更新过来再插卡；插卡后，请至少等待 1S，让 AP RILD ready 再进行拔卡动作。若拔插太快，sim state 出现混乱，就无法正确处理 SIM 热插拔动作，就会出现某次插入无法识别 SIM 的问题。

3、复现问题后，请再次拔卡，再插卡，若能再次识别到卡，就说明是拔插太快导致的不识别卡问题。是测试手法的问题，非热插拔功能出现问题，需要按照热拔插间隔标准复测。

附：

双卡双待手机中：MOD_SIM 指的是卡槽一中的 SIM 卡，MOD_SIM_2 指的是卡槽二中的 SIM 卡。

拔卡动作搜索“MSG_ID_SIM_PLUG_OUT_IND”

Type	Index	Local Time	Source	Destination	SAP	Message
	7415	20:05:08:800 2015/11/13	MOD_UMAC		TRACE_WARNING	[Discard TB] : with bad CRC result and MAC header exist . TrCH ID = 31
	7416	20:05:08:800 2015/11/13	MOD_UMAC		TRACE_INFO	[RX TB SUMMARY] Bad CRC TBs = 0, Bad MAC Header TBs = 0, Total Received TBs =
	7417	20:05:08:800 2015/11/13	MOD_UL1		TRACE_GROUP_1	Internal Processing
	7418	20:05:08:800 2015/11/13	MOD_DHL		TRACE_INFO	[L2] flush from 0
	7419	20:05:08:800 2015/11/13	MOD_DHL		TRACE_INFO	[L2] flush 0-0
	7420	20:05:08:800 2015/11/13	MOD_SIM		TRACE_STATE	SIM PLUG OUT(0) -> PS(0)
	7421	20:05:08:800 2015/11/13	MOD_DRV_HISR	MOD_SIM	PS_SIM_SAP	MSG_ID_SIM_PLUG_OUT_IND
	7422	20:05:08:800 2015/11/13	MOD_NIL		TRACE_INFO	[SIM_DRV] 1164 : 0, 1115, 19764f, 3, 4
	7423	20:05:08:800 2015/11/13	MOD_SIM		TRACE_STATE	SIM PLUG OUT(1) -> PS(1)
	7424	20:05:08:800 2015/11/13	MOD_NIL		TRACE_INFO	SIM Plug Out but ignore!!!
	7425	20:05:08:800 2015/11/13	MOD_NIL		TRACE_INFO	[SIM_CUS_DRV:464]Remove SIM : 0, 0, 1, 1, 1, 1, 197652
	7426	20:05:08:800 2015/11/13	MOD_SIM		TRACE_GROUP_3	sim_stop_timer()
	7427	20:05:08:800 2015/11/13	MOD_SIM		TRACE_GROUP_3	SIM_STATUS : length: 5
	7428	20:05:08:800 2015/11/13	MOD_SIM		TRACE_GROUP_3	APDU tx 0: 80 F2 02 0C 00 F2 F2 F2 F2 F2 DB F1 00 00 00 00

插卡动作搜索“MSG_ID_SIM_PLUG_IN_IND”

Type	Index	Local Time	Source	Destination	SAP	Message
	20873	20:05:27:520 2015/11/13	MOD_SIM		TRACE_STATE	SIM PLUG IN(1) -> PS(1)
	20874	20:05:27:520 2015/11/13	MOD_DRV_HISR	MOD_SIM_2	PS_SIM_SAP	MSG_ID_SIM_PLUG_IN_IND
	20875	20:05:27:520 2015/11/13	MOD_NIL		TRACE_INFO	[SIM_CUS_DRV:498]Insert SIM : 0, 0, 0, 0, 0, 0, 22d277
	20876	20:05:27:520 2015/11/13	MOD_SIM		TRACE_GROUP_3	sim_stop_timer()
	20877	20:05:27:520 2015/11/13	MOD_NIL		TRACE_INFO	sim_stop_timer() but return out
	20878	20:05:27:520 2015/11/13	MOD_SIM	MOD_L4C	PS_SIM_SAP	MSG_ID_SIM_ERROR_IND
	20879	20:05:27:520 2015/11/13	MOD_SIM	MOD_SMU	PS_SIM_SAP	MSG_ID_SIM_ERROR_IND
	20880	20:05:27:520 2015/11/13	MOD_SIM	MOD_GMSS	PS_SIM_SAP	MSG_ID_SIM_ERROR_IND
	20881	20:05:27:520 2015/11/13	MOD_SIM	MOD_EVAL	PS_SIM_SAP	MSG_ID_SIM_ERROR_IND
	20882	20:05:27:520 2015/11/13	MOD_SIM	MOD_MM	PS_SIM_SAP	MSG_ID_SIM_ERROR_IND
	20883	20:05:27:520 2015/11/13	MOD_SIM		TRACE_STATE	SIM RESET at 1.8V
	20884	20:05:27:520 2015/11/13	MOD_SIM_2		TRACE_GROUP_3	sim_stop_timer()
	20885	20:05:27:520 2015/11/13	MOD_NIL		TRACE_INFO	sim_stop_timer() but return out
	20886	20:05:27:520 2015/11/13	MOD_SIM_2	MOD_L4C_2	PS_SIM_SAP	MSG_ID_SIM_ERROR_IND

B. case 2:判断插入的卡是 SIM1 还是 SIM2

搜索“SIM_RESET_ERROR”，

当 SIM_RESET_ERROR: DCL_USIM_NO_INSERT 表示没有插入卡

当 SIM_RESET_ERROR: DCL_USIM_NO_ERROR 表示识卡正常无误

红框内表示 SIM1 此时识卡正常，若是 SIM2 正常是卡会显示 MOD_SIM_2

Type	Index	Local Time	Source	Destination	SAP	Message
	14444	20:04:23:305 2015/11/13	MOD_CCCIRPC		TRACE_INFO	[CCCI_RPC] ccci_rpc_receive_cb event wakeup:0
	14445	20:04:23:305 2015/11/13	MOD_CCCIRPC		TRACE_INFO	[CCCI_RPC] IPC_RPC_Process_CMD PASS
	14446	20:04:23:305 2015/11/13	MOD_CCCIRPC		TRACE_INFO	[CCCI_RPC] IPC_RPC_CCCI_Read START
	14447	20:04:23:305 2015/11/13	MOD_CCCIRPC		TRACE_INFO	[CCCI_RPC] CCCI Header 0 0X28 0XE0021 0
	14448	20:04:23:305 2015/11/13	MOD_CCCIRPC		TRACE_INFO	[CCCI_RPC] RPC Header OPID=0XFFFF4005 NUM_PARA=0X2
	14449	20:04:23:305 2015/11/13	MOD_CCCIRPC		TRACE_INFO	[CCCI_RPC] IPC_RPC_CCCI_Read PASS
	14450	20:04:23:305 2015/11/13	MOD_CCCIRPC		TRACE_INFO	[CCCI_RPC] IPC_RPC_Wrapper PASS
	14451	20:04:23:305 2015/11/13	MOD_SIM_DRV		TRACE_INFO	EINT: 0, 0 0 10 0 0 1
	14452	20:04:23:305 2015/11/13	MOD_SIM_DRV		TRACE_INFO	EINT: MD1_SIM1_HOT_PLUG_EINT
	14453	20:04:23:305 2015/11/13	MOD_SIM		TRACE_INFO	SIM_RESET_ERROR: DCL_USIM_NO_ERROR
	14454	20:04:23:305 2015/11/13	MOD_SIM		TRACE_GROUP_3	SIM_SELECT : length: 8
	14455	20:04:23:305 2015/11/13	MOD_SIM		TRACE_GROUP_3	APDU_tx 0: 00 A4 08 04 02 2F E2 00 F2 F2 F2 F2 F2 F2 F2 46
	14456	20:04:23:305 2015/11/13	MOD_SIM_DRV		TRACE_INFO	L1sim_Cmd_Layer_MTK(0) P3=2 txSize=8, rxData!=NULL, *rxSize=256
	14457	20:04:23:305 2015/11/13	MOD_SIM_DRV		TRACE_INFO	[MOD_SIM_DRV] CMD header: 0 a4 8 4 2, txSize:7, rxSize:0
	14458	20:04:23:305 2015/11/13	MOD_CCCIRPC		TRACE_INFO	[CCCI_RPC] ccci_rpc_receive_cb PASS
	14459	20:04:23:305 2015/11/13	MOD_CCCIRPC		TRACE_INFO	[CCCI_RPC] ccci_rpc_send_cb START
	14460	20:04:23:305 2015/11/13	MOD_CCCIRPC		TRACE_INFO	[CCCI_RPC] ccci_rpc_send_cb PASS
	14461	20:04:23:505 2015/11/13	MOD_DHL		TRACE_INFO	[L2] flush from 1
	14462	20:04:23:505 2015/11/13	MOD_DHL		TRACE_INFO	[L2] flush 1-1

二、Register（注册网络）

(一)　开机搜网流程

开机搜网的过程主要分为两部分，第一部分主要是切换成飞行模式，读取 SIM 卡，第二部分从 command: AT+EFUN=1 开始，表明关闭飞行模式，开启搜网过程。

第一部分：处于飞行模式下，无与网络交互的内容，主要是读取 SIM 卡，包括读取 IMSI,读取 PLMN，BA list，判断是否是同一张卡，等等

```
[RRM] RPLMN: 46000f
[RRM] Read SCSI data...
[RRM] BA list in SCSI exist!
[RRM] Read EF-BCCH in SIM and init to SCSI
[RRM] SIM status: RRM_SIM_IS_READY
MSG_ID_SIM_MM_READY_IND
[ENS] HPLMN: 460000
[ENS] HPLMN search period: 480 minutes
[MM] MM_PLMNSEL[0]: 46000f , RAT_NONE
[MM] MM_PLMNSEL[1]: 46002f , RAT_NONE
[MM] MM_PLMNSEL[2]: 52501f , RAT_NONE
gsm update status is set to MM_U1_UPDATED
gprs update status is set to GU1_UPDATED
[MM] RPLMN: 46000f, RAT_GSM; Previous RPLMN: ffffff, RAT_NONE
```

从上面的 LOG 可以看出，RPLMN 为 46000F，Hplmn 为 46000，PLMNSEL:手机端维持的 PLMN 列表，为 46000 和 46002，所以第一部分主要确定了 PLMN 的优先级列表，如果没更换 SIM 卡，则优先级为：RPLMN HPLMN EHPLMN PLMNSEL，当更换了 SIM 卡时，RPLMN 和 PLMNSEL 无效，具体还有很多种类型，关于 PLMN 的优先级可以网上搜索下，第一部分确定了需要搜索的 PLMN 列表之后，第二部分开始搜索网络。

这里没更换 SIM 卡，BA 表有效：

1. 先确定 PLMN 优先级

MM new State: MM_IDLE_PLMN_SEARCH

[MM] RESET_PLMN_SEARCH_LIST

在这之后会按照优先级打印出可以注册的 PLMN 列表

```
MM new State: MM_IDLE_PLMN_SEARCH
[MM] RESET_PLMN_SEARCH_LIST
[MM] RPLMN source: MM_VALID_RPLMN
[MM] PLMN_SEARCH_LIST_TYPE MM_LIST_AUTO_POWER_ON_RECOVERY
[MM] PLMN_SEARCH_LIST 0, 46000f , RAT_GSM , MM_NOT_SEARCHED , RAT_UMTS , MM_NOT_SEARCHED , KAL_TRUE
[MM] PLMN_SEARCH_LIST 1, 460000 , RAT_NONE , MM_SEARCHED , RAT_NONE , MM_SEARCHED , KAL_TRUE
[MM] PLMN_SEARCH_INDEX 0, RAT_GSM
MSG_ID_MM_RATCM_PLMN_SEARCH_REQ
MSG_ID_RATCM_GAS_PLMN_SEARCH_REQ
```

点开 MSG_ID_RATCM_GAS_PLMN_SEARCH_REQ，在 plmn_id 项可以看到待搜索的 PLMN 列表

2.测量周边小区强度

由于我们的 BA LIST 是存在的，所以会优先搜索 BA LIST 中保存的频点，需要说明的是，在协议中一般是以 arfcn，也就是频点号为准，一个小区对应一个 arfcn，而不是对应一个 cell id

```
[RCS] PLMN search starting...
[RRM] Read SCSI data...
[RRM] BA list in SCSI exist!
```

测量从 MSG_ID_RR_MPAL_SEARCH_RF_REQ 命令开始，点开该消息能看到所有待测量的 arfcn，

以 MSG_ID_MPAL_RR_SEARCH_RF_CNF 结束，点开消息能看到所有的 arfcn 和其对应的 dbm 值，其中这里测到的 DBM 值和上层 dbm 值为 4 倍的关系，绝对值越小说明信号强度越好

3.按照之前测量的强度从高到底依次尝试同步到该小区

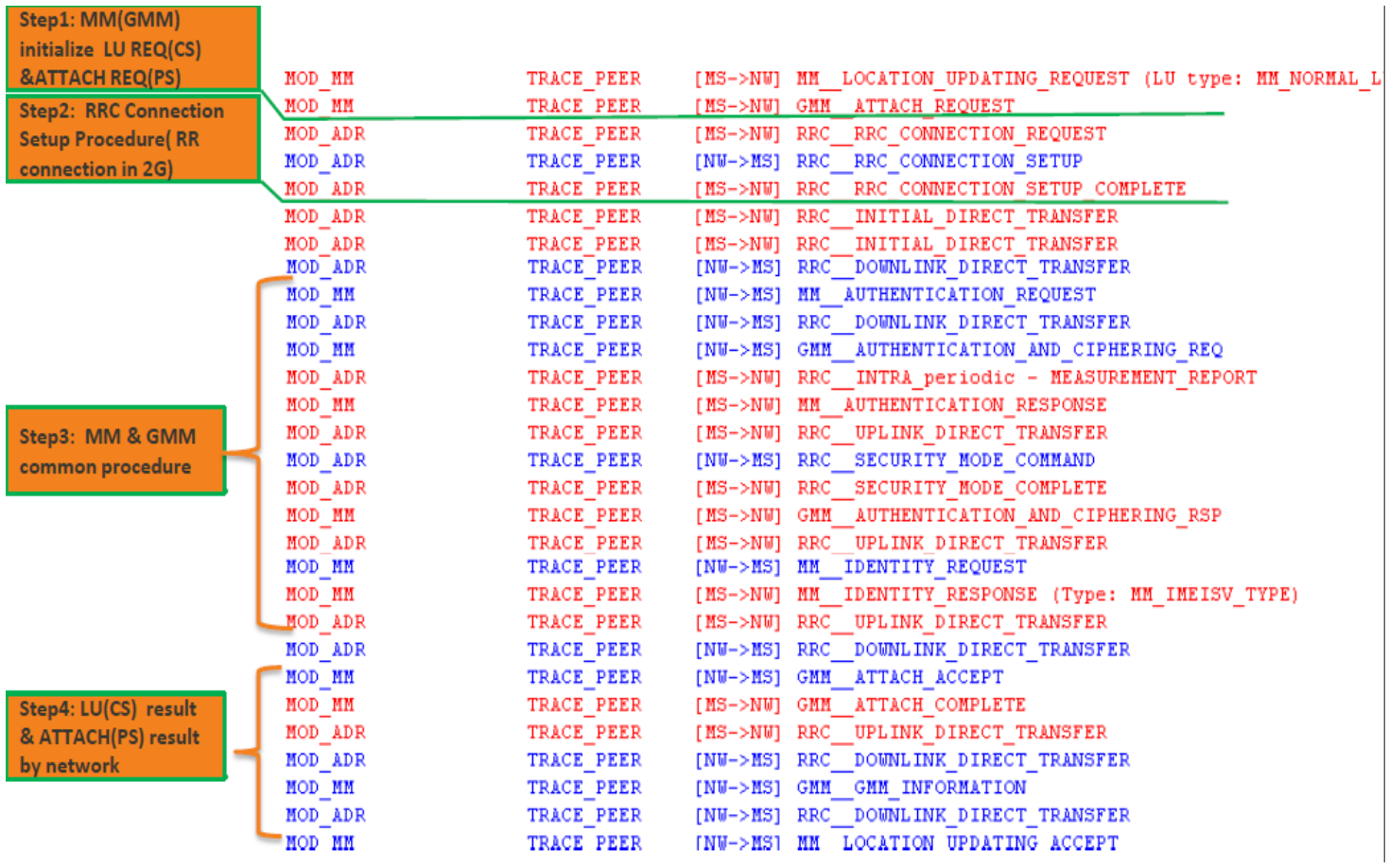
```
[RCS] Need frequency correction
[RCS] There are [8] ARFCNs to try
```

每个 arfcn 的同步都从 MSG_ID_RR_MPAL_BSIC_SYNC_REQ 消息开始，该消息包含了需要同步的 arfcn 号，以 MSG_ID_MPAL_RR_BSIC_SYNC_CNF 结束，这时 UE 主要是执行解析 FCCH 和 SCH 的工作，通过解析 FCCH 调谐到该 ARFCN，然后通过解析 SCH 信道来解析小区的一些信息，包括 BSIC 等

当 UE 成功的解析出 SCH 信道，并且该小区的各项参数满足条件时，UE 选择驻留在该小区，当不满足时，继续解析下一个 arfcn。

至此，小区选择的过程完成，如果手机无法解析出任何 arfcn 的 SCH 信道，手机进入 NO CELL AVAILABEL 状态，此时 UE 无任何可用的无线资源，无法进行紧急呼叫，这种情况一般是与同步相关的天线性能的问题，当手机选择了小区后，MS 进入 ATTEMPTING TO UPDATE 状态，下一步的动作就是尝试在网络上注册。

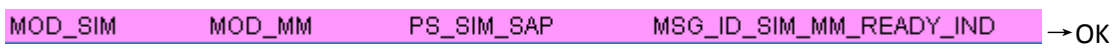
(二)　2G/3G Register



A. Step 1: MM(GMM)initialize LU REQ(CS) &ATTACH REQ(PS)

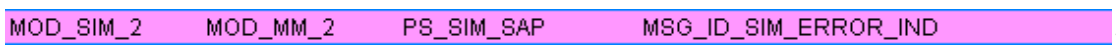
如果没有找到 LU REQ or ATTACH REQ 相关字段:可能 SIM 卡有错误或没有移动网络覆盖。

例：

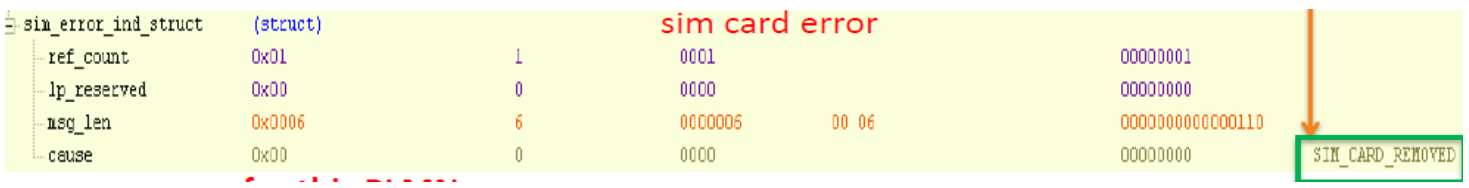


→OK

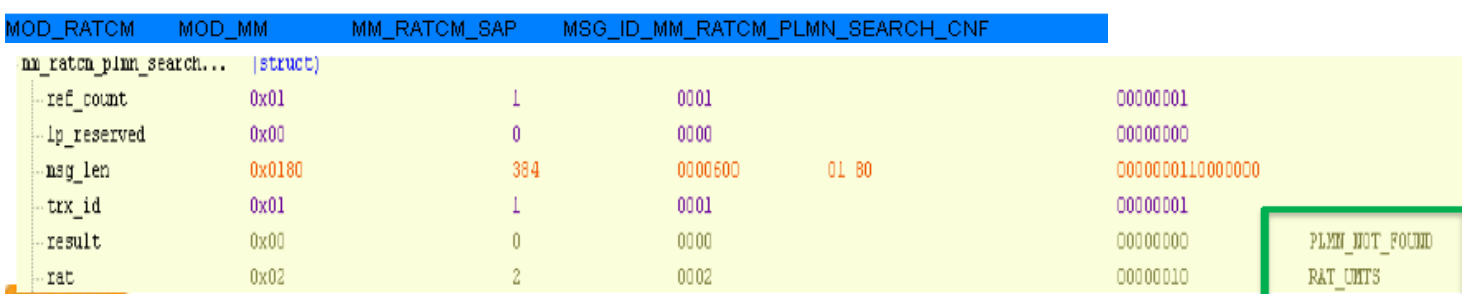
SIM 错误：



→No OK



没有网络覆盖：



B. Step 2: RRC Connection Setup Procedure(or RR connection in 2G)

在 UE 发送 LU REQ or ATTACH REQ 之后, RRC connection (AS)需要连接成功. 如果失败，则可能是由于信号差或是网络拒绝连接。

例：

[NW->MS] RR__IMMEDIATE_ASSIGNMENT 该信令是申请 SDCCH 信道资源的，当发现信令流程中在这一步断了，一般是因为该小区 SDCCH 拥塞造成，不仅是位置更新，在任何专有流程中都有这一步，作用也是一样

For 3G:

```
MOD_ADR TRACE_PEER [MS->NW] RRC__RRC_CONNECTION_REQUEST
MOD_ADR TRACE_PEER [NW->MS] RRC__RRC_CONNECTION_SETUP
MOD_ADR TRACE_PEER [MS->NW] RRC__RRC_CONNECTION_SETUP_COMPLETE
```

For 2G:

```
MOD_RRM TRACE_PEER [MS->NW] RR__CHANNEL_REQUEST
MOD_RRM TRACE_PEER [NW->MS] RR__IMMEDIATE_ASSIGNMENT
```

C. Step 3: MM & GMM common procedure

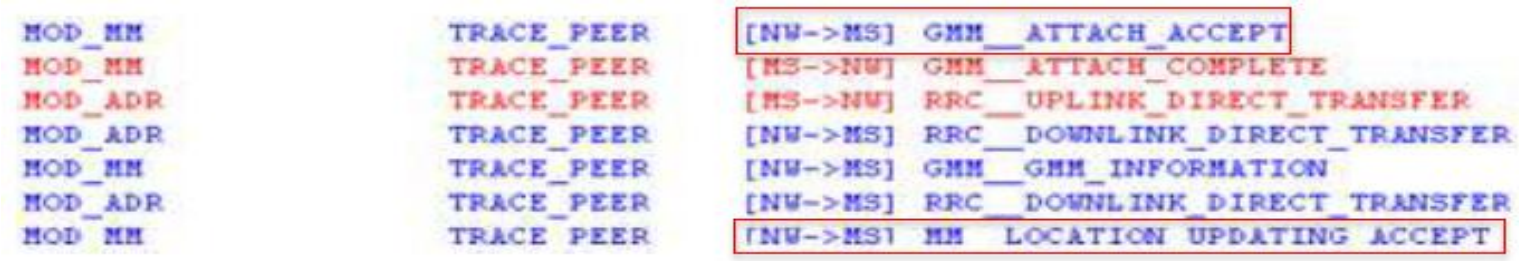
当网络接受 LU 或 ATTACH 请求，网络会检查 UE 身份（如 IMEI，IMSI 等），验证合法 USIM 卡（SIM）卡，如果网络拒绝，则可能原因是 SIM 卡错误或是余额不足，如果同 SIM 卡在对比机中正常请提交 MTK。

[NW->MS] MM__AUTHENTICATION_REQUEST 这就是鉴权操作，UE 从 SIM 卡中读取加密密钥经过加密算法和 MSC 端的数据进行对比，不匹配即为鉴权失败，可以查看鉴权拒绝的 cause。

[NW->MS] MM__IDENTITY_REQUEST 也就是标示流程，在手机没插 SIM 卡，而且也没写 IMEI 时，发起此流程可能会被网络给拒绝，该流程是对 UE IMSI 或者 IMEI 的检查

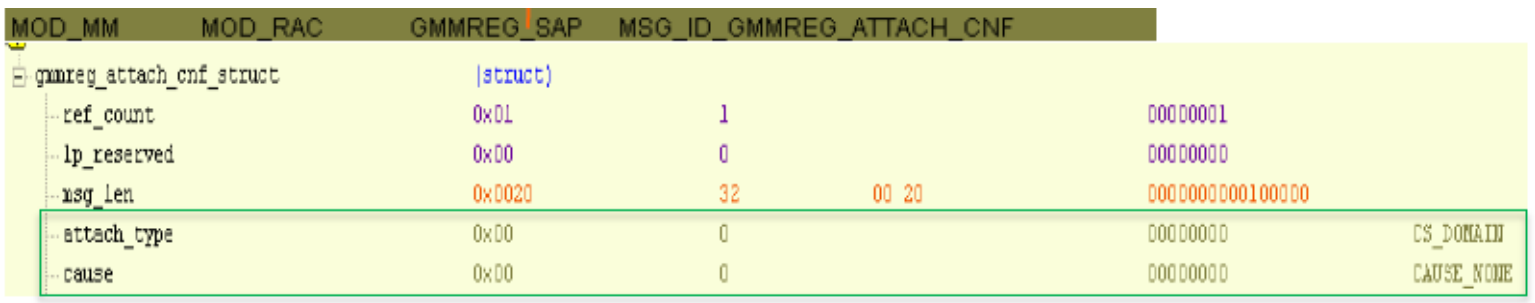
D. Step 4: LU(CS) result & ATTACH(PS) result by network

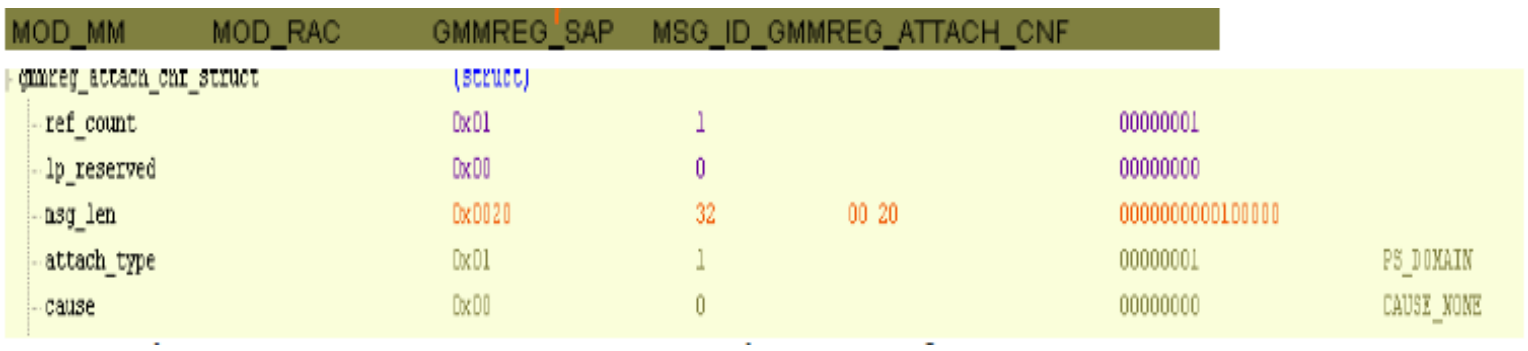
如果网络同意 UE 注册，UE 会接收到来自网络端的 LU ACCEPT and ATTACH ACCEPT 请求。



完成后[NW->MS] RR__CHANNEL_RELEASE 更新完成后释放 radio resources，也即释放 SDCCH 资源

搜索 “GMMREG_ATTACH_CNF”查看 UE 注册状态 CS domain and PS domain，如果 cause= cause_none 则是成功。





E. 案例：注册成功后掉网

a. GPRS 鉴权被拒

从 mdlog 的 system trace 里查看到没写入 IMEI,
Message: IMEI of SIM1:ffffffffffffff0
在 mdlog 的 Trace peer window 查看到 GPRS 鉴权时被拒
MOD_MM TRACE_PEER [NW->MS] GMM__AUTHENTICATION_AND_CIPHERING_REJ

b. 写了 IMEI，但是不合法

在 Location update 时被网络以 Illegal MEI 拒绝，
Frame #: Time: 939835 Local Time: 14:37:43:719 2014/09/11 Message: IMEI of SIM1:865627022306010
MOD_MM TRACE_PEER [NW->MS] MM__LOCATION_UPDATING_REJECT
MOD_MM TRACE_INFO Location Update is rejected with cause ILLEGAL_ME

c. 网络不稳定 redirect

OTA, 803270, 62103, 08:14:01:995, ERRC_CONN, [NW->MS] ERRC_RRCConnectionRelease(cause:[ReleaseCause_other], redirectInfo:[1]),
OTA, 804965, 62281, 08:14:02:795, MM, [MS->NW] MM__LOCATION_UPDATING_REQUEST (LU type: MM_NORMAL_LU)

d. 切换网络数据卡后，会掉网。

这个是 google 在 L 上的设计，3G/4G 能力会跟着 default data sim 设置，即默认数据设在哪张卡上，3/4G 能力就切到那张卡上去。所以切换数据卡不仅是切换默认数据在哪张卡上，同时也会设置 3/4G 能力在哪张卡上，当 3/4G 能力切换之后，便会进行 modem reset，这个过程才算完成。Google 这样设计的目的是为了是数据卡更好的享有网络。

该设计可以由 MTK_DISABLE_CAPABILITY_SWITCH 宏控制，现在项目上默认为 no，MTK_DISABLE_CAPABILITY_SWITCH=yes 那么 3/4G 能力只在一张卡上（双卡下默认卡 1 不能随数据卡变化而变，一张卡没有区别）,切换数据不会搜网。

具体 AP 端 log 可查询 radio_log：

22:15:30.394 1400 5339 D SubscriptionController: [setDefaultDataSubId] subId=2//设置默认卡 subid 是指设置的 sim 的 id 由系统生成
22:15:30.432 5285 5295 I RIL : requestSetRadioCapability resetRadio//重启 modem
22:15:43.456 1400 1531 I RILJ : (0) Connected to 'rild' socket// modem 重启成功
22:15:45.916 11992 11996 D AT : AT> AT+EFUN=3// sim 卡恢复正常模式
22:15:54.471 11992 12014 D AT : AT< +COPS: 0,2,"64003"
22:16:01.200 11992 12008 D AT : AT< +COPS: 0,2,"64004"//对应网络注册成功

+COPS:<mode>[,<format>[,<oper>]]

<mode>

0：自动模式（缺省值）；

1：手动模式；

2：撤销注册，ME 在选择了<mode>=或<mode>=1 后才能撤销注册；

3：仅用于设置<format>参数；

4：手动/自动参数<oper>的格式。

<format>：试着参数<的格式>。

0：短字母型；

1：短字母型；

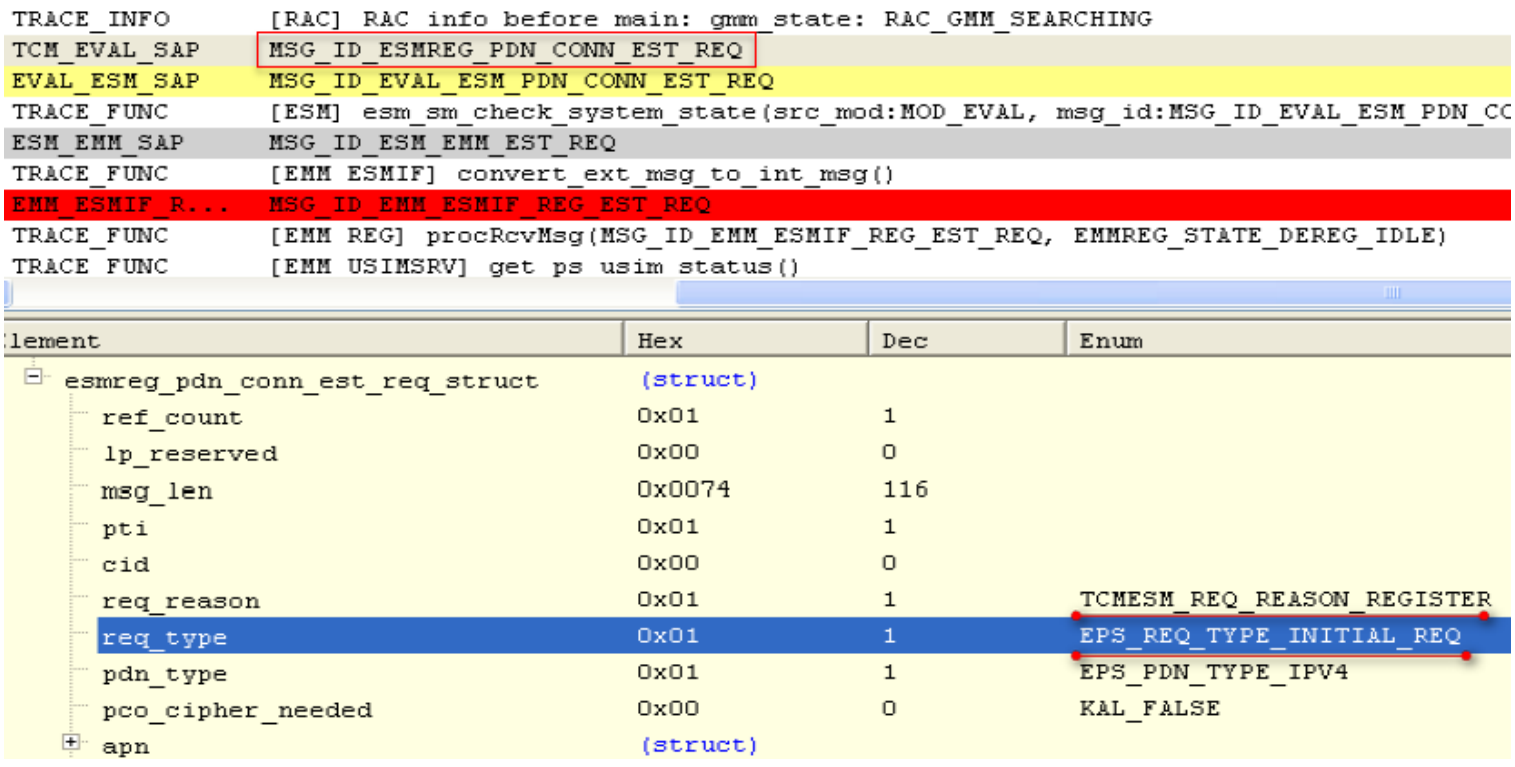
2：数字型（缺省值）。

<oper>：运营商标识（仅可选择数字格式的 MCC/MNC 运营商）。

(三) 4G Register

A. Step 1: Initialize PDN CONN REQ/Attach REQ

UE 在发送 NAS（(PDN CONN REQ/Attach REQ)）请求前，需要确保一切条件都符合 4G 要求，如果搜索不到“MSG_ID_ESMREG_PDN_CONN_EST_REQ”，则可能是由于 UE 找不到合适的网络环境。



B. Step 2: RRC Connection setup procedure

UE 开始发送连接请求时需要确保 UE 的 RRC 连接建立成功。如果找不到可能是信号强度差或是网络拒绝或释放了 RRC 连接。

```
Message
[NW->MS] ESM MSG PDN CONNECTIVITY REQUEST (PTI:1, EBI:0)
[MS->NW] ERRC_RRCConnectionRequest
[NW->MS] ERRC_RRCConnectionSetup
[MS->NW] EMM_Attach_Request(EPS attach type="EMM_ATTACH_TYPE_COMBINED_ATTACH")
[MS->NW] ERRC_RRCConnectionSetupComplete
[NW->MS] ERRC_DLInformationTransfer
```

C. Step 3: EMM Common procedure

在 UE 发送连接请求 NAS message (Attach Request)时，网络会检查 UE 身份（如 IMEI，IMSI 等），验证合法 USIM 卡（SIM）卡，如果网络拒绝则可能原因是 SIM 卡错误或是余额不足，如果同 SIM 卡在对比机中正常请提交 MTK。

```
Message
[MS->NW] EMM_Attach_Request(EPS attach type="EMM_ATTACH_TYPE_COMBINED_ATTACH")
[NW->MS] EMM_Identity_Request(identity type="D_EMM_ID_TYPE_IMSI")
[MS->NW] EMM_Identity_Response
[NW->MS] EMM_Authentication_Request
[MS->NW] EMM_Authentication_Response
[NW->MS] EMM_Security_Mode_Command
[MS->NW] EMM_Security_Mode_Complete
[NW->MS] EMM_Attach_Accept(EPS attach result="EMM_ATTACH_RESULT_COMBINED_ATTACHED")
```

D. Step 4: PDN Activation Result Judgment by NW

UE 完成 EMM 普通流程后，网络将决定 UE 是否成功激活 PDN，如果无法找到“Activate Default EPS Bearer Context Request”或 UE 接收到“PDN CONN Reject”，则可能是 PDN 配置错误，请提交 MTK。

```
Message
[NW->MS] EMM_Security_Mode_Command
[MS->NW] EMM_Security_Mode_Complete
[NW->MS] EMM_Attach_Accept(EPS attach result="EMM_ATTACH_RESULT_COMBINED_ATTACHED")
[NW->MS] ESM_MSG_ACTIVATE_DEFAULT_EPS_BEARER_CONTEXT_REQUEST (PTI:1, EBI:5)
[NW->MS] ESM_MSG_ACTIVATE_DEFAULT_EPS_BEARER_CONTEXT_ACCEPT (PTI:0, EBI:5)
[MS->NW] EMM_Attach_Complete
```

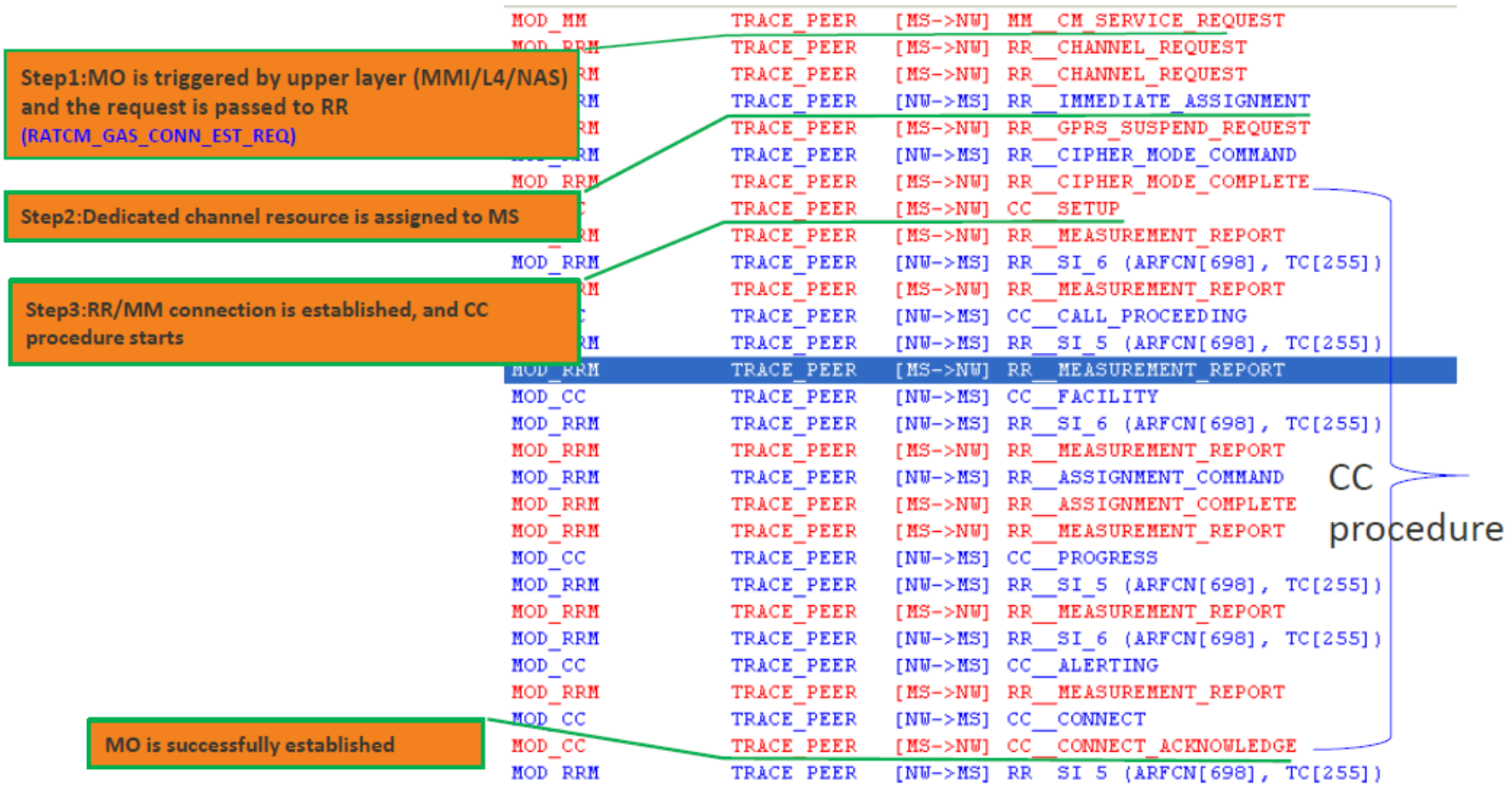
E. Step 5: Attach Result Judgment by UE

UE 完成 EMM 普通流程后，网络会决定是否允许用户访问，如果网络拒绝，可能是网络错误或是配置错误，如果对比机正常请提交 MTK。

```
Message
[EMM SEC] >> CEmmSec::chkRcvMsgType()
[EMM NASMSG] proc_HeadMsg_Plain()
[EMM NASMSG] dispatchEmmMsg()
[NW->MS] EMM_Attach_Reject(EMM cause="EMM_CAUSE_NO_SUITABLE_CELL_IN_TA")
[EMM NASMSG] snd_RcvAttachRejectInd()
MSG_ID_EMM_NASMSG_REG_RCV_ATTACH_REJECT_IND
[EMM NASMSG] freeAndInitRcvNASmsgListOnce()
[EMM NASMSG] proc_FollowingMsg()
[EMM NASMSG] IDLE
[EMM REG] procRcvMsg(MSG_ID_EMM_NASMSG_REG_RCV_ATTACH_REJECT_IND, EMMREG_S
[EMM NMSRV]  decodeAttachReject
[EMM REG] ATTACH-REJECT decode result = D_EMM_DEC_SUC
[EMM REG] ATTACH-REJECT cause 15
[EMM TIMER] TIMER ID: EMM_T3410 is stopped by EMM
```

三、MO Call（主叫）

(一)　2G MO Call



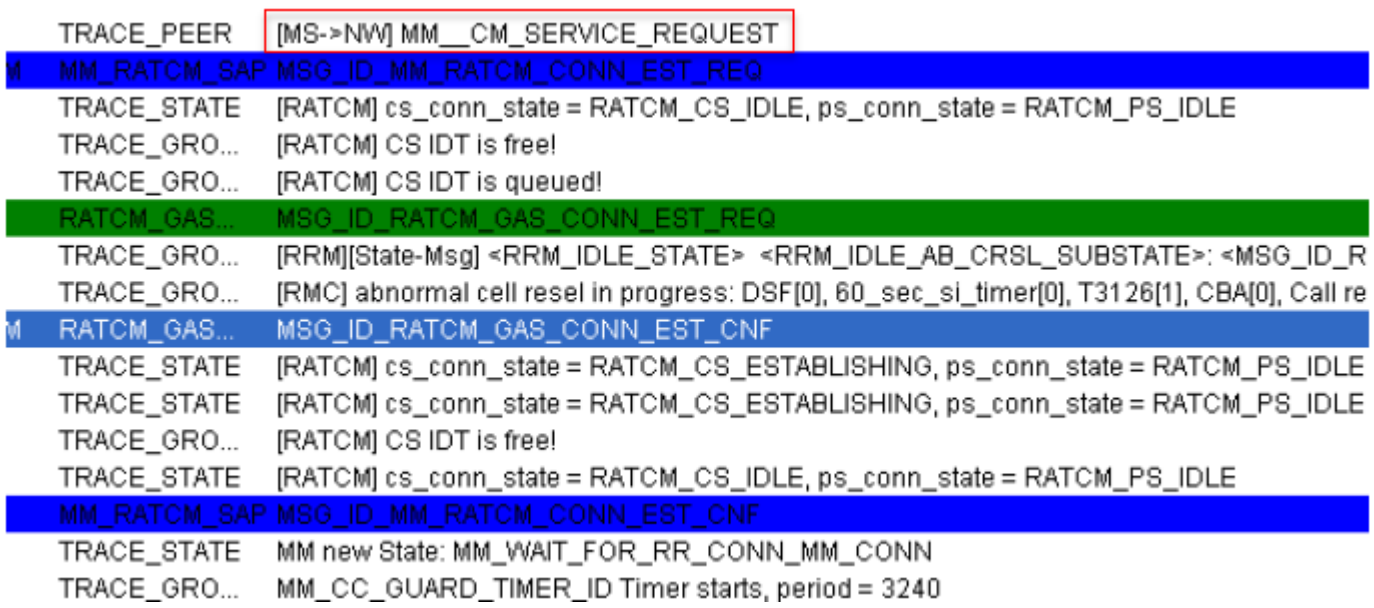
大致的 MO 端通话流程：

MOD_MM, , TRACE_PEER, [MS->NW] MM__CM_SERVICE_REQUEST 手机建立呼叫请求
MOD_RRM, , TRACE_PEER, [MS->NW] RR__CHANNEL_REQUEST 2G频道请求
MOD_MM, , TRACE_PEER, [NW->MS] MM__AUTHENTICATION_REQUEST 网络验证请求
MOD_MM, , TRACE_PEER, [MS->NW] MM__AUTHENTICATION_RESPONSE 手机回应请求
MOD_MM, , TRACE_PEER, [NW->MS] MM__CM_SERVICE_ACCEPT 网络接受呼叫
MOD_CC, , TRACE_PEER, [MS->NW] CC__SETUP 呼叫建立
MOD_CC, , TRACE_PEER, [NW->MS] CC__CALL_PROCEEDING 网络相应呼叫
MOD_CC, , TRACE_PEER, [NW->MS] CC__ALERTING 网络发信号
MOD_CC, , TRACE_PEER, [NW->MS] CC__CONNECT 网络建立通话
MOD_CC, , TRACE_PEER, [MS->NW] CC__CONNECT_ACKNOWLEDGE 手机应答
MOD_CC, , TRACE_PEER, [NW->MS] CC__DISCONNECT 网络断开
MOD_CC, , TRACE_PEER, [MS->NW] CC__RELEASE 手机释放通话
MOD_CC, , TRACE_PEER, [NW->MS] CC__RELEASE_COMPLETE 网络彻底释放
MOD_RRM, , TRACE_PEER, [NW->MS] RR__CHANNEL_RELEASE 2G频段释放通话

A.　Step 1: CM SERVICE REQUEST

a.　搜索“CM_SERVICE_REQUEST”

如果没有找到，但 log 中包含 MSG_ID_MMCC_EST_REJ，一般是由于信号差，或者不在网络覆盖范围内，如果对比机正常请提交 MTK。



b.　未呼通的几种 case

如果 MO 端在通话建立时，MT 端在做以下动作，则未呼通属于网络原因。

1).LU

10:21:32:030 2015/08/20, MOD_MM, TRACE_PEER,[MS->NW] MM__LOCATION_UPDATING_REQUEST (LU type: MM_NORMAL_LU)　手机端发出 LU 请求

10:21:33:430 2015/08/20, MOD_MM, TRACE_PEER,[NW->MS] MM__LOCATION_UPDATING_ACCEPT 网络端接受请求

2).TAU

10:08:45:500 2015/08/20, MOD_EMM_NASMSG, TRACE_PEER,[MS->NW] EMM_Tracking_Area_Update_Request(EPS update type="EMM_UPDATE_TYPE_COMBINED_TAU", active flag="KAL_FALSE") 手机端发出跟踪区更新;位置更新

10:08:46:100 2015/08/20, MOD_EMM_NASMSG, TRACE_PEER,[NW->MS] EMM_Tracking_Area_Update_Accept(EPS update result="EMM_UPDATE_RESULT_COMBINED_UPDATED") 网络端接受请求

3).Detach

10:44:58:980 2015/08/20, MOD_EMM_NASMSG, TRACE_PEER,[NW->MS] EMM_Detach_Request(Detach type="MT_REATTACH_NOT_REQUIRED", EMM cause="(-14)") 网络端发出断开请求，一般是由于信号差

10:44:58:980 2015/08/20, MOD_EMM_NASMSG, TRACE_PEER,[MS->NW] EMM_Detach_Accept 手机端接受断开

B. Step 2: RA and immediate assignment

搜索“RR_IMMEDIATE_ASSIGNMNET”和“MSG_ID_RATCM_GAS_CONN_EST_CNF”且结果 result = “AS_CONN_EST_SUCC”

```
MOD_MM      [MS->NW] MM__CM_SERVICE_REQUEST
MOD_RRM     [NW->MS] RR__IMMEDIATE_ASSIGNMENT
MOD_RRM     [MS->NW] RR__CLASSMARK_CHANGE
MOD_RRM     [MS->NW] RR__GPRS_SUSPEND_REQUEST
MOD_MM      [NW->MS] MM__IDENTITY_REQUEST
MOD_MM      [MS->NW] MM__IDENTITY_RESPONSE (Type: MM_IMEI_TYPE)
MOD_RRM     [MS->NW] RR__MEASUREMENT_REPORT
MOD_MM      [NW->MS] MM__CM_SERVICE_ACCEPT
MOD_CC      [MS->NW] CC__SETUP
MOD_RRM     [MS->NW] RR__MEASUREMENT_REPORT
MOD_CC      [NW->MS] CC__CALL_PROCEEDING
```

C. Step 3: CM connection setup

在完整窗口搜索“MM_CONN_ACTIVE”，如果有则网络发送寻呼电话。

```
MM_RATCM_SAP  MSG_ID_MM_RATCM_CS_DATA_IND
TRACE_PEER    [NW->MS] MM__CM_SERVICE_ACCEPT
MM_CC_SAP     MSG_ID_MMCC_EST_CNF
TRACE_GRO...  MM_T3230_TIMER_ID Timer stopped
TRACE_STATE   MM new State: MM_CONN_ACTIVE
TRACE_INFO    ILM RECEIVED: MESSAGE ID=624
TRACE_PEER    [MS->NW] CC__SETUP
MM_CC_SAP     MSG_ID_MMCC_DATA_REQ
MM_RATCM_SAP  MSG_ID_MM_RATCM_CS_DATA_REQ
TRACE_STATE   [RATCM] cs_conn_state = RATCM_CS_ESTABLISHED, ps_conn_state = RATCM_PS_IDLE
```

D. Step 4: RR assignment for the call

搜索“RR_ASSIGNMENT_COMPLETE”，如找到则 TCH 设置成功。

```
MOD_CC      [NW->MS] CC__CALL_PROCEEDING
MOD_RRM     [MS->NW] RR__MEASUREMENT_REPORT
MOD_RRM     [NW->MS] RR__ASSIGNMENT_COMMAND
MOD_RRM     [MS->NW] RR__ASSIGNMENT_COMPLETE
MOD_RRM     [MS->NW] RR__MEASUREMENT_REPORT
MOD_RRM     [MS->NW] RR__MEASUREMENT_REPORT
MOD_CC      [NW->MS] CC__ALERTING
```

(二) 3G MO Call

MO is triggered by upper layer (MMI/L4/NAS) and the request is passed to RRC (RATCM_RRCE_CONN_EST_REQ)

CS signaling connection setup complete and CC procedure start

CS radio bearer resource allocation

MO call is successfully established

CC procedure

```
MOD_MM    [MS->NW] MM__CM_SERVICE_REQUEST
MOD_SIBE  [NW->MS] RRC_SI_SIB7 (UARFCN:[10738], PSC:[304])
MOD_ADR   [MS->NW] RRC__RRC_CONNECTION_REQUEST
MOD_ADR   [NW->MS] RRC__RRC_CONNECTION_SETUP
MOD_ADR   [MS->NW] RRC__RRC_CONNECTION_SETUP_COMPLETE
MOD_ADR   [MS->NW] RRC__INITIAL_DIRECT_TRANSFER
MOD_ADR   [NW->MS] RRC__MEASUREMENT_CONTROL__setup [1] - INTRA
MOD_ADR   [NW->MS] RRC__SECURITY_MODE_COMMAND
MOD_ADR   [MS->NW] RRC__SECURITY_MODE_COMPLETE
MOD_CC    [MS->NW] CC__SETUP
MOD_ADR   [MS->NW] RRC__UPLINK_DIRECT_TRANSFER
MOD_ADR   [MS->NW] RRC__INTRA_e1A [306] [232] - MEASUREMENT_REPORT
MOD_ADR   [NW->MS] RRC__DOWNLINK_DIRECT_TRANSFER
MOD_MM    [NW->MS] MM__IDENTITY_REQUEST
MOD_MM    [MS->NW] MM__IDENTITY_RESPONSE (Type: MM_IMEISV_TYPE)
MOD_ADR   [MS->NW] RRC__UPLINK_DIRECT_TRANSFER
MOD_ADR   [NW->MS] RRC__ADD PSC [306] [232] - RRC__ACTIVESET_UPDATE
MOD_ADR   [MS->NW] RRC__ACTIVE_SET_UPDATE_COMPLETE
MOD_ADR   [NW->MS] RRC__DOWNLINK_DIRECT_TRANSFER
MOD_CC    [NW->MS] CC__CALL_PROCEEDING
MOD_ADR   [NW->MS] RRC__DOWNLINK_DIRECT_TRANSFER
MOD_CC    [NW->MS] CC__FACILITY
MOD_ADR   [NW->MS] RRC__MEASUREMENT_CONTROL__modify [1] - INTRA
MOD_ADR   [NW->MS] RRC__RADIO_BEARER_SETUP
MOD_ADR   [NW->MS] RRC__MEASUREMENT_CONTROL__setup [2] - UeInternal
MOD_ADR   [MS->NW] RRC__RADIO_BEARER_SETUP_COMPLETE
MOD_ADR   [NW->MS] RRC__DOWNLINK_DIRECT_TRANSFER
MOD_CC    [NW->MS] CC__ALERTING
MOD_ADR   [NW->MS] RRC__DOWNLINK_DIRECT_TRANSFER
MOD_CC    [NW->MS] CC__CONNECT
MOD_CC    [MS->NW] CC__CONNECT_ACKNOWLEDGE
```

A. Step 1: CM service request

通话开始后搜索“RATCM_RRCE_CONN_EST_REQ”和“CM_SERVICE_REQUEST”，如果没找到则搜索“MSG_ID_MMCC_EST_REJ ”，通常大部分原因是由于信号差或是无网络，如果对比机正常则提交 MTK。

MOD_CC	MOD_MM	MM_CC_SAP	MSG_ID_MMCC_EST_REQ
MOD_MM		TRACE_GRO...	CM service rejected because of MM STATE = MM_IDLE_NO_
MOD_MM	MOD_CC	MM_CC_SAP	MSG_ID_MMCC_EST_REJ
MOD_CC		TRACE_STATE	STATE CHANGE: TI=0, STATE=194, AUX STATE=0
MOD_CC		TRACE_INFO	ILM RECEIVED: MESSAGE ID=625
MOD_CC	MOD_CSM	MNCC_SAP	MSG_ID_MNCC_REJ_IND

B. Step 2: RRC connection setup

RRC 需要建立成功。

```
MOD_MM     [MS->NW] MM__CM_SERVICE_REQUEST
MOD_SIBE   [NW->MS] RRC_SI_SIB7 (UARFCN:[10738], PSC:[304])
MOD_ADR    [MS->NW] RRC__RRC_CONNECTION_REQUEST
MOD_ADR    [NW->MS] RRC__RRC_CONNECTION_SETUP
MOD_ADR    [MS->NW] RRC__RRC_CONNECTION_SETUP_COMPLETE
MOD_ADR    [MS->NW] RRC__INITIAL_DIRECT_TRANSFER
```

C. Step 3: CM connection setup

搜索“MM new State: MM_CONN_ACTIVE”，如果没有，则可能是身份验证失败或信号差。

MOD_RATCM	MOD_MM	MM_RATCM_SAP	MSG_ID_MM_RATCM_SECURITY_MODE_COMPLETE_IND
MOD_MM		TRACE_GROUP_1	MM_T3218_TIMER_ID Timer stopped
MOD_MM	MOD_CC	MM_CC_SAP	MSG_ID_MMCC_EST_CNF
MOD_MM		TRACE_GROUP_1	MM_T3230_TIMER_ID Timer stopped
MOD_MM		TRACE_STATE	MM new State: MM_CONN_ACTIVE
MOD_MM	MOD_...	NWSEL_MM_SAP	MSG_ID_NWSEL_MM_EVENT_IND

D. Step 4: RB setup for the call

搜索“MSG_ID_MM_RATCM_SYNC_IND”，此时可能是由于信号差或网络原因造成的。

```
MOD_ADR    [NW->MS] RRC__RADIO_BEARER_SETUP
MOD_ADR    [NW->MS] RRC__MEASUREMENT_CONTROL__setup [2] - UeInternal
MOD_ADR    [MS->NW] RRC__RADIO_BEARER_SETUP_COMPLETE
MM_RATCM_SAP   MSG_ID_MM_RATCM_SYNC_IND
```

ement	Value
Local Parameter	0x18ac74c
mm_ratcm_sync_ind_struct	(struct)
ref_count	0x01 (1)
lp_reserved	0x00 (0)
msg_len	0x000a (10)
cause	UAS_RAB_EST
channel_type	PBCCH
channel_mode	UMTS_RAB_SPEECH

(三) 4G CSFB MO Call

IDLE

```
[MS->NW]ERRC_RRCConnectionRequest
[NW->MS]ERRC_RRCConnectionSetup
[MS->NW] EMM_Extended_Service_Request(service type="MO_CSFB", CSFB response="CSFB_UNUSED")
[MS->NW]ERRC_RRCConnectionSetupComplete
[NW->MS]ERRC_RRCConnectionRelease(cause:[ReleaseCause_other], redirectInfo:[KAL_TRUE])
```

Connected

```
[MS->NW] EMM_Extended_Service_Request(service type="MO_CSFB", CSFB response="CSFB_UNUSED")
[MS->NW] ERRC_ULInformationTransfer
[NW->MS] ERRC_RRCConnectionRelease(cause:[ReleaseCause_other], redirectInfo:[1])
```

LU

CC

```
[MS->NW] MM__LOCATION_UPDATING_REQUEST (LU type: MM_NORMAL_LU)
[MS->NW] RR__CHANNEL_REQUEST
[MS->NW] RR__CHANNEL_REQUEST
[NW->MS] RR__IMMEDIATE_ASSIGNMENT
[NW->MS] RR__SI_6 (ARFCN[610], TC[255])
[MS->NW] RR__CLASSMARK_CHANGE
[MS->NW] RR__GPRS_SUSPEND_REQUEST
[MS->NW] RR__MEASUREMENT_REPORT
[NW->MS] RR__SI_5 (ARFCN[610], TC[255])
[NW->MS] MM__AUTHENTICATION_REQUEST
[MS->NW] RR__MEASUREMENT_REPORT
[MS->NW] MM__AUTHENTICATION_RESPONSE
[NW->MS] RR__SI_5TER (ARFCN[610], TC[255])
[NW->MS] MM__LOCATION_UPDATING_ACCEPT
[MS->NW] MM__CM_SERVICE_REQUEST
[MS->NW] RR__MEASUREMENT_REPORT
[NW->MS] RR__MEASUREMENT_INFORMATION
[NW->MS] MM__CM_SERVICE_ACCEPT
[MS->NW] CC__SETUP
```

- LU is Optional

A. Step 1: Check register result

查找 Attach 或 TAU，确保 attach 结果为 COMBINED_ATTACHED

```
MOD_EMM_NASMSG    [NW->MS] EMM_Attach_Accept(EPS attach result="EMM_ATTACH_RESULT_COMBINED_ATTACHED")
MOD_ESM           [NW->MS] ESM_MSG_ACTIVATE_DEFAULT_EPS_BEARER_CONTEXT_REQUEST (PTI:1, EBI:5)
MOD_ESM           [MS->NW] ESM_MSG_ACTIVATE_DEFAULT_EPS_BEARER_CONTEXT_ACCEPT (PTI:0, EBI:5)

[NW->MS] EMM_Tracking_Area_Update_Accept(EPS update result="EMM_UPDATE_RESULT_COMBINED_UPDATED")
[MS->NW] EMM_Tracking_Area_Update_Complete
```

B. Step 2: MM send CSFB request to EMM

在完整窗口中查找“MM_EMM_CSFB_REQ”，如果没找到提交 MTK。

PS Integrated

Source	Destination	Message
MOD_MM		MM_FN_mm_construct_local_para
MOD_MM	MOD_EMM	MSG_ID_MM_EMM_CSFB_REQ
MOD_EMM_MMIF		[EMM MMIF] convert_ext_msg_to_int_msg()
MOD_EMM_MMIF	MOD_EMM_CALL	MSG_ID_EMM_MMIF_CALL_CSFB_REQ
MOD_EMM_CALL		[EMM CALL] procRcvMsg() : current state =

Bookmark/Comment

All

Type	Index	Time	Local Time	Message
PS	100233	16296	18:14:19:444	[AT_I p2, s5]ATD123;
PS	100305	16296	18:14:19:444	MSG_ID_L4CCSM_CC_CALL_SETUP_REQ
PS	100313	16296	18:14:19:444	MSG_ID_L4CCSM_CC_CALL_INFO_IND
PS	100356	16297	18:14:19:444	MSG_ID_MNCC_SETUP_REQ
PS	100359	16297	18:14:19:444	MSG_ID_MMCC_START_CALL_REQ
PS	100361	16297	18:14:19:444	MSG_ID_MMCC_EST_REQ
PS	100370	16297	18:14:19:444	MSG_ID_MM_EMM_CSFB_REQ
PS	100372	16297	18:14:19:444	MSG_ID_EMM_MMIF_CALL_CSFB_REQ

C. Step 3: RRC connection setup

查找“MS->NW] ERRC_RRCConnectionRequest”，如果没找到，则可能是 RF 未校准。

```
TRACE_PEER      [NW->MS] SystemInformationBlockType1 (EARFCN[38350], PCI[241])
TRACE_PEER      [MS->NW] ERRC_RRCConnectionRequest
TRACE_PEER      [MS->NW] ERRC_RRCConnectionRequest
TRACE_PEER      [MS->NW] ERRC_RRCConnectionRequest
```

D. Step 4: EMM send Extended_service_request

查找“EMM_Extended_Service_Request”。

```
[MS->NW] ERRC_RRCConnectionRequest
[NW->MS] ERRC_RRCConnectionSetup
[MS->NW] EMM_Extended_Service_Request(service type="MO_CSFB", CSFB response="CSFB_UNUSED")
[MS->NW] ERRC_RRCConnectionSetupComplete
[NW->MS] ERRC_RRCConnectionRelease(cause:[ReleaseCause_other], redirectInfo:[KAL_TRUE])
```

E. Step 5: NW Configure UE redirect/handover to 2G or 3G

查找“redirectInfo:[1]”，如果没有，则无法重定向到 2G 网络进行通话,重定向和切换都是由网络决定的，如果对比机正常则提交 MTK。

```
[MS->NW] EMM_Extended_Service_Request(service type="MO_CSFB", CSFB response="CSFB_UNUSED")
[MS->NW] ERRC_ULInformationTransfer
[NW->MS] ERRC_RRCConnectionRelease(cause:[ReleaseCause_other], redirectInfo:[1])
```

→重定向

```
[NW->MS] ERRC_MobilityFromEUTRACommand(CSFB:[1],purpose:[MobilityFromEUTRACommand_r8_IEs_purpose_handover_selected],
[NW->MS] RRC__HANDOVER_TO_UTRAN_COMMAND
[MS->NW] RRC__HANDOVER_TO_UTRAN_COMPLETE
```

→网络切换，流程同 2G/3G

四、MT Call（被叫）

(一)　2G MT call

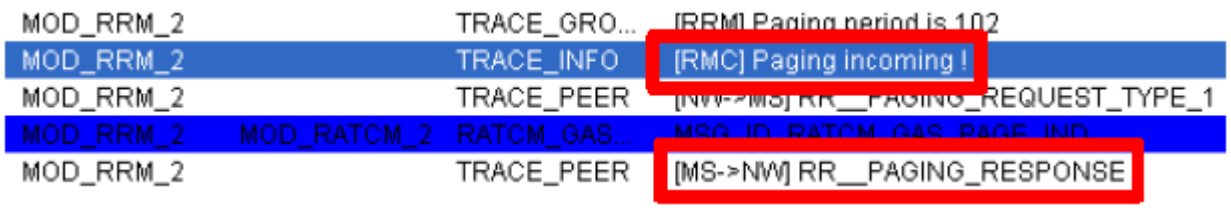
大致被叫流程：

MOD_RRM, , TRACE_PEER, [MS->NW] RR__PAGING_RESPONSE 手机相应网络寻呼
MOD_RRM, , TRACE_PEER, [MS->NW] RR__CHANNEL_REQUEST 2G频道请求
MOD_CC, , TRACE_PEER, [NW->MS] CC__SETUP 呼叫建立
MOD_CC, , TRACE_PEER, [MS->NW] CC__CALL_CONFIRMED 手机确认呼叫
MOD_CC, , TRACE_PEER, [MS->NW] CC__ALERTING 手机发信号
MOD_CC, , TRACE_PEER, [MS->NW] CC__CONNECT 手机建立通话
MOD_CC, , TRACE_PEER, [NW->MS] CC__CONNECT_ACKNOWLEDGE 网络应答
MOD_CC, , TRACE_PEER, [MS->NW] CC__DISCONNECT 手机断开
MOD_CC, , TRACE_PEER, [NW->MS] CC__RELEASE 网络释放
MOD_CC, , TRACE_PEER, [MS->NW] CC__RELEASE_COMPLETE 手机彻底释放
MOD_RRM, , TRACE_PEER, [NW->MS] RR__CHANNEL_RELEASE 2G频段释放通话

A.　Step 1: Receive the paging

搜索“[RMC] Paging incoming !”

当 UE 收到网络的寻呼后发送寻呼响应，如果没有相应 PAGING 请提交 MTK，如果没有收到 paging 则可能手机端正在做 LU，是正常的网络问题。



B.　Step 2: RA and immediate assignment(Same as MO call)

C.　Step 3: CM connection setup(Same as MO call)

D.　Step 4: RR assignment for MT call(Same as MO call)

(二)　3G MT CALL

A. Step 1 :Paging Response

查找“is for this UE”

MOD_ADR	TRACE_GRO...	[AdrUnpack]: The PCCH-Message [type = RRC_PCCH_MessageType_pagingType1_selected,
MOD_ADR	TRACE_PEER	[NW->MS] RRC__PAGING_TYPE1
MOD_ADR	TRACE_GRO...	[AdrUnpack]: Translation result is [decode status = 8, destination process = 5, interpreted even
MOD_RRCE	TRACE_INFO	Paging record 2 not for this UE.
MOD_RRCE	TRACE_INFO	Paging record 1 is for this UE.
MOD_RRCE	TRACE_INFO	CN Paging: CS_DOMAIN, TMSI_TYPE, RRC_PagingCause_terminatingConversationalCall

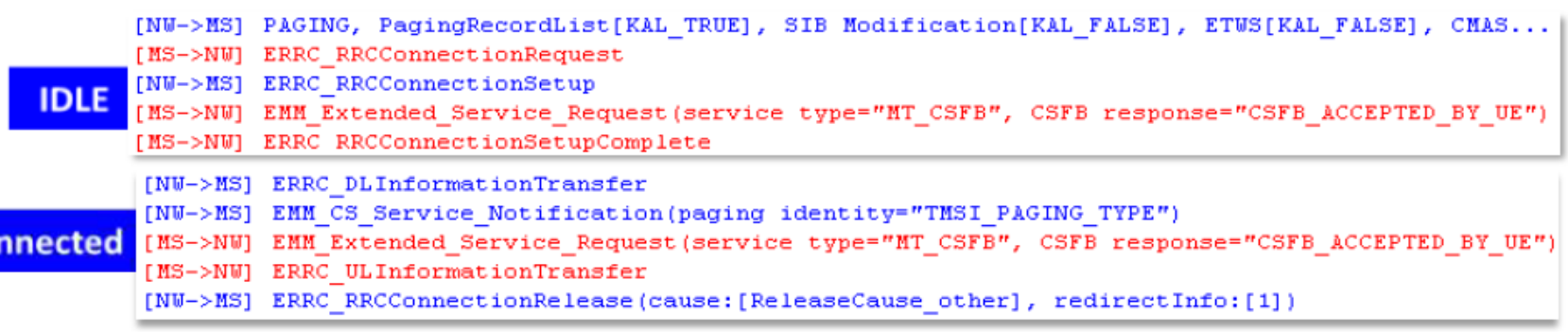
查找“ MM_PAGING_RESPONSE”

MOD_ADR [NW->MS] RRC__PAGING_TYPE1
MOD_MM [MS->NW] MM__PAGING_RESPONSE
MOD_ADR [MS->NW] RRC__RRC_CONNECTION_REQUEST
MOD_ADR [NW->MS] RRC__RRC_CONNECTION_SETUP
MOD_ADR [MS->NW] RRC__RRC_CONNECTION_SETUP_COMPLETE

如果都没有则可能是由于信号差或正在做 LU，以至于错过寻呼，是网络原因。

B. Step 2: RRC connection setup (same as 3G MO CALL)
C. Step 3: CM connection setup (same as 3G MO CALL)
D. Step 4: RB setup (same as 3G MO CALL)

(三) 4G CSFB MT Call



A. **Step 1: Check register result(same as MO case)**
B. **Step 2: Receive paging**

查找“PAGING”,

Idle

```
[NW->MS] PAGING, PagingRecordList[KAL_TRUE], SIB Modification[KAL_FALSE], ETWS[KAL_FALSE], CMAS...
[MS->NW] ERRC_RRCConnectionRequest
[NW->MS] ERRC_RRCConnectionSetup
[MS->NW] EMM_Extended_Service_Request(service type="MT_CSFB", CSFB response="CSFB_ACCEPTED_BY_UE")
[MS->NW] ERRC_RRCConnectionSetupComplete
```

Connected

```
[NW->MS] ERRC_DLInformationTransfer
[NW->MS] EMM_CS_Service_Notification(paging identity="TMSI_PAGING_TYPE")
[MS->NW] EMM_Extended_Service_Request(service type="MT_CSFB", CSFB response="CSFB_ACCEPTED_BY_UE")
[MS->NW] ERRC_ULInformationTransfer
[NW->MS] ERRC_RRCConnectionRelease(cause:[ReleaseCause_other], redirectInfo:[1])
```

C. **Step 3: RRC connection setup(same as MO case)**
D. **Step 4: EMM send Extended_service_request**

查找“EMM_Extended_Service_Request”

```
[NW->MS] ERRC_DLInformationTransfer
[NW->MS] EMM_CS_Service_Notification(paging identity="TMSI_PAGING_TYPE")
[MS->NW] EMM_Extended_Service_Request(service type="MT_CSFB", CSFB response="CSFB_ACCEPTED_BY_UE")
[MS->NW] ERRC_ULInformationTransfer
[NW->MS] ERRC_RRCConnectionRelease(cause:[ReleaseCause_other], redirectInfo:[1])
```

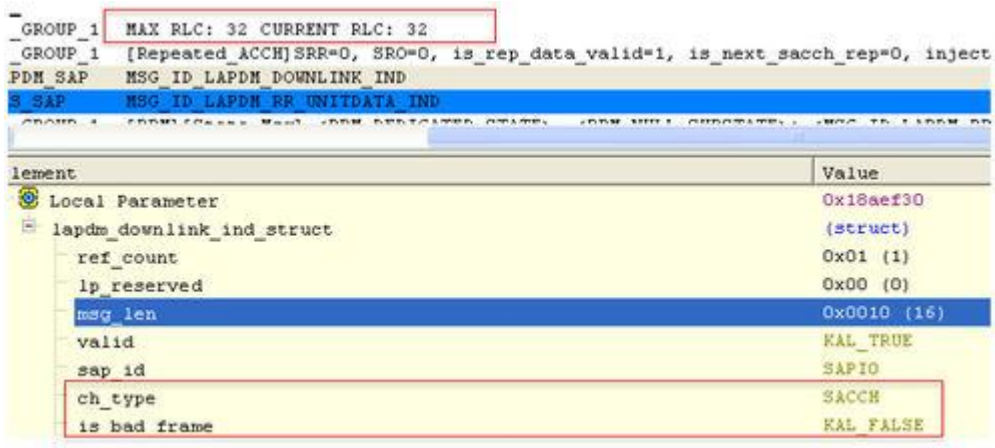
E. **Step 5: NW Configure UE redirect/handover to 2G or 3G(same as MO case)**

五、Call Drop（掉话）

(一)　2G Call Drop

A.　case 1: SACCH/SDCCH 信道解码错误

集成窗口中搜索“MAX RLC”，如果“Current RLC”和“MAX RLC”值不一样，且“Current RLC”值变到 0，通常情况下都是由于信号差引起的。



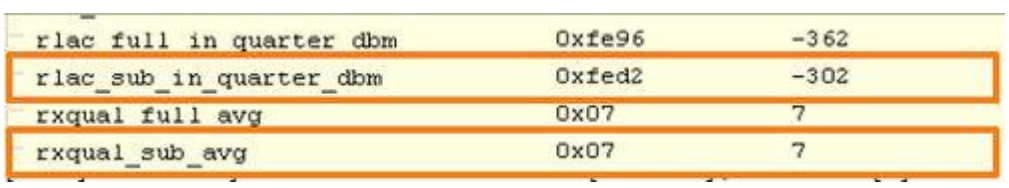
B.　case 2: 网络释放通话

如果手机在没有发送或是接收到“CC_DISCONNECT”但是有“CHANNEL_RELEASE”， 通常此情况下是由于信号差、网络原因引起。

然后继续搜索关键字以确认上述判断：MSG_ID_MPAL_RR_SERV_DEDI_MEAS_IND，

RSSI = rlac_sub_in_quarter_dbm / 4

BER = rxqual_sub_avg (rxqual_full_avg 值的取值为 0---7，如果该值为 7，则掉话是必然的，因为此时接受的坏帧太多，rxqual_full_avg = 0xff，可归为信号差或网络原因



C.　case 3: 弱信号未挂断

搜索“MSG_ID_CPHY_RL_FAILURE_IND”

MOD_TL1, MOD_RRCE, RRCE_TL1_SAP, MSG_ID_CPHY_RL_FAILURE_IND

信号差发生 RLF，这时候 UE 发起 cell update。

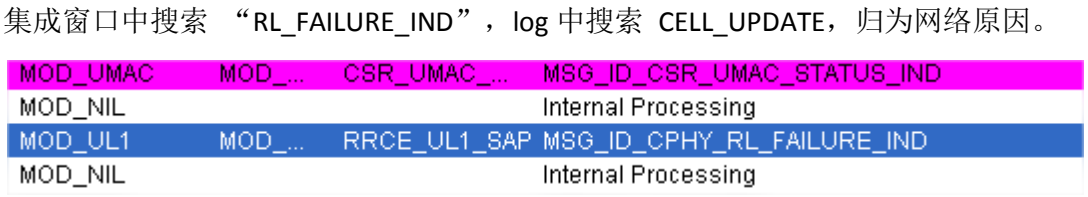
MOD_RRCE, TRACE_INFO, RRCE: Starts the timer RRCE_T314_TIMER_ID for 180 seconds and 0 milliseconds

此计时器为 180s。故这个时间之后电话在界面上才会自动挂断。此为 mtk design。

(二)　3G Call Drop

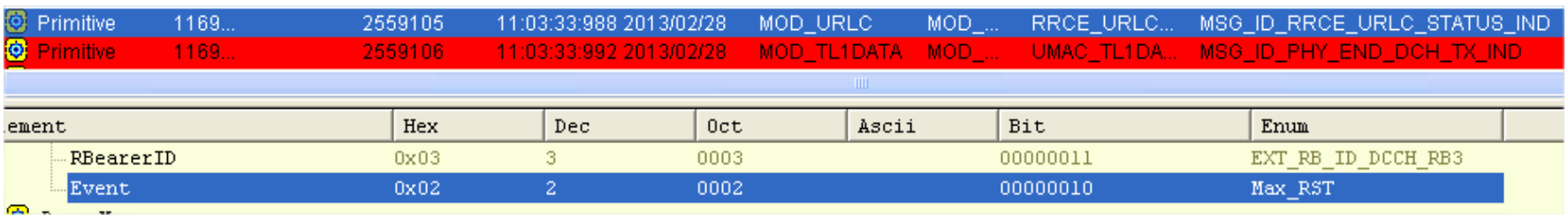
A.　case 1 : Radio Link Failure（无线链路失败）

集成窗口中搜索 “RL_FAILURE_IND”，log 中搜索 CELL_UPDATE，归为网络原因。



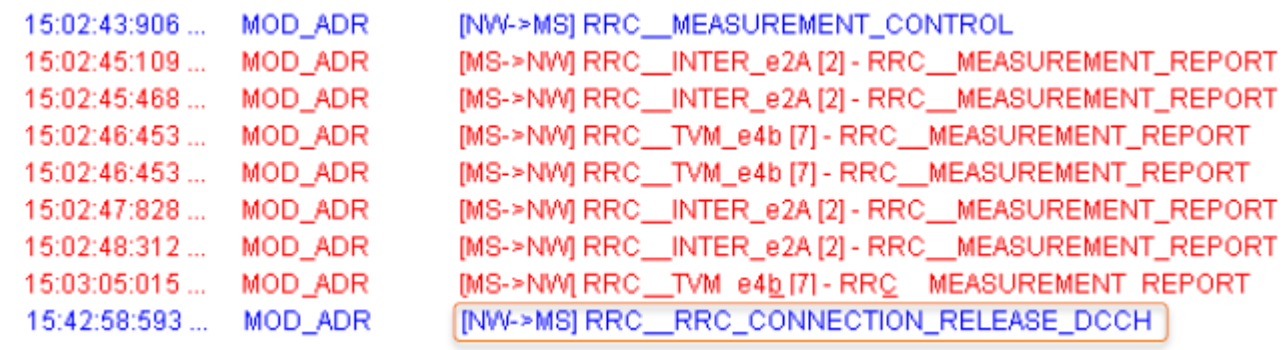
B.　case 2 : CELL_UPDATE - RLC unrecoverable error

集成窗口中搜索 “URLC_STATUS_IND”， log 中搜索 CELL_UPDATE，无线链路控制层协议错误，归为网络原因。

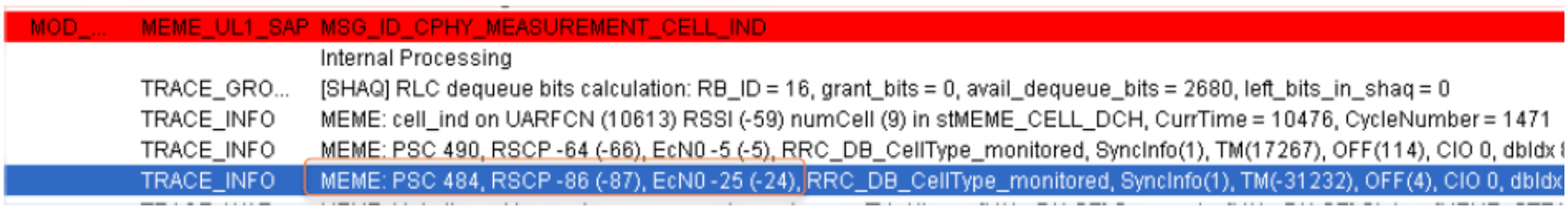


C. case 3: Received RRC connection release when the disconnect procedure is not trigger

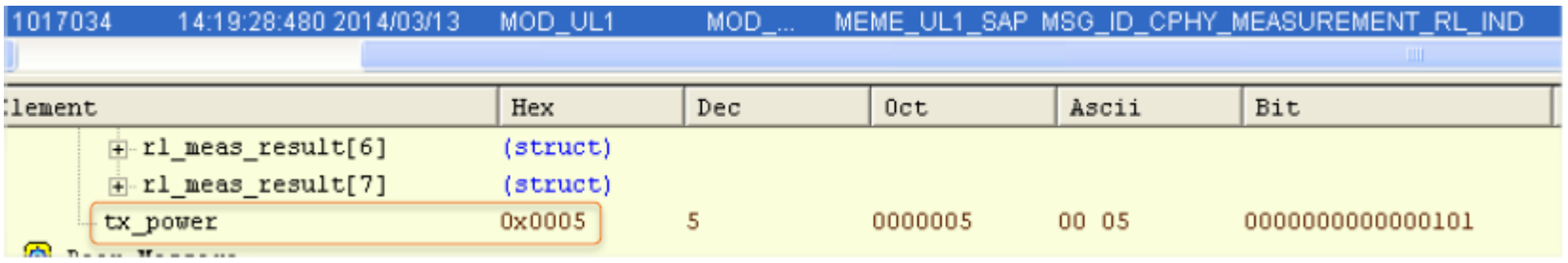
如果没有接收或是挂断的请求且有“RRC_CONNECTOIN_RELEASE”，多是由于网络信号差引起的，然后进行下一步检查确认



检查射频校准和天线性能，射频校准要成功完成，天线性能应符合标准，无问题的话在集成窗口中搜索“RSCP”或是“EcNO”，检查 RLF（无线链路失败）前的信号强度状态。



检查手机的 TX power（发射功率），在集成窗口中搜索“RL_IND”，检查是否达到最大功率。



六、Cell Reselection（小区重选）

小区重选是终端在非 Cell-DCH 状态下完成的小区再选择。当 UE 驻留在小区中时，随着 UE 的移动，当前小区和附近小区的信号强度在不断变化。如果 UE 所在小区的信号质量越来越差，低于某一门限值，UE 就测量其他小区的信号，选择一个更合适的小区。当其他小区的信号强度大于本服务小区的信号强度并且持续一段时间（重选时间），UE 就进行小区的重新选择。这就是小区重选过程。

(一) 2G cell reselection

A. Step 1: neighbor cells list in SI_2

查找“SI_2”，查看小区的 ARFCNs（绝对无线频道编号 （Absolute Radio Frequency Channel Number - ARFCN ））。

Neighbor cell in SI_2

```
MOD_RRM                    TRACE_PEER     [NW->MS] RR__SI_2
GSM CCCH - System Information Type 2
    L2 Pseudo Length
        0101 10.. = L2 Pseudo Length value: 22
    Protocol Discriminator: Radio Resources Management messages
        .... 0110 = Protocol discriminator: Radio Resources Management messages (0x06)
        0000 .... = Skip Indicator: No indication of selected PLMN (0)
    Message Type: System Information Type 2
    Neighbour Cell Description - BCCH Frequency List
        ..0. .... = EXT-IND: The information element carries the complete BA (0)
        ...1 .... = BA-IND: 1
        00.. 000. = Format Identifier: bit map 0 (0x00)
        List of ARFCNs = 72 70 62 61 60 59 57 55 53 51 49
```

B. Step 2: C2 of serving cell and neighbor cell

在集成窗口中查找“MSG_ID_MPAL_RR_SERV_IDLE_MEAS_IND”,查看之后的信息。

C2 of neighbor cell is 600, C2 of serving cell is 544

C2 reselection is trigger, target arfcn is 80

```
MOD_RRM_2   TRACE_GRO...   [RCS] PLMN ID: [46000f] LAI: [25 d3] type: RRM_UNKNOWN_LA
MOD_RRM_2   TRACE_GRO...   [RMC] Nbr arfcn[80]: C1[160], C2[600], GPRS_ind[1], is_the_same_rac_as_serv[1]
MOD_RRM_2   TRACE_GRO...   [RCS] PLMN ID: [46000f] LAI: [25 d3] type: RRM_UNKNOWN_LA
MOD_RRM_2   TRACE_GRO...   [RMC] Nbr arfcn[67]: C1[157], C2[597], GPRS_ind[1], is_the_same_rac_as_serv[1]
MOD_RRM_2   TRACE_GRO...   [RCS] PLMN ID: [46000f] LAI: [25 d3] type: RRM_UNKNOWN_LA
MOD_RRM_2   TRACE_GRO...   [RMC] Nbr arfcn[633]: C1[140], C2[604], GPRS_ind[1], is_the_same_rac_as_serv[1
MOD_RRM_2   TRACE_GRO...   [RCS] PLMN ID: [46000f] LAI: [25 d3] type: RRM_UNKNOWN_LA
MOD_RRM_2   TRACE_GRO...   [RCS] PLMN ID: [46000f] LAI: [25 d3] type: RRM_UNKNOWN_LA
MOD_RRM_2   TRACE_GRO...   [RCS] PLMN ID: [46000f] LAI: [25 d3] type: RRM_UNKNOWN_LA
MOD_RRM_2   TRACE_GRO...   [RMC] rmc_update_cvalues()
MOD_RRM_2   TRACE_GRO...   [RMC] Serv arfcn[635]: RAC[3], C1[64], C2[544]
MOD_RRM_2   TRACE_GRO...   [RMC] Monitoring [2]st nbr_arfcn[65]->counter[2]->C2[559], TBF_exist [TBF_NONE]!
MOD_RRM_2   TRACE_GRO...   [RMC] Monitoring [1]st nbr_arfcn[80]->counter[2]->C2[600], TBF_exist [TBF_NONE]!
MOD_RRM_2   TRACE_GRO...   [RMC] C2_reselection on arfcn = 80
```

C. Step 3: cell reselection perform

在集成窗口中查找“MSG_ID_RR_MPAL_SPECIFIC_SYNC_REQ”、“MSG_ID_RATCM_GAS_SYS_INFO_IND”、“RRM_STATE = RRM_CELL_RESEL_STATE”

reselection target arfcn is 80,arfcn_sync is 80

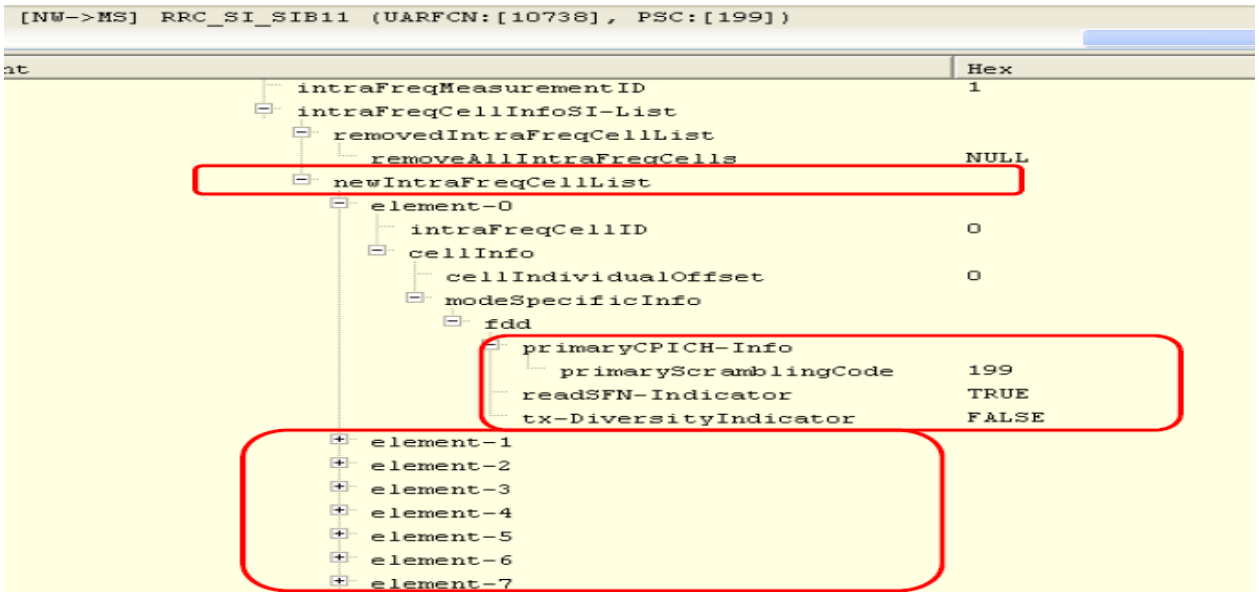
Cell info

```
MOD_RRM_2       TRACE_STATE   RRM_STATE = RRM_CELL_RESEL_STATE
MOD_RRM_2   MOD_MPAL_2   RRM_MPAL_SAP MSG_ID_RR_MPAL_SPECIFIC_SYNC_REQ
  arfcn_sync                0x0050      80
  bsic                      0x0e        14
MOD_RRM_2   MOD_RATCM_2  RATCM_GAS...  MSG_ID_RATCM_GAS_SYS_INFO_IND
- plmn_id                  (struct)
    mcc1                   0x04        4       0004          00000100
    mcc2                   0x06        6       0006          00000110
    mcc3                   0x00        0       0000          00000000
    mnc1                   0x00        0       0000          00000000
    mnc2                   0x00        0       0000          00000000
    mnc3                   0x0f        15      0017          00001111
  cell_id                  0x7c4d      31821   0076115  7c 4d  01111100001001101
  cell_type                0x00        0       0000          00000000  CELL_TYPE_SUITABLE
  access_class             0x0000      0       0000000  00 00  0000000000000000
  cell_support_ps          0x01        1       0001          00000001  KAL_TRUE
  cell_support_cs          0x01        1       0001          00000001  KAL_TRUE
- la_code                  Array [2]               25 d3
    la_code[0]             0x25        37      0045     %    00100101
    la_code[1]             0xd3        211     0323          11010011
```

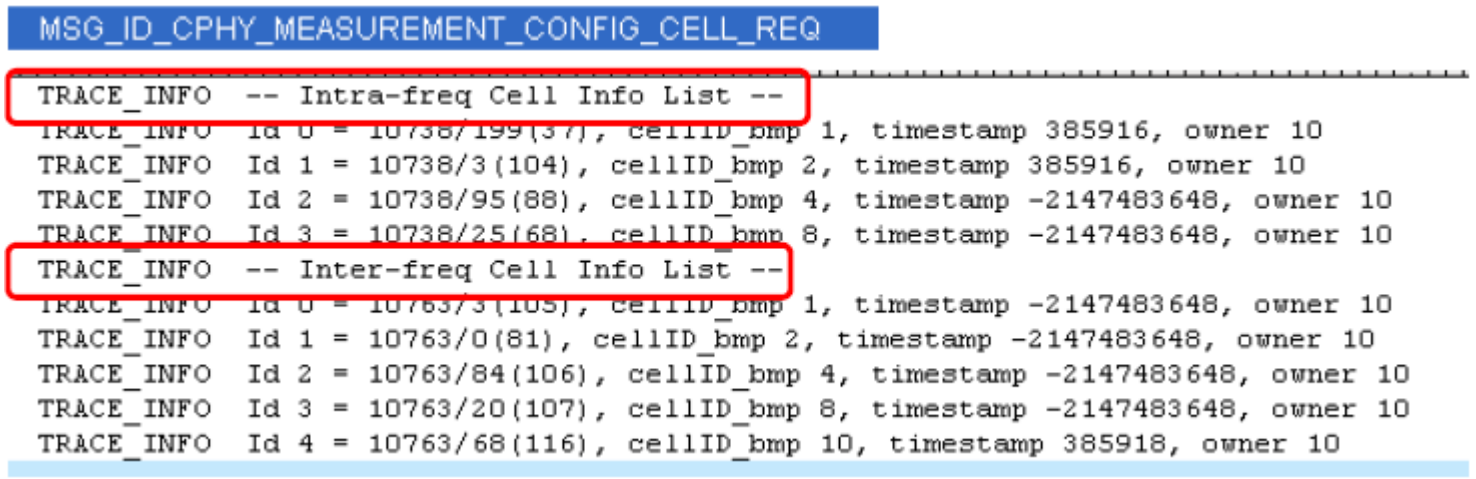
(二) 3G cell reselection

A. Step 1: NW configure 3G neighboring cell

搜索“‘[NW->MS] RRC_SI_SIB11”，



如果没有收到为 SIB11 但已经驻留相邻小区，搜索“MSG_ID_CPHY_MEASUREMENT_CONFIG_CELL_REQ”并检查一下参数。



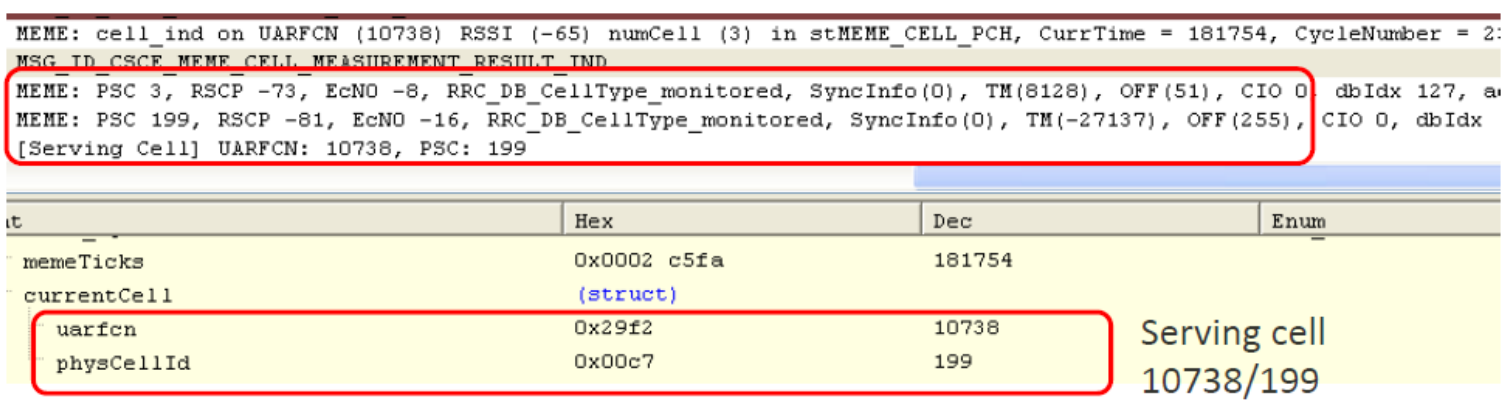
如果找不到为 SIB11 和参数以上，大多数情况下是因为网络问题。

B. Step 2: 3G measurement(intra-f)

搜索“MSG_ID_CSCE_MEME_CELL_MEASUREMENT_RESULT_IND”并查看以下参数，

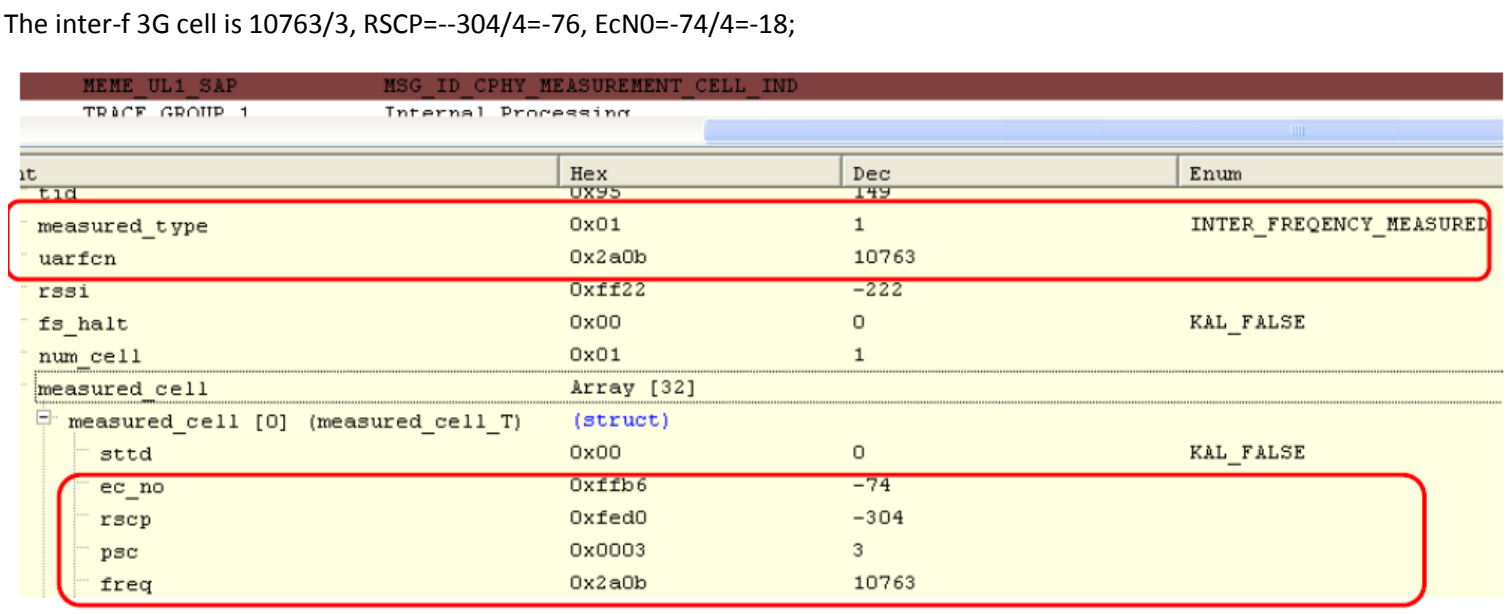
The serving cell is 10738/199, RSCP=-81, EcN0=-16;

The intra-f 3G cell is 10738/3, RSCP=-73, EcN0=-8;



搜索“MSG_ID_CPHY_MEASUREMENT_CELL_IND”并查看以下参数确定信号强度，

The inter-f 3G cell is 10763/3, RSCP=--304/4=-76, EcN0=-74/4=-18;



如果找不到 intra-f 3G cell measurement 且对比机能搜索到，请提交 MTK。

C. Step 3: 3G cell reselection criteria

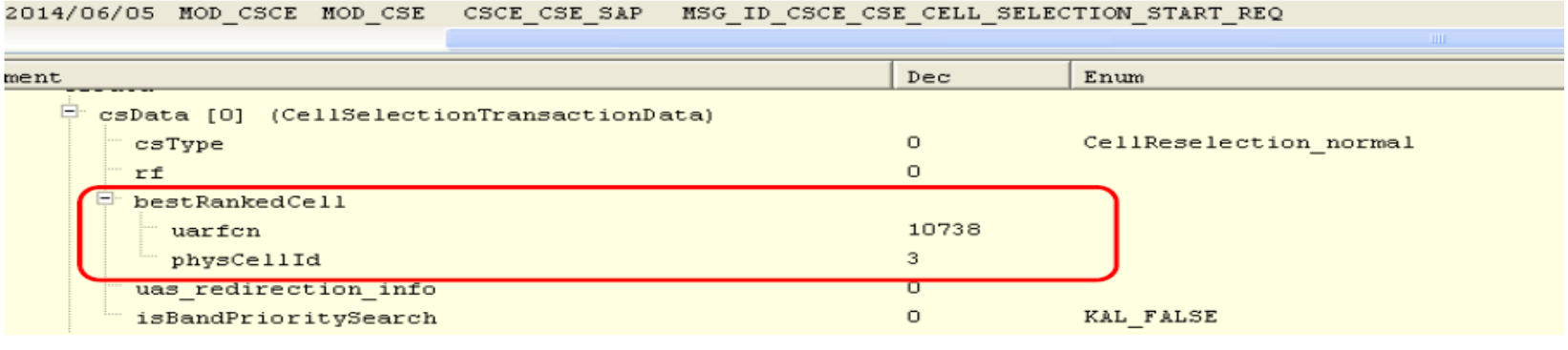
搜索“MSG_ID_CSCE_MEME_CELL_MEASUREMENT_RESULT_IND”并且检查 R value and TReselection，INTER_FREQENCY_CELL_chosen,Cell idx=127，10738/3 满足 3G 小区重选条件，R Value=-32768 最大，且 Treselection 持续时间 1320ms>1000ms

```
MSG_ID_CPHY_MEASUREMENT_CELL_IND
MEME: cell_ind on UARFCN (10763) RSSI (-63) numCell (1) in stMEME_CELL_PCH, CurrTime = 181759, CycleNumber = 14
MSG_ID_CSCE_MEME_CELL_MEASUREMENT_RESULT_IND
MEME: PSC 199, RSCP -84, EcNO -21, RRC_DB_CellType_monitored, SyncInfo(1), TM(-27137), OFF(195), CIO 0, dbIdx 73, active 0
[Serving Cell] UARFCN: 10738, PSC: 199

CSCE R ranking result(descending): CellIndex = 127, R_value = -32768, H_value = 40960, HCS_PRIO = 0, CellType = INTRA_FREQUENCY_CELL_Chosen, ChannelFailFlag = 0
CSCE R ranking result(descending): CellIndex = 132, R_value = -49152, H_value = 8192, HCS_PRIO = 0, CellType = SERVING_CELL_Chosen, ChannelFailFlag = 0
CSCE R ranking result(descending): CellIndex = 99, R_value = -66560, H_value = 31744, HCS_PRIO = 0, CellType = INTER_FREQUENCY_CELL_Chosen, ChannelFailFlag = 0
Found Cell Idx: 127, waiting for incremental TReselection [accumulated: 1320(ms) >= total: 1000(ms)]
Best Cell, CellType = INTRA_FREQUENCY_CELL_Chosen, R Value = -32768, Idx = 127
```

D. Step 4: Execute 3G cell reselection

搜索“MSG_ID_CSCE_CSE_CELL_SELECTION_START_REQ”，如果没找到请提交 MTK。

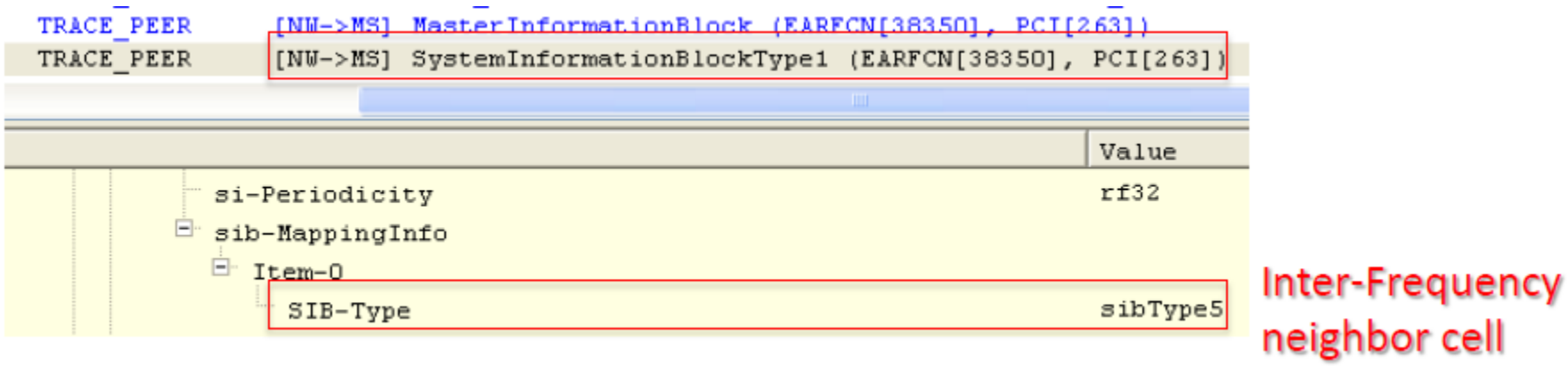


(三) 4G Cell Reselection

A. Step 1: 4G neighbor cell in the SI(inter-frequency)

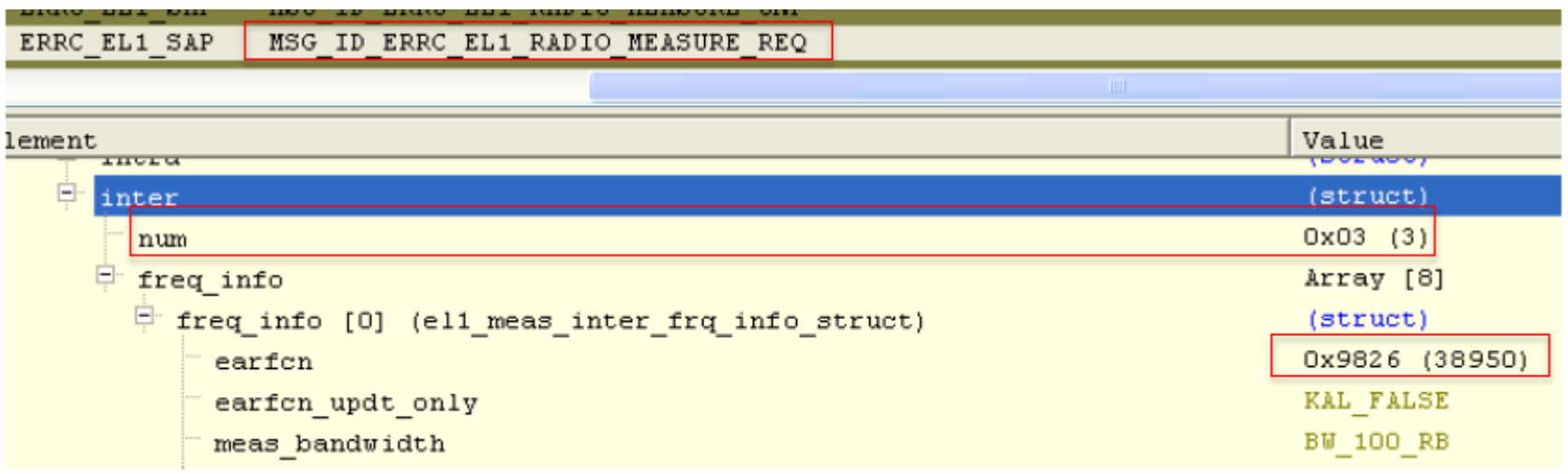
搜索“[NW->MS] SystemInformationBlockType1 (EARFCN”

如果没有 SIB4 的配置，UE 也可以进行 intra-frequency（频内测量），如果没有找到 SIB5 也不意味着没有 4G 小区的服务，也有可能是 UE 保存着之前的小区配置信息，如果不能找到 SIB5，请跳至第二部继续排查，如果没有 4G 小区网络，则 UE 无法重选，这是正常的网络原因。



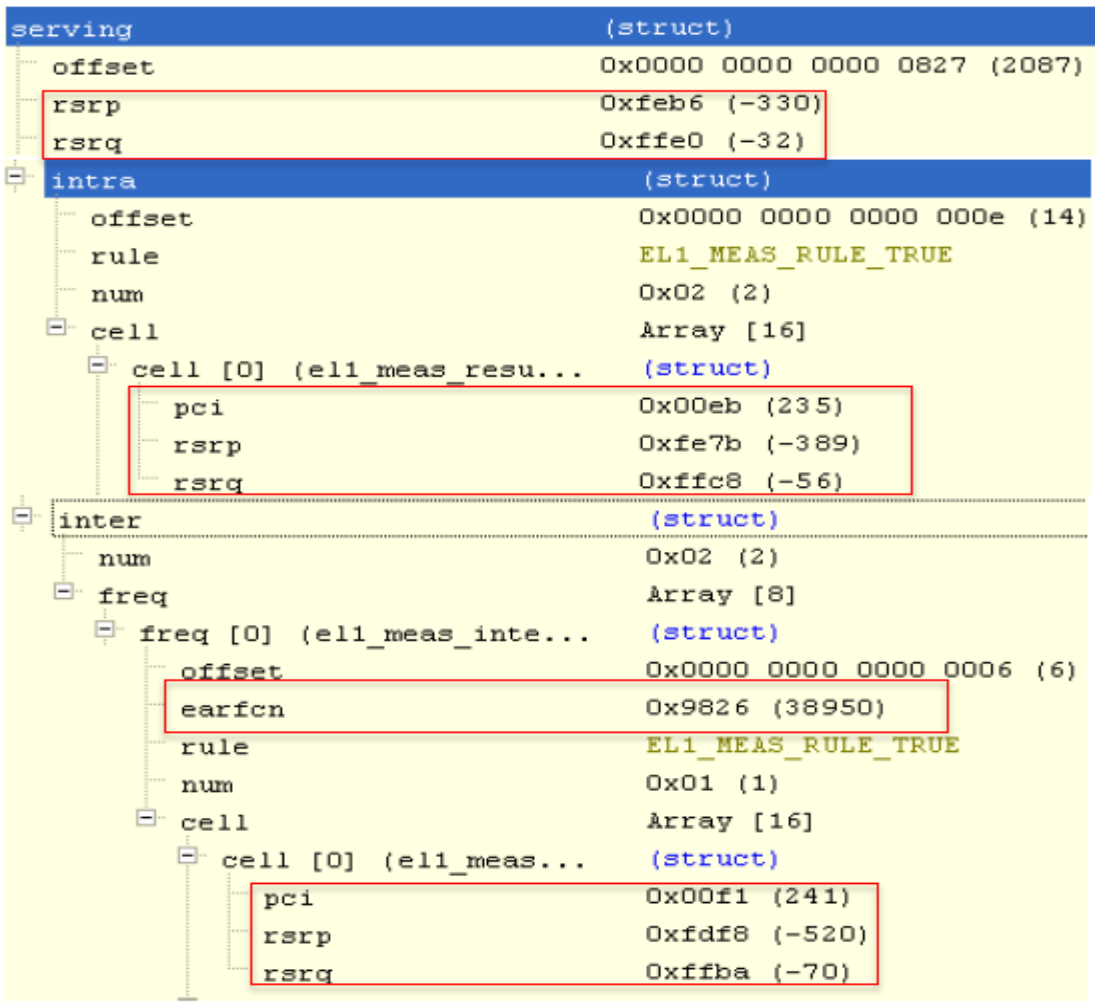
B. Step 2: 4G neighbor cell measurement configure

在完整窗口中搜索“MSG_ID_ERRC_EL1_RADIO_MEASURE_REQ”，



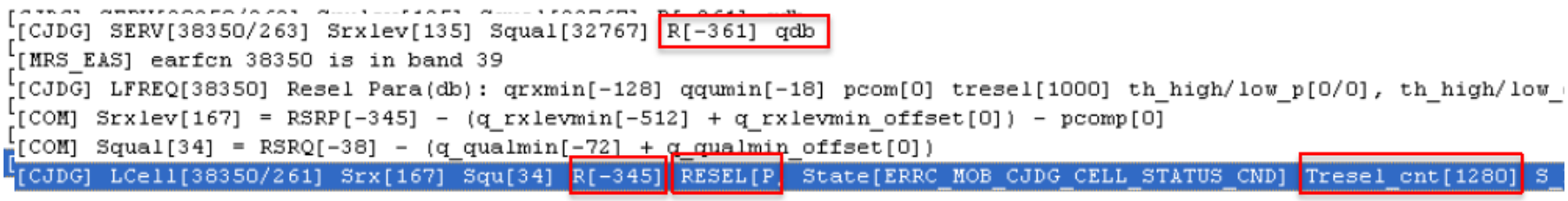
C. Step 3: 4G neighbor cell measurement result

在完整窗口中搜索“MSG_ID_ERRC_EL1_RADIO_MEASURE_IND”

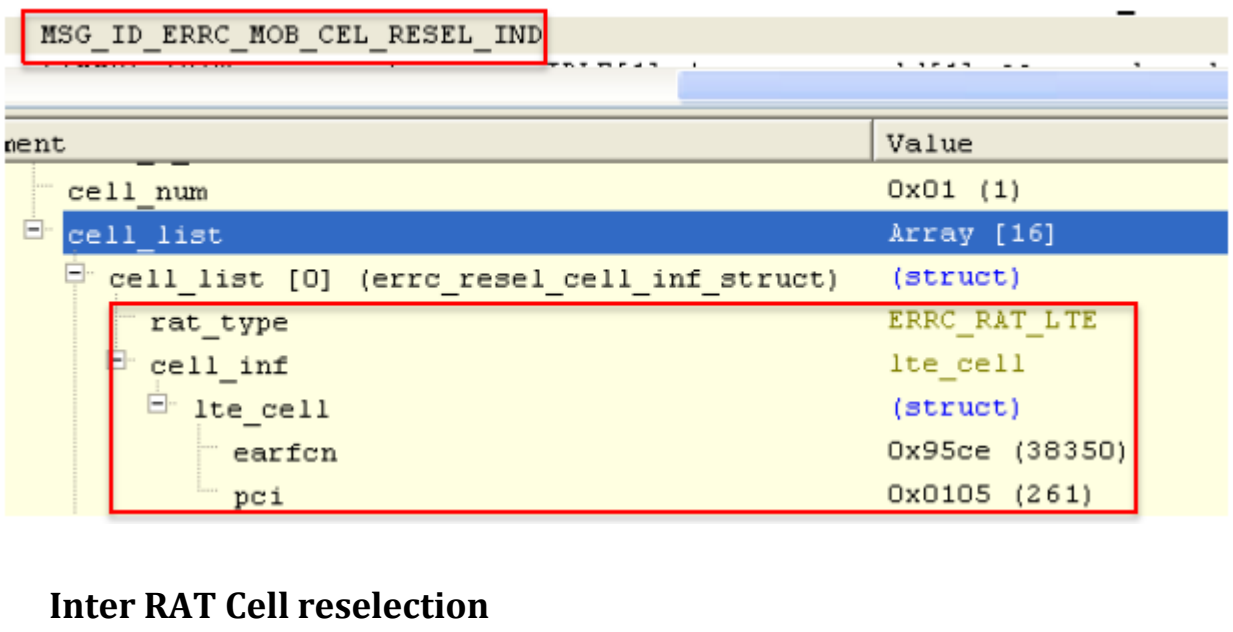


D. Step 4: Criteria of cell reselection

在完整窗口中搜索“[CJDG]”和“RESEL”，



通过搜索“MSG_ID_ERRC_MOB_CEL_RESEL_IND”来查看触发小区重选。

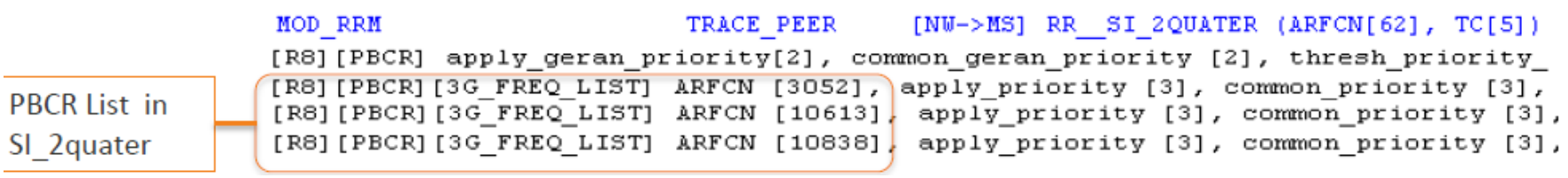


(四) Inter RAT Cell reselection

A. 2G->3G

a. Step 1: 3G neighbor cell in SI_2quater

搜索“SI_2quater”



（PBCR: partial backoff coordination resolution,一种网络协议上的东西，不懂）

b. Step 2: 3G neighbor cell measurement

搜索“MSG_ID_GAS_UAS_UCELL_MEAS_IND”

RSCP and EC_N0 of 3G neighbor cell

MOD_MEME	MOD_RRM	GAS_MEME_SAP	MSG_ID_GAS_UAS_UCELL_MEAS_IND
ir_reported_fdd_cells_me...	(struct)		
scrambling_code	0x0019	25	
cpich_rscp	0xfee7	-281	
cpich_ec_n0	0xfff0	-16	

```
[GERAN_R8][PBCR] UMTS FDD Cell UARFCN[10613], PSC[25], HIGH_PRIO_HIT[1],
MOD_RRM     TRACE_GROUP_2  [RNC] UMTS cell candidate for FDD reselection: UARFCN[10613], PSC[25], hit duration[500 ms],
MOD_RRM     TRACE_GROUP_2  [RNC] UMTS cell candidate for FDD reselection: UARFCN[10613], PSC[25], hit duration[500 ms],
MOD_RRM     TRACE_GROUP_2  [RNC] UMTS cell candidate for FDD reselection: UARFCN[10613], PSC[25], hit duration[1460 ms],
MOD_RRM     TRACE_GROUP_2  [RNC] UMTS cell candidate for FDD reselection: UARFCN[10613], PSC[25], hit duration[2420 ms],
MOD_RRM     TRACE_GROUP_2  [RNC] UMTS cell candidate for FDD reselection: UARFCN[10613], PSC[25], hit duration[5105 ms],
```

Hit duration of same cell

c. Step 3: Evaluate 3G NBR cell

完整窗口中搜索“MSG_ID_GAS_UAS_EVALUATE_UCELL_REQ”和“MSG_ID_GAS_UAS_EVALUATE_UCELL_CNF”来评估相邻 3G 小区，UARFCN 和 SCRAMBLING_CODE 相同，重选成功。

Uarfcn and Scrambling is same ,success reselection to 3G cell

MOD_RRM	MOD_CSCE	GAS_CSCE_SAP	MSG_ID_GAS_UAS_EVALUATE_UCELL_REQ
ir_cell_change_trigger	0x00	0	IR_CELL_RESELECTION
notToCheck3rdCriterion	0x01	1	KAL_TRUE
plmn_search_type	0x01	1	GIVEN_PLMN_EXCLUDE_FORBIDDEN_LA_FOR_ROAMING
target_cell	(struct)		
mode	0x01	1	UMTS_FDD_MODE
fdd_cell	(struct)		
uarfcn	0x2975	10613	
scrambling_code	0x0019	25	

MOD_CSCE	MOD_RRM	GAS_CSCE_SAP	MSG_ID_GAS_UAS_EVALUATE_UCELL_CNF
ir_cell_change_trigger	0x00	0	IR_CELL_RESELECTION
notToCheck3rdCriterion	0x01	1	KAL_TRUE
plmn_search_type	0x01	1	GIVEN_PLMN_EXCLUDE_FORBIDDEN_LA_FOR_ROAMING
target_cell	(struct)		
mode	0x01	1	UMTS_FDD_MODE
fdd_cell	(struct)		
uarfcn	0x2975	10613	
scrambling_code	0x0019	25	

B. 2G->4G

a. Step 1: SI_2quater collection

在 peer window 中搜索“SI_2quater”， integrated window 中搜索“MSG_ID_GAS_EAS_LTE_MEASUREMENT_REQ”

LTE NBR cell in SI_2quater

```
TRACE_PEER     [NW->MS] RR__SI_2QUATER (ARFCN[11], TC[4])
  E-UTRAN Neighbour Cells
      1... ....: E-UTRAN Neighbour Cells Struct: Present
      .100 1010  1110 0111  0... .... = EARFCN: 38350
      .0.. ....: Measurement Bandwidth: Not Present
      ..0. ....: E-UTRAN Neighbour Cells Struct: Not Present
      ...1 ....: E-UTRAN Priority: Present
      .... 111. = E-UTRAN_PRIORITY: 7
      .... ...0  0101 .... = THRESH_EUTRAN_high: 10 dB (5)
      .... 1...: Threshold E-UTRAN Low: Present
      .... .101  00.. .... = THRESH_EUTRAN_low: 40 dB (20)
      ..1. ....: E-UTRAN Qrxlev Min: Present
      ...0 0000 = E-UTRAN_QRXLEVMIN: -140 dBm (0)
  0... ....: Repeated E-UTRAN Neighbour Cells: Not Present
      .0.. ....: Repeated E-UTRAN Not Allowed Cells: Not Present
      ..0. ....: Repeated E-UTRAN PCID to TA mapping: Not Present
```

MOD_RRM	MOD_ERRC	GAS_EAS_SAP	MSG_ID_GAS_EAS_LTE_MEASUREMENT_REQ
freq [0] (eas_meas_freq_in...	(struct)		
earfcn	0x95ce	38350	
meas_bandwidth	0x00	0	
skip_black_list	0x00	0	

b. Step 2: LTE NBR cell measurement

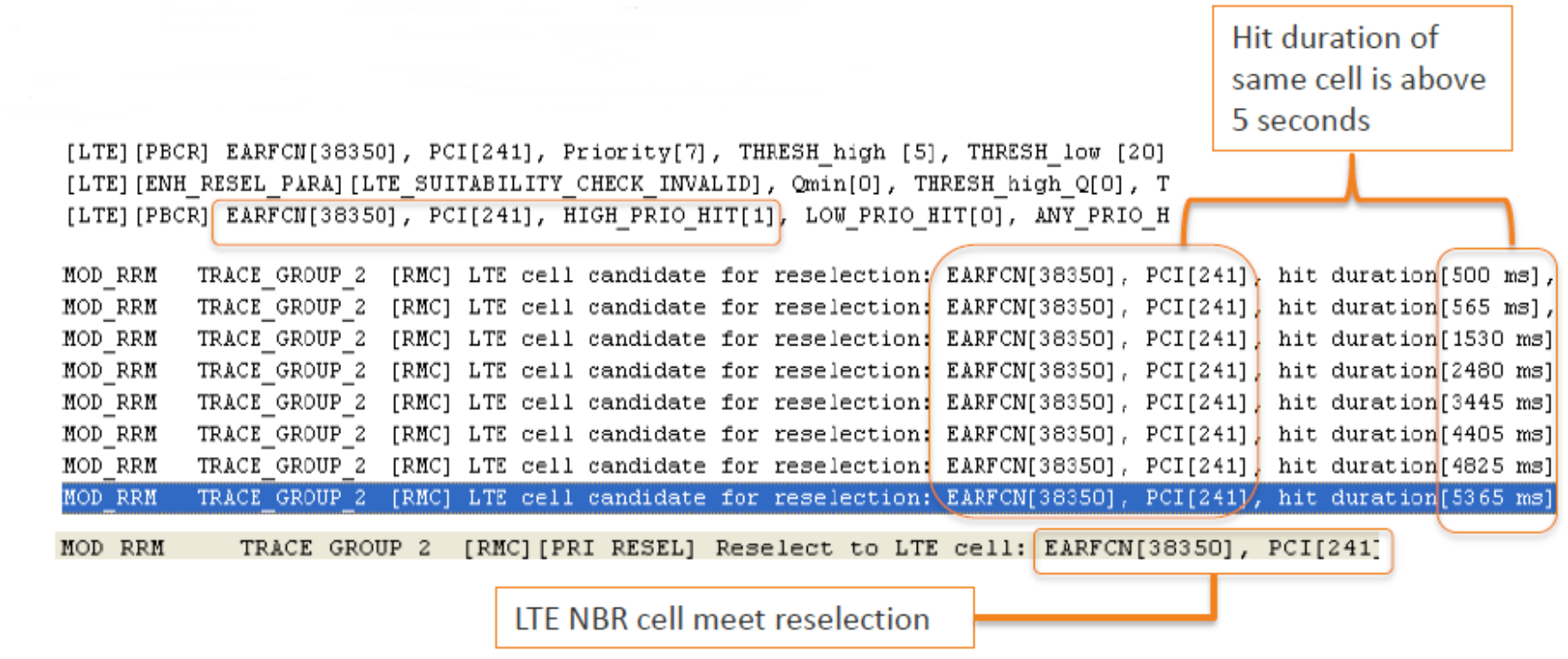
integrated window 中搜索“MSG_ID_GAS_EAS_LTE_MEASUREMENT_IND”，

Measurement of LTE NBR cell

MOD_ERRC	MOD_RRM	GAS_EAS_SAP	MSG_ID_GAS_EAS_LTE_MEASUREMENT_IND
MOD_ERRC	MOD_RRM	GAS_EAS_SAP	MSG_ID_GAS_EAS_LTE_MEASUREMENT_IND
freq [0] (eas_meas_freq_rs...	(struct)		
earfcn	0x95ce	38350	
cell_num	0x01	1	
cell	Array [16]		
cell [0] (eas_meas_ce...	(struct)		
pci	0x00f1	241	
rsrp	0xfe9e	-354	
rsrq	0xffe4	-28	

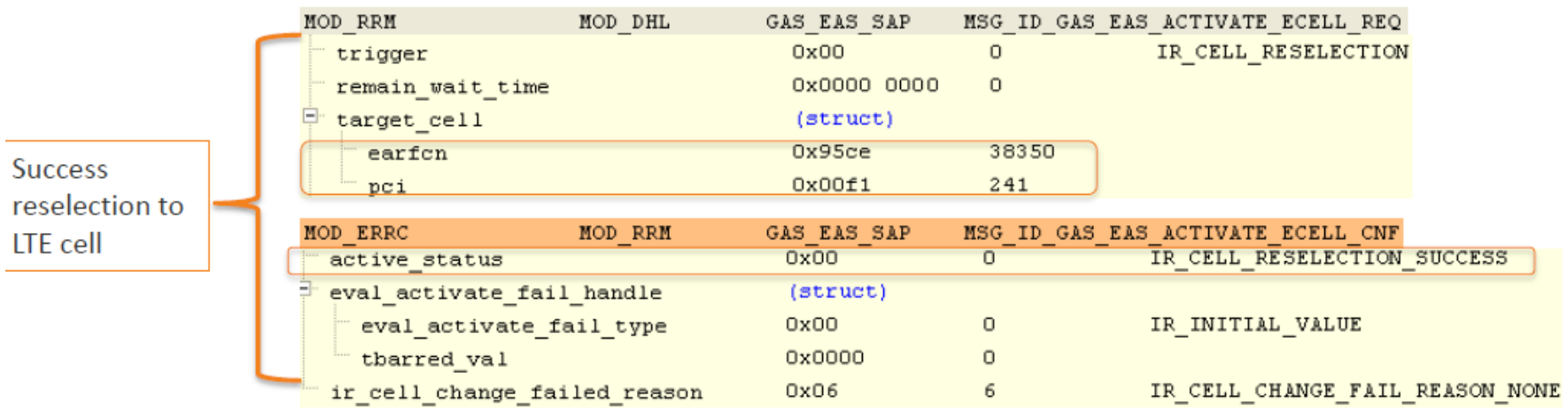
c. Step 3: hit duration of LTE NBR cell

integrated window 中搜索“Reselection to LTE cell”



d. Step 4: reselection to LTE cell

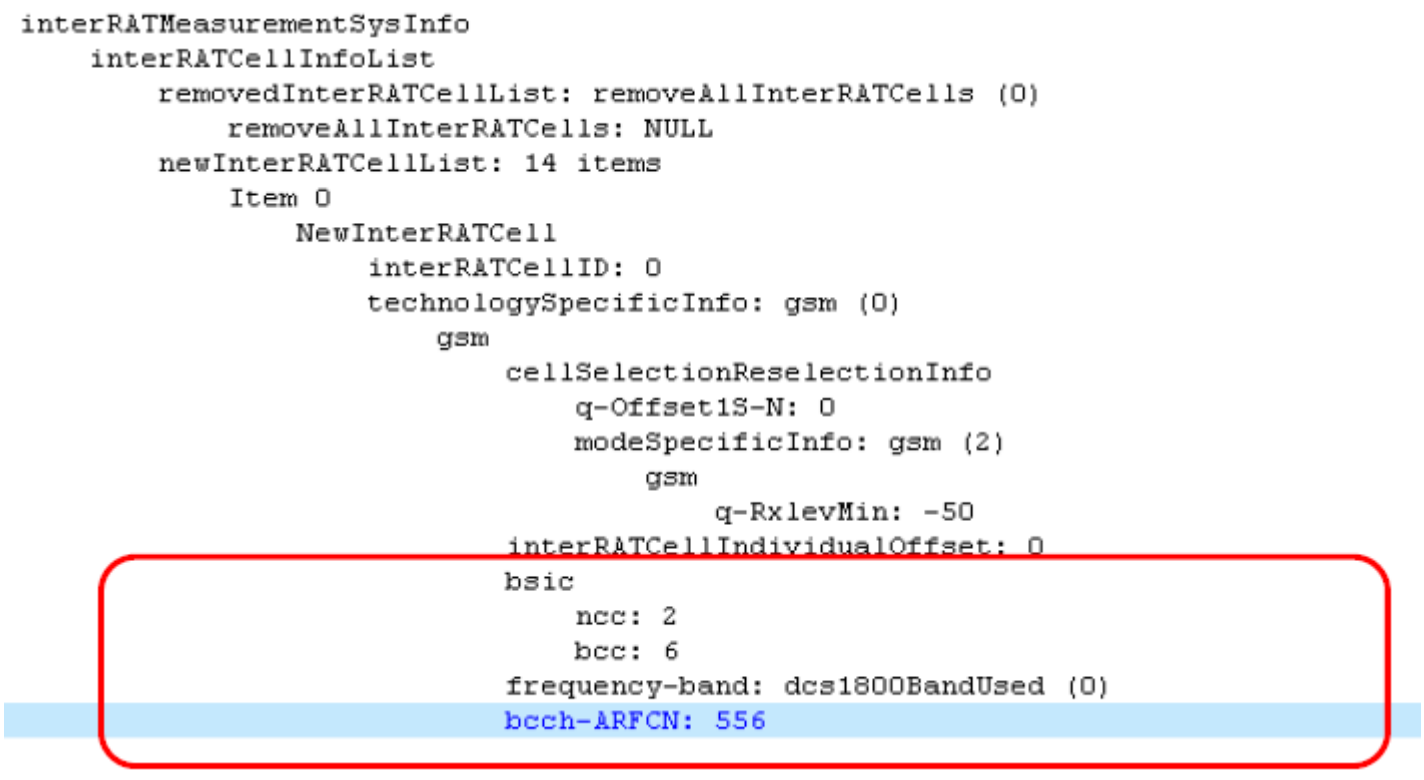
integrated window 中搜索“MSG_ID_GAS_EAS_ACTIVATE_ECELL_REQ”和“MSG_ID_GAS_EAS_ACTIVATE_ECELL_CNF”



C. 3G->2G

a. Step 1: NW configure 2G neighboring cell

搜索“‘[NW->MS] RRC_SI_SIB11”



如果 UE 没有收到 SIB11，但是已经驻留在相邻小区，搜索“MSG_ID_CPHY_MEASUREMENT_CONFIG_CELL_REQ”并查看参数

MSG_ID_CPHY_MEASUREMENT_CONFIG_CELL_REQ

```
-- Inter-RAT Cell Info List --
Id 0 = 0/578/33(43), cellID_bmp 1, timestamp 385765, owner 0
Id 1 = 0/64/2(96), cellID_bmp 2, timestamp 385765, owner 0
Id 2 = 0/36/62(77), cellID_bmp 4, timestamp 385765, owner 0
Id 3 = 0/580/33(97), cellID_bmp 8, timestamp 385765, owner 0
Id 4 = 0/582/30(99), cellID_bmp 10, timestamp 385765, owner 0
Id 5 = 0/566/36(78), cellID_bmp 20, timestamp 385765, owner 0
Id 6 = 0/573/30(47), cellID_bmp 40, timestamp 385765, owner 0
```

b. Step 2: 2G measurement

搜索“MSG_ID_UAS_GAS_GCELL_MEAS_IND”和“MSG_ID_MPAL_RR_UMTS_GSM_MEAS_IND”并查看参数

只有当 bsic_valid=1，这个 2G 小区才被认为是有效地。

RRM_MPAL_SAP	MSG_ID_MPAL_RR_UMTS_GSM_MEAS_IND
TRACE_GRO...	[RRM][State-Msg] <RRM_INACTIVE_STATE> <RRM_NULL_SUBSTATE>: <MSG_ID_MPAL_RR_UMTS_GSM_MEAS_IND>
TRACE_GRO...	[RMC] arfcn[64],Pwr[-349],bsic_valid[0],counter[19760], F.O[0],E.B[0]
TRACE_GRO...	[RMC] arfcn[36],Pwr[-355],bsic_valid[0],counter[9520], F.O[0],E.B[0]
TRACE_GRO...	[RMC] arfcn[566],Pwr[-355],bsic_valid[1],counter[19760], F.O[822944],E.B[6034]
TRACE_GRO...	[RMC] arfcn[573],Pwr[-421],bsic_valid[1],counter[30000], F.O[202695],E.B[2980]

MSG_ID_UAS_GAS_GCELL_MEAS_IND

```
MEME: update meme_time 640428 to 640433, sysTick prev = 2318300, now = 2318311, diff = 11 (1s = 217.5 ticks)
MEME: gcell rssi ind, num_carriers 7, list_ref 1, in <stMEME_Idle>
MEME: gcell[6] = 0/578/33, rssi -107, timestamp 640433, resel_status IR_BAR_STATUS_NOT_BARRED
MEME: gcell[5] = 0/64/2, rssi -87, timestamp 640433, resel_status IR_BAR_STATUS_NOT_BARRED
MEME: gcell[4] = 0/36/62, rssi -88, timestamp 640433, resel_status IR_BAR_STATUS_NOT_BARRED
MEME: gcell[3] = 0/580/33, rssi -125, timestamp 640433, resel_status IR_BAR_STATUS_NOT_BARRED
MEME: gcell[2] = 0/582/30, rssi -107, timestamp 640433, resel_status IR_BAR_STATUS_NOT_BARRED
MEME: gcell[1] = 0/566/36, rssi -88, timestamp 640433, resel_status IR_BAR_STATUS_NOT_BARRED
MEME: gcell[0] = 0/573/30, rssi -105, timestamp 640433, resel_status IR_BAR_STATUS_NOT_BARRED
```

c. Step 3: 3G2 IRCR criteria

搜索“MSG_ID_CSCE_MEME_CELL_MEASUREMENT_RESULT_IND”，并查看 R value and TReselection，

2G cell arfcn 566 满足 3G->2G 标准，满足 S criteria，R_value 值最大，且 Treselection 持续时间 2700>2000ms

MSG_ID_CSCE_MEME_CELL_MEASUREMENT_RESULT_IND

```
CSCE current Delta Meas Tick Time = 760(ms)
CSCE[HMD] current RI: 310000(ms) in [8] element.
Designated cell  [UARFCN = 10120, PHYSCELLID = 100] S criteria satisfied [Squal = 1, Sndev = 7168]
CS_Evaluate_S_Criterion_ServingCell(): [The cell passed S criteria? KAL_TRUE], [connected = KAL_FALSE, cell's validity = 0, q_RxLevMin = -97, maxRachPwr = 24, technolc
[FastMoving? KAL_FALSE][HCS? KAL_FALSE] (o S_IntraSearch 51) (o S_InterSearch 51) (o S_SearchHCS 92) (o S_SearchRAT 3) (o S_HCS_RAT 92) (o S_LimitSearchRAT
Check measurement rules, MeasTargetGroup(NextRankCand) = 000000111
Unsuitability mask calculated is 0x7da, based on [isConnect = KAL_FALSE, PLMN Search Type = GIVEN_PLMN_EXCLUDE_FORBIDDEN_LA_FOR_ROAMING]
GSM Cell (BCCH_ARFCN:578, FREQ_BAND:0, BSIC:33, CellIndex:10), S criteria NOT satisfied, RSSI: -107, RxLevMin: -97
GSM cell (BCCH_ARFCN:64, FREQ_BAND:0, BSIC:2, CellIndex:9), S criteria satisfied but BSIC is not verified, RSSI: -87, RxLevMin: -97 !!
GSM cell (BCCH_ARFCN:36, FREQ_BAND:0, BSIC:62, CellIndex:6), S criteria satisfied but BSIC is not verified, RSSI: -89, RxLevMin: -97 !!
GSM Cell (BCCH_ARFCN:580, FREQ_BAND:0, BSIC:33, CellIndex:3), S criteria NOT satisfied, RSSI: -125, RxLevMin: -97
GSM Cell (BCCH_ARFCN:582, FREQ_BAND:0, BSIC:30, CellIndex:2), S criteria NOT satisfied, RSSI: -108, RxLevMin: -97
GSM Cell (BCCH_ARFCN:566, FREQ_BAND:0, BSIC:36, CellIndex:1), S criteria satisfied, RSSI: -89, RxLevMin: -97
GSM Cell (BCCH_ARFCN:573, FREQ_BAND:0, BSIC:30, CellIndex:48), S criteria NOT satisfied, RSSI: -105, RxLevMin: -97
CSCE R ranking result(descending): CellIndex = 1, R_value = -363520, CellType = INTER_RAT_CELL_Chosen, ChannelFailFlag = 0, Reset Treselection? KAL_FALSE
CSCE R ranking result(descending): CellIndex = 65, R_value = -373760, CellType = SERVING_CELL_Chosen, ChannelFailFlag = 0, Reset Treselection? KAL_FALSE
Found Cell Idx: 1, waiting for incremental TReselection [accumulated: 2700(ms) >= total: 2000(ms)]
Best Cell, CellType = INTER_RAT_CELL_Chosen, R Value = -363520, Idx = 1
```

d. Step 4: Execute 3G2 IRCR

搜索“MSG_ID_CSCE_RRCE_SUITABLE_CELL_SELECTED_REQ”

MSG_ID_CSCE_RRCE_SUITABLE_CELL_SELECTED_REQ

reset rrce_context.v300:0

	Hex	Dec	Oct	Bit	Enum
	0xF09B5698				
ct	(struct)				
	0x01	1	0001	00000001	
	0x68	104	0150	01101000	
	0x000e	14	0000016	0000000000001110	
	(struct)				
	0x02	2	0002	00000010	RRC_DB_SelectedCellTechnology_gsm_selected
	umts (union)				
	(struct)				
	0x0000	0	0000000	0000000000000000	
	0x0236	566	0001066	0000001000110110	
	0x01	1	0001	00000001	CSCE_CELL_SELECT_AUTO

当 3G->2G 执行成功后，UE 会发送 LU 请求。

D. 3G->4G

```
[NW->MS] RRC SI SIB19 (UARFCN:[10563], PSC:[100])
[APBCR] CSCE_ComposePriorityInfoList: LTE info idx = 0, earfcn = 300, prio = 6, QrxlevmiTRA = -110, Threshx_high
[APBCR] CSCE_ComposePriorityInfoList: prio_status: 0, Serving cell info prio = 2, search1 = 0, search2 = 0, Threshs
[CSCE context] [APBCR] apbcrEnabledInfo: ReselType: CSCE_MEME_MEAS_RULE_AND_APB_H_PRIO, apbMeasTargetCells: 10, uar
[CSCE context] [APBCR] apbcrEnabledInfo: ApbEuarfcnCount: 1, euarfcn:[300][811][0][57][0][1152][0][903]
MSG_ID_CSCE_MEME_MEAS_MANIPULATION_REQ
MSG_ID_UAS_EAS_LTE_MEASUREMENT_REQ
MSG_ID_UAS_EAS_LTE_MEASUREMENT_IND
MSG_ID_CSCE_MEME_CELL_MEASUREMENT_RESULT_IND
[APBCR] LTE Cell (EARFCN:300, PCI:0, CellIndex:0, ApbcrValidity: 3), S criteria satisfied, RSRP: -95, RxLevMin: -11
[APBCR] Lte Cell earfcn = 300, pci = 0, Criteria_1, NeiSrxlev: 60416, Threshx_high: 0, satisfied = KAL_TRUE
[APBCR]: Best Cell, CellType = LTE_CELL_Chosen, Srxlev = 60416, Idx = 0
MSG_ID_CSCE_RRCE_SUITABLE_CELL_SELECTED_REQ
MSG_ID_UAS_EAS_EVALUATE_ECELL_REQ
MSG_ID_UAS_EAS_EVALUATE_ECELL_CNF
MSG_ID_RATCM_UAS_RAT_CHANGE_IND
MSG_ID_UAS_EAS_ACTIVATE_ECELL_CNF
MSG_ID_RATCM_UAS_RAT_CHANGE_RES
```

a. Step 1: check SIB19 exist

搜索“RRC_SI_SIB19”，如果没有找到，请搜索“MSG_ID_UAS_EAS_LTE_MEASUREMENT_REQ”，如果没找到，则是网络问题。

如果对比机能在相同情况下搜索到 SIB19，请提交 MTK 处理。

```
MOD_SIBE    [NW->MS] RRC_SI_SIB19 (UARFCN:[10713], PSC:[401])

Element                                          Hex          Dec
  RRC_SysInfoType19
    utra-PriorityInfoList
      utra-ServingCell
        priority                                 4
        s-PrioritySearch1                        2
        s-PrioritySearch2                        2
        threshServingLow                         1
    eutra-FrequencyAndPriorityInfoList
      element-0
        earfcn                                   1750
        measurementBandwidth                     mbw6
        priority                                 6
        qRxLevMinEUTRA                           -64
        threshXhigh                              6
        threshXlow                               2
        eutraDetection                           TRUE
      element-1
```

4G Neighbor cell info

b. Step 2: check the measurement result

integration window 中搜索“UAS_EAS_LTE_MEASUREMENT_IND”

```
MOD_ERRC    MSG_ID_UAS_EAS_LTE_MEASUREMENT_IND

  freq_num                                       0x01         1
  freq                                           Array [8]
    freq [0] (eas_meas_freq_rslt_struct)         (struct)
      earfcn                                     0x012c       300
      cell_num                                   0x01         1
      cell                                       Array [16]
        cell [0] (eas_meas_cell_rslt_struct)     (struct)
          pci                                    0x0000       0
          rsrp                                   0xfe83       -381
          rsrq                                   0xffeb       -21
```

RSRP = -95 dB, RSRQ = -5 dB

c. Step 3: check the 3G4 IRCR criteria

搜索“CSCE_RRCE_SUITABLE_CELL_SELECTED_REQ”

```
MOD_CSCE  [APBCR] LTE Cell (EARFCN:37900, PCI:385, CellIndex:0, ApbcrValidity: 3|, 3 criteria satisfied, RSRP: -93, RxLevMin:
MOD_CSCE  [APBCR] Lte Cell earfcn = 37900, pci = 385, Criteria 1, NeiSrxlev: 149504, Threshx high: 14, satisfied = KAL_TRUE
MOD_CSCE  Found Cell Idx: 0, waiting for incremental TReselection [accumulated: 2040(ms) >= total: 2000(ms)]
MOD_CSCE  [APBCR]  ranking result(descending): CellIndex = 0, prio = 7, Treselection = 40, Srxlev = 149504, CellType = LTE_CEL
MOD_CSCE  [APBCR]: Best Cell, CellType = LTE_CELL_Chosen, Srxlev = 149504, Idx = 0
MOD_CSCE  [CSCE context] lastMeasOperation: CSCE_MEASUREMENT_START, lastMeasTarget: 3, nLastRelayCtrl: 1, isLastHCSused: KAL_F
MOD_CSCE  [CSCE context] [APBCR] lastReselType: CSCE_MEME_MEAS_RULE_AND_APB_H_PRIO, lastApbMeasTargetCells: 10, uarfcn1: 0 , u
MOD_CSCE  [CSCE context] [APBCR] lastApbEuarfcnCount: 2, euarfcn:[-27636][-26286][0][0][0][0][0][0]
MOD_CSCE  current CISE Proc = INVALID_PROC and ongoing CISE Proc = CELL_RESELECTION_PROC
MOD_CSCE  [CSCE context] currentCISEProcedure: INVALID_PROC -> CELL_RESELECTION_PROC
MOD_CSCE  MSG ID CSCE RRCE SUITABLE CELL SELECTED REQ
```

Element	Hex	Dec	Enum
Local Parameter	0x18ae4b4		
csce_rrce_suitable_cell_selected_req...	(struct)		
ref_count	0x01	1	
lp_reserved	0xc2	194	
msg_len	0x000e	14	
dbCell	(struct)		
selection	0x03	3	RRC_DB_SelectedCellTechnology_eutra_selected
choice	eutra		eutra
eutra	(struct)		
earfcn	0x940c	37900	
pci	0x0181	385	
cellSelectCause	0x01	1	CSCE_CELL_SELECT_AUTO

d. Step 4: check the 3G4 IRCR evaluation result

搜索“UAS_EAS_EVALUATE_ECELL_CNF”确认 eval_status=IR_CELL_RESELECTION_SUCCESS

MOD_ERRC MSG_ID_UAS_EAS_EVALUATE_ECELL_CNF

Element	Hex	Dec	Enum
Local Parameter	0x18ae7f4		
uas_eas_evaluate_ecell_cnf_struct	(struct)		
ref_count	0x01	1	
lp_reserved	0xed	237	
msg_len	0x000a	10	
eval_status	0x00	0	IR_CELL_RESELECTION_SUCCESS
eval_activate_fail_handle	(struct)		
eval_activate_fail_type	0x00	0	IR_INITIAL_VALUE
tbarred_val	0x0000	0	

e. Step 5: check the 3G4 IRCR activation result

搜索“UAS_EAS_ACTIVATE_ECELL_CNF”确认 eval_status=IR_CELL_RESELECTION_SUCCESS

MOD_ERRC MSG_ID_UAS_EAS_ACTIVATE_ECELL_CNF

MOD_ER... [CEL DI] IR to LTE acti result: status[IR_CELL_RESELECTION_SUCCESS], fai

Element	Hex	Dec	Enum
Local Parameter	0x18ad648		
uas_eas_activate_ecell_cnf_struct	(struct)		
ref_count	0x02	2	
lp_reserved	0x00	0	
msg_len	0x000a	10	
active_status	0x00	0	IR_CELL_RESELECTION_SUCCESS
eval_activate_fail_handle	(struct)		

E. 4G->2G/3G

a. Step 1: 23G neighbor cell in the SI

搜索“[NW->MS] SystemInformationBlockType1 (EARFCN”

```
[NW->MS] SystemInformationBlockType1 (EARFCN[40340], PCI[196])
[NW->MS] SystemInformation (EARFCN[40340], PCI[196])
```

Value
SchedulingInfo
si-Periodicity: rf64
sib-MappingInfo
Item-0
SIB-Type: sibType6
Item-1
SIB-Type: sibType7

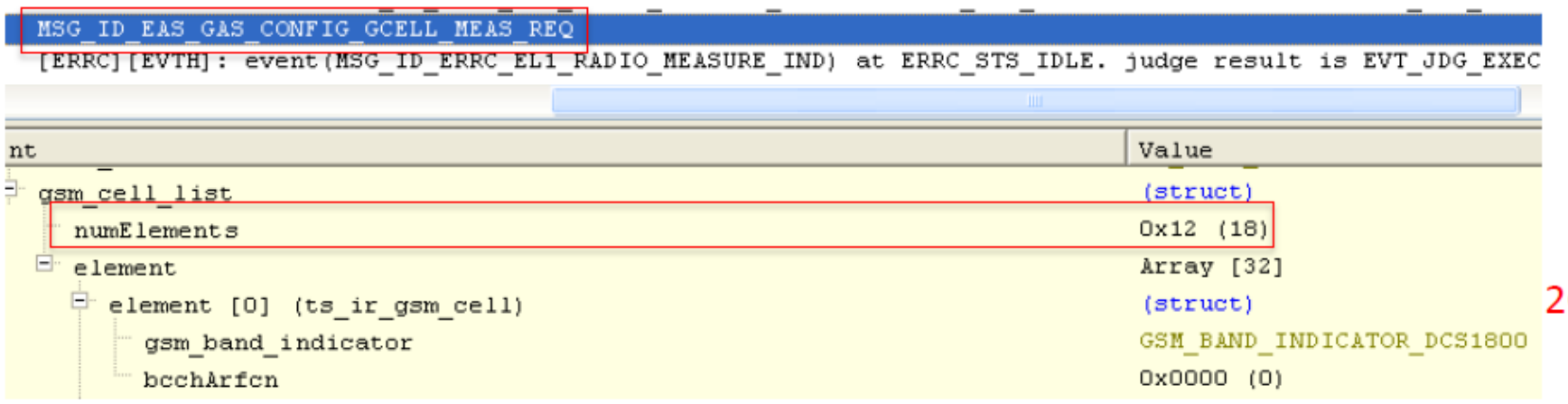
3G nbr cell

2G nbr cell

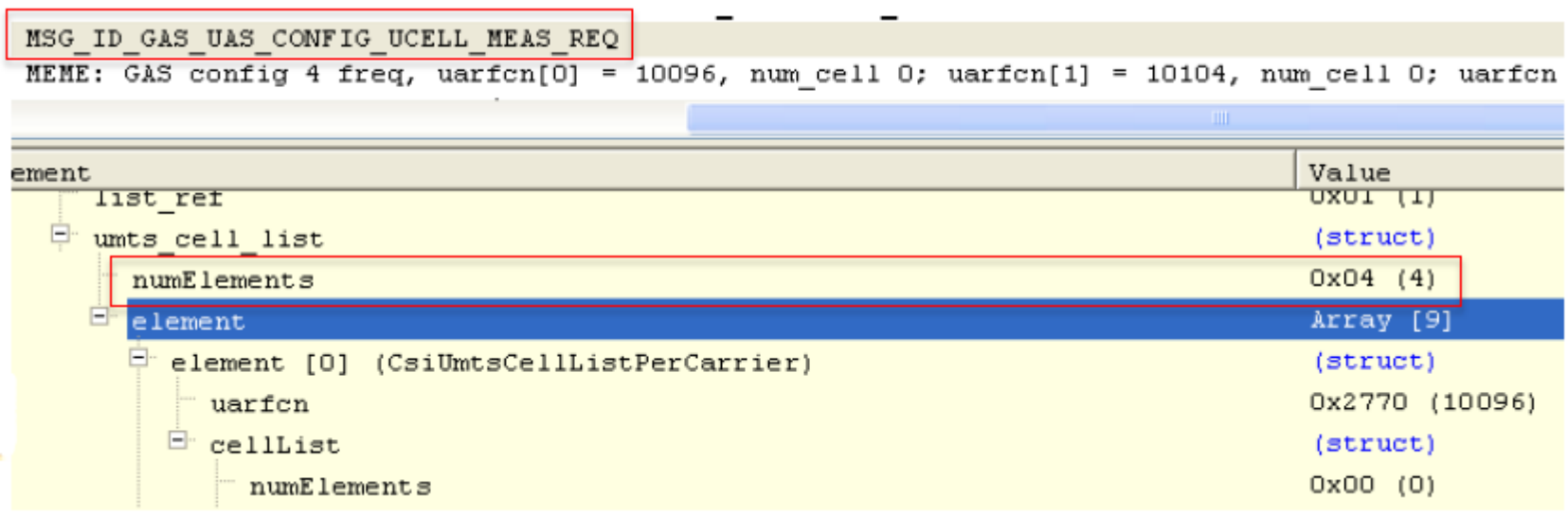
如果没有找到 SIB6、SIB7 不意味没有 2G、3G 小区信号，有可能是仍驻留在 4G 小区，然后进行下一步。
如果没有 2G/3G 的小区信息，则 UE 无法重选到 2G、3G 是正常的，是网络原因造成的。

b. Step 2: 2G/3G neighbor cell measurement configure.

integration window 中搜索“MSG_ID_EAS_GAS_CONFIG_GCELL_MEAS_REQ”

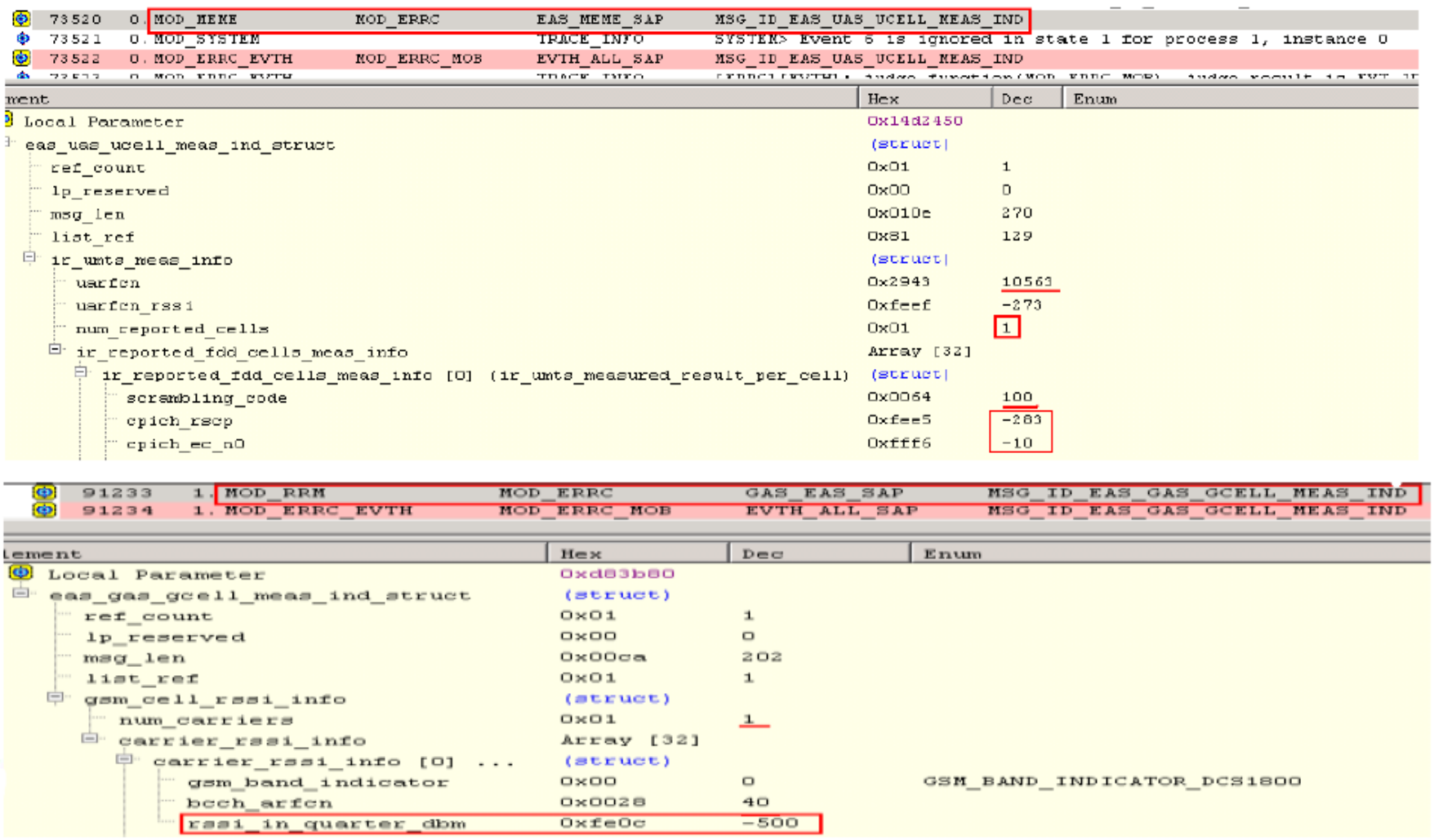


integration window 中搜索“MSG_ID_GAS_UAS_CONFIG_UCELL_MEAS_REQ”



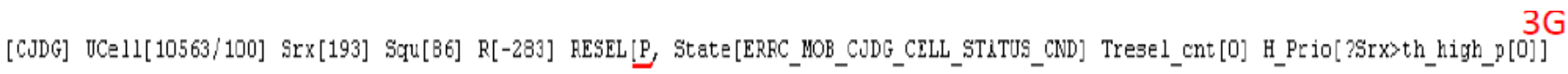
c. Step 3: 23G neighbor cell measurement result.

搜索“GCELL_MEAS_IND”/”UCELL_MEAS_IND”查看测量结果



d. Step 4: Criteria of IRCR.

搜索“[CJDG]” 和 “RESEL”



```
[CJDG] GFREQ[100] Resel Para(db): qrxmin[-55] pcom[0] tresel[2000] th_high/low_p[0/0]
[COM] Srxlev[20] = RSRP[-200] - (q_rxlevmin[-220] + q_rxlevmin_offset[0]) - pcomp[0]
[CJDG] GCell[100/255] BSIC not decoded yet, keep as temp candidate
[CJDG] GCell[100/255] Srx[20] RESEL[P, State[ERRC_MOB_CJDG_CELL_STATUS_TEMP] Tresel_cnt[2000] L_Prio[?Serv_Srx<th_s_low_p[160] Srx>th_low_p[0]]
```

2G

Treselection 没有实现(Tresel_cnt<tresel)，所以不能作为被选小区

```
[CJDG] GCell[40/5] Srx[358] RESEL[P, State[ERRC_MOB_CJDG_CELL_STATUS_CND] Tresel_cnt[602] L_Prio[?Serv_Srx<th_s_low_p[240] Srx>th_low_p[248]]
```

搜索“MSG_ID_ERRC_MOB_CEL_RESEL_IND”来判断小区触发重选

e. Step 5: Evaluate for 2G/3G cell.

搜索“MSG_ID_EAS_UAS_EVALUATE_UCELL_CNF”

Evaluation begin

Evaluation end

PS Integrated

```
[CEL_DI](CR)cand evaluate begin
MSG_ID_EAS_UAS_EVALUATE_UCELL_REQ
[CELLRMNG] --End   Evt[ERRC_CEL_EXEVT_EVALUATE_XCELL_CNF], state[ERRC_CEL_CELLRMNG_STATE_WAIT_IRFR
[CTRL] End evt[ERRC_CEL_EXEVT_EVALUATE_XCELL_CNF], Exec Func[ERRC_CEL_FUNC_CELLRMNG], exec_sts[ERR
[DHL Reader][UT] Receive one inject UT message. Src_id=MOD_CSCE, dst_id=MOD_ERRC_CEL, msg_id=MSG_I
[DHL Reader][UT] Allocate a local buffer. Addr: 0x1B104AC, Size: 0x10
MSG_ID_EAS_UAS_EVALUATE_UCELL_CNF
MSG_ID_EAS_UAS_EVALUATE_UCELL_CNF
VALUATE_UCELL_CNF) at ERRC_STS_IDLE. judge result is EVT_JDG_E
[CTRL] Input MSG[MSG_ID_EAS_UAS_EVALUATE_UCELL_CNF], Curr CEL MNG State[ERRC_CEL_STATE_IDLE], Curr
[CTRL] Begin evt[ERRC_CEL_EXEVT_EVALUATE_XCELL_CNF], Verdict[ERRC_CEL_CTRL_EXE_VERDICT_EXE], Exec
[CELLRMNG] --Begin Evt[ERRC_CEL_EXEVT_EVALUATE_XCELL_CNF], state[ERRC_CEL_CELLRMNG_STATE_WAIT_IRFR
[CEL_DI](CR)cand evaluate end--, result[IR_CELL_RESELECTION_FAILURE], (if fail)cause[CELL_BARRED]
```

Element	Hex	Dec	Enum
Local Parameter	0x1b104ac		
eas_uas_evaluate_ucell_cnf_struct	(struct)		
ref_count	0x01	1	
lp_reserved	0x00	0	
msg_len	0x0010	16	
ir_cell_eval_status	0x0000 0001	1	IR_CELL_RESELECTION_FAILURE
Eval_activate_fail_handle	(struct)		
eval_activate_fail_type	0x0000 0004	4	CELL_BARRED
tbarred_val	0x0000	0	

如果以上任意一步失败，且对比机正常，则提交 MTK。

七、Handover（切换）

所谓切换，就是指当移动台在通话过程中从一个基站覆盖区移动到另一个基站覆盖区，或者由于外界干扰而造成通话质量下降时，必须改变原有的话音信道而转接到一条新的空闲话音信道上去，以继续保持通话的过程。

(一)　2G Handover

```
MOD_RRM        [MS->NW] RR__MEASUREMENT_REPORT
MOD_RRM        [NW->MS] RR__HANDOVER_COMMAND
MOD_RRM        [NW->MS] RR__PHYSICAL_INFORMATION
MOD_RRM        [MS->NW] RR__HANDOVER_COMPLETE
MOD_RRM        [MS->NW] RR__MEASUREMENT_REPORT
MOD_RRM        [MS->NW] RR__MEASUREMENT_REPORT
```

A.　Step 1: measurement procedure

在 peer window 搜索“RR__SI_5”和“RR__MEASUREMENT_REPORT”

```
MOD_RRM                    TRACE_PEER      [NW->MS] RR__SI_5 (ARFCN[579], TC
 Neighbour Cell Description - BCCH Frequency List
     ..0. .... = EXT-IND: The information element carries the complete BA (0)
     ...0 .... = BA-IND: 0
     10.. 111. = Format Identifier: variable bit map (0x47)
     List of ARFCNs = 549 569 572 576 581 584 616
```

```
MOD_RRM                    TRACE_PEER      [MS->NW] RR  MEASUREMENT_REPORT
 Measurement Results
     0... .... = BA-USED: 0
     .1.. .... = DTX-USED: DTX was used
     ..00 1101 = RXLEV-FULL-SERVING-CELL: -98 <= x < -97 dBm (13)
     0... .... = 3G-BA-USED: 0
     .0.. .... = MEAS-VALID: The measurement results are valid
     RXLEV-SUB-SERVING-CELL: -98 <= x < -97 dBm (13)
     .000 .... = RXQUAL-FULL-SERVING-CELL: BER < 0.2%, Mean value 0.14% (0)
     .... 000. = RXQUAL-SUB-SERVING-CELL: BER < 0.2%, Mean value 0.14% (0)
     .... ...0  10.. .... = NO-NCELL-M: 2 neighbour cell measurement result (2)
     ..00 1100 = RXLEV-NCELL: 12
     0110 1... = BCCH-FREQ-NCELL: 13
     .... .110  000. .... = BSIC-NCELL: 48
     ...0 0011  0... .... = RXLEV-NCELL: 6
     .011 11.. = BCCH-FREQ-NCELL: 15
     .... ..10  1110 .... = BSIC-NCELL: 46
```

B.　Step 2: handover from network

查找“RR__HANDOVER_COMMAND”

Target arfcn for handover

MOD_RRM	MOD_MPAL	RRM_MPAL_SAP	MSG_ID_RR_MPAL_HANDOVER_REQ			
after_time_channel	(struct)					
time_slot	0x03	3	0003		00000011	
ch_type	0x1b	27	0033		00011011	TCH_F
ch_mode	0x21	33	0041	!	00100001	SPEECH_FUI
freq_params	(struct)					
is_hopping	0x00	0	0000		00000000	KAL_FALSE
tsc	0x04	4	0004		00000100	
tsc_set	0x00	0	0000		00000000	
freq_comp	(struct)					
arfcn	0x02c0	704	0001300	02 c0	0000001011000000	

C.　Step 3: synchronization on target channel

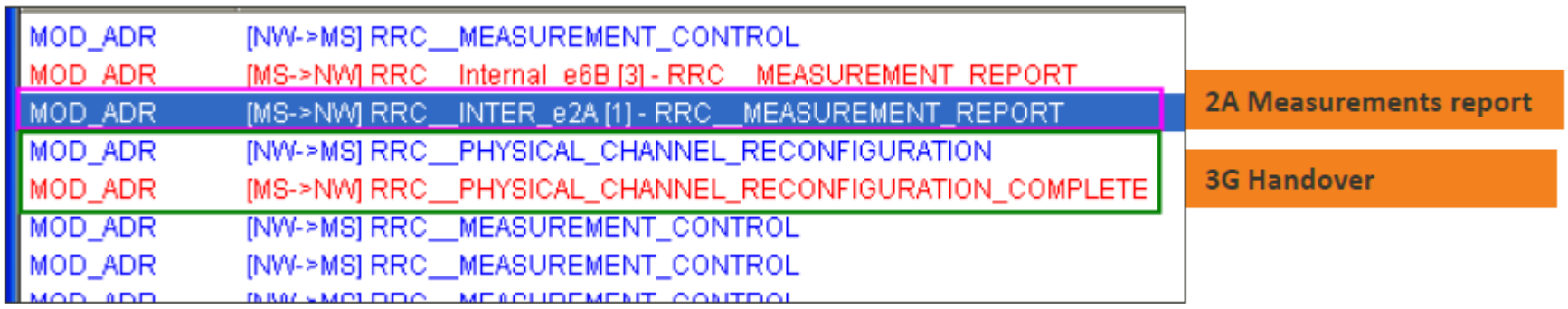
搜索“MSG_ID_MPAL_RR_HANDOVER_SUCCESS_IND

Handover success

MOD_RRM	MOD_MPAL	RRM_MPAL_SAP	MSG_ID_RR_MPAL_HANDOVER_STOP_REQ
MOD_RRM		TRACE_PEER	[NW->MS] RR__PHYSICAL_INFORMATION
MOD_MPAL	MOD_RRM	RRM_MPAL_SAP	MSG_ID_MPAL_RR_HANDOVER_SUCCESS_IND
MOD_RRM		TRACE_GRO...	[RRM][State-Msg] <RRM_DEDICATED_STATE> <RF
MOD_RRM	MOD_LAPDM	RRM_LAPDM...	MSG_ID_RR_LAPDM_RESUME_REQ
MOD_L1	MOD_LAPDM	L1_LAPDM_SAP	MSG_ID_LAPDM_DOWNLINK_IND
MOD_L1	MOD_RRM	L1_GAS_SAP	MSG_ID_LAPDM_RR_RESUME_CONF

”

(二)　3G Handover



Measurement event：

- Event 2a: Change of best frequency.
- Event 2d: The estimated quality of the currently used frequency is below a certain threshold
- Event 2f: The estimated quality of the currently used frequency is above a certain threshold
- event 1A: A Primary CPICH enters the reporting range
- event 1B: A primary CPICH leaves the reporting range
- event 1C: A non-active primary CPICH becomes better than an active primary CPICH
- event 1D: Change of best cell
- event 1F: A Primary CPICH becomes worse than an absolute threshold

A. Step 1: Receive the measurement control for inter handover from NW

搜索“RRC_MEASUREMENT_CONTROL”用来确认 2A 测量的网络配置

Source	Message
MOD_ADR	[NW->MS] RRC__MEASUREMENT_CONTROL
MOD_URR	Message has IntegrityCheckInfo present (message=9)
MOD_URR	performIntegrityCheck(): RB Id - 2, IP Config Idx - 0. Fresh value is 19880.
MOD_URR	Received SN(3) >= DL_SN(2) as it should be
MOD_URR	f9 Inputs count_i=3 fresh=19880, Key Index in DB= 1
MOD_URR	Used IK 5 77 3b fb 20 2 e7 fb 25
MOD_URR	USED IK 75 dc 0 5 77 3b fb
MOD_URR	f9 MAC=a2 e0 c8 87
MOD_URR	Received pIntegrityCheckInfo->messageAuthenticationCode = a2 e0 c8 87
MOD_URR	Integrity PASSED
MOD_ADR	[AdrUnpack]: Translation result is [decode status = 8, destination process = 4, interpreted event = 0] -- Lookup enumFile.txt for exact meaning.
MOD_MEME	MEME: update meme_time 383313 to 383315, sysTick prev = 1761204, now = 1761208, diff = 4 (1 s = 217.5 ticks)
MOD_MEME	MEME: meas ctrl measId 1, MEME_SETUP, RRC_DB_MI_measurementType_interFrequency, reportingMode(1), AddMeasList(0), MEME_MEA
MOD_MEME	MEME: measurement config by RRC_DB_MI_measurementConfiguredBy_measControl --> RRC_DB_MI_measurementConfiguredBy_m
MOD_MEME	MEME: reporting criteria eventList (1), MEME_SETUP
MOD_MEME	MEME: e2a-> h 12, RRC_TimeToTrigger_ttt 1280, rcs(1) RRC_ReportingCellStatus_withinMonitoredSetNonUsedFreq_selected
MOD_MEME	MEME: measId 1 ref RRC_FilterCoefficient_fc5, already exists fcIdx 0, bitmap 0

B. Step2: Measurement report

搜索“RRC__INTER_e2A [1] - RRC__MEASUREMENT_REPORT”

MOD_TL1	MSG_ID_CPHY_MEASUREMENT_CELL_IND
MOD_MEME	MEME: update meme_time 383955 to 383958, sysTick prev = 1762597, now = 1762602, diff = 5 (1 s = 217.5 ticks)
MOD_MEME	MEME: cell_ind (INTER_FREQUENCY_MEASURED) num_cell (15), iscp_included (0), <stMEME_CELL_DCH>, tid 161, fs_hal
MOD_MEME	MEME: uarfcn 10055, rssi -292
MOD_MEME	MEME: measReport allow = KAL_TRUE <- L1 tx allow (1), security mode (0), <stMEME_CELL_DCH>
MOD_MEME	MEME: evaluate and report of measId 1, RRC_DB_MI_measurementType_interFrequency, RRC_DB_MI_ReportCriteriaType_eventTrigge
MOD_MEME	MEME: usedFreq cell 10120/1 exists as intra-freq cell, cellID 0, cellID_bitmap 1
MOD_MEME	MEME: [e2a] best freq cell 10120/1, Q = -351678, h = 24576, ttt = 128, RRC_FilterCoefficient_fc5
MOD_MEME	MEME: evtInfo 10120/1, filteredRscp = -351678 (CIO = 0), RRC_DB_MI_eventStates_notSatisfied, triggerTime -2147483648
MOD_MEME	MEME: [e2a] best freq changed to nonUsedFreq, 10120/1 Q -351678 to 10055/68 Q -313446
MOD_MEME	MEME: evtInfo 10055/68, filteredRscp = -313446 (CIO = 12288), RRC_DB_MI_eventStates_satisfiedAndTriggered, triggerTime 383958
MOD_MEME	MEME: inter-freq measId 1 has evt triggered, addMeasWaitingList_bitmap = 0
MOD_MEME	MEME: pMI_rcs = RRC_ReportingCellStatus_withinMonitoredSetNonUsedFreq_selected, maxNumOfRepCells = 6
MOD_MEME	MEME: sortList[0] = cellId [3] 10055/68(116), rscp -325734
MOD_MEME	MEME: check for rcs type1, quota left = 6, RRC_ReportingCellStatus_withinMonitoredSetNonUsedFreq_selected
MOD_MEME	MEME: check and update leftNumOfRepCells [32] 10055/68, rcs type = 1, quota = 5, isAddCell = 1
MOD_MEME	MEME: cellMeasResults += 10055/68, pccpchRscp(1) = 36, pathloss(0) = 0, cellSyncInfo(1)
MOD_ADR	[AdrPack]: adr_pack_sendDCCH(): The UL-DCCH-Message [type = RRC_UL_DCCH_MessageType_measurementReport_selected, MU
MOD_ADR	[AdrPack]: The UL-DCCH-Message [type = RRC_UL_DCCH_MessageType_measurementReport_selected, length = 21 bytes] is encode
MOD_ADR	[MS->NW] RRC__INTER_e2A [1] - RRC__MEASUREMENT_REPORT

C. Step3: Physical channel reconfiguration

搜索“RRC_PHYSICAL_CHANNEL_RECONFIGURATION_COMPLETE”

```
MOD_ADR     [NW->MS] RRC__PHYSICAL_CHANNEL_RECONFIGURATION
MOD_ADR     [MS->NW] RRC__PHYSICAL_CHANNEL_RECONFIGURATION_COMPLETE

MOD_SLCE    MSG_ID_RRCE_SLCE_RECONFIG_COMPLETE_IND
MOD_SLCE    stSLCE_Configured
MOD_SLCE    [SLCE] Target state: stSLCE_Configured,  Ongoing procedure: NULL_PROC
MOD_RRCE    MSG_ID_CPHY_CHANNEL_PRIORITY_ADJUSTMENT_REQ
MOD_RRCE    Adjust channel prioirty to 0, purpose=SYNCA_PROCEDURE
MOD_RRCE    RRCE free the cell with psc = 68 and freq = 10055
MOD_RRCE    TM BHO: success
MOD_URR     Deleting configuration at index 0
MOD_ADR     [AdrPack]: adr_pack_sendDCCH(): The UL-DCCH-Message [type = RRC_UL_DCCH_Mes
MOD_ADR     [AdrPack]: The UL-DCCH-Message [type = RRC_UL_DCCH_MessageType_physicalChar
MOD_ADR     [MS->NW] RRC__PHYSICAL_CHANNEL_RECONFIGURATION_COMPLETE
```

(三) 4G Handover

A. Step1: Measurement configuration

在完整窗口中查找“[RPT] add measId””

```
[RPT] add LTE measObjId[2] earfcn[3200] bandwidth[0] port[0] ncellCfg[1] offFreq[0] cgi[65535]
[RPT] add LTE measObjId[2] earfcn[3200] cell list num[255] pci[348][0] [69][0] [13][0] [178][0] [310][0] [148][0] ...
[RPT] add LTE measObjId[3] earfcn[1351] bandwidth[0] port[0] ncellCfg[1] offFreq[0] cgi[65535]
[RPT] add LTE measObjId[3] earfcn[1351] cell list num[0] pci[0][0] [0][0] [0][0] [0][0] [0][0] [0][0] [0][0] [0][0]
[RPT] add EUTRA reportConfigId[1] event A1 thres[60] ThresholdEUTRA_threshold_RSRP_selected
[RPT] add EUTRA reportConfigId[2] event A2 thres[30] ThresholdEUTRA_threshold_RSRP_selected
[RPT] add EUTRA reportConfigId[15] event A4 thres[38] ThresholdEUTRA_threshold_RSRP_selected
[RPT] add EUTRA reportConfigId[16] event A3 offset[2] reportOnLeave[0]
[RPT] add measId[3] measObjId[1] reportConfigId[1]
[RPT] add measId[4] measObjId[2] reportConfigId[15]
[RPT] add measId[5] measObjId[3] reportConfigId[16]
[RPT] gap_valid[1] s_meas[0]=[-564]ERRC_MOB_SPEED_PARS_NO_CONFIG
```

Event Type	Meaning
Event A1	Serving becomes better than threshold
Event A2	Serving becomes worse than threshold
Event A3	Neighbor becomes offset better than serving
Event A4	Neighbor becomes better than threshold
Event A5	Serving becomes worse than threshold1 and neighbor becomes better than threshold2
Event B1	Inter RAT neighbor becomes better than threshold
Event B2	Serving becomes worse than threshold1 and inter RAT neighbor becomes better than threshold2

Used for Intra-LTE HO

Used for inter-RAT HO

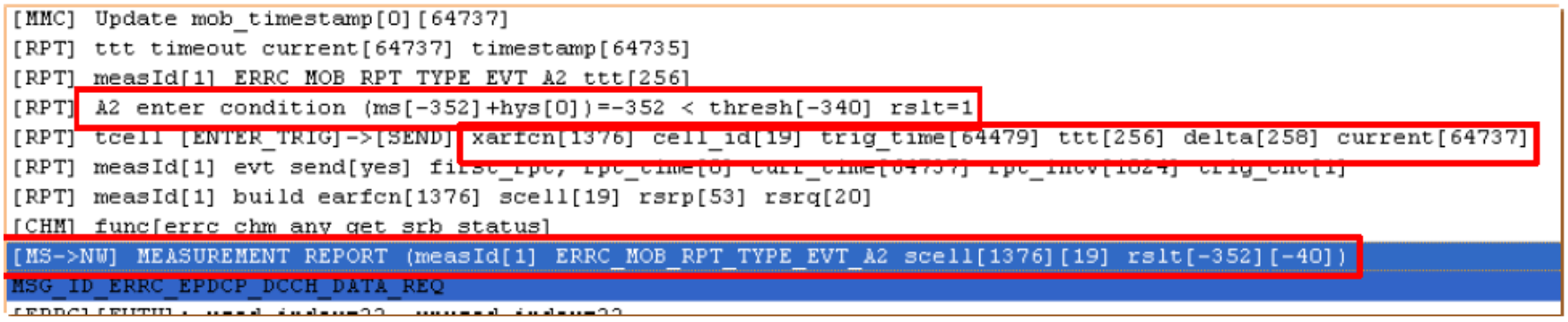
B. Step2: Measurement report

在完整窗口中查找“MSG_ID_ERRC_EL1_RADIO_MEASURE_IND”得到小区的测量结果

```
SAP    MSG_ID_ERRC_EL1_RADIO_MEASURE_IND
```

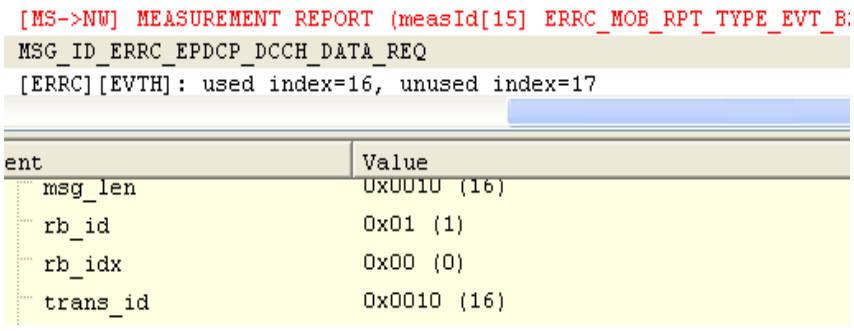
ement	Value
serving	(struct)
intra	(struct)
offset	0x0000 0000 0000 00
rule	EL1_MEAS_RULE_TRUE
num	0x04 (4)
cell	Array [16]
cell [0] (el1_meas_result_struct)	(struct)
pci	0x00bd (189)
rsrp	0xfe40 (-448)
rsrq	0xffc5 (-59)

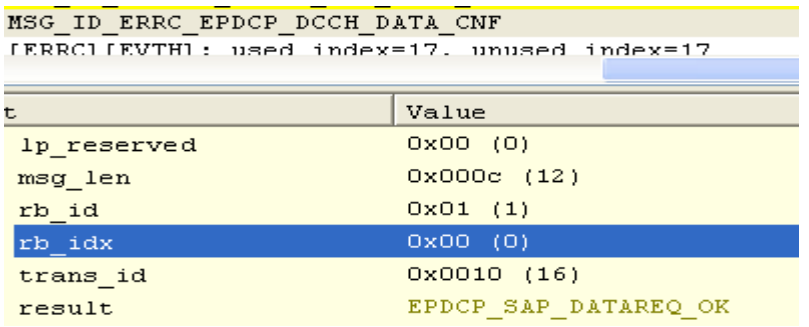
查找“evt send[yes]”



C. Step3: Measurement report send

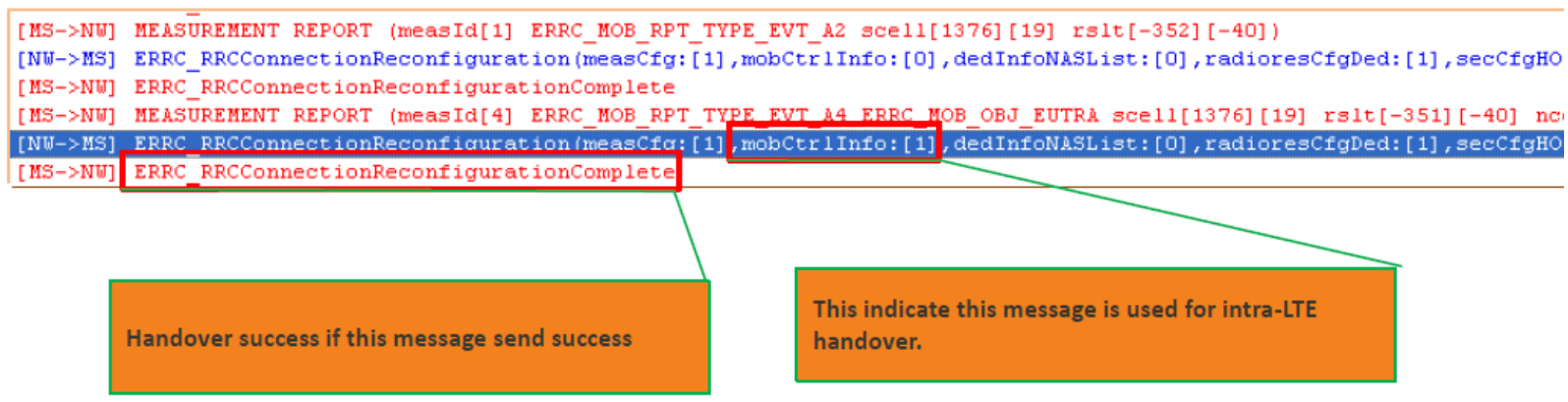
查找“MSG_ID_ERRC_EPDCP_DCCH_DATA_REQ”和“MSG_ID_ERRC_EPDCP_DCCH_DATA_CNF”查看测量报告，“trans_id”需要相等才说明测量报告是发送成功的。





D. Step4: Handover command

搜索“mobCtrlInfo: [1]”



如果以上任一步骤失败，请提交 MTK。

(四) Inter RAT Handover

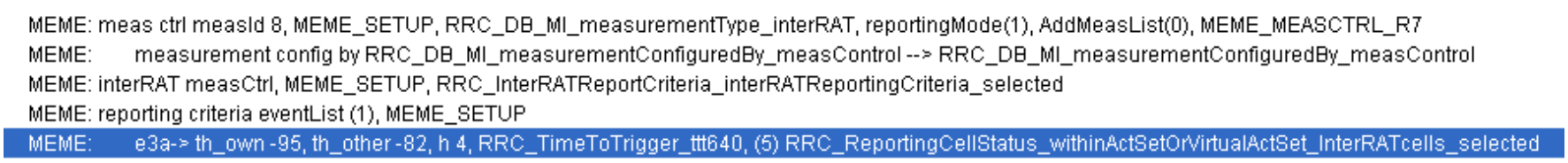
A. 3G->2G

a. Step 1: Inter RAT Measurement control

搜索“[NW->MS] RRC__MEASUREMENT_CONTROL__setup [6] – IR”并查看参数

如果没有找到，大部分原因是由于网络问题，此时需要查看对比及情况

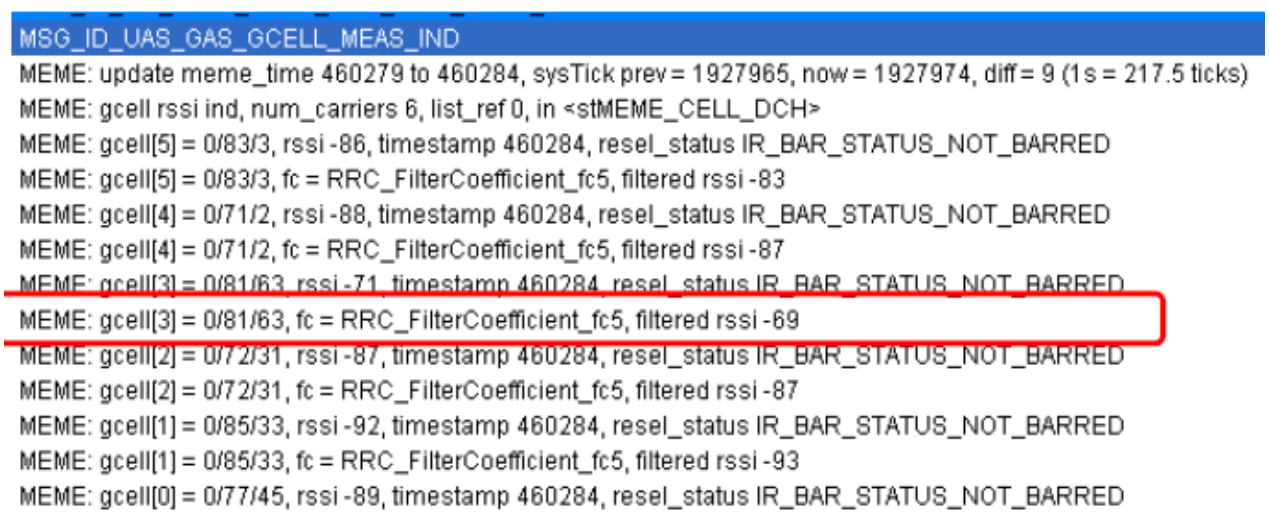
3G 阀值为-95-h/2=-97，2G 阀值为-82+h/2=-80, ttt=640ms

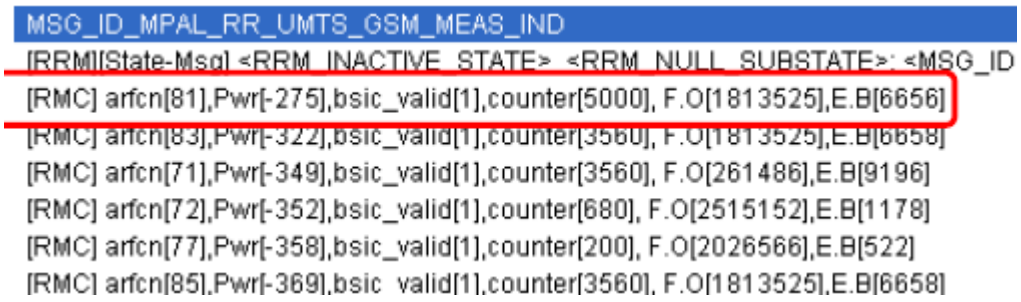


b. Step 2: Measure 2G cell

搜索“MSG_ID_UAS_GAS_GCELL_MEAS_IND”和“MSG_ID_MPAL_RR_UMTS_GSM_MEAS_IND”

如果没有找到，大部分原因是由于网络没有配置 3A 测量控制



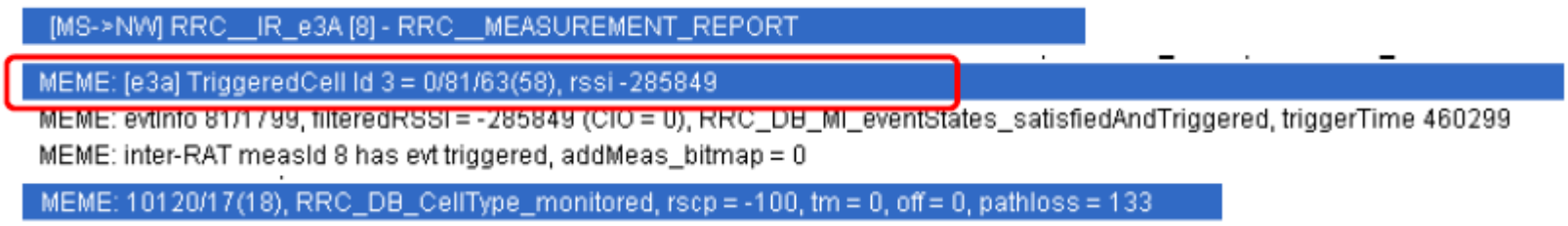


c. Step 3: Report inter RAT report(eg：3A)

搜索“RRC__IR_e3A - RRC__MEASUREMENT_REPORT”

如果没有找到，大部分原因是小区的 2G、3G 不满足 3A 测量条件

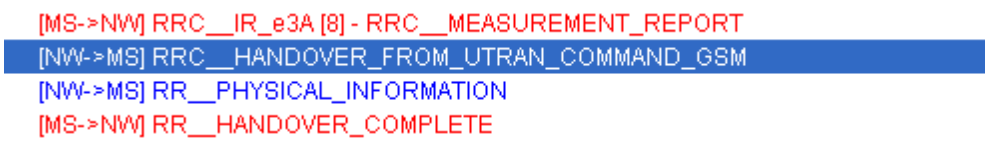
2G：arfcn 81,RSSI=-71>-80；3G：RSCP=-100<-97，均满足条件，所以 UE 向网络发送测量报告。



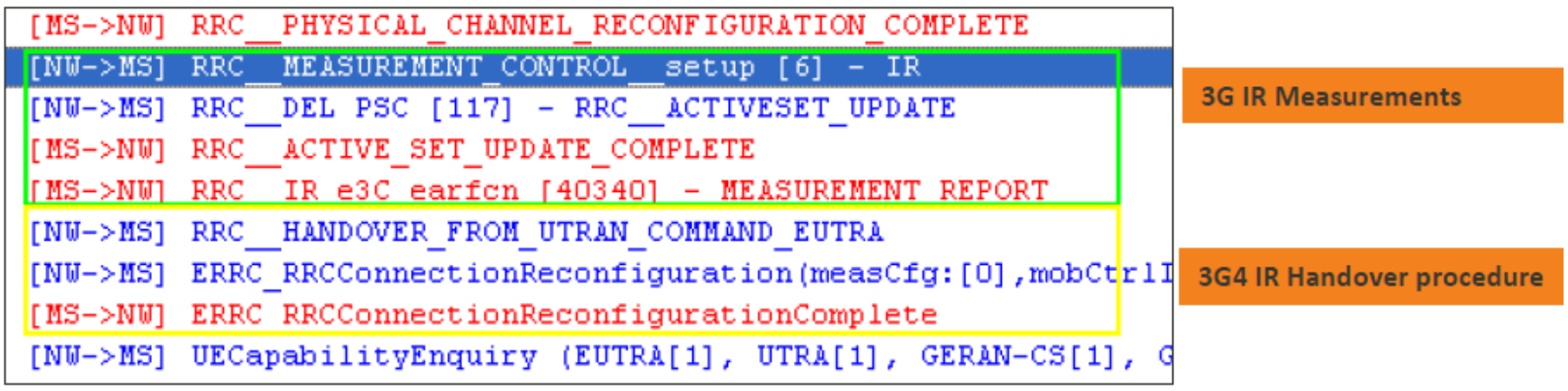
d. Step 4: Handover

搜索“RRC__HANDOVER_FROM_UTRAN_COMMAND_GSM”和“RR__HANDOVER_COMPLETE”

如果没有搜到，大部分情况是由于 3G 信号差，或是 UE 发生链路失败，此时可参考对比机

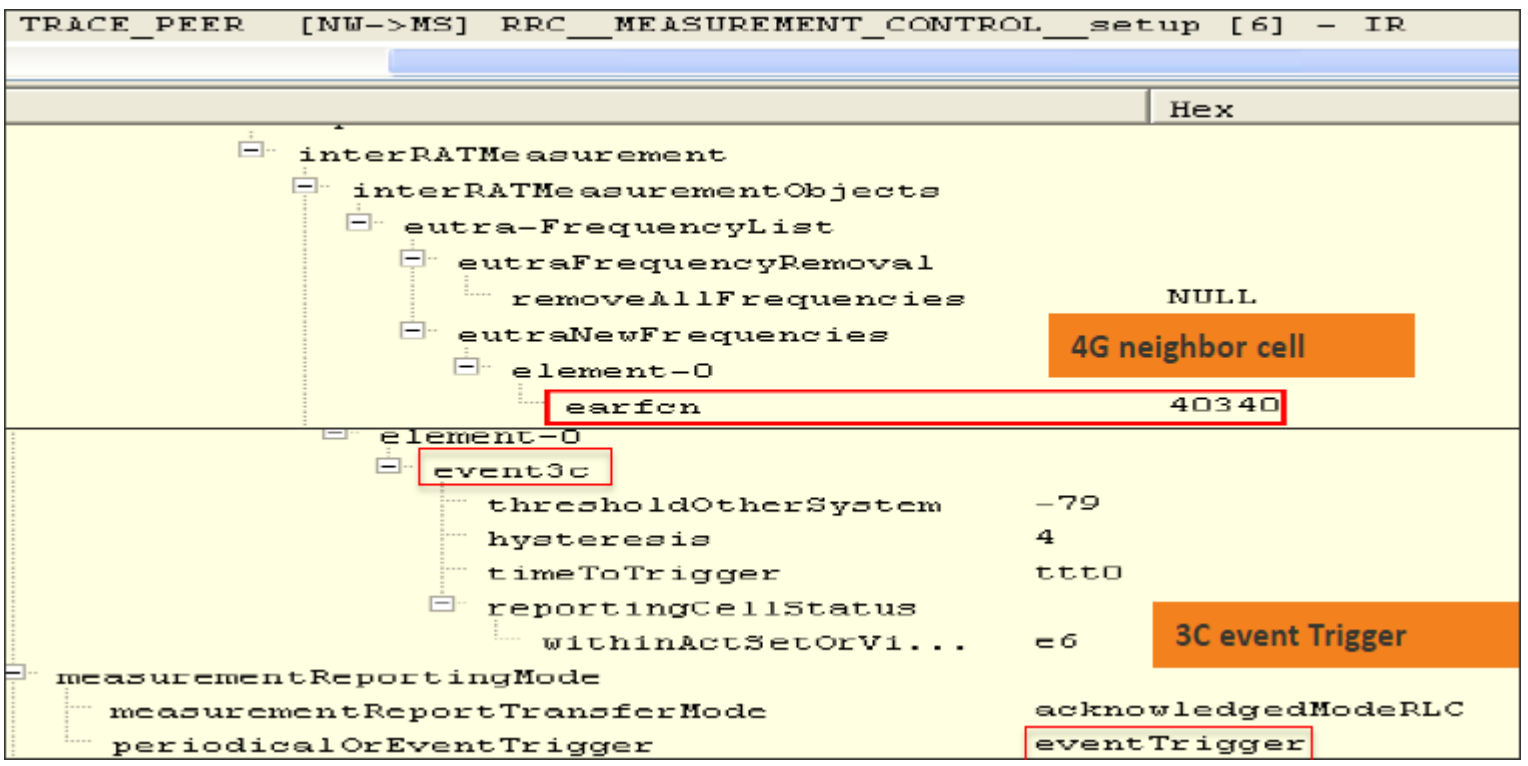


B. 3G->4G



a. Step 1: Receive the measurement control for handover from NW

搜索“MEASUREMENT_CONTROL__setup [?] - IR”

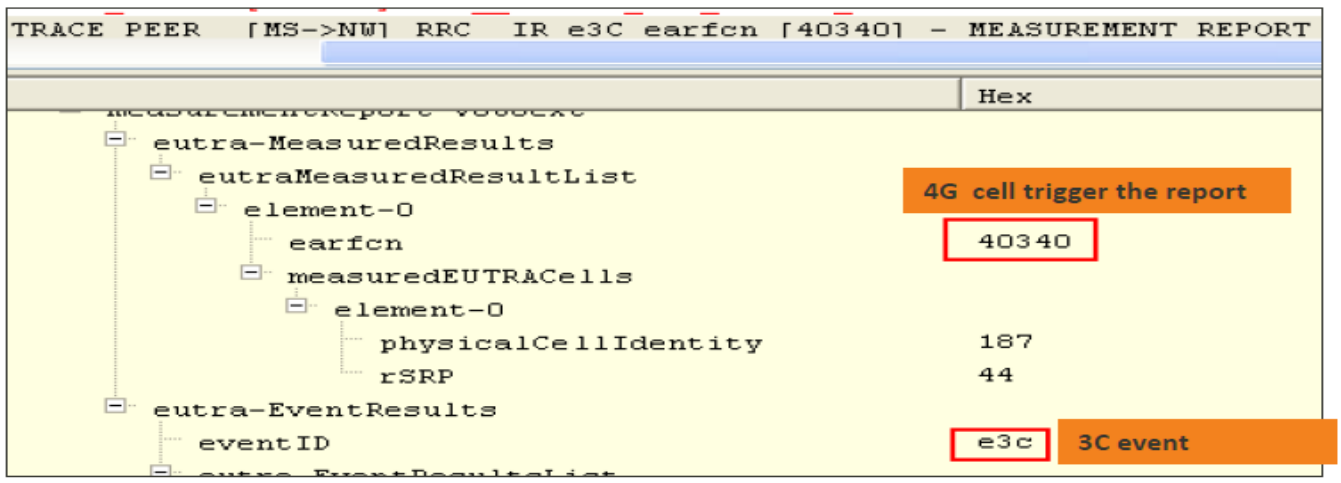


b. Step 2: 3G4 handover Measurements report

搜索“MEME: Add LTE event result EARFCN”

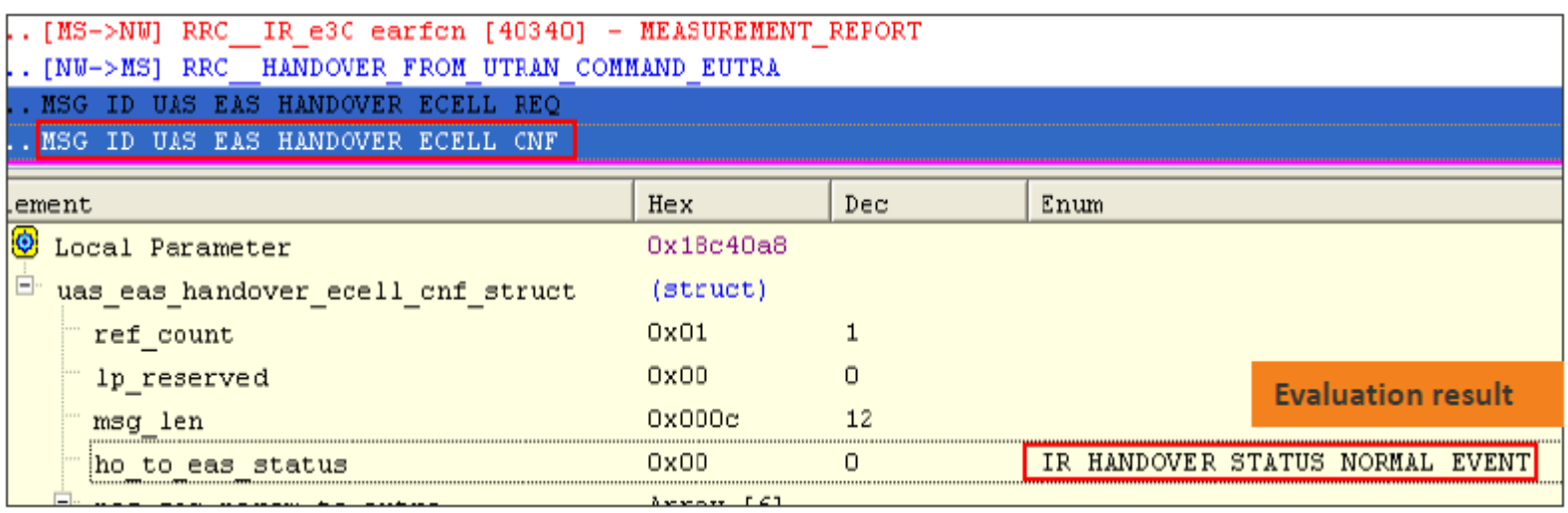
```
MEME: measId 6, e3c, Thre -104, H 4, TTT RRC_TimeToTrigger_ttt0
MEME: measId 6, RRC_InterRATEvent_event3c_selected, LTE DB cell index 0, measQT:
RRC_MeasurementQuantityEUTRA_rrsp =-97, changed from RRC_DB_MI_eventStates_stateUnknown to
DB_MI_eventStates_satisfiedButNotTriggered, CurrTime=1318934, NextTime=1318934
MEME: measId 6, RRC_InterRATEvent_event3c_selected, LTE DB cell index 0 (EARFCN=-25196, PCI=187), changed from
RRC_DB_MI_eventStates_satisfiedButNotTriggered to RRC_DB_MI_eventStates_satisfiedAndTriggered
MEME: Add LTE event result EARFCN: 40340, PCI: 187 for event RRC_EventIDInterRAT_e3c, RSRP: -96, RSRQ: -7
MEME: Add LTE measured result EARFCN: 40340, PCI: 187, RSRP 44
MEME: send MEASUREMENT REPORT using RRC_TransferMode_acknowledgedModeRLC
[AdrPack]: adr_pack_sendDCCH(): The UL-DCCH-Message [type = RRC_UL_DCCH_MessageType_measurementReport_selected,
MUI = 1932, rbID = RRC_DB_RB_ID_dcch2, ackRequired = 1, ackEvent = 25, src_mod_id = MOD_MEME, sap_id =
MEME_DRLC_SAP]
[AdrPack]: The UL-DCCH-Message [type = RRC_UL_DCCH_MessageType_measurementReport_selected, length = 19 bytes] i
encoded successfully for delivering to RLC.
MSG_ID_USER_WAKEUP_3G_LOCK_REQ
f9 Inputs count_i=11 fresh=24517, Key Index in DB= 0
f9 MAC=43 87 23 dd
MSG_ID_USER_WAKEUP_3G_UNLOCK_REQ
[MS->NW] RRC__IR_e3C earfcn [40340] - MEASUREMENT_REPORT
```

搜索“MEASUREMENT_REPORT”查看 UE 向网络发送的测量报告



c. Step 3 : Evaluation phase

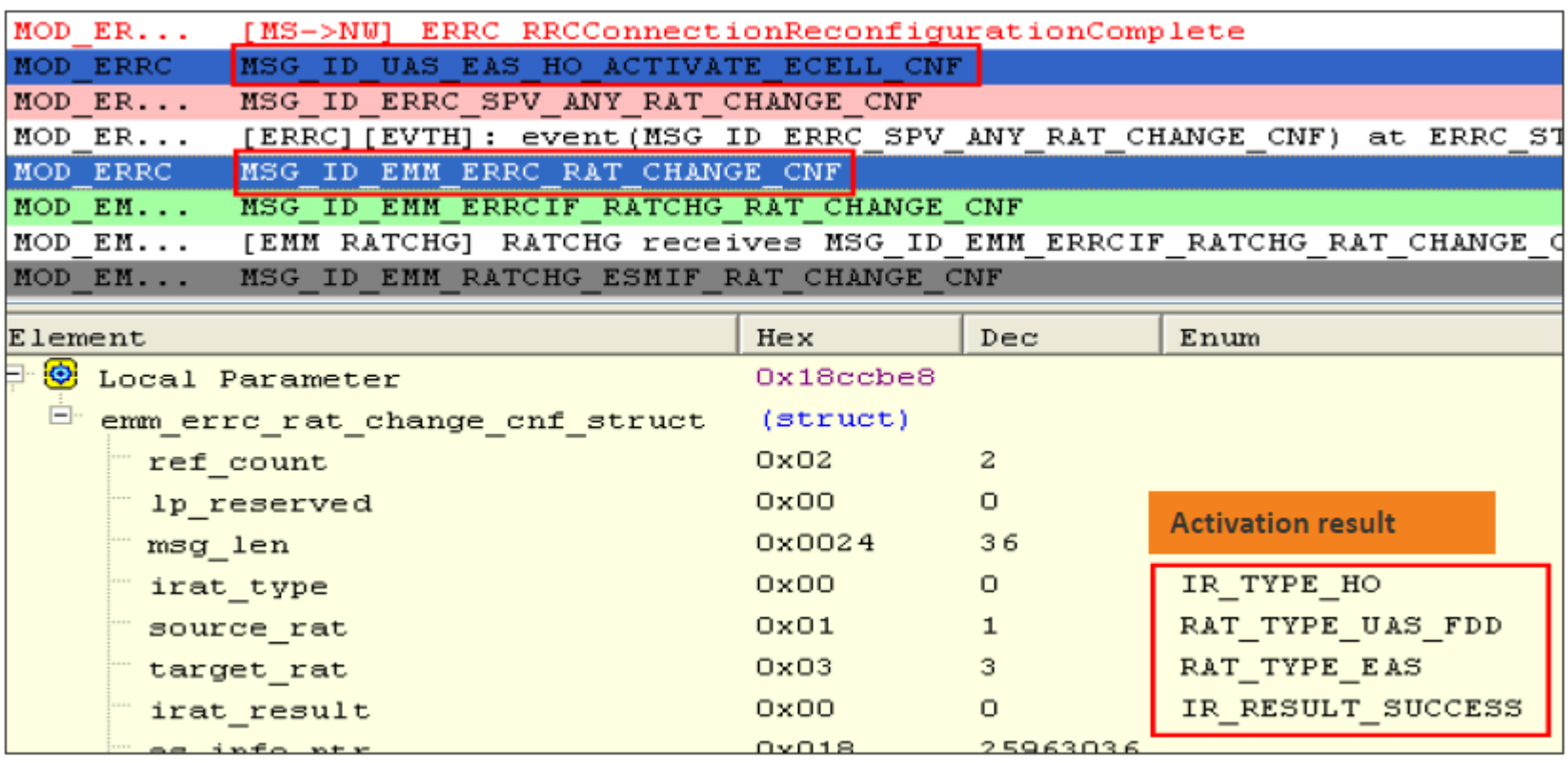
搜索“UAS_EAS_HANDOVER_ECELL_CNF



”

d. Step 4 : Activation phase

搜索“EMM_ERRC_RAT_CHANGE_CNF”



C. 4G->3G

a. Step 1: Measurement configuration(same as 4G handover)

b. Step 2: Measurement report evaluate

搜索“MSG_ID_EAS_UAS_UCELL_MEAS_IND”

```
MSG_ID_CSCE_MEME_CELL_MEASUREMENT_RESULT_IND
MEME: PSC 399, RSCP -81, EcNO -8, RRC_DB_CellType_monitored, SyncInfo(0), TM(0
MEME: PSC 194, RSCP -82, EcNO -9, RRC_DB_CellType_monitored, SyncInfo(0), TM(0
MEME: PSC 193, RSCP -92, EcNO -19, RRC_DB_CellType_monitored, SyncInfo(0), TM(0
MSG_ID_EAS_UAS_UCELL_MEAS_IND
[ERRC][EVTH]: judge function(MOD_ERRC_MOB), judge result is EVT_JDG_EXECUTE, f
[ERRC][EVTH]: event(MSG_ID_EAS_UAS_UCELL_MEAS_IND) at ERRC_STS_CONNECTED. judge
[MMC] Update mob_timestamp[0][955498]
[IMRM] Update umts cell info: uarfcn[10713], psc[399], rscp[-340], ec_n0[-53]
[IMRM] Update umts cell info: uarfcn[10713], psc[194], rscp[-325], ec_n0[-38]
[IMRM] Update umts cell info: uarfcn[10713], psc[193], rscp[-347], ec_n0[-59]
```

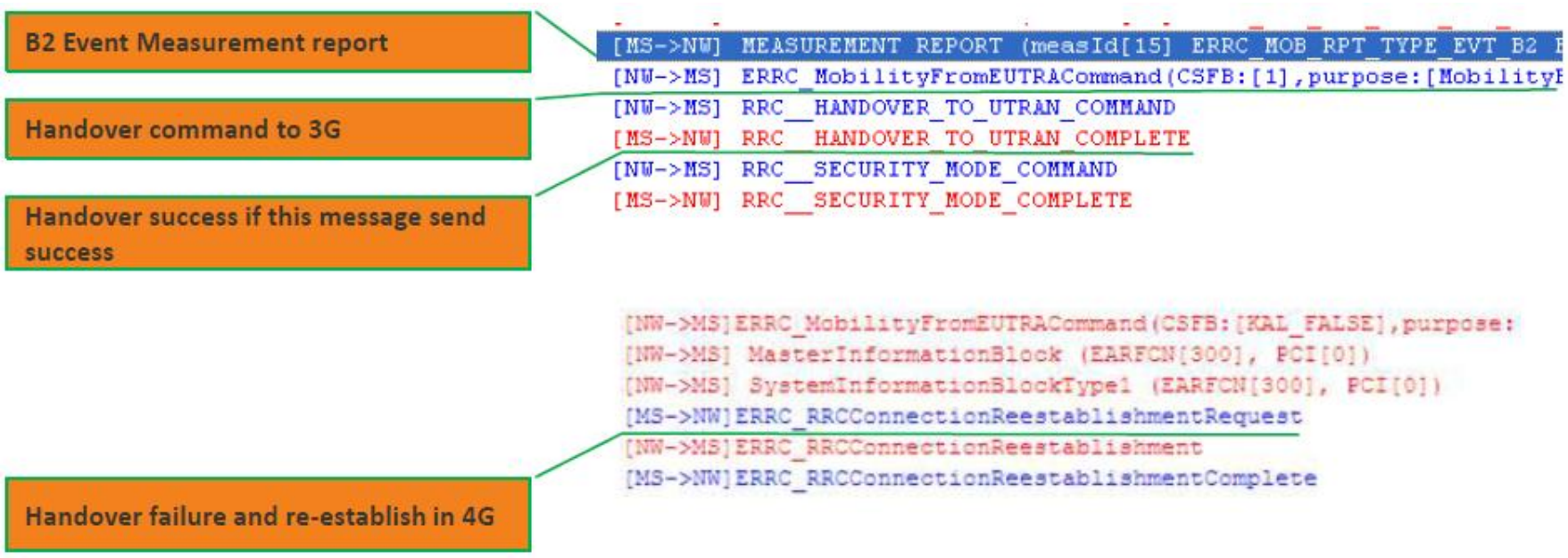
搜索“evt send[yes]”

```
[RPT] B1 enter cell_id[399] (mn[-340]+ofn[0]-hys[4])=-344 > thresh[-412]) rslt=1
[RPT] measId[5] tcell [ENTER_TRIG]->[SEND] xarfcn[10713] cell_id[399] trig_time[954865] ttt[640] delta[642] current|
[RPT] B1 enter cell_id[194] (mn[-325]+ofn[0]-hys[4])=-329 > thresh[-412]) rslt=1
[RPT] measId[5] tcell [ENTER_TRIG]->[SEND] xarfcn[10713] cell_id[194] trig_time[954865] ttt[640] delta[642] current|
[RPT] B1 enter cell_id[193] (mn[-347]+ofn[0]-hys[4])=-351 > thresh[-412]) rslt=1
[RPT] measId[5] tcell [ENTER_TRIG]->[SEND] xarfcn[10713] cell_id[193] trig_time[954865] ttt[640] delta[642] current|
[RPT] measId[5] evt send[yes] first_rpt, rpt_time[0] curr_time[955507] rpt_intv[480] trig_cnt[3]
[RPT] measId[5] build earfcn[40340] scell[186] rsrp[33] rsrq[19]
[RPT] measId[5] build uarfcn[10713] psc[194] rscp[34]=[-325] (ecn0[-38])
[RPT] measId[5] build uarfcn[10713] psc[399] rscp[31]=[-340] (ecn0[-53])
[RPT] measId[5] build uarfcn[10713] psc[193] rscp[29]=[-347] (ecn0[-59])
[CHM] func[errc_chm_any_get_srb_status]
[MS->NW] MEASUREMENT REPORT (measId[5] ERRC_MOB_RPT_TYPE_EVT_B1 ERRC_MOB_OBJ_UTRA scell[40340][186] rslt[-431][-42]
```

c. Step 3: Measurement report send success(same as 4G handover)

d. Step 4: Handover command

搜索“ERRC_MobilityFromEUTRACommand”



八、 PDP Activate

(一) 2/3G PDP Activate

A. 2G PDP Activate Normal Flow

AP Send AT command to Activate PDP, you can check PDP parameters from these AT commands
1.AT+CGDCONT is used to set APN
2.AT+CGPRCO is used to set "User name" "Password" and "Auth_type"
3.AT+CGACT is used to activate PDP

Sys Trace

Local Time	Message
10:59:53:025 2013/11/29	[AT_R p44, s7]+COPS: 0,2,"46000"
10:59:53:025 2013/11/29	[AT_R p44, s7]OK
10:59:53:025 2013/11/29	[AT_I p42, s5]AT+CGDCONT=1,"IP","cmwap",,0,0
10:59:53:025 2013/11/29	[AT_R p42, s5]OK
10:59:53:025 2013/11/29	[AT_I p42, s5]AT+CGEREP=1,0
10:59:53:025 2013/11/29	[AT_R p42, s5]OK
10:59:53:025 2013/11/29	[AT_I p42, s5]AT+CGPRCO=1,"","","",",2,1
10:59:53:025 2013/11/29	[AT_R p42, s5]OK
10:59:53:025 2013/11/29	[AT_I p42, s5]AT+CGACT=1,1
10:59:53:025 2013/11/29	[AT_R p42, s5]+CGEV: ME PDN ACT 1
10:59:53:025 2013/11/29	[AT_R p42, s5]OK

APN

User name and Password

Auth_type
0: PAP
1: CHAP
2: None
3: PAP+CHAP

0: deactivate
1: activate

Primitive Log : TracePeer Window for Air Mes... ly.

When receive the AT command Modem will send SM__ACTIVATE_PDP_CONTEXT_REQUEST Then the Network will answer SM__ACTIVATE_PDP_CONTEXT_ACCEPT

Local Time	Source	Message
10:59:53:009 ...	MOD_RRM	[NW->MS] RR__PACKET_UPLINK_ACK_NACK
10:59:53:009 ...	MOD_RRM	[MS->NW] RR__PACKET_DOWNLINK_ACK_NACK (FN=1692002 TS=2)
10:59:53:025 ...	MOD_RRM	[MS->NW] RR__PACKET_DOWNLINK_ACK_NACK (FN=1692015 TS=2)
10:59:53:025 ...	MOD_SM	[MS->NW] SM__ACTIVATE_PDP_CONTEXT_REQUEST
10:59:53:025 ...	MOD_RRM	[NW->MS] RR__PACKET_UPLINK_ACK_NACK
10:59:53:025 ...	MOD_RRM	[NW->MS] RR__PACKET_UPLINK_ACK_NACK
10:59:53:025 ...	MOD_SM	[NW->MS] SM__ACTIVATE_PDP_CONTEXT_ACCEPT
10:59:53:025 ...	MOD_RRM	[NW->MS] RR__PACKET_UPLINK_ACK_NACK

B. 3G PDP Activate Normal Flow

AP Send AT command to Activate PDP, you can check PDP parameters from these AT commands
1.AT+CGDCONT is used to set APN
2.AT+CGPRCO is used to set "User name" "Password" and "Auth_type"
3.AT+CGACT is used to activate PDP

Sys Trace

Local Time	Message
10:59:53:025 2013/11/29	[AT_R p44, s7]+COPS: 0,2,"46000"
10:59:53:025 2013/11/29	[AT_R p44, s7]OK
10:59:53:025 2013/11/29	[AT_I p42, s5]AT+CGDCONT=1,"IP","cmwap",,0,0
10:59:53:025 2013/11/29	[AT_R p42, s5]OK
10:59:53:025 2013/11/29	[AT_I p42, s5]AT+CGEREP=1,0
10:59:53:025 2013/11/29	[AT_R p42, s5]OK
10:59:53:025 2013/11/29	[AT_I p42, s5]AT+CGPRCO=1,"","","",",2,1
10:59:53:025 2013/11/29	[AT_R p42, s5]OK
10:59:53:025 2013/11/29	[AT_I p42, s5]AT+CGACT=1,1
10:59:53:025 2013/11/29	[AT_R p42, s5]+CGEV: ME PDN ACT 1
10:59:53:025 2013/11/29	[AT_R p42, s5]OK

When receive the AT command Modem will send GMM_SERVICE_REQUEST to establish the PS signaling, after security mode complete, modem will send SM__ACTIVATE_PDP_CONTEXT_REQUEST then the Network will setup radio bearer and answer SM__ACTIVATE_PDP_CONTEXT_ACCEPT

[MS->NW]	GMM__SERVICE_REQUEST
[NW->MS]	RRC_SI_SIB7 (UARFCN:[9405], PSC:[103])
[MS->NW]	RRC__RRC_CONNECTION_REQUEST
[NW->MS]	RRC__RRC_CONNECTION_SETUP
[MS->NW]	RRC__RRC_CONNECTION_SETUP_COMPLETE
[MS->NW]	RRC__INITIAL_DIRECT_TRANSFER
[NW->MS]	RRC__MEASUREMENT_CONTROL__setup [2] - INTER
[NW->MS]	RRC__DOWNLINK_DIRECT_TRANSFER
[NW->MS]	GMM__IDENTITY_REQUEST
[MS->NW]	GMM__IDENTITY_RESPONSE
[MS->NW]	RRC__UPLINK_DIRECT_TRANSFER
[NW->MS]	RRC__SECURITY_MODE_COMMAND
[MS->NW]	RRC__SECURITY_MODE_COMPLETE
[MS->NW]	SM__ACTIVATE_PDP_CONTEXT_REQUEST
[MS->NW]	RRC__UPLINK_DIRECT_TRANSFER
[NW->MS]	RRC__RADIO_BEARER_SETUP
[MS->NW]	RRC__RADIO_BEARER_SETUP_COMPLETE
[NW->MS]	RRC__DOWNLINK_DIRECT_TRANSFER
[NW->MS]	SM__ACTIVATE_PDP_CONTEXT_ACCEPT

C. 2/3G PDP Activate Fail

a. case 1：网络没有响应 SM__ACTIVATE_PDP_CONTEXT_ACCEPT

搜索“PDP”，可以看到没有 PDP ACCEPT，原因可能是：1.参数不正确；2.网络问题；3.PDP 没有发送成功

然后检查参数如 APN，用户名，密码，auth_type 等，如果一致请提交 MTK

MOD_SM	TRACE_PEER	[MS->NW] SM__ACTIVATE_PDP_CONTEXT_REQUEST
MOD_SM	TRACE_PEER	[MS->NW] SM__ACTIVATE_PDP_CONTEXT_REQUEST
MOD_SM	TRACE_PEER	[MS->NW] SM__ACTIVATE_PDP_CONTEXT_REQUEST
MOD_SM	TRACE_PEER	[MS->NW] SM__ACTIVATE_PDP_CONTEXT_REQUEST
MOD_SM	TRACE_PEER	[MS->NW] SM__ACTIVATE_PDP_CONTEXT_REQUEST

b. case 2：网络响应 SM__ACTIVATE_PDP_CONTEXT_REJECT

搜索“PDP”，可以看到 PDP 被网络拒绝，原因可能是：1.参数不对；2.网络问题

然后检查参数如 APN，用户名，密码，auth_type 等，如果一致请提交 MTK

```
MOD_SM        TRACE_PEER        [MS->NW] SM__ACTIVATE_PDP_CONTEXT_REQUEST
MOD_SM        TRACE_PEER        [NW->MS] SM__ACTIVATE_PDP_CONTEXT_REJECT
```

(二) 2/3G PS Issue Checklist

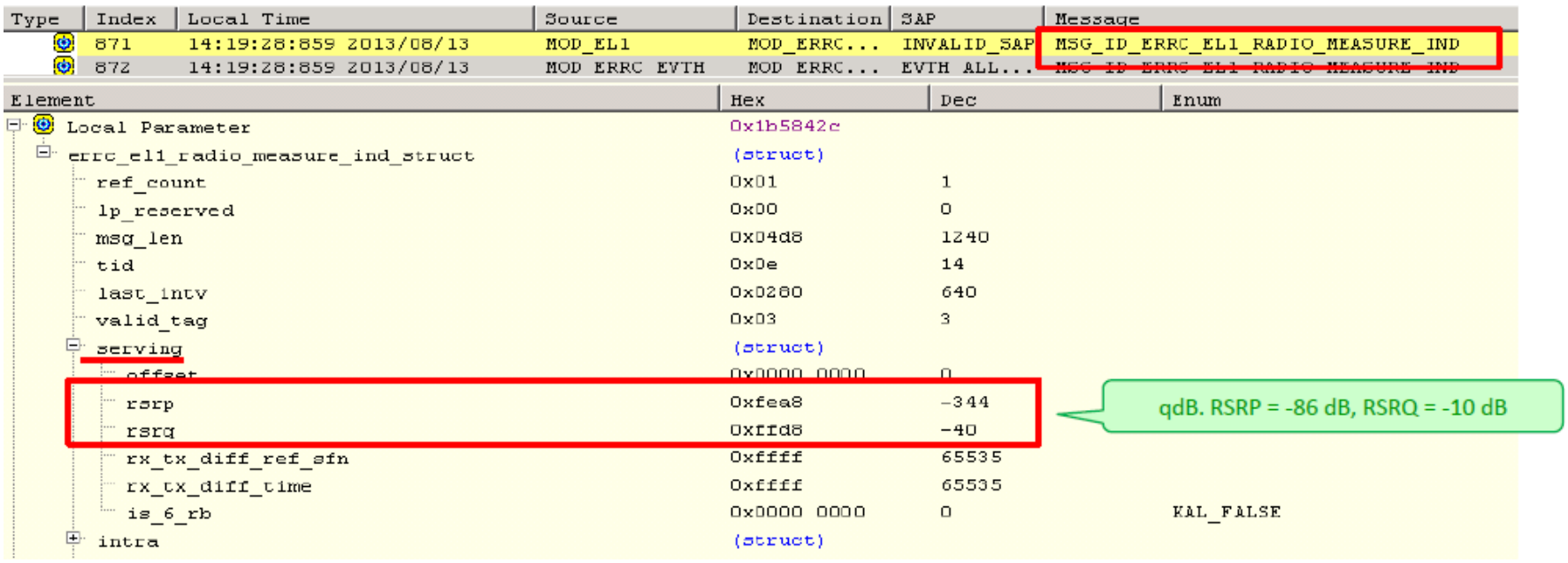
例如无法打开 WAP、打开 WAP 慢慢、不能发送彩信，发送彩信，或 PS 吞吐量问题，检查如下项

A. **[23G] Check the Parameters the same as REF, such as APN, User Name, Password,Auth_type**
B. **[2G]Check the PA with your RF engineer , if the PA is not linear and not support Uplink EDGE, you should turn off Uplink EDGE in Modem Make File, add CUSTOM_OPTION +=__EPSK_TX_SW_SWITCH_OFF__ in the Modem Make File**
C. **[23G]Check the RF calibration and Antenna Performance, RF calibration should be done successfully, Antenna Performance should meet the FT standard**
D. **[23G]Check the REF Phone, to see whether it is ok or not , please do the test under the same conditions with MTK Phone**
E. **[23G]If the Issue is related to PS throughput , you can set MTK Phone to “Data Prefer” and test again (Engineering Mode->Telephony->Mobile data service preferred->Reboot)**
F. **[23G]If you have already checked these, you can submit CR to MTK**

九、 Appendix（附录）

(一) 4G signal power

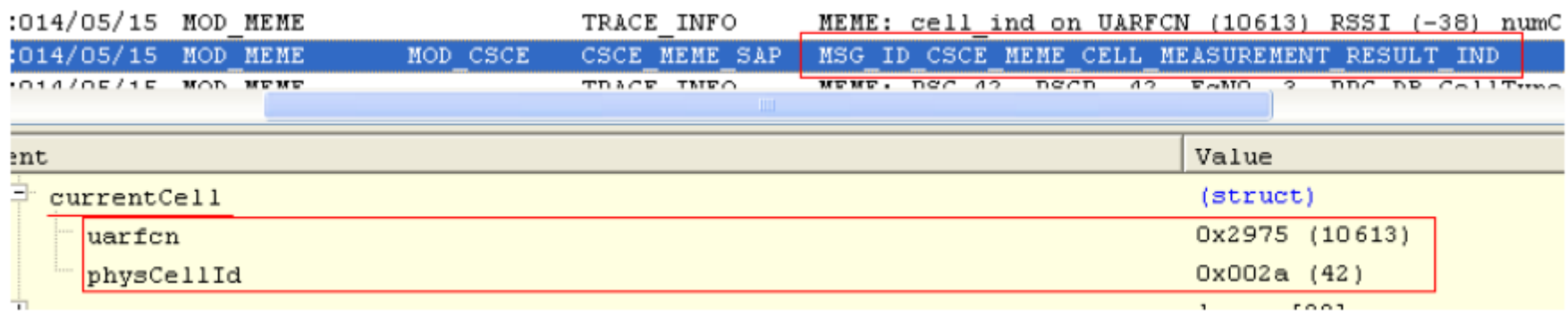
搜索“MSG_ID_ERRC_EL1_RADIO_MEASURE_IND”



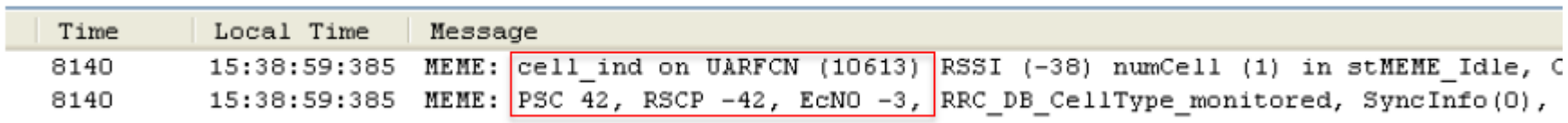
(二) 3G signal power

A. For 3G serving cell in idle mode

搜索“MSG_ID_CSCE_MEME_CELL_MEASUREMENT_RESULT_IND”

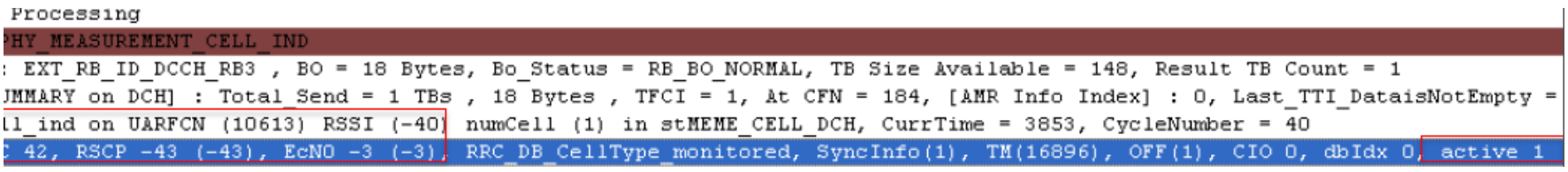


搜索“MEME: cell_ind on UARFCN”



B. For FDD connected mode

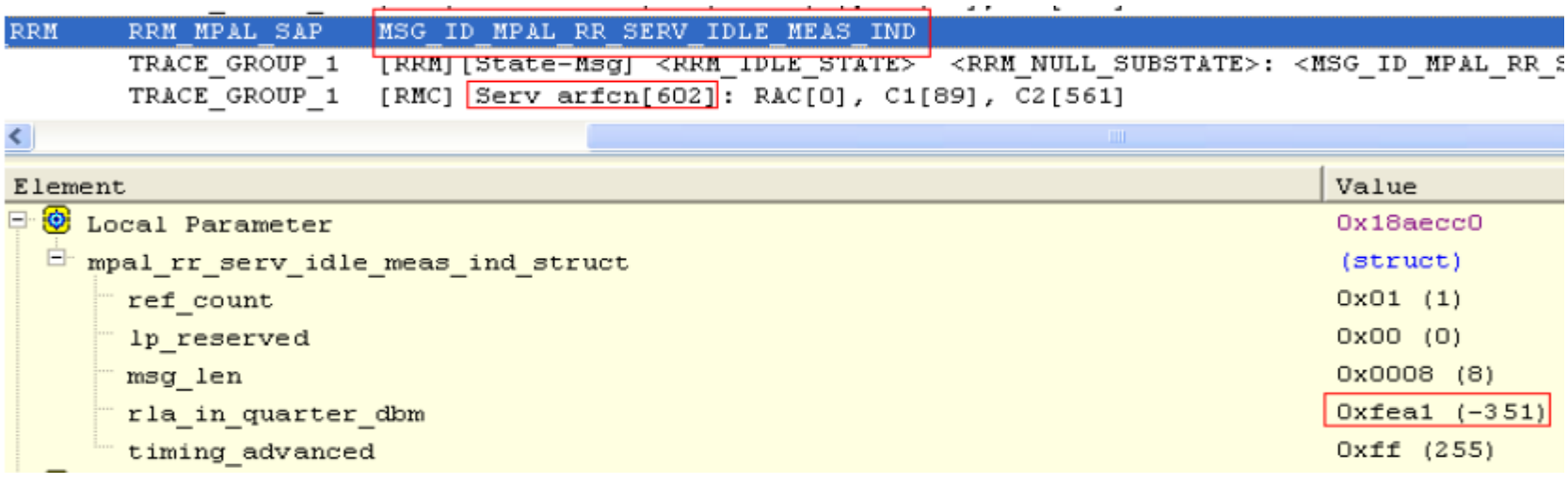
搜索“active 1”



(三) 2G signal power

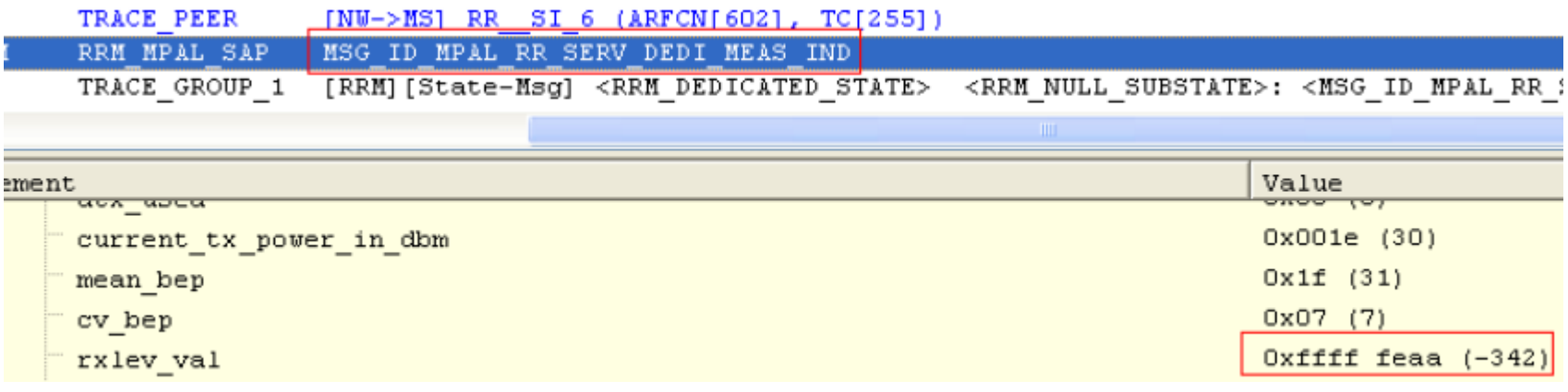
A. For 2G idle mode

搜索“MSG_ID_MPAL_RR_SERV_IDLE_MEAS_IND”



B. For 2G dedicated mode

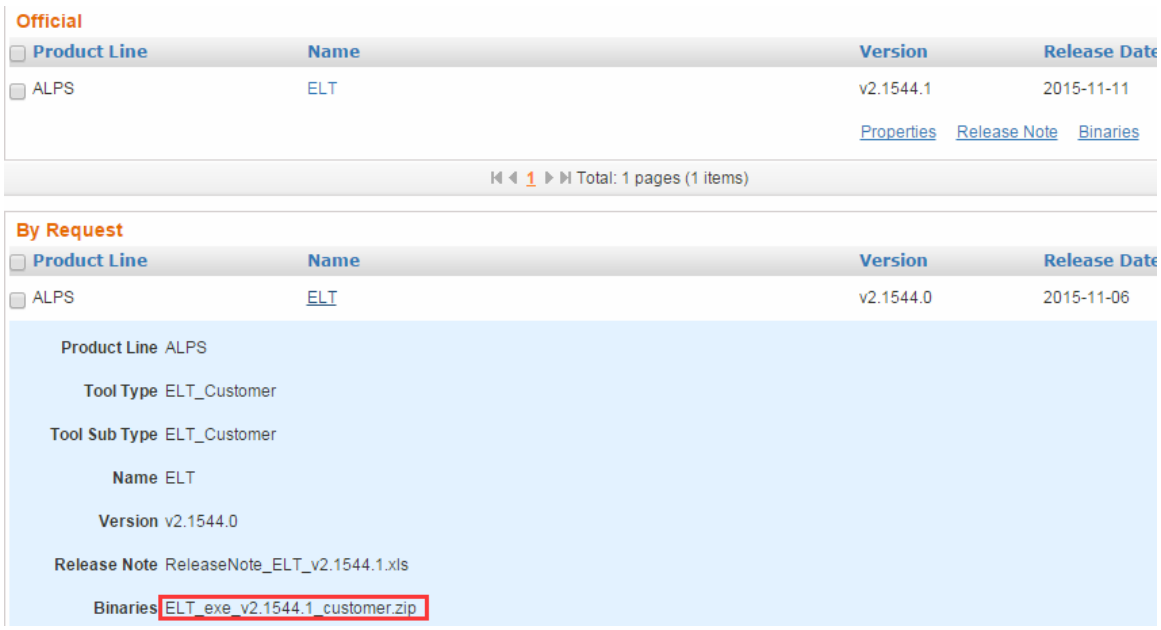
搜索“MSG_ID_MPAL_RR_SERV_DEDI_MEAS_IND”



十、 ELT Tools

(一) Download

在 MTK online 上搜索 ELT，会出现两个，DCC 下载的版本后缀为 Lite，这个是简版，好多窗口无法打开，需要 request 后缀为 customer 的版本。



(二) Simple Introduction