



Unisoc Confidential For hiar

# GSM LOG 分析指南

文档版本  
发布日期

V1.0  
2020-11-20

**版权所有 © 紫光展锐（上海）科技有限公司。保留一切权利。**

本文件所含数据和信息都属于紫光展锐（上海）科技有限公司（以下简称紫光展锐）所有的机密信息，紫光展锐保留所有相关权利。本文件仅为信息参考之目的提供，不包含任何明示或默示的知识产权许可，也不表示有任何明示或默示的保证，包括但不限于满足任何特殊目的、不侵权或性能。当您接受这份文件时，即表示您同意本文件中内容和信息属于紫光展锐机密信息，且同意在未获得紫光展锐书面同意前，不使用或复制本文件的整体或部分，也不向任何其他方披露本文件内容。紫光展锐有权在未经事先通知的情况下，在任何时候对本文件做任何修改。紫光展锐对本文件所含数据和信息不做任何保证，在任何情况下，紫光展锐均不负任何与本文件相关的直接或间接的、任何伤害或损失。

请参照交付物中说明文档对紫光展锐交付物进行使用，任何人对紫光展锐交付物的修改、定制化或违反说明文档的指引对紫光展锐交付物进行使用造成的任何损失由其自行承担。紫光展锐交付物中的性能指标、测试结果和参数等，均为在紫光展锐内部研发和测试系统中获得的，仅供参考，若任何人需要对交付物进行商用或量产，需要结合自身的软硬件测试环境进行全面的测试和调试。

Unisoc Confidential For hiar

**紫光展锐（上海）科技有限公司**



# 前言

## 概述

本文档详细介绍了使用展锐工具分析 GSM/EDGE 下常见问题的方法。

## 读者对象

本文档主要适用于需要分析 GSM/EDGE 下通讯问题的所有人员。


## 缩略语

缩略语	英文全名	中文解释
ACK	Acknowledge Character	确认字符
AGCH	Access Brant Channel	允许接入信道
AS	Access Stratum	接入层
BCCH	Broadcast Control Channel	广播控制信道
BSIC	Base Station Identity Code	基站识别码
CT	Candidate Time	候选时间
EDGE	Enhanced Data Rate for GSM Evolution	增加型数据速率 GSM 演进技术
EPLMN	Equivalent PLMN	等效 PLMN
FACCH	Fast Associated Control Channel	快速随路控制信道
GPRS	General Packet Radio Service	通用无线分组业务
GSM	Global System for Mobile Communications	全球移动通讯系统
LAI	Location Area Identity	位置区识别码
NAS	Non-Access Stratum	非接入层
NCC	Network Color Code	网络色码
PLMN	Public Land Mobile Network	公共陆地移动网
PRACH	Physical Radom Access Channel	物理随机接入信道
RACH	Radom Access Channel	随机接入信道
RR	Radio Resource	无线资源管理

缩略语	英文全名	中文解释
RSSI	Received Signal Strength Indication	接收的信号强度指示
SDCCH	Stand-Alone Dedicated Control Channel	独立专用控制信道
SCH	Synchronization Channel	同步信道
SACCH	Slow Associated Control Channel	慢速随路控制信道
TD	Time Division-Synchronous CDMA	移动 3G 网（时分同步 CDMA）
USIM	Universal Subscriber Identity Module	全球用户识别卡
3GPP	3rd Generation Partnership Project	第三代合作伙伴项目

## 符号约定

在本文中可能出现下列标志，它所代表的含义如下。

符号	说明
 说明	用于突出重要/关键信息、补充信息和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害。

## 变更信息

文档版本	发布日期	修改说明
V1.0	2020-11-20	第一次正式发布。

## 关键字

GSM、EDGE、Log 分析。

# 目 录

1 GSM.....	1
1.1 找网流程.....	1
1.2 小区重选.....	9
1.3 GSM 测量.....	11
2 EDGE.....	17
2.1 网络支持 EDGE 情况.....	17
2.2 UE 支持 EDGE 情况.....	19
2.3 网络给 UE 配置 EDGE 资源.....	19
2.4 终端和网络的相互确认机制.....	21
2.5 Timer.....	22
3 常见问题.....	24
3.1 GSM 常见问题.....	24
3.2 GSM/EDGE 常见问题.....	29

Unisoc Confidential For hiar

# 图目录

图 1-1 GSM 发起找网.....	1
图 1-2 POWER SWEEP .....	3
图 1-3 DECODE BSIC .....	5
图 1-4 DECODE BCCH .....	6
图 1-5 BCCH DATA .....	7
图 1-6 驻留小区 .....	8
图 1-7 启动 GSM 小区重选.....	9
图 1-8 小区重选 .....	10
图 1-9 IDLE 下的测量 .....	11
图 1-10 CS 连接模式下的测量 .....	12
图 1-11 GPRS 连接模式下的测量报告 .....	13
图 1-12 GSM 下 TD 测量报告 .....	14
图 1-13 GSM 下 WCDMA 测量报告.....	15
图 1-14 GSM 下 LTE 测量报告.....	16
图 2-1 系统消息 13 中的 EDGE 相关信息.....	17
图 2-2 MSG_ID_GMMAS_CURR_NW_CAPABILITY_IND .....	18
图 2-3 UE 上报 EDGE 能力 .....	19
图 2-4 网络分配的 EDGE 信道.....	20
图 2-5 MAC_RLC_UPLACK_IND .....	21
图 2-6 PH_MAC_DATA_REQ.....	22
图 3-1 POWER SWEEP 结果 .....	24
图 3-2 EPLMN 配置.....	25
图 3-3 MM_RR_ACT_REQ 中的 PLMN 配置.....	26
图 3-4 MM_RR_MM_INFO_REQ 中的 FPLMN 配置 .....	26
图 3-5 系统消息中的 PLMN 不匹配 .....	27
图 3-6 MDL_ERR_IND.....	28

图 3-7 MPH_ERROR_IND .....	28
图 3-8 T3126 超时 .....	29
图 3-9 MM_RR_ACT_IND.....	30
图 3-10 MSG_ID_RR_PLM_SYS_INFO_IND .....	31

Unisoc Confidential For hiar

## 表目录

表 1-1 MM_RR_ACT_REQ 主要参数表 .....	2
表 1-2 MPH_RXPOWER_SWEEP_REQ 主要参数表 .....	3
表 1-3 MPH_BSIC_LIST_DECODE_REQ 主要参数表 .....	5
表 1-4 MPH_BSIC_DECODE_CNF 主要参数表 .....	5
表 1-5 系统消息列表 .....	7
表 2-1 Timer 描述 .....	22

Unisoc Confidential For hiar



# 1 GSM

## 1.1 找网流程

GSM 找网流程主要包括 POWER SWEEP, DECODE BSIC 和 DECODE BCCH。

在 GSM 模式下, PLM 模块向 NAS SWITCH 模块发送 MSG\_ID\_PLM\_AS\_GPRS\_PLMN\_SEL\_REQ, 然后 NAS SWITCH 模块做一些参数转换向 GSM RR 层发送 MM\_RR\_ACT\_REQ, 如图 1-1 所示, 发起找网。MM\_RR\_ACT\_REQ 包含目标 PLMN, BA 表等参数, 具体请参见表 1-1。

图1-1 GSM 发起找网

213-24	14:18:51.020	FF	0x3C07	MSG_ID_PLM_AS_GPRS_PLMN_SEL_REQ	MOD_PLM_1->MOD_NAS_SWTH_1
213-25	14:18:51.020	FF	0x581A	MSG_ID_PLM_AS_GPRS_PLMN_SEL_REQ	MOD_PLM_1->MOD_NAS_SWTH_1
213-43	14:18:51.020	FF	0x01E9	MM_RR_ACT_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
213-46	14:18:51.020	FF	0x02F6	MPH_CHANGE_MODE	MOD_GRR_1->MOD_GRR_1
213-69	14:18:51.020	FF	0x0546	RRA_WRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_WRRCA
213-71	14:18:51.020	FF	0x0124	RRA_MPH_CHANGE_MODE	MOD_GRR_1->MOD_GRR_1
213-82	14:18:51.020	FF	0x0378	RRA_MPH_CHANGE_MODE_CNF	MOD_GRR_1->MOD_GRR_1
213-133	14:18:51.020	FF	0x0079	WRRCA_WL1C_STATUS_UPDATE_CMD	MOD_WRRCA->MOD_WL1SIM
213-137	14:18:51.020	FF	0x0214	MPH_CHANGE_MODE_CNF	MOD_GRR_1->MOD_GRR_1
213-148	14:18:51.020	FF	0x03B9	WRRCA_MM_PLMN_CAMPING_REQ	MOD_NAS_SWTH_1->MOD_WRRCA
214-1	14:18:51.020	FF	0x03B9	WRRCA_MM_PLMN_CAMPING_REQ	MOD_NAS_SWTH_1->MOD_WRRCA
214-13	14:18:51.020	FF	0x01EC	MM_RR_EPLMN_LIST_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
214-16	14:18:51.020	FF	0x01E4	MM_RR_ACT_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
214-35	14:18:51.020	FF	0x24A4	MSG_ID_MM_RR_GERAN_CAP_IND	MOD_GRR_1->MOD_GMM_1
214-39	14:18:51.020	FF	0x02D4	MPH_ACTIVE_REQ	MOD_GRR_1->MOD_GRR_1
214-64	14:18:51.020	FF	0x0354	GRR_1_LRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_LRRCA
214-65	14:18:51.020	FF	0x013A	GRR_1_NRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_NRRCA
214-68	14:18:51.020	FF	0x0101	RRA_MPH_ACTIVE_REQ	MOD_GRR_1->MOD_GRR_1
214-73	14:18:51.020	FF	0x034F	MSG_ID_LRRCA_LRRCA_STATUS_UPDATE_IND	MOD_LRRCA->MOD_LASM_1
214-82	14:18:51.020	FF	0x02D6	MPH_RXPOWER_SWEEP_REQ	MOD_GRR_1->MOD_GRR_1

[LOCAL] MM_RR_ACT_REQ_MSG	
ref_count	= 0x1
rr_act_type	= RR_ACT_NORMAL
sel_param	
plmn	
mcc	= 0x1cc
mnc	= 0x1
mnc_digit_num	= 0x2
select_any_plmn	= 0x0
ba_undecoded	
bis_ba_undecoded	
arfcn_list_first	= 0x1
arfcn_list	
ignore_forbid_plmn_list	= 0x0
ms_band	= GSM850_EGSM_DCS_PCS_QUALBAND
gprs_requested	= 0x1
manual_select_plmn	= 0x0
sel_hplmn	= 0x1
band_filter	
band_filter_on	= 0x0
start_arfcn	= 0x3e8
end_arfcn	= 0x3fb
emergency_select_flag	= 0x0
ms_mode	= 0x0
is_no_sim	= 0x0
is_only_search_ba	= 0x0

表1-1 MM\_RR\_ACT\_REQ 主要参数表

参数	含义
rr_act_type	<ul style="list-style-type: none"> <li>0: 正常找网。</li> <li>1: 紧急呼叫。</li> <li>2: 无服务（当前模式在 TD 时，用来更新参数）。</li> </ul>
plmn	目标 PLMN。
select_any_plmn	是否任意选网。
ba_undecoded, bis_ba_undecoded	BA 表。
ignore_forbid_plmn_list	是否忽略 FPLMN 列表。
ms_band	NV 中手机支持的 BAND(一般支持 4 频)。
gprs_requested	是否需要 GPRS 业务。
band_filter	找网中过滤掉的频点。

## 说明

BA 表即邻区频点列表，该参数来自与最后驻留的小区的广播消息，连接模式下的测量配置消息，关机后会存储在 SIM/USIM 中，该表用来提高 POWER SWEEP 命中率，在找网过程中优先使用 BA 表中的频点。

## POWER SWEEP

GSM RR 模块收到 MM\_RR\_ACT\_REQ 之后，发起 POWER SWEEP。

GSM RR 通过命令 MPH\_RXPOWER\_SWEEP\_REQ 驱动物理层进行扫频操作，如图 1-2 所示，物理层扫频结束后通过 MPH\_RXPOWER\_SWEEP\_CNF 向 GSM RR 报告扫到的频点和功率，

MPH\_RXPOWER\_SWEEP\_REQ 参数详情请参见表 1-2。

图1-2 POWER SWEEP

15846-1	10:18:25.312	--	0x06AF	MSG_ID_CL1_CRRA_UPDATE_INFO_CNF	MOD_C2K->MOD_CRRA
15918-1	10:18:25.312	--	0x02D4	MPH_RXPOWER_SWEEP_REQ	MOD_GRR_1->MOD_GRR1
15958-1	10:18:25.312	--	0x0103	RRA_MPH_RXPOWER_SWEEP_REQ	MOD_GRR1->MOD_GL1SIM
15966-1	10:18:25.312	--	0x0349	GRR1_LRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_LRRCA
15972-1	10:18:25.312	--	0x041A	POWER_SWEEP	MOD_GRR_1->MOD_GRR_1
16019-1	10:18:25.312	--	0x0D1E	MSG_ID_MNM_PHONE_REGN_STAT_IND	MOD_MNM_1->MOD_MN_AL_
16020-1	10:18:25.312	--	0x0D34	MSG_ID_MNM_PHONE_ACTIVATE_PROTOCOL_STACK_CNF	MOD_MNM_1->MOD_MN_AL_
16049-1	10:18:25.312	--	0x0001	MSG_ID_CSM_INPUT_EVENT	MOD_MN_AL_1->MOD_CSM_
16052-1	10:18:25.312	--	0xA128	APP_MN_SIM_POWER_OFF_CNF	P_MN->P_ATC
16053-1	10:18:25.312	--	0xA128	APP_MN_PS_POWER_ON_CNF	P_ATC->P_ATC
16072-1	10:18:25.312	--	0x1817	ATC_PSIT_ATCMD_RESULT_CODE	P_ATC->P_ATC
16092-1	10:18:25.312	--	0x000E	MSG_ID_ISIP_SAPP_SERVICE_MSG	MOD_ISI_PRO_1->MOD_SAI
16100-1	10:18:25.312	--	0x000E	MSG_ID_ISIP_SAPP_SERVICE_MSG	MOD_ISI_PRO_1->MOD_SAI
16134-1	10:18:25.328	--	0x5C57	MSG_ID_RRC_SIM_READ_COMP_IND	MOD_SIM_1->MOD_RRC_1
16139-1	10:18:25.328	--	0x5C4B	MSG_ID_DM_UTRAN_CLASSMARK_REQ	MOD_RRC_1->MOD_RRC_1
16143-1	10:18:25.328	--	0x24A2	MSG_ID_GMMAS_UTRAN_CAP_IND	MOD_RRC_1->MOD_GMM_1
16144-1	10:18:25.328	--	0x4C7B	MSG_ID_DM_UTRAN_CLASSMARK_IND	MOD_RRC_1->MOD_RRC_1
16195-1	10:18:25.359	--	0x5C57	MSG_ID_RRC_SIM_READ_COMP_IND	MOD_SIM_1->MOD_RRC_1
16200-1	10:18:25.359	--	0x5C4B	MSG_ID_DM_UTRAN_CLASSMARK_REQ	MOD_RRC_1->MOD_RRC_1
16204-1	10:18:25.359	--	0x24A2	MSG_ID_GMMAS_UTRAN_CAP_IND	MOD_RRC_1->MOD_GMM_1
16205-1	10:18:25.359	--	0x4C7B	MSG_ID_DM_UTRAN_CLASSMARK_IND	MOD_RRC_1->MOD_RRC_1
16440-1	10:18:27.372	--	0x0202	MPH_RXPOWER_SWEEP_CNF	MOD_GL1SIM->MOD_GRR1
16474-1	10:18:27.372	--	0x0349	GRR1_LRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_LRRCA
16481-1	10:18:27.372	--	0x0202	MPH_RXPOWER_SWEEP_CNF	MOD_GRR1->MOD_GRR_1
16503-1	10:18:27.372	--	0x02D9	MPH_BSIC_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRR1
16551-1	10:18:27.372	--	0x0108	RRA_MPH_BSIC_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
16559-1	10:18:27.372	--	0x041A	WAIT BSIC BCCH DECODE	MOD_GRR_1->MOD_GRR_1

[[LOCAL] MPH\_RXPOWER\_SWEEP\_REQ\_MSG

- ref\_count = 0x1
- band = GSM850\_EGSM\_DCS\_PCS\_QUALBAND
- ph\_ba\_list
  - num = 0x0
  - arfcn\_list\_arr
  - ph\_ba\_valid = 0x0
- ph\_band\_list
  - ba\_sweep\_type = BA\_SWEEP\_DEFAULT
  - prefer\_bsic\_decode = 0x1

表1-2 MPH\_RXPOWER\_SWEEP\_REQ 主要参数表

参数	含义
band	扫频的 BAND 0: EGSM900 0 1: DCS1800 2: EGSM_DCS_DUALBAND

参数	含义
	3: PCS1900 4: GSM850 5: EGSM_PCS_DUALBAND 6: GSM850_DCS_DUALBAND 7: GSM850_PCS_DUALBAND 8: GSM850_EGSM_DUALBAND 9: GSM850_EGSM_PCS_TRIBAND 10: GSM850_EGSM_DCS_TRIBAND 11: EGSM_DCS_PCS_TRIBAND 12: GSM850_EGSM_DCS_PCS_QUALBAND 13: DCS_PCS_DUALBAND 14: GSM850_DCS_PCS_TRIBAND
ph_ba_list	是否包含 BA 表。
ph_ba_valid	<ul style="list-style-type: none"> <li>ph_ba_valid=1, 只扫 BA 表中的频点。</li> <li>ph_ba_valid≠1, 按照 BAND 来扫频。</li> </ul>

## DECODE BSIC

DECODE BSIC 的主要目的是找到 GSM 载波的 SCH 位置，解出 NCC 和 BCC。通常按照 POWER SWEEP 结果从强到弱依次进行 BSIC 解码，直到找到可以驻留的小区。

RR 通过 MPH\_BSIC\_LIST\_DECODE\_REQ 命令物理层进行 SCH 同步和解码，物理层通过 MPH\_BSIC\_DECODE\_CNF 上报同步和解码的结果，如图 1-3 所示。

图1-3 DECODE BSIC

16440-1	10:18:27.372	--	0x0202	MPH_RXPOWER_SWEEP_CNF	MOD_GL1SIM->MOD_GRRR
16474-1	10:18:27.372	--	0x0349	GRRR_LRRCA_STATE_NOTIFY	MOD_GRRR_1->MOD_LRRCA
16481-1	10:18:27.372	--	0x0202	MPH_RXPOWER_SWEEP_CNF	MOD_GRRR->MOD_GRRR_1
16503-1	10:18:27.372	--	0x02D9	MPH_BSIC_LIST_DECODE_REQ	MOD_GRRR_1->MOD_GRRR
16551-1	10:18:27.372	--	0x0108	RRA_MPH_BSIC_LIST_DECODE_REQ	MOD_GRRR->MOD_GL1SIM
16559-1	10:18:27.372	--	0x041A	WAIT_BSIC_BCCH_DECODE	MOD_GRRR_1->MOD_GRRR_1
16579-1	10:18:27.871	--	0x0205	MPH_BSIC_DECODE_CNF	MOD_GL1SIM->MOD_GRRR
16584-1	10:18:27.871	--	0x0205	MPH_BSIC_DECODE_CNF	MOD_GL1SIM->MOD_GRRR
16589-1	10:18:27.871	--	0x0205	MPH_BSIC_DECODE_CNF	MOD_GRRR->MOD_GRRR_1
16596-1	10:18:27.871	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRRR_1->MOD_GRRR
16646-1	10:18:27.871	--	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRRR->MOD_GL1SIM
16658-1	10:18:27.871	--	0x041A	WAIT_BSIC_BCCH_DECODE	MOD_GRRR_1->MOD_GRRR_1
16659-1	10:18:27.871	--	0x0205	MPH_BSIC_DECODE_CNF	MOD_GRRR->MOD_GRRR_1
16666-1	10:18:27.871	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRRR_1->MOD_GRRR
16716-1	10:18:27.871	--	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRRR->MOD_GL1SIM
16728-1	10:18:27.871	--	0x041A	WAIT_BSIC_BCCH_DECODE	MOD_GRRR_1->MOD_GRRR_1
16748-1	10:18:28.074	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRRR
16753-1	10:18:28.074	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRRR
16758-1	10:18:28.074	--	0x0005	MPH_BCCH_INFO_IND	MOD_GRRR->MOD_GRRR_1
16789-1	10:18:28.089	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRRR_1->MOD_GRRR
16840-1	10:18:28.089	--	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRRR->MOD_GL1SIM
16883-1	10:18:28.089	--	0x0005	MPH_BCCH_INFO_IND	MOD_GRRR->MOD_GRRR_1
16911-1	10:18:28.089	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRRR_1->MOD_GRRR
16962-1	10:18:28.089	--	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRRR->MOD_GL1SIM
17024-1	10:18:28.292	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRRR
17029-1	10:18:28.292	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRRR
17034-1	10:18:28.292	--	0x0005	MPH_BCCH_INFO_IND	MOD_GRRR->MOD_GRRR_1

[LOCAL] MPH_BSIC_LIST_DECODE_REQ_MSG	
ref_count	= 0x1
bsic_decode_num	= 0x2
bsic_list	
[0]	
arfcn	= 0x14
band	= EGSM900
bsic_priority	= 0xb4
[1]	
[2]	

表1-3 MPH\_BSIC\_LIST\_DECODE\_REQ 主要参数表

参数	含义
arfcn	进行同步和解码的频点。

表1-4 MPH\_BSIC\_DECODE\_CNF 主要参数表

参数	含义
arfcn	进行同步和解码的频点。
bsic	共 6bit，NCC 和 BCC 各 3bit。

如果同步和解码失败，物理层会向 RR 上报 MPH\_BSIC\_DECODE\_FAIL，RR 收到消息以后，继续对下一个频点进行 DECODE。如果 POWER SWEEP 结果中的所有 BA 频点都进行了 DECODE，未找到合适小区，则进行全频段的 POWER SWEEP 流程，结束后向物理层发送 MM\_RR\_ACT\_IND（若参数 RR\_ACT\_TYPE=2，表示 NO SERVICE）。

BSIC 解码成功以后，需要接收系统消息。在 GSM 网络下，系统消息 1、2、3、4 必须接收，如果要进行 GPRS 业务还需要接收系统消息 13。

## DECODE BCCH

RR 向物理层发 MPH\_BCCH\_LIST\_DECODE\_REQ 进行 BCCH 的接收和解码，如图 1-4 所示。物理层收到 BCCH 数据后通过 MPH\_BCCH\_INFO\_IND 上报 RR，如图 1-5 所示。一般情况下，可根据 MPH\_BCCH\_INFO\_IND 中的数据快速判断找网是否正常，在找网过程中需要接收的系统消息请参见表 1-5。

图1-4 DECODE BCCH

16646-1	10:18:27.871	--	0x0106	RRA MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
16658-1	10:18:27.871	--	0x041A	WAIT_BSIC_BCCH_DECODE	MOD_GRR1->MOD_GRR1
16659-1	10:18:27.871	--	0x0205	MPH_BSIC_DECODE_CNF	MOD_GRR1->MOD_GRR1
16666-1	10:18:27.871	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GRR1
16716-1	10:18:27.871	--	0x0106	RRA MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
16728-1	10:18:27.871	--	0x041A	WAIT_BSIC_BCCH_DECODE	MOD_GRR1->MOD_GRR1
16748-1	10:18:28.074	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
16753-1	10:18:28.074	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
16758-1	10:18:28.074	--	0x0005	MPH_BCCH_INFO_IND	MOD_GRR1->MOD_GRR1
16789-1	10:18:28.089	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GRR1
16840-1	10:18:28.089	--	0x0106	RRA MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
16883-1	10:18:28.089	--	0x0005	MPH_BCCH_INFO_IND	MOD_GRR1->MOD_GRR1
16911-1	10:18:28.089	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GRR1
16962-1	10:18:28.089	--	0x0106	RRA MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
17024-1	10:18:28.292	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
17029-1	10:18:28.292	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
17034-1	10:18:28.292	--	0x0005	MPH_BCCH_INFO_IND	MOD_GRR1->MOD_GRR1
17064-1	10:18:28.292	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GRR1
17115-1	10:18:28.292	--	0x0106	RRA MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
17159-1	10:18:28.292	--	0x0005	MPH_BCCH_INFO_IND	MOD_GRR1->MOD_GRR1
17187-1	10:18:28.292	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GRR1
17238-1	10:18:28.292	--	0x0106	RRA MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
17317-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
17322-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
17327-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
17332-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1

```

[LOCAL] MPH_BCCH_LIST_DECODE_REQ_MSG
--ref_count = 0x1
--read_mode = CON_BCCH
--bcch_decode_num = 0x1
--bcch_list
--[0]
--arfcn = 0xa
--tc_mask = 0xcc
--band = EGSM900
--bcch_first = 0x0
--bcch_priority = 0xb3
--force_decode = 0x0
--[1]

```

图1-5 BCCH DATA

17159-1	10:18:28.292	--	0x0005	MPH_BCCH_INFO_IND	MOD_GRR1->MOD_GRR_1
17187-1	10:18:28.292	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRR1
17238-1	10:18:28.292	--	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
17317-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
17322-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
17327-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
17332-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
17337-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
17342-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR1
17347-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GRR1->MOD_GRR_1
17372-1	10:18:28.510	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRR1
17423-1	10:18:28.510	--	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
17467-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GRR1->MOD_GRR_1
17492-1	10:18:28.510	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRR1
17543-1	10:18:28.510	--	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
17569-1	10:18:28.510	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRR1
17620-1	10:18:28.510	--	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
17631-1	10:18:28.510	--	0x0005	MPH_BCCH_INFO_IND	MOD_GRR1->MOD_GRR_1
17659-1	10:18:28.510	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRR1
17710-1	10:18:28.510	--	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
17749-1	10:18:28.510	--	0x02D5	MPH_BCCH_CAMP_REQ	MOD_GRR_1->MOD_GRR1
17791-1	10:18:28.510	--	0x0104	RRA_MPH_BCCH_CAMP_REQ	MOD_GRR1->MOD_GL1SIM
17799-1	10:18:28.510	--	0x0203	MPH_BCCH_CAMP_CNF	MOD_GL1SIM->MOD_GRR1
17850-1	10:18:28.510	--	0x0349	GRR1_LRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_LRRCA
17851-1	10:18:28.510	--	0x0683	GRR1_CRRA_STATE_NOTIFY	MOD_GRR1->MOD_CRRA

```

[LOCAL] MPH_BCCH_INFO_IND_MSG
--ref_count = 0x1
--chan_type = BCCH
--ph_arfcn = 0x14
--ph_block
--[0] = 0x55
--[1] = 0x6
--[2] = 0x19
--[3] = 0x0
--[4] = 0x0
--[5] = 0x0
  
```

表1-5 系统消息列表

消息名称	特征数值	描述
系统消息 1	0x19	小区信息，RACH 信息。
系统消息 2	0x1a	小区信息，RACH 信息，邻小区信息。
系统消息 3	0x1b	小区选择信息，LAI 等。
系统消息 4	0x1c	小区选择信息，RACH 信息，LAI 等。
系统消息 13	0x00	GPRS 小区信息。
系统消息 2 QUATER	0x07	邻小区信息，包括 3G 和 4G。

RR 先配置接收系统消息 1，2，3，4，如果需要进行 GPRS 业务，则配置接收系统消息 13。RR 成功接收系统消息 13 后驻留小区，上报 NAS，等待空闲时间再接收系统消息 2 QUATER。

系统消息接收完成后，RR 发送 MPH\_BCCH\_CAMP\_REQ 驻留小区，如图 1-6 所示。在 LOG 分析过程中，可以通过搜索 MPH\_BCCH\_CAMP\_REQ 快速分析小区变化过程。

图1-6 驻留小区

17710-1	10:18:28.510	--	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
17749-1	10:18:28.510	--	0x02D5	MPH_BCCH_CAMP_REQ	MOD_GRR1->MOD_GRR1
17791-1	10:18:28.510	--	0x0104	RRA_MPH_BCCH_CAMP_REQ	MOD_GRR1->MOD_GL1SIM
17799-1	10:18:28.510	--	0x0203	MPH_BCCH_CAMP_CNF	MOD_GL1SIM->MOD_GRR1
17850-1	10:18:28.510	--	0x0349	GRR1_LRRCA_STATE_NOTIFY	MOD_GRR1->MOD_LRRCA
17851-1	10:18:28.510	--	0x0683	GRR1_CRRA_STATE_NOTIFY	MOD_GRR1->MOD_CRRA
17853-1	10:18:28.510	--	0x0683	GRR1_CRRA_STATE_NOTIFY	MOD_GRR1->MOD_CRRA
17879-1	10:18:28.510	--	0x60BE	MSG_ID_RRA_RRCA_STATE_NOTIFY	MOD_GRR1->MOD_RRC_ADAF
18036-1	10:18:28.510	--	0x041A	WAIT_BCCH_CAMP	MOD_GRR1->MOD_GRR1

```

[LOCAL] MPH_BCCH_CAMP_REQ_MSG
--ref_count = 0x1
--bcch_camp_param
--arfcn = 0x14
--si13_ind = SI13_NORM
--combined_ccch = 0x0
--ccch_group = 0x0
--paging_group = 0x18
--bs_agblks_res = 0x0
--bs_pamfrms = 0x5
--txpwr = 0x0
--paging_mode = PAGING_NORMAL
--ba_list
--pwr = 0x0
--dtx_allowed = NEITHER_USE_DTX
--radio_link_timeout = 0x8
--cbch_present = 0x0
--cbch_desc
--cbch_ma_list
--gprs_requested = 0x1
--global_pwr_param
--access_burst_type = AB_11
--short_vic_dsc_used = 0x0
--bep_period = 0x0
--pch_tbf_nv_allowed = 0x0
--pch_tbf_net_allowed = 0x0
--is_nv_pag_coord = 0x0
--card_mask = 0x0
--is_master = 0x0
--rr_service_state = GSM_GPRS_SERVICE
--ms_band = GSM850_EGSM_DCS_TRIBAND

```



## 1.2 小区重选

终端驻留在某个 GSM 小区时，会周期性对服务小区和邻小区进行测量，每次收到 MPH\_IDLE\_SCELL\_MEAS\_IND 都会判断是否需要开启小区重选的 Timer (RR\_RESEL\_EXP\_IND)。

RR\_RESEL\_EXP\_IND 超时一般会有以下 3 种操作。

- 小区不变，停止该 Timer，服务小区好，不需要重选。
- 小区不变，继续该 Timer，需要继续进行重选评估，如果连续 5 次都满足重选条件，重选小区。
- 小区重选，已经满足评估时间和重选条件。

图1-7 启动 GSM 小区重选

312-73	20:35:16.952	FF	0x0106	RRA_MPH_BOCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
314-7	20:35:17.764	FF	0x025A	RR_RESEL_EXP_IND	MOD_TIMER->MOD_GRR_1
314-17	20:35:17.764	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR_1->MOD_GRR1
318-27	20:35:18.762	FF	0x0361	RRA_MPH_IDLE_NCELL_MEAS_IND	MOD_GL1SIM->MOD_GRR1
318-31	20:35:18.762	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRR1
318-37	20:35:18.762	FF	0x0089	MPH_IDLE_NCELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
318-52	20:35:18.762	FF	0x008A	MPH_IDLE_SCELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
318-102	20:35:18.762	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GRR1->MOD_GRR_1
321-7	20:35:19.760	FF	0x025A	RR_RESEL_EXP_IND	MOD_TIMER->MOD_GRR_1
321-17	20:35:19.760	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR_1->MOD_GRR1
324-3	20:35:20.759	FF	0x025B	RR_UPDATE_EXP_IND	MOD_TIMER->MOD_GRR_1
328-33	20:35:21.757	FF	0x0361	RRA_MPH_IDLE_NCELL_MEAS_IND	MOD_GL1SIM->MOD_GRR1
328-37	20:35:21.757	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRR1
328-43	20:35:21.757	FF	0x025A	RR_RESEL_EXP_IND	MOD_TIMER->MOD_GRR_1
328-53	20:35:21.757	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR_1->MOD_GRR1
328-58	20:35:21.757	FF	0x0009	MPH_IDLE_NCELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
328-92	20:35:21.757	FF	0x000A	MPH_IDLE_SCELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
328-141	20:35:21.757	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GRR1->MOD_GRR_1
334-7	20:35:23.754	FF	0x025A	RR_RESEL_EXP_IND	MOD_TIMER->MOD_GRR_1
334-17	20:35:23.754	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR_1->MOD_GRR1
339-27	20:35:24.753	FF	0x0361	RRA_MPH_IDLE_NCELL_MEAS_IND	MOD_GL1SIM->MOD_GRR1
339-31	20:35:24.753	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRR1
339-37	20:35:24.753	FF	0x0009	MPH_IDLE_NCELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
339-71	20:35:24.753	FF	0x000A	MPH_IDLE_SCELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
339-121	20:35:24.753	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GRR1->MOD_GRR_1
342-10	20:35:25.455	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRR1
342-16	20:35:25.455	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GRR1->MOD_GRR_1
343-1	20:35:25.751	FF	0x025A	RR_RESEL_EXP_IND	MOD_TIMER->MOD_GRR_1
343-11	20:35:25.751	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR_1->MOD_GRR1
343-19	20:35:25.751	FF	0x02B9	GRR_MM_SUSPEND_GMM_IND	MOD_GRR_1->MOD_NAS_SWTH_1
343-20	20:35:25.751	FF	0x0322	GRR_RLC_SUSPEND_REQ	MOD_GRR_1->MOD_GRR1
343-41	20:35:25.751	FF	0x018E	RRA_GRR_RLC_SUSPEND_REQ	MOD_GRR1->MOD_GRLC
343-42	20:35:25.751	FF	0x0418	RLC_SUSPEND	MOD_GRLC->MOD_GRLC
343-57	20:35:25.751	FF	0x02D9	MPH_BOCH_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRR1

Traces	
Content	
[MNSIM_SimuGetVSIMFuncSwitch]:[0]:sim_simu_driver_switch_g[0]=0	
RR: IsNC2Valid, m_nc = 0, c_nc = 0, gmm_state=4, cell_p=1, cell_pb_p=0	
rat=0 cell_arfcn=512, bsic_psc_pci=9, is_in_blackcell=0	
RR: resel: card 0, scell: a=0x14, c1=4, c2=14; max_rssi_ncell: a=0x200, c1=65, c2=53; ct=0	
RR: ProcessReselTimer, rr_service_state=3, mm_act_type=0, gmm_state=4, resel_type=5, resel_action=2	
RR TIMER: stop timer RR_T3122_EXP_IND	

如图 1-7 所示，RR 收到 MPH\_IDLE\_NCELL\_MEAS\_IND，MPH\_IDLE\_SCELL\_MEAS\_IND 对服务小区和邻小区的评估。NCELL 的 C2 比 SCELL 高，CT 表示第几秒，当 CT 累加到 5 时，表示已经对 NCELL 进行了连续 5 秒的评估，再完成一次 RR\_RESEL\_EXP\_IND 则可以换小区。

图1-8 小区重选

312-73	20:35:16.952	FF	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GL1SIM
314-7	20:35:17.764	FF	0x025A	RR_RESEL_EXP_IND	MOD_TIMER->MOD_GRR_1
314-17	20:35:17.764	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR_1->MOD_GRR1
318-27	20:35:18.762	FF	0x0361	RRA_MPH_IDLE_NCELL_MEAS_IND	MOD_GL1SIM->MOD_GRR1
318-31	20:35:18.762	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRR1
318-37	20:35:18.762	FF	0x0009	MPH_IDLE_NCELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
318-52	20:35:18.762	FF	0x000A	MPH_IDLE_SCELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
318-102	20:35:18.762	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GRR1->MOD_GRR_1
321-7	20:35:19.760	FF	0x025A	RR_RESEL_EXP_IND	MOD_TIMER->MOD_GRR_1
321-17	20:35:19.760	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR_1->MOD_GRR1
324-3	20:35:20.759	FF	0x025B	RR_UPDATE_EXP_IND	MOD_TIMER->MOD_GRR_1
328-33	20:35:21.757	FF	0x0361	RRA_MPH_IDLE_NCELL_MEAS_IND	MOD_GL1SIM->MOD_GRR1
328-37	20:35:21.757	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRR1
328-43	20:35:21.757	FF	0x025A	RR_RESEL_EXP_IND	MOD_TIMER->MOD_GRR_1
328-53	20:35:21.757	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR_1->MOD_GRR1
328-58	20:35:21.757	FF	0x0009	MPH_IDLE_NCELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
328-92	20:35:21.757	FF	0x000A	MPH_IDLE_SCELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
328-141	20:35:21.757	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GRR1->MOD_GRR_1
334-7	20:35:23.754	FF	0x025A	RR_RESEL_EXP_IND	MOD_TIMER->MOD_GRR_1
334-17	20:35:23.754	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR_1->MOD_GRR1
339-27	20:35:24.753	FF	0x0361	RRA_MPH_IDLE_NCELL_MEAS_IND	MOD_GL1SIM->MOD_GRR1
339-31	20:35:24.753	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRR1
339-37	20:35:24.753	FF	0x0009	MPH_IDLE_NCELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
339-71	20:35:24.753	FF	0x000A	MPH_IDLE_SCELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
339-121	20:35:24.753	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GRR1->MOD_GRR_1
342-10	20:35:25.455	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRR1
342-16	20:35:25.455	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GRR1->MOD_GRR_1
343-1	20:35:25.751	FF	0x025A	RR_RESEL_EXP_IND	MOD_TIMER->MOD_GRR_1
343-11	20:35:25.751	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR_1->MOD_GRR1
343-19	20:35:25.751	FF	0x02B9	GRR_MM_SUSPEND_GMM_IND	MOD_GRR_1->MOD_NAS_SWTH_1

LOCAL

sdi\_msg\_user\_data\_struct

ref\_count = 0x1

Traces

Content

[MNSIM\_SimuGetVSIMFuncSwitch]:[0]:sim\_simu\_driver\_switch\_g[0]=0  
RRC:IsNC2Valid,m\_nc=0,c\_nc=0,gmm\_state=4,cell\_p=1,cell\_pb\_p=0  
RRC:resel: card 0, scell: a=0x14,c1=4,c2=14; max\_rssi\_ncell: a=0x200,c1=65,c2=53; ct=5  
RRC:ProcessReselTimer, rr\_service\_state=3,mm\_act\_type=0,gmm\_state=4, resel\_type=5, resel\_action=0  
RR\_TIMER: start timer RR\_RESEL\_EXP\_IND, dur 2000

如图 1-8 所示，0x200 小区连续 5 次满足评估条件，进行了重选。若 5 次评估中间有不满足条件的情况，则 TRACE 中的 CT 值会变成 0，一般情况下 RR\_RESEL\_EXP\_IND 定时器也会停止。

## 1.3 GSM 测量

GSM 下的测量比较简单，通过 LOG 可以看到服务小区和 6 个最强邻区的测量结果。

在 IDLE 下，物理层通过 MPH\_IDLE\_NCELL\_MEAS\_IND 上报邻区测量结果。通过 MPH\_IDLE\_SCELL\_MEAS\_IND 上报服务小区测量结果，如图 1-9 所示。

ARM 端看到的 RSSI 都是 LEVEL，LEVEL-110 表示对应的实际 dBm 值。

图1-9 IDLE 下的测量

339-31	20:35:24.753	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRRR
339-37	20:35:24.753	FF	0x0003	MPH_IDLE_NCELL_MEAS_IND	MOD_GRRR->MOD_GRR_1
339-71	20:35:24.753	FF	0x000A	MPH_IDLE_SCELL_MEAS_IND	MOD_GRRR->MOD_GRR_1
339-121	20:35:24.753	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GRRR->MOD_GRR_1
342-10	20:35:25.455	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRRR
342-16	20:35:25.455	FF	0x000D	MPH_TD_MEAS_REPORT_IND	MOD_GRRR->MOD_GRR_1
343-1	20:35:25.751	FF	0x025A	RR_RESEL_EXP_IND	MOD_TIMER->MOD_GRR_1
343-11	20:35:25.751	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR_1->MOD_GRRR
343-19	20:35:25.751	FF	0x02B9	GRR_MM_SUSPEND_GMM_IND	MOD_GRR_1->MOD_NAS_SWTH_1
343-20	20:35:25.751	FF	0x0322	GRR_RLC_SUSPEND_REQ	MOD_GRR_1->MOD_GRRR
343-41	20:35:25.751	FF	0x018E	RRA_GRR_RLC_SUSPEND_REQ	MOD_GRRR->MOD_GRLC
343-42	20:35:25.751	FF	0x0418	RLC_SUSPEND	MOD_GRLC->MOD_GRLC
343-57	20:35:25.751	FF	0x02D9	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRRR
343-95	20:35:25.751	FF	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRRR->MOD_GL1SIM
343-108	20:35:25.751	FF	0x0418	RRC Resel	MOD_GRR_1->MOD_GRR_1
343-111	20:35:25.751	FF	0x0418	NORM_IDLE_MODE	MOD_GRR_1->MOD_GRR_1
343-113	20:35:25.751	FF	0x4407	MSG_ID_ILGMM_SUSPEND_REQ	MOD_GMM_1->MOD_NAS_SWTH_1
343-114	20:35:25.751	FF	0x3010	MSG_ID_MMMSMS_SUSPEND_REQ	MOD_GMM_1->MOD_SMS_1
343-115	20:35:25.751	FF	0x3416	MSG_ID_GMMSM_SUSPEND_REQ	MOD_GMM_1->MOD_SM_1
343-119	20:35:25.751	FF	0x01B6	GMM_LLME_SUSPEND_REQ	MOD_NAS_SWTH_1->MOD_GLLC
343-123	20:35:25.751	FF	0x20E8	MSG_ID_DSM_DSB_SUSPEND_IND	MOD_MN_AL_1->MOD_DSM
343-126	20:35:25.751	FF	0x20E8	MSG_ID_DSM_DSB_SUSPEND_IND	MOD_MN_AL_2->MOD_DSM
344-18	20:35:25.954	FF	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRRR
344-23	20:35:25.954	FF	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRRR

```

[LOCAL] MPH_IDLE_NCELL_MEAS_IND_MSG
  ref_count = 0x1
  ph_ncell_meas_num = 0x1
  ph_ncell_meas_list
    [0]
      arfcn = 0x200
      bsic = 0x9
      rxlev = 0x41
      delta_fn = 0x2
      otd = 0x0
      dsc_cur = 0x0
      rxlev_level = 0x0
    [1]
      arfcn = 0x0
      bsic = 0x0
      rxlev = 0x0
      delta_fn = 0x0
      otd = 0x0
  
```

通话过程中物理层通过 MPH\_CELL\_MEAS\_IND 上报服务小区和邻小区的测量值，如图 1-10 所示。

图1-10 CS 连接模式下的测量

279-103	21:09:28.509	FF	0x0115	RRA_MPH_RADIO_LINK_TIMEOUT_REQ	MOD_GRR1->MOD_GL1SIM
279-105	21:09:28.509	FF	0x02D2	RR_MN_SCELL_INFO_IND	MOD_GRR1->MOD_NAS_SWTH_1
279-109	21:09:28.509	FF	0x000B	MPH_CELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
279-127	21:09:28.509	FF	0x0002	DL_UNIT_DATA_REQ	MOD_GRR1->MOD_GRR1
279-133	21:09:28.509	FF	0x0156	RRA_DL_UNIT_DATA_REQ	MOD_GRR1->MOD_GL1SIM
279-177	21:09:28.509	FF	0x02CC	RR_MN_SCELL_RSSI_IND	MOD_GRR1->MOD_NAS_SWTH_1
279-178	21:09:28.509	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR1->MOD_GRR1
280-1	21:09:28.509	FF	0x000B	MPH_CELL_MEAS_IND	MOD_GRR1->MOD_GRR_1
280-19	21:09:28.509	FF	0x0002	DL_UNIT_DATA_REQ	MOD_GRR1->MOD_GRR1
280-25	21:09:28.509	FF	0x0156	RRA_DL_UNIT_DATA_REQ	MOD_GRR1->MOD_GL1SIM
280-70	21:09:28.509	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR1->MOD_GRR1
280-80	21:09:28.509	FF	0x0125	MSG_ID_AS_L4_SIGNAL_QUALITY_IND	MOD_NAS_SWTH_1->MOD_MNM_1
280-82	21:09:28.509	FF	0x0125	MSG_ID_AS_L4_SIGNAL_QUALITY_IND	MOD_NAS_SWTH_1->MOD_MNM_1
280-84	21:09:28.509	FF	0x2425	MSG_ID_GMMAS_ESTABLISH_CNF	MOD_NAS_SWTH_1->MOD_GMM_1
280-86	21:09:28.509	FF	0x0124	MSG_ID_AS_L4_SCELL_INFO_IND	MOD_NAS_SWTH_1->MOD_MN_AL_1

```

[LOCAL] MPH_CELL_MEAS_IND_MSG
  ref_count = 0x1
  ph_dtx_used = 0x0
  ph_ncell_meas_num = 0x2
  ph_ncell_meas_list
    [0]
      arfcn = 0xe
      bsic = 0x9
      rxlev = 0x14
      delta_fn = 0x2
      ctd = 0x0
      dsc_cur = 0x0
      rxlev_level = 0x0
    [1]
    [2]
    [3]
    [4]
    [5]
  ph_scell_meas
    rxlev_full = 0x41
    rxlev_sub = 0x41
    rxqual_full = 0x0
    rxqual_sub = 0x0
    txpwr = 0x5
    rlt_cur = 0x34
  is_meas_valid = 0x1
  
```

GPRS/EDGE 下物理层通过 MPH\_NC\_MEAS\_REPORT\_IND 上报服务小区和邻小区测量报告，如图 1-11 所示。

图1-11 GPRS 连接模式下的测量报告

234-20	20:23:01.606	FF	0x01A2	MAC_RLC_UPLACK_IND	MOD_GMAC->MOD_GRLC
234-30	20:23:01.622	FF	0x01B1	MSG_ID_L1SIM_BSSIM_2G_DATA_REQ	MOD_GL1SIM->MOD_GL1SIM
234-34	20:23:01.622	FF	0x0007	PH_MAC_DATA_IND	MOD_GL1SIM->MOD_GL1SIM
234-42	20:23:01.622	FF	0x0178	RLC_MAC_DATA_REQ	MOD_GRLC->MOD_GMAC
234-43	20:23:01.622	FF	0x01B2	MSG_ID_L1SIM_BSSIM_2G_DATA_IND	MOD_GL1SIM->MOD_GL1SIM
237-19	20:23:02.402	FF	0x000C	MPH_NC_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRR1
237-23	20:23:02.402	FF	0x000C	MPH_NC_MEAS_REPORT_IND	MOD_GRR1->MOD_GRR1
237-87	20:23:02.402	FF	0x025A	RR_RESEL_EXP_IND	MOD_TIMER->MOD_GRR1
237-91	20:23:02.402	FF	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR1->MOD_GRR1
238-10	20:23:02.667	FF	0x01B1	MSG_ID_L1SIM_BSSIM_2G_DATA_REQ	MOD_GL1SIM->MOD_GL1SIM
238-14	20:23:02.667	FF	0x0007	PH_MAC_DATA_IND	MOD_GL1SIM->MOD_GL1SIM
238-18	20:23:02.667	FF	0x0007	PH_MAC_DATA_IND	MOD_GL1SIM->MOD_GMAC
238-19	20:23:02.667	FF	0x01A2	MAC_RLC_UPLACK_IND	MOD_GMAC->MOD_GRLC
238-21	20:23:02.667	FF	0x01CD	RLC_LL_PDU_SEND_CNF	MOD_GRLC->MOD_GLLC

[LOCAL] MPH\_NC\_MEAS\_REPORT\_IND\_MSG

```

ref_count = 0x1
ph_idle_scell_meas
  arfcn = 0x14
  bsic = 0x9
  rxlev = 0x41
  delta_fn = 0x0
  otd = 0x0
  dsc_cur = 0x0
  rxlev_level = 0x0
ph_ncell_meas_num = 0x1
ph_ncell_meas_list
  [0]
    arfcn = 0x200
    bsic = 0x9
    rxlev = 0x0
    delta_fn = 0x2
    otd = 0x0
    dsc_cur = 0x0
    rxlev_level = 0x0
  [1]
    arfcn = 0xff
    bsic = 0x0
    rxlev = 0x0
    delta_fn = 0x0

```

物理层通过 MPH\_TD\_MEAS\_REPORT\_IND 上报 GSM 下 TD 系统的测量报告，如图 1-12 所示。

图1-12 GSM 下 TD 测量报告

300-163	21:09:29.616	FF	0x0126	RRA_MPH_UPDATE_TD_MEAS_REQ	MOD_GRR1->MOD_GL1SIM
301-95	21:09:29.616	FF	0x0000	MPH_TD_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRR1
301-112	21:09:29.616	FF	0x02D7	MPH_BCCH_CAMP_REQ	MOD_GRR1->MOD_GRR1
301-141	21:09:29.616	FF	0x0104	RRA_MPH_BCCH_CAMP_REQ	MOD_GRR1->MOD_GL1SIM
301-149	21:09:29.616	FF	0x0205	MPH_BCCH_CAMP_CNF	MOD_GL1SIM->MOD_GRR1
301-169	21:09:29.616	FF	0x0354	GRR1_LRRCA_STATE_NOTIFY	MOD_GRR1->MOD_LRRCA
301-170	21:09:29.616	FF	0x0354	GRR1_LRRCA_STATE_NOTIFY	MOD_GRR1->MOD_LRRCA
301-183	21:09:29.616	FF	0x013A	GRR1_NRRCA_STATE_NOTIFY	MOD_GRR1->MOD_NRRCA
301-184	21:09:29.616	FF	0x013A	GRR1_NRRCA_STATE_NOTIFY	MOD_GRR1->MOD_NRRCA
301-185	21:09:29.616	FF	0x60D3	MSG_ID_RRA_RRCA_STATE_NOTIFY	MOD_GRR1->MOD_RRC_ADAPTER
301-196	21:09:29.616	FF	0x034F	MSG_ID_LRRCA_LRRCA_STATUS_UPDATE_IND	MOD_LRRCA->MOD_LASM_1
302-21	21:09:29.616	FF	0x0418	WAIT_BCCH_CAMP_IN_REL	MOD_GRR1->MOD_GRR1
302-22	21:09:29.616	FF	0x0005	MPH_BCCH_INFO_IND	MOD_GRR1->MOD_GRR1

```

[LOCAL] MPH_TD_MEAS_REPORT_IND_MSG
  ref_count = 0x1
  td_meas_report
    td_sync_ind = 0x1
    td_meas_type = TD_INFO_WITH_ARFCN_BUT_MIDAMBLE
    cell_num = 0x0
    td_meas_result
      [0]
        arfcn = 0x0
        cell_param_id = 0x0
        rscp = 0x0
      [1]
        arfcn = 0x0
        cell_param_id = 0x0
        rscp = 0x0
      [2]
        arfcn = 0x0

```

Unisoc Confidential For hiar

图1-13 GSM 下 WCDMA 测量报告

325-92	10:56:10.207	FF	0x012E	RRA_MPH_GSM_MEAS_WCDMA_CONFIG_REQ	MOD_GRRR->MOD_GL1SIM
325-97	10:56:10.207	FF	0x037A	RRA_MPH_FDD_MEAS_REPORT_IND	MOD_GL1SIM->MOD_GRRR
325-103	10:56:10.207	FF	0x02C3	MM_RR_WFREQ_IND	MOD_GRR_1->MOD_NAS_SWTH_1
325-106	10:56:10.207	FF	0x000E	MPH_FDD_MEAS_REPORT_IND	MOD_GRRR->MOD_GRR_1
325-137	10:56:10.207	FF	0x2466	MSG_ID_RR_PLM_SYS_INFO_IND	MOD_NAS_SWTH_1->MOD_PLM_1
325-138	10:56:10.207	FF	0x246D	MSG_ID_RR_PLM_STATE_CHANGE_IND	MOD_NAS_SWTH_1->MOD_PLM_1
325-139	10:56:10.207	FF	0x2467	MSG_ID_GMMAS_CURR_NW_CAPABILITY_IND	MOD_NAS_SWTH_1->MOD_GMM_1
325-143	10:56:10.207	FF	0x0125	MSG_ID_AS_L4_SIGNAL_QUALITY_IND	MOD_NAS_SWTH_1->MOD_MNM_1
325-145	10:56:10.207	FF	0x24A3	MSG_ID_PLM_WCDMA_NC_IND	MOD_NAS_SWTH_1->MOD_PLM_1

```

[LOCAL] MPH_FDD_MEAS_REPORT_IND_MSG
  ref_count = 0x1
  fdd_meas_report
    fdd_meas_type = FDD_INFO_WITH_ARFCN_AND_CELL
    cell_num = 0x1
    fdd_cell_meas_result
      [0]
        arfcn = 0x29cc
        cell_param_id = 0x64
        rscp = 0x14
        ecno = 0x23
      [1]
        arfcn = 0x0
        cell_param_id = 0x0
        rscp = 0x0
        ecno = 0x0
      [2]
        arfcn = 0x0
        cell_param_id = 0x0
        rscp = 0x0
        ecno = 0x0
      [3]
        arfcn = 0x0
        cell_param_id = 0x0
        rscp = 0x0
        ecno = 0x0
      [4]

```

物理层通过 MSG\_ID\_TM\_GSM\_MEAS\_LTE\_RESULT\_IND 上报 GSM 下 LTE 系统的测量报告，如图 1-14 所示。

图1-14 GSM 下 LTE 测量报告

418-83	10:44:23.955	FF	0x0127	MSG_ID_TM_LTE_MEAS_RESULT_TO_GSM_IND	MOD_LCONTROL_1->MOD_LLAYER1
418-89	10:44:23.955	FF	0x026B	RR_EUTRAN_CELL_RESEL_EXP_IND	MOD_TIMER->MOD_GRR_1
419-1	10:44:23.955	FF	0x000F	MSG_ID_TM_GSM_MEAS_LTE_RESULT_IND	MOD_LLAYER1_ADX->MOD_GRR_1
419-23	10:44:24.048	FF	0x01B1	MSG_ID_L1SIM_BSSIM_2G_DATA_REQ	MOD_GL1SIM->MOD_GL1SIM
419-27	10:44:24.048	FF	0x0007	PH_MAC_DATA_IND	MOD_GL1SIM->MOD_GL1SIM
419-31	10:44:24.048	FF	0x0007	PH_MAC_DATA_IND	MOD_GL1SIM->MOD_GMAC
419-32	10:44:24.048	FF	0x01A2	MAC_RLC_UPLACK_IND	MOD_GMAC->MOD_GRLC
419-42	10:44:24.048	FF	0x01B1	MSG_ID_L1SIM_BSSIM_2G_DATA_REQ	MOD_GL1SIM->MOD_GL1SIM
419-46	10:44:24.048	FF	0x0007	PH_MAC_DATA_IND	MOD_GL1SIM->MOD_GL1SIM
419-54	10:44:24.048	FF	0x0178	RLC_MAC_DATA_REQ	MOD_GRLC->MOD_GMAC
419-55	10:44:24.048	FF	0x01B2	MSG_ID_L1SIM_BSSIM_2G_DATA_IND	MOD_GL1SIM->MOD_GL1SIM
421-2	10:44:24.376	FF	0x025B	RR_UPDATE_EXP_IND	MOD_TIMER->MOD_GRR_1
424-20	10:44:25.109	FF	0x01B1	MSG_ID_L1SIM_BSSIM_2G_DATA_REQ	MOD_GL1SIM->MOD_GL1SIM
424-24	10:44:25.109	FF	0x0007	PH_MAC_DATA_IND	MOD_GL1SIM->MOD_GL1SIM

[LOCAL] MPH\_LTE\_MEAS\_REPORT\_IND\_MSG

```

ref_count = 0x1
card_id = 0x0
msg
  usMeasReqId = 0x0
  freq_num = 0x1
  lte_meas_freq_result
    [0]
      earfcn = 0x4e2
      cell_num = 0x1
      lte_meas_cell_result
        [0]
          pcid = 0x0
          rsrp = 0xf880
          rsrq = 0xff10
        [1]
          pcid = 0x0
          rsrp = 0x0
          rsrq = 0x0
        [2]
          pcid = 0x0
          rsrp = 0x0
          rsrq = 0x0
        [3]
          pcid = 0x0
          rsrp = 0x0
          rsrq = 0x0

```



# 2

## EDGE

### 2.1 网络支持 EDGE 情况

网络在系统消息 13 中会广播是否支持 EDGE。

图2-1 系统消息 13 中的 EDGE 相关信息

161549...	14:36:59.308	0x0005	MPH_BCCH_INFO_IND	MOD_GRRRA->MOD_GRR_1
161549...	14:36:59.326	0x0005	MPH_BCCH_INFO_IND	MOD_GLAYER1->MOD_GRRRA
16154980-1	14:36:59.326	0x0005	MPH_BCCH_INFO_IND	MOD_GRRRA->MOD_GRR_1
161550...	14:36:59.354	0x0006	MPH_DATA_IND	MOD_GLAYER1->MOD_GRRRA
161550...	14:36:59.354	0x0006	MPH_DATA_IND	MOD_GRRRA->MOD_GRR_1
161550...	14:36:59.372	0x0006	MPH_DATA_IND	MOD_GLAYER1->MOD_GRRRA
161550...	14:36:59.372	0x0006	MPH_DATA_IND	MOD_GRRRA->MOD_GRR_1
161550...	14:36:59.400	0x0006	MPH_DATA_IND	MOD_GLAYER1->MOD_GRRRA
161550...	14:36:59.400	0x0006	MPH_DATA_IND	MOD_GRRRA->MOD_GRR_1
161550...	14:36:59.418	0x0006	MPH_DATA_IND	MOD_GLAYER1->MOD_GRRRA
161550...	14:36:59.418	0x0006	MPH_DATA_IND	MOD_GRRRA->MOD_GRR_1

[LOCAL] MPH\_BCCH\_INFO\_IND\_MSG

ref\_count = 0x1

chan\_type = BCCH

ph\_arfcn = 0x7a

ph\_block

[0] = 0x1

[1] = 0x6

[2] = 0x0

[3] = 0xd0

[4] = 0x0

[5] = 0x58

[6] = 0x47

[7] = 0x0

Time	RAT	Content
6:59.326	GSM	Time:2234057 RRC: Useless not use tc5:1, 1, 1
6:59.326	GSM	Time:2234057 RRC: si2_p=1,si3_p=1,si4_p=1,2ter_ind=0,gprs_ind_p=1,2q_ind=1,2ter_not_use
6:59.326	GSM	Time:2234057 RRPROC: 0 findRcell, a 0x0 p 0, a 0x0 p 0, a 0x0 p 0, a 0x0 p 0, a 0x0 p 0,
6:59.326	GSM	Time:2234057 RRC: Ext info LEN = 16, left_len=102
6:59.326	GSM	Time:2234057 EGPRS info included in GPRS_CELL_OPTION
6:59.326	GSM	Time:2234057 RRC:CCN_ACTIVE 1 in GPRS_CELL_OPTION
6:59.326	GSM	Time:2234057 RRC:Si13 arfcn=122, bsic =37,bss_pag_coord=0
6:59.326	GSM	Time:2234057 RRC: SGSNR 1

若系统消息 13 中包含 EDGE 的参数，TRACE 中会打印 EGPRS info included in GPRS\_CELL\_OPTION。

#### 说明

系统消息 13 的解码参考 3GPP Protocol 44018 9.1.43a,44018 10.5.2.37b,44060 12.24。

RR 会通过 MSG\_ID\_GMMAS\_CURR\_NW\_CAPABILITY\_IND 向上层报告是否支持 EDGE。

edge\_support=1 表示支持 EDGE，如图 2-2 所示。

图2-2 MSG\_ID\_GMMAS\_CURR\_NW\_CAPABILITY\_IND

161328...	14:36:51.798	0x2464	MSG_ID_RR_PLM_SYS_INFO_IND	MOD_NAS_SWTH_1->MOD_PLM_1
161328...	14:36:51.798	0x246A	MSG_ID_RR_PLM_STATE_CHANGE_IND	MOD_NAS_SWTH_1->MOD_PLM_1
161328...	14:36:51.798	0x2465	MSG_ID_GMMAS_CURR_NW_CAPABILITY_IND	MOD_NAS_SWTH_1->MOD_GMM_1
161328...	14:36:51.799	0x0124	MSG_ID_AS_I4_SIGNAL_QUALITY_IND	MOD_NAS_SWTH_1->MOD_MNM_1
161328...	14:36:51.799	0x2432	MSG_ID_MM_PLM_SYS_INFO_IND	MOD_PLM_1->MOD_GMM_1
161328...	14:36:51.799	0x249B	MSG_ID_MM_PLMN_INFO_IND	MOD_PLM_1->MOD_GMM_1
161329...	14:36:51.799	0x0134	MSG_ID_GMMREG_CURRENT_RAT_INFO_IND	MOD_GMM_1->MOD_MNM_1
161329...	14:36:51.799	0x480E	MSG_ID_CURRENT_RAT_INFO_IND	MOD_GMM_1->MOD_CC_1

```

[LOCAL] gmmas_curr_nw_capability_ind_struct
--ref_count = 0x1
--cell_capability_info
--hsdpa_support = 0x0
--hsupa_support = 0x0
--mbms_support = 0x0
--edge_support = 0x1
--hspa_plus_supported = 0x0
--fast_dormancy_supported_flag = 0x0
--fast_dormancy_supported = 0x0
--e_utran_ca_supported_flag = 0x0
--e_utran_ca_supported = 0x0
[PEER] NO_CONTENT_INSIDE

```

Unisoc Confidential For hiar

## 2.2 UE 支持 EDGE 情况

LOG 中可以了解 UE 上报网络是否支持 EDGE，如图 2-3 所示。UE 在 ATTACH REQUEST 的参数 ms\_ra\_acc\_cap 中上报了终端对 EDGE 的支持情况，可根据 3GPP Protocol 24.008/ 10.5.5.12a MS Radio Access capability 进行解码，若支持 EDGE，需要填写 8PSK 调制相关参数。

图2-3 UE 上报 EDGE 能力

16138367-1	14:36:54.260	SIM1		<- LOCATION_UPDATING_ACCEPT	
16139260-1	14:36:54.495	SIM1	GSM		<- CHANNEL_RELEASE
16140491-1	14:36:54.755	SIM1		<- ATTACH_REQUEST	
16141949-1	14:36:55.098	--	GSM		<- IMMEDIATE_ASSIGNMENT
16141953-1	14:36:55.098	SIM1	GSM		<- IMMEDIATE_ASSIGNMENT
16142147-1	14:36:55.147	--	GSM		<- PACKET_DL_DUMMY_CTRL_RL

SN	UE Time	MSG ID	Content	Module
161404...	14:36:54.755	0x4812	MSG_ID_ILGMM_RESET_ILC_PARAM_REQ	MOD_GMM_1->MOD_NAS_SWTH_1
161404...	14:36:54.755	0x4404	MSG_ID_ILGMM_ASSIGN_REQ	MOD_GMM_1->MOD_NAS_SWTH_1
161404...	14:36:54.755	0x3419	MSG_ID_GHSM_TLLI_REQ	MOD_GMM_1->MOD_SM_1
161404...	14:36:54.755	0x5811	MSG_ID_GMM_AS_CPES_IDENTITY_UPDATE_REQ	MOD_GMM_1->MOD_NAS_SWTH_1
16140491-1	14:36:54.755	0x0025	MSG_ID_ILGMM_UNITDATA_REQ	MOD_GMM_1->MOD_NAS_SWTH_1
161404...	14:36:54.755	0x4C18	MSG_ID_GMM_AS_CPES_NON_DRX_BEGIN_REQ	MOD_GMM_1->MOD_NAS_SWTH_1
161404...	14:36:54.755	0x2464	MSG_ID_RR_PLM_SYS_INFO_IND	MOD_NAS_SWTH_1->MOD_PLM_1
161405...	14:36:54.755	0x246A	MSG_ID_RR_PLM_STATE_CHANGE_IND	MOD_NAS_SWTH_1->MOD_PLM_1
161405...	14:36:54.756	0x0124	MSG_ID_AS_L4_SIGNAL_QUALITY_IND	MOD_NAS_SWTH_1->MOD_MNM_1

```
ptmsi_or_insi
[0] = 0xf4
[1] = 0xf3
[2] = 0x16
[3] = 0xb0
[4] = 0x1b
rai_val
ms_ra_acc_cap
[0] = 0x1b
[1] = 0x33
[2] = 0x43
[3] = 0x2b
[4] = 0x25
[5] = 0x96
[6] = 0x42
[7] = 0x0
[8] = 0x40
[9] = 0x0
[10] = 0x0
[11] = 0x0
[12] = 0x19
[13] = 0xc0
[14] = 0x2c
[15] = 0x64
[16] = 0x20
```

## 2.3 网络给 UE 配置 EDGE 资源

通过 PH\_MAC\_TBF\_CONNECT\_REQ 可快速查看网络是否给终端配置了 EDGE 资源。

图 2-4 表示网络给终端分配的 EDGE 信道，参数 tbf\_mode 为 0 表示分配的是 GPRS 信道，参数为 1 表示分配的是 EDGE 信道。

图2-4 网络分配的 EDGE 信道

161424...	14:36:55.266	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161424...	14:36:55.267	0x0139	PH_MAC_TA_PWR_REQ	MOD_GMAC->MOD_GLAYER1
16142421-1	14:36:55.267	0x0136	PH_MAC_TBF_CONNECT_REQ	MOD_GMAC->MOD_GLAYER1
161424...	14:36:55.267	0x0176	PH_MAC_TBF_CONNECT_CNF	MOD_GLAYER1->MOD_GMAC
161424...	14:36:55.267	0x019E	MAC_RLC_TBF_ASSIGNMENT_IND	MOD_GMAC->MOD_GRLC
161424...	14:36:55.275	0x000C	MPH_NC_MEAS_REPORT_IND	MOD_GLAYER1->MOD_GRR1
161424...	14:36:55.275	0x000C	MPH_NC_MEAS_REPORT_IND	MOD_GRR1->MOD_GRR_1
161425...	14:36:55.285	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161425...	14:36:55.293	0x0175	RLC_MAC_DATA_REQ	MOD_GRLC->MOD_GMAC
161425...	14:36:55.309	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161425...	14:36:55.311	0x0175	RLC_MAC_DATA_REQ	MOD_GRLC->MOD_GMAC
161426...	14:36:55.326	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161426...	14:36:55.327	0x01A0	MAC_RLC_CONN_RESP_IND	MOD_GMAC->MOD_GRLC

```

chann_cfg
├── tsc = 0x1
├── ul_timeslot_masks = 0x4
├── dl_timeslot_masks = 0x0
├── ptch_timeslot = 0xff
├── arfcn = 0x0
├── hsn = 0x18
├── channel_hopping = 0x1
├── maio = 0x0
├── ma_list
├── starting_time
├── ph_mac_mode
├── meas_param
├── ms_band = EGSM_DCS_DUALBAND
├── tfi = 0xff
├── tbf_mode = 0x1
├── egprs_tbf_param
├── bep_period2 = 0x5
├── arq = 0x1
├── multiblock_num = 0x0
├── dl_qlc_mode = 0xff

```

Unisoc Confidential For hiar

## 2.4 终端和网络的相互确认机制

网络会给终端上行的数据进行确认，终端也会对网络下行的数据进行确认。

一般情况可以通过 MAC\_RLC\_UPLACK\_IND 查看上行数据的情况，分成 GPRS 和 EDGE 两部分参数，在对应的参数查看分配的资源。这两部分都包含 final\_ack\_ind 参数，如图 2-5 所示，若该参数为 1，表示终端上行的数据 GPRS 和 EDGE 网络都已收到。

图2-5 MAC\_RLC\_UPLACK\_IND

161488...	14:36:57.100	0x0010	MPH_RR_CELLS_INFO_REQ	MOD_GRR1->MOD_GRR1
161488...	14:36:57.108	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161489...	14:36:57.126	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161490...	14:36:57.145	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
16149023-1	14:36:57.145	0x019F	MAC_RLC_UPLACK_IND	MOD_GMAC->MOD_GRLC
161490...	14:36:57.145	0x040D	RLC_RELEASE	MOD_GRLC->MOD_GRLC
161491...	14:36:57.168	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161491...	14:36:57.176	0x0008	PH_MAC_DATA_REQ	MOD_GRLC->MOD_GMAC
161491...	14:36:57.176	0x0178	PH_MAC_UL_REL_REQ	MOD_GMAC->MOD_GMAC
161491...	14:36:57.176	0x0137	PH_MAC_TBF_RELEASE_REQ	MOD_GMAC->MOD_GLAYER1
161491...	14:36:57.177	0x0177	PH_MAC_TBF_RELEASE_REQ	MOD_GLAYER1->MOD_GMAC

[LOCAL] MAC\_RLC\_UPLACK\_IND MSG

```

ref_count = 0x01
ack_desc =
  final_ack_ind = 0x00
  ssn = 0xU(U)
  RBB = 00,00,00,00,00,00,00,00,
  RBB:ack_BSN = 0~~255
  RBB:nack_BSN = 64~~127
  mcs = 0x0010
  is_tbf_est = 0x00
  ts_num = 0x0001
  abs_fn = 0x1812cb(1577675)
  re_sgmt = 0x00
  pre_empty = 0x01

```

终端对网络下行数据的 ACK 包含在 PH\_MAC\_DATA\_REQ 中，点开查看 MCS 是否等于 EGPRS\_DL\_ACKNACK，注意参数 SSN 和 ack\_before\_BSN，一般情况当 SSN=ack\_before\_BSN+1 时，表示终端下行数据 GPRS 和 EDGE 网络都收到，如图 2-6 所示。

图2-6 PH\_MAC\_DATA\_REQ

161495...	14:36:57.307	0x01A1	MAC_RLC_DATA_IND	MOD_GMAC->MOD_GRLC
161495...	14:36:57.307	0x01C4	RLC_LLC_DUMMYUI_IND	MOD_GRLC->MOD_GLLC
161496...	14:36:57.325	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
16149680-1	14:36:57.338	0x0008	PH_MAC_DATA_REQ	MOD_GRLC->MOD_GMAC
161497...	14:36:57.348	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161497...	14:36:57.366	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161498...	14:36:57.385	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161498...	14:36:57.408	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161499...	14:36:57.426	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161500...	14:36:57.446	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161500...	14:36:57.446	0x01A1	MAC_RLC_DATA_IND	MOD_GMAC->MOD_GRLC
161500...	14:36:57.446	0x01C4	RLC_LLC_DUMMYUI_IND	MOD_GRLC->MOD_GLLC
161500...	14:36:57.468	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161500...	14:36:57.476	0x0008	PH_MAC_DATA_REQ	MOD_GRLC->MOD_GMAC
161501...	14:36:57.486	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161501...	14:36:57.505	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC
161502	14:36:57.528	0x0007	PH_MAC_DATA_IND	MOD_GLAYER1->MOD_GMAC

```

puncture_type = 0x0000
array = data
  MCS = EGPRS_DL_ACKNACK
  R = U
  PAYLOAD_TYPE = 1
  DOWNLINK_TFI = 30
  is_OutMem = 0
  is_ChNQua = 1
  is_ChNReq = 0
  is_Pfi = 0
  LENGTH_PRESENT = 1
  LENGTH = 15
  FINAL_ACK_IND = 0
  is_BOW = 1
  is_EOW = 1
  SSN = 6
  is_Compressed = 0
  URBB_LEN = 0
  ack_before_BSN = 5
  nack_BSN = 5
  CRBB = NONE
  
```

## 2.5 Timer

在 EDGE 下会出现很多 Timer 超时的消息 TXXXX\_EXP\_IND，不同 Timer 代表的含义请参见表 2-1。

表2-1 Timer 描述

Timer	含义	是否正常	可能的问题
3192	收到 FINAL BLCOK 后等待释放。	正常	无。
3182	发送完最后一包上行数据，等待 UPLINK ACK/NACK 消息。	异常	可能是上行出现问题。

Timer	含义	是否正常	可能的问题
3168	等待上行的资源。	异常	出现一次问题不严重，如果出现四次，会释放链路。可能是下行链路不好，也可能是上行出现问题。
3166	发送完第一包上行数据，等待 UPLINK ACK/NACK 消息。	异常	可能是上行出现问题。
3146	进行 PRACH 接入。	异常	可能是 PRACH 没有发送到网络端，或者下行出现问题没有到资源配置消息。

## 说明

Timer 请参考 3GPP Protocol 44060 13.1 13.3 Timers on the Mobile Station side。

Unisoc Confidential For hiar

# 3 常见问题

## 3.1 GSM 常见问题

### 信号覆盖差

根据 POWER SWEEP 得出的结果，检查 MPH\_RXPOWER\_SWEEP\_CNF 上报的各个频点的功率，如果频点功率都是 0x10（经验数据）以下，表示信号强度不佳。

图3-1 POWER SWEEP 结果

16440-1	10:18:27.372	--	0x0202	MPH_RXPOWER_SWEEP_CNF	MOD_GL1SIM->MOD_GRRRA
16474-1	10:18:27.372	--	0x0349	GRRRA_LRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_LRRCA
16481-1	10:18:27.372	--	0x0202	MPH_RXPOWER_SWEEP_CNF	MOD_GRRRA->MOD_GRR_1
16503-1	10:18:27.372	--	0x02D9	MPH_BSIC_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRRRA
16551-1	10:18:27.372	--	0x0108	RRA_MPH_BSIC_LIST_DECODE_REQ	MOD_GRRRA->MOD_GL1SIM
16559-1	10:18:27.372	--	0x041A	WAIT_BSIC_BCCH_DECODE	MOD_GRR_1->MOD_GRR_1
16579-1	10:18:27.871	--	0x0205	MPH_BSIC_DECODE_CNF	MOD_GL1SIM->MOD_GRRRA
16584-1	10:18:27.871	--	0x0205	MPH_BSIC_DECODE_CNF	MOD_GL1SIM->MOD_GRRRA
16589-1	10:18:27.871	--	0x0205	MPH_BSIC_DECODE_CNF	MOD_GRRRA->MOD_GRR_1
16596-1	10:18:27.871	--	0x02D7	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRRRA
16646-1	10:18:27.871	--	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRRRA->MOD_GL1SIM

[LOCAL] MPH_RXPOWER_SWEEP_CNF MSG	
ref_count	= 0x1
ph_rxlev_arr	
[0]	= 0x0
[1]	= 0x0
[2]	= 0x0
[3]	= 0x0
[4]	= 0x0
[5]	= 0x0
[6]	= 0x0
[7]	= 0x0
[8]	= 0x0
[9]	= 0x0
[10]	= 0xa
[11]	= 0x0
[12]	= 0x0
[13]	= 0x0
[14]	= 0x0
[15]	= 0x0
[16]	= 0x0
[17]	= 0x0
[18]	= 0x0
[19]	= 0x0

网络覆盖不好或者强干扰现象会导致 BSIC DECODE 失败。如果对应频点的 POWER SWEEP 结果比较低，BSIC 解码失败的概率增加，如果所有的频点都 DECODE FAIL，则向 NAS 上报 MM\_RR\_ACT\_IND（参数 RR\_ACT\_TYPE=2，表示 NO SERVICE）。



## BCCH 不匹配

常见的不匹配原因是 PLMN 不匹配。

PLMN 参数需要看以下 4 条消息：

- MM\_RR\_EPLMN\_LIST\_REQ, 配置 EPLMN, 如图 3-2 所示。
- MM\_RR\_ACT\_REQ, 包含目标 PLMN, 如图 3-3 所示。
- MM\_RR\_MM\_INFO\_REQ, 包含 UE 当前 FPLMN 和 FLAI 列表, 如图 3-4 所示。
- MPH\_BCCH\_INFO\_IND (系统消息 3,4), 广播网络的 PLMN, 如图 3-5 所示。

图3-2 EPLMN 配置

2300-23	13:15:15.023	FF	0x2430	MSG_ID_MM_PLMN_STATE_CHANGE_IND	MOD_PLMN_1->MOD_GMM_1
2300-43	13:15:15.023	FF	0x01EC	MM_RR_EPLMN_LIST_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
2300-46	13:15:15.023	FF	0x01E4	MM_RR_ACT_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
2301-1	13:15:15.023	FF	0x04DA	WDM_GSM_BAND_IND	MOD_GRR_1->MOD_WRRRC_1
2301-2	13:15:15.023	FF	0x04DA	WDM_GSM_BAND_IND	MOD_GRR_1->MOD_WRRRC_1
2301-6	13:15:15.023	FF	0x04D9	WDM_GSM_CLASSMARK_IND	MOD_GRR_1->MOD_WRRRC_1
2301-7	13:15:15.023	FF	0x04D9	WDM_GSM_CLASSMARK_IND	MOD_GRR_1->MOD_WRRRC_1
2301-24	13:15:15.023	FF	0x24A4	MSG_ID_MM_RR_GERAN_CAP_IND	MOD_GRR_1->MOD_GMM_1
2301-39	13:15:15.023	FF	0x02D4	MPH_ACTIVE_REQ	MOD_GRR_1->MOD_GRRCA
2301-58	13:15:15.023	FF	0x0354	GRRCA_LRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_LRRCA
2301-59	13:15:15.023	FF	0x0139	GRRCA_NRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_NRRCA
2302-5	13:15:15.023	FF	0x034F	MSG_ID_LRRCA_LRRCA_STATUS_UPDATE_IND	MOD_LRRCA->MOD_LASM_1
2302-13	13:15:15.023	FF	0x02D6	MPH_RXPOWER_SWEEP_REQ	MOD_GRR_1->MOD_GRRCA
2302-43	13:15:15.023	FF	0x0139	GRRCA_NRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_NRRCA

```

[LOCAL] MM_RR_EPLMN_LIST_REQ_MSG
- ref_count = 0x1
- eplmn_list
  - length = 0x1
  - plmn_arr
    - [0]
      - mcc = 0x100
      - mnc = 0x1
      - mnc_digit_num = 0x2
    - [1]
      - mcc = 0x0
      - mnc = 0x0
      - mnc_digit_num = 0x0
    - [2]
      - mcc = 0x0
      - mnc = 0x0
      - mnc_digit_num = 0x0
    - [3]
      - mcc = 0x0
      - mnc = 0x0
      - mnc_digit_num = 0x0
    - [4]
      - mcc = 0x0
      - mnc = 0x0
      - mnc_digit_num = 0x0
    - [5]
      - mcc = 0x0
      - mnc = 0x0
      - mnc_digit_num = 0x0
  
```

图3-3 MM\_RR\_ACT\_REQ 中的 PLMN 配置

2299-25	13:15:15.023	FF	0x2465	MSG_ID_RR_PLM_HANDSHAKE_RSP	MOD_NAS_SWTH_1->MOD_PLM_1
2300-21	13:15:15.023	FF	0x581A	MSG_ID_PLM_AS_GPRS_PLMN_SEL_REQ	MOD_PLM_1->MOD_NAS_SWTH_1
2300-23	13:15:15.023	FF	0x2430	MSG_ID_MM_PLM_STATE_CHANGE_IND	MOD_PLM_1->MOD_GMM_1
2300-43	13:15:15.023	FF	0x01EC	MM_RR_EPLMN_LIST_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
2300-46	13:15:15.023	FF	0x01E4	MM_RR_ACT_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
2301-1	13:15:15.023	FF	0x04DA	WDM_GSM_BAND_IND	MOD_GRR_1->MOD_WRRRC_1
2301-2	13:15:15.023	FF	0x04DA	WDM_GSM_BAND_IND	MOD_GRR_1->MOD_WRRRC_1
2301-6	13:15:15.023	FF	0x04D9	WDM_GSM_CLASSMARK_IND	MOD_GRR_1->MOD_WRRRC_1
2301-7	13:15:15.023	FF	0x04D9	WDM_GSM_CLASSMARK_IND	MOD_GRR_1->MOD_WRRRC_1
2301-24	13:15:15.023	FF	0x24A4	MSG_ID_MM_RR_GERAN_CAP_IND	MOD_GRR_1->MOD_GMM_1
2301-39	13:15:15.023	FF	0x02D4	MPH_ACTIVE_REQ	MOD_GRR_1->MOD_GRR_1
2301-58	13:15:15.023	FF	0x0354	GRR_1_LRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_LRRCA
2301-59	13:15:15.023	FF	0x0139	GRR_1_NRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_NRRCA
2302-5	13:15:15.023	FF	0x034F	MSG_ID_LRRCA_LRRCA_STATUS_UPDATE_IND	MOD_LRRCA->MOD_LASM_1
2302-13	13:15:15.023	FF	0x02D6	MPH_RXPOWER_SWEEP_REQ	MOD_GRR_1->MOD_GRR_1
2302-43	13:15:15.023	FF	0x0139	GRR_1_NRRCA_STATE_NOTIFY	MOD_GRR_1->MOD_NRRCA

```

[LOCAL] MM_RR_ACT_REQ_MSG
--ref_count = 0x1
--rr_act_type = RR_ACT_NORMAL
--sel_param
--plmn
--mcc = 0x1cc
--mnc = 0x1
--mnc_digit_num = 0x2
--select_any_plmn = 0x0
--ba_undecoded
--bis_ba_undecoded
--arfcn_list_first = 0x1
--arfcn_list
--ignore_forbid_plmn_list = 0x0
--ms_band = GSM850_EGSM_DCS_PCS_QUALBAND
--gprs_requested = 0x1
--manual_select_plmn = 0x0
--sel_hplmn = 0x0
--band_filter
--band_filter_on = 0x0
--start_arfcn = 0x3e8
--end_arfcn = 0x3fb
--emergency_select_flag = 0x0
--ms mode = 0x0

```

图3-4 MM\_RR\_MM\_INFO\_REQ 中的 FPLMN 配置

2299-1	13:15:15.023	FF	0x01E8	MM_RR_MM_INFO_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
2299-5	13:15:15.023	FF	0x01E8	MM_RR_MM_INFO_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
2299-10	13:15:15.023	FF	0x01E8	MM_RR_MM_INFO_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
2299-16	13:15:15.023	FF	0x01ED	MM_RR_MS_PREFERRED_RAT_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
2299-22	13:15:15.023	FF	0x02BD	MM_RR_MS_PREFERRED_RAT_RSP	MOD_GRR_1->MOD_NAS_SWTH_1
2299-25	13:15:15.023	FF	0x2465	MSG_ID_RR_PLM_HANDSHAKE_RSP	MOD_NAS_SWTH_1->MOD_PLM_1
2300-21	13:15:15.023	FF	0x581A	MSG_ID_PLM_AS_GPRS_PLMN_SEL_REQ	MOD_PLM_1->MOD_NAS_SWTH_1
2300-23	13:15:15.023	FF	0x2430	MSG_ID_MM_PLM_STATE_CHANGE_IND	MOD_PLM_1->MOD_GMM_1
2300-43	13:15:15.023	FF	0x01EC	MM_RR_EPLMN_LIST_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
2300-46	13:15:15.023	FF	0x01E4	MM_RR_ACT_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
2301-1	13:15:15.023	FF	0x04DA	WDM_GSM_BAND_IND	MOD_GRR_1->MOD_WRRRC_1

```

[LOCAL] MM_RR_MM_INFO_REQ_MSG
--ref_count = 0x1
--tmsi
--imsi
--kc
--kc128
--cksn = 0x2
--flai_list_r
--acc_class = 0x80
--rr_hplmn
--mcc = 0x1cc
--mnc = 0x1
--mnc_digit_num = 0x2
--fplmn_list
--length = 0x7
--fplmn_arr
--rai_info
--mcc = 0x1cc
--mnc = 0x1
--mnc_digit_num = 0x2
--lac = 0xa802
--rac = 0x2
--flai_list_s

```

图3-5 系统消息中的 PLMN 不匹配

2460-6	13:15:17.322	FF	0x0026	MSG_ID_ATC_MUX_RECV_AT_CMD	MOD_DUMMY_MMI->MOD_DUMMY_MMI
2460-13	13:15:17.322	FF	0x4011	MSG_ID_MNM_RESTRICT_SIM_ACCESS_REQ	MOD_MNC_1->MOD_SIM_1
2460-25	13:15:17.351	FF	0x0005	MPH_BCCH_INFO_IND	MOD_GLAYER1->MOD_GRR
2460-30	13:15:17.351	FF	0x0005	MPH_BCCH_INFO_IND	MOD_GRR->MOD_GRR_1
2461-17	13:15:17.351	FF	0x02D9	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRR
63764-32	13:15:17.381	F5	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRR->MOD_GLAYER1
63764-60	13:15:17.381	F5	0x03BB	ES_EVENT_CANCEL_REQ	MOD_GLAYER1->MOD_ESHANDLE
63765-18	13:15:17.381	F5	0x0108	RRA_MPH_BSIC_LIST_DECODE_REQ	MOD_GRR->MOD_GLAYER1
2463-9	13:15:17.351	FF	0x02DB	MPH_BSIC_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRR

LOCAL MPH\_BCCH\_INFO\_IND\_MSG

ref\_count = 0x1

chan\_type = BCCH

ph\_arfcn = 0x6

ph\_block

[0] = 0x49

[1] = 0x6

[2] = 0x1b

[3] = 0x50

[4] = 0x6f

[5] = 0x64

[6] = 0xf0

[7] = 0x0

[8] = 0x18

RAT	Core	Content
GSM	FF	-----: cell 3,a 0x7b,tc 0x0   cell 4,a 0x305,tc 0x0   cell 5,a 0x2fd,tc 0x0
GSM	FF	RRCCELL: ecid cell arfcn 0x6, bsic 0x2a, cell_num 0, update_num 0, msg_type 27
GSM	FF	RRC: g_rx_ex[0]->supported=0, arfcn=6, cell_ptr->cl=34
GSM	FF	rat=0 cell arfcn=6, bsic_psc_pci=42, is_in_blackcell=0
GSM	FF	[MNSIM_SimuGetVSIMFuncSwitch]: [0]:sim_simu_driver_switch_g[0]=0
GSM	FF	RR_GetCellSelPriority, cell 0x6 is in fplan list, cell prio ACCEPT cell
GSM	FF	rat=0 cell arfcn=6, bsic_psc_pci=42, is_in_blackcell=0
GSM	FF	rat=0 cell arfcn=6, bsic_psc_pci=42, is_in_blackcell=0
GSM	FF	RRA: rra_sub_state[0~1]: [active,search,cell_decode] [null], sig_code:0x2d9
GSM	FF	RRA: upper_layer_gsm_rat_flag[0~1]: [0x1] [0xff]

如图 3-5 所示，RR 收到的系统消息 3 中的 PLMN 是 460 00，不在图 3-2 图 3-3 的合集中，而是在图 3-4 所示的 fplmn 列表中。在这种情况下，RR 会停止系统消息的接收，重新换频点进行 BSIC DECODE 和 BCCH DECODE。

## 掉话

GSM 系统下掉话有两种常见情况。

- MDL\_ERR\_IND：一般是 SDCCH 或者 FACCH 链路出现问题，DL 的链接无法恢复，如图 3-6 所示。
- MPH\_ERROR\_IND：连续收到若干包 SACCH 解码失败，bad SA counter 减为 0，如图 3-7 所示。

图3-6 MDL\_ERR\_IND

303455...	15:54:33.611	--	0x035A	MSG_ID_TM_GSM_TO_LTE_GAP_CONFIG_REQ	MOD_L1AYER1-AD-→MOD_GLAYER1
303455...	15:54:33.848	--	0x0156	PH_DATA_IND	MOD_GLAYER1-→MOD_GDL
303456...	15:54:33.874	--	0x0158	DL_SAPIO_T200_EXP_IND	MOD_TIMER-→MOD_GDL
303456...	15:54:33.874	--	0x0335	RRA_MDL_ERR_IND	MOD_GDL-→MOD_GRR
303456...	15:54:33.874	--	0x032F	RRA_DL_RELEASE_IND	MOD_GDL-→MOD_GRR
303456...	15:54:33.874	--	0x0227	MDL_ERR_IND	MOD_GRR-→MOD_GRR_1
303456...	15:54:33.874	--	0x0223	DL_RELEASE_IND	MOD_GRR-→MOD_GRR_1
303456...	15:54:33.874	--	0x02EA	MPH_CHAN_REL_REQ	MOD_GRR_1-→MOD_GRR
303456...	15:54:33.874	--	0x011A	RRA_MPH_CHAN_REL_REQ	MOD_GRR-→MOD_GLAYER1
303456...	15:54:33.875	--	0x034E	MSG_ID_TM_GSM_TO_LTE_GAP_CANCEL_REQ	MOD_GLAYER1-→MOD_L1AYER1_AD
303456...	15:54:33.875	--	0x00AF	GL1C_WL1C_NOTICE_G_TRAFFIC_IND_EX	MOD_GLAYER1-→MOD_SSI_2
303456...	15:54:33.875	--	0x00AF	GL1C_WL1C_NOTICE_G_TRAFFIC_IND_EX	MOD_GLAYER1-→MOD_WL1Meas
303456...	15:54:33.875	--	0x041A	PG_REORG_CAMPED	MOD_GLAYER1-→MOD_GLAYER1
303456...	15:54:33.875	--	0x013B	MSG_ID_CMD_GSM_LTE_GAP_CONFIG_REQ	MOD_L1AYER1_AD-→MOD_LCONTR
303457...	15:54:33.876	--	0x00AE	GL1C_WL1C_NOTICE_G_TRAFFIC_IND	MOD_WL1Meas-→MOD_WL1Meas
303457...	15:54:33.876	--	0x030A	MDL_RELEASE_REQ	MOD_GRR_1-→MOD_GRR
303457...	15:54:33.876	--	0x0155	RRA_MDL_RELEASE_REQ	MOD_GRR-→MOD_GDL

[LOCAL] MDL_ERR_IND_MSG					
ref_count	=	0x1			
sapi	=	0x0			
chan_type	=	SDCCH			
dl_err_cause	=	DL_ERR_T200_EXPIRED			

图3-7 MPH\_ERROR\_IND

105395...	10:11:59.547	FF	0x015B	PH_DATA_REQ	MOD_GDL-→MOD_GDL
105395...	10:11:59.918	FF	0x0211	MPH_ERROR_IND	MOD_GLAYER1-→MOD_GRR
105395...	10:11:59.918	FF	0x0157	PH_DATA_IND	MOD_GLAYER1-→MOD_GDL
105395...	10:11:59.918	FF	0x0211	MPH_ERROR_IND	MOD_GRR-→MOD_GRR_1
105395...	10:11:59.918	FF	0x02E9	MPH_CHAN_REL_REQ	MOD_GRR_1-→MOD_GRR
105396...	10:11:59.918	FF	0x030B	MDL_RELEASE_REQ	MOD_GRR_1-→MOD_GRR
105396...	10:11:59.918	FF	0x0156	RRA_MDL_RELEASE_REQ	MOD_GRR-→MOD_GDL
105396...	10:11:59.918	FF	0x02B2	MM_RR_ABORT_IND	MOD_GRR_1-→MOD_NAS_SWTH_1
1053961-1	10:11:59.918	FF	0x02FD	MPH_TM_GSM_MEAS_LTE_REQ	MOD_GRR_1-→MOD_GRR
1053962-1	10:11:59.918	FF	0x0338	MSG_ID_TM_GSM_MEAS_LTE_REQ	MOD_GRR_1-→MOD_L1AYER1_AD
1053963-1	10:11:59.918	FF	0x0000	MSG_ID_LTE_TM_GSM_LTE_MEAS_REQ:SEGMENT240...	----->----
1053963-2	10:11:59.918	FF	0x0000	MSG_ID_LTE_TM_GSM_LTE_MEAS_REQ:SEGMENT240...	----->----
1053964-1	10:11:59.918	FF	0x0000	MSG_ID_LTE_TM_GSM_LTE_MEAS_REQ:SEGMENT240...	----->----

[LOCAL] MPH_ERROR_IND_MSG					
ref_count	=	0x1			
ph_arfcn	=	0x26a			
ph_error	=	RADIO_LINK_FAIL			
decode_band	=	DCS1800			
card_id	=	0x1			

## 接入失败

在 GSM 系统下，终端和网络建立双向连接都需要进行 RACH 过程。RACH 信道向网络发送接入请求后，终端在 AGCH 信道收到 IMMEDIATE ASSIGNMENT 消息。

接入过程中，如果第一个 RACH 没有收到相应的 AGCH，会重新发送若干次 RACH（重发次数参考 3GPP Protocol 44018 10.5.2.29 RACH Control parameters）。重发次数达到最大重发次数还没有收到 AGCH 时，等待 T3126，超时表示此次随机接入失败。

图3-8 T3126 超时

354-18	15:38:02.177	FF	0x0361	RRA_MPH_IDLE_NCELL_MEAS_IND	MOD_GL1SIM->MOD_GRR_A
354-23	15:38:02.177	FF	0x0009	MPH_IDLE_NCELL_MEAS_IND	MOD_GRR_A->MOD_GRR_1
362-24	15:38:05.173	FF	0x0361	RRA_MPH_IDLE_NCELL_MEAS_IND	MOD_GL1SIM->MOD_GRR_A
362-29	15:38:05.173	FF	0x0009	MPH_IDLE_NCELL_MEAS_IND	MOD_GRR_A->MOD_GRR_1
363-2	15:38:05.391	FF	0x024D	RR_T3126_EXP_IND	MOD_TIMER->MOD_GRR_1
363-4	15:38:05.391	FF	0x02EC	MPH_CHAN_REL_REQ	MOD_GRR_1->MOD_GRR_A
363-24	15:38:05.391	FF	0x011A	RRA_MPH_CHAN_REL_REQ	MOD_GRR_A->MOD_GL1SIM
363-40	15:38:05.391	FF	0x0005	MPH_BCCH_INFO_IND	MOD_GL1SIM->MOD_GRR_A
363-45	15:38:05.391	FF	0x02B4	MM_RR_ABORT_IND	MOD_GRR_1->MOD_NAS_SWTH_1
363-53	15:38:05.391	FF	0x02D9	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRR_A
363-112	15:38:05.391	FF	0x0418	RRC Idle	MOD_GRR_1->MOD_GRR_1
363-115	15:38:05.391	FF	0x02D7	MPH_BCCH_CAMP_REQ	MOD_GRR_1->MOD_GRR_A
363-146	15:38:05.391	FF	0x0418	WAIT_BCCH_CAMP_RESEL	MOD_GRR_1->MOD_GRR_1
363-147	15:38:05.391	FF	0x0005	MPH_BCCH_INFO_IND	MOD_GRR_A->MOD_GRR_1
363-150	15:38:05.391	FF	0x2827	MSG_ID_CCAS_RAB_REL_IND	MOD_NAS_SWTH_1->MOD_CC_1
363-151	15:38:05.391	FF	0x2426	MSG_ID_GMMAS_ESTABLISH_REJ	MOD_NAS_SWTH_1->MOD_GMM_1

!!!

[LOCAL] sdi\_msg\_user\_data\_struct  
ref\_count = 0x1

分析 LOG 时，如果 T3126 超时，观察 RACH 发送到 T3126 超时这段时间 TRACE 中是否有 BAD AGCH。如果没有大概率是 RACH 上行问题，如果出现很多 BAD AGCH，则是下行接收问题。

## 3.2 GSM/EDGE 常见问题

### 进行数据业务时接不到电话

在 GSM/EDGE 系统下，WAP 或者 QQ 测试被叫成功，但手机经常接受不到被叫寻呼。

一般有两种情况，可能手机是 CLASS B 类型，不支持语音数据并发功能，也有可能是网络因素 NMO (Network Mode of Operation)。

#### NMO (2 bit field)

This field is the binary representation of the Network Mode of Operation, see 3GPP TS 23.060:

Bit

2 1

0 0	Network Mode of Operation I //网络在数据信道上发电路业务寻呼
0 1	Network Mode of Operation II //不在数据信道上发电路业务寻呼
1 0	Network Mode of Operation III //不在数据信道上发电路业务寻呼，也不在CCCH上发数据业务寻呼
1 1	Reserved.

此参数包含于系统消息 13/GPRS cell options 中，具体请参考 3GPP Protocol 44018 10.5.2.37b, 44060 12.24。

在 LOG 中有三种方法可以查看当前网络的 NMO。

- 方法一：解码系统消息 13，按照协议逐 BIT 解码。
- 方法二：查看 MM\_RR\_ACT\_IND 消息，如图 3-9 所示。
- 方法三：查看 MSG\_ID\_RR\_PLM\_SYS\_INFO\_IND，如图 3-10 所示。

图3-9 MM\_RR\_ACT\_IND

297-48	15:37:48.028	FF	0x0161	RRA_GRR_MAC_PARAM_REQ	MOD_GRR1->MOD_GMAC
297-50	15:37:48.028	FF	0x0317	GRR_MAC_FREQ_REQ	MOD_GRR1->MOD_GRR1
297-57	15:37:48.028	FF	0x0162	RRA_GRR_MAC_FREQ_REQ	MOD_GRR1->MOD_GMAC
297-65	15:37:48.028	FF	0x02B5	MM_RR_ACT_IND	MOD_GRR1->MOD_NAS_SWTH_1
297-68	15:37:48.028	FF	0x0385	GRR_GMM_ACCESS_BAR_IND	MOD_GRR1->MOD_NAS_SWTH_1
297-69	15:37:48.028	FF	0x0327	GRR_RLC_ACT_REQ	MOD_GRR1->MOD_GRR1
297-80	15:37:48.028	FF	0x0193	RRA_GRR_RLC_ACT_REQ	MOD_GRR1->MOD_GRR1
297-89	15:37:48.028	FF	0x02D8	MPH_IDLE_BA_UPDATE_REQ	MOD_GRR1->MOD_GRR1
297-95	15:37:48.028	FF	0x0105	RRA_MPH_IDLE_BA_UPDATE_REQ	MOD_GRR1->MOD_GRR1
297-117	15:37:48.028	FF	0x0418	RRC Idle	MOD_GRR1->MOD_GRR1
297-123	15:37:48.028	FF	0x02CC	RR_MN_SCELL_RSSI_IND	MOD_GRR1->MOD_NAS_SWTH_1
297-133	15:37:48.028	FF	0x02D9	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GRR1
298-33	15:37:48.028	FF	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GRR1
298-50	15:37:48.028	FF	0x0418	NORM_IDLE_MODE	MOD_GRR1->MOD_GRR1
298-56	15:37:48.028	FF	0x2466	MSG ID RR PLM SYS INFO IND	MOD_NAS_SWTH_1->MOD_PLM_1

```

ba_undecoded
ba_valid = 0x1
bis_ba_undecoded
bis_ba_valid = 0x0
arfcn = 0x14
band = EGSM900
mscr = 0x1
gsm_band = EGSM900
cell_access_class = 0x0
plmn_ba_band = EGSM900
ba_list
+ gprs_info
+ network_oper_mode = GPRS_MNO_TWO
+ rai
+ mcc = 0x1cc
+ mnc = 0x0
+ mnc_digit_num = 0x2
+ lac = 0x1
+ rac = 0x5
+ is_supp_egprs = 0x0
+ sgsnr = 0x1
+ is_cnf_to_mm_req = 0x0
+ emergency_select_flag = 0x1
+ network_umts_type = NETWORK_UTRAN_INVALID
+ is_only_search_ba = 0x0
+ is_non_home_zone_cell = 0x0
+ is_out_of_lock_cell = 0x0

```

图3-10 MSG\_ID\_RR\_PLM\_SYS\_INFO\_IND

297-133	15:37:48.028	FF	0x02D9	MPH_BCCH_LIST_DECODE_REQ	MOD_GRR_1->MOD_GRR1
298-33	15:37:48.028	FF	0x0106	RRA_MPH_BCCH_LIST_DECODE_REQ	MOD_GRR1->MOD_GLISIM
298-50	15:37:48.028	FF	0x0418	NORM_IDLE_MODE	MOD_GRR_1->MOD_GRR_1
298-56	15:37:48.028	FF	0x2466	MSG_ID_RR_PLM_SYS_INFO_IND	MOD_NAS_SWTH_1->MOD_PLM_1
298-57	15:37:48.028	FF	0x246D	MSG_ID_RR_PLM_STATE_CHANGE_IND	MOD_NAS_SWTH_1->MOD_PLM_1
298-62	15:37:48.028	FF	0x0125	MSG_ID_AS_L4_SIGNAL_QUALITY_IND	MOD_NAS_SWTH_1->MOD_MNM_1
298-83	15:37:48.028	FF	0x5816	MSG_ID_PLM_AS_GPRS_REGN_STATUS_UPDATE_REQ	MOD_PLM_1->MOD_NAS_SWTH_1
298-105	15:37:48.028	FF	0x2430	MSG_ID_MM_PLM_STATE_CHANGE_IND	MOD_PLM_1->MOD_GMM_1
298-123	15:37:48.028	FF	0x140C	MSG_ID_GMMREG_TCRB_STATUS_IND	MOD_GMM_1->MOD_MNM_1
298-131	15:37:48.028	FF	0x01E8	MM_RR_MM_INFO_REQ	MOD_NAS_SWTH_1->MOD_GRR_1
298-132	15:37:48.028	FF	0x0D29	MSG_ID_MNM_PHONE_SIGNAL_QUALITY_IND	MOD_MNM_1->MOD_MNC_1
298-135	15:37:48.028	FF	0x0D29	MSG_ID_MNM_PHONE_SIGNAL_QUALITY_IND	MOD_MNC_1->MOD_SSI_1
298-137	15:37:48.028	FF	0x0D29	MSG_ID_MNM_PHONE_SIGNAL_QUALITY_IND	MOD_SSI_1->MOD_MN_AL_1

```

[LOCAL] rr_plm_plan_sys_info_ind_struct

```

```

ref_count = 0x1
trans_id = 0x0
plmn_sel_mode = AUTOMATIC_PLMN_SEL
plmn_search_type = FOREGROUND_SEARCH
la_code
ra_code = 0x5
nmo = 0x1:NMO-II
t3212_timer_val = 0x0
ps_service_avail_for_nmo3 = 0x1
band_supported = 0x3
att_flag = 0x1
acc_class_validity = 0x1
cycle_len_coff = 0x0
cell_id = 0x1
cell_id_ext = 0x0
cell_support_ps = 0x1
cell_support_cs = 0x1
service_type = NORMAL_SERVICE
access_tech_type = GSM_BAND_E
acc_class
plmn_id
sgsnr_flag = 0x1
mscr_flag = 0x1
ta_code = 0x0
csg_indication = 0x0
csg_cell_flag = 0x0
csg_id = 0x0

```

Unisoc Confidential For hiar