



目录

LTE入网流程分析	错误！未定义书签。
Revision Record 修订记录	错误！未定义书签。
1 入网流程	2
1.1 UE初始化	3
1.2 PLMN选择	4
1.3 扫频	4
1.4 小区搜索	7
1.5 解系统消息（System Information）	8
1.6 小区选择	10
1.7 小区驻留（Camped on the Cell）：	10
1.8 Attach request	10
1.9 RRC CONNECTION Request	11
1.10 随机接入	11
1.11 RRC连接建立	12
1.12 Attach accept / Attach complete	12
2 搜网相关AT命令	13
2.1 AT+COPS命令	13
2.2 扩展系统配置参考设置命令 AT^syscfgex命令	13
3 UE LTE网络入网log抓取与查看	14
3.1 LTE入网log抓取	14
3.2 UE入网log查看	15
4 LTE的锁频方法	16
5 QCN的备份与导入	17
6 参考资料	18

1 入网流程

LTE入网是指UE开机上电后搜网，并注册到网络的过程。入网基本流程图如下图所示：

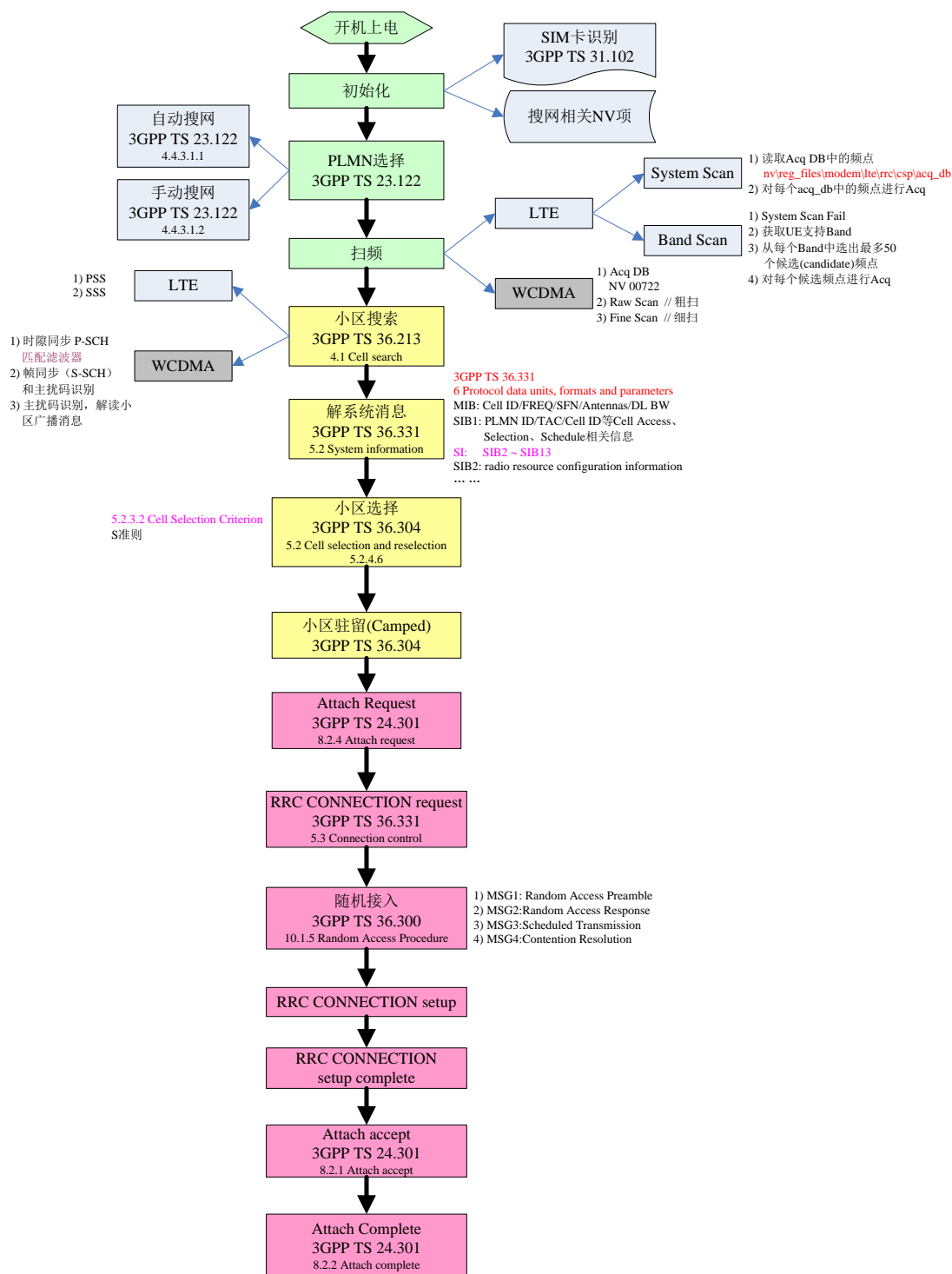


图1.1 入网基本流程图

LTE入网的详细流程分析如下：

1.1 UE 初始化

UE的初始化主要包含SIM卡识别和搜网相关NV项读取两部分内容。

SIM相关信息主要包括以下几项（参考协议3GPP TS 31.102）：

- 1) EF_{HPLMNwAcT}: HPLMN selector with Access Technology, 文件类型定义如图1.2;

EF_{HPLMNwAcT} (HPLMN selector with Access Technology)

Identifier: '6F62'		Structure: Transparent		Optional
SFI: '13'				
File size: 5n (n ≥ 1) bytes		Update activity: low		
Access Conditions:				
READ		PIN		
UPDATE		ADM		
DEACTIVATE		ADM		
ACTIVATE		ADM		
Bytes	Description		M/O	Length
1 to 3	1 st PLMN (highest priority)		M	3 bytes
4 to 5	1 st PLMN Access Technology Identifier		M	2 bytes
6 to 8	2 nd PLMN		O	3 bytes
9 to 10	2 nd PLMN Access Technology Identifier		O	2 bytes
:	:			
(5n-4) to (5n-2)	n th PLMN (lowest priority)		O	3 bytes
(5n-1) to 5n	n th PLMN Access Technology Identifier		O	2 bytes

MCC + MNC

图1.2 EF_{HPLMNwAcT}文件格式

- 2) EF_{OPLMNwAcT}: Operator controlled PLMN selector with Access Technology
- 3) EF_{PLMNwAcT}: User controlled PLMN selector with Access Technology
- 4) EF_{FPLMN}: Forbidden PLMNs
- 5) EF_{EHPLMN}: Equivalent HPLMN

搜网相关NV项，主要有以下几项：

- 1) NV 00010: Digital/Analog Mode Preference, 接入技术，通常采用Auto/2G/3G/4G四个选项；
- 2) NV 00849: Network Selection Mode Preference, 搜网模式，存在Auto和Manual两个选项；
- 3) NV 00850: Service Domain Preference, 服务域选取，可以是仅PS、仅CS或者PS+CS；
- 4) NV 00722: Acquisition Database, 用来存放WCDMA的历史频点信息；
- 5) LTE的频段信息存放在nv/item_files/modem/mmode/lte_bandpref文件中，参考图1.2；

关于lte_bandpref文件内容说明参考图1.3，其为E589u-12的lte_bandpref文件，说明

E589u-12支持Band1，Band3，Band7，Band8和Band20频段；

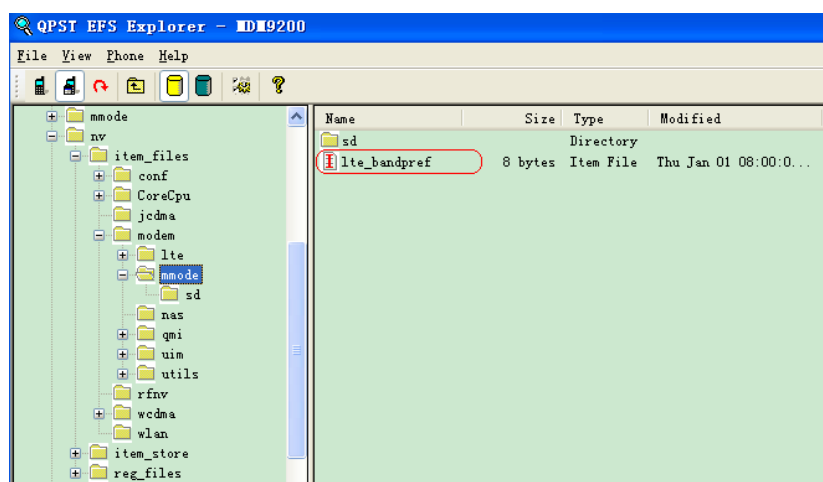


图1.3 lte_bandpref路径图

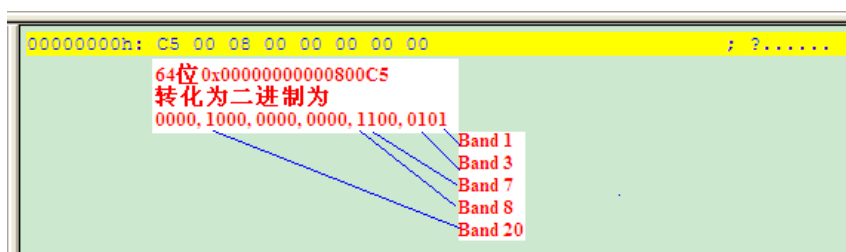


图1.4 lte_bandpref文件结构解析

1.2 PLMN 选择

PLMN选择分为自动搜网和手动搜网两种模式：

- 1) 自动搜网：UE按照协议23.122 4.4.3.1.1 Automatic Network Selection Mode Procedure规定的PLMN优先级进行搜网，即RPLMN->HPLMN->UPLMN->OPLMN。
- 2) 手动搜网：搜索RPLMN，协议23.122 4.4.3.1.2 Manual Network Selection Mode Procedure；UE会把所有的PLMN，包括不可用的PLMN列出来，供用户选择去注册；
- 3) 当没有找到可用的PLMN，单板会发起**MMR_REG_REQ PLMN(0-0) RAT(LTE)**的请求，这样单板就可以获得限制服务，如紧急呼叫。

1.3 扫频

LTE扫频有两种方式：system scan和band scan。

- 1) System Scan会扫历史记录频点，LTE的历史频点存放在NV的acq_db文件中，其具体保存路径为nv/reg_files/modem/lterrc/csp/acq_db (最多保存10个历史频点)，可以通过QPST查看，如图1.5所示；其文件结构解析如图1.6所示（蓝色标记数字为历史频点

QPST Explorer - MD19200

File View Phone Help

File operations toolbar: New, Open, Save, Print, Copy, Paste, Find, Help.

Left pane (File System):

- CGPS_PE
- CGPS_SM
- client-cert
- client-key
- gnss
- hdev
- mmode
- nv
 - item_files
 - item_store
 - reg_files
 - modem
 - lte
 - rrc
 - osp
 - nv_restore_log
 - nvmm
- OEMConfig
- pdp_profiles
- sd
- sms
- SUPL

Right pane (Table):

Name	Size	Type	Modified	Attr...	Mode	CTYP
acq_db	344 bytes	File	Sun Jan 06 08:00:0...	-AD	100666	S...

Status bar: For Help, press F1 | COM5 (N/A) | DEAD000D 11.433.13.00.964

[illegible]

第 5 页, 共 18 页

```
lte_rrc_csp.c 01746 CSP: Preparing supported bands
lte_rrc_csp.c 01749 CSP: Initing band scan list
lte_rrc_csp.c 01756 CSP: BS last_tried_index = -1
lte_rrc_csp.c 01762 CSP: Band1 supported
lte_rrc_csp.c 01774 CSP: Band3 supported
lte_rrc_csp.c 01798 CSP: Band7 supported
lte_rrc_csp.c 01804 CSP: Band8 supported
lte_rrc_csp.c 01864 CSP: Band20 supported
lte_rrc_csp.c 01942 CSP: There are 5 supported bands
lte_rrc_csp.c 01967 CSP: MRU band present and need to optimize
lte_rrc_csp.c 01978 CSP: Band list optimized
lte_rrc_csp.c 02013 CSP: Band is supported
lte_rrc_csp.c 04367 CSP: Band is supported
lte_rrc_csp.c 02013 CSP: Band is supported
lte_rrc_csp.c 04367 CSP: Band is supported
lte_rrc_csp.c 02013 CSP: Band is supported
lte_rrc_csp.c 04367 CSP: Band is supported
lte_rrc_csp.c 04412 CSP: Found 3 systems to scan
lte_rrc_csp.c 08693 CSP: Starting System Scan on Mode Change Cnf
lte_rrc_csp.c 02109 CSP: Roaming restriction is allow none
lte_rrc_csp.c 02289 CSP: SS req trans ID = 3
lte_rrc_csp.c 02304 CSP: The 3 systems are:
lte_rrc_csp.c 02309 CSP: earfcn= 1250
lte_rrc_csp.c 02309 CSP: earfcn= 50
lte_rrc_csp.c 02309 CSP: earfcn= 6350
lte_rrc_csp.c 02317 CSP: Sent System Scan Request for 3 systems
lte_rrc_csp.c 09753 CSP: Received System Scan Cnf
lte_rrc_csp.c 09768 CSP: System Scan Cnf returned 3 systems
```

图1.7 System Scan log

- 2) Band Scan: 当System Scan中的历史记录频点Acq都失败时, 会进行band scan; 按照单板支持的band, 一般情况下会从Band1开始扫每个Band的频点, 而在每个Band中会将所有频点按照RSSI排序, 将达到信号强度门限值的频点按信号强度从高到低列出来, 最多列出50个频点作为候选频点, 然后在这50个频点中找一个合适的频点, 直到找到一个符合当前网络的频点。可以通过QXDM过滤LTE RRC/CSP的log来查看扫频的过程时, 如图1.8所示; Band Scan扫频时对每个频点Acq log信息参考图1.9;

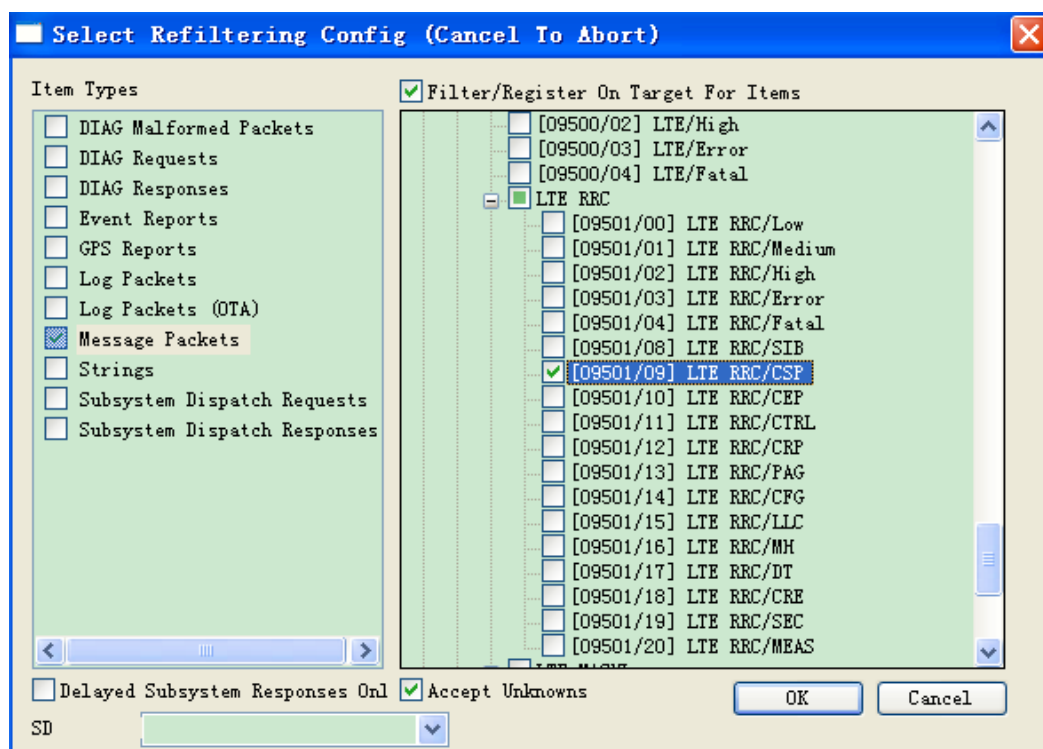


图1.8 LTE搜网log过滤

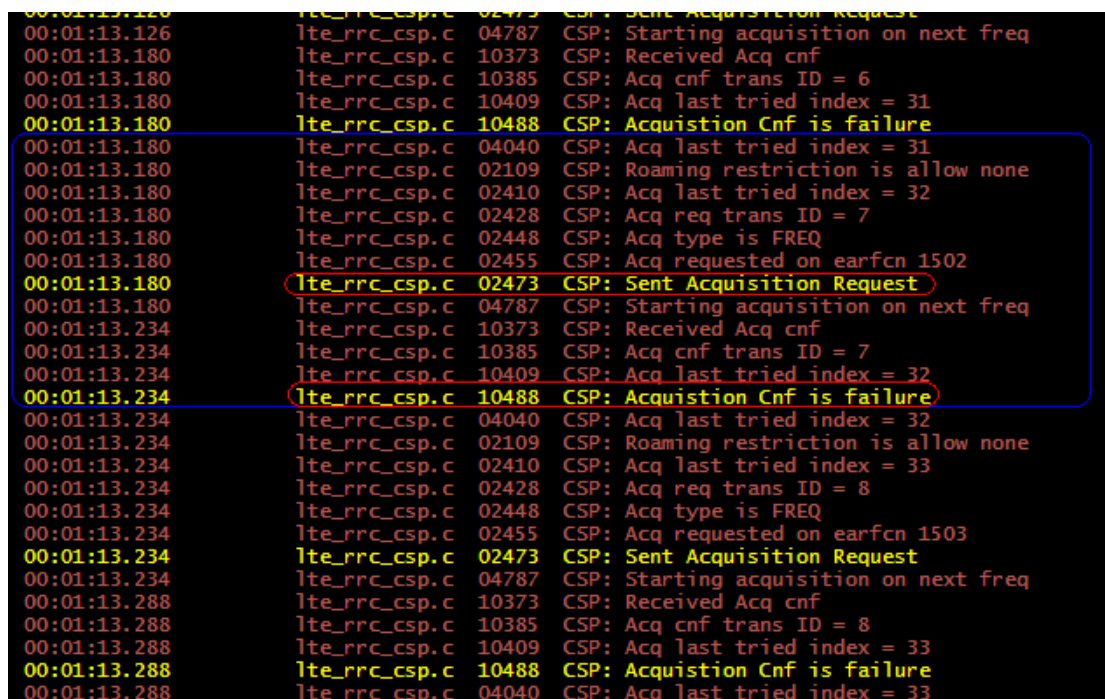


图1.9 LTE Band Scan频点Acq log

1.4 小区搜索

LTE小区搜索实际上就是PSS (Primary Synchronization Signal) / SSS (Secondary

Synchronization Signal)同步，实现UE对小区的识别和下行同步。

这样单板就能收到小区广播的MIB消息和SIB消息。

1.5 解系统消息 (System Information)

系统消息解析主要是去读取MIB (Master Information Block)消息和SIB (System Information Block)消息。系统消息的详细定义可以参考协议3GPP TS 36.331 5.2 System information。系统消息的获取流程如图1.10。

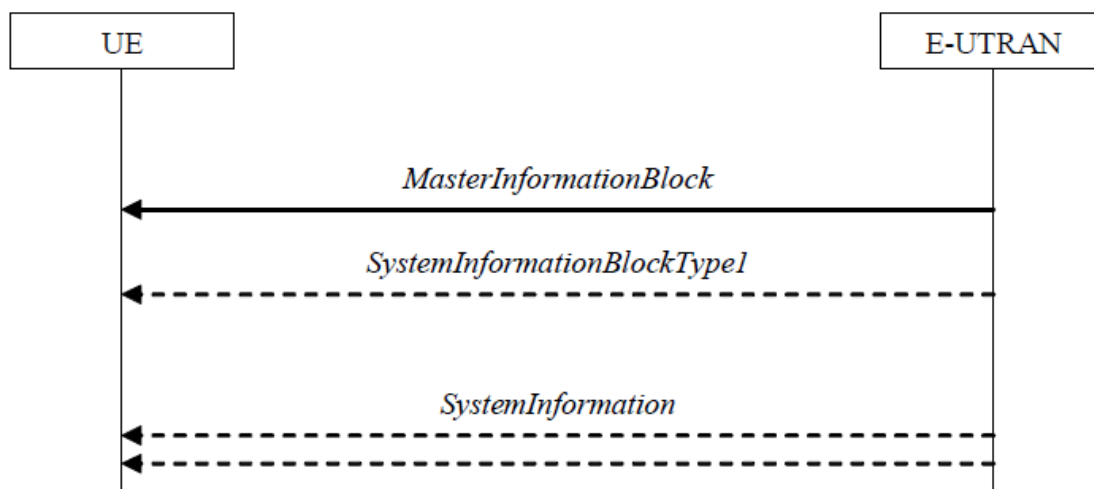


图1.10 System information acquisition, normal

MIB消息包含天线数、下行带宽、小区ID、注册的频点等消息，其格式定义如图1.11。

空口消息解析如图1.12

```
-- ASN1START
MasterInformationBlock ::= SEQUENCE {
    dl-Bandwidth          ENUMERATED {
                           n6, n15, n25, n50, n75, n100},
    phich-Config          PHICH-Config,
    systemFrameNumber     BIT STRING (SIZE (8)),
    spare                 BIT STRING (SIZE (10))
}
-- ASN1STOP
```

图1.11 MasterInformationBlock

```
Day 0 00:00:14.783 [00] 0xB0C1 LTE RRC MIB Message Log Packet
Version = 1
Physical cell ID = 10
FREQ = 1300
SFN = 192
Number of TX Antennas = 2
DL Bandwidth = 20 MHz (100)
```

图1.11 MIB OTA Message

SIB消息会包含PLMN、小区ID、S准则中的 $q-RxLevMin$ （sib3中）等消息，当该PLMN、和第二步得到的PLMN一致时才可以进行下一步；否则扫下一个频点，同时解系统消息会得到S准则中参考信号功率的值和随机接入时PreamblesGroup以及功率攀升因子等消息。

查看MIB、SIB消息可以通过QCAT过滤空口（OTA）消息来获取，请参考图1.12。消息解析可以参考图1.13

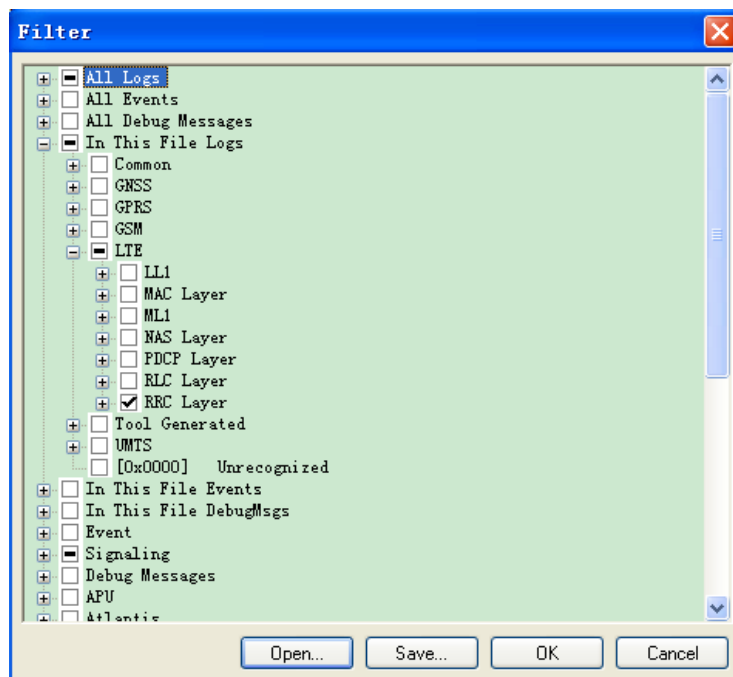


图1.12 MIB/SIB OTA Message Filter

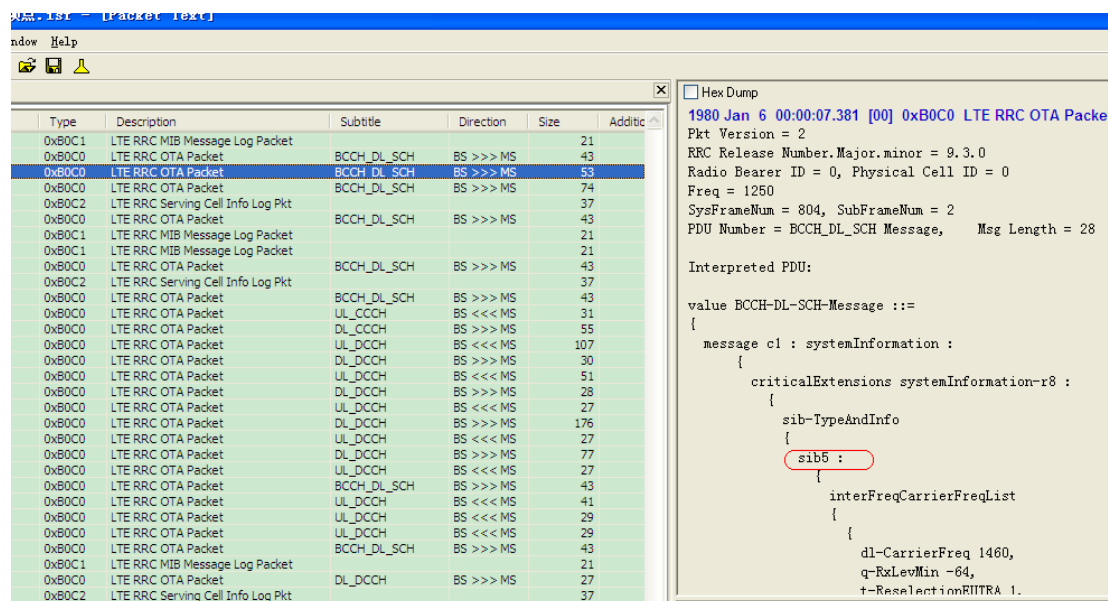


图1.13 MIB/SIB解析

1.6 小区选择

小区选择过程就是S准则的判断，可以参考协议3GPP TS 36.304 5.2 *Cell selection and reselection*和3GPP TS 36.304 5.2.4.6 *Intra-frequency and equal priority inter-frequency Cell Reselection criteria*。LTE的S准则定义为：

$$S_{qual} = Q_{qualmeas} - Q_{qualmin}$$

$$S_{rxlev} = Q_{rxlevmeas} - Q_{rxlevmin} - P_{compensation}$$

其中：

S _{qual}	Cell Selection quality value, (dB) Not applicable for TDD cells or GSM cells.
S _{rxlev}	Cell Selection RX level value (dB)
Q _{qualmeas}	Measured cell quality value. The quality of the received signal expressed in CPICH E _c /N ₀ (dB) for FDD cells. Not applicable for TDD cells or GSM cells.
Q _{rxlevmeas}	Measured cell RX level value. This is received signal, CPICH RSCP for FDD cells (dBm), P-CCPCH RSCP for TDD cells (dBm) and RXLEV for GSM cells (dBm).
Q _{qualmin}	Minimum required quality level in the cell (dB). Not applicable for TDD cells or GSM cells.
Q _{rxlevmin}	Minimum required RX level in the cell. (dBm)
P _{compensation}	Max(UE_TXPWR_MAX_RACH – P_MAX, 0) (dB)
UE_TXPWR_MAX_RACH	Maximum TX power level an UE may use when accessing the cell on RACH (read in system information), (dBm)
P_MAX	Maximum RF output power of the UE, (dBm)

当Acq频点满足UE要求的信号强度时，继续下一步小区驻留；不满足时扫下一个频点。

1.7 小区驻留（Camped on the Cell）：

扫到的一个频点满足S准则，小区选择成功后进行小区驻留。小区驻留log参考图1.14。

```

LTE RRC/CSF      00:00:13.516      lte_rrc_csf.c  09191  CSF: Camped after cell selection
LTE RRC/CSF      00:00:13.516      lte_rrc_csf.c  09244  CSF: Camped on physical cell ID 0 on earfcn 1250 小区驻留成功
LTE RRC/CSF      00:00:13.516      lte_rrc_csf.c  02717  CSF: Sent RRC Camped Ind
LTE RRC/CSF      00:00:13.516      lte_rrc_csf.c  02797  CSF: SIB8 Available = 0
LTE RRC/CSF      00:00:13.516      lte_rrc_csf.c  02800  CSF: T311 rem time = 0 ms
LTE RRC/High/CSF 00:00:13.516      lte_rrc_csf.c  02816  CSF: TDD pruning is required
LTE RRC/High/CSF 00:00:13.516      lte_rrc_csf.c  02838  CSF: Sending NAS Service Ind
LTE RRC/High/CTRL 00:00:13.516      lte_rrc_controller.c 03319  RRCC: Received camped indi
  
```

图1.14 Cell Camped log

1.8 Attach request

当驻留到小区后，UE要注册到网络就要发起Attach request。

1.9 RRC CONNECTION Request

发起Attach Request请求后，若要传输信令就要建立RRC连接，所以发起RRC连接请求。

1.10 随机接入

RRC连接要建立，就要进行上行同步，也就是随机接入，随机接入过程参考协议3GPP TS 36.300 10.1.5 Random Access Procedure。随机接入流程可以参考图1.15。随机接入流程的OTA消息可以通过QCAT: Filter --> In This File Logs --> LTE --> ML1过滤，如图1.16。相关log信息可以参考图1.17。

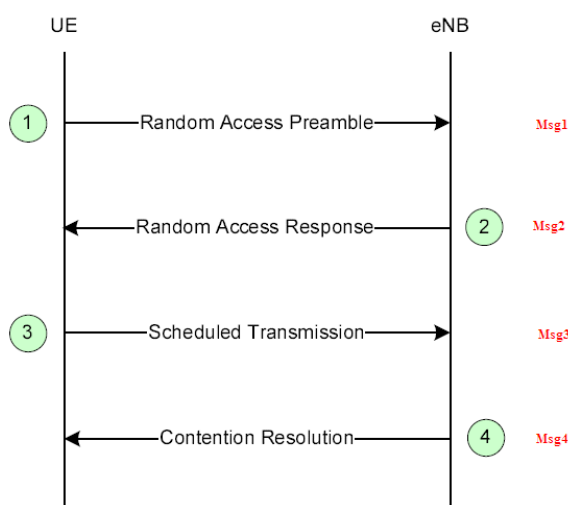


图1.15 Contention based Random Access Procedure

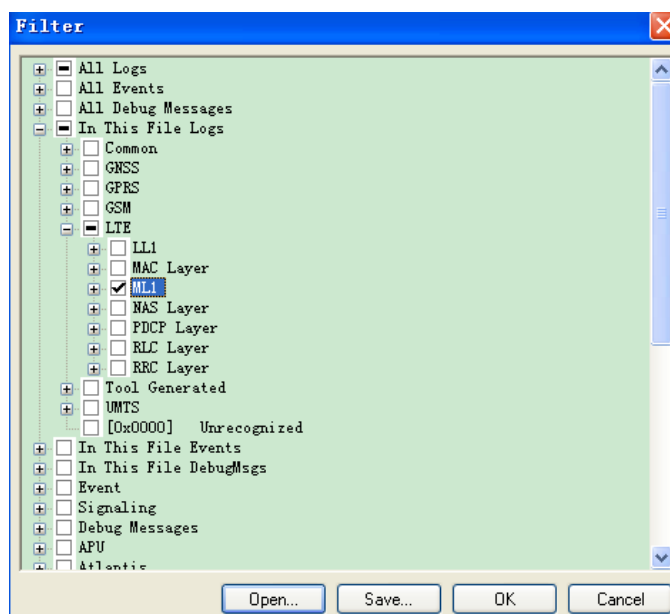


图1.16 RAP OTA messages Filter

Type	Description	S...	D...	Size	Ad...
0xB17D	LTE M1 Idle Measurement Request			76	
0xB187	LTE M1 Idle IRAT Measurement Request			76	
0xB1A7	Reserved			308	
0xB1A7	Reserved			308	
0xB1A7	Reserved			308	
0xB1A7	Reserved			308	
0xB167	LTE Random Access Request (MSG1) Report			40	
0xB168	LTE Random Access Response (MSG2) Report			24	
0xB1A7	Reserved			308	
0xB1A7	Reserved			308	
0xB1A7	Reserved			308	
0xB169	LTE UE Identification Message (MSG3) Report			24	
0xB1A7	Reserved			308	
0xB16A	LTE Contention Resolution Message (MSG4) Report			20	
0xB1A7	Reserved			308	
0xB161	LTE Downlink Dedicated Configuration			32	
0xB163	LTE Uplink Dedicated Configuration			36	
0xB165	LTE Grant Manager Dedicated Configuration			72	
0xB1A7	Reserved			308	
0xB1A7	Reserved			308	
0xB178	Reserved			308	
0xB1A7	Reserved			308	
0xB1A7	Reserved			308	
0xB1A7	Reserved			308	
0xB1A7	Reserved			308	

☐ Hex Dump
1980 Jan 6 00:00:13.689 [00] 0xB167 LTE Random Access Request (MSG1) Report
Version = 5
Preamble Sequence = 15
Physical Root Index = 178
Cyclic Shift = 225
PRACH Tx Power = -7 dBm
Beta PRACH = 242
PRACH Frequency Offset = 6
Preamble Format = 0
Duplex Mode = FDD
Density Per 10 ms = 6
PRACH Timing SFN = 411
PRACH Timing Sub-fn = 4
PRACH Window Start SFN = 411
PRACH Window Start Sub-fn = 7
PRACH Window End SFN = 412
PRACH Window End Sub-fn = 7
RA RNTI = 5
PRACH Actual Tx Power = -7

图1.17 RAP OTA messages

随机接入分为竞争和非竞争两种：

1) 基于竞争的随机接入的场景有：①从RRC_IDLE状态接入②无线链路失败发起的接入③UE处于RRC_CONNECTED时有上行数据要发送；

2) 基于非竞争的随机接入场景有：①切换过程的随机接入②UE处于RRC_CONNECTED时有下行数据到达

1.11 RRC 连接建立

1.12 Attach accept / Attach complete

2 搜网相关 AT 命令

2.1 AT+COPS 命令

用于设置网络选择模式，网络运营商名字显示格式，接入技术以及查询当前运营商信息列表等。

具体可以参考协议3GPP TS 27.007 AT command set for User Equipment (UE) 7.3 PLMN selection +COPS。AT+COPS parameter command syntax定义如图2.1。

Command	Possible response(s)
+COPS=[<mode>[,<format>[,<oper>[,<AcT>]]]]	+CMEERROR: <err>
+COPS?	+COPS: <mode>[,<format>,<oper>[,<AcT>]] +CME ERROR: <err>
+COPS=?	+COPS: [list of supported (<stat>, long alphanumeric <oper> , short alphanumeric <oper>, numeric <oper>[, <AcT>]) s] [, , (list of supported <mode>s), (list of supported <format>s)] +CME ERROR: <err>

图2.1 AT+COPS parameter command syntax

2.2 扩展系统配置参考设置命令 AT^syscfgex 命令

该命令是华为自己添加的，可以实现设置网络接入次序、频带、漫游支持和domain等特性。以通过该命令更改接入顺序，如对于该命令的第一个参数<acqorder>，设置为”020103”就可以实现先WCDMA然后GSM再是LTE。

具体可以参考《HUAWEI 终端设备AT命令接口规范(GSM&WCDMA&TD-SCDMA分册)V1.3.7》文档。语法结构如图2.2。

Command	Possible response(s)
^SYSCFGEX=<acqorder>,<band>,<roam>,<srvdomain>,<lteband>,<reserve1>,<reserve2>	<CR><LF>OK<CR><LF>
^SYSCFGEX?	<CR><LF>^SYSCFGEX: <acqorder>,<band>,<roam>,<srvdomain>,<lteband><CR><LF><CR><LF>OK<CR><LF>
^SYSCFGEX=?	^SYSCFGEX:(list of supported < acqorder >s), (list of supported(<band >,<band_name>)s), (list of supported < roam >s), (list of supported < srvdomain >s), (list of supported(<lteband >,<lteband_name>)s), <CR><LF><CR><LF>OK<CR><LF>

图2.2 AT^syscfgex 语法结构

3 UE LTE 网络入网 log 抓取与查看

3.1 LTE 入网 log 抓取

使用QXDM抓取入网log，由于单板在上电之后就会搜网，而我们设置QXDM的端口时需要先在设备管理器中查看是哪个端口，所以可能抓不到完整的log。

因此我们可以通过以下方法抓取完整的log。

方法1：对单板设置使能pin码。设置后我们可以先连接好QXDM的端口，然后输入pin码，如图3.1。

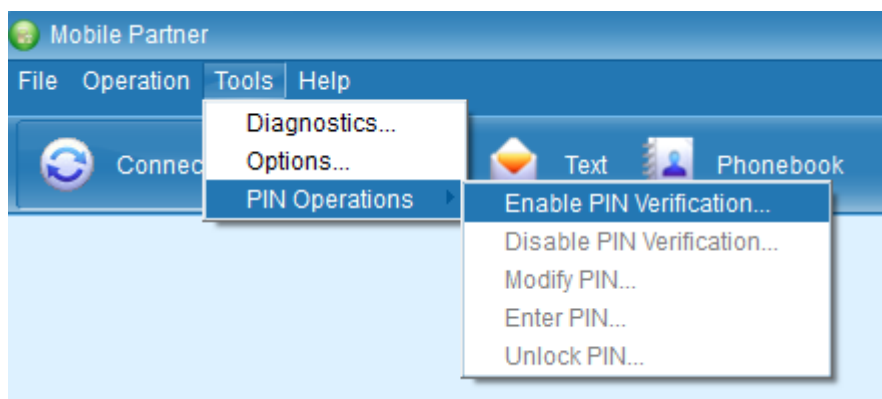


图3.1 PIN码使能

方法2：插上单板，连上QXDM，通过菜单“Options->Set Target Offline”，设置单板为Offline模式，再通过“Options->Reset Target”使单板重启。

单板会自动重启，重启完成之后QXDM会自动连上，这时也能抓取搜网初始化的Log，如图3.2。

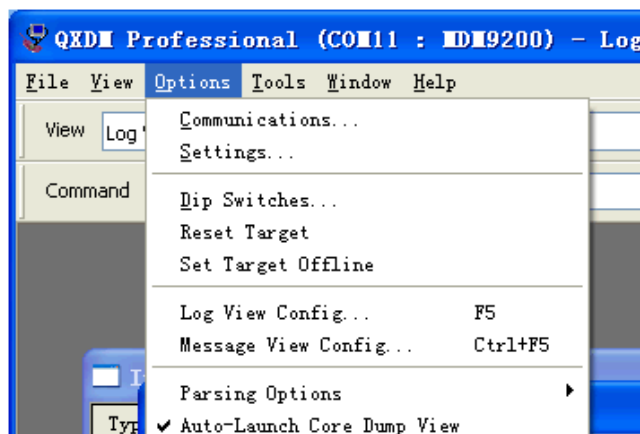


图3.2 Reset Target

注意：这种方式会保存历史频点，而直接拔掉单板是不会保存历史频点的。历史频点保存的条件是当前注册上LTE网络，然后进行网络模式的切换，或者通过QXDM进行offline和reset。

3.2 UE 入网 log 查看

使用QXDM抓log时，为保证抓取全面的信息，可以将log view和message view全部勾选。分析log时可以先使用QCAT查看空口消息（OTA Message），log过滤方法为QCAT: Filter --> In This File Logs --> LTE --> NAS Layer和RRC Layer，如下图3.1。

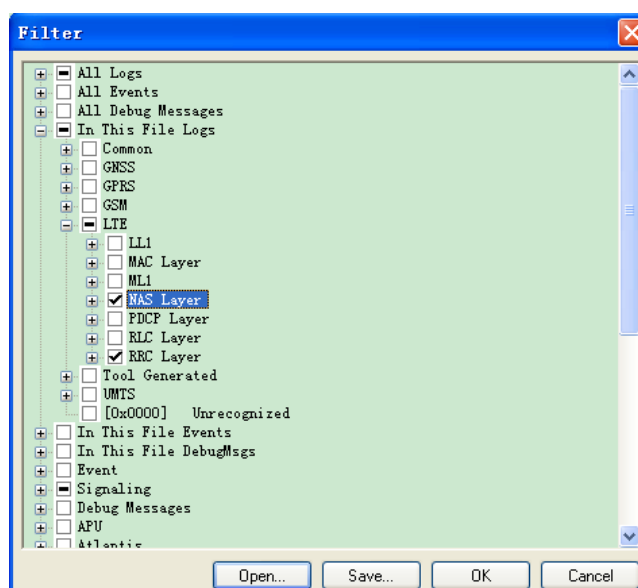


图3.1 OTA Message Filter

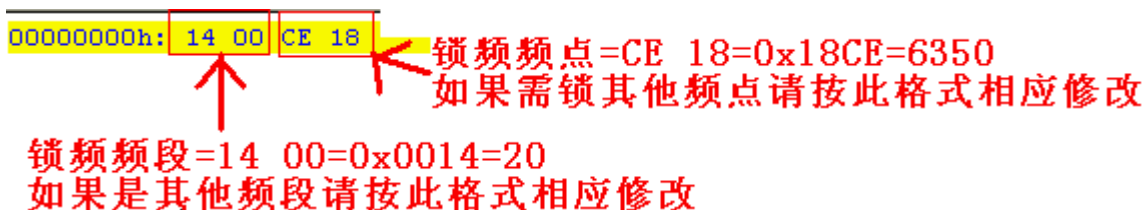
通过Filter之后的log逐步定位问题，入网流程越往后走，我们定位问题越容易；而例如扫频等问题定位，高通不会向我们公开他们的算法，如果那出问题，我们只能推动高通解决。

4 LTE 的锁频方法

可以通过QPST对单板在LTE网络下锁频，从而使单板只会注册到特定频点。LTE的锁频方法如下：

1、在nv/item_files/modem/lte/ML1目录下添加命名为camp_band_earfcn的文件，如果不存在ML1文件夹路径，则在nv/item_files/modem/lte目录下创建ML1文件夹；

2、camp_band_earfcn文件格式如图4.1。



锁频频点=CE 18=0x18CE=6350
如果需锁其他频点请按此格式相应修改

锁频频段=14 00=0x0014=20
如果是其他频段请按此格式相应修改

图4.1 camp_band_earfcn文件格式

3、按照上图格式修改相应的频点信息和band信息（请勿删除空格或增加空格）

5 QCN 的备份与导入

不同的单板总有一些差异，我们通过NV进行校准。我们经常通过互相导QCN来排除是否是NV项的原因。

1、QCN的备份，如图5.1。选择QPST software，选择UE端口（application口），选择Backup，然后选择好路径备份。

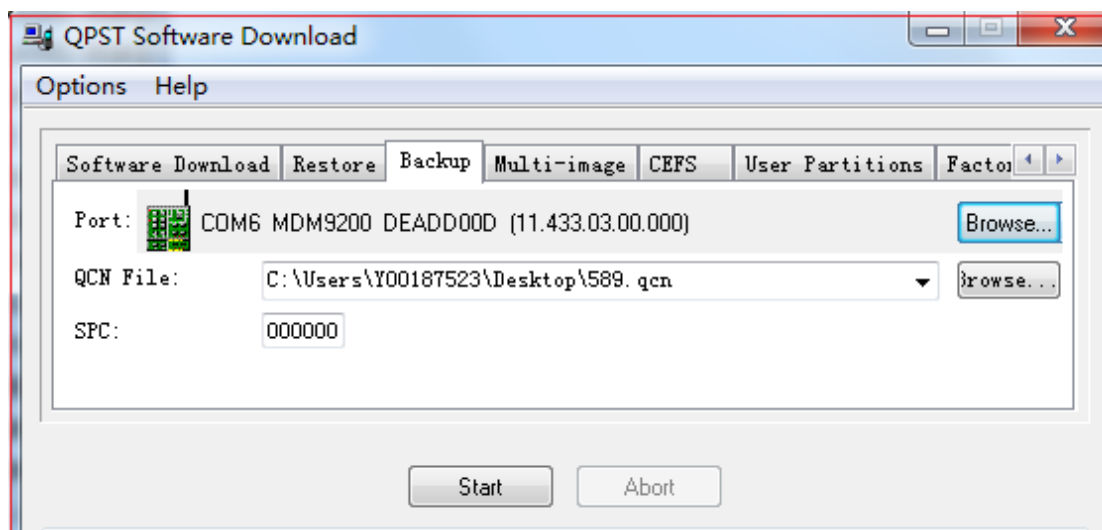


图5.1 NV备份

2、QCN的导入，如图5.2，选择Restore，在QCN File里选择要导入的QCN。

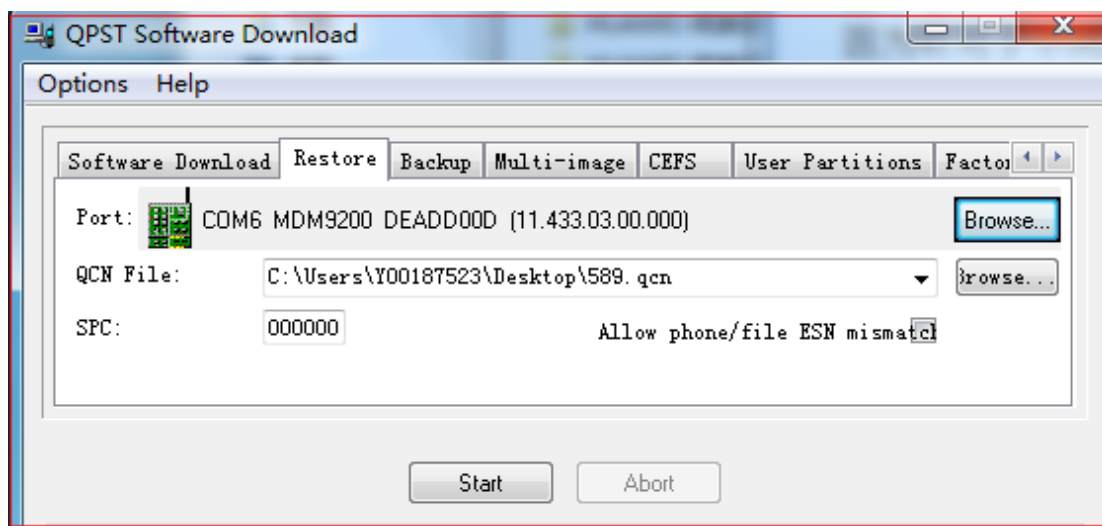


图5.2 NV导入

6 参考资料

- [1]. 3GPP TS 31.102 Characteristics of the Universal Subscriber Identity Module (USIM) application
- [2]. 3GPP TS 23.122 Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode
- [3]. 3GPP TS 24.301 Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)
- [4]. 3GPP TS 31.102 Characteristics of the Universal Subscriber Identity Module (USIM) application
- [5]. 3GPP TS 36.213 Physical layer procedures
- [6]. 3GPP TS 36.300 Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN)
- [7]. 3GPP TS 36.304 User Equipment (UE) procedures in idle mode
- [8]. 3GPP TS 36.307 Requirements on User Equipments (UEs) supporting a release-independent frequency band
- [9]. 3GPP TS 36.322 Radio Link Control (RLC) protocol specification
- [10]. 3GPP TS 36.331 Radio Resource Control (RRC); Protocol specification
- [11]. HUAWEI 终端设备 AT 命令接口规范(GSM&WCDMA&TD-SCDMA 分册)V1.3.7