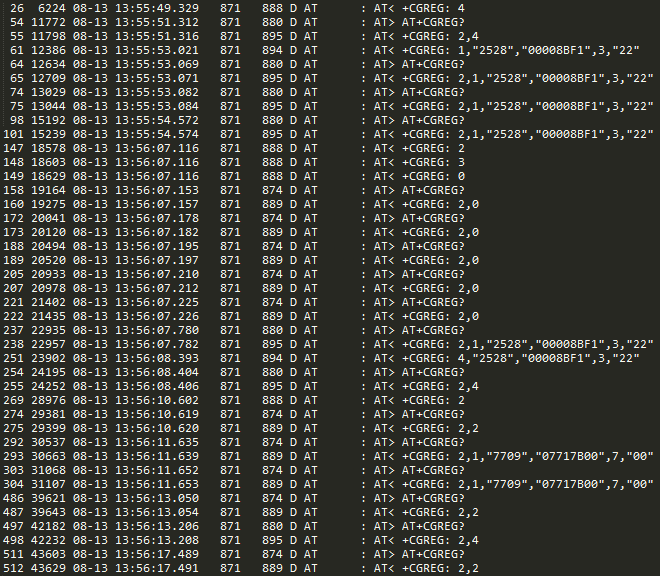
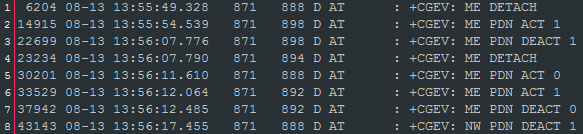
## 〇、AT CMD

### 1、AT+CGREG：GPRS网络注册状态

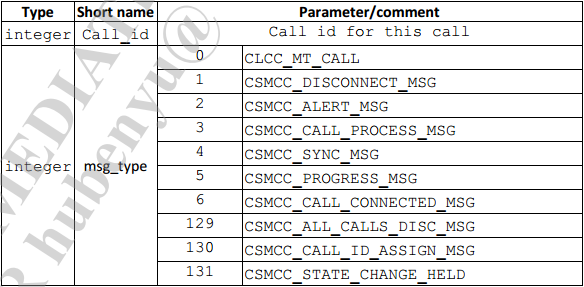
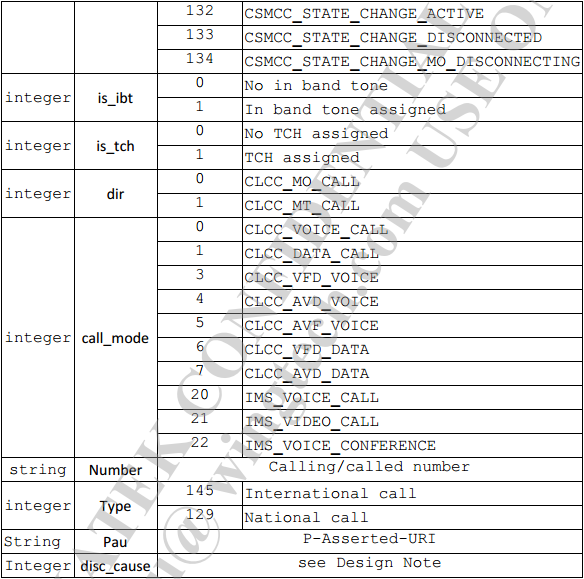


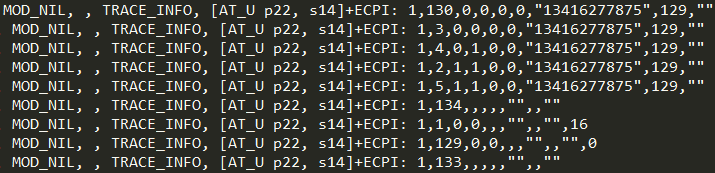
### 2、+CGEV：



### 3、ECPI：呼叫进程信息

命令参数：





呼叫信令流程：

1）①1为call\_id；②130表示call\_id的分配消息；④0表示TCH未分配；⑤0表示移动主叫；⑥0表示语音通话；⑦呼叫的电话号码；⑧129表示国内通话。

2）②3表示call process呼叫处理。

3）②4表示正在同步。④1表示TCH已经分配。

4）②2表示开始振铃。

5）②5表示progress，呼叫正在进行。

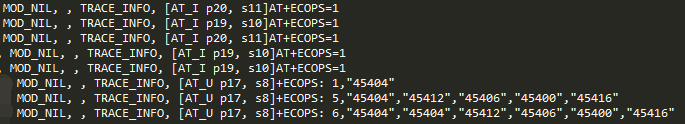
6）②134表示主叫端挂掉电话。

7）②1表示正在disconnect断开连接。

8）②129表示断开所有通话连接。

9）②133表示通话状态改变为未连接。

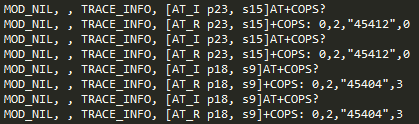
### 4、ECOPS：控制modem是否上报PLMN list



1）AT+ECOPS=1：开启上报。

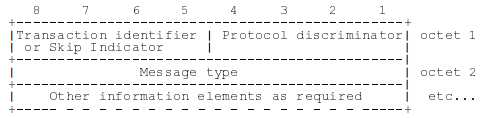
2）+ECOPS：1，“45404”：扫描到的PLMN的数量以及PLMN list。

**5、COPS：运营商选择**

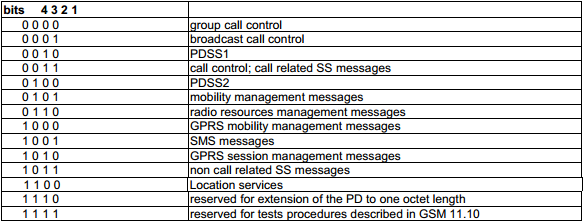


## 一、L3空口消息

### 0.标准L3信息结构：



**（1）protocol discriminator：协议鉴别符**

****

**（2）transaction identifier or skip indicator：事务标示或忽略指示**

每个RR层、MM层和GPRS移动管理层的消息都包含skip indicator，skip indicator如果不为0000则表示该消息应该被忽略；如果是0000则不能忽略。

CC层、呼叫相关的SS层和会话管理（Session Management）都包含transaction identifier（TI）。

**（3）message type：消息类型**

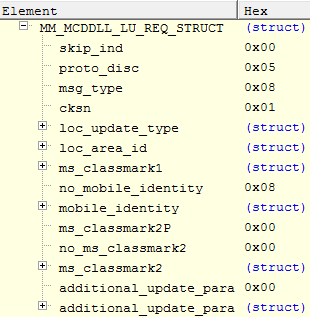
10.4/GSM 0408。

**（4）其他元素信息：根据消息的不同**

### 1.位置更新、鉴权：



（1）MS向NW发送位置更新请求：LOCATION\_UPDATING\_REQUEST



①Skip Indicator

②Protocol discriminator

③Request message type

④Ciphering key sequence number

⑤Location updating type

⑥Location area identification

⑦Mobile station classmark

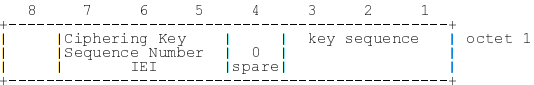
⑧Mobile identity

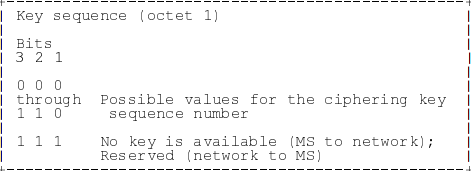
①、②、③的内容见0.标准L3信息结构。

④密钥（kc）序列号。可以用来标识MS中的kc，以此略过鉴权流程。它由NW生成，并通过AUTHENTICATION\_REQUEST消息发送给MS，跟kc存储在一起。

消息元素内容：

消息元素格式：



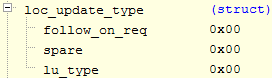


key sequence的值：0~6即所有序列号的可能取值；7的时候，MS到NW表示无key sequence可用，NW到MS作为保留位。

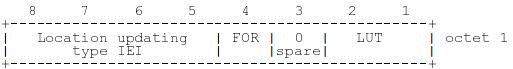
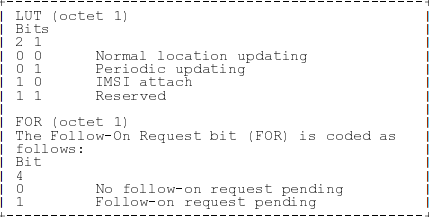
（CKSN和kc是一一对应的，如果MS的第一条层三消息SABM帧里面的CKSN和网络端的CKSN一致，则认为不用进行鉴权过程，直接进行加密过程，若不一致则要经过鉴权过程，才能进行加密过程。）

⑤位置更新类型。用来指示是普通位置更新、周期性（periodic）位置更新还是IMSI附着。

消息元素内容：

 普通位置更新

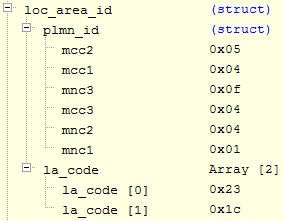
no follow-on

消息元素格式：

bit 4的follow-on request表示是否要维持RR连接，以初始化后续的MM连接。

⑥位置区标识。

消息元素内容：



LAI

MCC

MNC

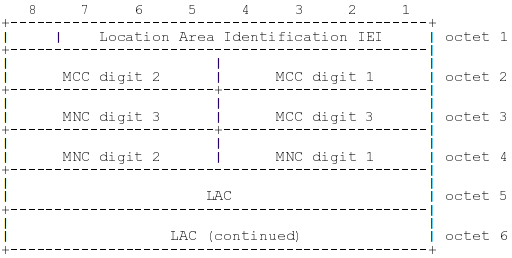
LAC

消息元素格式：

MCC：Mobile country code。当MCC包含除数字外的字符，则要以16进制的形式发送给NW，NW将其视为清除的状态。

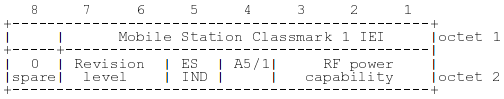
MNC：Mobile network code。MNC3置为“1111”表示只用MNC2和MNC1两个数字，可能导致MS无法注册到广播信息中包含MNC3的NW。

LAC：Location area code。一共16bit。清除LAC的时候最低bit置0，其他bit置1。

⑦MS类别标记。标识了MS的设备相关信息。

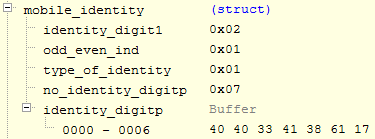
消息元素格式：

包括A5加密算法是否可用（1为不可用），RF射频等级。



⑧移动身份标识。包括IMSI（少于15位数字）、TMSI、P-TMSI（32位数字）、IMEI（15位数字）、IMEISV（16位数字）等。

消息元素内容：



移动身份标识的选择优先级的规则是（优先使用前者，不可用再使用后者）：

* 分组寻呼：P-TMSI→IMSI。
* 移动被叫：使用与PAGING\_REQUEST消息中类型相同的移动身份标识。
* 紧急呼叫建立和重建立：TMSI→IMSI→IMEI（前两者均不可用或SIM卡不可用）。
* 身份鉴别和GMM身份鉴别：根据NW的请求确定。
* 加密、GMM鉴权加密：IMEISV。
* 其他情况：TMSI→IMSI。

消息元素格式：

