**4G VPDN业务中终端不能上传账号的问题分析**

**中国电信云南公司省NOC交换核心网团队 陈江**

**案例摘要：**

VPDN业务开通和测试过程中发现：有的终端，在绑定内网（即只有VPDN业务，没有开通INTERNET）的时候，附着时没有携带必要参数User-Name信息，导致AAA认证失败，整个附着流程无法继续进行。经过多次测试和分析确定为终端问题，需要终端进行升级改造解决，并提供参考建议。

**关键词：**

4G VPDN 附着 User-Name PGW 参数

# 问题描述

在VPDN业务开通和测试过程中发现：有的终端，在绑定内网（即只有VPDN业务，没有开通INTERNET）的时候，附着时没有携带必要参数User-Name信息，导致AAA认证失败，整个附着流程无法继续进行。

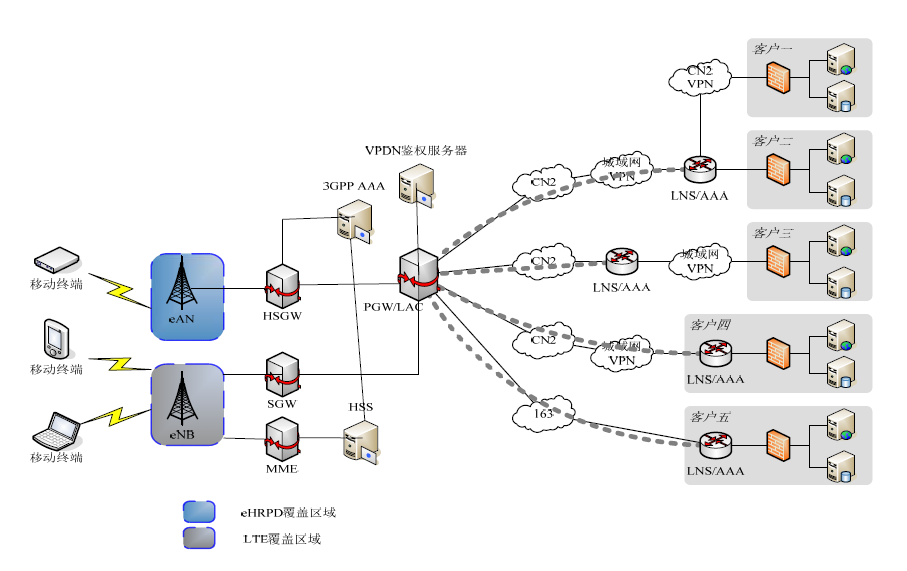
# 问题分析

## VPDN业务介绍

根据集团规范，以及现场实际情况，我省采用了L2tp隧道的VPDN方式。

## 网络架构

4G网络基于L2tp隧道的VPDN业务网络架构图



## 涉及的4G核心网网元

4G核心网在VPDN业务中，主要涉及网元及对应角色如下：

|  |  |  |
| --- | --- | --- |
| 网元 | VPDN业务角色 | 功能 |
| MME/HSGW/SGW |  | 网络接入 |
| PGW | LAC | 隧道、会话建立起点 |
| HSS/3GPP AAA | VPDN用户模板 | 4G用户鉴权 |

## VPDN业务流程

无论是LTE接入还是EHRPD接入，都是终端通过无线将附着请求发送到核心网，通过PGW触发VPDN隧道/会话的建立。

当PGW收到VPDN用户的附着请求时，会向AAA服务器发送一次认证请求，认证请求通过，AAA会向PGW返回相关信息。

PGW在收到必要的参数后，将会向LNS发起隧道/会话的建立请求，LNS将相关信息发给LNS AAA认证，通过后，再进行一系列的LCP协商、PAP/CHAP协商、IPCP协商，协商通过，就可以发起计费请求与回应。

至此，整个流程结束，可以进行VPDN业务。

集团公司VPDN规范规定PGW向AAA请求Access-Request时需携带信息：

|  |  |  |
| --- | --- | --- |
| 参数 | 选项 | 备注 |
| **User-Name** | **M** | **PGW从终端附着是PCO消息中获取** |
| User-Password | O | PGW从终端附着是PCO消息中获取 |
| CHAP-Password | O | PGW从终端附着是PCO消息中获取 |
| NAS-IP-Address | Oc | PGW RADIUS Client IP地址 |
| **Called-Station-Id** | **M** | **填充为APN** |
| Calling- Station-Id | Oc | 填充为MSISDN |
| CHAP-Challenge | Oc | PGW从终端附着是PCO消息中获取 |
| IMSI | O | 填充为IMSI |

其中**M**为必选参数

AAA向PGW返回Access-Accept时需携带信息：

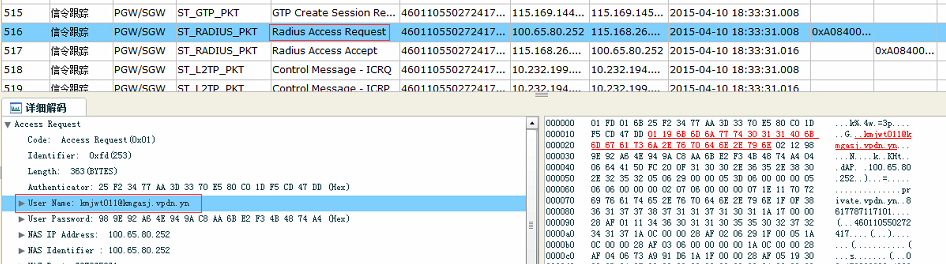
|  |  |  |
| --- | --- | --- |
| 参数 | 选项 | 备注 |
| User-Name | O |  |
| Tunnel-Type | Oc | 集团定义为3 |
| Tunnel-Medium-Type | Oc | 集团定义为1：IPV4 |
| Tunnel-Server-Endpoint | Oc | LNS IP地址 |
| Tunnel-Password | Oc | LNS和LAC之间密码 |
| Tunnel-Private-Group-ID | O |  |
| Tunnel-Assignment-ID | Oc |  |
| Tunnel-Preference | O |  |
| Tunnel-Client-Auth-ID | O |  |
| Tunnel-Server-Auth-ID | O |  |

# 问题排查

## 正常终端附着时信令情况

### 正常终端在发起VPDN业务的必带参数：

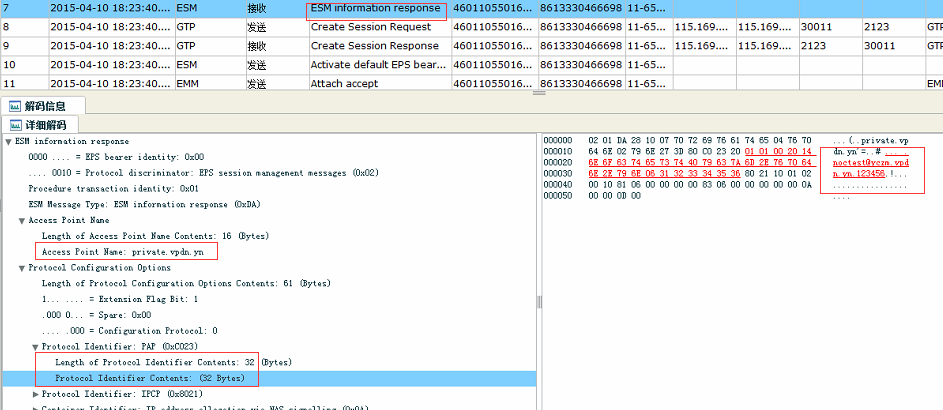
正常附着时，可以看到主要参数：PGW->AAA Radius Access Request消息中User Name字段是有具体参数值。



相关参数是从终端上报的PCO消息中提取的。

### 情况1:附着前终端就已经选择了VPDN的APN：

附着前终端就已经选择了VPDN的APN时（即在开机/关闭飞行模式前已经选好了APN），在终端上报给MME的信令ESM information response中携带正确的APN，PCO字段中携带正确的账号、密码。见下图：



### 情况2：终端附着前选择了外网的APN时

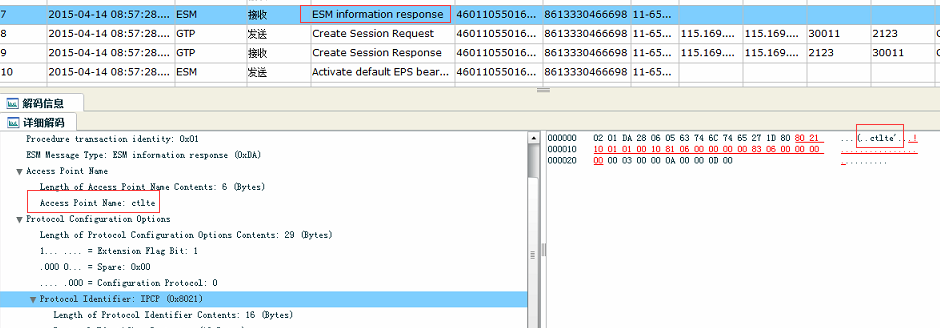
终端附着前选择了外网的APN时（即在开机/关闭飞行模式前已经选好了APN），在终端上报给MME的信令ESM information response中携带的是外网的APN，外网附着通过；切换到VPDN时，终端会发起去附着请求，然后再发起一个VPDN的附着请求。

整体流程图，外网附着完成，去附着，VPDN附着完成：

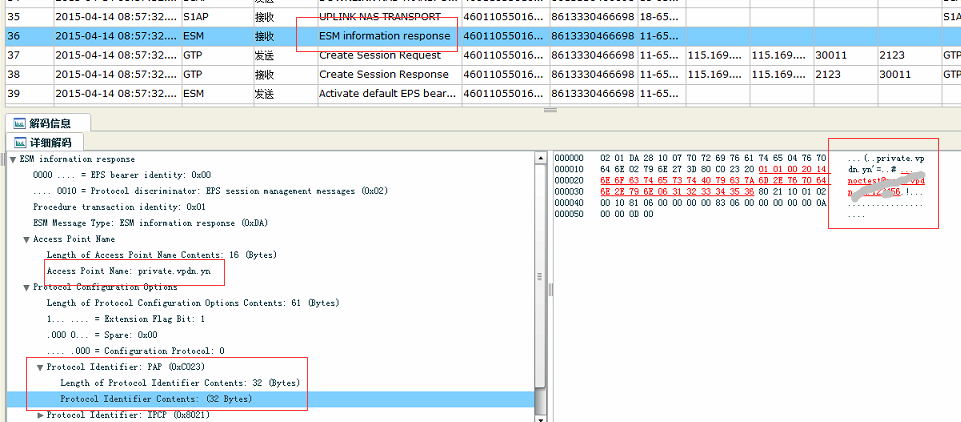




第一次附着的是外网，在ESM information response信令中只携带外网APN，无其它参数



第二次附着是VPDN，在ESM information response信令中携带正确的APN，账号、密码等参数

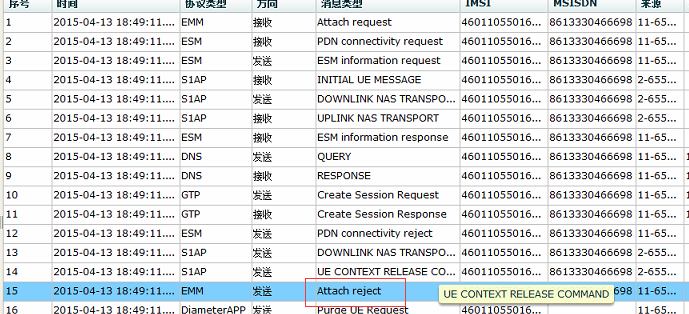


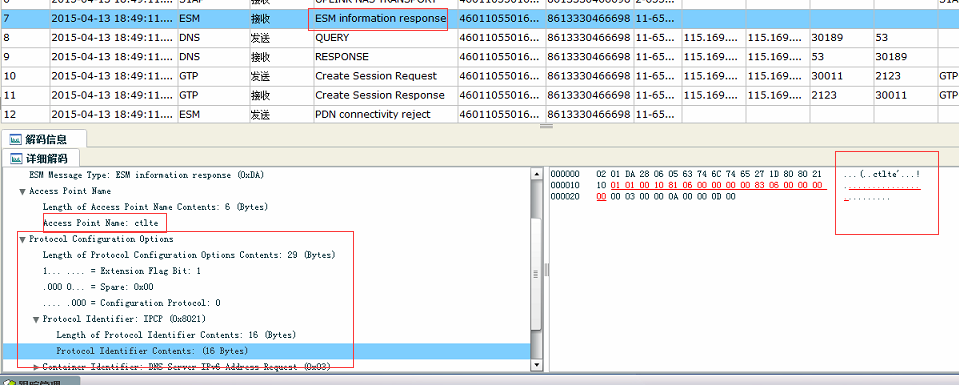
### 正常终端绑定内网的情况

前文提过，按照集团规范定义必带参数是：账号（在User Nmae字段携带），APN，两个参数。

正常终端附着前已经选择VPDN的APN时，附着流程与[章节3.1.2](#_附着前就已经选择了VPDN的APN时)相同，此时终端能够正常使用VPDN。

如果正常终端当附着前选择的是外网APN时，由于终端携带的参数都不正确，此时附着会被拒绝，用户也不能正常使用VPDN。

正常终端绑定内网选择外网APN时，附着也不成功，如下图所示：



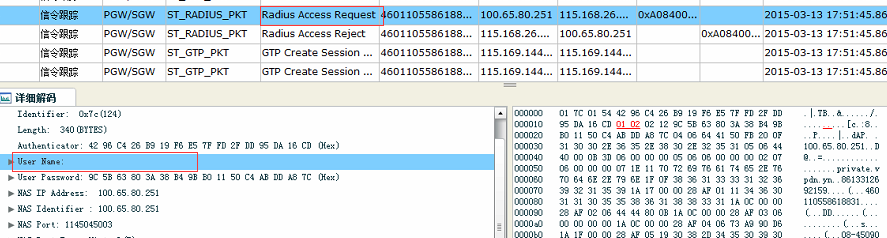
可以看到选择外网ANP时，终端携带的是外网APN，PCO字段中不携带任何账号、密码等信息。

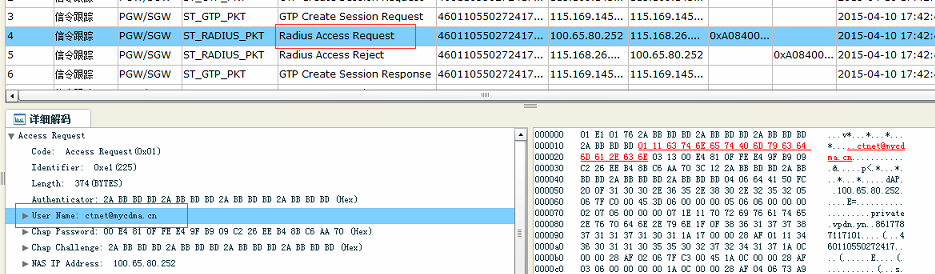
## 异常终端附着时信令

测试中发现，很多终端，操作界面看到选择了VPDN的APN，但是信令中看到其实终端没有使用选定的APN上报信息，而使用了一些如ctlte、ctnet。

### 异常终端发起VPDN业务时的参数情况

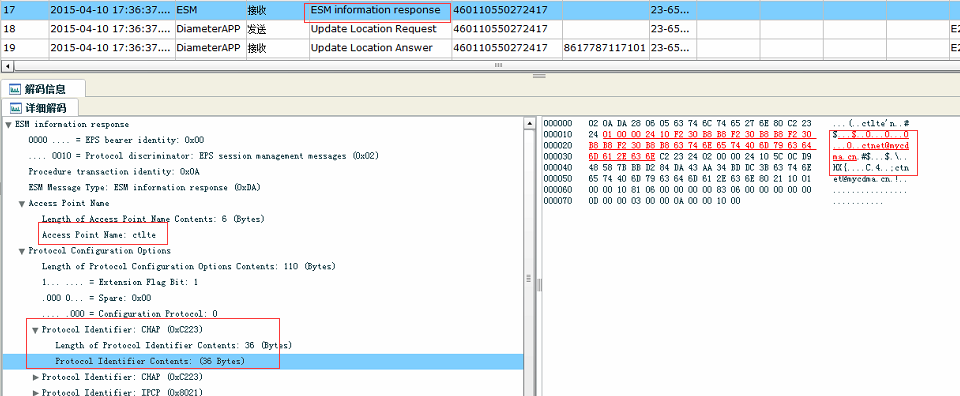
异常终端附着情况，主要参数：PGW->AAA Radius Access Request消息中User Name字段没有值，或者带错误的值，如下图所示：





### 异常终端携带信息情况

携带错误的APN和错误的账号、或密码：



### 部分异常终端在不绑定内网时可以使用VPDN情况

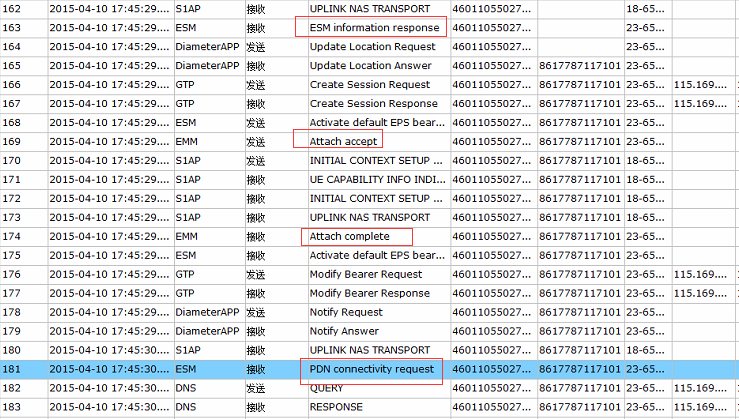
1. 附着前选择的是外网APN

此类终端，在附着前选择的是外网APN（即在开机/关闭飞行模式前已经选好了APN），其过程与正常终端流程相同，见[章节3.1.3](#_附着前选择了外网的APN时)。虽然终端携带上来的错误的/多余的信息，但是，附着外网时，并不需要到AAA认证，也不检测那些信息，所以外网能够正常附着。当从外网APN切换到VPDN的时候，终端可能不会成功，因为终端携带的APN名称不对；但反复重启，有可能会携带正确APN，从而附着成功。

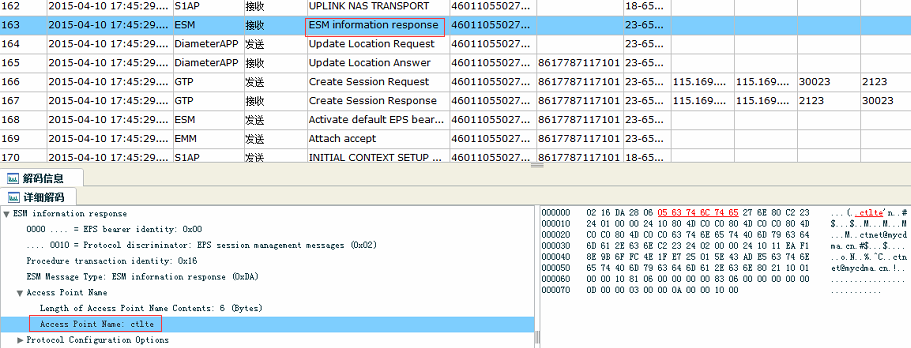
1. 附着前选择的是VPDN的APN

此类终端，在附着前选择了VPDN的APN时（即在开机/关闭飞行模式前已经选好了APN），实际上终端上报给MME的信令ESM information response中携带的还是外网的APN，外网附着通过。此时终端还会主动发起一个新的PDN连接请求，在信令PDN connetctivity request中会携带正确的APN，PCO字段中携带正确的账号、密码。

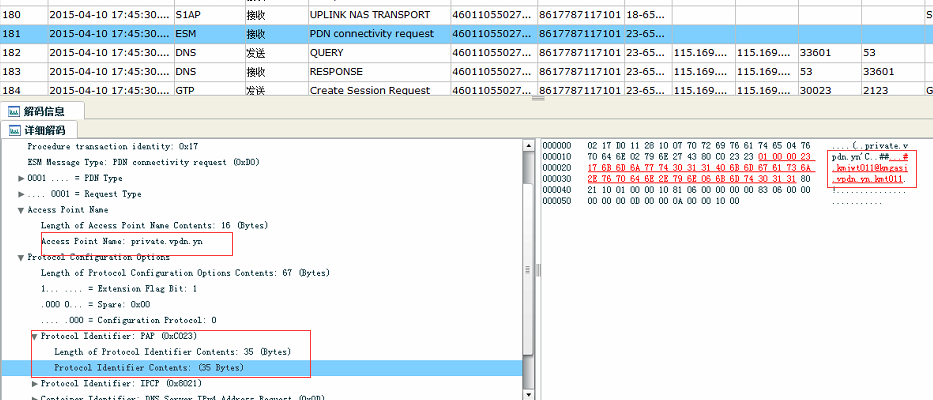
整个流程见下图所示：



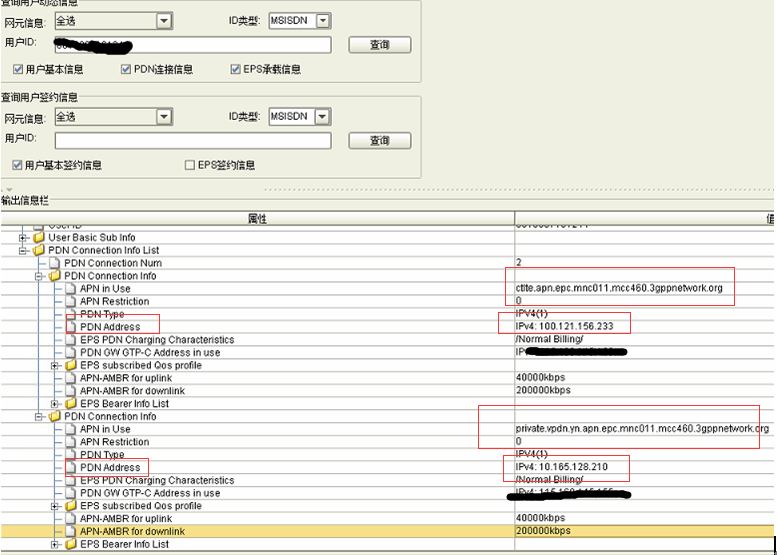
可见初始附着携带的也是外网APN，如下图所示：



而新建PDN连接携带了VPDN正确的参数信息，如下图示：



此时终端可能占有两个ip地址的，一个是外网的ip地址，一个是内网的ip地址



### 测试情况汇总

异常终端有可能出现以下几种状况，不论那种情况，最终都是携带的账号信息有误导致附着失败：

1. 不管是否绑定内网都不能成功附着。此种终端就是无论如何设置都不能携带账号信息。
2. 不绑定内网可以成功附着。此种终端是上报信息是混乱的，常见为没有以选定APN来附着，或者选的APN是外网的，但是会带VPDN的参数。
3. LTE网络下能够成功，eHRPD网络不能成功。

# 问题处理及建议

## 采用GRE方式

如果采用GRE隧道方式，不需要账号信息。就不存在上述问题，但安全性没有L2tp方式高。

按照电信集团规范，我省内VPDN搭建时，企业既有3G、又有4G，就必须选用L2tp的方式，不能使用GRE方式。

## 终端升级

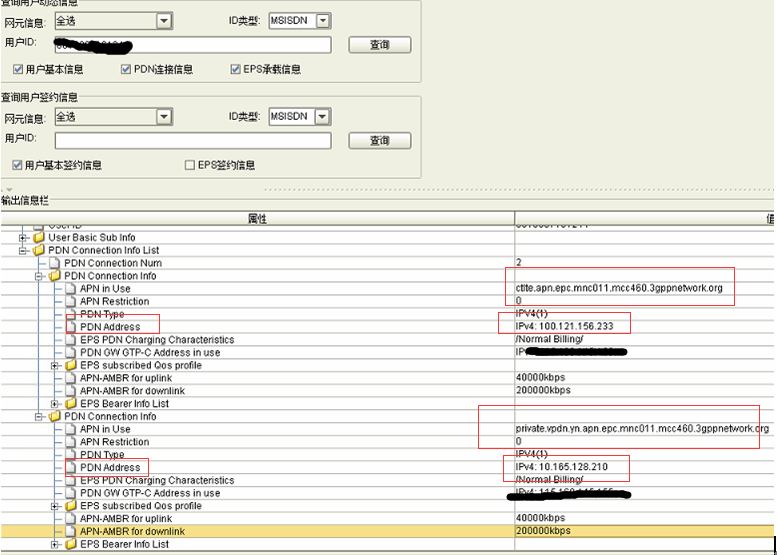
在开通测试过程中已经证明，部分终端是可以通过升级终端软件，解决账号携带问题的。

## 多pdn连接技术

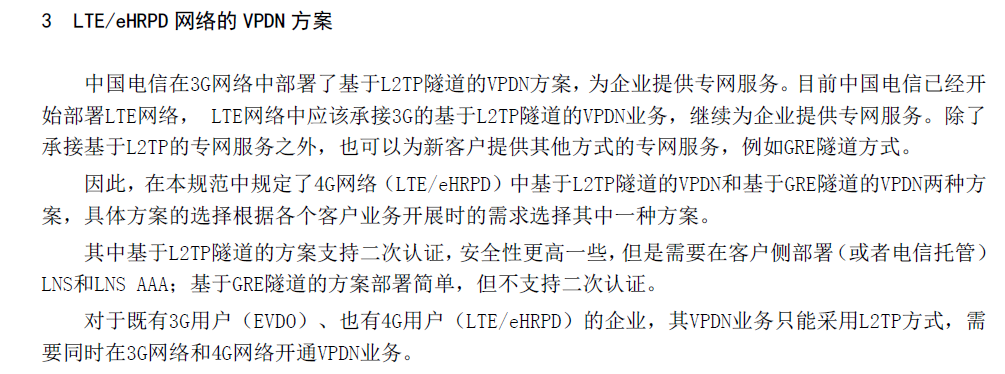
有的异常终端为什么在不绑定内网的情况下可以成功附着，是终端有多pdn连接。即终端会有两个连接，一个外网连接，一个内网连接。

这个过程是终端自行发起的，从信令上可以看出，终端首先用外网APN进行了附着，接着用内网APN再次附着。

此时终端可能占有两个ip地址的，一个是外网的ip地址，一个是内网的ip地址



## 电信集团4G VPDN规范参考

电信集团公司下发4G VPDN规范《中国电信网发〔2014〕13号集团4G-VPDN技术规范》中描述了对L2tp、GRE的选择：

在本规范中还明确规定了终端对相关字段携带的要求：

