## GPRS介绍

### GSN

为了支持更快速的分组交换数据业务，相对于GSM网络，GPRS网络新增加了GPRS支持节点GSN（GPRS Support Node，GPRS支持节点）。并且根据GSN节点的位置和功能的不同，GSN节点分成了SGSN（Serving GPRS Support Node，服务GPRS支持节点）和GGSN（Gateway GPRS Support Node，网关GPRS支持节点）两类。它们是位于GPRS核心网侧的两个最主要节点。

SGSN主要负责处理MS到GPRS网络之间的通信，负责转发MS的数据到GPRS核心网，并需要根据MS在网络中的具体位置进行移动性管理和会话管理。

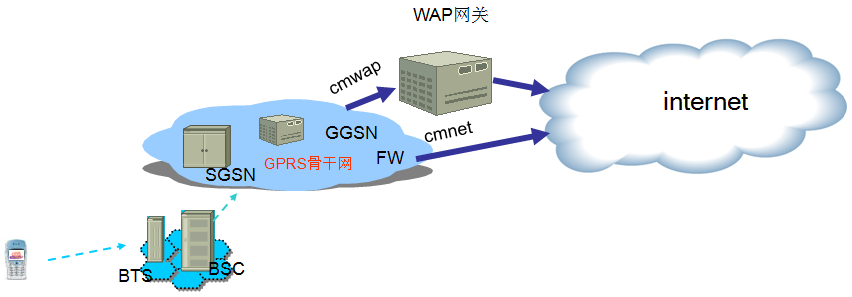
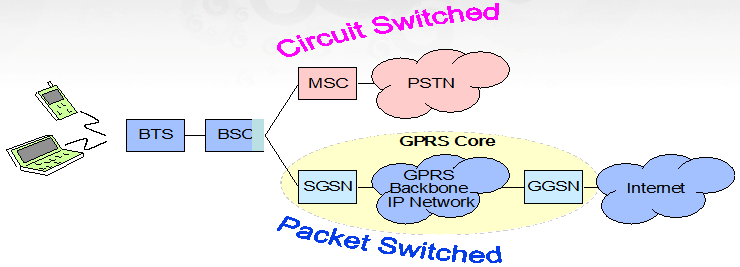
GGSN则主要负责在SGSN和外部分组数据网络（Packet Data Network，PDN）之间为MS转发上下行用户数据报文。

在一个PLMN网络中，可能有多个GSN节点。BSC和SGSN之间的接口称为Gb接口，一个PLMN网络内GSN节点之间的接口称为Gn接口。

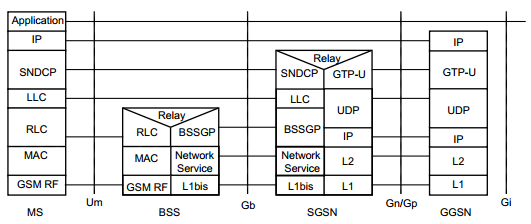
### PDN

Packet Data Network，包交换数据网络。顾名思义，PDN是指基于分组报文传送的网络，比较常见的是基于IP技术构建的分组数据网络，例如Internet。PDN网络提供了MS期望访问的各种数据应用，通过GGSN和GPRS网络相连，需要执行两个网络协议（例如上行方向：GTP到IP）的转换。电信运营商可以通过将相同类型的业务合并，设置不同的PDN网络为用户提供服务。常见的PDN网络主要有Internet、专门提供WAP类业务的数据网络、企业用户内部网络等。GGSN和外部PDN网络的接口称为Gi接口。

### GPRS网络结构



### GPRS用户面



### GPRS移动台三种状态

**1．Idle状态**

在Idle状态下，MS没有附着到GPRS网络，SGSN中没有关于用户位置及路由的相关信息，因此网络侧也无法完成对移动用户的数据传输或对用户的寻呼。在该状态下，MS被认为是不可达的状态，常见的场景包括MS处于关机的状态、MS不在GSM无线网络覆盖区域、GPRS附着不成功等。

MS可以通过发起GPRS附着流程切换到Ready状态。

**2．Ready状态**

在Ready状态下，MS已附着到GPRS网络，并可以发送和接收外部PDN的报文；SGSN中的移动性管理上下文中关于用户位置的信息精确到小区级别。在该状态下，网络侧不需要对MS执行寻呼流程，就可以直接将用户的下行数据传送到负责该小区的BSS，再由BSS转发给MS。

MS在Ready状态下可以执行PDP上下文激活、去激活等会话管理流程。

即使是在用户没有数据传递的时候，移动性管理状态仍然可能会停留在Ready状态，而不管无线资源是否被分配给用户。因此，为了节省无线侧的资源，需要有一个计时器来监控Ready状态，这就是Ready timer，当Ready timer超时后，移动性管理状态将从Ready切换到Standby。除此以外，MS还可以通过发起去附着流程来从Ready状态直接切换到Idle状态。当MS在Ready状态下移动到了其他小区时，将发起小区更新流程并通知SGSN。

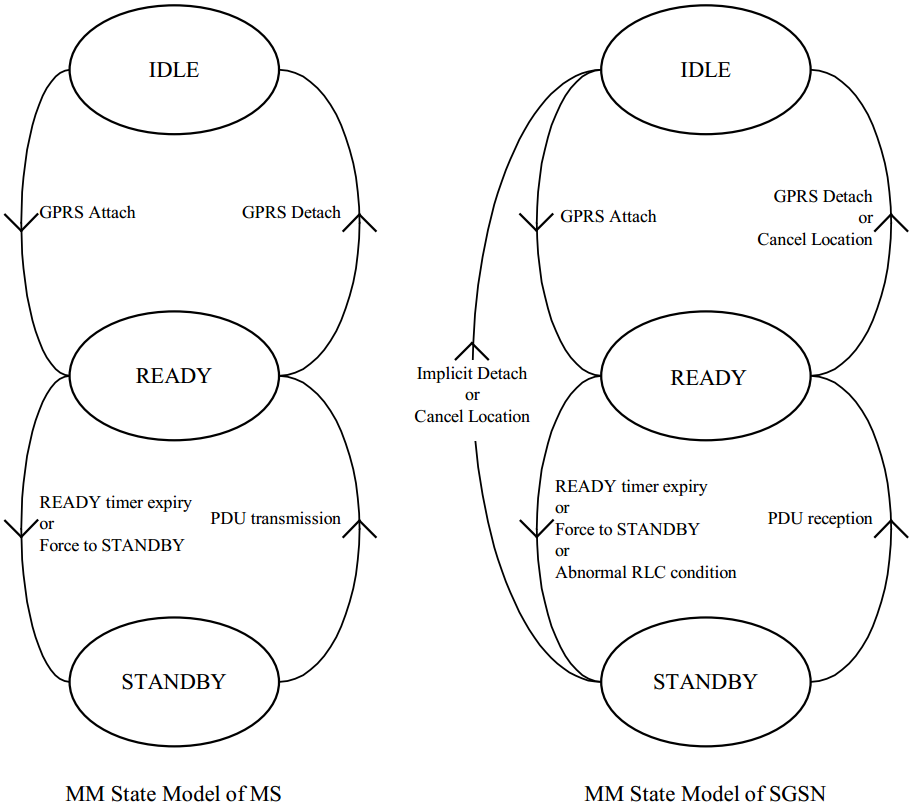
**3．Standby状态**

在Standby状态下，MS已附着到GPRS网络，MS和SGSN都已经为签约用户建立了移动性管理上下文。SGSN中的移动性管理上下文关于用户位置的信息精确到路由区级别。在该状态下，SGSN可以对用户发起寻呼，但仍不能为用户路由和转发数据报文。

MS在该状态下执行的是路由区更新流程以及在本地执行GPRS小区选择和重选流程，MS需要通过执行路由区更新流程来通知SGSN它已经进入了一个新的路由区。但MS如果只是在相同路由区下不同小区之间发生了位置移动，则MS不会通知SGSN关于小区位置的变化。因此，在Standby状态下，SGSN中移动性管理上下文中的位置信息只包含标识路由区的RAI。

由于已经完成GPRS附着，所以MS可以在Standby状态下直接发起PDP上下文的激活等会话管理相关流程。在传送或接收与PDN之间的数据之前，必须要先创建一个PDP上下文。

MS或SGSN都可以发起GPRS去附着流程将用户的移动性管理状态切换到Idle，并且在SGSN上的移动可达性计时器（Mobile Reachable Timer）超时之后，SGSN可以执行一个隐式的去附着（即不通知MS）流程，将用户移动性管理状态切换到Idle，移动性管理和PDP上下文可以被SGSN删除。



如果在Ready状态下长时间不上网，则将切换到Standby状态，相应的无线资源及核心网资源将被释放，SGSN也只需要在一个更大的服务范围路由区内追踪用户就可以了，网络侧的资源利用效率将得到极大的提升。

### GPRS上网流程

1）GPRS Attach：MM管理部分。建立MM上下文，进入READY状态，准备PDP上下文激活。包括两种attach：仅给GPRS服务使用的IMSI attach 和给GPRS服务、非GPRS服务使用的IMSI attach。

2）PDP Context Activation：SM管理部分。建立PDP上下文，向网络请求一个IP地址，并获得处理分组数据包所需要的路由及映射信息。

3）之后开始数据传输。

### [GPRS-PDP上下文的激活过程](http://blog.chinaunix.net/uid-24227137-id-2920887.html)

GPRS无线数据传输终端利用网络实现与上位机的全双工数据通信。终端需附着GPRS网络，登陆Internet与连接其上的任意一台普通PC机建立数据链路并随时进行数据传输。欲完成这一过程必须实现GPRS的附着和PDP(PacketDataProtoco1分组数据协议)上下文的激活。通过GPRS的附着登记用户信息，对用户进行移动性管理激活过程用于激活IP协议，保证数据能以IP报的形式进行传送，使移动台与GGSN(Gateway GPRS Support Node，网关GPRS节点)建立一条逻辑通路，进行数据传输。可见，激活过程是系统实现的关键，他由中央控制器软件来实现。分组数据协议的激活涉及到网络的多个协议，如PPP协议、LCP(Link Control Protocol 链路控制协议)、NCP(Network Control Protocol，网络控制协议)、 PAP(Password Authentication Protocol，密码认证协议)和 IPCP(Internet Protocol，Internet协议控制协议)等。

分组数据协议上下文激活过程

(1)终端设备向移动终端发送AT指令激活IP协议，在指令中包含终端想要连接的APN(Access Point Name访问点名称)。

(2)终端设备向移动终端发送PPPPLC帧给移动终端，表明PAP是在PDP激活过程中的身份认证协议。

(3)终端设备开始进行PAP认证，认证通过后，移动终端将对终端设备给以回应，表明承认其身份，并且会将用户ID和密码储存下来。

(4)终端设备通过发送NCP-IPCP配置请求信息给移动终端，帧内IP地址为空，表明请求动态分配IP地址。

(5)移动终端向SGSN(Servicing GPRS Support Node，服务GPRS节点)发送激活PDP上下文的请求信息，信息中包含如下信息：APN、PDP类型PDP地址为空，代表请求动态分配IP地址。

(6)SGSN请求DNS(Domain Name System，域名系统)服务器对APN进行解析，得到APN对应的GGSN的IP地址。

(7)SGSN发送建立PDP上下文的请求消息给被选定的GGSN，消息中应包含：APN、PDP类型PDP地址为空，代表请求动态分配IP地址、用户更改的QoS和其他选项。

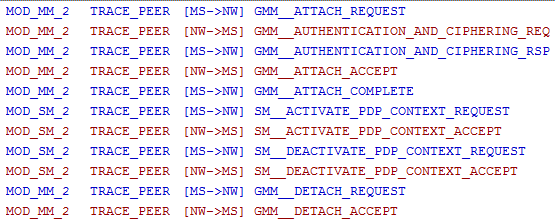
(8)GGSN对用户进行认证，认证通过后，使用RADIUS(Remote Authentication Dia-in User Service，远程认证拨入用户服务)服务器、DHCP(Dynamic Host Configuration Protocol，动态主机配置协议)服务器或直接由GGSN为用户分配动态IP地址，GGSN向SGSN返回建立PDP上下文相应消息。

(9)SGSN向移动终端发送激活PDP、上下文接受消息。

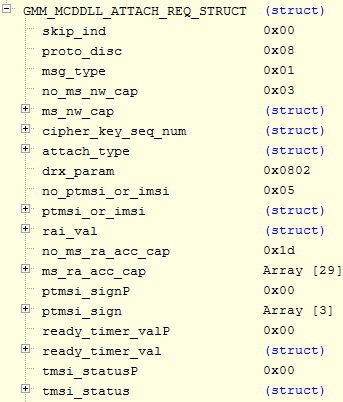
(10)移动终端发送NCP-IPCP配置回应帧给终端设备，回应帧包含了被动态分配的IP地址。

至此PDP上下文的激活过程全部完成，移动终端与外部数据网建立起数据通路，数传终端就可以和监控中心以IP数据报的形式进行通信。

## 信令流程



**1）MS向NW发送****ATTACH REQUEST。**



协议鉴别符：GMM

消息类型：ATTACH REQUEST

MS的网络能力

密钥序列号

attach类型

身份标识：IMSI or P-TMSI

路由区标识

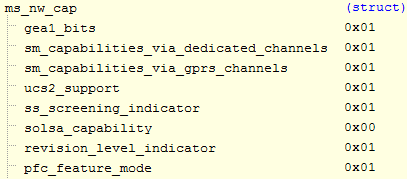
MS无线接入能力

P-TMSI签名

READY定时器的值

TMSI状态

MS的网络能力：



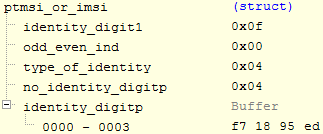
MS支持专用信 道上的点对点 SMS，MS支持 GPRS信道上的 点对点SMS

attach类型：



GPRS Attach（IMSI未附着）

身份标识：

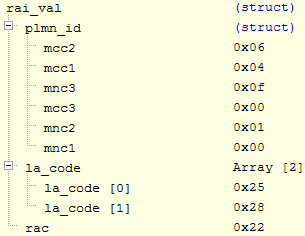


P-TMSI的情况下，该域为0x0f

类型为P-TMSI

P-TMSI的值

路由区标识：



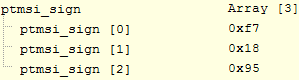
MCC

MNC

LAC

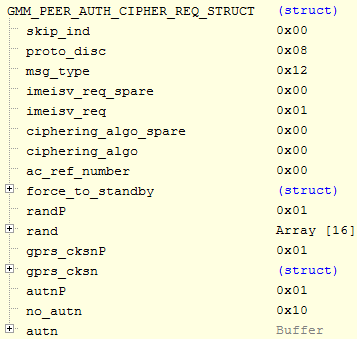
RAC

P-TMSI签名：标识了MS的一个GMM上下文

大端

小端

**2）NW向MS发起鉴权流程，发送Authentication and ciphering request。**



表明需要MS提供IMEISV

不使用加密

该域用于标识对应的鉴 权加密消息的req和resp

强制MS停止READY计时 器来防止小区更新

MS用来计算密钥和鉴权 响应序列号的随机数

密钥序列号

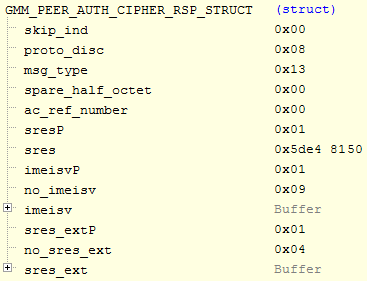
Force to standby为0，Force to standby不起作用。



密钥序列号为3。



**3）MS向NW发送Authentication and ciphering response。**



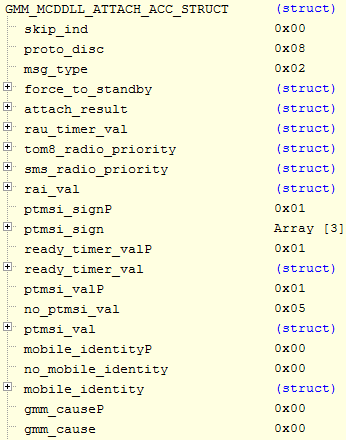
该域的值对应于A&C Req中的ref number

MS计算出的鉴权响应 序列号

MS返回的IMSISV



**4）NW向MS发送Attach Accept，表示附着请求被接受。**



attach的结果

周期性路由区更新计时器 的值

SMS MOC中MS应该使用 的优先级

路由区标识

P-TMSI签名

READY定时器的值

P-TMSI的值

移动身份标识

attach结果：



GPRS only attached

NW分配给MS rau timer初值。在Standby状态下的MS，需要周期性地执行路由区更新流程，周期性地向网络侧报告自己当前的路由区信息。



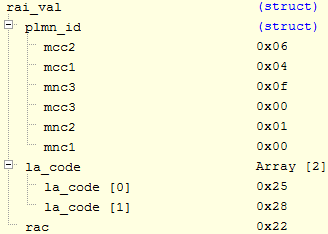
timer值的单位是1/10小时

timer值0x09

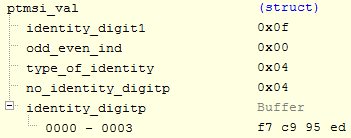
SMS MOC中MS应该使用的优先级。为1。



路由区标识。



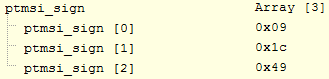
P-TMSI进行了重分配。P-TMSI签名也改变了。



P-TMSI的情况下，该域为 0x0f

类型为P-TMSI

P-TMSI的值



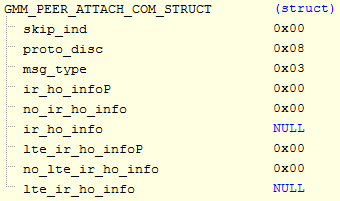
NW分配给MS READY timer初值。



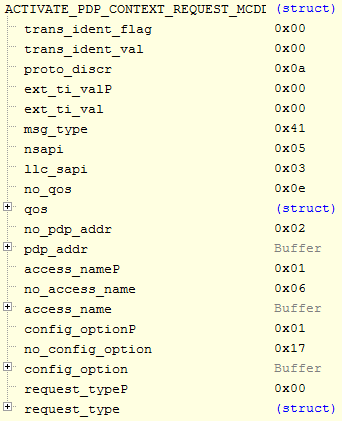
timer值的单位是1分钟

timer值0x01

**5）得到NW分配的TMSI或者P\_TMSI之后，MS向NW发送Attach Complete，表示附着完成。**



**6）MS发送****Activate PDP Context Request消息来请求激活PDP上下文。**

****

协议鉴别符：SM（Session）

网络服务接入点标识，范围 [5,15]，一个MS可同时拥有 11个PDP上下文（**层3**）

LLC服务接入点标识，标识 在**LLC层**传输的GPRS数据的 接入点

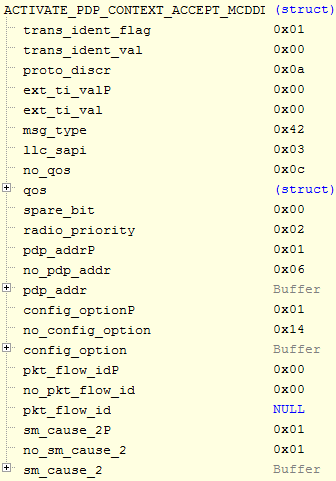
为PDP上下文指定QoS参数

PDP地址（**网络层**）

接入点

配置选项

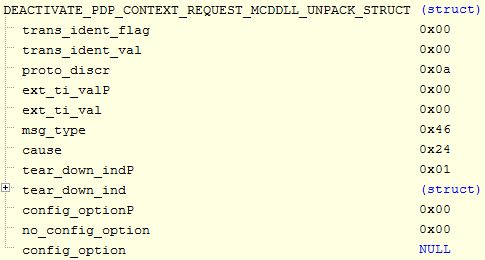
**7）NW回复Activate PDP Context Accept消息，接受激活PDP上下文。**



NW分配给MS的PDP地址

PDP地址。21表示是IP V4，地址是10.163.12.128。

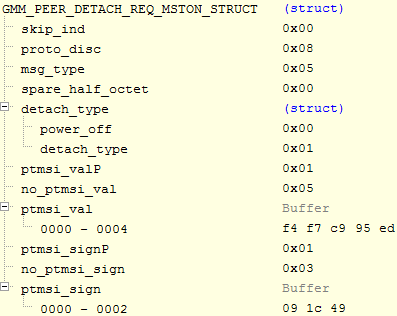
**8）MS发送Deactivate PDP Context Request消息，去活PDP上下文。**



去活的原因：常规去活

**9）NW发送Deactivate PDP Context Accept消息，接受去活PDP上下文。**

**10）MS发送Detach Request消息，发起分离流程。**



分离的类型

常规分离

GPRS分离

MS的P-TMSI

P-TMSI签名

**11）NW发送Detach Accept消息，分离流程结束。**