第23讲 | 移动网络：去巴塞罗那，手机也上不了脸书

2018-07-09 刘超

第23讲 | 移动网络：去巴塞罗那，手机也上不了脸书
朗读人：刘超　22'11'' | 8.89M

前面讲的都是电脑上网的场景，那使用手机上网有什么不同呢？

移动网络的发展历程

你一定知道手机上网有 2G、3G、4G 的说法，究竟这都是什么意思呢？有一个通俗的说法就是：用 2G 看 txt，用 3G 看 jpg，用 4G 看 avi。

2G 网络

手机本来是用来打电话的，不是用来上网的，所以原来在 2G 时代，上网使用的不是 IP 网络，而是电话网络，走模拟信号，专业名称为公共交换电话网（PSTN，Public Switched Telephone Network）。

那手机不连网线，也不连电话线，它是怎么上网的呢？

手机是通过收发无线信号来通信的，专业名称是 Mobile Station，简称 MS，需要嵌入 SIM。手机是客户端，而无线信号的服务端，就是基站子系统（BSS，Base Station SubsystemBSS）。至于什么是基站，你可以回想一下，你在爬山的时候，是不是看到过信号

塔？我们平时城市里面的基站比较隐蔽，不容易看到，所以只有在山里才会注意到。正是这个信号塔，通过无线信号，让你的手机可以进行通信。

但是你要知道一点，无论无线通信如何无线，最终还是要连接到有线的网络里。前面讲数据中心的时候我也讲过，电商的应用是放在数据中心的，数据中心的电脑都是插着网线的。

因而，基站子系统分两部分，一部分对外提供无线通信，叫作基站收发信台（BTS，Base Transceiver Station），另一部分对内连接有线网络，叫作基站控制器（BSC，Base Station Controller）。基站收发信台通过无线收到数据后，转发给基站控制器。

这部分属于无线的部分，统称为无线接入网（RAN，Radio Access Network）。

基站控制器通过有线网络，连接到提供手机业务的运营商的数据中心，这部分称为核心网（CN，Core Network）。核心网还没有真的进入互联网，这部分还是主要提供手机业务，是手机业务的有线部分。

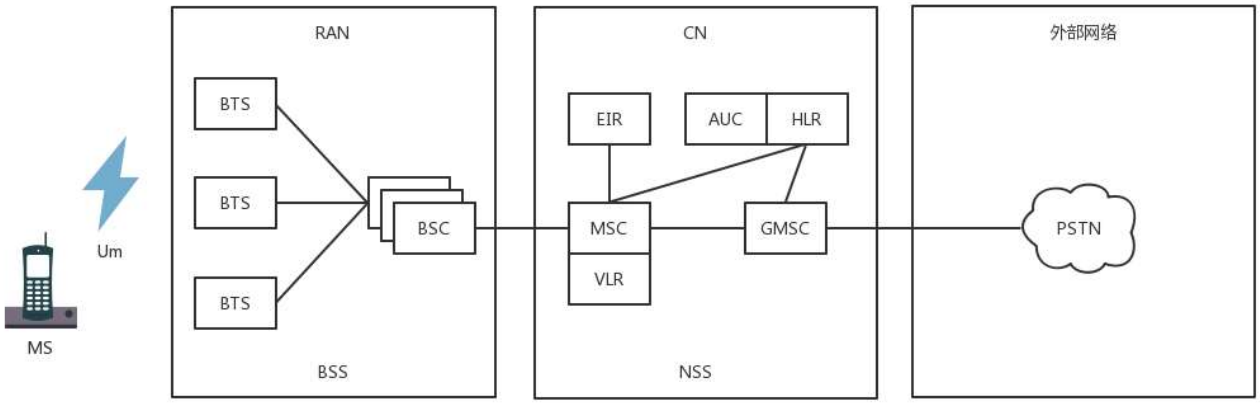
首先接待基站来的数据的是移动业务交换中心（MSC，Mobile Service Switching Center），它是进入核心网的入口，但是它不会让你直接连接到互联网上。

因为在让你的手机真正进入互联网之前，提供手机业务的运营商，需要认证是不是合法的手机接入。别你自己造了一张手机卡，就连接上来。鉴权中心（AUC，Authentication Center）和设备识别寄存器（EIR，Equipment Identity Register）主要是负责安全性的。

另外，需要看你是本地的号，还是外地的号，这个牵扯到计费的问题，异地收费还是很贵的。访问位置寄存器（VLR，Visit Location Register）是看你目前在的地方，归属位置寄存器（HLR，Home Location Register）是看你的号码归属地。

当你的手机卡既合法又有钱的时候，才允许你上网，这个时候需要一个网关，连接核心网和真正的互联网。网关移动交换中心（GMSC ，Gateway Mobile Switching Center）就是干这个的，然后是真正的互连网。在 2G 时代，还是电话网络 PSTN。

数据中心里面的这些模块统称为网络子系统（NSS，Network and Switching Subsystem）。



因而 2G 时代的上网如图所示，我们总结一下，有这几个核心点：

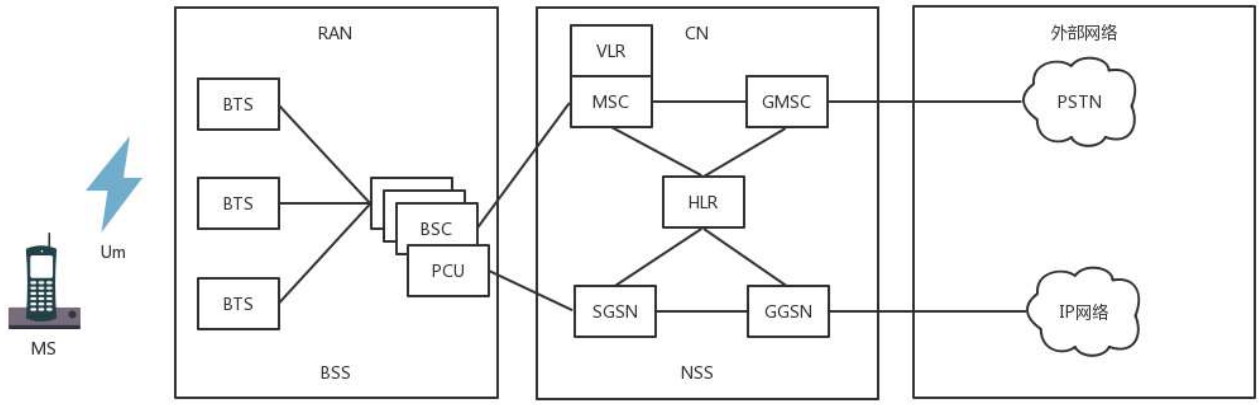
- 手机通过无线信号连接基站；
- 基站一面朝前接无线，一面朝后接核心网；
- 核心网一面朝前接到基站请求，一是判断你是否合法，二是判断你是不是本地号，还有没有钱，一面通过网关连接电话网络。

2.5G 网络

后来从 2G 到了 2.5G，也即在原来电路交换的基础上，加入了分组交换业务，支持 Packet 的转发，从而支持 IP 网络。

在上述网络的基础上，基站一面朝前接无线，一面朝后接核心网。在朝后的组件中，多了一个分组控制单元（PCU，Packet Control Unit），用以提供分组交换通道。

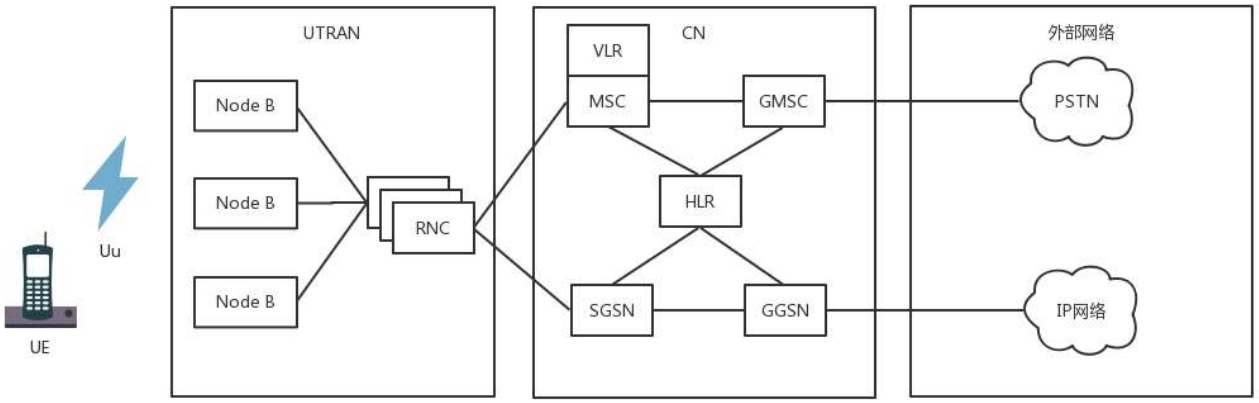
在核心网里面，有个朝前的接待员（SGSN，Service GPRS Supported Node）和朝后连接 IP 网络的网关型 GPRS 支持节点（GGSN，Gateway GPRS Supported Node）。



3G 网络

到了 3G 时代，主要是无线通信技术有了改进，大大增加了无线的带宽。

以 W-CDMA 为例，理论最高 2M 的下行速度，因而基站改变了，一面朝外的是 Node B，一面朝内连接核心网的是无线网络控制器（RNC，Radio Network Controller）。核心网以及连接的 IP 网络没有什么变化。

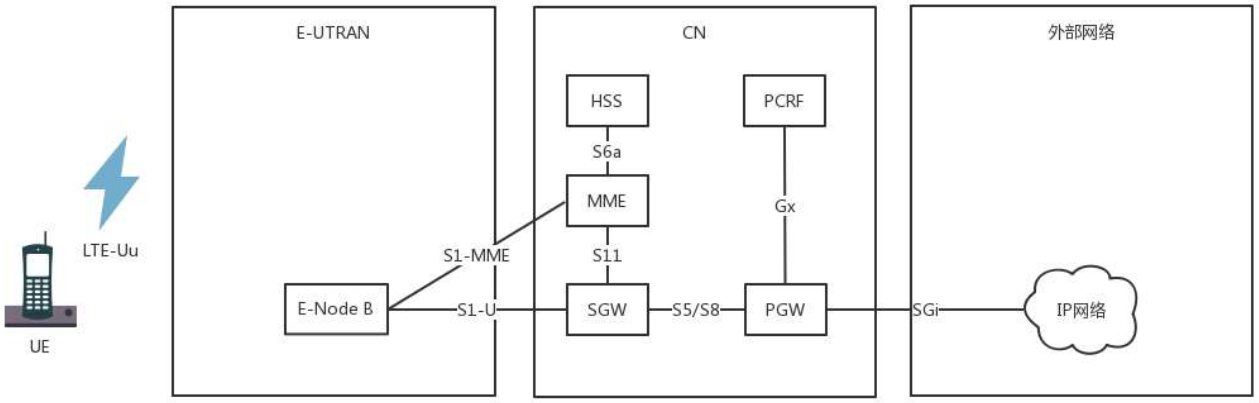


4G 网络

然后就到了今天的 4G 网络，基站为 eNodeB，包含了原来 Node B 和 RNC 的功能，下行速度向百兆级别迈进。另外，核心网实现了控制面和数据面的分离，这个怎么理解呢？

在前面的核心网里面，有接待员 MSC 或者 SGSN，你会发现检查是否合法是它负责，转发数据也是它负责，也即控制面和数据面是合二为一的，这样灵活性比较差，因为控制面主要是指令，多是小包，往往需要高的及时性；数据面主要是流量，多是大包，往往需要吞吐量。

于是有了下面这个架构。



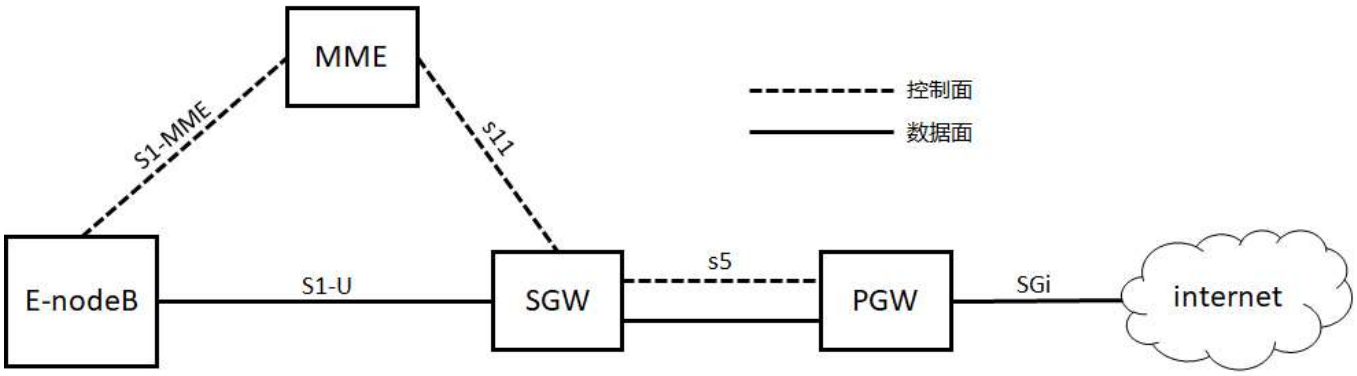
HSS 用于存储用户签约信息的数据库，其实就是你这个号码归属地是哪里的，以及一些认证信息。

MME 是核心控制网元，是控制面的核心，当手机通过 eNodeB 连上的时候，MME 会根据 HSS 的信息，判断你是否合法。如果允许连上来，MME 不负责具体的数据的流量，而是 MME 会选择数据面的 SGW 和 PGW，然后告诉 eNodeB，我允许你连上来了，你连接它们吧。

于是手机直接通过 eNodeB 连接 SGW，连上核心网，SGW 相当于数据面的接待员，并通过 PGW 连到 IP 网络。PGW 就是出口网关。在出口网关，有一个组件 PCRF，称为策略和计费控制单元，用来控制上网策略和流量的计费。

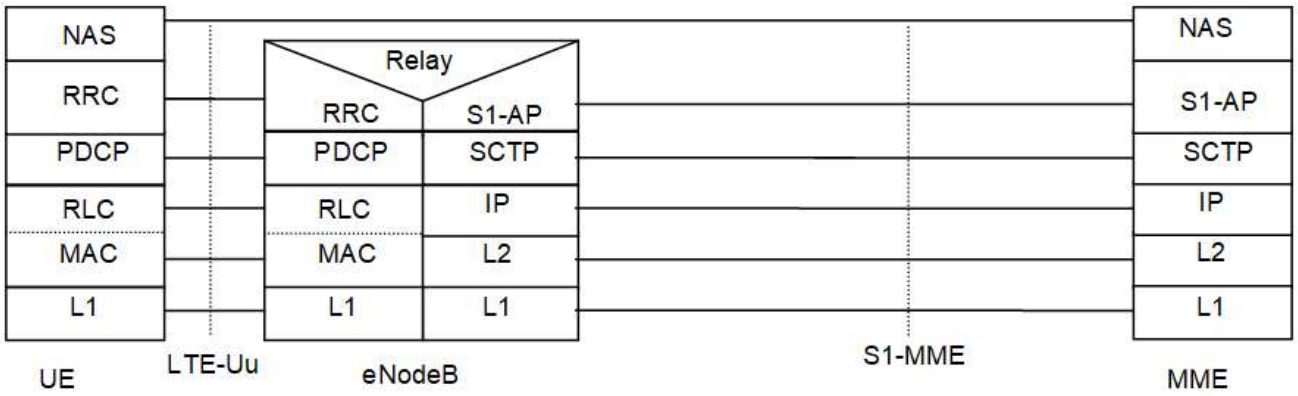
4G 网络协议解析

我们来仔细看一下 4G 网络的协议，真的非常复杂。我们将几个关键组件放大来看。



控制面协议

其中虚线部分是控制面的协议。当一个手机想上网的时候，先要连接 eNodeB，并通过 S1-MME 接口，请求 MME 对这个手机进行认证和鉴权。S1-MME 协议栈如下图所示。



UE 就是你的手机，eNodeB 还是两面派，朝前对接无线网络，朝后对接核心网络，在控制面对接的是 MME。

eNodeB 和 MME 之间的连接就是很正常的 IP 网络，但是这里面在 IP 层之上，却既不是 TCP，也不是 UDP，而是 SCTP。这也是传输层的协议，也是面向连接的，但是更加适合移动网络。 它继承了 TCP 较为完善的拥塞控制并改进 TCP 的一些不足之处。

SCTP 的第一个特点是**多宿主**。一台机器可以有多个网卡，而对于 TCP 连接来讲，虽然服务端可以监听 0.0.0.0，也就是从哪个网卡来的连接都能接受，但是一旦建立了连接，就建立了四元组，也就选定了某个网卡。

SCTP 引入了联合（association）的概念，将多个接口、多条路径放到一个联合中来。当检测到一条路径失效时，协议就会通过另外一条路径来发送通信数据。应用程序甚至都不必知道发生了故障、恢复，从而提供更高的可用性和可靠性。

SCTP 的第二个特点是将一个联合分成多个流。一个联合中的所有流都是独立的，但均与该联合相关。每个流都给定了一个流编号，它被编码到 SCTP 报文中，通过联合在网络上传送。在 TCP 的机制中，由于强制顺序，导致前一个不到达，后一个就得等待，SCTP 的多个流不会相互阻塞。

SCTP 的第三个特点是四次握手，防止 SYN 攻击。在 TCP 中是三次握手，当服务端收到客户的 SYN 之后，返回一个 SYN-ACK 之前，就建立数据结构，并记录下状态，等待客户端发送 ACK 的 ACK。当恶意客户端使用虚假的源地址来伪造大量 SYN 报文时，服务端需要分配大量的资源，最终耗尽资源，无法处理新的请求。

SCTP 可以通过四次握手引入 Cookie 的概念，来有效地防止这种攻击的产生。在 SCTP 中，客户机使用一个 INIT 报文发起一个连接。服务器使用一个 INIT-ACK 报文进行响应，其中就包括了 Cookie。然后客户端就使用一个 COOKIE-ECHO 报文进行响应，其中包含了服务器所发送的 Cookie。这个时候，服务器为这个连接分配资源，并通过向客户机发送一个 COOKIE-ACK 报文对其进行响应。

SCTP 的第四个特点是将消息分帧。TCP 是面向流的，也即发送的数据没头没尾，没有明显的界限。这对于发送数据没有问题，但是对于发送一个个消息类型的数据，就不太方便。有可能客户端写入 10 个字节，然后再写入 20 个字节。服务端不是读出 10 个字节的一个消息，再读出 20 个字节的一个消息，而有可能读入 25 个字节，再读入 5 个字节，需要业务层去组合成消息。

SCTP 借鉴了 UDP 的机制，在数据传输中提供了消息分帧功能。当一端对一个套接字执行写操作时，可确保对等端读出的数据大小与此相同。

SCTP 的第五个特点是断开连接是三次挥手。在 TCP 里面，断开连接是四次挥手，允许另一端处于半关闭的状态。SCTP 选择放弃这种状态，当一端关闭自己的套接字时，对等的两端全部需要关闭，将来任何一端都不允许再进行数据的移动了。

当 MME 通过认证鉴权，同意这个手机上网的时候，需要建立一个数据面的数据通路。建立通路的过程还是控制面的事情，因而使用的是控制面的协议 GTP-C。

建设的数据通路分两段路，其实是两个隧道。一段是从 eNodeB 到 SGW，这个数据通路由 MME 通过 S1-MME 协议告诉 eNodeB，它是隧道的一端，通过 S11 告诉 SGW，它是隧道的另一端。第二端是从 SGW 到 PGW，SGW 通过 S11 协议知道自己是其中一端，并主动通过 S5 协议，告诉 PGW 它是隧道的另一端。

GTP-C 协议是基于 UDP 的，这是UDP 的“城会玩”中的一个例子。如果看 GTP 头，我们可以看到，这里面有隧道的 ID，还有序列号。

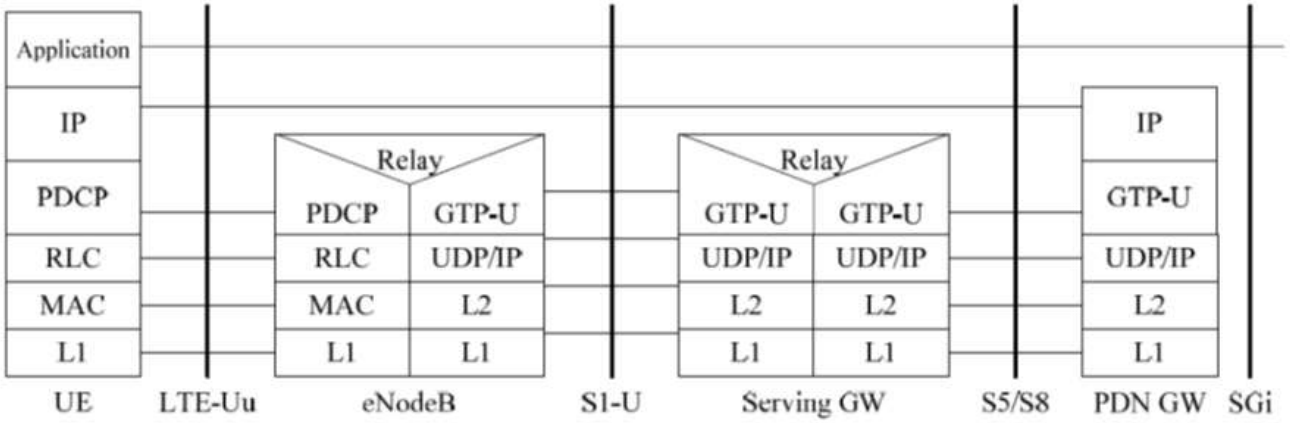
Octets	8	7	6	5	4	3	2	1
1	版本号			协议类型	(*)	E	S	PN
2	消息类型							
3	长度(1st Octet)							
4	长度 (2nd Octet)							
5	隧道端点标识符TEID(1st Octet)							
6	隧道端点标识符TEID(2nd Octet)							
7	隧道端点标识符TEID(3rd Octet)							
8	隧道端点标识符TEID(4th Octet)							
9	序号(1st Octet)1) 4)							
10	序号(2nd Octet)1) 4)							
11	N-PDU编号2) 4)							
12	下一个扩展头类型3) 4)							

通过序列号，不用 TCP，GTP-C 自己就可以实现可靠性，为每个输出信令消息分配一个依次递增的序列号，以确保信令消息的按序传递，并便于检测重复包。对于每个输出信令消息启动定时器，在定时器超时前未接收到响应消息则进行重发。

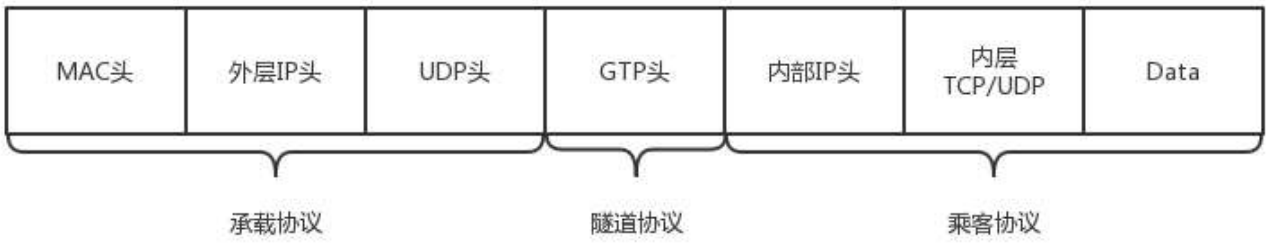
数据面协议

当两个隧道都打通，接在一起的时候，PGW 会给手机分配一个 IP 地址，这个 IP 地址是隧道内部的 IP 地址，可以类比为 IPsec 协议里面的 IP 地址。这个 IP 地址是归手机运营商管理的。然后，手机可以使用这个 IP 地址，连接 eNodeB，从 eNodeB 经过 S1-U 协议，通过第一段隧道到达 SGW，再从 SGW 经过 S8 协议，通过第二段隧道到达 PGW，然后通过 PGW 连接到互联网。

数据面的协议都是通过 GTP-U，如图所示。



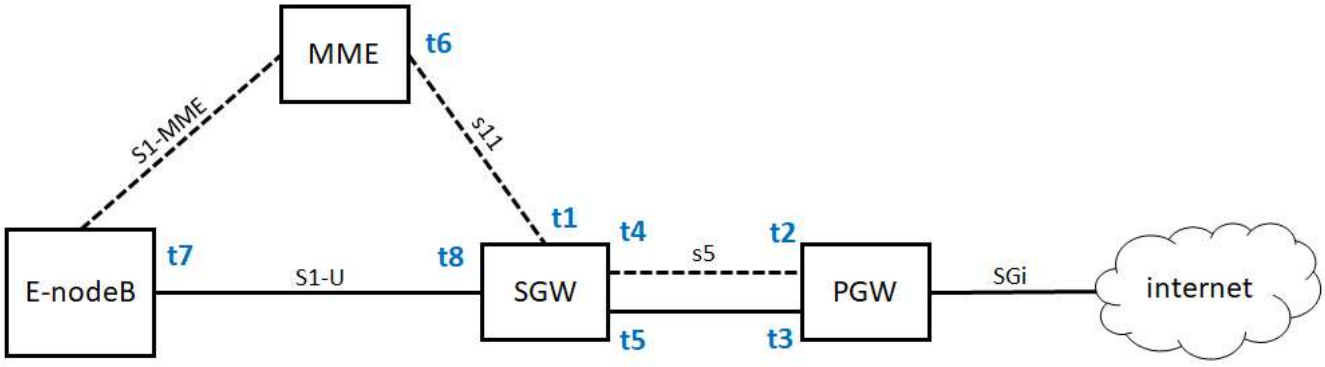
手机每发出的一个包，都由 GTP-U 隧道协议封装起来，格式如下。



和 IPsec 协议很类似，分为乘客协议、隧道协议、承载协议。其中乘客协议是手机发出来的包，IP 是手机的 IP，隧道协议里面有隧道 ID，不同的手机上线会建立不同的隧道，因而需要隧道 ID 来标识。承载协议的 IP 地址是 SGW 和 PGW 的 IP 地址。

手机上网流程

接下来，我们来看一个手机开机之后上网的流程，这个过程称为Attach。可以看出来，移动网络还是很复杂的。因为这个过程要建立很多的隧道，分配很多的隧道 ID，所以我画了一个图来详细说明这个过程。



1. 手机开机以后，在附近寻找基站 eNodeB，找到后给 eNodeB 发送 Attach Request，说“我来啦，我要上网”。
2. eNodeB 将请求发给 MME，说“有个手机要上网”。

3. MME 去请求手机，一是认证，二是鉴权，还会请求 HSS 看看有没有钱，看看是在哪里上网。
4. 当 MME 通过了手机的认证之后，开始分配隧道，先告诉 SGW，说要创建一个会话（Create Session）。在这里面，会给 SGW 分配一个隧道 ID t1，并且请求 SGW 给自己也分配一个隧道 ID。
5. SGW 转头向 PGW 请求建立一个会话，为 PGW 的控制面分配一个隧道 ID t2，也给 PGW 的数据面分配一个隧道 ID t3，并且请求 PGW 给自己的控制面和数据面分配隧道 ID。
6. PGW 回复 SGW 说“创建会话成功”，使用自己的控制面隧道 ID t2，回复里面携带着给 SGW 控制面分配的隧道 ID t4 和控制面的隧道 ID t5，至此 SGW 和 PGW 直接的隧道建设完成。双方请求对方，都要带着对方给自己分配的隧道 ID，从而标志是这个手机的请求。
7. 接下来 SGW 回复 MME 说“创建会话成功”，使用自己的隧道 ID t1 访问 MME，回复里面有给 MME 分配隧道 ID t6，也有 SGW 给 eNodeB 分配的隧道 ID t7。
8. 当 MME 发现后面的隧道都建设成功之后，就告诉 eNodeB，“后面的隧道已经建设完毕，SGW 给你分配的隧道 ID 是 t7，你可以开始连上来了，但是你也要给 SGW 分配一个隧道 ID”。
9. eNodeB 告诉 MME 自己给 SGW 分配一个隧道，ID 为 t8。
10. MME 将 eNodeB 给 SGW 分配的隧道 ID t8 告知 SGW，从而前面的隧道也建设完毕。

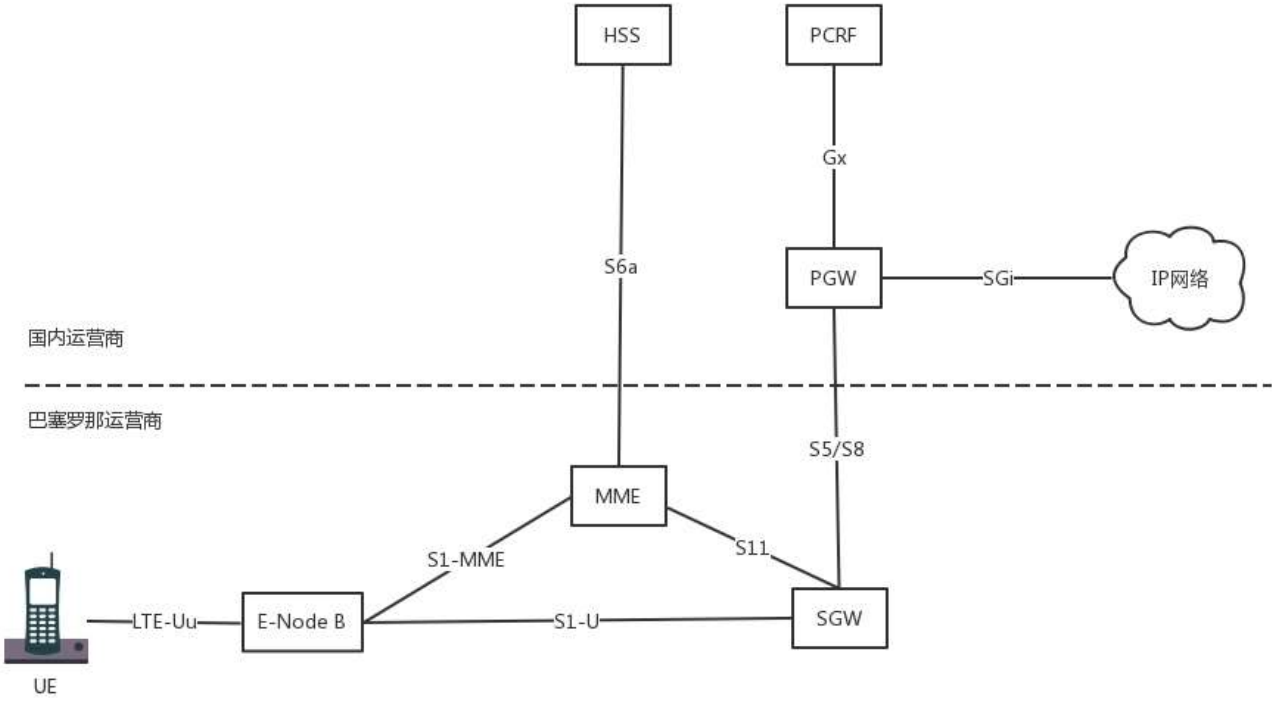
这样，手机就可以通过建立的隧道成功上网了。

异地上网问题

接下来我们考虑异地上网的事情。

为什么要分 SGW 和 PGW 呢，一个 GW 不可以吗？SGW 是你本地的运营商的设备，而 PGW 是你所属的运营商的设备。

如果你在巴塞罗那，一下飞机，手机开机，周围搜寻到的肯定是巴塞罗那的 eNodeB。通过 MME 去查寻国内运营商的 HSS，看你是否合法，是否还有钱。如果允许上网，你的手机和巴塞罗那的 SGW 会建立一个隧道，然后巴塞罗那的 SGW 和国内运营商的 PGW 建立一个隧道，然后通过国内运营商的 PGW 上网。



这样判断你是否能上网的在国内运营商的 HSS，控制你上网策略的是国内运营商的 PCRF，给手机分配的 IP 地址也是国内运营商的 PGW 负责的，给手机分配的 IP 地址也是国内运营商里统计的。运营商由于是在 PGW 里面统计的，这样你的上网流量全部通过国内运营商即可，只不过巴塞罗那运营商也要和国内运营商进行流量结算。

由于你的上网策略是由国内运营商在 PCRF 中控制的，因而你还是上不了脸书。

小结

好了，这一节就到这里了，我们来总结一下：

- 移动网络的发展历程从 2G 到 3G，再到 4G，逐渐从打电话的功能为主，向上网的功能为主转变；
- 请记住 4G 网络的结构，有 eNodeB、MME、SGW、PGW 等，分控制面协议和数据面协议，你可以对照着结构，试着说出手机上网的流程；
- 即便你在国外的运营商下上网，也是要通过国内运营商控制的，因而也上不了脸书。

最后，给你留两个思考题：

1. 咱们上网都有套餐，有交钱多的，有交钱少的，你知道移动网络是如何控制不同优先级的用户的上网流量的吗？
2. 前面讲过的所有的网络都是基于物理机的，随着云计算兴起，无论是电商，还是移动网络都要部署在云中了，你知道云中网络的设计有哪些要点吗？

我们的专栏更新到第 23 讲，不知你掌握得如何？每节课后我留的思考题，你都有没有认真思考，并在留言区写下答案呢？我会从已发布的文章中选出一批认真留言的同学，赠送学习奖励礼券和我整理的独家网络协议知识图谱。

欢迎你留言和我讨论。趣谈网络协议，我们下期见！

精选留言

萌 0
刘老师，一直在听您的课，条理很清晰，很佩服，想说，看您能否出一套关于操作系统的课程。。。
2018-07-09

赤脚小子 0
非常感谢作者，最近接触的5g,和中国移动项目，都需要大量的网络知识，可惜看着课程表没有sdn，nfv的内容了，您的课每一篇都值得仔细阅读，比买过的其他课好太多了。期待您的新课程或者新著作。
2018-07-09


蓝色理想 0
老师蓝牙wifi会讲吗？
2018-07-09


蓝色理想 0
老师如此博学
2018-07-09