# 4G公网通信调研

# 背景

电子车牌读写设备采用4G模块进行无线通信，4G模块分配的IP为基站下的局域网IP，外网无法ping通。为实现电子车牌读写设备与PC机进行公网通信，使用公司的固定IP在路由中做端口映射，映射到指定的PC机上，电子车牌读写设备作为客户端（socket client），PC机作为服务端（socket server）。

# 环境搭建

## 端口映射

[内网](https://baike.baidu.com/item/%E5%86%85%E7%BD%91" \t "https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3%E6%98%A0%E5%B0%84/_blank)的一台电脑要上因特网对外开放服务或接收数据，都需要端口映射。端口映射分为动态和静态。

动态端口映射：[内网](https://baike.baidu.com/item/%E5%86%85%E7%BD%91" \t "https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3%E6%98%A0%E5%B0%84/_blank)中的一台电脑要访问网站，会向NAT[网关](https://baike.baidu.com/item/%E7%BD%91%E5%85%B3" \t "https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3%E6%98%A0%E5%B0%84/_blank)发送[数据包](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%8C%85" \t "https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3%E6%98%A0%E5%B0%84/_blank)，[包头](https://baike.baidu.com/item/%E5%8C%85%E5%A4%B4" \t "https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3%E6%98%A0%E5%B0%84/_blank)中包括对方网站IP、端口和本机IP、端口，NAT[网关](https://baike.baidu.com/item/%E7%BD%91%E5%85%B3" \t "https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3%E6%98%A0%E5%B0%84/_blank)会把本机IP、端口替换成自己的公网IP、一个未使用的端口，并且会记下这个映射关系，为以后转发数据包使用。然后再把数据发给网站，网站收到数据后做出反应，发送数据到NAT[网关](https://baike.baidu.com/item/%E7%BD%91%E5%85%B3" \t "https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3%E6%98%A0%E5%B0%84/_blank)的那个未使用的端口，然后NAT网关将数据转发给[内网](https://baike.baidu.com/item/%E5%86%85%E7%BD%91" \t "https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3%E6%98%A0%E5%B0%84/_blank)中的那台电脑，实现内网和公网的通讯。当连接关闭时，NAT网关会释放分配给这条连接的端口，以便以后的连接可以继续使用。动态端口映射其实也就是NAT[网关](https://baike.baidu.com/item/%E7%BD%91%E5%85%B3" \t "https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3%E6%98%A0%E5%B0%84/_blank)的工作方式。

静态端口映射：就是在NAT[网关](https://baike.baidu.com/item/%E7%BD%91%E5%85%B3" \t "https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3%E6%98%A0%E5%B0%84/_blank)上开放一个固定的端口，然后设定此端口收到的数据要转发给[内网](https://baike.baidu.com/item/%E5%86%85%E7%BD%91" \t "https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3%E6%98%A0%E5%B0%84/_blank)哪个IP和端口，不管有没有连接，这个映射关系都会一直存在。就可以让公网主动访问[内网](https://baike.baidu.com/item/%E5%86%85%E7%BD%91" \t "https://baike.baidu.com/item/%E7%AB%AF%E5%8F%A3%E6%98%A0%E5%B0%84/_blank)的一台电脑。我们采用的就是这种映射方式实现4G和PC机通信，如图1所示。

图1



## 内网穿透

网络地址转换（Network Address Translation，NAT）机制的问题在于，NAT设备自动屏蔽了非内网主机主动发起的连接，也就是说，从外网发往内网的数据包将被NAT设备丢弃，这使得位于不同NAT设备之后的主机之间无法直接交换信息。这一方面保护了内网主机免于来自外部网络的攻击，另一方面也为P2P通信带来了一定困难。Internet上的NAT设备大多是地址限制圆锥形NAT或端口限制圆锥形 NAT，外部主机要与内网主机相互通信，必须由内网主机主动发起连接，使 NAT设备产生一个映射条目，这就有必要研究一下内网穿透技术。

内网穿透，也即 NAT 穿透，进行 NAT 穿透是为了使具有某一个特定源 IP 地址和源端口号的数据包不被 NAT 设备屏蔽而正确路由到内网主机。

## 花生壳

花生壳是款具备内网穿透和端口映射功能的软件。花生壳内网穿透，是通过云服务器快速与内网服务器建立连接，同时把内网端口映射到云端，实现各类基于域名的互联网应用服务。花生壳的内网穿透功能不需要公网IP即可实现。

同时，花生壳上可以申请免费的域名，将公网IP和域名进行绑定，从而可以通过域名访问该公网IP。