终端劫持设计

# 核心目标：

手机上安装我们自己写的App，来远程控制路由器进行终端劫持。（不一定要连接上这个路由器的WiFi才能控制，手机用流量上网也可以控制）

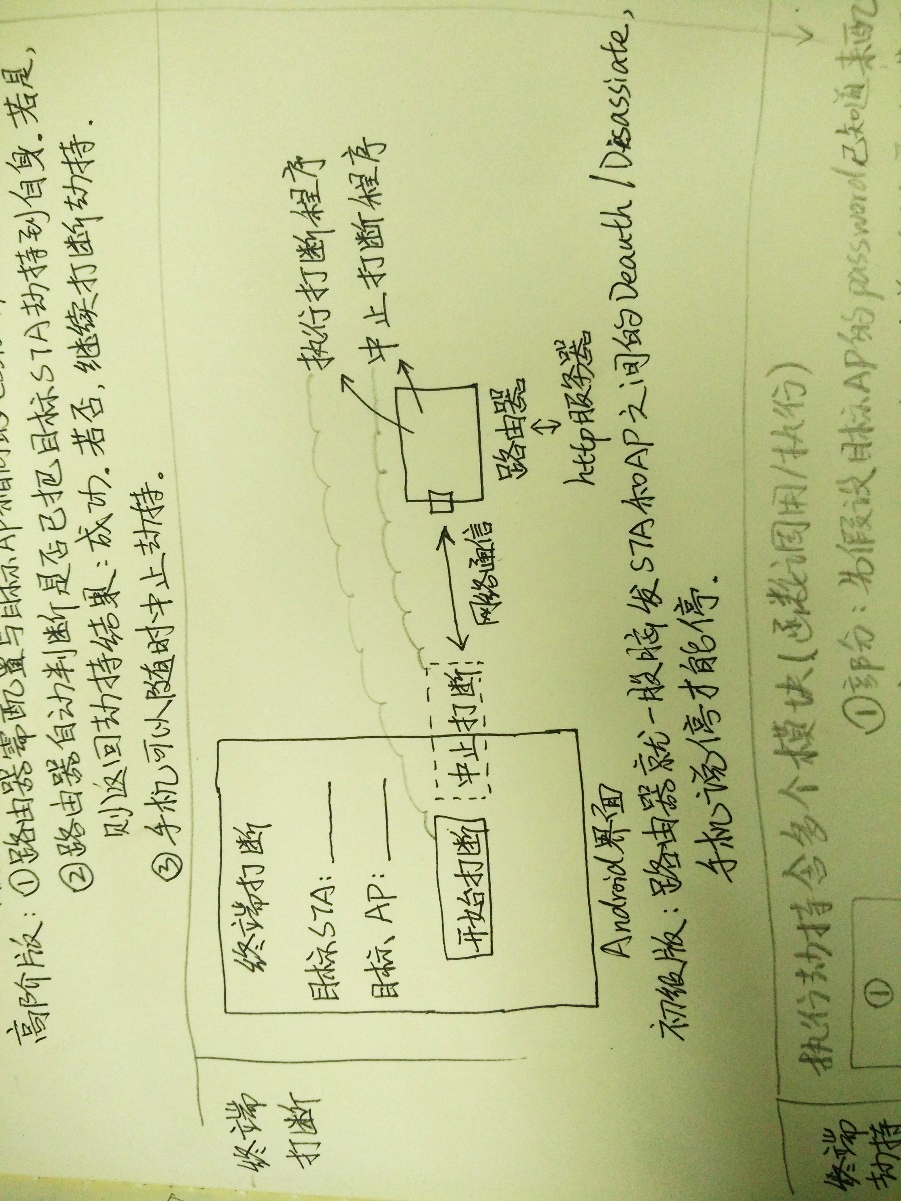
# 涉及要素：

1. Android下的网络通信编程知识；（如HttpClient）
2. openWRT路由器的http服务器配置；
3. 以上两者的信息交互；
4. 之前写好的打断代码；

# 预期功能设计：

1. **初级练手版**

如下图所示，我们只需在路由器配好http服务器，在Android写个界面，能够发送打断/中断的信号让路由器识别并执行就好了。



具体的，

（1）Android界面包含元素：

目标STA的mac输入，目标AP的mac输入，开始打断/中止打断按钮。

（2）操作流程：

用户点击输入STA和AP后，点击‘开始打断’按钮，程序携带sta，ap数据和打断信号向路由器发post请求，路由器识别并执行打断程序（你之前写的breakConnect代码）

用户点击‘中止打断’按钮，程序携带中止信号向路由器发post请求，路由器识别并中止程序的执行。

（3）信号交互举例：

如我可以设置发‘breakConnect’或‘1’等等，是要执行打断程序的意思。伪代码可能是，

if(receive==‘breakConnect’){

sta\_mac=XXXXX;

ap\_mac=XXXXXX;

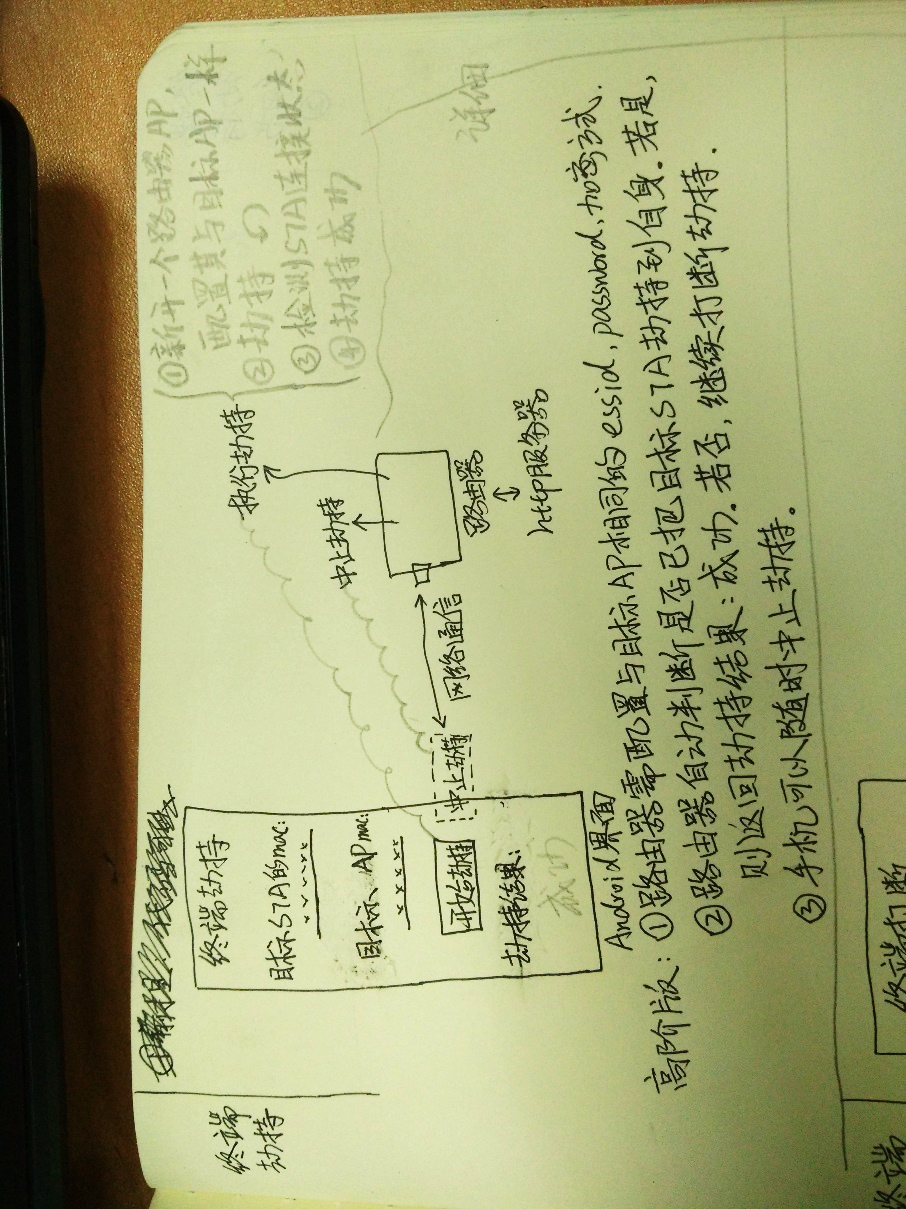
System（”sudo ./breakConnect mon0”+sta\_mac+ap\_mac）；

}else if(receive==XXX){

}

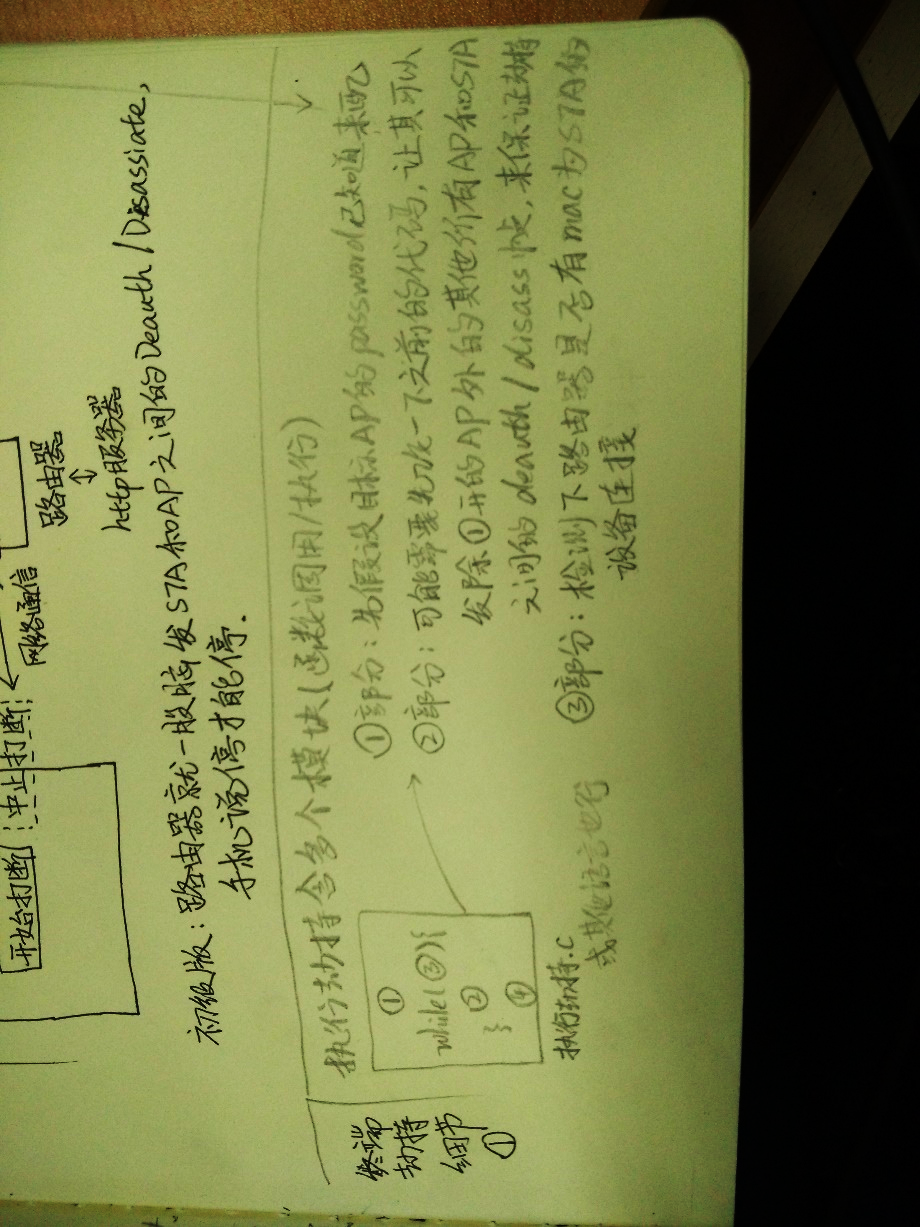
1. **高阶装逼版**

如下图所示，我们不仅仅只是打断连接，我们还要把目标STA劫持到我们路由器新开的一个AP上（若已经有第二个AP了，那就不用新开，而是修改）。

****

具体的，

1. 与初级版不同的地方，见图中黑体字。
2. 在执行劫持部分多了其他的内容，见图中铅笔字，可能看不清，这里再重复一次。
   * 1. 在路由器上新开一个AP（若有第二个了，就只是配置就好），配置其与目标AP一样（即wifi名称，密码，加密方式）
     2. 劫持（还是你之前写的BreakConnect代码）
     3. 检测STA的连接状态
     4. 劫持成功，返回信号。
3. (2)部分每个小点更具体的细节,见下图



# 参考资料：

1. 关于openWRT配置http服务器

<http://www.szchehang.com/news/10602.html>

1. 关于Android的HttpClient实现网络通信

书《Android编程实战学习手册》等

1. socket知识，辅助开发中遇到的一些问题理解

<http://www.jianshu.com/p/90348ef3f41e>