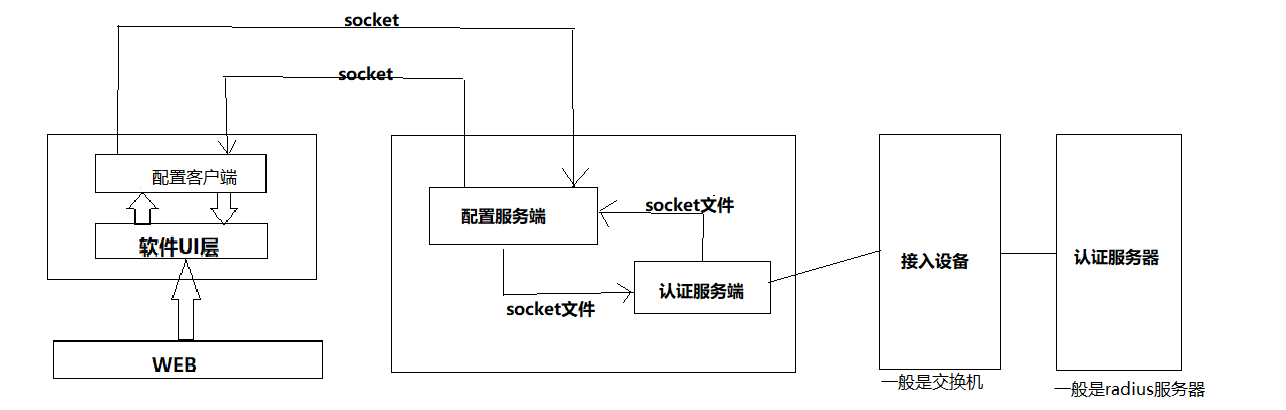
802.1X 认证

# 概述需求

在原生安卓中，Android 仅仅支持WLAN dot1x认证模式，没有集成Wired 的802.1x认证，。所以我们需要手动集成此项功能，在需求中，需要完成MD5,TLS,PEAP认证，完成客户基本需求。

# 软件结构



# 模块介绍

1.Web层

Web层用来配置文件，Web层选择认证方式后，将认证identity 和password ，ca证书路径等写入配置文件，然后通知软件UI层去调用读取。

2.软件UI层

软件UI层，是一个apk软件的上层，用来接收配置客户端消息和调度配置客户端。此软件执行uid为0，此软件执行必须是root用户下去执行，因为apk获取root后，软件仅仅能执行一次su权限，执行完一次root权限后，再无法执行，故此，我们的解决方法是：将apk加入到系统软件去执行。

3.配置客户端

软件的配置客户端，是apk软件的下层，用来和配置服务端通信的部分。基本流程如下，ui通知启动配置客户端启动，连接配置服务端。配置客户端端发送完消息后，等待接受从配置服务端发来的消息，然后将数据同步到apk上层。

4.配置服务端

配置服务端，是用来处理配置数据，并将数据发送到认证服务端所创建的sock文件接口，我们项目需求中，一般是以eth0 作为通信接口。此外，配置服务端还需要去获取认证服务端的连接状态，根据要求，如果获取到成功或者失败，将数据立即发送至配置客户端，其余状态不发送。

5.认证服务端

认证服务端，将wpa\_supplicant 通信，wpa\_supplicant启动，创建一个通信文件，比如eth0文件。在此应用中，通信接口是/data/local/tmp/eth0。

6.接入设备:

交换机，一般是H3C等带802.1x的交换机

7.认证服务器

一般是radius 服务器，市场是以freeradius ，ACS等为主要认证设备。

# 传输数据格式

MD5通信

eap=md5

name=admin

password=admin

TLS通信

eap=tls

identity=admin

ca\_cert=/data/local/tmp/ca.pem

client\_cert=/data/local/tmp/client.crt

private\_key=/data/local/tmp/client.key

private\_key\_passwd=whatever

3．TTLS通信

eap=ttls

identity=user@example.com

password=admin

anonymous\_identity=anonymous@example.com

ca\_cert=/data/local/tmp/ca.pem

4. PEAP通信

eap=peap

identity=user@example.com

password=foobar

ca\_cert=/data/local/tmp/ca.pem

# 软件通信

软件通信过程中，我们主要采用select方式实现软件异步，解决阻塞问题。

# 要点

1.wpa\_supplicant 启动时，如果上次系统非正常关闭，会留下eth0文件，如果/data/local/tmp/eth0文件存在，会造成wpa\_supplicant启动失败，所以在启动wpa\_supplicant时，需要判断/data/local/tmp/eth0是否存在，如果存在。则需要删除此文件。

2.配置服务端和配置客户端共同运行时，如果配置客户端没有关闭，配置服务端直接关闭，会造成系统time\_wait。

3.配置服务端启动时，需要判断系统中端口是否占用，如果占用，需要先杀死该端口占用的进程，否则会造成配置服务端启动失败。

4.决定此系统需不需要802.1X认证，需要在脚本中判断，如果配置服务端不启动，则系统不认证。