**Lab 4: WPA/WPA2 Enterprise (TKIP/AES +PEAP/TTLS) Network Setup**

201311211918 汪大洋

其他组员：杜蓉、任梅、汪大洋

**一、实验介绍**

The purpose of this lab is to setup a WPA/WPA2 Enterprise (TKIP/AES + EAPTTLS/PEAP) enforced wireless network using FreeRadius and OpenWRT on a WNDR3700v4 router. In addition, you will configure both Windows and Linux clients to connect to a WPA/WPA2 + Radius enabled wireless network. A basic reference for this lab can be found here:

<http://wiki.openwrt.org/doc/uci/wireless#wpa.enterprise.access.point>.

The detailed steps are as follows:

这个实验的目的是通过使用FreeRadius和OpenWRT，在WNDR3700v4路由器上设置一个WPA / WPA2企业版(TKIP / AES + EAPTTLS /PEAP)加密的无线网络。此外，您将配置Windows和Linux的客户端使其连接到一个WPA/ WPA2 +认证协议无线网络。这个实验的一个基本参考资料验可以在这里找到:

http://wiki.openwrt.org/doc/uci/wireless wpa.enterprise.access.point。

详细的步骤如下:

Section 1: Equipment List 第一部分：设备清单

Section 2: Install OpenWRT and FreeRadius 第二部分：安装openwrt和freeradius

Section 3: Configure FreeRadius 第三部分：配置freeradius

Section 4: Configure Linux Wireless Clients 第四部分：配置linux的无线客户端

Section 5: Configure Windows Wireless Clients 第五部分：配置windows的无线客户端

Section 6: Deploy a Certificate on the AP 第六部分：制作AP的证书

**二、实验过程**

**Section 1: Equipment List 第一部分：设备清单**

In this lab, every group will use the NETGEAR access point (AP) and two laptops running on Linux and/or Windows.

一个AP，一个笔记本（和实验一基本一样）。

**Section 2: Install OpenWRT and FreeRadius**

**第二部分：安装openwrt和freeradius**

Note that all the packages (including the OpenWRT firmware) are stored in the following directory (It is very important that you use the packages from this directory. Otherwise, it may not work!)

这一步的主要任务是安装OpenWRT和FreeRadius，要注意一定要安装到正确目录下，否则会出错。

flash your router with the openwrt-ar71xx-nand-wndr3700v4-ubi-factory.img.

1、在windows操作系统下重置路由器，具体过程和实验一中一样。

2、切换到fedora系统，打开终端，由于之前关了网络服务，因此要重新启动，输入：

chkconfig NetworkManger on

service NetworkManger start

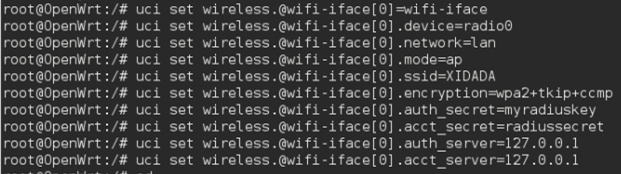
3、输入ssh 192.168.1.1，发现出错，因为路由器刷机后的RSA key要重写。编辑/root/.ssh/known\_hosts文件，将这个文件的内容都删掉。再次ssh登录，输入密码，成功登录。

4、在路由器root身份下的终端输入：opkg remove wpad-mini，再打开一个终端，在本机的身份下进入wpad安装包的目录下，输入：scp \* root@192.168.1.1:/tmp，输入密码，将安装包复制到路由器的/tmp目录下。

5、回到第一个终端，进入tmp目录，输入：opkg install \*.ipk，安装所有的安装包。

Setup a WPA2 wireless network on the router using the Web GUI or command line (uci set)

6、安装好之后进行无线网络设置，输入命令：



最后输入 uci commit wireless && wifi，确认信息。

Install the OpenSSL and FreeRadius packages on the router

7、到第二个终端（本机），把openssl和freeradius两个文件夹复制到路由器tmp目录：

scp –r openssl [root@192.168.1.1:/tmp](mailto:root@192.168.1.1:/tmp)

scp –r freeradius root@192.168.1.1:/tmp

8、回到第一个终端（路由器），进入/tmp/openssl目录，输入opkg install \*.ipk安装openssl，再进入/tmp/freeradius目录，输入opkg install \*.ipk安装freeradius，注意这个安装顺序不能错，否则安装不成功。

整个过程结束，安装完成。

**Section 3: Configure FreeRadius 第三部分：配置freeradius**

Configuring FreeRadius is the hardest part of this lab. It requires a lot of attention and patience. There are four files need to be configured for FreeRadius: clients.conf, eap.conf, radiusd.conf and users (no suffix .conf for the users file). These four files are all located in the /etc/freeradius2 directory on the router. Now, SSH login to your router as root, and go to the /etc/freeradius2 directory on the router.

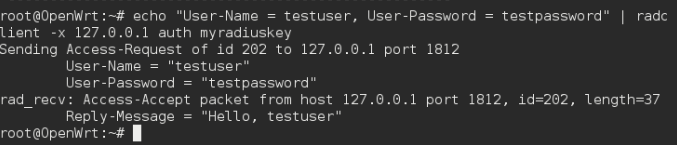
在路由器的终端下，进入/etc/freeradius2目录，按照实验要求编辑clients.conf、eap.conf、radiusd.conf 和users这四个文件，为了避免出错彻底重做，在编辑前把每个文件都备份。

一切都修改完后，输入radiusd –X，重启路由器，打开新的终端，输入：

echo "User-Name = testuser, User-Password = testpassword" | radclient -x 127.0.0.1 auth myradiuskey

可以看到正确信息，可以搜索到自己的wifi，尝试连接会发现要求输入密码。

3.1 Provide a screenshot of your radiusd running and accepting incoming an authentication request from a wireless client.



3.2 Which directory did the package freeradius-democerts\_1.0.5-1\_mipsel.ipk create?

答：freeradius2

**Section 4: Configure Linux Wireless Clients**

**第四部分：配置linux的无线客户端**

由于fedora下的配置较为复杂，因此跳过。

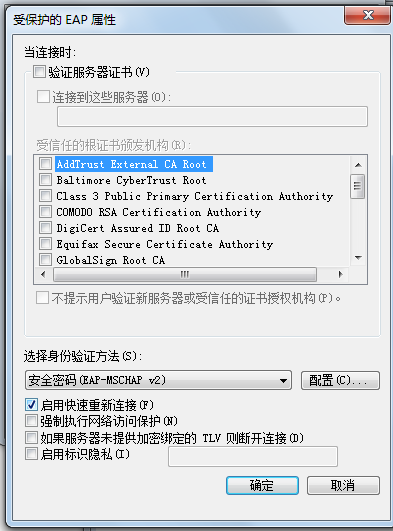
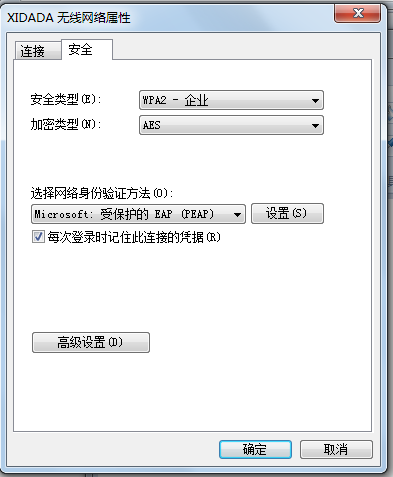
**Section 5: Configure Windows Wireless Clients**

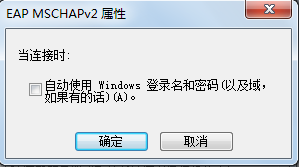
**第五部分：配置windows的无线客户端**

Open the properties of your wireless network connection on your desktop. Click the link of managing your wireless, add your wireless network and follow those instructions. Under the association tab, fill out the information. Then click on the Configuration button. Select the following options according to the figures below. Save all the settings and you are ready to connect.

1、进入windows系统，打开网络和共享中心，打开左边栏的管理无线网络，单击添加，选择手动创建网络配置文件，按照实验要求进行各项属性的配置。配置完成后关闭，可以开始连接自己的无线网络，连接时提示输入WPA密码，输入密码后连接成功。

5.1 Provide a screenshot your connection status with the network properties displayed (WPA2+AES).





输入：*cp -s /etc/init.d/radiusd /etc/rc.d/S70radiusd*

修改/etc/init.d/radius 文件中的“*radiusd -i $IPADDR -p 1812,1813 $OPTIONS”为“radiusd -i 127.0.0.1 -p 1812,1813 $OPTIONS”*

重启路由器看是否还能连接，并请第三个人来连接。

2、打开putty，正确连接路由器后，输入raidusd –X，再打开一个putty，同样连接路由器，输入cp -s /etc/init.d/radiusd /etc/rc.d/S70radiusd，并按照实验要求编辑/etc/init.d/radius文件，然后重启路由器，再次连接也成功了。

**Section 6: Deploy a Certificate on the AP 第六部分：制作AP的证书**

1、下载安装openssl的附加项：yum -y install openssl\*

go to the /usr/local/openssl/ssl/misc/etc/pki/tls/misc directory. There will a file named CA.pl. We will use this file to create the root certificate and other certificates. This creates a new root certificate in the directory /etc/pki/CA. The new root certificate file is named as cacert.pem.

2、进入路由器的/etc/pki/tls/misc目录，输入./CA.pl –newca，然后按照提示进行设置，设置完成后，在/etc/pki/CA下会看到cacert.pem文件。

3、回到/etc/pki/tls/misc目录下，输入./CA.pl –newreq，按照提示输入信息，可以发现创建了newreq.pem文件。

4、在/etc/pki/tls/misc目录下，输入openssl req -text -noout < newreq.pem，看到信息后接着输入./CA.pl –sign，然后按照提示输入信息。一切都完成后，可以在/etc/pki/tls/misc/目录下看到三个新的文件：newcert.pem、 newreq.pem (encrypted) 和 newkey.pem (unencrypted)。

5、把证书从PEM格式转换到DER格式，在CA目录下输入：

openssl x509 -in cacert.pem -inform PEM -out my-rootCA.der -outform DER

6、把文件复制到/etc/freeradius2/certs目录（路由器上），回到misc目录，输入：

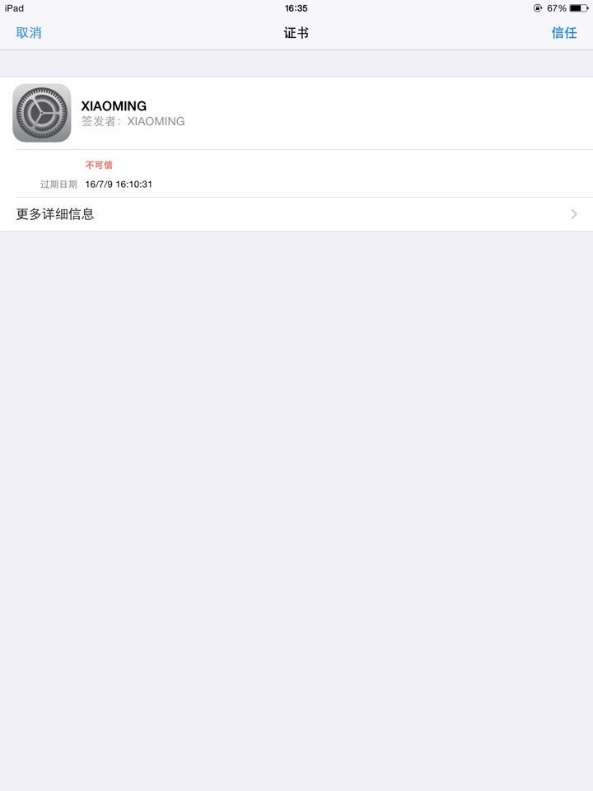
scp newcert.pem [root@192.168.1.1:/etc/freeradius2/certs](mailto:root@192.168.1.1:/etc/freeradius2/certs)

scp newkey.pem [root@192.168.1.1:/etc/freeradius2/certs](mailto:root@192.168.1.1:/etc/freeradius2/certs)

再转到CA目录下，输入：

scp cacert.pem [root@192.168.1.1:/etc/freeradius2/certs](mailto:root@192.168.1.1:/etc/freeradius2/certs)

7、再打开一个终端，登录路由器，进入/etc/freeradius2目录，按照实验要求编辑eap.conf文件。一切都设置好以后，重启路由器。用其他设备（ipad）连接自己的无线，输入用户名和密码后，可以看到有安全证书，打开后可以看到自己设置的信息。

**三、遇到的问题**

这个实验虽然内容较多，但由于做的时候很小心，所以几乎没有遇到什么问题。只是在windows连接无线的时候，一开始总是不停地弹出登录验证的窗口，重启路由器后就好了。此外，在最一开始用uci set命令设置无线信息时忘记uci commit了，导致无线信息没有重置，重新设置并commit后就可以正常看到自己的wifi了。

**四、实验体会**

1、在连接陌生wifi或浏览网页时要注意是否有安全证书以及证书是否可信。

2、做实验时wifi名字等一定要用自己设置的，不要用例子给的，否则可能会和其他组的冲突。

**五、参考资料**

1、关于RADIUS：

<http://www.docin.com/p-924116196.html>；

RADIUS的百度百科

2、证书管理机构——CA 百度百科