**EAP Test Procedure**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision | Revision History | Author | Date |
| 0.1 | Initial version | Jiaxin | 12/20/2014 |

# 预备知识

Roles:

* Ubuntu: Certificate Authority (CA) and Radius server,
* Windows PC or android phone: WIFI client.
* TP-LINK TL-WR802N: AP

Network topology:



Firstly, you should understand the following command:

* openssl req
* openssl x509
* openssl pkcs12

Then, install openssl and freeradius on Ubuntu:

* sudo apt-get install openssl
* sudo apt-get install freeradius

After that, you can continue with the following steps…

# 创建CA



生成根 CA 私钥：

openssl req -new -md5 -keyout rootkey.pem -out rootreq.pem -days 3650

生成根证书（只有公钥），并用私钥签名：

openssl x509 -req -in rootreq.pem -md5 -signkey rootkey.pem -out rootcert.pem -days 3650

(如果需要der格式：openssl x509 -in rootcert.pem -inform PEM -out rootcert.der -outform DER)

组合证书与私钥，形成 CA 根证书（包含私钥和公钥）：

cat rootcert.pem rootkey.pem > root.pem

显示根证书：

openssl x509 -text -noout -in root.pem

*(*

*如果需要创建二级 CA 私钥:*

*openssl req -new -md5 -keyout subcakey.pem -out subcareq.pem -days 3650*

*生成二级 CA 证书，并用根 CA 证书签名(在指定common name的时候一定不能和CA的common name一样):*

*openssl x509 -req -in subcareq.pem -md5 -CA root.pem -CAkey root.pem* *-CAcreateserial -out subcacert.pem -days 3650*

*组合二级 CA 证书与二级CA 私钥，形成二级 CA 证书:*

*cat subcacert.pem subcakey.pem rootcert.pem > subca.pem*

*显示二级 CA 证书:*

*openssl x509 -text -noout -in subca.pem*

*)*

\*.pem 的证书是 BASE64 形式的，要转成 PKCS12 才能装到 Windows 上（包含私钥和公钥）:

openssl pkcs12 -export -in root.pem -out root.pfx

# 使用根 CA 为 freeradius 颁发服务器证书

创建服务器证书私钥：

openssl req -new -md5 -keyout serverkey.pem -out serverreq.pem -days 3650

创建服务器证书（只有公钥），并签名(在指定common name的时候一定不能和CA的common name一样，最好为服务器IP地址或域名)：

openssl x509 -req -in serverreq.pem -md5 -CA root.pem -CAkey root.pem -CAcreateserial -out servercert.pem -days 3650

组合私钥与证书，形成服务器证书（包含私钥和公钥）：

cat servercert.pem serverkey.pem rootcert.pem > server.pem

显示服务器证书

openssl x509 -text -noout -in server.pem

(Linux上可以省略: \*.pem 的证书是 BASE64 形式的，要转成 PKCS12 才能装到 Windows 上（包含私钥和公钥）:

openssl pkcs12 -export -in servercert.pem -inkey serverkey.pem -out server.pfx 或

openssl pkcs12 -export -in servercert.pem -inkey serverkey.pem -out server.p12 或

openssl pkcs12 -export -in server.pem -out server.pfx )

# 使用根 CA 为Wifi颁发客户端证书

创建客户端证书私钥:

openssl req -new -md5 -keyout clientkey.pem -out clientreq.pem -days 3650

*req - PKCS#10 certificate request and certificate generating utility.*

*The current RsaGetPrivateKeyFromPem() implementation only support PKCS#1 private key format, which is one legacy OpenSSL ASN.1 format as denoted by*

*-----BEGIN RSA PRIVATE KEY-----*

*When we use PKCS#10 certificate request (“openssl req ….” Command) to generate the private key, the output private key will be PKCS#8 format, as denoted by*

*-----BEGIN ENCRYPTED PRIVATE KEY-----*

*If we would like to convert one PKCS#8 format to PKCS#1 format, we can use the command simply:*

* *Openssl rsa –in clientkey.pem –out clientkey2.pem*

创建客户端证书（只有公钥），并签名(在指定common name的时候一定不能和CA的common name一样):

openssl x509 -req -in clientreq.pem -md5 -CA root.pem -CAkey root.pem -CAcreateserial -out clientcert.pem -days 3650

组合私钥与证书，形成客户端证书:

cat clientcert.pem clientkey.pem root.pem > client.pem

显示客户端证书

openssl x509 -text -noout -in client.pem

\*.pem 的证书是 BASE64 形式的，要转成 PKCS12 才能装到 Windows 上（包含私钥和公钥）:

openssl pkcs12 -export -in client.pem -out client.pfx

# 验证服务器端和客户端证书：

server.pem and client.pem should be verified by CA:

* + openssl verify -CAfile root.pem server.pem
  + openssl verify -CAfile root.pem client.pem

# 部署CA,客户端证书到windows：

将root.pfx和client.pfx 复制到 Windows PC 上，将root.pfx导入IE 浏览器的受信任的根证书库，将client.pfx导入 IE 浏览器的个人证书区。

# 配置freeradius

* 配置 radiusd.conf

确认 eap 没有被注释掉 ：$INCLUDE eap.conf

修改 log 段，启用认证日志：auth = yes

* 将服务器证书 server.pem（带私钥）和根 CA 证书 rootcert.pem（不带私钥）复制到 freeradius 的certs目录下：

sudo cp /home/wujx/tianoCA02/server.pem /etc/freeradius/certs/

sudo cp /home/wujx/tianoCA02/rootcert.pem /etc/freeradius/certs/

* 需要修改/etc/freeradius/certs/的权限，否则 freeradius 不能读取证书

sudo cd /etc/freeradius/certs

sudo chmod -R ug+rwx .

* 配置 eap.conf，启用 eap-tls

cd /etc/freeradius

sudo gedit eap.conf

关键语句如下：

eap {

default\_eap\_type = tls #认证类型：tls

tls {

certdir = ${confdir}/certs #服务器证书目录

cadir = ${confdir}/certs #CA 证书目录

private\_key\_password = efi;0000 #服务器私钥密码

private\_key\_file = ${certdir}/server.pem #服务器私钥文件

certificate\_file = ${certdir}/server.pem #服务器证书文件

CA\_file = ${cadir}/rootcert.pem #CA 证书文件

}

}

* 配置 clients.conf：

cd /etc/freeradius

sudo gedit clients.conf

client 192.168.1.253/24{ #AP 地址

secret =efi;0000 #预共享密钥

shortname = EAP\_Test #AP SSID

}

* 重启 freeradius 服务:

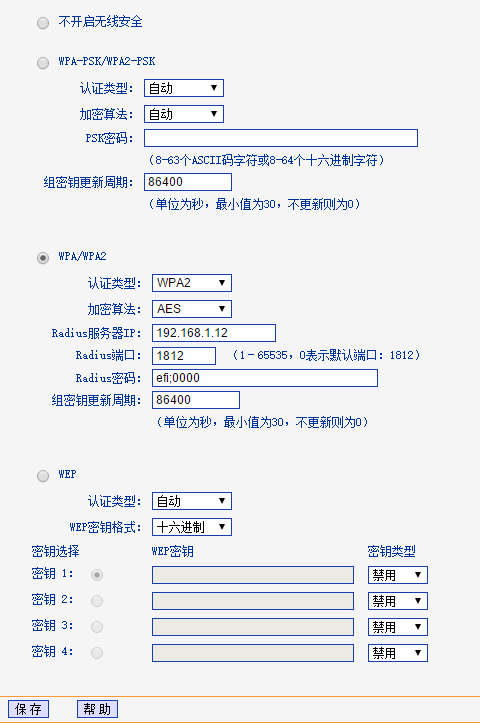
sudo service freeradius restart

如果启动失败，查看端口占用情况：sudo lsof -i :1812

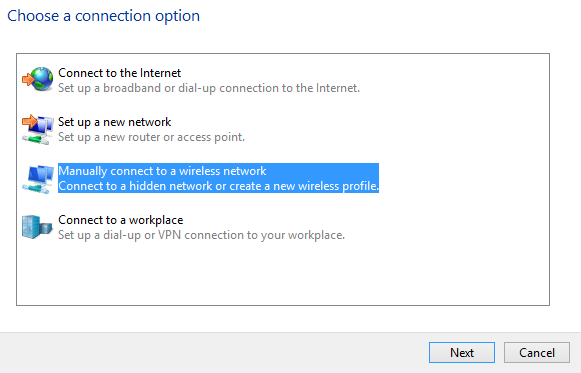
结束端口的占用（杀死进程）：sudo kill (PID Nnumber)

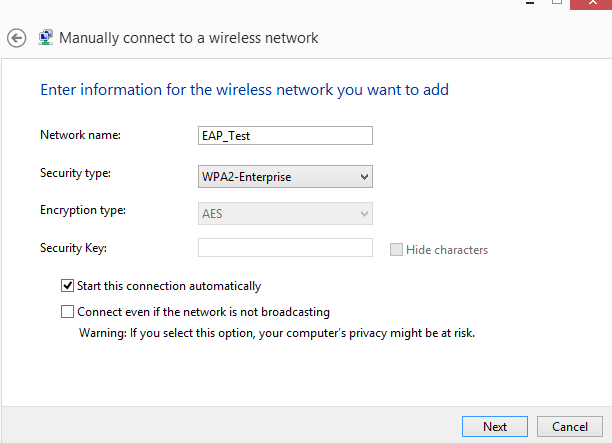
# 配置 AP

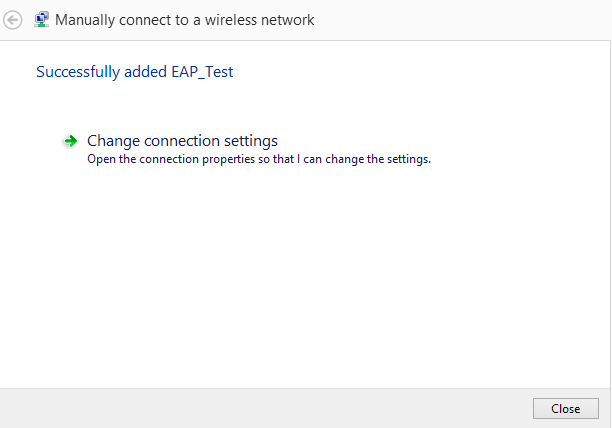


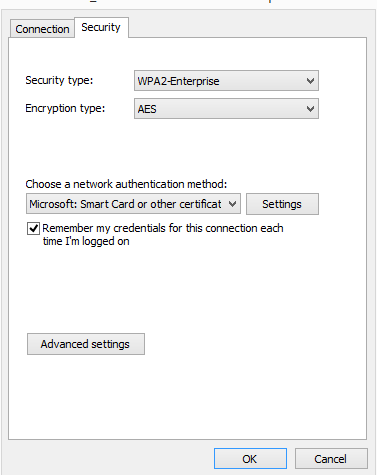


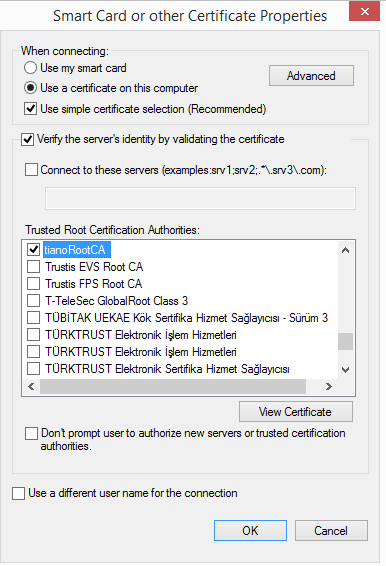
# Windows wifi 设置

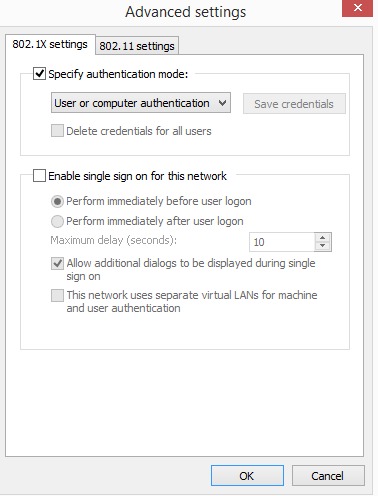












# Android wifi 设置

//TODO…

HTTPS:

用keytool创建一个证书库，里面存放服务器信任的CA证书，也就是只有这些CA签发的客户端个人证书才被服务器信任，才能通过HTTPS访问服务器。这就是“HTTPS服务器验证客户端证书”的关键配置。这里，我们假设客户端个人证书是由测试CA签发的，所以我们要把cacert.pem证书导入信任证书库：  
keytool -keystore truststore.jks -keypass efi;0000 -storepass efi;0000 -alias root -import -trustcacerts -file rootcert.pem  
   
可以用以下命令查看信任证书库内容：  
keytool -keystore truststore.jks -keypass efi;0000 -storepass efi;0000 -list –v