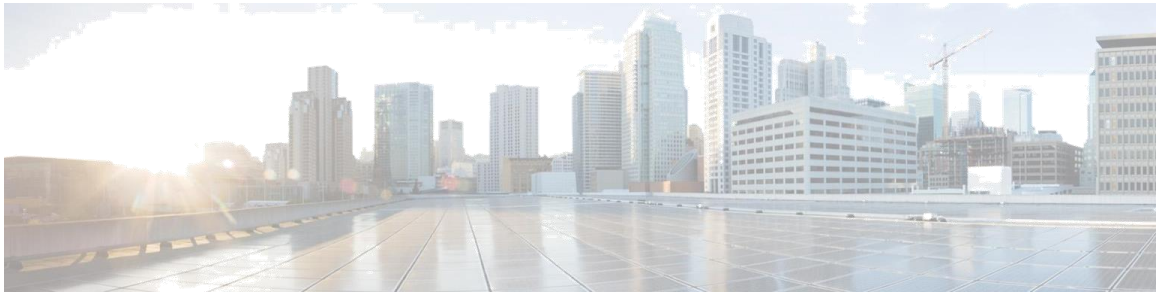


思科无线局域网 Passpoint™ 配置手册

Last Updated: August, 2013

概述

本文档的目的是提供必要的 Passpoint 相关配置实例，用于演示采用WiFi联盟Passpoint™认证的无线接入点和无线客户端的自动网络发现、选择 和连接等功能。通过使用该文档, 你可以像配置 Passpoint 1.0认证系统一样配置思科无线接入点/无线控制器。无线接入点和终端设备要求使用通过 WiFi 联盟(WiFi Alliance)Passpoint 认证的设 备。通过无线接入点支持 IEEE 802.11u协议 - 进行网络信息和其他必要信息的收集，并通过使用 ANQP (访问网络查询协议)来实现终端和网络侧信息的交互。

支持 802.11u 的手机网络发现和选择是在 预关联阶段 从 无线接入点/无线控制器 收集的信息来进行判断的。手机已经预先设置了相关的网络信息，如 Home OI(Organization Identifier)、 Domain name 和 Realm name 等信息，并保存在终端设备的配置文件里面。此外，终端设备可以从 SIM/USIM 卡上获取 IMSI 数据。

支持802.11u的无线接入点可以提供各种信息列表，热点业主的详细资料，漫游合作伙伴名单，领域列表，3GPP手机信息和域。领域列表列表还提供域名和其相关的EAP认证类型映射列表。了解这些信息对于一个电话客户端是必不可少的, 这样做可以保证正确的EAP认证交换发生。

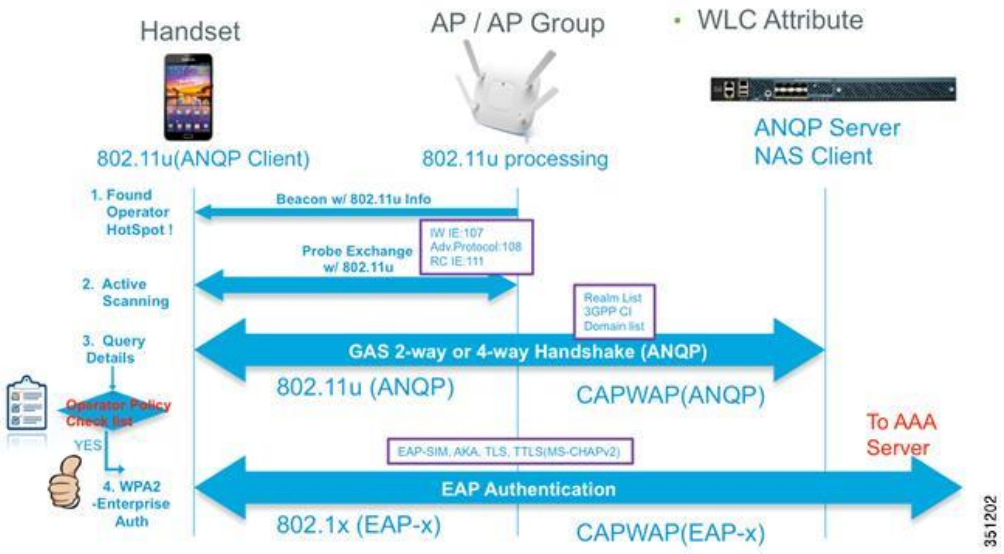
目前已经有很多设备通过了 Passpoint 的认证，包括Samsung Galaxy-S4和Intel Centrino 6230 WiFi 芯片组。本文给出的相关配置是基于终端Samsung Galaxy S4(OS v4.2.2) 。

本文档中描述的程序的显著优点是提供了一种在支持Passpoint的手机客户端设备和无线接入点之间的无缝认证手段, 这种认证可以在运营商内或跨运营商之间进行。通过这种无需干预的过程，最终用户将体验如同3G或蜂窝服务一样的网络连接。

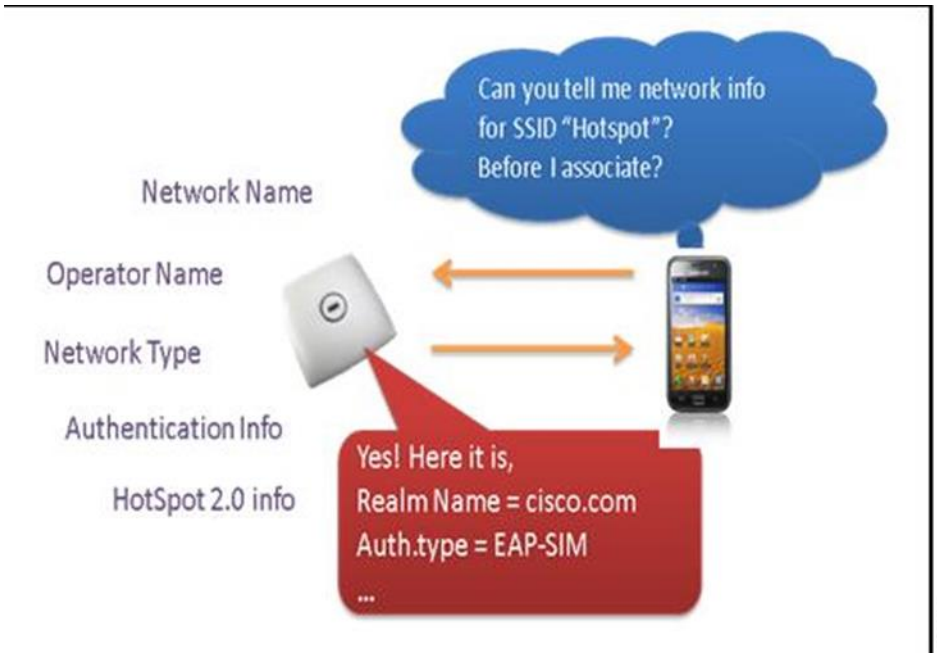
Passpoint的一个好处是加强了对于非法无线接入点的安全性。在网络发现的过程中，服务提供商的合法无线接入点会进行身份认证以便可以阻止来自非法无线接入点的电话客户端的加入。验证过程中, 无线接入点的信息会出现在特定的Passpoint装置中以防止无意的连接，如ad-hoc和其他恶意无线接入点广播的错误SSID标记。Passpoint系统介绍的其它几项技术和方法可以让企业中的WPA2安全方式更强大。GTK随机化可以用来缓解WPA2 -“hole-196”的脆弱性, 它被更广泛的应用于在公共WiFi热点屏蔽P2P流量。

本文档中描述的配置列表按顺序写明了必要的证明和测试步骤。在这个演示中，对于WLAN的配置，包括无线控制器的配置，单个和多个SSID的配置将都会涉及必要的Passpoint信息。这些额外的Passpoint信息会在信标或探针的响应信息中进行添加，这样拥有Passpoint功能的手机客户端设备可以通过检测和查询无线接入点以获取进一步的信息。在查询过程中，一种被称为ANQP(Access Network Query Protocol - 接入网络查询协议)的标准被遵循。该协议通过标准的2路或4路握手过程从无线接入点和ANQP服务器中获得足够的信息，以确定手机客户端设备可以验证和关联的最佳无线接入点。这个过程被称为GAS（Generic Advertisement Service - 通用通告服务）协议，该标准在IEEE802.11u中定义。

图 1　　基本的 Passpoint 工作行为



在查询过程中，手机客户端设备将收集更多的信息而不仅仅是SSID，如实际地点的名称，实际热点运营商的名称和领域名称，这些都将作为主要元素可用于识别其认证资格。还有许多其他的参数和信息可以用来作为标准来启动从电话客户端的移动设备的自动连接。在这份文件中，我们会涉及不同的使用情况和详细配置。



手机客户端设备通过读取信标或探针中802.11u/HotSpot 2.0关于无线接入点能力的响应来开始自动发现过程。一旦手机客户端设备识别并确定邻接无线接入点的Passpoint能力，手机客户端设备会开始一个ANQP查询以得到3GPP蜂窝信息（3GPP CI）或领域名称和域名信息。3GPP CI和领域名称将显示服务提供商列表，手机客户端装置可以以此发起认证请求。该ANQP响应还包含一个域名列表。如果场地热点中响应的无线接入点是为家庭网络或访问操作提供信息（漫游）网络，那么将会提供域名列表信息。一旦手机客户端设备收集所需的所有信息，如果手机客户端装置成功地通过自己的连接规则，该规则在Passpoint中定义的配置文件在其用户目录下，其文件名为“cred.conf”，手机客户端设备使用802.1x/EAP认证开始建立一个到无线接入点的安全连接。在这个例子中，“cred.conf”文件名是三星Galaxy S4所独有的。如果有任何其他Passpoint 1.0认证设备，它将会有一个不同的名称或格式的客户端配置文件。

需求

下面的主题包含使用思科无线接入点 /无线控制器基础设施时的设备度量，图纸，配置，和必要的Passpoint配置步骤。

Passpoint已测试设备

设备型号	支持的设备	软件	注意事项
无线局域网控制器	CT5508 WISM2 CT8510 CT7510 CT2504 vWLC	7.3.112以及更高版本	本文档基于的软件版本是7.5
无线接入点	LAP1042,	同上	同时支持本地模式和FlexConnect模式(连接模式)

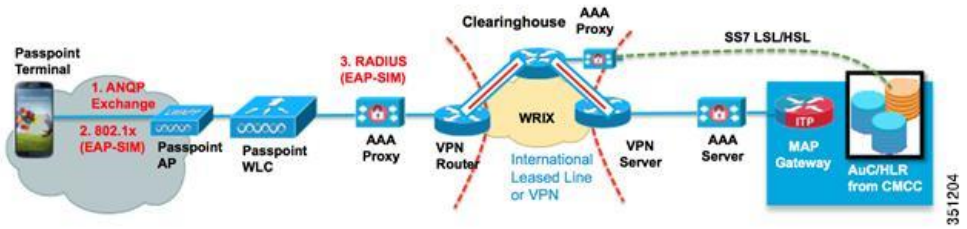
	LAP1142, CAP1602, CAP2600, CAP3502, CAP3602, CAP1552		
电话客户端设备	Samsung Galaxy-S4	默认操作系统	安卓操作系统 4.2.2

系统设计

本章介绍一些组网方式用于 Passpoint 的演示。

漫游－认证通过第三方的 Clearing House

图 2　　通过Passpoint来进行访客网络连接

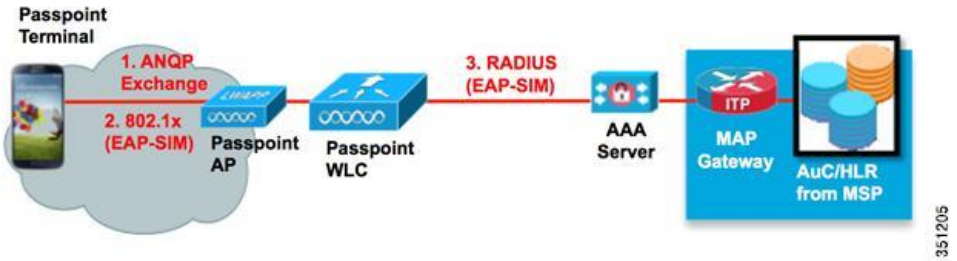


在访客网络的情况下，Passpoint配置的无线控制器通过多种方式可以获得在热点的漫游合作伙伴网络的网络信息和自己的网络信息。

Realm 名称是典型的实现方式, 一个 SSID 可以支持多个 Realm （最 多 32 个），每个 Realm 可以有不同的注册用户。如果用户有SIM卡或者主动订阅的USIM卡，用户设备可以查询3GPP。终端用户还可以通过3GPP运营商标识符来获取漫游合作伙伴的信息，该标识符是MCC（移动国家代码）和MNC（移动网络代码）组合而成。在这种类型的用户的情况下，802.11u IES（互通信息元素和漫游联盟信息元素）是最常被用到的。

本地网络的自动发现和关联（非运营商漫游）

图 3　　使用Passpoint进行家庭网络连接



本场景适用于非漫游的情况，Passpoint 主要用于多个 AP 环境下 AP 的选择过程。这个无线接入点选择过程可以提供更好的无线连接（连接的用户数量少，利用率量低的），回程速度和容量，网络服务（IPSec VPN，VOIP等等）的可用性 。在以上

的应用场景中， HS2.0 IE是最经常使用的信息。

配置

场景1–第三方clearing house

配置概述

此配置使用第三方Clearing House的私网地址。管理员可能需要配置VPN网络来连接第三方的中心网络。如果您希望快速了解该配置，可以点击 初始化无线控制器 配置手册

无线控制器配置

目前 Cisco Passpoint 的配置是基于无线控制器的架构实现的，这种架构使用无线控制器来作为集中化配置和管理无线接入点的中心。所有的配置可以通过无线控制器或 PI 来实现

配置可以通过 Console/Telnet/SSH /GUI或NMS(使用思科Prime Infrastructure 1.4及以上版本) 来实现。在本指南中，我们将使用CLI和网页的接口说明如何配置思科无线基础设施来配置Passpoint设置。

图 4　　本手册使用支持 Passpoint 的思科无线接入点/无线控制器

WLC1

```
config wlan create 2 profile_hs20 HS20_TEST
```

//此命令用于创建新的 WLAN, SSID 名为 “HS20_TEST”, INDEX 为 2

```
config wlan hotspot dot11u enable 2
```

// 此命令用于启动 802.11u 服务

```
config wlan hotspot hs2 enable 2
```

// 此命令用于启动 Hotspot20 服务

```
config wlan hotspot dot11u 3gpp-info add 1 310090 2
```

//此命令用于配置3GPP CI来做EAP-SIM认证. 为WLAN 2的本地和漫游网络添加MCC-MNC

```
config wlan hotspot dot11u roam-oi add 2 1 004096 1
```

//此命令用于在 Beacon 和 Probe response 中增加 OI (Organizational Identifier)

```
config wlan hotspot dot11u nai-realm add realm-name 2 1 realm.com
```

//此命令用于在WLAN 2上增加 Realm 的信息

```
config wlan hotspot dot11u nai-realm add eap-method 2 1 1 3
```

//此命令用于增加 EAP 的认证信息，对于每个 Realm 支持哪些 EAP 的认证类型。

```
config wlan hotspot dot11u nai-realm add eap-method 2 1 2 6
```

//此命令用于增加 EAP 的认证信息，对于每个 Realm 支持哪些 EAP 的认证类型。

```
config wlan hotspot dot11u nai-realm add auth-method 2 1 2 1 1 4
```

//此命令用于 EAP 配置 method 参数，比如是否适用 inner auth method 和 ms-chapv2

```
config wlan hotspot dot11u domain add 21 home.com
```

//为WLAN2添加域名"home.com"

```
config wlan hotspot hs2 operator-name add 2 1 "ACME-operator" eng
```

//添加操作员名字"NGH-operator "

```
config wlan enable 1
```

//激活WLAN 1

```
config radius auth add 1 192.168.1.11 1812 ascii 12345678
```

//添加RADIUS认证服务器

```
config radius acct add 1 192.168.1.11 1813 ascii 12345678
```

//添加RADIUS计费服务器

思科无线局域网基础设施支持Passpoint认证的802.11u IES和HotSpot 2.0 IES。当前的目标电话客户端会通过信标和探针的响应来检测自身的11u IE以及hotspot 2.0 IE的体验度以展开进一步的ANQP进度。如果在信标上11u和hotspot 2.0 的IE信息可以通过设备的自动连接策略，设备可以不通过ANQP步骤就进入802.1x认证流程，进而连接到一个AP上。例如，如果普通HESSID是在单一的移动域中使用，该装置不需要为位于同一地区的每个无线接入点使用ANQP查询。

(Cisco Controller) >config wlan create 2 profile_hs20 HS20_TEST

这条命令会创建一个拥有"HS20_TEST"SSID的WLAN。这个新的WLAN将会被赋予WLAN 2作为索引以方便被后期的命令所应用。SSID"HS20_TEST"在被网络管理员显示的使用命令config wlan enable 2或在网页GUI界面， 在**WLANs > Edit**启用该特性之前， 都不能传输广播

(Cisco Controller) >config wlan hotspot dot11u enable 2

这条命令为WLAN索引2开启802.11u的服务。在开启hotspot 2服务之前必须要开启802.11u服务

(Cisco Controller) >config wlan hotspot hs2 enable 1

This command will enable HotSpot2 services in WLAN index 2. 该命令会开启WLAN索引2的hotspot 2服务

(Cisco Controller) >config wlan hotspot dot11u 3gpp-info add 1 310 090 2

该命令会给WLAN索引2添加3GPP蜂窝信息；在该例子中，使用310作为移动国家代码同时将090映射到移动网络代码。MCC和MNC对于每一个运营商来说是一个唯一值，同时在手机客户端设备中可以使用UICC卡来访问。手机客户端设备将从UICC卡读取本地PLMN数，并从PLMN提取MCC /MNC信息。手机客户端设备将使用HotSpot 2.0 ANQP将其MCC / MNC数量与无线接入点的3GPP蜂窝信息进行对比，随后选择一个无线接入点发起EAP-SIM认证。

如果MNC只由两个数字组成，那么在您的配置中使用2个数字替代3个数字。例如，如果MCC/MNC是520/99，那么使用99来作为MNC的区域代码。当手机客户端设备找到一个匹配的3GPP-CI值，它将会根据EAP-SM或AKA来设置自己的配置信息。

```
(Cisco Controller) >config wlan hotspot dot11u roam-oi add 2 1 004096 1
```

这个命令将添加OI（组织识别）信息到信标和探测响应。本例中使用”004096”来作为一个例子，该值对于一个操作来说是唯一的

OI的信息会被从IEEE注册机关注册，并且可以从IEEE首页进行提交
(http://standards.ieee.org/develop/regauth/oui/public.html)

拥有一个OI值并不是一个强制性条件；它是从手机客户端设备选择另一个无线接入点的条件

```
(Cisco Controller) >config wlan hotspot dot11u nai-realm add realm-name 2 1
realm.com
```

这个命令将添加域名信息到NAI服务器列表。在该例中使用的域名是”realm.com”。一旦手机客户端装置从无线接入点使用ANQP手机域名信息，手机客户端设备将会同自己设备HS 2.0描述中的域名进行比较。域名对于每个操作员来说是唯一的，通常将 “@”分隔符后面的部分作为用户部分进行认证。一个单一的SSID可以有多个定义的域名，最大可达32个。域名在配置时不从域名列表中区分本地域名和漫游域名。

该域名将随着EAP认证类型一起发送，该信息将会作为漫游联盟的信息元素，会在下一个命令中进行定义。

```
(Cisco Controller) >config wlan hotspot dot11u nai-realm add eap-method 2 1 1 3
```

这个命令将添加EAP身份验证信息，会根据每一个域名提供EAP协议所需要的信息。这个特定的命令可以为第二WLAN索引，第一域名添加EAP-TLS协议，作为第一个EAP方法。

```
(Cisco Controller) >config wlan hotspot dot11u nai-realm add eap-method 2 1 2 6
```

这个命令将添加EAP身份验证信息，这个信息将会被根据域名给予到对应的EAP协议。这个特定的命令可以为第二WLAN索引，第一种域名索引添加EAP-TTLS协议，作为第二个方法。

```
(Cisco Controller) >config wlan hotspot dot11u nai-realm add auth-method 2 1 2 1
1 4
```

这个命令将添加认证方法的信息，将这个需要的认证信息类型给到对应的EAP协议。这个特定的命令配置MS-CHAPv2认证类型到第二WLAN索引，第一域名索引，EAP-TTLS作为EAP方法（2），第一认证索引，非EAP内部的方法（4）。

```
(Cisco Controller) >config wlan hotspot dot11u domain add 2 1 home.com
```

为本地服务提供商添加”home.com”域名。这个将会被用来确认当前无线接入点连接是属于本地网络还是漫游网络

```
(Cisco Controller) >config wlan hotspot hs2 operator-name add 2 1 "ACME-operator"
eng
```

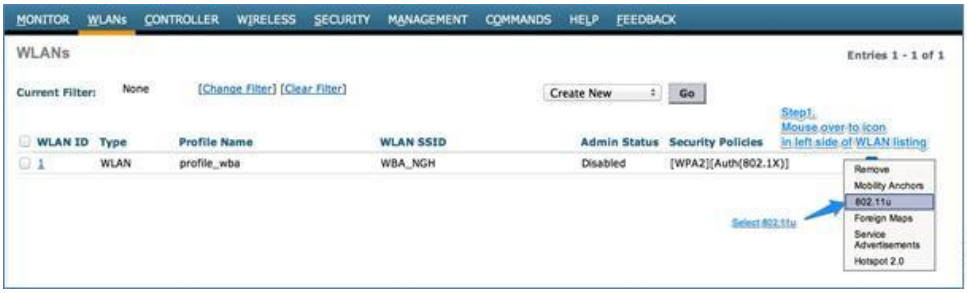
为HotSpot 2.0 IE添加操作员名字。如果管理员想添加空格字符，使用双引号标记操作者的名称字段。另外，语言代码可以是2或3字节大小。

```
(Cisco Controller) >config wlan enable 2
```

最后，通过启用WLAN来启动服务

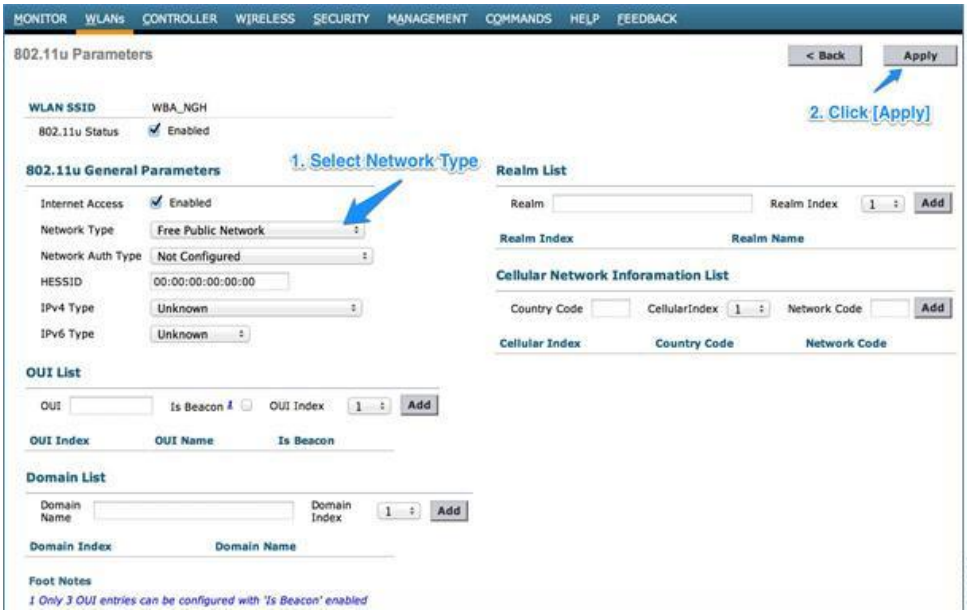
同样的，也可以使用思科无线控制器的GUI界面来完成上述配置。

步骤1 在WLANs选项卡中访问802.11u配置页面

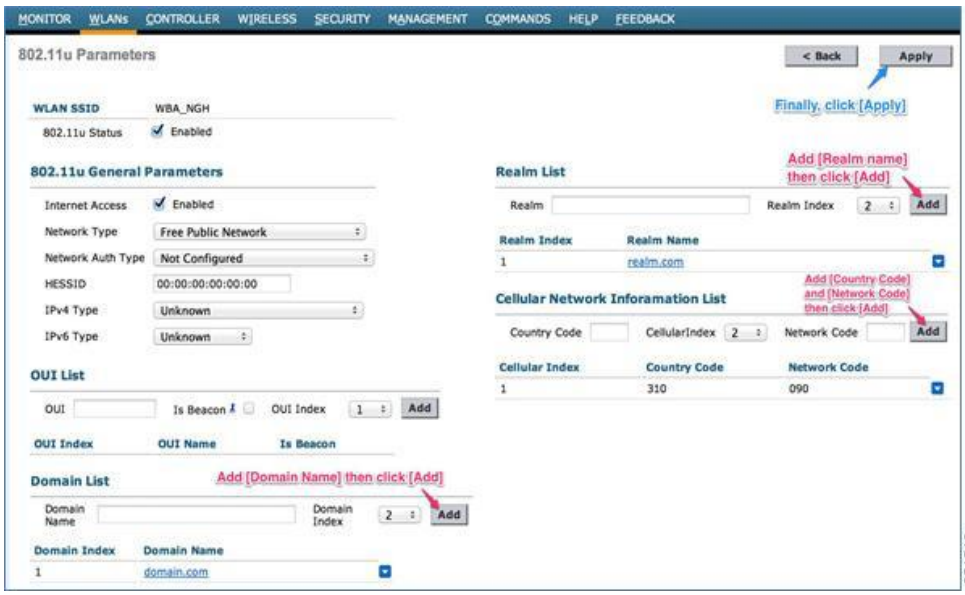


步骤2 开启802.11u

步骤3 在802.11u IE配置页面中，在802.11u General Parameters选项卡下，选择[Network Type]然后点击**Apply**

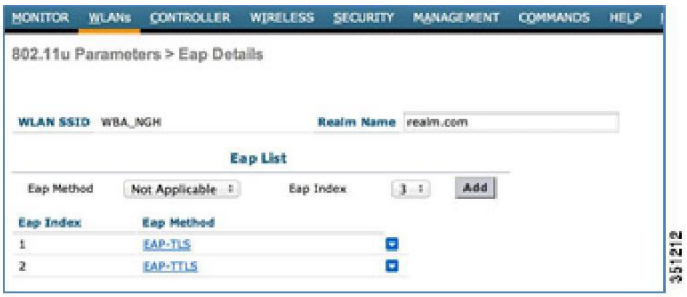


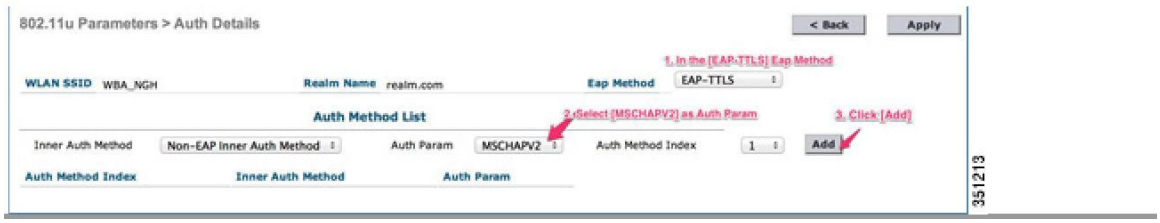
步骤4 配置3GPP CI，Realm以及Domain name信息，之后单击Apply



步骤5 为Realm配置EAP

步骤6　在802.11u GUI界面中添加EAP协议和认证类型





电话设备

我们将推荐使用 WFA Passpoint 认证过的手机终端。本文中我们将使用 Samsung-S4 作为客户端设备。终端设备通过两种方法获取网络信息。

第一个获取信息的地方是UICC卡。UICC卡拥有IMSI信息，这个信息包括一个15个数字长度的MCC和MNC。这个数字将被提取并用于3GPP CI进行比较。

可选地，管理员可以手动配置3GPP-CI 提供的手机内Passpoint配置文件。第二的位置是一个静态

的域名定义文件，位于“/storage/emulated/0”。它在默认情况下没有被保存，该cred.conf文件必须使用文本编辑器或类似工具来单独创建。目前来说，自动创建默认配置还不支持。

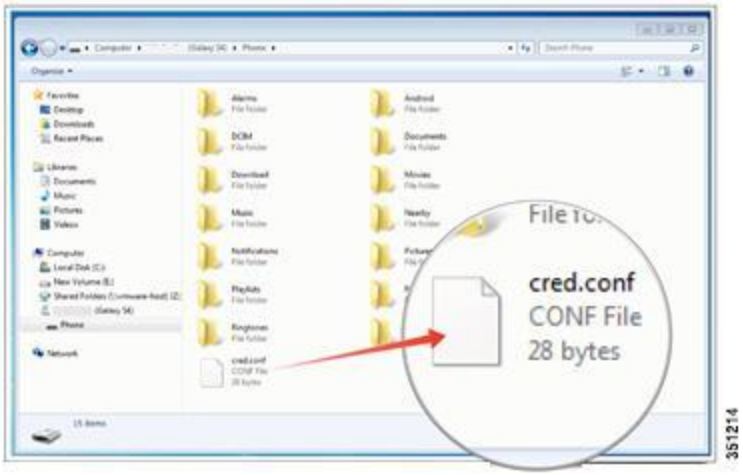
下面是一个在SGS4上一个典型的基于Passpoint/EAP-SIM的认证配置文件”cred.conf”

```
cred={
imsi= “?”
 eap=SIM
}
```

有几种方法生成此文件”cred.conf”并保存到/storage/emulated/0 目录。

方法1

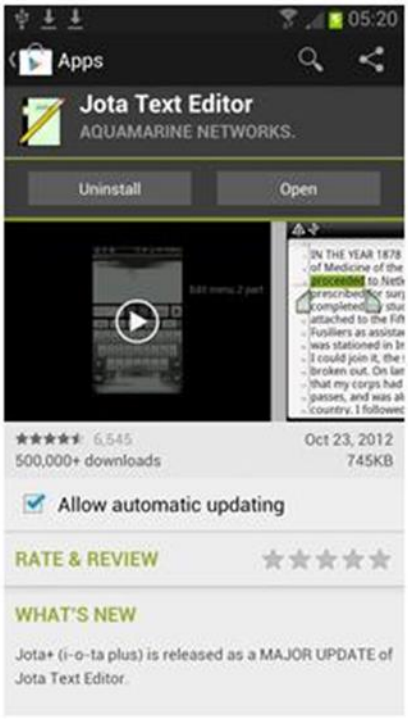
这种方法需要一台windows PC机。您必须通过USB连接电缆将电话和您的PC连接在一起。将电话配置为可移动硬盘。一旦当电话被识别，拷贝”cred.conf”到电话的根目录中。



方法2

在安卓手机上使用文本编辑器，直接在手机终端上创建”cred.conf”文件， 然后直接保存在您的手机设备上。

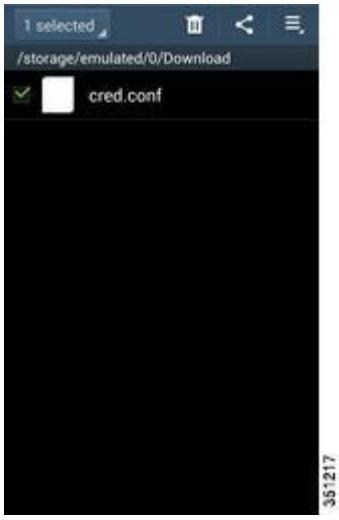
1. 到Google的”play store”上搜索文本编辑器
2. 下载” Jota Text Editor”或其他建议文本编辑器
3. 打开文本编辑器并输入在屏幕上显示的文本信息
4. 在/storage/emulated/0文件夹中保存该文件并重命名为”cred.conf”



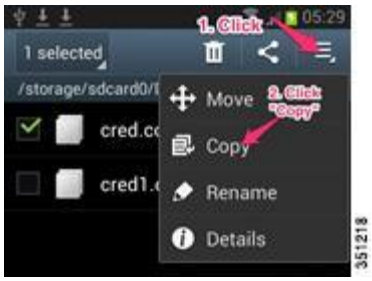
方法3

1. 在另一台设备上写一个配置文件，例如PC机或苹果笔记本，随后以”cred.conf”文件另存为。
2. 将”cred.conf”文件通过e-mail附件的方式发送到电话上。
3. 通过默认Gmail阅读器或电子邮件阅读器打开收到的邮件文件夹，单击在手机设备保存文件附件。使用默认的存储地址“/storage/emulated/0/Download”。
4. 选择”my files”应用程序

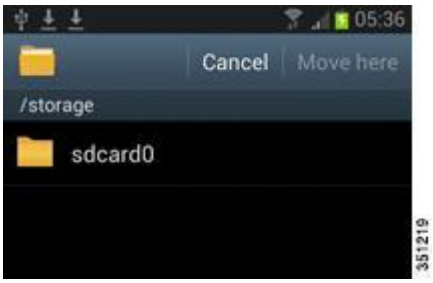
5.点击**All Files > Download**然后选择“cred.conf”.



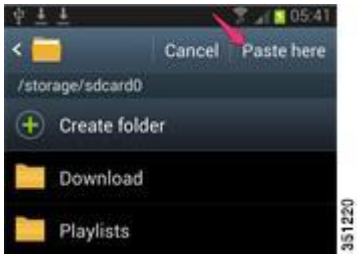
6. 点击您电话屏幕右上角的”=”图标或长按”cred.conf”文件。选择复制或移动选项



7. 选择“/storage/emulated/0”文件夹



8. 点击“Paste here”或“Move here”按钮来完成复制或移动流程



方法4

1. 同方法3，可以使用外部的编辑器来创建配置文件，并另存为”cred.conf”
2. 将文件保存到外部存储卡中（迷你SD卡）
3. 将迷你SD卡插入到电话设备中

4. 运行”my files”应用程序
5. 找到目录/extSdCard并确认”cred.conf”文件是否已经复制完成(该文件已经在步骤2中复制到外部存储卡中)。
6. 长按”cred.conf”文件直到显示copy菜单
7. 选择”copy”并粘贴文件到父目录/sdcard0

如果Passpoint系统被配置为EAP-TLS，CA证书和用户证书必须使用SD卡来进行复制。该文件还可以发送电子邮件，因为PKCS# 12 SGS4支持多个证书编码格式。推荐使用”p.12”格式的证书

场景2—不使用第三方AAA服务器的独立演示配置

本主题不包括运营商使用第三方AAA服务器的情况

使用思科CAR来配置AAA

以RADIUS电话的方式添加WLC设备

以RADUIS电话的方式来添加WLC设备

CAR

```
cd /radius/phones          // cd到RADIUS电话选项
add hs20wlc          //以RADIUS电话的方式添加无线控制器设备
cd hs20wlc/            // cd到安装目录
IPAddress = 10.11.23.102   //配置无线控制器管理IP
Sharedsecret = 思科123                                  // radius密码
save                 //保存配置
```

以远程服务器的方式定义ITP MAP网关

以远程服务器的方式定义ITP MAP网关

CAR

```
cd /Radius/RemoteServers
                                  //cd到远端AAA服务器，指向ITP MAP GW路由器

add itp1             //添加一个叫做itp1的网关
cd itp1/                                          // cd到itp 1来安装
Protocol = map-gateway    //设置协议为map-gateway
IPAddress = 10.11.24.11   //设置map-gateway的IP地址
Port = 12345
ReactivateTimerInterval = 300000
Sharedsecret = itpmap1
MaxTries = 3
Initial
Timeout =
45000 save
```

定义EAP-SIM服务

To define EAP-SIM service:

CAR

cd ..

add eap-sim

cd eap-sim

set Type eap-sim

cd RemoteServers/

add 1 itp1

save

定义基于认证的EAP-SIM域名规则

定义基于认证的EAP-SIM域名规则

CAR

```
cd /radius/Rules                    //定位到Rules目录
add sim-operator1.com               使用add命令来添加新的规则名称
set Script ExecRealmRule            //定义ExecRealm规则
cd Attributes/                      // cd到Attribute目录
Set Authentication-service eap-sim  //定义eap-sim作为认证方式
Set Authorization-service auth-local //定义local为认证方式
Set realm @sim-operator1.com        //设置域名
save                                //保存配置
```

基于认证定义EAP-SIM需要的策略

To define policy for EAP-SIM Realm based authentication基于认证定义EAP-SIM需要的策略:

CAR

```
cd /radius/Policies
add SelectPolicy                    // Added Policy 添加策略
Set Grouping sim-operator1.com      //Set grouping to the name of rules为规则设置组
save                                //save configuration保存配置
```

定义EAP-SIM订阅者

定义EAP-SIM订阅者:

CAR

```
cd /Radius/UserLists/subscribers-local  // cd到local subscriber
add 1102030405060708                // 基于IMSI添加新的用户名
set AllowNullPassword TRUE          //为EAP-SIM用户允许空密码
```

```
save                                                    //保存配置
```

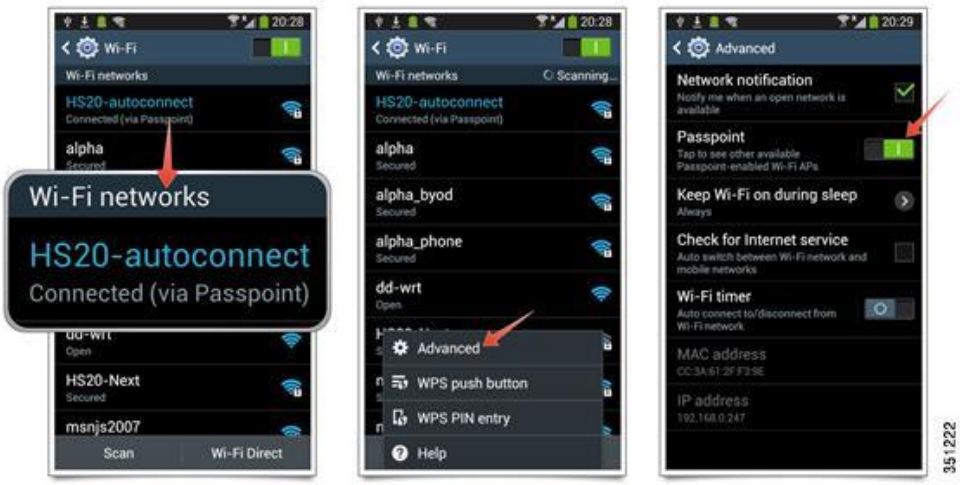
为每一个用户重复以上的步骤

无线控制器配置

和AAA Configuration using Cisco CAR配置相同，但是针对本地分配的IP地址可以不一样

电话配置

电话上 Passpoint 配置缺省是关闭的。如果需要打开，需要进入 Setting , 选择Wifi Option , 点击 Menu － (Home 左侧), 启动 Passpoint。

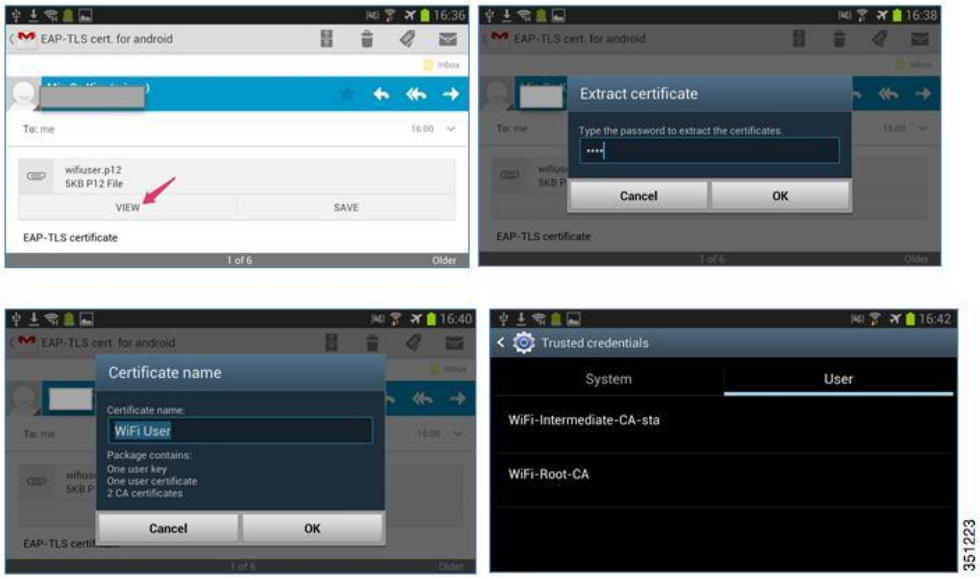


1. 根据操作员的漫游需求编辑完成“cred.conf”,并拷贝到/sdcard0/目录下。
2. 电话设备使用“cred.conf”文件来做EAP-SIM认证
3. EAP-TLS/TTLS需要预先定义证书，同时需要cred.conf文件已经包括用户的ID和密码，文件插入的方法是一样的

   实际导入的证书可以通过手动认证副本做安装或使用Gmail在您的手机导入证书

   使用手机中的Gmail

a. 把证书以附件方式发到手机注册的 Gmail 邮箱。
b. 从您的安卓手机上打开 Gmail 邮箱并读出带有证书的邮件。
c. 点击[View]
d. 如果存在证书那么输入证书口令。



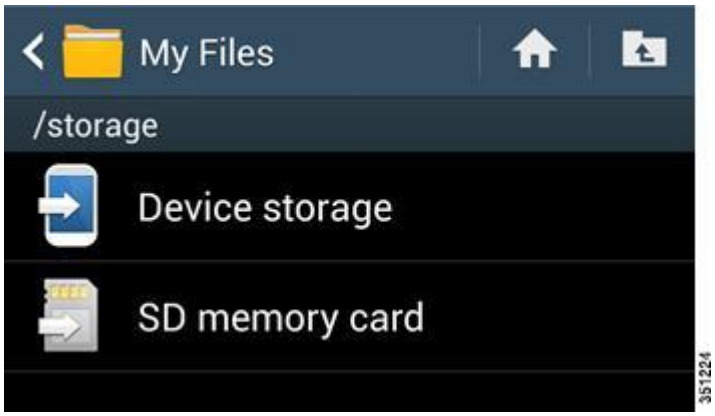
此外证书可以通过**[Settings] > [More] > [Security] > [Trusted Credential] > Select [User] Tab**的方式进行确认

e. 管理员需要使安全PIN码，如果证书是第一次加入，那么需要输入代码

使用microSD卡手动复制证书程序

这个操作可以通过外部的迷你SD卡来完成

a. 外部迷你SD卡可以通过”MyFiles”中的”SD memory card”来访问



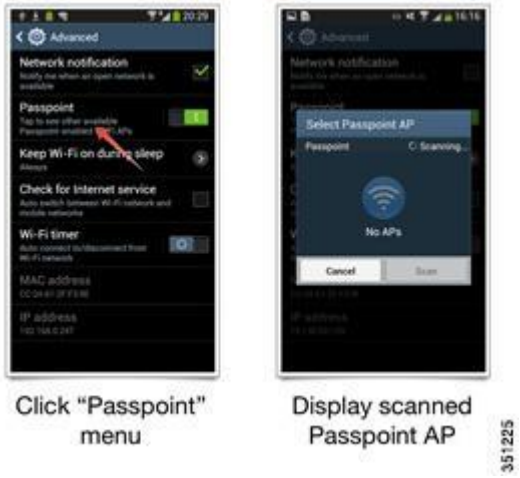
b. 选择EAP-TLS证书，将其复制到/storage/emulated/0 folder文件夹下

c. 转移到目录**[Settings] > [more] > [Security] > [Install from device storage]**

4. 一旦当所有的设置都配置完毕，打开WiFi接口。如果电话设备自动强制连接到HotSpot 2.0 无线接入点上，它将会自动运行包括在”cred.conf”中的802.1x认证程序。除非用户成功通过身份验证连接，电话设备将不显示任何特定的启用了Passpoint-enabled SSID标识符

5. 在任何时间，如果用户关闭了Passpoint特性，那么SSID的自动连接将会被断开

6. 如果您通过高级菜单点击了[Passpoint]切换菜单，那么电话设备将会显示已经扫描到的Passpoint AP



特定案例的配置手册

开启设备打开Wi-Fi无线功能

EAP-SIM的预配置案例

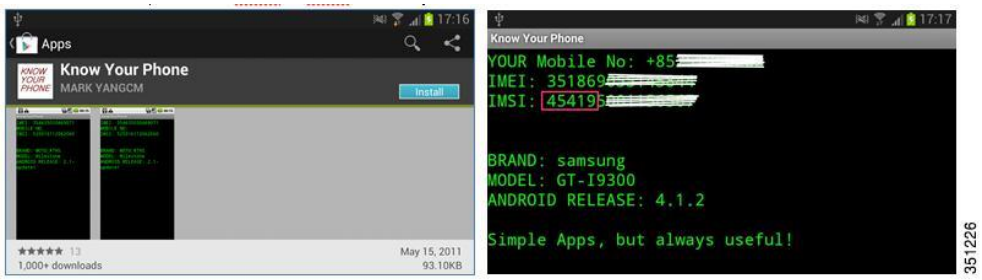
当配置电话设备时，您必须要按照如下的格式创建”cred.conf”文件

```
cred={imsi= “mncmcc-simno”
eg.domain=home.com}
cred={imsi= “19454-simno”
domain=home.com}
```

“mncmcc”部分由两位或三位数的MNC和三位数的MCC组成。在MNCMCC数字后，加上”－(DASH)simno(字符串:”simno”)。可选的，”cred.conf”文件可以用来验证漫游域的定义，该域通过比较从无线接入点过来的ANQP响应信息和电话与配置中的域名信息来验证漫游网络。如果从无线接入点域名(由ANQP查询得到的结果)与cred.conf文件的域名匹配，无线接入点将被视为内部网络。如果imsi值相同但是域名不同，这将会被认为是在访问漫游网络。MCC和MNC的序列在无线接入点/无线控制器的3GPP CI信息标签是相反的。

无线控制器

无线控制器必须知道被测试SIM卡的3GPP CI信息。要获得此信息，管理员必须加载实体电话上的IMSI读取器。IMSI读取器可以从谷歌商店中通过搜索关键字 “IMSI”来找到。搜索结果显示之后，选择” Know Your Phone”应用程序



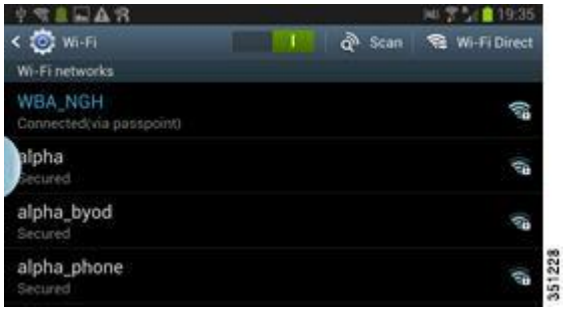
在上面的例子中，”454”被识别为移动国家代码(MNC)，同时”19”被识别为移动网络代码(MCC)。这个值可以通过在手机客户端设备的Passpoint的模块进行加载，该值将会被作为ANQP查询的结果用来和3GPP CI进行比较。

无线控制器可以配置匹配的MCC和MNC值，您可以在802.11u的配置界面中在3GPP CI选项卡中配置MCC为454、MNC为19。

通过CLI进行配置

使用命令: `(Cisco Controller) >config wlan hotspot dot11u 3gpp-info add 1 454 19 1`

一旦手机客户端设备连接成功，一个”连接”消息将通过Passpoint显示。



为EAP-AKA配置SIM

Configuration from Phone从电话端进行配置

EAP-AKA与EAP-SIM并没有太多的不同。当您从电话端进行配置时，您必须要使用如下的格式创建”cred.conf”文件

```
cred={imsi= “mncmcc-simno”

eg. eap=AKA

domain=home.com}

cred={imsi= “19454-simno”

eap=AKA

domain=home.com}
```

“mncmcc”部分由两位或三位数的MNC和三位数的MCC组成。在MNCMCC数字后，加上”－(DASH)simno(字符串:”simno”)。电话的IMSI顺序是MNC-MCC。无线控制器的11u 3GPP CI顺序是MCC-MNC。

与EAP-SIM类似，”cred.conf”文件可选的包含域定义信息，可通过比较电话中的配置信息以及从无线接入点的ANQP响应信息中包括的域名信息来验证漫游(游客）网络

EAP-TLS

通过电话端进行配置

手机客户端设备必须有预配置证书 - CA证书（如果是在测试环境中，可以使用私人CA或安卓手机上的默认CA根证书），服务器证书，证书和一个电话。安卓操作系统4.1.2版本可以支持*.p12, *.pfx and *.cer 格式的证书文件作为导入的证书。单个*.p12文件可以打包成多个证书和密钥文件

“cred.conf”文件必须采用不同类型的证书：

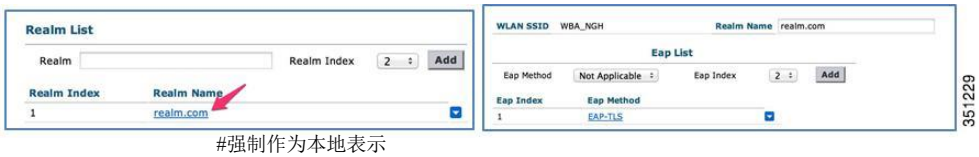
```
cred={
usernam
e="user
-name"
realm="realm.com"
domain="home.com"
ca_cert="keystore://CACERT_certificate-name-
installed"
phone_cert="keystore://USRCERT_certificate-
name-installed"
private_key="keystore://USRPKEY_privatekey-
name-used"
}
```

通过无线控制器进行配置

网络管理员可以使用同 WLC Configuration一样的配置步骤

通过GUI配置

转移至[WLANs][802.11u]安装界面



#强制作为本地表示

通过CLI配置

```
Cisco Controller) >config wlan hotspot dot11u nai-realm add realm-name 1 1
realm.com (Cisco Controller) >config wlan hotspot dot11u nai-realm add
eap-method 1 1 1 3
```

EAP-TTLS

通过电话端进行配置

手机客户端设备必须有预配置证书 - CA证书（如果是在测试环境中，可以使用私人CA或安卓手机上的默认CA根证书），服务器证书，证书和一个电话。

```
cred={
username="user-name"
password="password"
realm="realm.com"
domain="home.com" #mandatory for home identification
ca_cert="keystore://CACERT_certificate-name-installed"
```

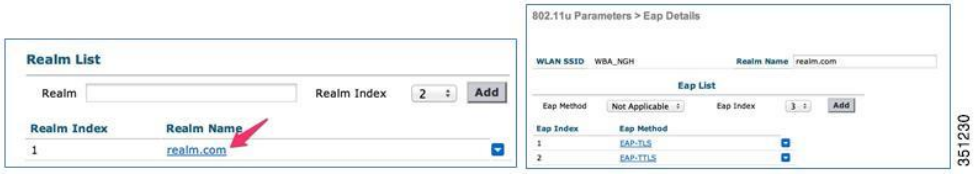
```
}
```

通过无线控制器进行配置

网络管理员可以使用同 WLC Configuration一样的配置步骤

通过GUI进行配置

转移至[WLANs][802.11u]安装界面



通过CLI进行配置

按照同 WLC Configuration一样的配置步骤完成

```
(Cisco Controller) >config wlan hotspot dot11u nai-realm add eap-method 1 1
2 6
```

//在域名中添加EAP-TTLS作为EAP-method的类型

```
(Cisco Controller) >config wlan hotspot dot11u nai-realm add auth-method 1 1
2 1 1 4
```

//在域名中添加MS-CHAPv2作为EAP-TTLS EAP-method的认证方式

非配置EAP-SIM

从电话端进行配置

在假定使用SIM卡的情况下，手机客户端设备通过SIM卡读取3GPP蜂窝信息（3GPP CI）并自动填写必要的MCC /MNC信息。手机客户端设备将使用SIM卡的信息，并与无线接入点中的3GPP CI ANQP查询信息进行比较。没有明确的或预先定义在手机客户端设备的配置文件所需的IMSI信息。如果无线接入点响应相同的3GPP CI值，手机客户端设备会自动连接EAP-SIM。因为这里没有定义任何本地域，所有的自动连接都将被认为是漫游网络

目前，手机客户端设备不从现有包中生成默认的”cred.conf”。最基本的手动配置仍然需要

以下是”cred.conf”文件所需要的内容：

```
cred={

imsi= “?”

eap=SIM

}
```

从无线控制器进行配置

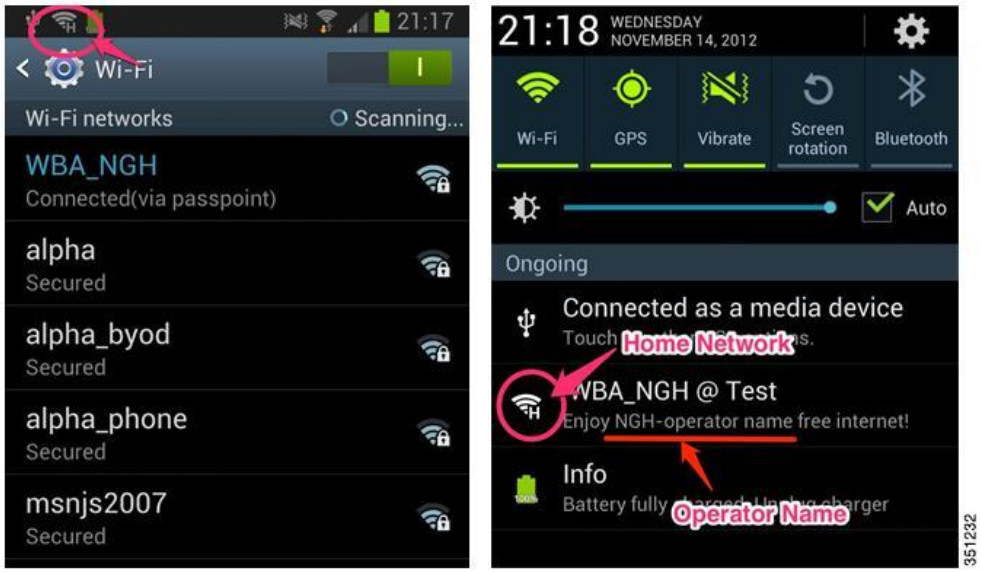
与前一篇测试案例相同 – WLC Configuration.

非配置EAP-AKA

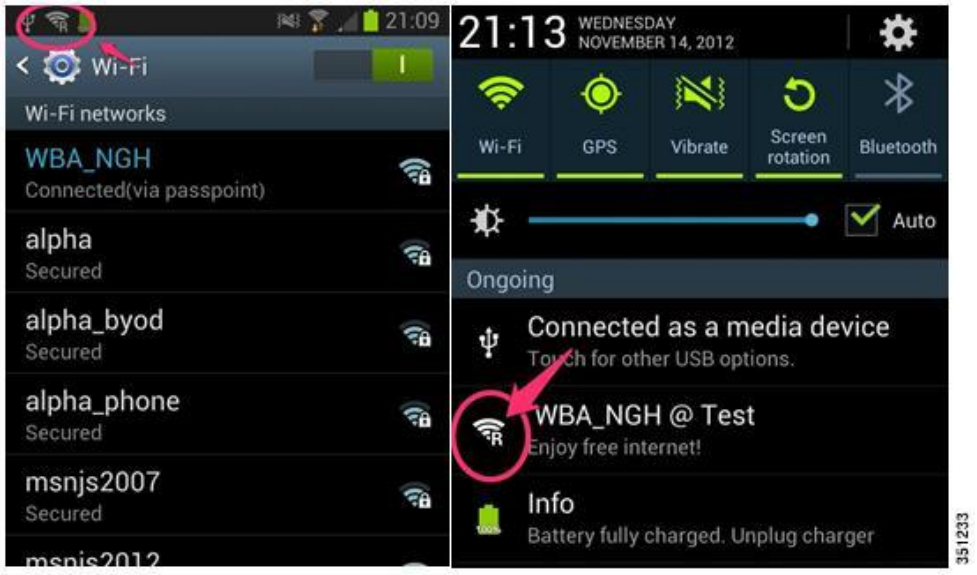
EAP-AKA和EAP-SIM的配置案例几乎类似，如下所示的EAP类型的定义是唯一的不同之处：

```
cred={
imsi= "?"
eap=AKA
}
```

本地网络连接的结果图



漫游网络连接的结果图



在访问网络上的本地网络优先级设置(不需要提供域名)

电话配置

由于不需要预配置域名，所以需要使用预先配置域名领域验证HSP或访问网络。

无线控制器配置

创建两个启用了Passpoint的SSID，在这两个SSID上配置相同的3GPP CI。您必须在其中一个SSID上定义"home.com"为指定域名，而另一个不需要配置域名。拥有"home.com"域名的SSID将会变为HSP，而另一个没有域名的SSID将会成为访问网络。

对目前话机的观察，手机客户端设备即使在HSP网络可以重新上线访问时也不会断开到访问网络的连接

调试

通过无线控制器调试命令

通过使用以下命令在无线控制器上进行调试

```
(Cisco Controller) >debug hotspot event enable
```
//显示HS2.0的事件调试信息

```
(Cisco Controller) >debug hotspot packet enable
```
//显示HS2.0的数据包调试信息

电话终端上的Debug

Step 1. 管理员需要先安装Java SDK , 然后安装DDMS.

Step 2. Android SDK 需要安装DDMS (Dalvik Debug Monitor Server)，从Android开发网站下载安装DDMS 。DDMS 是Android 的调试工具包括Android SDK。

http://developer.android.com/sdk/index.html

Step 3. 连接Samsung 终端到已安装SDK 的PC(MAC)
如果电话显示未连接，确认USB debug 选项enabled［setting][Developer options]

Step 4. 选择Phone并Enable DDMS

Step 5. 增加Filter

启动DDMS
a. Windows PC

\AppData\Local\Android\android-sdk\tools>ddms.bat
b. MACOS
/Applications/android-sdk-macosx/tools/ddms.bin

原文链接：http://www.cisco.com/en/US/docs/wireless/controller/technotes/7.5/Hotspot_057.html
翻译人：姚远
校对：谢清
翻译时间：2013年9月