目录

简介

Cisco网络服务访问登记(AR) 3.0支持小型可扩展认证协议(LEAP) (Cisco无线)。本文显示如何配置无线Aironet客户端工具和Cisco Aironet 340， 350或者1200系列接入点(AP) LEAP认证的对Cisco AR。

先决条件

要求

本文档没有任何特定的前提条件。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Aironet® 340， 350或者1200系列接入点
- AP固件11.21或以上Cisco LEAP的
- Cisco Aironet 340或350系列网络接口界面卡(NIC)
- 固件版本4.25.30或以上Cisco LEAP的
- 网络驱动程序接口技术规范(NDIS) 8.2.3或以上Cisco LEAP的
- Aironet客户端工具(ACU)版本5.02或以上
- Cisco Access Registrar 3.0或以后要求运行和验证Cisco LEAP和MAC验证请求

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置 EAP-Cisco 无线 (CISCO LEAP)

此部分包括Cisco LEAP基本配置在思科AR服务器、AP和多种客户端的。

逐步指导

遵从这些说明配置LEAP ：

1. 更换思科AR服务器的端口。AP发送关于用户数据报协议(UDP)端口1812 (验证)和1813的RADIUS信息(核算)。默认情况下因为思科AR在UDP端口1645和1646侦听，您在UDP端口1812和1813必须配置思科AR侦听。发出**cd /radius/advanced/ports**命令。发出**add 1812命令**添加端口1812。如果计划执行核算，发出**add 1813命令**添加端口1813。保存配置，然后重新启动服务。
2. 添加对思科AR服务器的AP，发出这些命令：**cd /Radius/Clients添加ap350-1cd ap350-1设置IP地址171.69.89.1设置sharedsecret cisco**
3. 要配置有线等效保密(WEP)密钥会话超时，请发出这些命令：**注意：** 802.1x指定重新验证选项。Cisco LEAP算法使用此选项超时用户的当前WEP会话密钥和发出一新的WEP会话密钥。**cd /Radius/Profiles添加ap-profilecd ap-profilecd属性设置session-timeout 600**
4. 要创建使用配置文件的用户组在步骤3添加了，发出这些命令：**cd /Radius/Usergroups添加ap-groupcd ap-group设置baseprofile ap-profile**用户在此用户组中继承配置文件和反之接收会话超时。
5. 要创建用户列表和添加的用户用户对在步骤定义的用户组4，发出这些命令：**cd /Radius/Userlists添加ap用户cd ap用户添加user1cd user1set password思科集合组ap-group**
6. 要创建本地认证和授权服务使用UserService “ap-userservice”和设置服务类型为“eap-leap”，请发出这些命令：**cd /Radius/Services添加ap-localservicecd ap-localserviceset type eap-leap设置UserService ap-userservice**
7. 要创建用户服务“ap-userservice”使用定义的用户列表在步骤5，请发出这些命令：**cd /Radius/Services添加ap-userservicecd ap-localserviceset type本地设置userlist ap-users**
8. 要设置默认验证和授权请服务思科AR使用对定义的服务在步骤6，发出这些命令：**cd /radius设置defaultauthenticationservice ap-localservice设置defaultauthorizationservice ap-localservice**
9. 要保存和重新加载配置，请发出这些命令：**保存重新加载**

在 AP上 启用 EAP-Cisco (CISCO LEAP)

逐步指导

遵从这些步骤启用在AP的Cisco LEAP ：

1. 浏览对AP。
2. 从Summary Status页，请点击**设置**。
3. 在服务菜单，请点击**Security > Authentication服务器**。
4. 选择802.1x版本运行在802.1x协议版本下拉菜单的此AP。
5. 配置思科AR的IP地址在服务器名/IP文本框的。
6. 验证下拉菜单设置为**RADIUS的**服务器类型。

7. 更换波尔特文本框到**1812**。这是使用的正确IP端口号与思科AR。
8. 配置有在思科AR使用的值的共享秘密文本框。
9. 选择**EAP Authentication复选框**。
10. 修改超时文本框，如果如此希望。这是认证请求的超时值思科AR的。
11. 点击OK键返回到Security Setup屏幕。如果也执行认为的RADIUS，请验证核算设置页的端口与在思科AR配置的端口一致(1813的集)。
12. 单击 **Radio Data Encryption (WEP)**。
13. 通过键入在WEP密钥1文本框的一40或128比特的关键值配置广播WEP密钥。
14. 选择认证类型使用。确保，最少， **Network-EAP复选框**选择。
15. 验证下拉菜单设置为**可选或全部加密的**Use of Data Encryption。可选允许使用非WEP和WEP客户端同样AP的。注意这是不安全操作模式。请使用完全加密，当可能。
16. 点击OK键完成。

配置ACU 6.00

逐步指导

遵从这些步骤配置ACU ：

1. 打开 ACU。
2. 点击工具栏的**配置文件管理器**。
3. 单击**添加**创建新配置文件。
4. 输入在文本框的配置文件名称，然后点击OK键。
5. 输入在SSID1文本框的适当的服务集标识(SSID)。
6. 点击**网络安全**。
7. 选择从网络安全类型下拉菜单的**LEAP**。
8. 单击 **Configure**。
9. 配置密码设置当必要时。
10. 单击 **Ok**。
11. 点击OK键在Network Security屏幕的。

从 Cisco AR 跟踪

发出**trace /r 5**得到在思科AR的trace输出。如果需要AP调试，您能连接到AP通过Telnet和发出**eap_diag1_on**和**eap_diag2_on**命令。

相关信息

- Cisco Access Registrar支持页面
- 技术支持和文档 - Cisco Systems