通过 SDM 的固定 ISR 上的无线认证类型配置示例

目录

简介

本文提供解释如何配置不同的层在Cisco无线集成的固定配置路由器的2认证类型与Security Device Manager的配置示例(SDM)的无线连接的。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 知识如何配置思科集成业务路由器(ISR)的基本参数与SDM
- 知识如何配置有Aironet Desktop软件的(ADU) 802.11a/b/g无线客户端适配器

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行Cisco IOS软件版本12.3(8)YI1的Cisco 877W ISR
- Cisco在ISR安装的SDM版本2.4.1
- 与Aironet Desktop软件版本3.6的笔记本电脑
- 802.11运行固件版本3.6的a/b/g客户端适配器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

Cisco SDM 是一个基于 Web 的直观设备管理工具，适用于基于 Cisco IOS 软件的路由器。Cisco SDM通过巧妙的向导简单化路由器和安全配置，帮助客户迅速和容易地配置，配置和监控Cisco系统®路由器，无需要求Cisco IOS软件命令行界面(CLI)的知识。

SDM可以从在Cisco.com的软件中心免费下载。

当在每分开的复制单个路由器或者在PC，可能也安装SDM可以独立地安装。在PC安装的思科SDM允许您使用SDM管理运行在网络的适当的IOS镜像的其他路由器。然而，在PC的SDM不支持路由器配置的重置制造默认。

本文使用在无线路由器安装的SDM配置无线验证的路由器。

思科SDM与路由器为两个目的联络：

- 访问下载的思科SDM应用文件到PC
- 读并且写入路由器配置和状态

思科SDM使用HTTP下载应用文件(sdm.tar， home.tar)到PC。HTTP和Telnet/SSH的组合用于读和写路由器配置。

支持SDM关于路由器的最新信息的参考的思科路由器和安全设备管理器Q&A和IOS软件版本。

参考请配置您的路由器支持SDM关于如何使用在路由器的思科SDM的更多信息。

参考安装SDM文件关于说明安装和下载SDM文件在路由器或在PC。

配置

本文解释如何通过SDM配置这些认证类型：

- 与WEP加密的开放式验证
- 打开与MAC验证
- 共享验证
- 802.1x/Extensible认证协议(EAP)验证
- Wi-Fi保护访问(WPA) -前共享密钥(PSK)验证
- WPA验证

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

此设置使用在无线ISR的本地RADIUS服务器验证使用802.1x验证的无线客户端。

配置SDM访问的路由器

完成这些步骤为了允许通过SDM将访问的路由器：

1. 配置访问使用解释的步骤配置您的路由器支持SDM的http/https的路由器。
2. 分配IP地址到有这些步骤的路由器：`Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#interface fastEthernet 0 Router(config-if)#ip address 10.77.244.197 255.255.255.224 % IP addresses cannot be configured on L2 links.` 在871W路由器中，您也许遇到这样错误消息。此错误消息显示快速以太网0是您不能配置任何IP地址的第2层链路。
3. 为了解决此问题，请创建第3层(VLAN)接口并且分配在同样的一个IP地址与这些步骤：`Router(config)#interface Vlan1 Router(config-if)#ip address 10.77.244.197 255.255.255.224`
4. 提供在第2层快速以太网的此VLAN与这些步骤的0个接口。本文配置快速以太网接口作为中继接口允许VLAN1。您能也配置它作为访问接口和允许在接口的VLAN1每您的网络设置。`Router(config)#interface fastEthernet 0 Router(config-if)#switchport trunk encapsulation dot1q Router(config-if)#switchport trunk allowed vlan add vlan1 !--- This command allows VLAN1 through the fast ethernet interface. !--- In order to allow all VLANs through this interface, issue the !--- switchport trunk allowed vlan add all command on this interface.`
   注意： 此示例假设，基本路由器和无线配置在路由器已经被执行。所以，下一步立刻是启动在路由器的无线应用程序配置验证参数。

启动在路由器的SDM无线应用程序

完成这些步骤为了启动无线应用程序：

1. 通过打开浏览器和输入您的路由器的IP地址开始SDM。提示您接受或拒绝如下所示:的Web浏览器安全警告窗口
2. 单击 **Yes** 以继续执行。
3. 在出现的窗口，请输入权限level_15用户名和密码为了访问路由器。此示例使用**admin**作为用

户名和密码：

4. 单击 **OK** 继续。输入同一信息，无论哪里要求。
5. 单击**是**和**OK**如适当在产生的页为了启动SDM应用程序。当SDM应用程序打开，安全警告窗口提示您接受一签字的安全证书。
6. 点击**是**接受签名证书。产生的Cisco路由器和SDM主页如下所示:
7. 在此页，请单击**配置**在顶部为了启动路由器Configure模式窗口。
8. 在Configure模式窗口，请选择**接口和连接**从出现在此页左侧的任务列。
9. 在接口和连接窗口，请点击**创建Connection选项**。这列出在路由器将配置的所有可用接口。
10. 为了启动无线应用程序，请从接口列表选择**无线**。然后，请点击**启动无线应用程序**。此屏幕画面解释步骤8， 9和10 ：这启动在多种认证类型可以配置的单独的窗口的SDM无线应用程序。SDM无线应用程序主页如下所示:注意到软件状态**禁用，**并且无线电(无线)接口的硬件状态发生故障，因为SSID在接口没有配置。其次，您配置Ssid和认证类型在此无线接口，以便无线客户端能通过此接口通信。

配置与WEP加密的开放式验证

开放式验证是空验证算法。接入点(AP)将同意验证的所有请求。开放式验证允许所有设备网络访问。如果不加密在网络启用，认识AP的SSID的所有设备能获得访问到网络。当WEP加密启用在AP，WEP密钥变为访问控制方法。如果设备没有正确WEP密钥，即使验证是成功的，设备无法通过AP传送数据。并且，它不能解密从AP发送的数据。

参考开放式验证到接入点欲知更多信息。

此示例使用这些配置参数开放式验证与WEP加密：

- SSID名称：**openwep**
- VLAN id ：**1**
- VLAN IP地址：**10.1.1.1/16**
- 此VLAN/SSID的无线客户端的DHCP地址范围：**10.1.1.5/16 - 10.1.1.10/16**

完成这些步骤为了配置与WEP的开放式验证：

1. 在无线应用程序主页，请点击**无线服务> VLAN**为了配置VLAN。
2. 选择从服务的**路由**：VLAN 页面。
3. 在服务：VLAN路由页，创建VLAN并且分配它到无线接口。这是配置窗口在无线接口的VLAN1。VLAN1本地VLAN在这里：
4. 在无线应用程序主页，请选择**无线安全> SSID管理器**为了配置SSID和认证类型。
5. 在安全：SSID管理器页，配置SSID并且分配SSID到在step1创建的VLAN为了启用在无线接口的SSID。
6. 在此页的验证设置部分下，请选择**开放式验证**。这是解释这些步骤的配置窗口：
7. 单击 **Apply**。**注意：** 对应于Open Authentication复选框的下拉框暗示另外开放式验证可以配置与几另外的认证类型，例如EAP或MAC验证。此部分讨论仅开放式验证没有新增内容(没有另外的认证类型)。
8. 配置此SSID/VLAN的WEP加密。在无线主页，请选择**无线安全>加密管理器**为了配置加密设置。在安全：加密管理器页，设置加密模式和密钥**VLAN1的**。选择**WEP加密：必须**作为加密模式。设置此VLAN的加密密钥。此部分使用这些加密密钥设置：加密密钥slot 1 ：使用作为传送密钥加密密钥大小：40 位加密密钥按十六进制值：1234567890**注意：** 应该使用同一加密密钥slot (1，在这种情况下)作为传送密钥在无线客户端。并且，无线客户端应该配置与同一关键值(1234567890在这种情况下)为了无线客户端能通信与此WLAN网络。此配置窗口解释这些

步骤：此无线安全页代表整个配置：

配置此VLAN的无线客户端的内部DHCP服务器

完成这些步骤为了配置在路由器的一个内部DHCP服务器。这可选，虽然推荐，方法分配IP地址给无线客户端。

1. 在SDM Configure模式窗口，请选择**另外的任务**在是在窗口的左边的任务列下。
2. 如此示例所显示，在**其他任务**页，请展开**DHCP**树并且选择**DHCP池**。在此页的右边显示的DHCP池列，请单击**添加**创建一个新的DHCP池。
3. 在添加DHCP池页，请指定DHCP地址池名称， DHCP地址池网络，子网掩码，开始IP地址，结束IP地址和默认路由器参数如此示例所显示：
4. 单击 **Ok**。内部DHCP服务器在路由器配置。

配置开放与MAC验证

在此种验证，只有当客户机的MAC地址在允许MAC地址下列表在认证服务器的无线客户端将允许访问WLAN网络。AP中继对一个RADIUS验证服务器的无线客户端设备的MAC地址在您的网络，并且服务器根据允许MAC地址列表检查地址。基于MAC验证来为没有EAP功能的客户端设备提供一备选认证方法。

参考MAC地址验证对网络欲知更多信息。

注意： 整个文档使用本地RADIUS服务器MAC验证、802.1x/EAP，以及WPA验证。

此示例使用这些配置参数开放与MAC验证：

- SSID名称：**openmac**
- VLAN id ：**2**
- VLAN IP地址：**10.2.1.1/16**
- 此VLAN/SSID的无线客户端的DHCP地址范围：**10.2.1.5/16 - 10.2.1.10/16**

完成这些步骤为了配置开放与MAC验证：

1. 在无线应用程序主页，请点击**无线服务> VLAN**为了配置VLAN。
2. 选择从服务的**路由**：VLAN 页面。在服务：VLAN路由页，创建VLAN并且分配它到无线接口。这是配置窗口在无线接口的**VLAN 2** ：
3. 配置MAC验证的本地RADIUS服务器。此本地RADIUS服务器将保持无线客户端的MAC地址其数据库的，并且请允许或拒绝客户端到WLAN网络根据验证结果。在无线主页，请选择**无线安全>**Server**管理器**为了配置本地RADIUS服务器。在Server Manager页，请配置IP地址、共享塞克雷和RADIUS服务器的验证和计费端口。由于它是一个本地RADIUS服务器，指定的IP地址是此无线接口地址。使用的共享密钥应该是相同的在AAA客户端配置。在本例中，共享机密是**cisco**。单击 **Apply**。把页移下来寻找默认服务器优先级部分。在此部分，请选择此RADIUS服务器(**10.2.1.1**)如此示例所显示，作为MAC验证的默认优先级服务器：为了配置AAA客户端和用户凭证，请选择**无线安全>**从无线主页的**本地RADIUS服务器**。在本地RADIUS服务器页，请点击**常规设置**。在常规设置页，请配置AAA客户端和共享密钥如显示。使用一个本地RADIUS服务器配置，服务器的IP地址和AAA客户端将是相同的。把常规设置页移下来寻找**个人用户**配置部分。在个人用户请区分，配置无线客户端的MAC地址作为用户名和密码。启用**仅MAC验证**复选框，然后单击**应用**。如此示例所显示，为了时常避免从认证失败的客户端，请指定客户端的MAC地址一个连续格式的，不用任何分离。

4. 在无线应用程序主页，请选择**无线安全> SSID管理器**为了配置SSID和认证类型。在安全：SSID管理器页，配置SSID并且分配SSID到在step1创建的VLAN为了启用在无线接口的SSID。在此页的验证设置部分下，请从对应的下拉框选择**开放式验证**和，选择**与MAC验证**。为了配置服务器优先级，请选择**自定义**在MAC下验证服务器并且选择本地RADIUS服务器**10.2.1.1的**IP地址。这是解释此步骤的示例：
5. 为了配置此VLAN的无线客户端的内部DHCP服务器，请完成在本文此VLAN部分的无线客户端的配置内部DHCP服务器解释的同样步骤与这些配置参数的：DHCP 地址池名称:VLAN 2DHCP 地址池网络:10.2.0.0子网掩码:255.255.0.0Starting IP（起始 IP 地址）：10.2.1.5Ending IP（结束 IP 地址）：10.2.1.10默认路由器：10.2.1.1

配置802.1x/EAP验证

此认证类型为您的无线网络提供最高水平安全。通过使用呼应的EAP与EAP兼容的RADIUS服务器，AP帮助一个无线客户端设备和RADIUS服务器进行相互验证和派生一把动态单播WEP密钥。RADIUS服务器发送使用它所有单播数据信号发送，或者接收，从客户端的WEP密钥对AP。

参考EAP验证对网络欲知更多信息。

注意： 有EAP验证联机几个方法。在本文中，它解释如何配置轻量级扩展身份认证协议(LEAP)作为EAP验证。LEAP使用用户名和密码作为用户凭证验证。

注意： 为了通过获取建立隧道(EAP-FAST)配置EAP灵活验证作为EAP验证类型，参考步骤的EAP-FAST版本1.02配置指南。

此示例使用这些配置参数EAP验证：

- SSID名称：**闰年**
- VLAN id ：**3**
- VLAN IP地址：**10.3.1.1/16**
- 此VLAN/SSID的无线客户端的DHCP地址范围：**10.3.1.5/16 - 10.3.1.10/16**

完成这些步骤为了配置EAP验证：

1. 重复步骤1和2 Configure开放与MAC验证为了创建和配置与这些配置参数的VLAN ：VLAN id ：3无线接口IP地址：10.3.1.1子网掩码:255.255.0.0
2. 然后，请配置客户端验证的本地RADIUS服务器。为了执行此，请重复步骤3a对Configure 3c开放与与这些配置参数的MAC验证：RADIUS服务器的IP地址：10.3.1.1共享密钥:cisco这是解释步骤2 EAP验证的配置屏幕：
3. 把页移下来寻找默认服务器优先级部分。在此部分，请选择此RADIUS服务器(**10.3.1.1**)如此示例所显示，作为EAP验证的默认优先级服务器。
4. 重复步骤3e和3f Configure打开与MAC验证。
5. 重复步骤3g和3h Configure打开与与这些配置参数的MAC验证EAP验证的：AAA客户端IP地址：10.3.1.1共享机密：cisco在个人用户部分下，请配置用户名和密码作为**user1**。
6. 在无线应用程序主页，请选择**无线安全> SSID管理器**为了配置SSID和认证类型。在安全：SSID管理器页，配置SSID并且分配SSID到在step1创建的VLAN为了启用在无线接口的SSID。在此页的验证设置部分下，请从对应的下拉框选择**开放式验证**和，选择**EAP验证**。并且，请选择**网络EAP验证**类型。为了配置服务器优先级，请选择**自定义**在EAP下验证服务器并且选择本地RADIUS服务器**10.3.1.1的**IP地址。这是解释这些步骤的示例：
7. 为了配置此VLAN的无线客户端的内部DHCP服务器，请完成在本文此VLAN部分的无线客户端的配置内部DHCP服务器解释的同样步骤与这些配置参数的：DHCP地址池名称：VLAN

3DHCP 地址池网络:10.3.0.0子网掩码:255.255.0.0Starting IP（起始 IP 地址）：10.3.1.5Ending IP（结束 IP 地址）：10.3.1.10默认路由器：10.3.1.1

8. 配置将用于动态密钥管理密码器在无线客户端的成功认证。在无线主页，请选择**无线安全>加密管理器**为了配置加密设置。在无线安全>加密在安全的管理器屏幕：加密管理器页，输入**3**集合加密模式和密钥的VLAN的。选择**密码器**作为加密模式，并且从下拉框选择密码器加密算法。此示例使用**TKIP**作为加密算法：**注意：** 使用在同一路由器的密码器加密模式当配置多次认证时在无线路由器键入通过SDM，它也许有时不是可能配置两不同的认证类型两个。在这类情况下，通过SDM配置的加密设置在路由器也许不应用。为了解决此，请通过CLI配置那些认证类型。

配置共享验证

思科提供共享密钥认证遵守IEEE 802.11b标准。

在共享密钥认证时， AP发送未加密质询文本文本字符串到该所有的设备尝试通信与AP。请求验证的设备加密质询文本并且送回它到AP。如果质询文本正确地加密， AP允许请求的设备验证。未加密挑战和已加密挑战可以是受监视。然而，这打开AP从通过比较未加密和已加密文本字符串计算WEP密钥的入侵者攻击。

参考共享密钥认证到接入点欲知更多信息。

此示例使用这些配置参数共享验证：

- SSID名称：**共享**
- VLAN id ：**4**
- VLAN IP地址：**10.4.1.1/16**
- 此VLAN/SSID的无线客户端的DHCP地址范围：**10.4.1.5/16 - 10.4.1.10/16**

完成这些步骤为了配置共享验证：

1. 重复步骤1和2 Configure开放与MAC验证为了创建和配置与这些配置参数的VLAN ：VLAN id ：4无线接口IP地址：10.4.1.1子网掩码:255.255.0.0
2. 在无线应用程序主页，请选择**无线安全> SSID管理器**为了配置SSID和认证类型。在安全：SSID管理器页，配置SSID并且分配SSID到在step1创建的VLAN为了启用在无线接口的SSID。在此页的验证设置部分下，请选择**共享验证**。这是解释这些步骤的配置屏幕：单击**Apply**。
3. 配置此SSID/VLAN的WEP加密。由于它是共享密钥认证，同一密钥使用验证。在无线主页，请选择**无线安全>加密管理器**为了配置加密设置。在安全：加密管理器页，输入**4**集合加密模式和密钥的VLAN的。选择**WEP加密：必须**作为加密模式。设置此VLAN的加密密钥。此部分使用这些加密密钥设置：加密密钥slot 1 ：使用作为传送密钥加密密钥大小：40 位加密密钥按十六进制值：1234567890**注意：** 应该使用同一加密密钥slot (1，在这种情况下)作为传送密钥在无线客户端。并且，无线客户端应该配置与同一关键值(1234567890在这种情况下)为了无线客户端能通信与此WLAN网络。此配置屏幕解释这些步骤：
4. 为了配置此VLAN的无线客户端的内部DHCP服务器，请完成解释的同样步骤配置本文此VLAN部分的无线客户端的内部DHCP服务器与这些配置参数的：DHCP地址池名称：VLAN 4DHCP 地址池网络:10.4.0.0子网掩码:255.255.0.0Starting IP（起始 IP 地址）：10.4.1.5Ending IP（结束 IP 地址）：10.4.1.10默认路由器：10.4.1.1

配置WPA验证

WPA基于标准的，严格增加存在和将来无线局域网系统的级别数据保护和访问控制的可互操作的安全增强。WPA密钥管理支持两个互相排斥的管理类型：WPA和WPA-PSK。

参考使用WPA密钥管理欲知更多信息。

使用EAP验证方法，使用WPA密钥管理，客户端和认证服务器彼此验证，并且客户端和服务器成对地生成一主密钥(PMK)。使用WPA，服务器动态地生成PMK并且通过它对AP。

此示例使用这些配置参数WPA验证：

- SSID名称：**WPA**
- VLAN id ：**5**
- VLAN IP地址：**10.5.1.1/16**
- 此VLAN/SSID的无线客户端的DHCP地址范围：**10.5.1.5/16 - 10.5.1.10/16**

完成这些步骤为了配置WPA验证：

1. 重复步骤1和2 Configure开放与MAC验证为了创建和配置与这些配置参数的VLAN ：VLAN id ：5无线接口IP地址：10.5.1.1子网掩码:255.255.0.0
2. 由于WPA是密钥管理标准，请配置将用于WPA密钥管理密码器。在无线主页，请选择**无线安全>加密管理器**为了配置加密设置。在无线安全>加密在安全的管理器屏幕：加密管理器页，输入**5**集合加密模式和密钥的VLAN的。选择**密码器**作为加密模式，并且从下拉框选择密码器加密算法。此示例使用**TKIP**作为加密算法：**注意：** 使用在同一路由器的密码器加密模式当配置多次认证时在无线路由器键入通过SDM，它也许有时不是可能配置两不同的认证类型两个。在这类情况下，通过SDM配置的加密设置在路由器也许不应用。为了解决此，请通过CLI配置那些认证类型。
3. 下一步是配置客户端验证的本地RADIUS服务器。为了执行此，请重复步骤3a对Configure 3c开放与与这些配置参数的MAC验证：RADIUS服务器的IP地址：10.5.1.1共享密钥:cisco把**Server Manager页移下来**寻找默认服务器优先级部分。在此部分，请选择此RADIUS服务器(**10.5.1.1**)如此示例所显示，作为EAP验证的默认优先级服务器：重复步骤3e和3f Configure打开与MAC验证。重复步骤3g和3h Configure打开与与这些配置参数的MAC验证EAP验证的：AAA客户端IP地址：10.5.1.1共享密钥:cisco在个人用户部分下，请配置用户名和密码作为**user2**。
4. 为了启用SSID的WPA，您需要启用开放与EAP或网络EAP在SSID。为了启用网络EAP，在无线应用程序主页，选择配置SSID和认证类型的**无线安全> SSID管理器**。在安全：SSID管理器页，配置SSID并且分配SSID到在step1创建的VLAN为了启用在无线接口的SSID。在此页的验证设置部分下，请从对应的下拉框选择**开放式验证**和，选择**EAP验证**。并且，请选择**网络EAP验证**类型。为了配置服务器优先级，请选择**自定义**在EAP下验证服务器并且选择本地RADIUS服务器**10.5.1.1的**IP地址。这是解释这些步骤的示例：
5. 把SSID管理器页移下来寻找**验证密钥管理**部分。
6. 在此部分，请从密钥管理下拉框选择**必须**，并且启用**WPA**复选框。这是解释这些步骤的配置窗口：
7. 单击 **Apply**。
8. 为了配置此VLAN的无线客户端的内部DHCP服务器，请完成解释的同样步骤配置本文此VLAN部分的无线客户端的内部DHCP服务器与这些配置参数的：DHCP 地址池名称:VLAN5DHCP 地址池网络:10.5.0.0子网掩码:255.255.0.0Starting IP（起始 IP 地址）：10.5.1.5Ending IP（结束 IP 地址）：10.5.1.10默认路由器：10.5.1.1

配置WPA-PSK验证

另一个WPA密钥管理类型呼叫WPA-PSK。WPA-PSK用于支持在基于802.1X的验证不是可用的无线局域网的WPA。使用此类型，您必须配置在AP的一预先共享密钥。您能输入预先共享密钥作为ASCII或十六进制字符。如果输入密钥作为ASCII字符，您输入在8个和63个字符之间，并且AP扩展密钥使用在基于密码的加密算法标准描述的进程(RFC2898)。如果输入密钥作为十六进制字符，您必须输入64十六进制字符。

此示例使用这些配置参数WPA-PSK验证：

- SSID名称：**WPA-PSK**
- VLAN id ：**6**
- VLAN IP地址：**10.6.1.1/16**
- 此VLAN/SSID的无线客户端的HCP地址范围：**10.6.1.5/16 - 10.6.1.10/16**

完成这些步骤为了配置WPA-PSK ：

1. 重复步骤1和2 Configure开放与MAC验证为了创建和配置与这些配置参数的VLAN ：VLAN id ：6无线接口IP地址：10.6.1.1子网掩码:255.255.0.0
2. 由于WPA-PSK是密钥管理标准，请配置将用于WPA密钥管理密码器。在无线主页，请选择**无线安全>加密管理器**为了配置加密设置。在安全的**无线安全>加密管理器窗口上**：加密管理器页，输入**6**集合加密模式和密钥的VLAN的。选择**密码器**作为加密模式，并且从下拉框选择密码器加密算法。此示例使用**TKIP+WEP 128bit**作为加密算法。**注意：** 使用在同一路由器的密码器加密模式当配置多次认证时在无线路由器键入通过SDM，它也许有时不是可能配置两不同的认证类型两个。在这类情况下，通过SDM配置的加密设置在路由器也许不应用。为了解决此，请通过CLI配置那些认证类型。
3. 为了启用SSID的WPA-PSK，您需要启用在SSID的开放式验证。为了启用开放式验证，请重复步骤6与WEP加密的Configure开放式验证。这是配置窗口WPA-PSK ：
4. 把SSID管理器页移下来寻找**验证密钥管理**部分。
5. 在此部分，请从密钥管理下拉框选择**必须**，启用**WPA**复选框并且输入在ASCII或十六进制格式的WPA预先共享密钥。此示例使用ASCII格式。应该使用同一个格式在客户端配置。这是解释步骤5的配置窗口：用于此配置的WPA预先共享密钥是1234567890。
6. 单击 **Apply**。
7. 为了配置此VLAN的无线客户端的内部DHCP服务器，请完成解释的同样步骤配置本文此VLAN部分的无线客户端的内部DHCP服务器与这些配置参数的：DHCP 地址池名称:VLAN 6DHCP 地址池网络:10.6.0.0子网掩码:255.255.0.0Starting IP（起始 IP 地址）：10.6.1.5Ending IP（结束 IP 地址）：10.6.1.10默认路由器：10.6.1.1

无线客户端配置

在您通过SDM后配置ISR，您需要配置不同的认证类型的无线客户端，以便路由器能验证这些无线客户端和提供存取对于WLAN网络。本文使用ADU客户端配置。

配置开放式验证的无线客户端与WEP加密

完成这些步骤：

1. 在 ADU 上的“Profile Management”窗口中，单击 **New** 以创建一个新配置文件。新窗口显示您能设置开放式验证的地方配置。
2. 在“General”选项卡下，输入客户端适配器将使用的配置文件名称和 SSID。在本例中，配置文件名称和SSID是**openwep**。**注意：** SSID在开放式验证的ISR必须匹配该的SSID您配置。

3. 点击**安全选项卡**并且留下安全选项作为预先共享密钥(静态WEP) WEP加密的。
4. 如此示例所显示，单击**配置**并且定义了预先共享密钥：
5. 单击在配置文件管理页和集合802.11认证模式的**高级选项卡。**如**开放**为开放式验证。
6. 为了验证开放与WEP身份验证，请激活配置的**openwep** SSID。
7. 验证无线客户端用路由器顺利地关联。这可以从使用**show dot11 associations命令的**无线路由器详细验证。示例如下：`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [openwep] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.1.1.5 CB21AG/PI21AG client self Assoc Others: (not related to any ssid)`

配置开放的无线客户端与MAC验证

完成这些步骤：

1. 在 ADU 上的“Profile Management”窗口中，单击 **New** 以创建一个新配置文件。新窗口显示您能设置开放式验证的地方配置。
2. 在“General”选项卡下，输入客户端适配器将使用的配置文件名称和 SSID。在本例中，配置文件名称和SSID是**openmac。注意：** SSID在开放式验证的ISR必须匹配该的SSID您配置。
3. 点击**安全选项卡**并且留下安全选项作为**无**开放的与MAC验证。然后，单击**OK**。
4. 为了验证开放与MAC验证，请激活配置的**openmac** SSID。
5. 验证无线客户端用路由器顺利地关联。这可以从使用**show dot11 associations命令的**无线路由器详细验证。示例如下：`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [openmac] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.2.1.5 CB21AG/PI21AG client1 self MAC-Assoc SSID [openwep] : Others: (not related to any ssid)`

配置802.1x/EAP验证的无线客户端

完成这些步骤：

1. 在 ADU 上的“Profile Management”窗口中，单击 **New** 以创建一个新配置文件。新窗口显示您能设置开放式验证的地方配置。
2. 在“General”选项卡下，输入客户端适配器将使用的配置文件名称和 SSID。在本例中，配置文件名称和SSID是**闰年。注意：** SSID在802.1x/EAP验证的ISR必须匹配该的SSID您配置。
3. 在配置文件管理下，请点击**安全选项卡**，设置安全选项作为**802.1x**并且选择适当的EAP类型。本文使用**LEAP**作为EAP类型验证。
4. 单击**配置**为了配置LEAP用户名和密码设置。在用户名和密码设置下，此示例选择**手工提示输入用户名和密码，**以便将提示客户端输入正确用户名和密码，当尝试连接到网络时。
5. 单击 **Ok**。
6. 为了验证EAP验证，请激活配置的**闰年**SSID。提示您输入LEAP用户名和密码。进入凭证作为**user1**并且点击OK键。
7. 验证无线客户端顺利地验证并且分配用IP地址。这可以清楚地验证从ADU状态窗口。这是从路由器的CLI的等同的输出：`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [leap] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.3.1.5 CB21AG/PI21AG client2 self EAP-Assoc SSID [openmac] : SSID [openwep] : Others: (not related to any ssid)`

配置共享验证的无线客户端

完成这些步骤：

1. 在 ADU 上的“Profile Management”窗口中，单击 **New** 以创建一个新配置文件。新窗口显示您能设置开放式验证的地方配置。
2. 在“General”选项卡下，输入客户端适配器将使用的配置文件名称和 SSID。在本例中，配置文件名称和SSID**共享**。**注意：** SSID在开放式验证的ISR必须匹配该的SSID您配置。
3. 点击**安全选项卡**并且留下安全选项作为预先共享密钥(静态WEP) WEP加密的。然后，请单击**配置**。
4. 如此示例所显示，定义预先共享密钥：
5. 单击 **Ok**。
6. 在配置文件管理下，请单击**高级选项卡。**和集合802.11认证模式如**共享**为共享验证。
7. 为了验证共享验证，请激活配置的**共享**SSID。
8. 验证无线客户端用路由器顺利地关联。这可以从使用**show dot11 associations命令的**无线路由器详细验证。示例如下：`Router#show dot11 associations 802.11 Client Stations on Dot11Radio0: SSID [shared] : MAC Address IP address Device Name Parent State 0040.96ac.e657 10.4.1.5 CB21AG/PI21AG WCS self Assoc`

配置WPA验证的无线客户端

完成这些步骤：

1. 在 ADU 上的“Profile Management”窗口中，单击 **New** 以创建一个新配置文件。新窗口显示您能设置开放式验证的地方配置。
2. 在“General”选项卡下，输入客户端适配器将使用的配置文件名称和 SSID。在本例中，配置文件名称和SSID是**WPA**。**注意：** SSID在WPA (与EAP)验证的ISR必须匹配该的SSID您配置。
3. 在配置文件管理下，请点击**安全选项卡**，设置安全选项作为**WPA/WPA2/CCKM**并且选择适当的WPA/WPA2/CCKM EAP类型。本文使用**LEAP**作为EAP类型验证。
4. 单击**配置**为了配置LEAP用户名和密码设置。在用户名和密码设置下，此示例选择**手工提示输入用户名和密码，**以便将提示客户端输入正确用户名和密码，当尝试连接到网络时。
5. 单击 **Ok**。
6. 为了验证EAP验证，请激活配置的闰年SSID。提示您输入LEAP用户名和密码。进入两个凭证作为**user2**，然后点击OK键。
7. 验证无线客户端顺利地验证并且分配用IP地址。这可以清楚地验证从ADU状态窗口。

配置WPA-PSK验证的无线客户端

完成这些步骤：

1. 在 ADU 上的“Profile Management”窗口中，单击 **New** 以创建一个新配置文件。新窗口显示您能设置开放式验证的地方配置。
2. 在“General”选项卡下，输入客户端适配器将使用的配置文件名称和 SSID。在本例中，配置文件名称和SSID是**WPA-PSK**。**注意：** SSID在WPA-PSK验证的ISR必须匹配该的SSID您配置。
3. 在配置文件管理下，请点击**安全选项卡**并且设置安全选项作为**WPA/WPA2 Passphrase**。然后，请单击**配置**为了配置WPA Passphrase。
4. 定义WPA预先共享密钥。密钥应该是长度8个到63个ASCII字符。然后，单击**OK**。
5. 为了验证WPA-PSK，请激活配置的**WPA-PSK** SSID。
6. 验证无线客户端用路由器顺利地关联。这可以从使用**show dot11 associations命令的**无线路由器详细验证。

故障排除

目前没有针对此配置的故障排除信息。

故障排除命令

可使用以下 **debug** 命令对配置进行故障排除。

- **调试全dot11 aaa的验证器**激活MAC和EAP验证数据包调试。
- **debug radius authentication** —显示在服务器和客户端之间的RADIUS协商。
- **debug radius local-server packets** —显示被发送并且接收RADIUS信息包的内容。
- **debug radius local-server client** —显示关于失败的客户端验证的错误消息。

相关信息

- 无线局域网控制器认证的配置示例
- 配置 VLAN
- 带内部DHCP和开放式认证的1800 ISR无线路由器配置示例
- Cisco无线ISR和HWIC访问接入节点配置指南
- 无线局域网连接使用与WEP加密和LEAP认证配置示例的一个ISR
- 配置身份验证类型
- 无线局域网连接使用与WEP加密和LEAP认证配置示例的一个ISR
- 技术支持和文档 - Cisco Systems