在RV320 VPN路由器、WAP321 Wireless-N接入点和Sx300系列交换机上启用多个无线网络

目标

在不断变化的业务环境中，您的小型企业网络必须具有强大、灵活、可访问且高度可靠的特性，尤其是当增长是首要任务时。无线设备的普及率呈指数级增长，这并不令人意外。无线网络具有成本效益、易于部署、灵活、可扩展和移动性，可无缝地提供网络资源。身份验证允许网络设备验证并保证用户的合法性，同时保护网络免受未授权用户的侵扰。部署安全且可管理的无线网络基础设施非常重要。

Cisco RV320双千兆WAN VPN路由器为您和您的员工提供可靠、高度安全的接入连接。支持单点设置的Cisco WAP321 Wireless-N可选频段接入点支持千兆以太网的高速连接。网桥以无线方式将LAN连接在一起，使小型企业更容易扩展其网络。

本文提供在思科小型企业网络中启用无线接入所需的配置的分步指导，包括虚拟局域网(VLAN)路由、多服务集标识符(SSID)以及路由器、交换机和接入点上的无线安全设置。

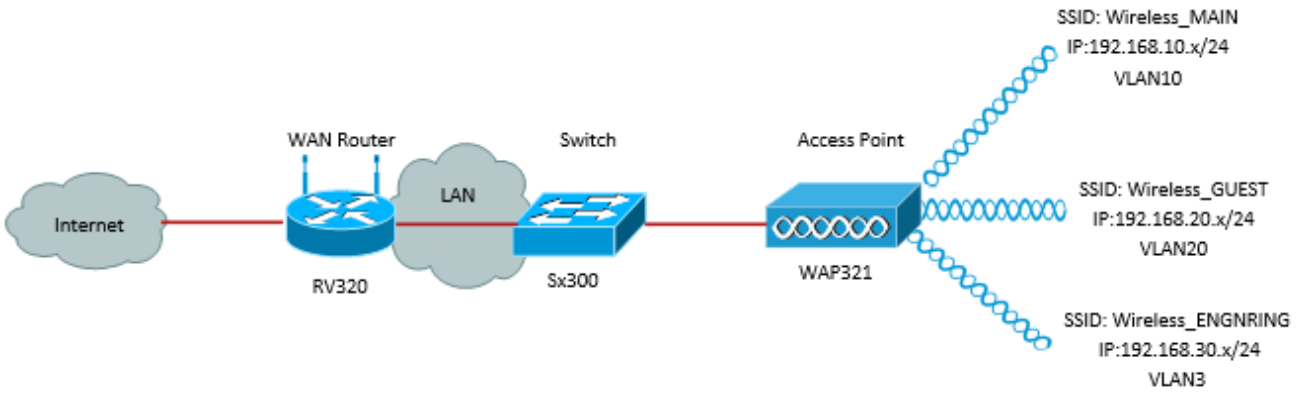
适用设备

·RV320 VPN路由器
· WAP321 Wireless-N接入点
· Sx300系列交换机

软件版本

·1.1.0.09(RV320)
· 1.0.4.2(WAP321)
· 1.3.5.58(Sx300)

网络拓扑



上图显示了使用多个SSID和思科S系列WAP、交换机和路由器进行无线接入的示例实施。WAP连接到交换机，并使用中继接口传输多个VLAN数据包。交换机通过中继接口连接到WAN路由器，WAN路由器执行VLAN间路由。WAN路由器连接到Internet。所有无线设备都连接到WAP。

主要特点

将Cisco RV路由器提供的VLAN间路由功能与小型企业接入点提供的无线SSID隔离功能相结合，可为任何现有思科小型企业网络的无线接入提供简单而安全的解决方案。

VLAN 间路由

不同VLAN中的网络设备无法与每台设备通信，而没有路由器在VLAN之间路由流量。在小型企业网络中，路由器对有线和无线网络执行VLAN间路由。当为特定VLAN禁用VLAN间路由时，该VLAN中的主机将无法与另一VLAN中的主机或设备通信。

无线SSID隔离

无线SSID隔离有两种类型。启用无线隔离（在SSID内）后，同一SSID上的主机将无法看到彼此。启用无线隔离（在SSID之间）后，一个SSID上的流量不会转发到任何其他SSID。

IEEE 802.1x

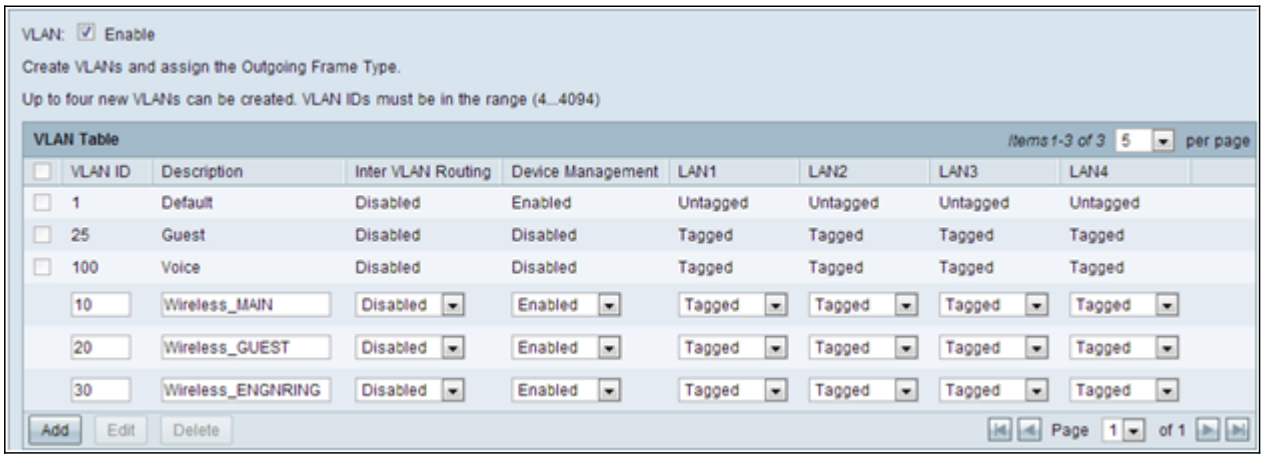
IEEE 802.1x标准指定了用于实施基于端口的网络访问控制的方法，该方法用于向以太网网络提供经过身份验证的网络访问。基于端口的身份验证是仅允许凭证交换通过网络的过程，直到连接到端口的用户通过身份验证。在凭证交换期间，该端口称为非受控端口。该端口在身份验证完成后称为受控端口。这基于单个物理端口中存在的两个虚拟端口。

这使用交换LAN基础设施的物理特征对连接到LAN端口的设备进行身份验证。如果身份验证过程失败，则可拒绝对端口的访问。此标准最初设计用于有线以太网，但已经适用于802.11无线LAN。

RV320配置

在此场景中，我们希望RV320充当网络的DHCP服务器，因此我们需要设置该服务器并在设备上配置单独的VLAN。要开始，请通过连接到以太网端口之一并转到192.168.1.1（假设您尚未更改路由器的IP地址）登录路由器。

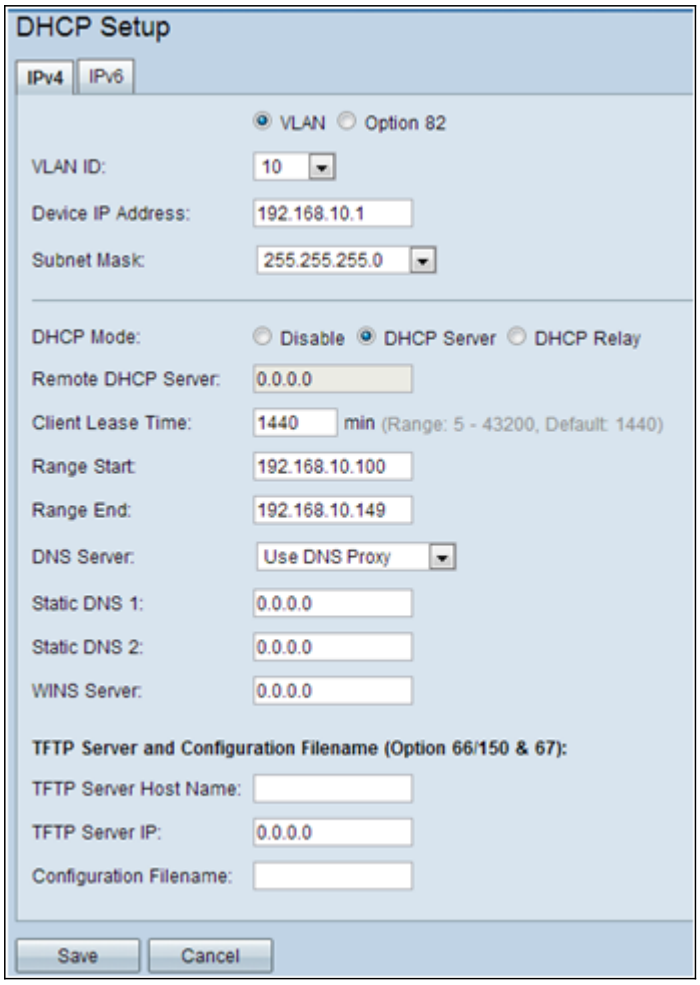
步骤1.登录Web配置实用程序，然后选择Port Management **> VLAN Membership**。将打开新页面。我们创建3个单独的VLAN来代表不同的目标受众。单击**Add**添加新行并编辑VLAN ID和说明。您还需要确保在需要传输的任何接口上，VLAN都设置为*标记*。



步骤2.登录Web配置实用程序并选择“DHCP菜单”**>“DHCP设置”**。“DHCP设*置”页面*随即打开：

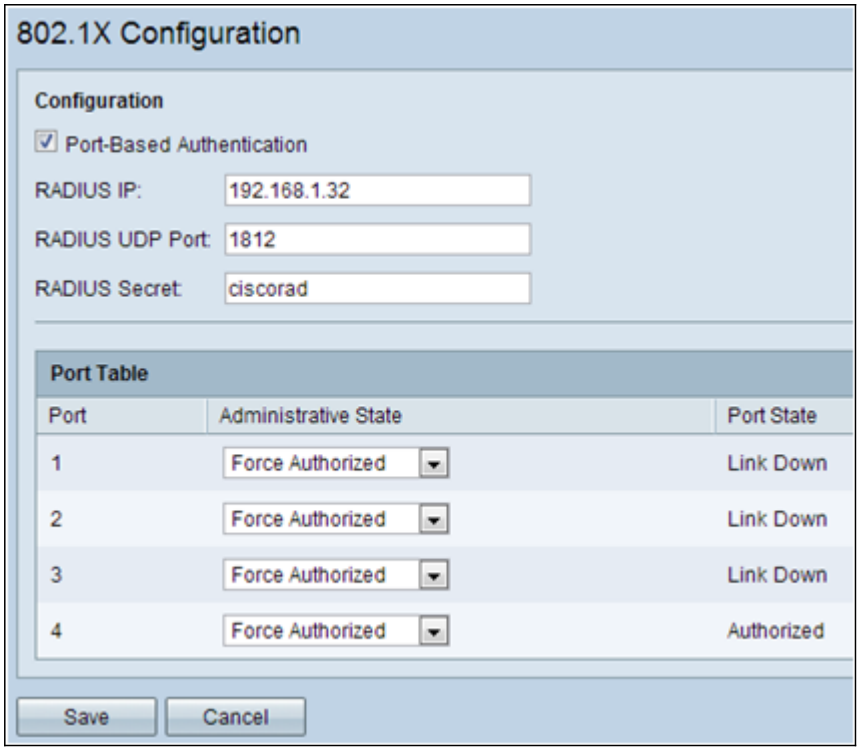
- 在VLAN ID下拉框中，选择要为（本例中为VLAN 10、20和30）设置地址池的VLAN。

- 配置此VLAN的设备IP地址，并设置IP地址范围。如果需要，您也可以在此处启用或禁用DNS代理，这取决于网络。在本例中，DNS代理将用于转发DNS请求。
- 单击**Save**，并为每个VLAN重复此步骤。



步骤3.在导航窗格中，选择**Port Management > 802.1x Configuration**。将打*开"802.1X配*置"页：

- 启用基于端口的身份验证并配置服务器的IP地址。
- RADIUS密钥是用于与服务器通信的身份验证密钥。
- 选择将使用此身份验证的端口，然后单击**Save**。

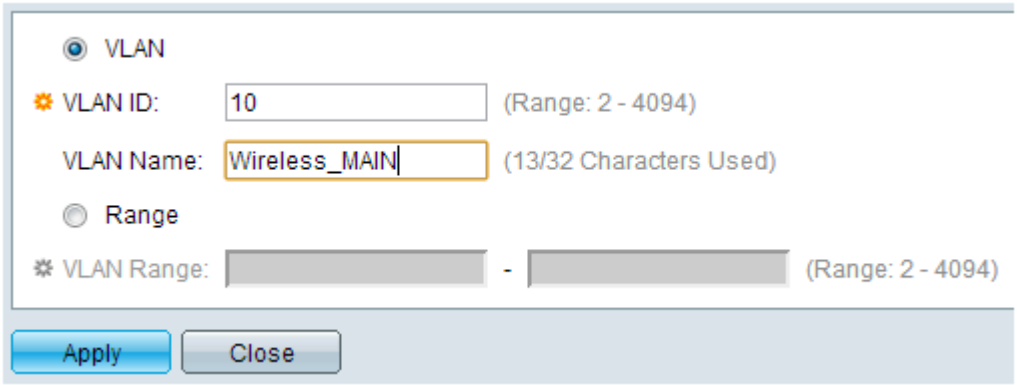


Sx300配置

SG300-10MP交换机充当路由器和WAP321之间的中间设备，以模拟真实的网络环境。交换机上的配置如下。

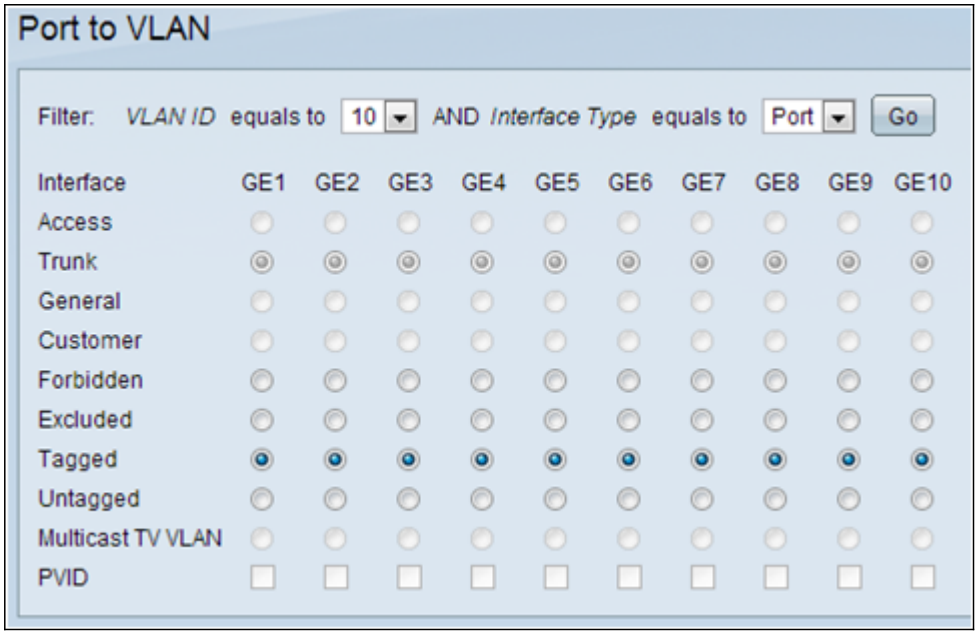
步骤1.登录Web配置实用程序，然后选择VLAN Management **> Create VLAN**。将打开一个新页面：

步骤2.单击“添**加”**。系统将显示新窗口。输入VLAN ID和VLAN名称（使用与第I节中的说明相同）。 点击Apply，然后对VLAN 20和VLAN 30重复此步骤。



步骤3.在导航窗格中，选择VLAN Management **> Port to VLAN**。将打开一个新页面：

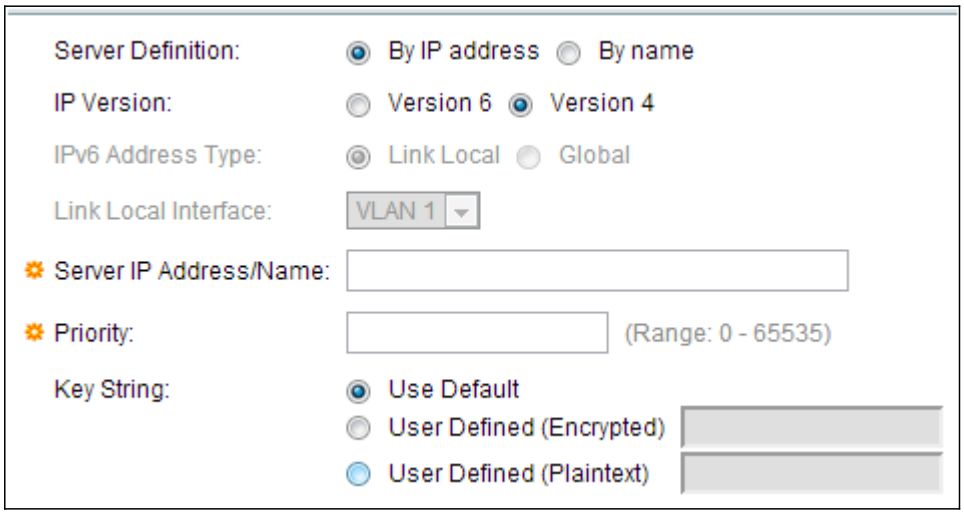
- 在页面顶部，将“VLAN ID equals to”设置为要添加的VLAN（本例中为VLAN 10），然后单击右侧的**Go**。这将使用该VLAN的设置更新页面。
- 更改每个端口上的设置，使VLAN 10现在为“已标记”而不是“已排除”。 对VLAN 20和VLAN 30重复此步骤。



步骤4.在导航窗格中，选择Security **> Radius**。RADIUS*页面*打开：

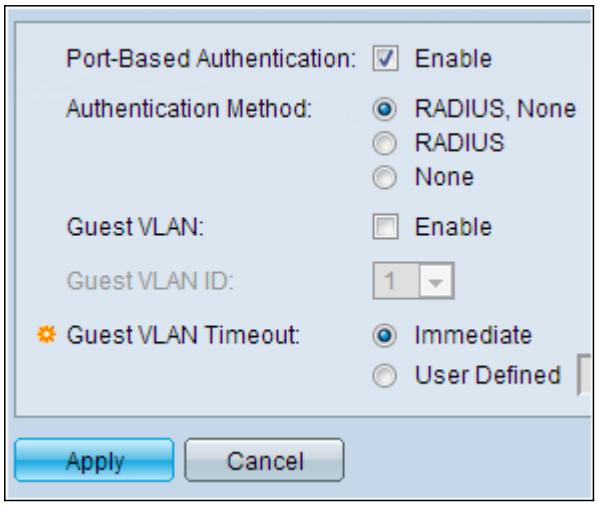
- 选择RADIUS服务器使用的访问控制方法，管理访问控制或基于端口的身份验证。选择基于端口的访问控制，然后单**击应用**。
- 单击页面底部的**Add**，添加要进行身份验证的新服务器。

步骤5.在显示的窗口中，您将配置服务器的IP地址（本例中为192.168.1.32）。您需要为服务器设置优先级，但是由于在本例中，我们只有一台服务器来按优先级进行身份验证并不重要。如果您有多个RADIUS服务器可供选择，则这一点非常重要。配置身份验证密钥，其余设置可保留为默认值。

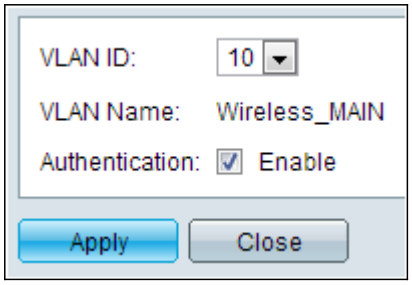


步骤6.在导航窗格中，选择**Security > 802.1X > Properties**。将打开一个新页面：

- 选中**Enable**以打开802.1x身份验证并选择身份验证方法。在这种情况下，我们使用RADIUS服务器，因此选择第一个或第二个选项。
- 单击 **Apply**。



步骤7.选择其中一个VLAN并单击**Edit**。系统将显示新窗口。选中**Enable** 以允许该VLAN上的身份验证，然后单击*Apply*。对每个VLAN重复上述步骤。



WAP321配置

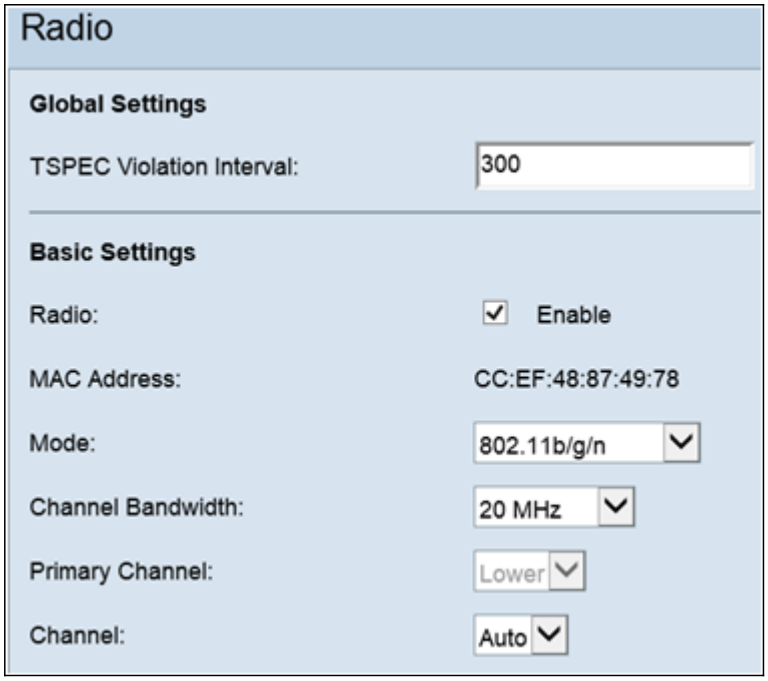
虚拟接入点(VAP)将无线LAN划分为多个广播域，这些广播域与以太网VLAN无线等效。VAP在一个物理WAP设备中模拟多个接入点。WAP121支持多达四个VAP，WAP321支持多达八个VAP。

除VAP0外，每个VAP都可以独立启用或禁用。VAP0是物理无线电接口，只要启用无线电，VAP0就保持启用状态。要禁用VAP0的操作，必须禁用无线电本身。

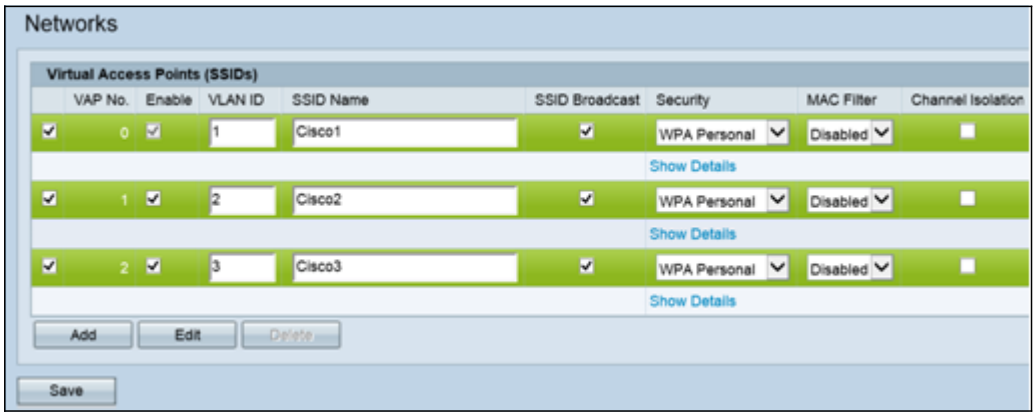
每个VAP由用户配置的服务集标识符(SSID)标识。 多个VAP不能具有相同的SSID名称。SSID广播可以在每个VAP上单独启用或禁用。SSID广播默认启用。

步骤1.登录Web配置实用程序并选择Wireless **> Radio**。此时将*打开*"Radio"页：

- 单击**Enable**复选框以启用无线电。
- Click **Save**.然后，无线电将打开。



步骤2.在导航窗格中，选择**Wireless > Networks**。“网络”页面打开：



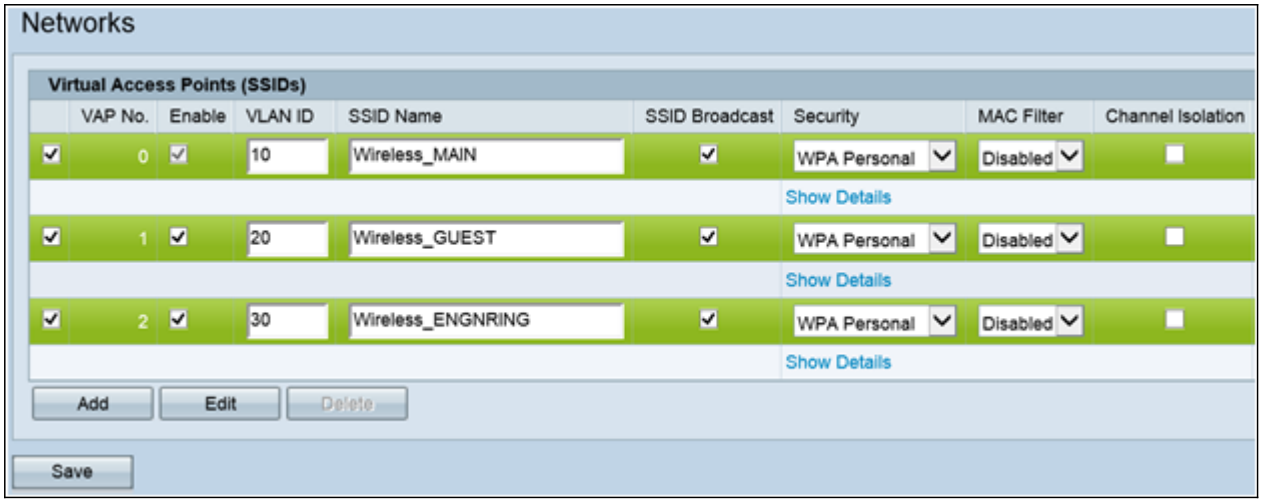
注意：VAP0的默认SSID是ciscosb。每创建一个额外的VAP都有一个空的SSID名称。所有VAP的SSID都可配置为其他值。

步骤3.每个VAP都与VLAN关联，VLAN由VLAN ID(VID)标识。VID可以是1到4094之间的任意值，包括。WAP121支持五个活动VLAN（四个用于WLAN，另外一个管理VLAN）。WAP321支持9个活动VLAN（8个用于WLAN，另外1个管理VLAN）。

默认情况下，分配给WAP设备配置实用程序的VID为1，也是默认的无标记VID。如果管理VID与分配给VAP的VID相同，则与此特定VAP关联的WLAN客户端可以管理WAP设备。如果需要，可以创建访问控制列表(ACL)，以禁用对WLAN客户端的管理。

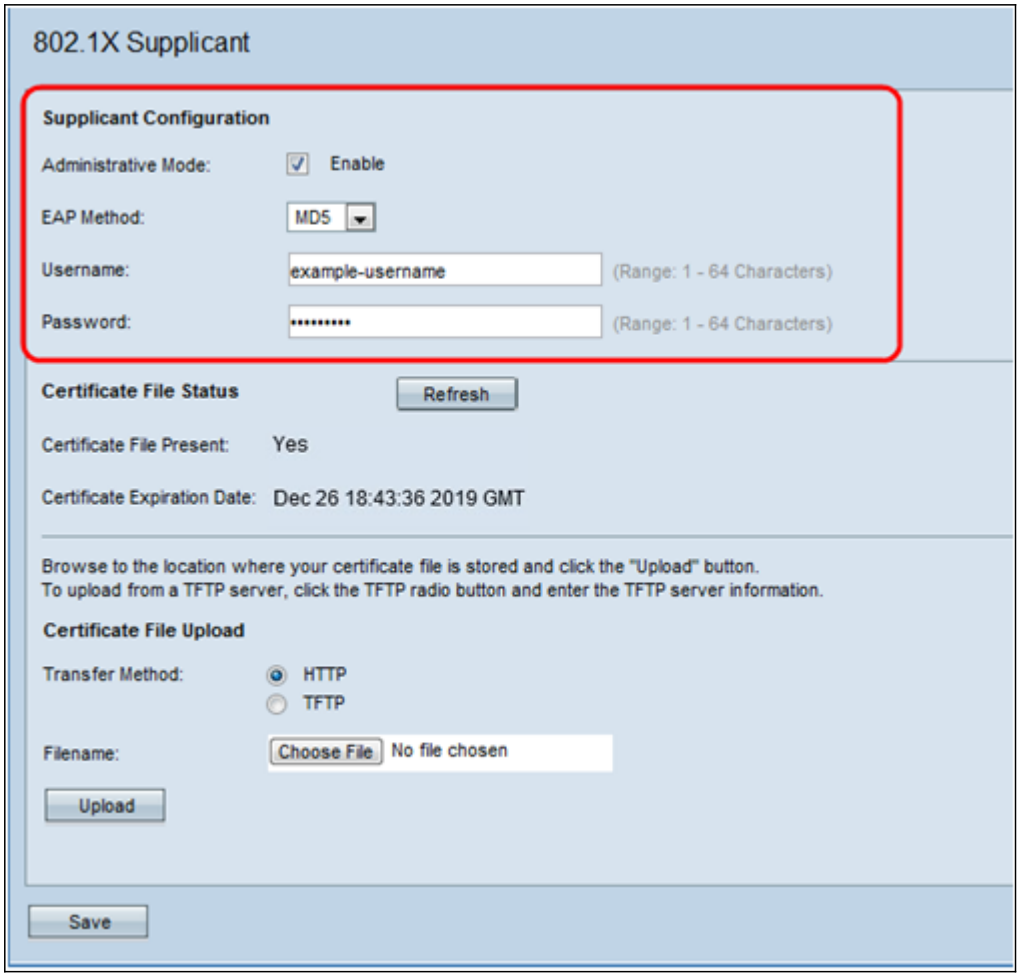
在此屏幕上，应执行以下步骤：

- 单击左侧的复选标记按钮编辑SSID:
- 在VLAN ID框中输入VLAN ID所需的值
- 输入SSID后，单击“保存”按钮。



步骤4.在导航窗格中，选择**System Security > 802.1X Supplicant客户端**。*“802.1X请求方”*页面打开：

- 在Administrative Mode字段中选中**Enable**，使设备能够在802.1X身份验证中充当请求方。
- 从“EAP方法”字段的下拉列表中选择适当类型的可扩展身份验证协议(EAP)方法。
- 在Username和Password字段中输入接入点用于从802.1X身份验证器获取身份验证的用户名和密码。用户名和密码的长度必须介于1到64个字母数字和符号字符之间。应已在身份验证服务器上配置。
- 点击 **Save（保存），以保存设置。**



注意：Certificate File Status区域显示证书文件是否存在。SSL证书是证书颁发机构数字签名的证书，它允许Web浏览器与Web服务器进行安全通信。要管理和配置SSL证书，请参阅[WAP121和WAP321接入点上的安全套接字层(SSL)证书管理文章]

步骤5.在导航窗格中，选择**Security > RADIUS Server**。RADIUS服务器页面打开。输入参数后，单击**Save**按钮。