在RV320 VPN路由器、WAP321無線 — N接入點和Sx300系列交換機上啟用多個無線網路

目標

在不斷變化的業務環境中，您的小型企業網路必須功能強大、靈活、易於訪問且高度可靠，尤其是在增長成為首要任務的情況下。無線裝置的普及程度呈指數級增長，這並不令人意外。無線網路具有成本效益、易於部署、靈活、可擴展和移動等特點，可無縫提供網路資源。身份驗證允許網路裝置驗證並確保使用者的合法性，同時保護網路免受未經授權使用者的侵害。部署安全且可管理的無線網路基礎設施非常重要。

Cisco RV320 Dual Gigabit WAN VPN路由器為您和您的員工提供可靠、高度安全的接入連線。採用單點設定的Cisco WAP321無線 — N接入點支援千兆乙太網的高速連線。網橋以無線方式將LAN連線在一起，使小型企業更容易擴展其網路。

本文提供在Cisco小型企業網路中啟用無線存取所需的設定逐步指南，包括虛擬區域網路(VLAN)間路由、多個服務組識別碼(SSID)以及路由器、交換機和存取點上的無線安全設定。

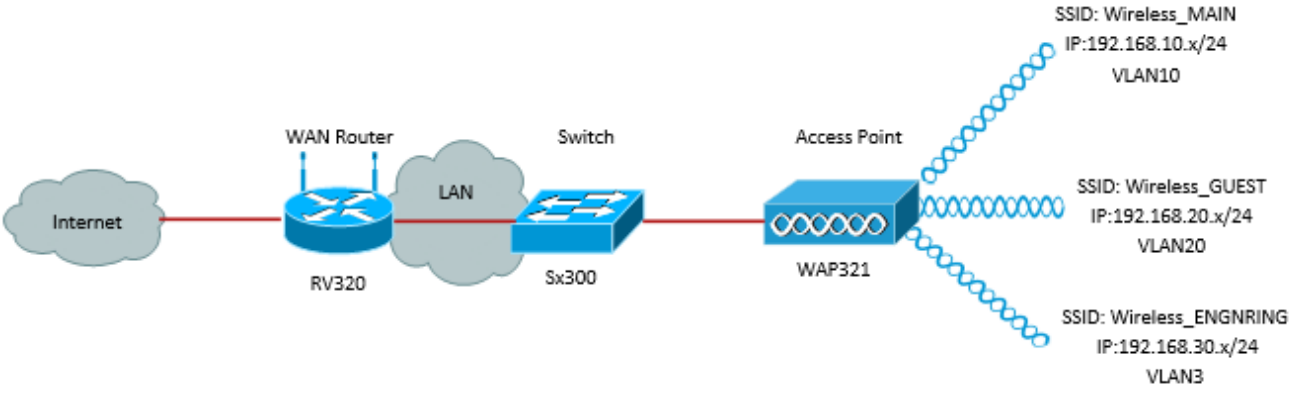
適用裝置

·RV320 VPN路由器
· WAP321無線 — N存取點
· Sx300系列交換器

軟體版本

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

網路拓撲



上圖顯示了使用多個SSID與Cisco小型企業WAP、交換機和路由器進行無線訪問的示例實施。WAP連線到交換機並使用中繼介面傳輸多個VLAN資料包。交換機通過中繼介面連線到WAN路由器，WAN路由器執行VLAN間路由。WAN路由器連線到Internet。所有無線裝置都連線到WAP。

主要功能

將Cisco RV路由器提供的Inter-VLAN路由功能與小型企業接入點提供的無線SSID隔離功能相結合，可為任何現有思科小型企業網路上的無線接入提供簡單而安全的解決方案。

VLAN間路由

若沒有路由器在VLAN之間路由流量，則不同VLAN中的網路裝置無法相互通訊。在小型企業網路中，路由器會為有線和無線網路執行VLAN間路由。當為特定VLAN禁用VLAN間路由時，該VLAN上的主機將無法與另一個VLAN上的主機或裝置通訊。

無線SSID隔離

有兩種型別的無線SSID隔離。啟用無線隔離（在SSID內）後，同一SSID上的主機將無法看到對方。啟用無線隔離（在SSID之間）後，一個SSID上的流量不會轉發到任何其他SSID。

IEEE 802.1x

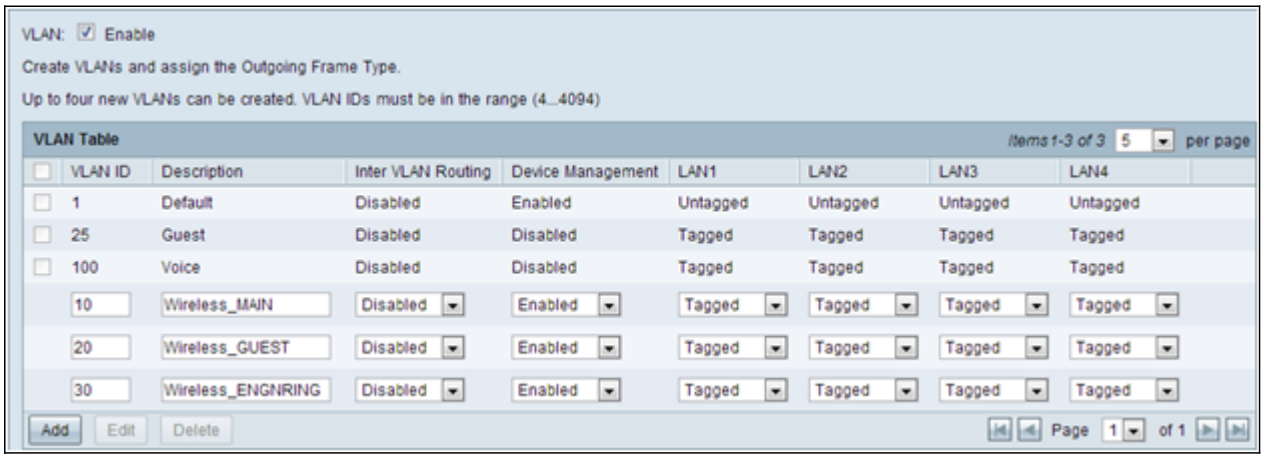
IEEE 802.1x標準指定用於實施基於埠的網路訪問控制的方法，這些網路訪問控制用於向乙太網路提供經過身份驗證的網路訪問。基於埠的身份驗證是僅允許憑證交換通過網路進行的過程，直到連線到埠的使用者通過身份驗證。憑證交換期間，連線埠稱為未受控制的連線埠。驗證完成後，連線埠稱為受控制連線埠。這基於一個物理埠內存在的兩個虛擬埠。

這會使用交換LAN基礎架構的物理特徵來驗證連線到LAN連線埠的裝置。如果驗證程式失敗，可能會拒絕存取連線埠。此標準最初是為有線乙太網路而設計，但現已調整為802.11無線LAN上使用。

RV320配置

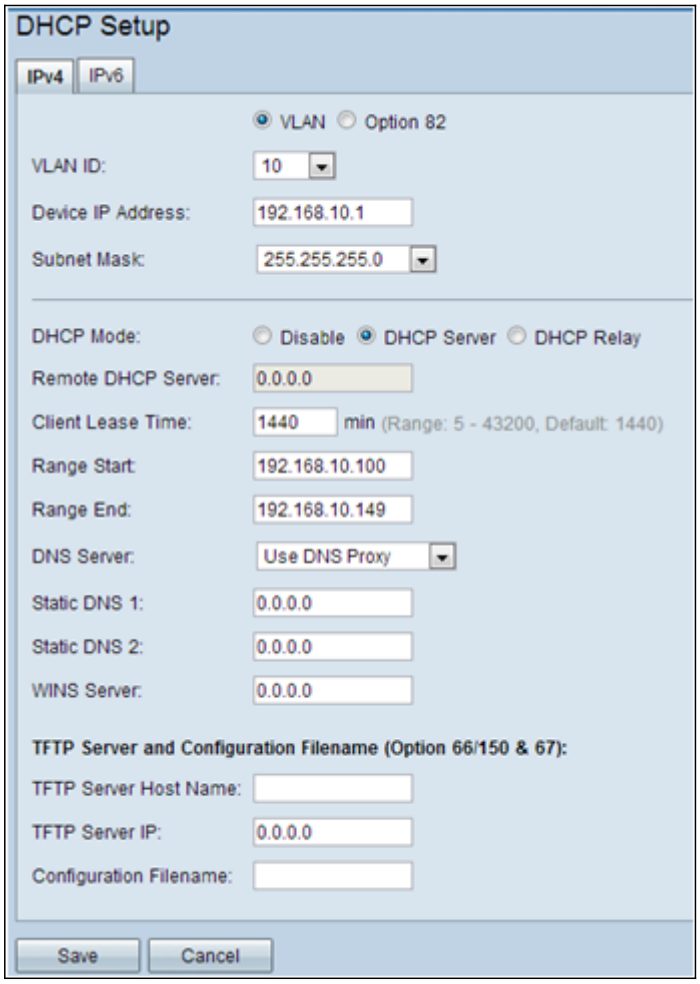
在此方案中，我們希望將RV320用作網路的DHCP伺服器，因此我們需要設定該伺服器，並在裝置上配置單獨的VLAN。首先，連線到其中一個乙太網埠並轉到192.168.1.1（假設您尚未更改路由器的IP地址）以登入到路由器。

步驟1.登入到Web配置實用程式並選擇**Port Management > VLAN Membership**。將開啟一個新頁面。我們正在建立3個單獨的VLAN來代表不同的目標受眾。按一下**Add**新增新行，並編輯VLAN ID和說明。您還需要確保在其需要傳輸的任何介面上將VLAN設定為*Tagged*。



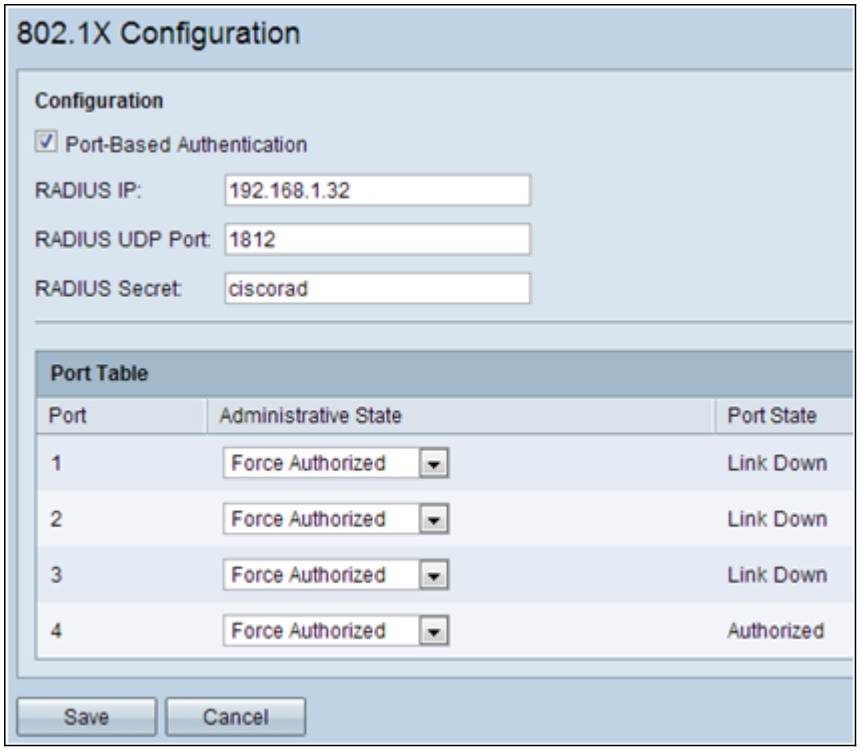
步驟2.登入到Web配置實用程式並選擇**DHCP Menu > DHCP Setup**。將開啟*DHCP Setup*頁面：

- 在VLAN ID下拉框中，選擇您要為其設定地址池的VLAN（在本例中為VLAN 10、20和30）。
- 為此VLAN配置裝置IP地址，並設定IP地址範圍。如果您願意，還可以在此處啟用或禁用DNS代理，這將取決於網路。在本例中，DNS代理將轉發DNS請求。
- 按一下「**Save**」，對每個VLAN重複此步驟。



步驟3.在導航窗格中，選擇**Port Management > 802.1x Configuration**。*802.1X Configuration*頁面隨即開啟：

- 啟用基於埠的身份驗證並配置伺服器的IP地址。
- RADIUS Secret是用於與伺服器通訊的身份驗證金鑰。
- 選擇將使用此身份驗證的埠，然後按一下**Save**。

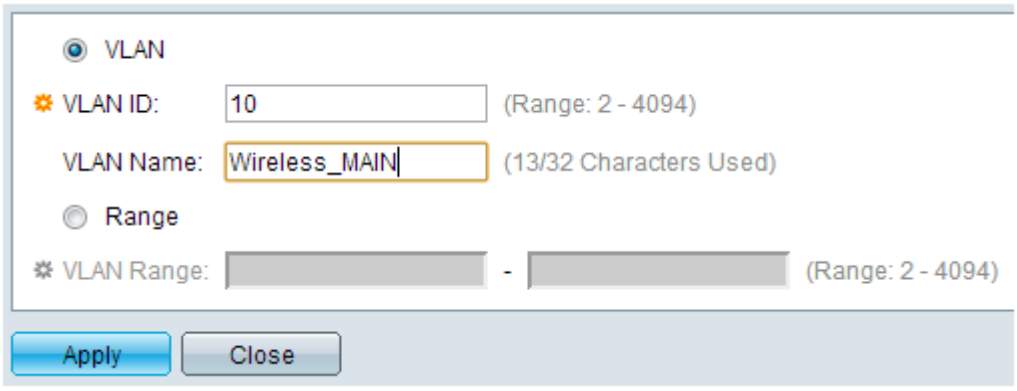


Sx300組態

SG300-10MP交換機作為路由器和WAP321之間的中間裝置，用於模擬真實的網路環境。交換機上的配置如下。

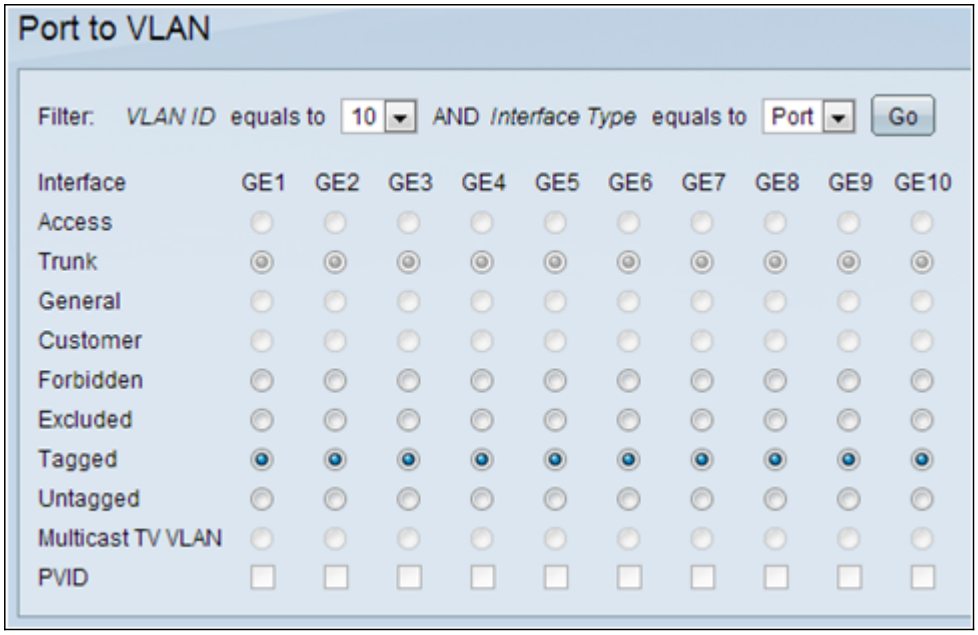
步驟1.登入到Web配置實用程式，然後選擇**VLAN管理>建立VLAN**。將開啟一個新頁面：

步驟2.按一下**Add**。出現一個新視窗。輸入VLAN ID和VLAN名稱（使用與I部分相同的說明）。 按一下應用，然後對VLAN 20和30重複此步驟。



步驟3.在導航窗格中，選擇**VLAN管理>埠到VLAN**。將開啟一個新頁面：

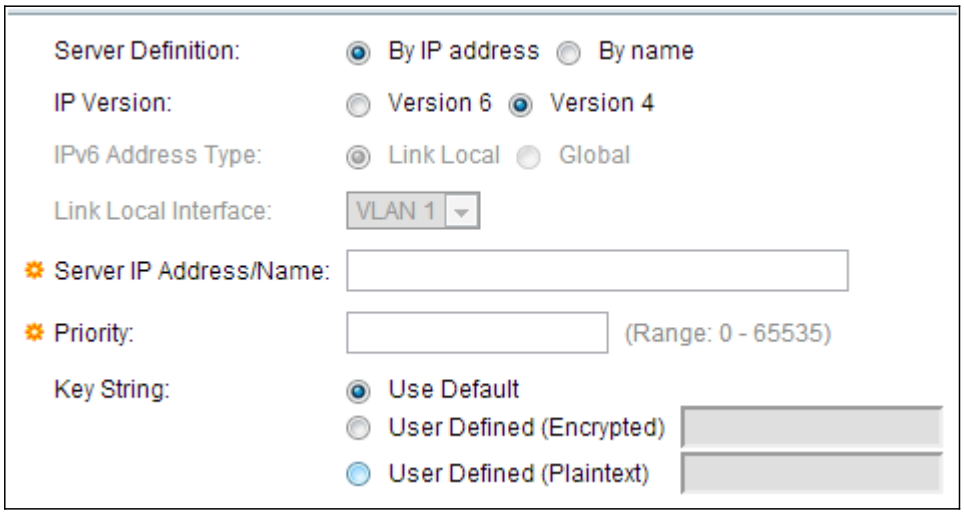
- 在頁面頂部，將「VLAN ID equals to」(VLAN ID equals to)設定為要新增的VLAN（本例中為VLAN 10），然後按一下右側的**Go**。這將使用該VLAN的設定更新該頁面。
- 更改每個埠上的設定，使VLAN 10現在為「已標籤」而不是「已排除」。 對VLAN 20和30重複此步驟。



步驟4.在導航窗格中，選擇**Security > Radius**。*RADIUS*頁面隨即開啟：

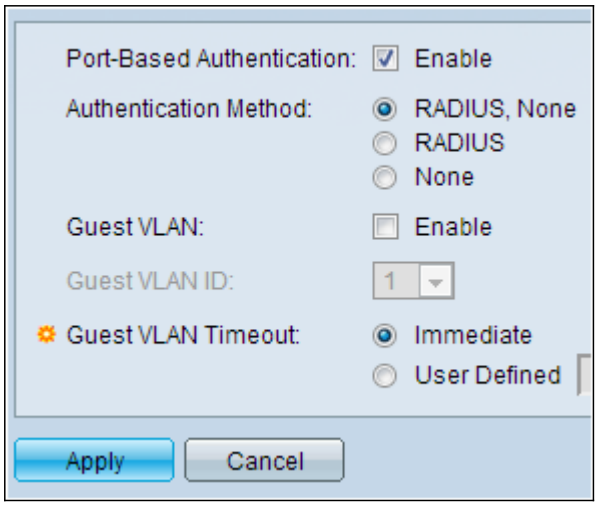
- 選擇RADIUS伺服器要使用的訪問控制方法，即管理訪問控制或基於埠的身份驗證。選擇Port Based Access Control，然後按一下**Apply**。
- 點選頁面底部的**Add**，新增要驗證的新伺服器。

步驟5.在顯示的視窗中，您將配置伺服器的IP地址，本例中為192.168.1.32。您需要為伺服器設定優先順序，但在本例中，我們僅有一台伺服器進行優先順序身份驗證，因此並不重要。如果您有多個RADIUS伺服器可選擇，這非常重要。配置身份驗證金鑰，其餘設定可以保留為預設值。

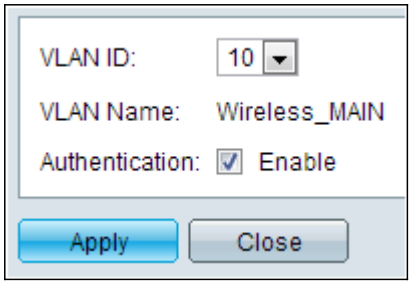


步驟6.在導航窗格中，選擇**Security > 802.1X > Properties**。將開啟一個新頁面：

- 選中**Enable**以啟用802.1x身份驗證，並選擇身份驗證方法。在這種情況下，我們使用的是RADIUS伺服器，因此選擇第一個或第二個選項。
- 按一下「**Apply**」。



步驟7.選擇其中一個VLAN，然後按一下**Edit**。出現一個新視窗。勾選「**Enable**」以允許該VLAN上的驗證，然後按一下「*Apply*」。對每個VLAN重複上述步驟。



WAP321配置

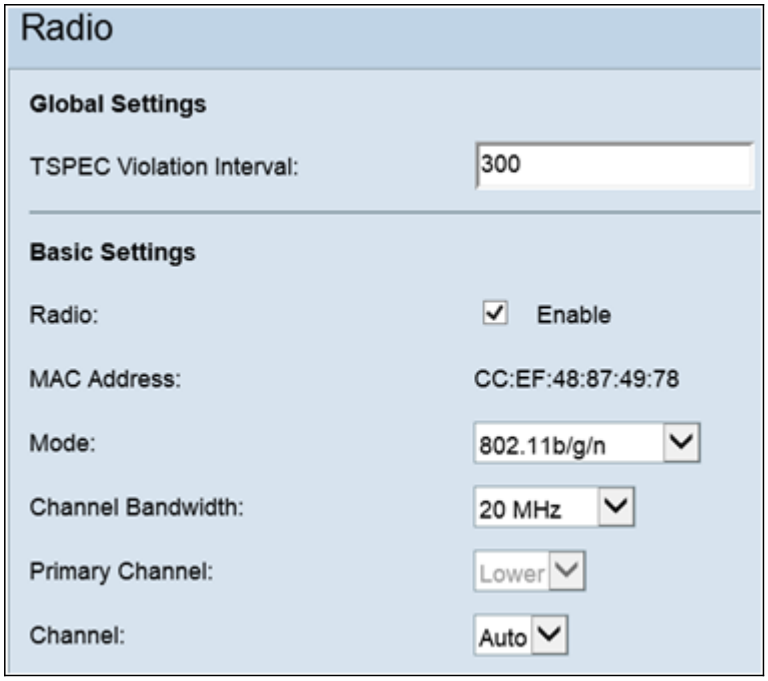
虛擬存取點(VAP)將無線LAN劃分為多個廣播網域，這些廣播網域相當於乙太網路VLAN。VAP在一個物理WAP裝置中模擬多個接入點。WAP121最多支援四個VAP，WAP321最多支援八個VAP。

可以單獨啟用或禁用每個VAP（VAP0除外）。VAP0是物理無線電介面，只要無線電已啟用，VAP0就會保持啟用狀態。要禁用VAP0的操作，必須禁用無線電本身。

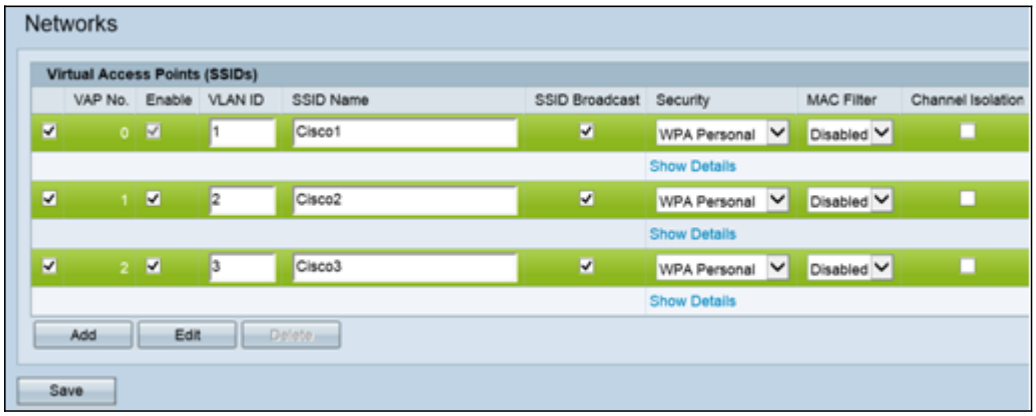
每個VAP由使用者配置的服務集識別符號(SSID)標識。 多個VAP不能具有相同的SSID名稱。可以在每個VAP上單獨啟用或禁用SSID廣播。預設情況下啟用SSID廣播。

步驟1.登入到Web配置實用程式並選擇**Wireless > Radio**。*Radio*頁面隨即開啟：

- 按一下**Enable**覈取方塊以啟用Wireless Radio。
- 按一下「**Save**」。然後開啟收音機。



步驟2.在導航窗格中，選擇**無線>網路**。*Network*頁面隨即開啟：



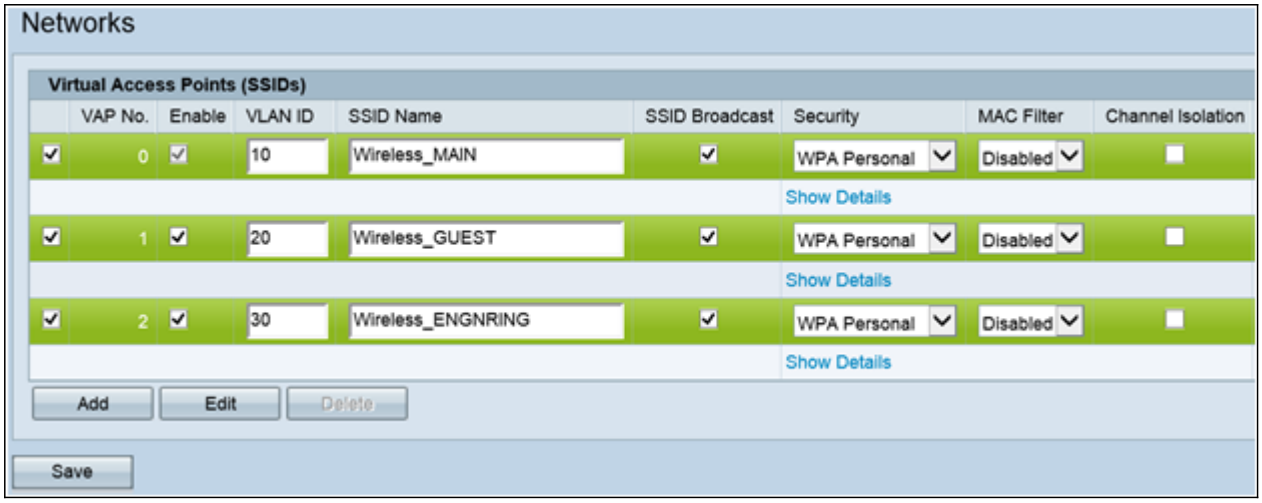
附註：VAP0的預設SSID是ciscosb。建立的每個附加VAP都有一個空白SSID名稱。可以將所有VAP的SSID配置為其他值。

步驟3.每個VAP與一個VLAN關聯，該VLAN由VLAN ID(VID)標識。VID可以是介於1和4094之間的任何值（包括1和4094）。WAP121支援五個活動VLAN（四個用於WLAN，一個管理VLAN）。 WAP321支援9個活動VLAN（8個用於WLAN，1個管理VLAN）。

預設情況下，分配給WAP裝置配置實用程式的VID為1，這也是預設的無標籤VID。如果管理VID與分配給VAP的VID相同，則與此特定VAP關聯的WLAN客戶端可以管理WAP裝置。如果需要，可以建立訪問控制清單(ACL)，以禁用WLAN客戶端的管理。

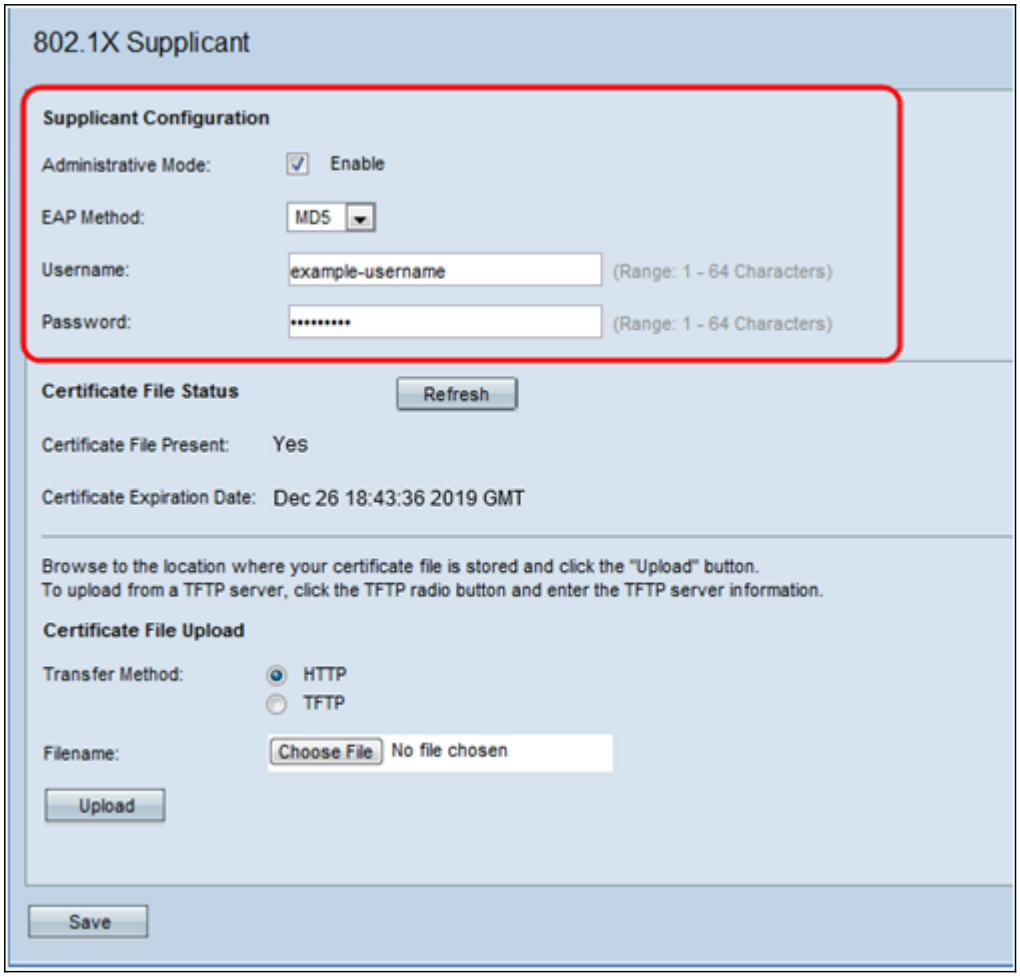
在此螢幕上，應執行以下步驟：

- 按一下左側複選標籤按鈕編輯SSID:
- 在VLAN ID框中輸入VLAN ID所需的值
- 輸入SSID後，按一下**Save**按鈕。



步驟4.在導航窗格中，選擇**System Security > 802.1X Supplicant**。*802.1X Supplicant*頁面開啟：

- 在Administrative Mode欄位中選中**Enable**，使裝置能夠充當802.1X身份驗證中的請求方。
- 從EAP Method欄位的下拉選單中選擇適當型別的可擴展身份驗證協定(EAP)方法。
- 在Username（使用者名稱）和Password（密碼）欄位中，輸入接入點用於從802.1X身份驗證器獲取身份驗證的使用者名稱和密碼。使用者名稱和密碼的長度必須介於1到64個字母數字和符號字元之間。應該在身份驗證伺服器上配置此項。
- 按一下「**Save**」以儲存設定。



附註：Certificate File Status區域顯示證書檔案是否存在。SSL證書是由證書頒發機構數位簽章的證書，它允許Web瀏覽器與Web伺服器進行安全通訊。要管理和配置SSL證書，請參閱[WAP121和WAP321接入點上的安全套接字層(SSL)證書管理]一文

步驟5.在導航窗格中，選擇**Security > RADIUS Server**。將開啟*RADIUS Server*頁面。輸入引數，並在輸入Radius伺服器引數後按一下**Save**按鈕。