RV320 VPNルータ、WAP321 Wireless-Nアクセスポイント、およびSx300シリーズスイッチでの複数のワイヤレスネットワークの有効化

目的

変化し続けるビジネス環境において、小規模企業のネットワークは、特に成長が優先される場合には、強力で柔軟性、アクセス性、および信頼性が必要です。ワイヤレスデバイスの人気は急激に高まっており、驚くべきことではありません。ワイヤレスネットワークは、コスト効率が高く、導入が容易で、柔軟性と拡張性に優れ、モバイル性に優れ、ネットワークリソースをシームレスに提供します。認証により、ネットワークデバイスは、ネットワークを不正ユーザから保護しながら、ユーザの正当性を検証および保証できます。セキュアで管理可能なワイヤレスネットワークインフラストラクチャを導入することが重要です。

Cisco RV320デュアルギガビットWAN VPNルータは、信頼性が高く安全性の高いアクセス接続を貴社と従業員に提供します。Cisco WAP321 Wireless-N Selectable-Band Access Point with Single Point Setupは、ギガビットイーサネットによる高速接続をサポートします。ブリッジはLANをワイヤレスで接続し、小規模企業のネットワーク拡張を容易にします。

この記事では、Cisco Small Businessネットワークでワイヤレスアクセスを有効にするために必要な設定の手順を説明します。たとえば、ルータ、スイッチ、およびアクセスポイントのInter-Virtual Local Area Network(VLAN)ルーティング、複数のService Set Identifier(SSID)、ワイヤレスセキュリティ設定などです。

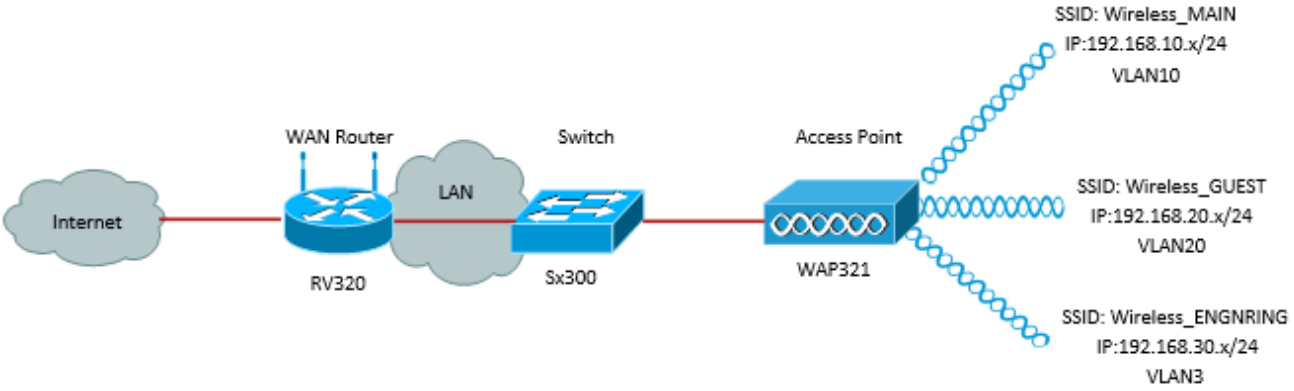
該当するデバイス

- RV320 VPNルータ
- WAP321 Wireless-Nアクセスポイント
- Sx300シリーズスイッチ

[Software Version]

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

Network Topology



上の図は、Cisco Small Business WAP、スイッチ、およびルータで複数のSSIDを使用したワイヤレスアクセスの実装例を示しています。WAPはスイッチに接続し、トランクインターフェイスを使用して複数のVLANパケットを転送します。スイッチはトランクインターフェイスを介してWANルータに接続し、WANルータはVLAN間ルーティングを実行します。WANルータはインターネットに接続します。すべてのワイヤレスデバイスがWAPに接続します。

主な特長

Cisco RVルータが提供するVLAN間ルーティング機能と、Small Businessアクセスポイントが提供するワイヤレスSSID分離機能を組み合わせることで、既存のCisco Small Businessネットワーク上のワイヤレスアクセスに対するシンプルで安全なソリューションが提供されます。

VLAN間ルーティング

異なるVLAN内のネットワークデバイスは、VLAN間でトラフィックをルーティングするルータがないと、相互に通信できません。スモールビジネスのネットワークでは、ルータは有線ネットワークとワイヤレスネットワークの両方でVLAN間ルーティングを実行します。特定のVLANに対してVLAN間ルーティングを無効にすると、そのVLAN上のホストは別のVLAN上のホストやデバイスと通信できなくなります。

ワイヤレスSSID分離

ワイヤレスSSID分離には2つのタイプがあります。ワイヤレス分離（SSID内）が有効になっていると、同じSSID上のホストは互いを認識できません。ワイヤレス分離（SSID間）が有効になっている場合、1つのSSID上のトラフィックは他のSSIDには転送されません。

IEEE 802.1x

IEEE 802.1x標準は、イーサネットネットワークへの認証されたネットワークアクセスを提供するために使用される、ポートベースのネットワークアクセスコントロールの実装に使用される方法を指定します。ポートベース認証は、ポートに接続されたユーザが認証されるまで、クレデンシャル交換だけがネットワークを通過できるようにするプロセスです。このポートは、クレデンシャルが交換される間、制御されないポートと呼ばれます。認証が完了すると、ポートは制御ポートと呼ばれます。これは、1つの物理ポート内に存在する2つの仮想ポートに基づいています。

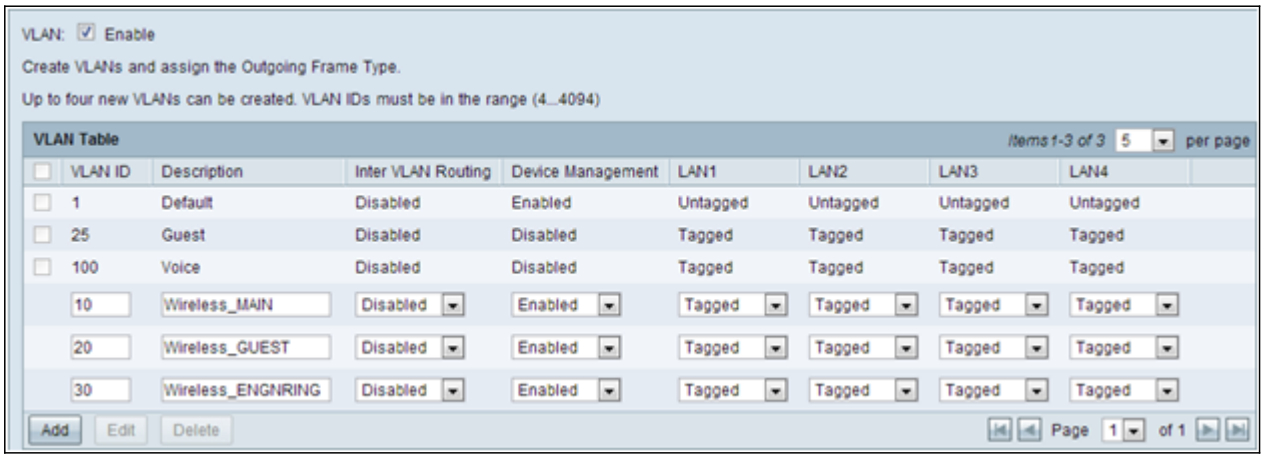
これは、スイッチ導入LANインフラストラクチャの物理特性を使用して、LANポートに接続されたデバイスを認証します。認証プロセスが失敗すると、ポートへのアクセスを拒否できます。この規格は、当初は有線イーサネットネットワーク用に設計されましたが、802.11ワ

イヤレスLANで使用するように設計されています。

RV320の設定

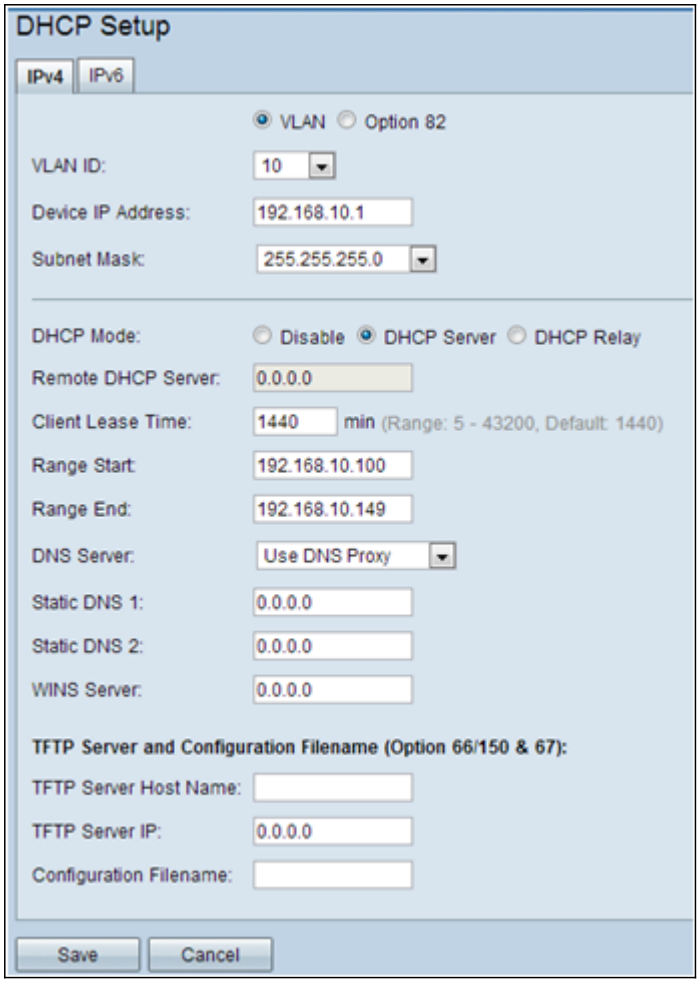
このシナリオでは、RV320をネットワークのDHCPサーバとして機能させるため、デバイス上で個別のVLANを設定するだけでなく、設定する必要があります。まず、イーサネットポートの1つに接続し、192.168.1.1に移動してルータにログインします（ルータのIPアドレスをまだ変更していない場合）。

ステップ1:Web設定ユーティリティにログインし、**[Port Management] > [VLAN Membership]を選択します**。新しいページが開きます。3つのVLANを別々に作成して、異なる対象ユーザを表します。[Add]をクリックして新しい行を追加し、VLAN IDと説明を編集します。また、VLANが移動する必要があるインターフェイスで*Tagged*に設定されていることも確認する必要があります。



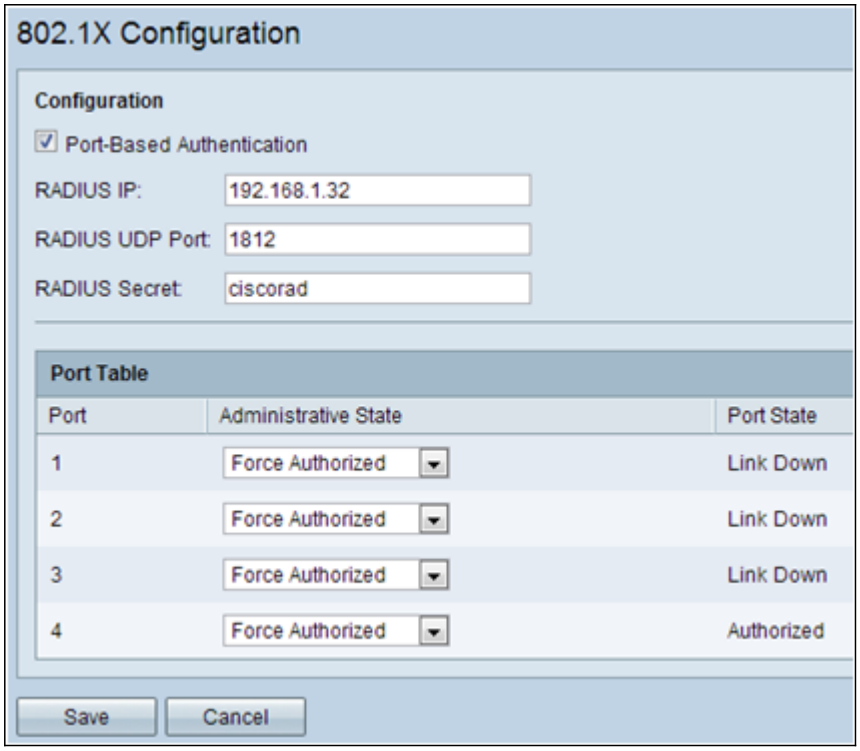
ステップ2:Web設定ユーティリティにログインし、**[DHCP Menu] > [DHCP Setup]を選択します**。「*DHCP* Setup」ページが開きます。

- [VLAN ID]ドロップダウンボックスで、アドレスプールを設定するVLAN（この例のVLAN 10、20、および30）を選択します。
- このVLANのデバイスIPアドレスを設定し、IPアドレス範囲を設定します。必要に応じて、ここでDNSプロキシを有効または無効にすることもできます。これはネットワークに依存します。この例では、DNSプロキシはDNS要求を転送します。
- [Save]をクリックし、各VLANでこの手順を繰り返します。



ステップ3：ナビゲーションペインで、[Port Management] > [802.1x Configuration]を選択します。[*802.1X Configuration]ページが開きます。*

- ポートベース認証を有効にし、サーバのIPアドレスを設定します。
- RADIUS Secretは、サーバとの通信に使用される認証キーです。
- この認証を使用するポートを選択し、[Save]をクリックします。

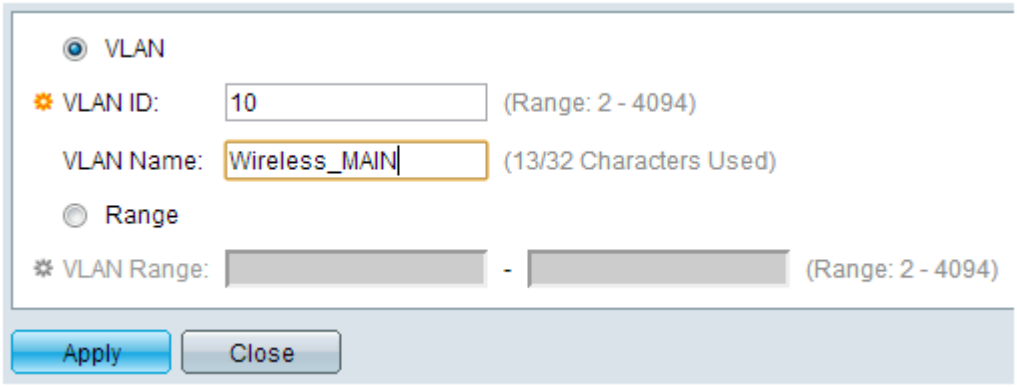


Sx300の設定

SG300-10MPスイッチは、現実的なネットワーク環境をシミュレートするために、ルータとWAP321の間の仲介役として機能します。スイッチの設定は次のとおりです。

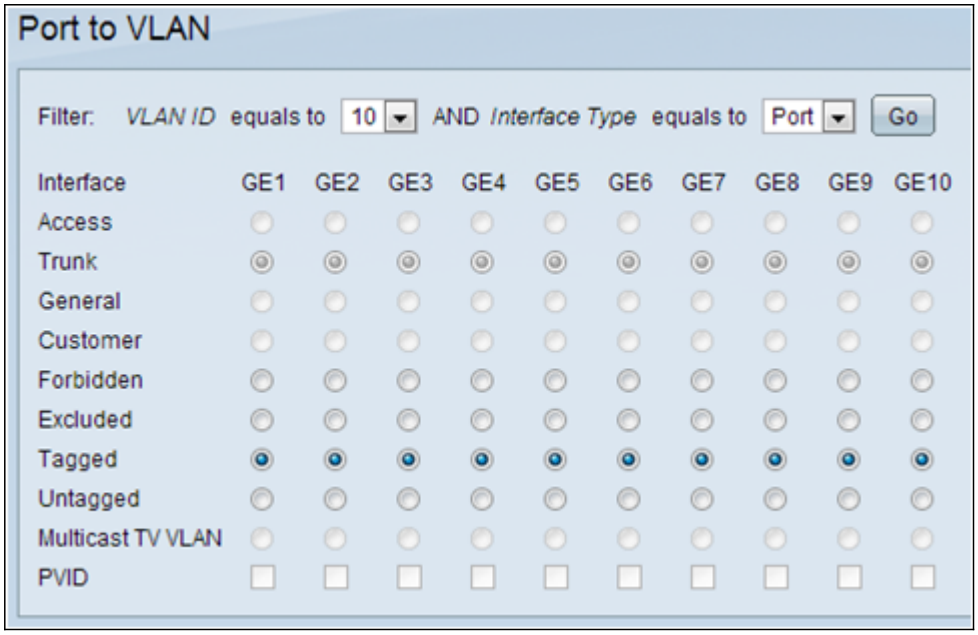
ステップ1:Web構成ユーティリティにログインし、**[VLAN Management] > [Create VLAN]を選択します**。新しいページが開きます。

ステップ2:[Add]をクリ**ックします**。新しいウィンドウが表示されます。VLAN IDとVLAN名を入力します（セクションIの説明と同じ説明を使用）。 [Apply]をクリックし、VLAN 20と30に対してこの手順を繰り返します。



ステップ3：ナビゲーションペインで、**[VLAN Management] > [Port to VLAN]を選択します**。新しいページが開きます。

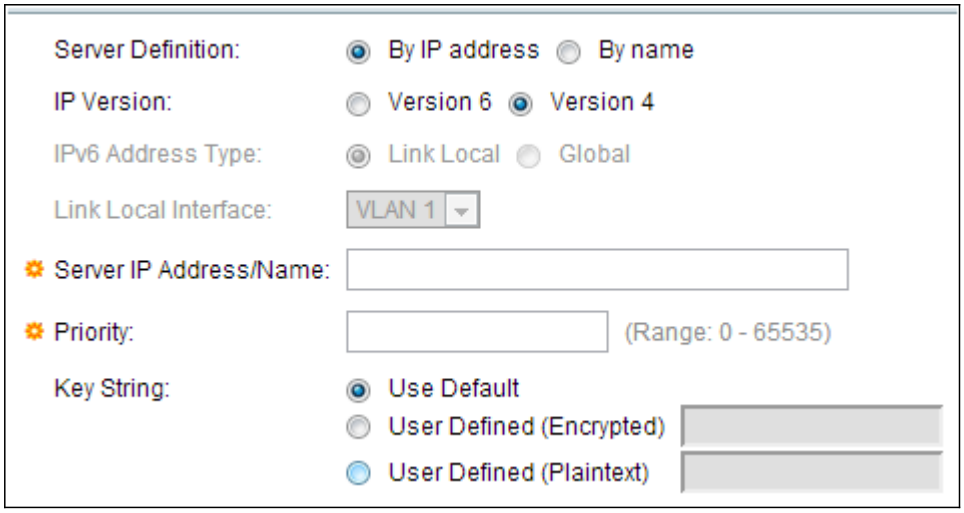
- ページの上部で、追加するVLAN（この場合はVLAN 10）に「VLAN ID equals to」を設定し、右側の[Go]をクリックします。これにより、そのVLANの設定でページが更新されます。
- 各ポートの設定を変更して、VLAN 10が「Excluded」ではなく「Tagged」になるようにします。 VLAN 20と30に対してこの手順を繰り返します。



ステップ4：ナビゲーションペインで、[**Security**] > [**Radius**]**を選択します。**[*RADIUS*]ページが開きます。

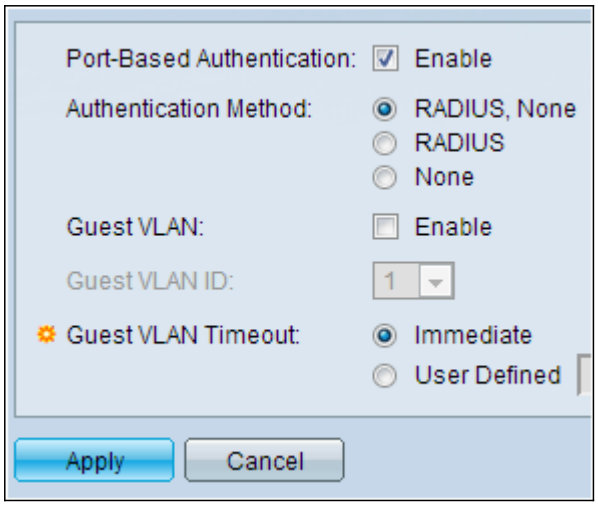
- RADIUSサーバで使用するアクセスコントロールの方式（管理アクセスコントロールまたはポートベース認証）を選択します。[Port Based Access Control]を選択し、[**Apply**]**をクリックします。**
- ページ下部の**[Add]**をクリックして、認証用の新しいサーバを追加します。

ステップ5：表示されるウィンドウで、サーバのIPアドレス(この場合は192.168.1.32)を設定します。サーバの優先度を設定する必要がありますが、この例では、優先度に対して認証するサーバは1台だけなので問題ありません。これは、複数のRADIUSサーバから選択する場合に重要です。認証キーを設定し、残りの設定はデフォルトのままにすることができます。

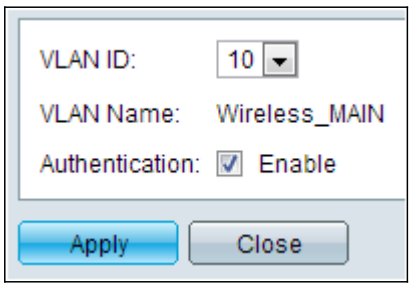


ステップ6：ナビゲーションペインで、**[Security] > [802.1X] > [Properties]を選択します**。新しいページが開きます。

- [Enable] をオンにして802.1x認証をオンにし、認証方式を選択します。この場合、RADIUSサーバを使用しているため、1つ目または2つ目のオプションを選択します。
- [Apply] をクリックします。



ステップ7:VLANの1つを選択し、**[Edit]をクリックします**。新しいウィンドウが表示されます。**[Enable]をオンに**して、そのVLANで認証を許可し、*[Apply]をクリックします*。各VLANについて繰り返します。



WAP321の設定

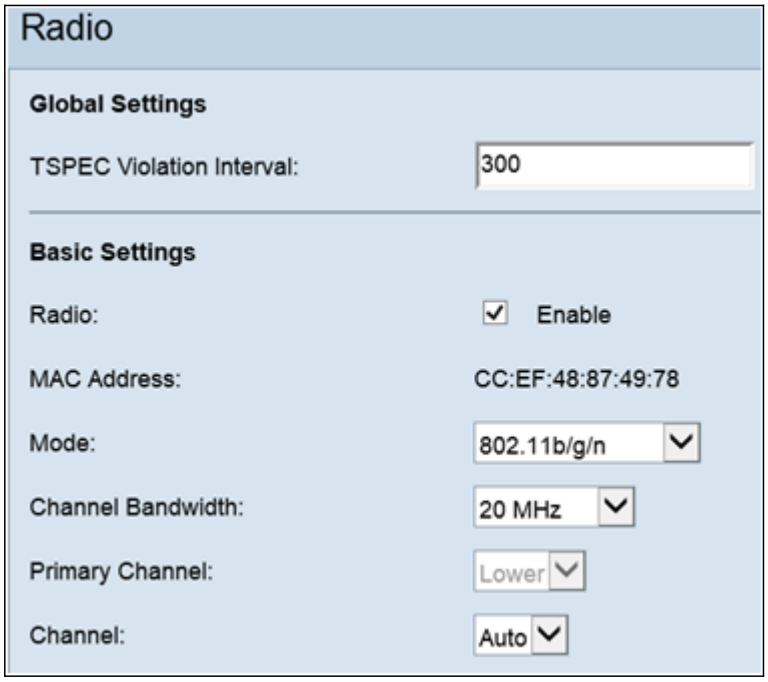
仮想アクセスポイント(VAP)は、イーサネットVLANと同等のワイヤレスである複数のブロードキャストドメインにワイヤレスLANをセグメント化します。VAPは、1つの物理WAPデバイスで複数のアクセスポイントをシミュレートします。WAP121では最大4つのVAPがサポートされ、WAP321では最大8つのVAPがサポートされます。

各VAPは、VAP0を除き、個別に有効または無効にできます。VAP0は物理無線インターフェイスであり、無線が有効である限り有効なままです。VAP0の動作を無効にするには、無線自体を無効にする必要があります。

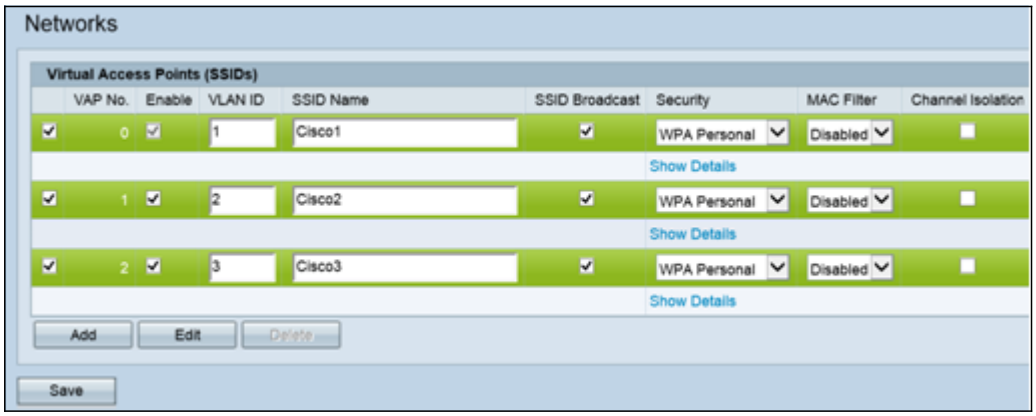
各VAPは、ユーザ設定のService Set Identifier(SSID)によって識別されます。 複数のVAPに同じSSID名を設定することはできません。SSIDブロードキャストは、各VAPで個別に有効または無効にできます。SSIDブロードキャストはデフォルトで有効になっています。

ステップ1:Web構成ユーティリティにログインし、**[Wireless] > [Radio]を選択します。** [Radio]ページが開きます。

- **[Enable]チェックボックスを**クリックして、ワイヤレスを有効にします。
- [Save] をクリックします。無線がオンになります。



ステップ2：ナビゲーションペインで**[Wireless] > [Networks]を選択します。**「ネットワーク」ページが開きます。



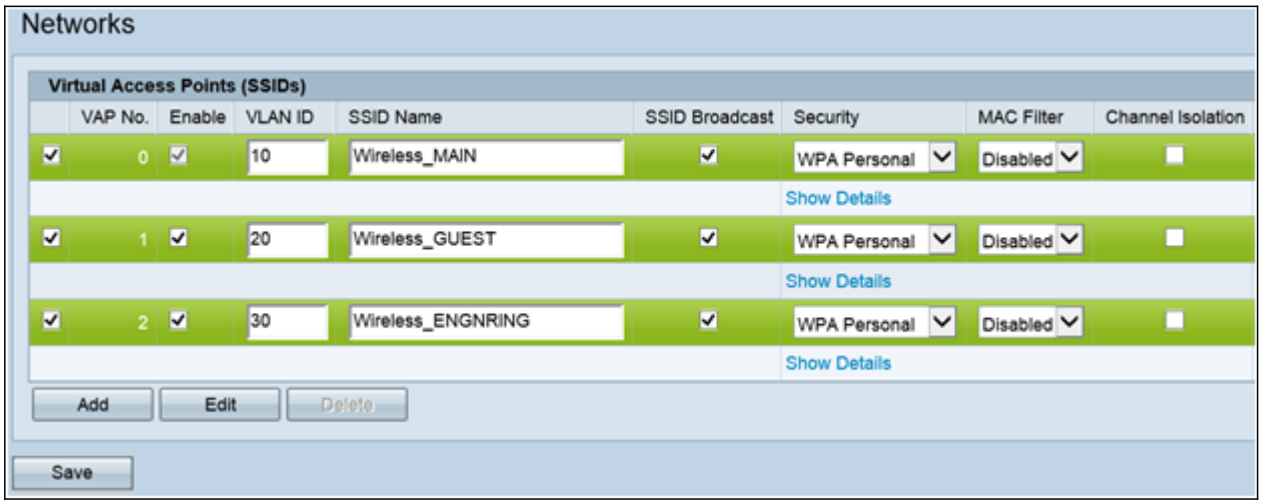
注：VAP0のデフォルトSSIDはciscosbです。作成された追加のVAPには、すべてブランクのSSID名が付いています。すべてのVAPのSSIDは、他の値に設定できます。

ステップ3：各VAPはVLAN ID(VID)で識別されるVLANに関連付けられます。VIDには、1 ~ 4094の任意の値を指定できます。WAP121は5つのアクティブVLAN（WLAN用に4つ、管理VLAN用に1つ）をサポートします。 WAP321は、9つのアクティブVLAN（WLAN用8つと管理VLAN 1つ）をサポートします。

デフォルトでは、WAPデバイスの設定ユーティリティに割り当てられたVIDは1です。これはタグなしのデフォルトのVIDでもあります。管理VIDがVAPに割り当てられたVIDと同じ場合、この特定のVAPに関連付けられたWLANクライアントはWAPデバイスを管理できます。必要に応じて、アクセスコントロールリスト(ACL)を作成して、WLANクライアントからの管理を無効にできます。

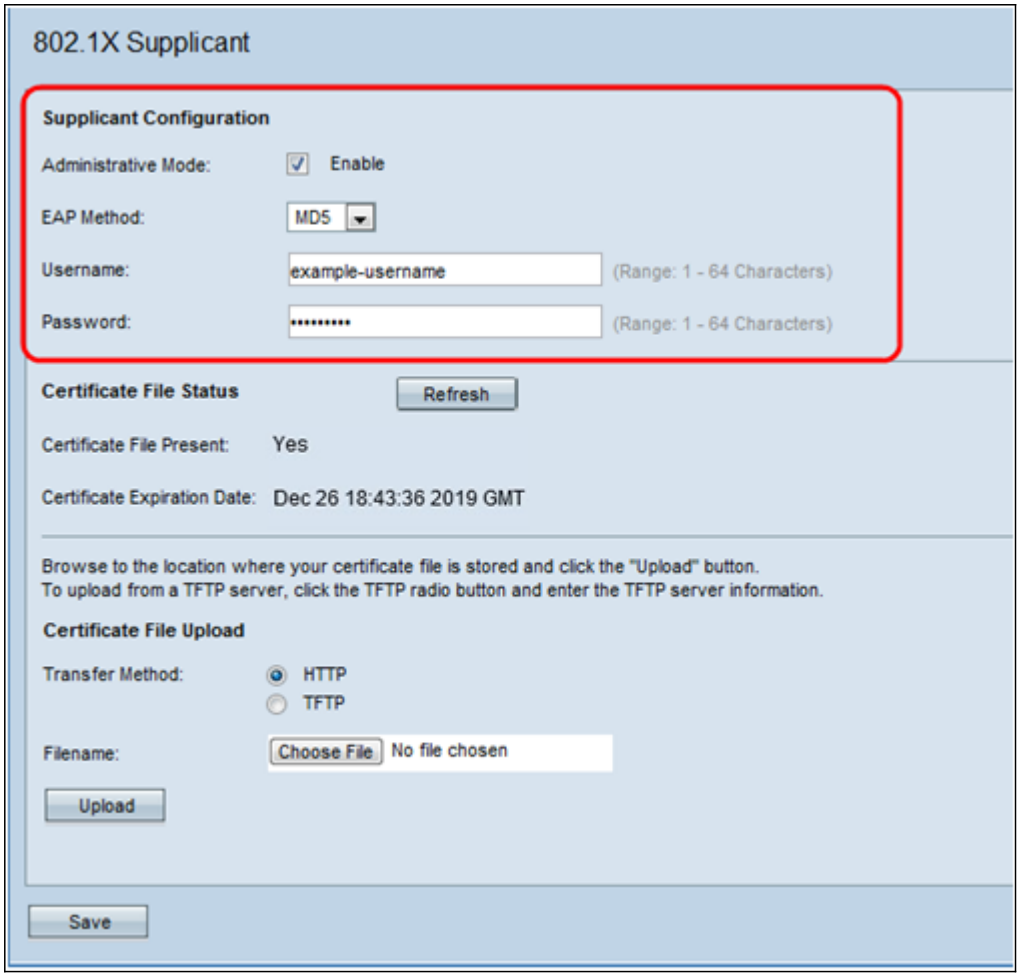
この画面では、次の手順を実行する必要があります。

- 左側のチェックマークボタンをクリックして、SSIDを編集します。
- [VLAN ID]ボックスにVLAN IDに必要な値を入力します
- SSIDを入力したら**[Save]**ボタンをクリックします。



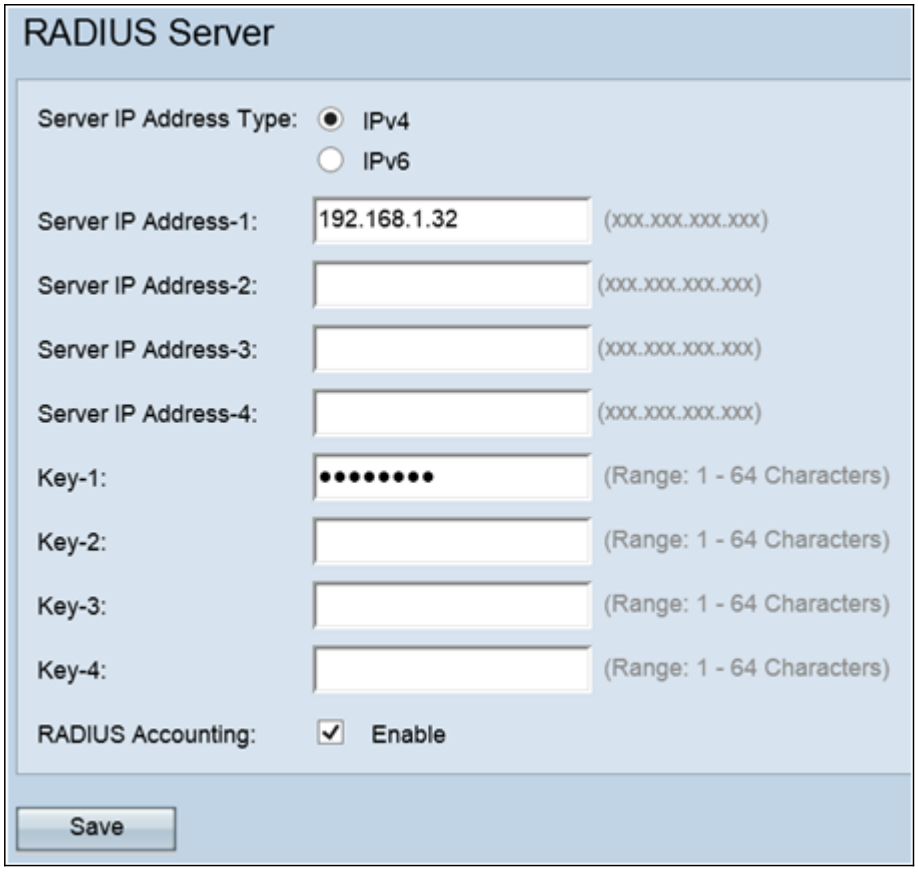
ステップ4：ナビゲーションペインで、**[System Security] > [802.1X Supplicant]を選択します。**[*802.1X Supplicant]ページが開き*ます。

- [Administrative Mode]フィールドの[Enable] をオンにして、デバイスが802.1X認証でサプリカントとして動作できるようにします。
- [EAP Method]フィールドのドロップダウンリストから、適切なタイプのExtensible Authentication Protocol(EAP)方式を選択します。
- アクセスポイントが802.1Xオーセンティケータから認証を取得するために使用するユーザ名とパスワードを[Username]フィールドと[Password]フィールドに入力します。ユーザ名とパスワードの長さは、1 ~ 64文字の英数字と記号で指定する必要があります。これは、認証サーバですでに設定されている必要があります。
- [Save] をクリックして、設定を保存します。



注：[Certificate File Status]領域には、証明書ファイルが存在するかどうかが表示されます。SSL証明書は、Webブラウザが Webサーバと安全に通信できるようにする認証局によってデジタル署名された証明書です。SSL証明書の管理と構成については、「WAP121および WAP321アクセスポイントでのSecure Socket Layer(SSL)証明書管理」を参照してください

ステップ5：ナビゲーションペインで、[**Security**] > [**RADIUS Server**]を選択します。[*RADIUS Server*]ページが開きます。パラメータを入力し、RADIUSサーバのパラメータを入力したら**Save**ボタンをクリックします。


RADIUS Server
Server IP Address Type:
IPv4
IPv6
Server IP Address-1:
192.168.1.32
(xxx.xxx.xxx.xxx)
Server IP Address-2:
(xxx.xxx.xxx.xxx)
Server IP Address-3:
(xxx.xxx.xxx.xxx)
Server IP Address-4:
(xxx.xxx.xxx.xxx)
Key-1:
(Range: 1 - 64 Characters)
Key-2:
(Range: 1 - 64 Characters)
Key-3:
(Range: 1 - 64 Characters)
Key-4:
(Range: 1 - 64 Characters)
RADIUS Accounting:
Enable
Save