Habilitação de várias redes sem fio em roteador VPN RV320, ponto de acesso Wireless-N WAP321 e switches Sx300 Series

Objetivo

Em um ambiente de negócios em constante mudança, a rede de sua pequena empresa precisa ser poderosa, flexível, acessível e altamente confiável, especialmente quando o crescimento é uma prioridade. A popularidade dos dispositivos sem fio cresceu exponencialmente, o que não é uma surpresa. As redes sem fio são econômicas, fáceis de implantar, flexíveis, escaláveis e móveis, fornecendo recursos de rede sem problemas. A autenticação permite que os dispositivos de rede verifiquem e garantam a legitimidade de um usuário enquanto protegem a rede de usuários não autorizados. É importante implantar uma infraestrutura de rede sem fio segura e gerenciável.

O roteador VPN WAN Gigabit duplo Cisco RV320 fornece uma conectividade de acesso confiável e altamente segura para você e seus funcionários. O ponto de acesso de banda selecionável Cisco WAP321 Wireless-N com configuração de ponto único suporta conexões de alta velocidade com Gigabit Ethernet. As bridges conectam as LANs sem fio, facilitando a expansão de redes pelas pequenas empresas.

Este artigo fornece orientação passo a passo para a configuração necessária para habilitar o acesso sem fio em uma rede de pequenas empresas da Cisco, incluindo roteamento de rede local inter-virtual (VLAN), vários SSIDs (Service Set Identifiers, identificadores de conjunto de serviços) e configurações de segurança sem fio no roteador, switch e pontos de acesso.

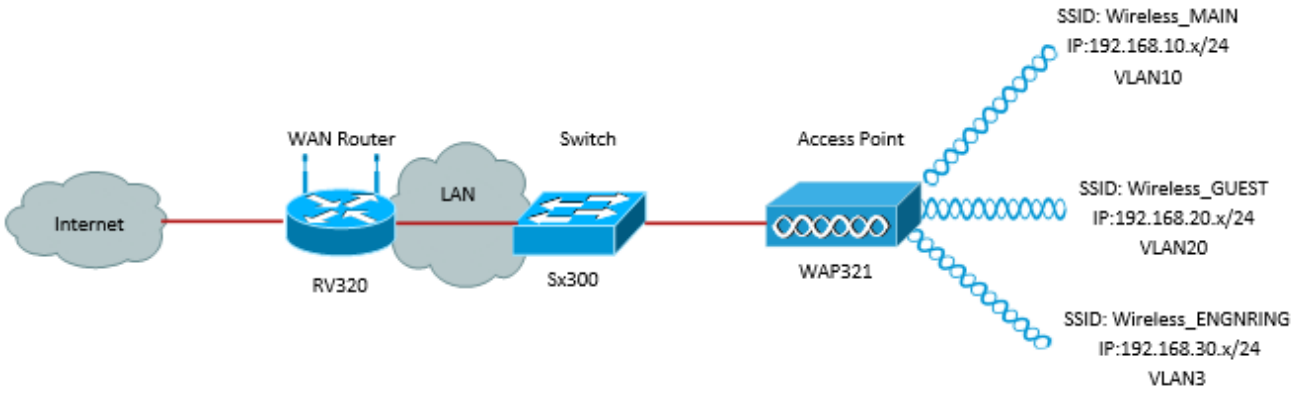
Dispositivos aplicáveis

RV320 Roteador VPN
WAP321 Ponto de acesso Wireless-N
Switch Sx300 Series

Versão de software

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

Topologia de rede



A imagem acima ilustra uma implementação de exemplo para acesso sem fio usando vários SSIDs com um WAP, switch e roteador para pequenas empresas da Cisco. O WAP se conecta ao switch e usa a interface de tronco para transportar vários pacotes de VLAN. O switch se conecta ao roteador WAN através da interface de tronco e o roteador WAN executa o roteamento entre VLANs. O roteador WAN se conecta à Internet. Todos os dispositivos sem fio se conectam ao WAP.

Recursos Principais

A combinação do recurso de roteamento entre VLANs fornecido pelo roteador Cisco RV com o recurso de isolamento de SSID sem fio fornecido por um ponto de acesso de pequenas empresas fornece uma solução simples e segura para acesso sem fio em qualquer rede de pequenas empresas da Cisco.

Roteamento entre VLANs

Os dispositivos de rede em diferentes VLANs não podem se comunicar com cada um sem que um roteador roteie o tráfego entre as VLANs. Em uma rede de pequena empresa, o roteador executa o roteamento entre VLANs para redes com e sem fio. Quando o roteamento entre VLANs é desabilitado para uma VLAN específica, os hosts nessa VLAN não poderão se comunicar com hosts ou dispositivos em outra VLAN.

Isolamento de SSID sem fio

Há dois tipos de isolamento de SSID sem fio. Quando o isolamento sem fio (dentro do SSID) está ativado, os hosts no mesmo SSID não poderão se ver. Quando o isolamento sem fio (entre SSID) está ativado, o tráfego em um SSID não é encaminhado para nenhum outro SSID.

IEEE 802.1x

O padrão IEEE 802.1x especifica os métodos usados para implementar o controle de acesso de redes baseadas em portas que é usado para fornecer acesso de rede autenticado a redes Ethernet. A autenticação baseada em porta é um processo que permite que somente as trocas de credenciais passem pela rede até que o usuário conectado à porta seja autenticado. A porta é chamada de porta descontrolada durante o tempo em que as credenciais são trocadas. A porta é chamada de porta controlada depois que a autenticação é concluída. Isso se baseia em duas portas virtuais existentes em uma única porta física.

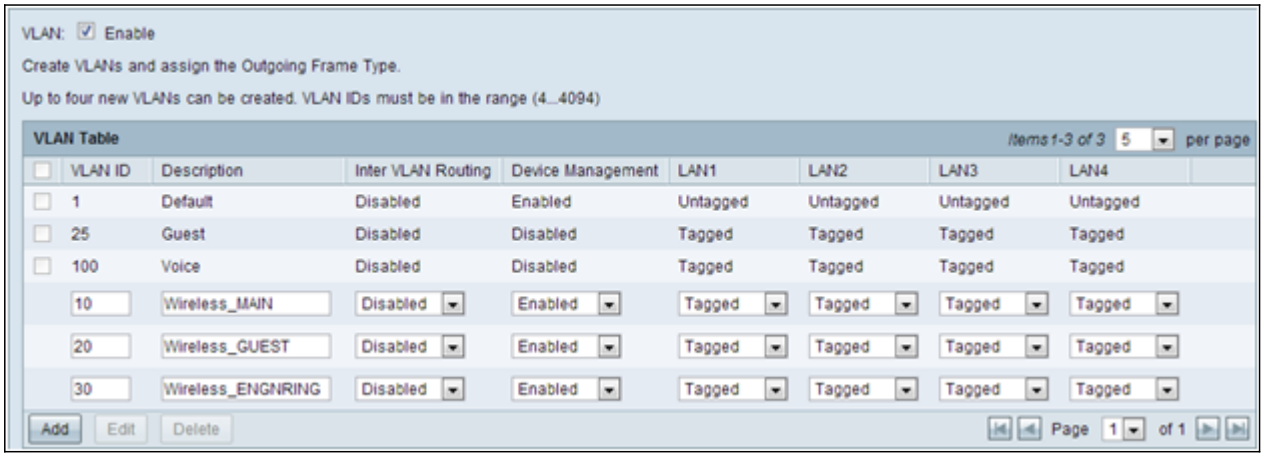
Isso usa as características físicas da infraestrutura de LAN comutada para autenticar

dispositivos conectados a uma porta de LAN. O acesso à porta pode ser negado se o processo de autenticação falhar. Este padrão foi originalmente projetado para redes Ethernet com fio, mas foi adaptado para uso em LANs sem fio 802.11.

Configuração do RV320

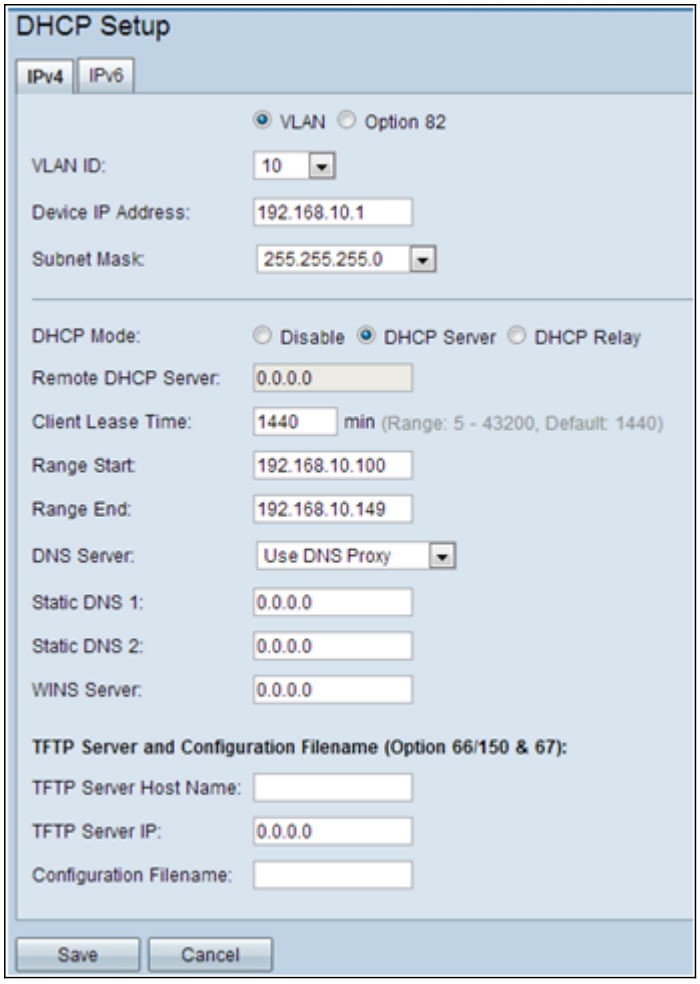
Neste cenário, queremos que o RV320 atue como o servidor DHCP da rede, portanto, precisaremos configurá-lo, bem como configurar VLANs separadas no dispositivo. Para iniciar, faça login no roteador conectando-se a uma das portas Ethernet e indo para 192.168.1.1 (supondo que você ainda não tenha alterado o endereço IP do roteador).

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Port Management > VLAN Membership**. Uma nova página é aberta. Estamos criando 3 VLANs separadas para representar públicos-alvo diferentes. Clique em **Adicionar** para adicionar uma nova linha e editar a ID e a descrição da VLAN. Você também precisará certificar-se de que a VLAN esteja definida como *Marcada* em qualquer interface na qual ele precise viajar.



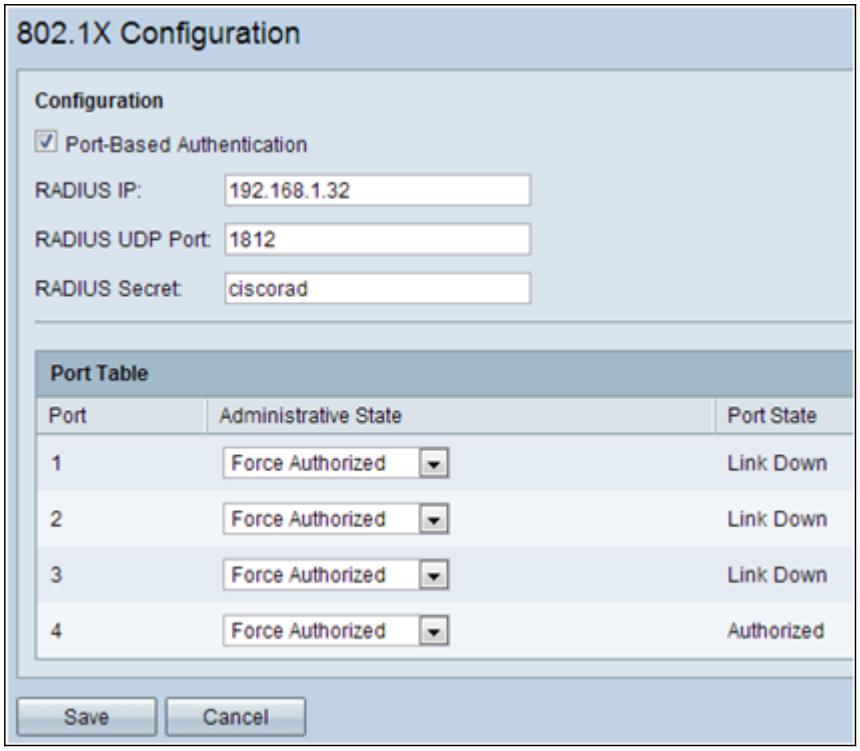
Etapa 2. Faça login no utilitário de configuração da Web e selecione **DHCP Menu > DHCP Setup**. A página *DHCP Setup (Configuração de DHCP)* é aberta:

- Na caixa suspensa VLAN ID, selecione a VLAN para a qual você está configurando o pool de endereços (neste exemplo, VLANs 10, 20 e 30).
- Configure o endereço IP do dispositivo para esta VLAN e defina o Intervalo de endereços IP. Você também pode habilitar ou desabilitar o proxy DNS aqui, se desejar, e isso dependerá da rede. Neste exemplo, o Proxy DNS trabalhará para encaminhar solicitações de DNS.
- Clique em **Salvar** e repita esta etapa para cada VLAN.



Etapa 3. No painel de navegação, selecione **Port Management > 802.1x Configuration**. A página *802.1X Configuration* é aberta:

- Ative a autenticação baseada em porta e configure o endereço IP do servidor.
- RADIUS Secret é a chave de autenticação usada para se comunicar com o servidor.
- Escolha quais portas usarão essa autenticação e clique em **Salvar**.

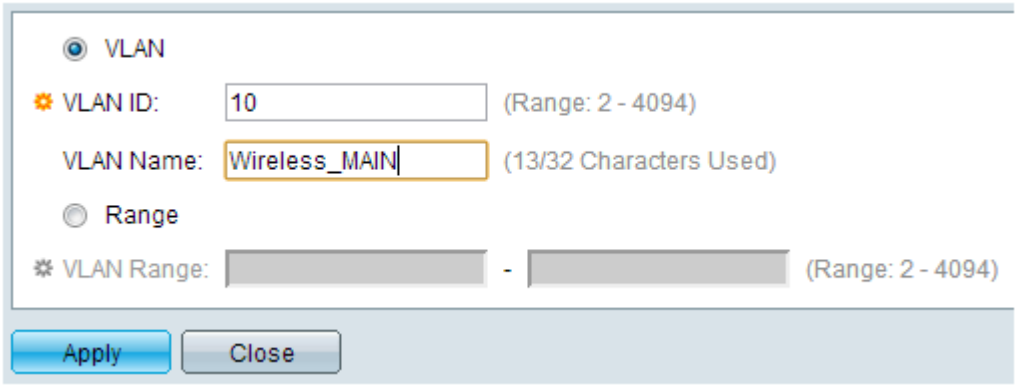


Configuração Do Sx300

O switch SG300-10MP funciona como um intermediário entre o roteador e o WAP321 para simular um ambiente de rede realista. A configuração no switch é a seguinte.

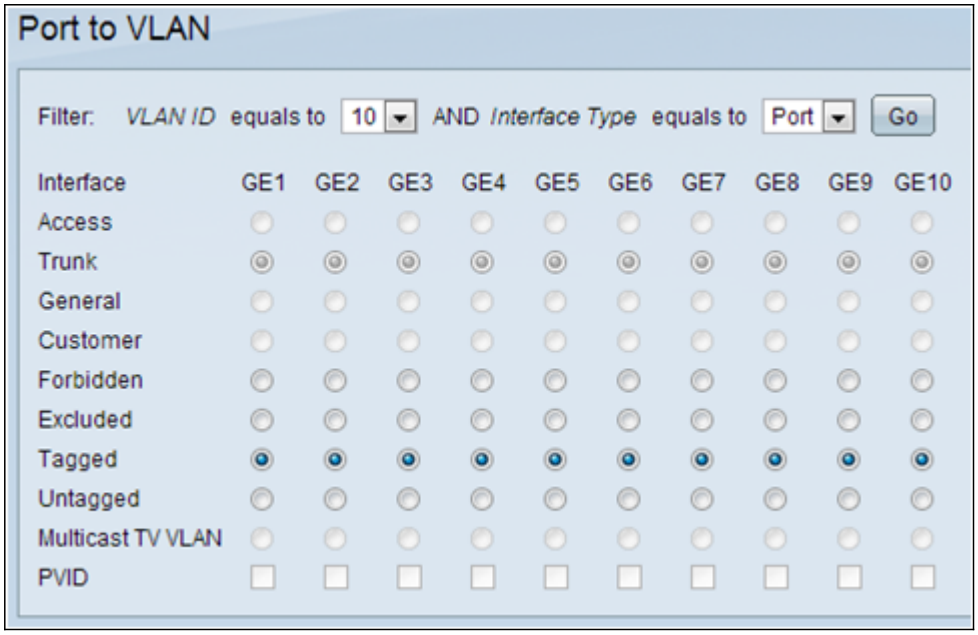
Etapa 1. Faça login no utilitário de configuração da Web e selecione **VLAN Management > Create VLAN**. Uma nova página é aberta:

Etapa 2. Clique em Add. Uma nova janela é exibida. Insira a ID da VLAN e o nome da VLAN (use a mesma descrição da Seção I). Clique em Apply (Aplicar) e repita esta etapa para as VLANs 20 e 30.



Etapa 3. No painel de navegação, selecione **VLAN Management > Port to VLAN**. Uma nova página é aberta:

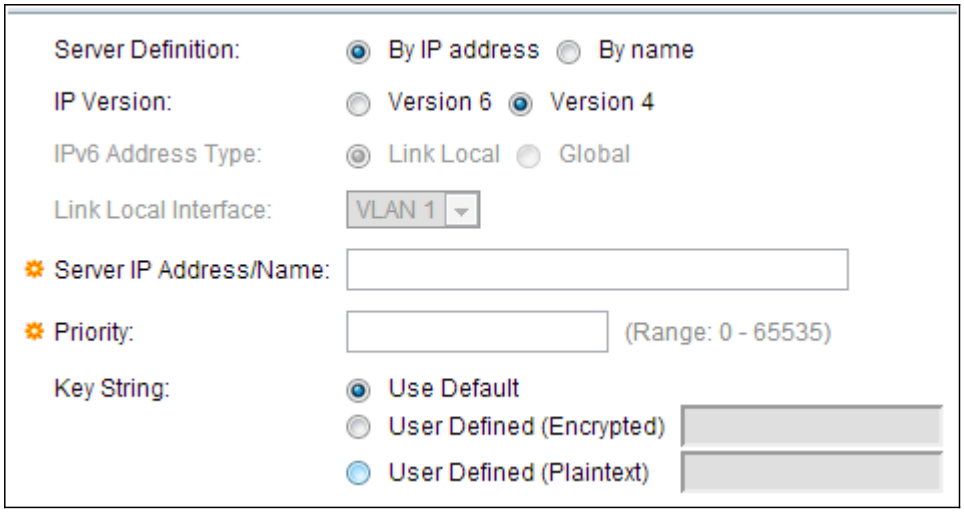
- Na parte superior da página, defina "VLAN ID igual a" para a VLAN que você está adicionando (neste caso, VLAN 10) e clique em **Ir** à direita. Isso atualizará a página com as configurações para essa VLAN.
- Altere a configuração em cada porta para que a VLAN 10 esteja agora "Marcada" em vez de "Excluída". Repita essa etapa para as VLANs 20 e 30.



Etapa 4. No painel de navegação, selecione **Security > Radius** . A página *RADIUS* é aberta:

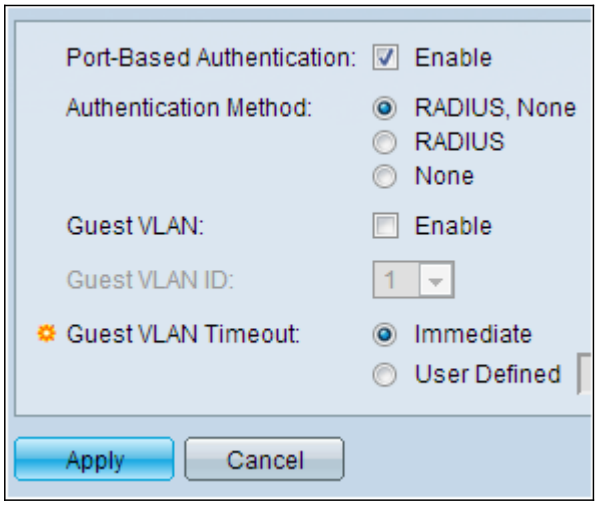
- Escolha o método de controle de acesso a ser usado pelo servidor RADIUS, seja controle de acesso de gerenciamento ou autenticação baseada em porta. Escolha Controle de acesso baseado em porta e clique em **Aplicar**.
- Clique em **Adicionar** na parte inferior da página para adicionar um novo servidor para autenticação.

Etapa 5. Na janela exibida, você configurará o endereço IP do servidor, nesse caso 192.168.1.32. Você precisará definir uma prioridade para o servidor, mas como neste exemplo temos apenas um servidor para autenticar na prioridade, não importa. Isso é importante se você tiver vários servidores RADIUS para escolher. Configure a chave de autenticação e o restante das configurações pode ser deixado como padrão.

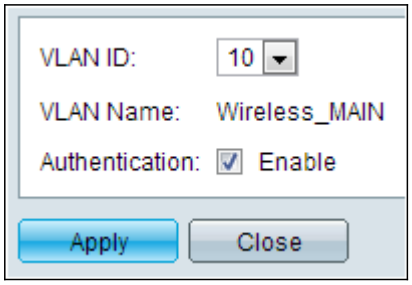


Etapa 6. No painel de navegação, selecione **Security > 802.1X > Properties**. Uma nova página é aberta:

- Marque **Enable** para ativar a autenticação 802.1x e escolha o método de autenticação. Nesse caso, estamos usando um servidor RADIUS, portanto, escolha a primeira ou a segunda opção.
- Clique em Apply.



Passo 7. Escolha uma das VLANs e clique em **Editar**. Uma nova janela é exibida. Marque **Enable** para permitir a autenticação nessa VLAN e clique em *Apply*. Repita para cada VLAN.



Configuração do WAP321

Os Pontos de Acesso Virtuais (VAPs) segmentam a LAN sem fio em vários domínios de broadcast que são o equivalente sem fio das VLANs Ethernet. Os VAPs simulam vários

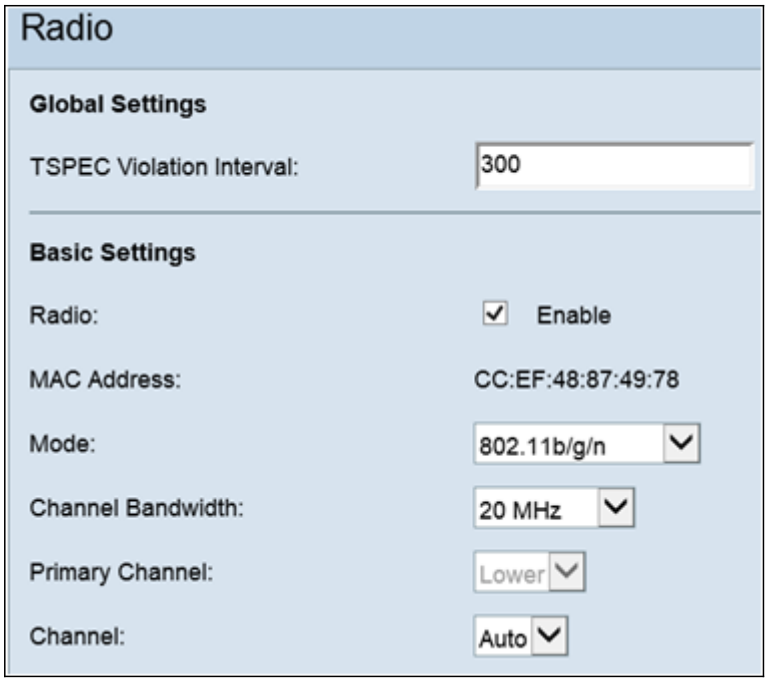
pontos de acesso em um dispositivo WAP físico. Até quatro VAPs são suportados no WAP121 e até oito VAPs são suportados no WAP321.

Cada VAP pode ser habilitado ou desabilitado independentemente, com exceção de VAP0. VAP0 é a interface física de rádio e permanece habilitada enquanto o rádio estiver ativado. Para desabilitar a operação do VAP0, o próprio rádio deve estar desabilitado.

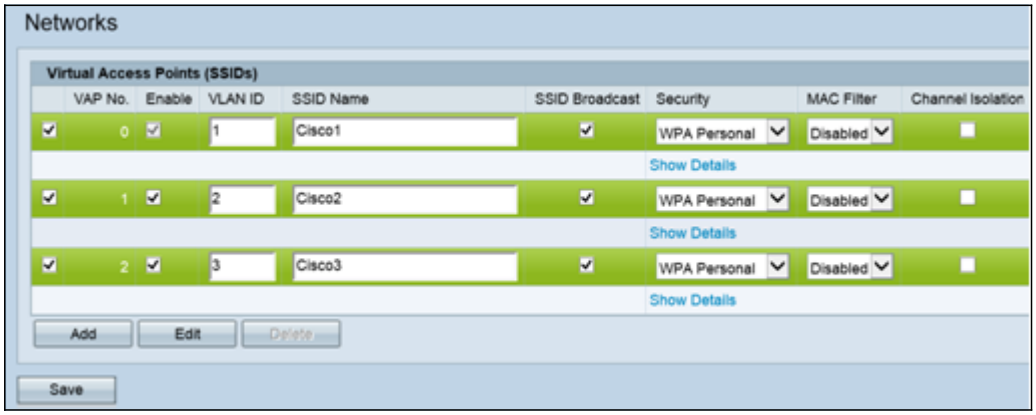
Cada VAP é identificado por um SSID (Service Set Identifier, identificador do conjunto de serviços) configurado pelo usuário. Vários VAPs não podem ter o mesmo nome SSID. Os broadcasts de SSID podem ser ativados ou desativados independentemente em cada VAP. A transmissão de SSID está habilitada por padrão.

Etapa 1. Faça login no utilitário de configuração da Web e selecione **Wireless > Radio**. A página *Rádio* é aberta:

- Clique na caixa de seleção **Habilitar** para habilitar o rádio sem fio.
- Click **Save**. O rádio será então ligado.



Etapa 2.No painel de navegação, selecione **Wireless > Networks**. A página *Rede* é aberta:



Note: O SSID padrão para VAP0 é ciscosb. Cada VAP adicional criado tem um nome SSID em branco. Os SSIDs para todos os VAPs podem ser configurados para outros valores.

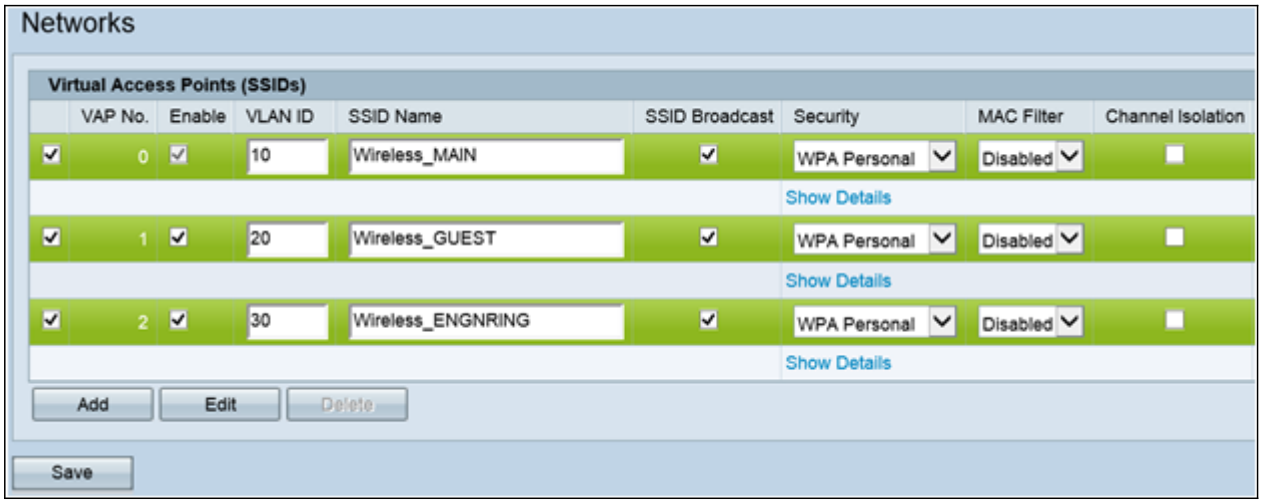
Etapa 3. Cada VAP é associado a uma VLAN, que é identificada por uma VLAN ID (VID).

Um VID pode ser qualquer valor de 1 a 4094, inclusive. O WAP121 suporta cinco VLANs ativas (quatro para WLAN mais uma VLAN de gerenciamento). O WAP321 suporta nove VLANs ativas (oito para WLAN mais uma VLAN de gerenciamento).

Por padrão, o VID atribuído ao utilitário de configuração para o dispositivo WAP é 1, que também é o VID não marcado padrão. Se o VID de gerenciamento for o mesmo que o VID atribuído a um VAP, os clientes WLAN associados a esse VAP específico podem administrar o dispositivo WAP. Se necessário, uma lista de controle de acesso (ACL) pode ser criada para desabilitar a administração de clientes WLAN.

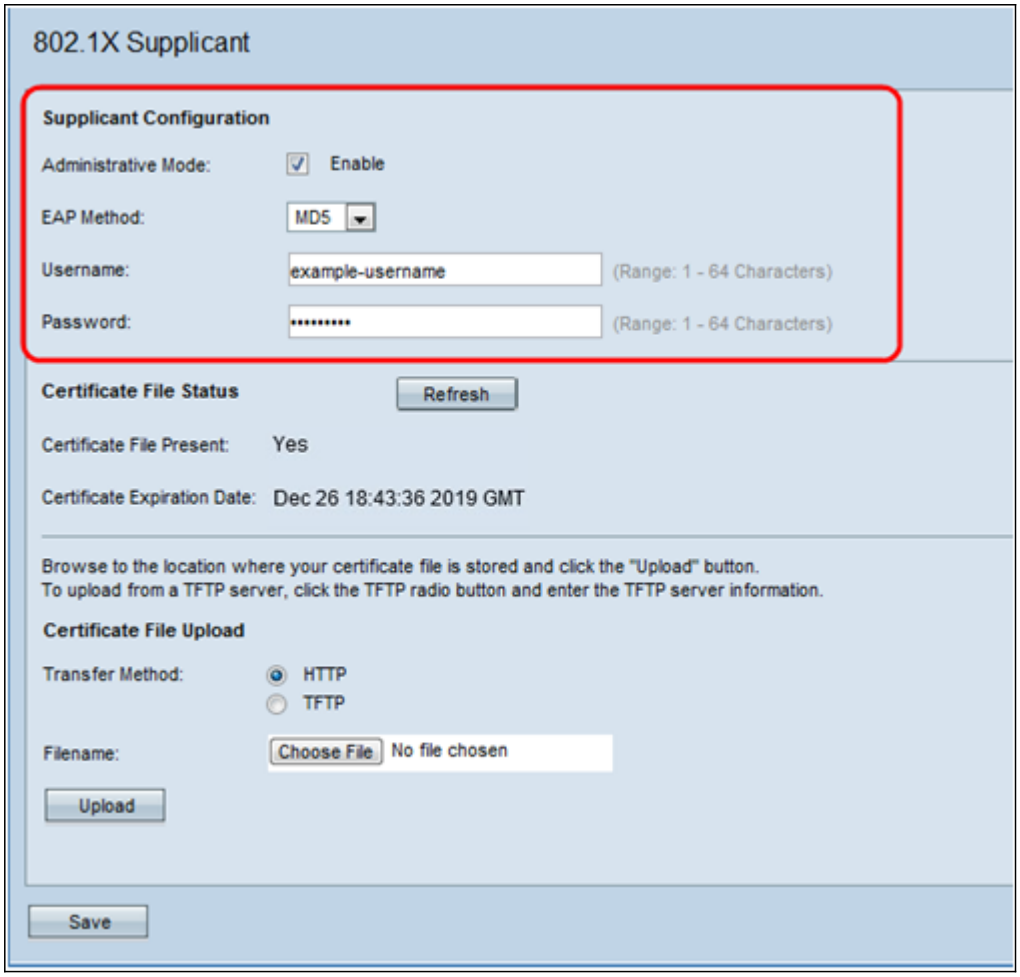
Nesta tela, as seguintes etapas devem ser executadas:

- Clique nos botões de marca de seleção à esquerda para editar os SSIDs:
- Digite o valor necessário para a ID da VLAN na caixa ID da VLAN
- Clique no botão **Salvar** depois que os SSIDs forem inseridos.



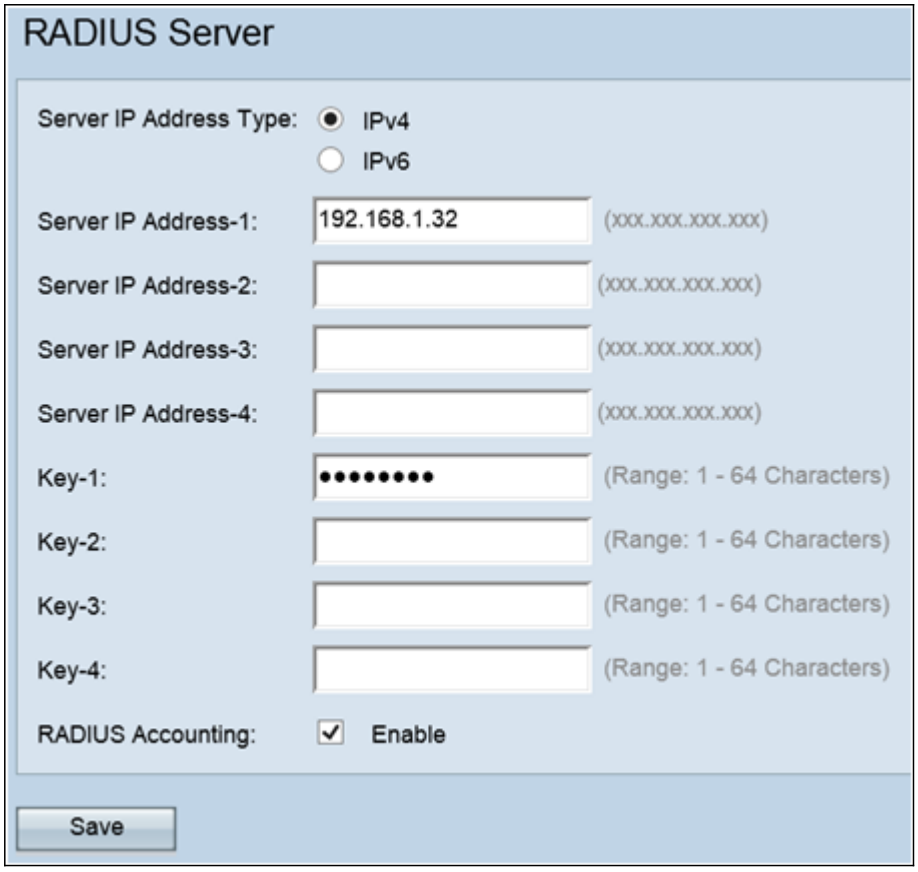
Etapa 4. No painel de navegação, selecione **Segurança do sistema > Requerente 802.1X**. A página *do requerente 802.1X* é aberta:

- Marque **Enable** no campo Administrative Mode (Modo administrativo) para permitir que o dispositivo atue como um suplicante na autenticação 802.1X.
- Escolha o tipo apropriado de método EAP (Extensible Authentication Protocol) na lista suspensa no campo EAP Method.
- Insira o nome de usuário e a senha que o ponto de acesso usa para obter autenticação do autenticador 802.1X nos campos Nome de usuário e Senha. O comprimento do nome de usuário e da senha deve ser de 1 a 64 caracteres alfanuméricos e de símbolo. Isso já deve ser configurado no servidor de autenticação.
- Clique em **Save (Salvar) para salvar as configurações.**



Note: A área Status do arquivo de certificado mostra se o arquivo de certificado está presente ou não. O certificado SSL é um certificado assinado digitalmente por uma autoridade de certificado que permite que o navegador da Web tenha uma comunicação segura com o servidor da Web. Para gerenciar e configurar o certificado SSL, consulte o artigo Gerenciamento de certificado SSL (Secure Socket Layer) em Pontos de acesso WAP121 e WAP321

Etapa 5. No painel de navegação, selecione **Security > RADIUS Server**. A página *Servidor RADIUS* é aberta. Insira os parâmetros e clique no botão **Save (Salvar)** depois que os parâmetros do servidor Radius tiverem sido inseridos.


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