Habilitando las redes inalámbricas múltiples en el Punto de acceso del VPN Router RV320, de la Tecnología inalámbrica-n WAP321, y Switches de las Sx300 Series

Objetivo

En un entorno comercial siempre cambiante, su red de la Pequeña empresa tiene que ser potente, flexible, accesible, y altamente confiable, especialmente cuando el crecimiento es una prioridad. El renombre de los dispositivos de red inalámbrica exponencial ha crecido, que no es una sorpresa. Las redes inalámbricas son rentables, fáciles de desplegar, flexible, scalable, y móvil, seemlessly proporcionando a los recursos de red. La autenticación permite que los dispositivos de red verifiquen y que garanticen la legitimidad de un usuario mientras que protege la red contra los usuarios no autorizados. Es importante desplegar una infraestructura de red inalámbrica segura y manejable.

El VPN Router PÁLIDO del gigabit dual de Cisco RV320 proporciona una Conectividad confiable, altamente del acceso seguro para usted y a sus empleados. El Punto de acceso de la A elección-banda de la Tecnología inalámbrica-n de Cisco WAP321 con la configuración monopunto soporta las conexiones de alta velocidad con Gigabit Ethernet. Los Bridges conectan los LAN juntos sin hilos, haciéndolo más fácil para que las Pequeñas empresas amplíen sus redes.

Este artículo proporciona la dirección gradual para la configuración requerida para habilitar el acceso de red inalámbrica en una red de la Pequeña empresa de Cisco, incluyendo la encaminamiento de la red de área local inter-virtual (VLA N), los identificadores del conjunto del servicio múltiple (SSID), y las configuraciones de la seguridad de red inalámbrica en el router, el Switch, y los Puntos de acceso.

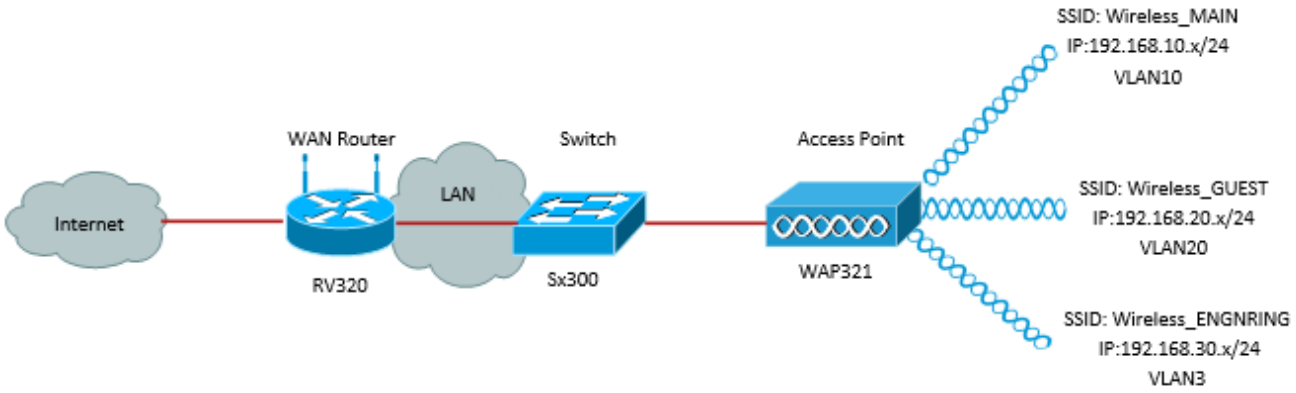
Dispositivos aplicables

- VPN Router RV320
- Punto de acceso de la Tecnología inalámbrica-n WAP321
- Switch de las Sx300 Series

Versión del software

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

Topología de red



La imagen antedicha ilustra una implementación de la muestra para el acceso de red inalámbrica usando los SSID múltiples con una Pequeña empresa WAP de Cisco, el Switch y el router. El WAP conecta con el Switch y utiliza la interfaz de tronco para transportar los paquetes del VLAN múltiple. El Switch conecta con el router de WAN a través de la interfaz de tronco y el router de WAN realiza el Routing entre VLAN. El router de WAN conecta con Internet. Todos los dispositivos de red inalámbrica conectan con el WAP.

Características fundamentales

Combinar la característica del Routing entre VLAN proporcionada por el router de Cisco rv con la característica del aislamiento de la Tecnología inalámbrica SSID proporcionada por un Punto de acceso de la Pequeña empresa proporciona un simple y asegura la solución para el acceso de red inalámbrica en cualquier red existente de la Pequeña empresa de Cisco.

Routing entre VLAN

Los dispositivos de red en diversos VLA N no pueden comunicar con cada uno sin un router para rutear el tráfico entre los VLA N. En una red de la Pequeña empresa, el router realiza el Routing entre VLAN para haber atado con alambre y las redes inalámbricas. Cuando el Routing entre VLAN se inhabilita para un VLA N específico, los host en ese VLA N no podrán comunicar con los host o los dispositivos en otro VLA N.

Aislamiento inalámbrico SSID

Hay dos tipos de aislamiento inalámbrico SSID. Cuando se habilita el aislamiento inalámbrico (dentro del SSID), los host en el mismo SSID no podrán considerarse. Cuando se habilita el aislamiento inalámbrico (entre el SSID), el tráfico en un SSID no se remite a ningún otro SSID.

IEEE 802.1X

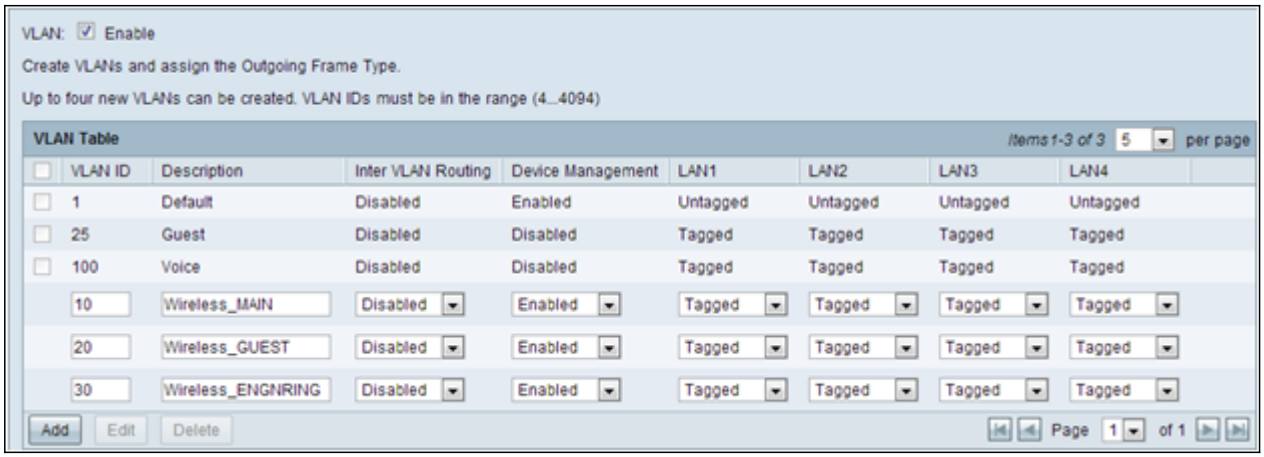
El estándar del IEEE 802.1X especifica los métodos usados para implementar el control de acceso de las redes del acceso basado que se utiliza para proporcionar el acceso a la red autenticado a las redes Ethernet. La autenticación del acceso basado es un proceso que permite que solamente los intercambios credenciales atraviesen la red hasta que autentiquen al usuario conectado con el puerto. El puerto se llama un puerto incontrolado durante el tiempo los intercambios de las credenciales. El puerto se llama un puerto controlado después de que se complete la autenticación. Esto se basa en dos puertos virtuales que existen dentro de un solo puerto físico.

Esto utiliza las características físicas de la infraestructura LAN conmutada para autenticar los dispositivos asociados a un puerto LAN. El acceso al puerto puede ser negado si el proceso de autenticación falla. Este estándar fue diseñado originalmente para las redes de los Ethernetes de cable, no obstante se ha adaptado para el uso en la Tecnología inalámbrica LAN del 802.11.

Configuración RV320

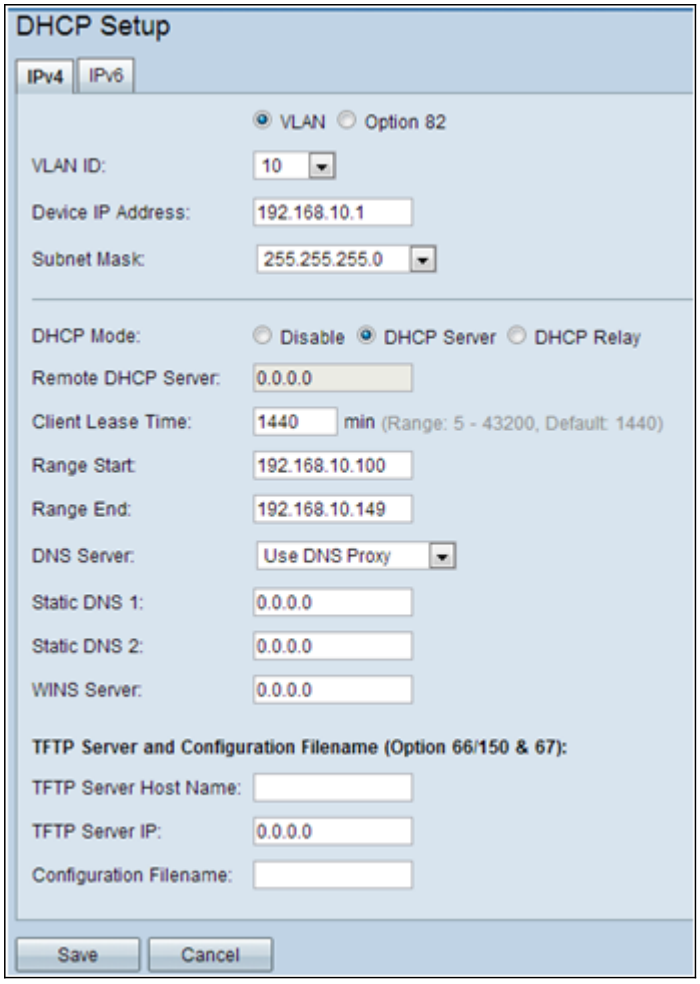
En este escenario quisiéramos que el RV320 actuara como el servidor DHCP para la red, así que necesitaremos fijar eso los VLAN distintos ascendentes así como de la configuración en el dispositivo. Para comenzar, iniciar sesión al router conectando con uno de los accesos de Ethernet y yendo a 192.168.1.1 (si se asume que le no han cambiado ya la dirección IP del router).

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **administración de puerto > la calidad de miembro de VLAN**. Una nueva página se abre. Estamos creando 3 VLAN distintos para representar a diversos públicos objetivos. Haga clic **agregan** para agregar una línea nueva y para editar el VLAN ID y la descripción. Usted también necesitará aseegurarse que el VLA N esté fijado a *marcado con etiqueta* en cualquier interfaz en la cual necesiten viajar.



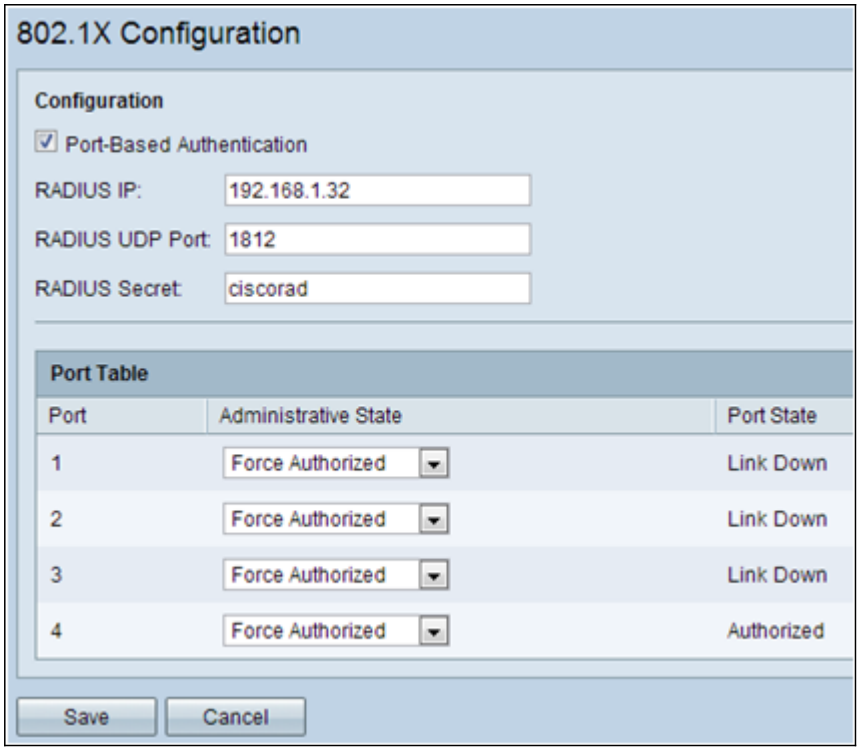
Paso 2. Inicie sesión a la utilidad de configuración de la red y seleccione el **menú del DHCP > la configuración del DHCP**. *La página de configuración del DHCP* se abre:

- En el cuadro del descenso VLAN ID, seleccione el VLA N que usted está configurando a la agrupación de direcciones para (en los VLA N 10, 20, y 30 de este ejemplo).
- Configure la dirección IP del dispositivo para este VLA N, y fije el alcance del IP Address. Usted puede también habilitar o inhabilitar el proxy DNS aquí si usted desea, y esto será dependiente en la red. En este ejemplo, el proxy DNS trabajará para remitir las peticiones DNS.
- Haga clic la **salvaguardia** y relance este paso para cada VLA N.



Paso 3. En el SCR_INVALID, seleccione la **administración de puerto > la configuración del 802.1x**. *La página de configuración del 802.1x* se abre:

- Habilite la autenticación del acceso basado y configure la dirección IP del servidor.
- El secreto RADIUS es la clave de autenticación usada para comunicar con el servidor.
- Elija qué puertos utilizarán esta autenticación y harán clic la **salvaguardia**.

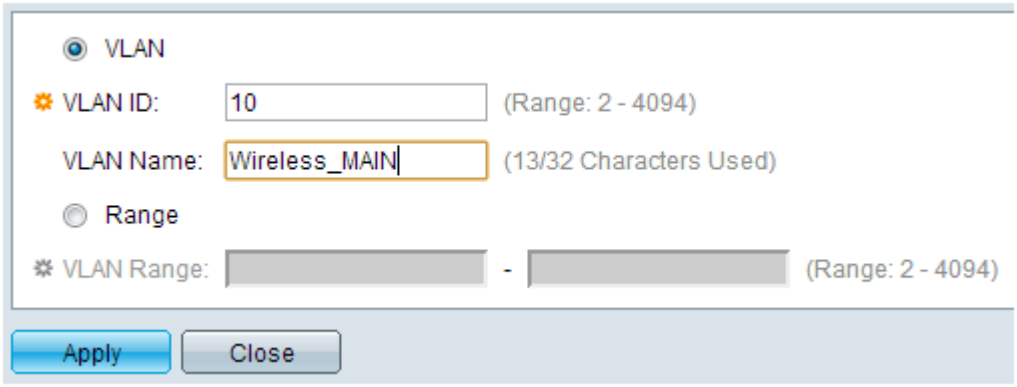


Configuración Sx300

El Switch SG300-10MP funciona como intermediario entre el router y el WAP321 para simular un entorno de red realista. La configuración en el Switch está como sigue.

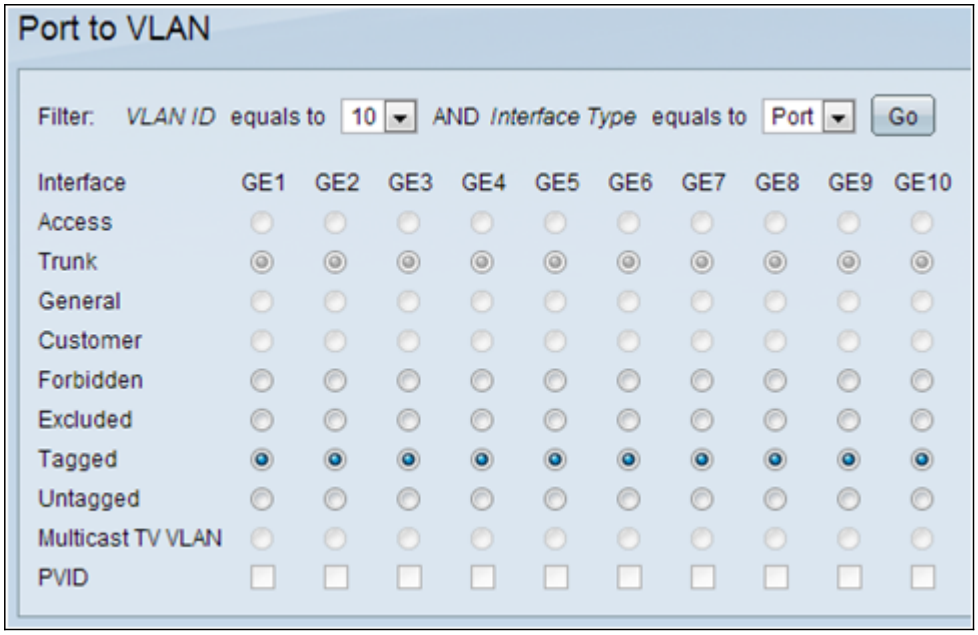
Paso 1. Inicie sesión a la utilidad de configuración de la red, y la **administración de VLAN** selecta **> crea el VLA N**. Una nueva página se abre:

Paso 2. Haga click en Add Una nueva ventana aparece. Ingrese el VLAN ID y el nombre del VLA N (utilice lo mismo que la descripción de la sección I). El tecleo aplica, y después relanza este paso para los VLA N 20 y 30.



Paso 3. En el SCR_INVALID, **administración de VLAN** selecta **> puerto al VLA N**. Una nueva página se abre:

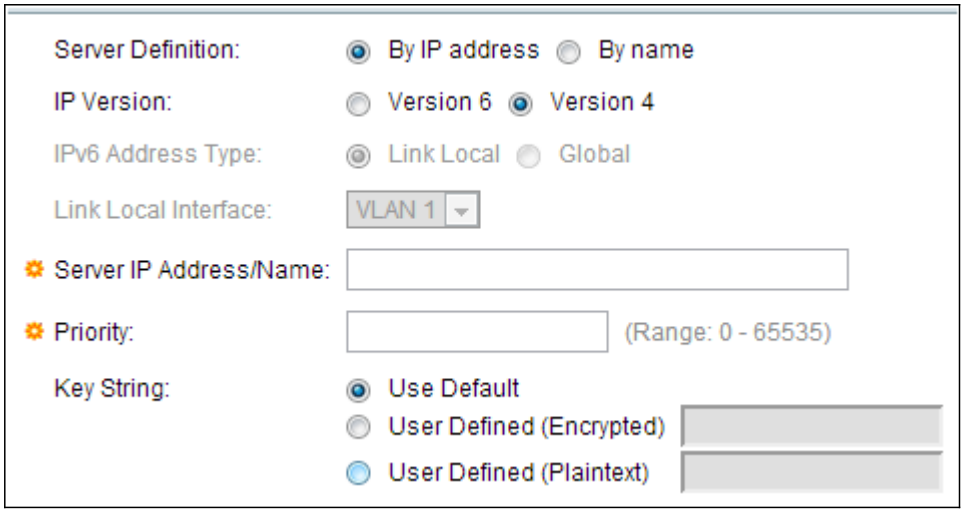
- En la cima de la página fijada los “iguales VLAN ID a” al VLA N usted está agregando (en este caso, el VLA N 10) y entonces hace clic **va** a la derecha. Esto pondrá al día la página con las configuraciones para ese VLA N.
- Cambie la configuración en cada puerto para “ahora marcar” el VLAN10 con etiqueta en vez de “excluido.” Relance este paso para los VLA N 20 y 30.



Paso 4. En el SCR_INVALID, seleccione la **Seguridad > el radio**. La página *RADIUS* se abre:

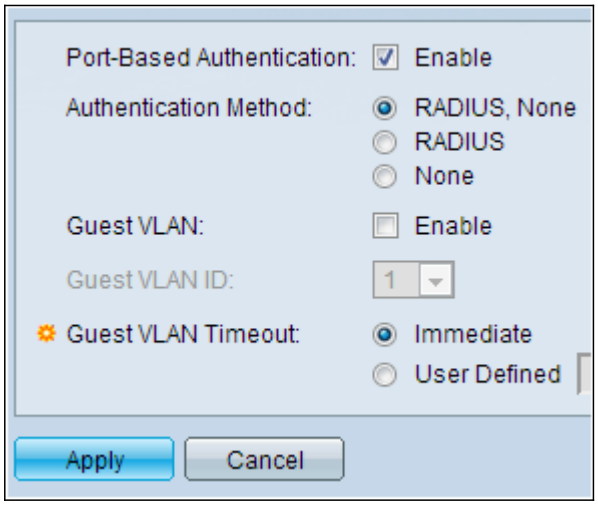
- Elija el método de control de acceso que se utilizará por el servidor de RADIUS, control de acceso de la Administración o autenticación del acceso basado. Elija el control de acceso basado puerto y el tecleo **se aplica**.
- El tecleo **agrega** en la parte inferior de la página para agregar un nuevo servidor para autenticar a.

Paso 5. En la ventana que aparece usted configurará la dirección IP del servidor, en este caso 192.168.1.32. Usted necesitará establecer una prioridad para el servidor, pero puesto que en este ejemplo tenemos solamente un servidor para autenticar a la prioridad no importa. Esto es importante si usted tiene los servidores de RADIUS múltiples a elegir de. Configure la clave de autenticación y el resto de las configuraciones se puede dejar como valor por defecto.

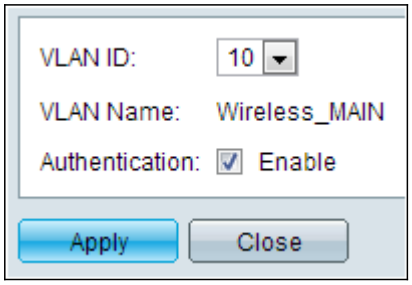


Paso 6. En el SCR_INVALID, seleccione la **Seguridad > el 802.1x > las propiedades**. Una nueva página se abre:

- Marque el **permiso** para girar la autenticación del 802.1x y para elegir el método de autentificación. En este caso estamos utilizando a un servidor de RADIUS así que elija la primera o segunda opción.
- Haga clic en Apply (Aplicar).



Paso 7. Elija uno de los VLA N y el tecleo **edita**. Una nueva ventana aparece. Marque el **permiso** para permitir la autenticación en ese VLA N y el tecleo *se aplica*. Relance para cada VLA N.



Configuración WAP321

Las puntas de acceso virtual (VAPs) dividen el Wireless LAN en segmentos en los dominios de broadcast múltiples que son el equivalente de la Tecnología inalámbrica de las redes

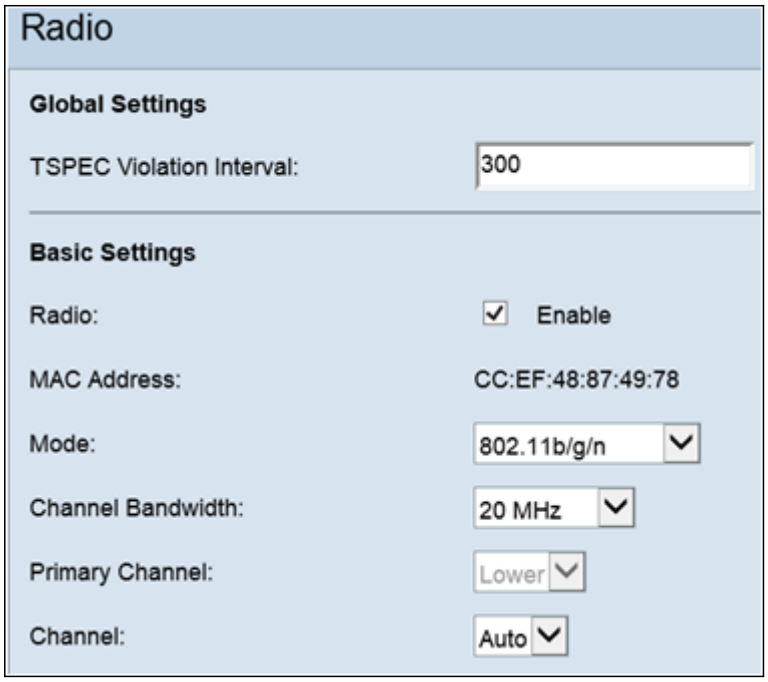
Ethernet VLAN. VAPs simula los múltiples puntos de acceso en un dispositivo físico WAP. Hasta cuatro VAPs se soportan en el WAP121 y hasta ocho VAPs se soportan en el WAP321.

Cada VAP se puede habilitar o inhabilitar independientemente, a excepción de VAP0. VAP0 es la interfaz radio física y sigue siendo habilitado mientras se habilite la radio. Para inhabilitar la operación de VAP0, la radio sí mismo debe ser inhabilitada.

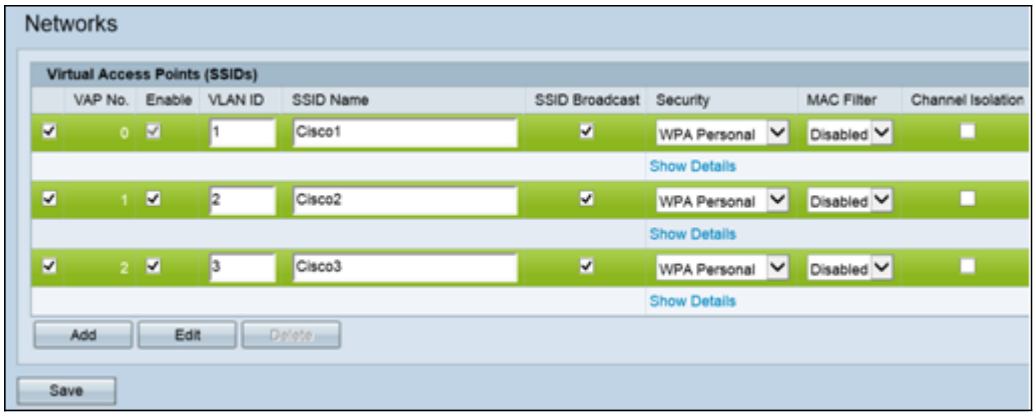
Cada VAP es identificado por un Service Set Identifier (SSID) del usuario configurado. VAPs múltiple no puede tener el mismo nombre SSID. Los broadcasts SSID se pueden habilitar o inhabilitar independientemente en cada VAP. El broadcast SSID se habilita por abandono.

Paso 1. Inicie sesión a la utilidad de configuración de la red y seleccione el **>Radio inalámbrico**. *La página de radio* se abre:

- Haga clic la casilla de verificación del **permiso** para habilitar la radio inalámbrica.
- Click **Save**. La radio entonces será girada.



Paso 2.On el SCR_INVALID, **Tecnología inalámbrica** selecta **> redes**. La página de la *red* se abre:



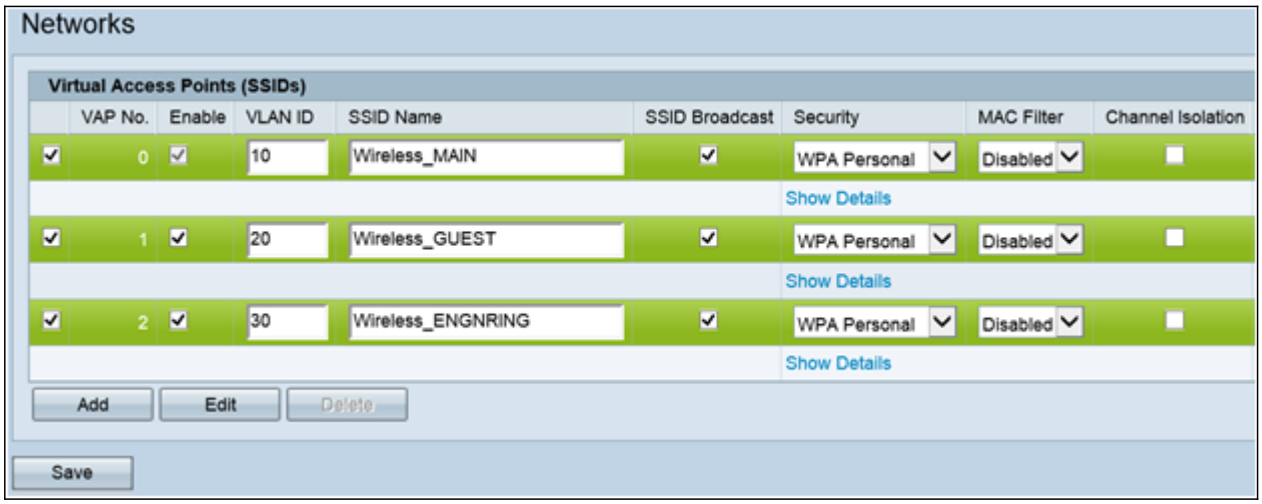
Nota: El SSID predeterminado para VAP0 es ciscosb. Cada VAP adicional creado tiene un nombre del SSID en blanco. Los SSID para todo el VAPs se pueden configurar a otros valores.

Paso 3. Cada VAP se asocia a un VLA N, que es identificado por un VLAN ID (VID). Un VID puede ser cualquier valor a partir de la 1 a 4094, inclusivo. El WAP121 soporta cinco VLAN activos (cuatro para la red inalámbrica (WLAN) más un VLAN de administración). El WAP321 soporta nueve VLAN activos (ocho para la red inalámbrica (WLAN) más un VLAN de administración).

Por abandono, el VID asignado a la utilidad de configuración para el dispositivo WAP es 1, que es también el VID untagged predeterminado. Si la Administración VID es lo mismo que el VID asignado a un VAP, después los clientes WLAN asociados a este VAP específico pueden administrar el dispositivo WAP. Si es necesario, un Access Control List (ACL) se puede crear para inhabilitar la administración de los clientes WLAN.

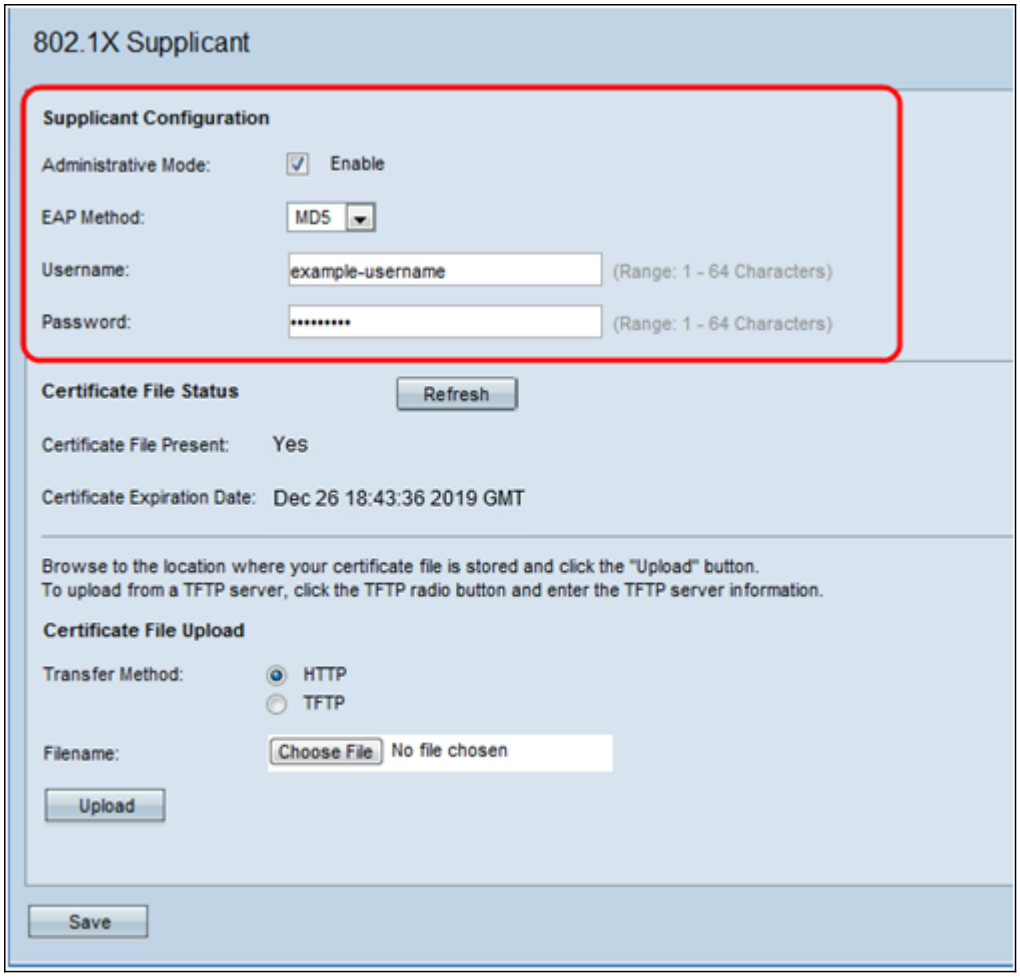
En esta pantalla, las medidas siguientes deben ser tomadas:

- Haga clic los botones de la marca de tilde en el lado izquierdo para editar los SSID:
- Ingrese el valor necesario el VLAN ID en el rectángulo VLAN ID
- Haga clic el **botón Save Button** una vez que se han ingresado los SSID.



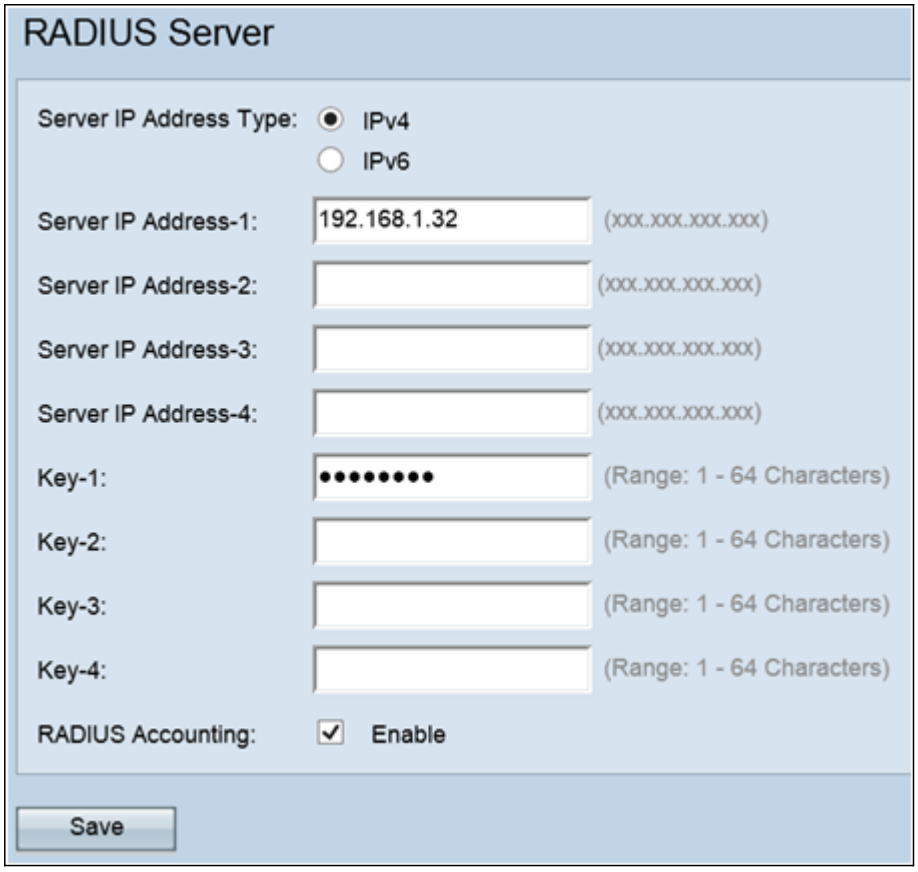
Paso 4. En el SCR_INVALID, seleccione el **supplicant de la seguridad del sistema > del 802.1x**. La página del *supplicant del 802.1x* se abre:

- Marque el **permiso** en el campo del modo administrativo para permitir al dispositivo para actuar como supplicant en la autenticación del 802.1x.
- Elija el tipo apropiado de método del Protocolo de Autenticación Extensible (EAP) de la lista desplegable en el campo del método EAP.
- Ingrese el nombre de usuario y contraseña que el Punto de acceso utiliza para conseguir a autenticación del authenticator del 802.1x en los campos del nombre de usuario y contraseña. La longitud del nombre de usuario y contraseña debe ser a partir 1 a 64 caracteres alfanuméricos y del símbolo. Esto se debe configurar ya en el servidor de autenticación.
- **Salvaguardia del** tecleo para salvar las configuraciones.



Nota: La área de estado del archivo de certificado muestra si el archivo de certificado está presente o no. El certificado SSL es un certificado firmado digitalmente por un Certificate Authority que permite que el buscador Web tenga una comunicación segura con el servidor Web. Para manejar y configurar el certificado SSL refiera a la administración de certificados del Secure Socket Layer (SSL) del artículo en los Puntos de acceso WAP121 y WAP321

Paso 5. En el SCR_INVALID, seleccione la **Seguridad > al servidor de RADIUS**. *La página del servidor RADIUS* se abre. Ingrese los parámetros, y haga clic el **botón Save Button** una vez que se han ingresado los parámetros del servidor de RADIUS.


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