Activant de plusieurs réseaux sans fil sur le Point d'accès du routeur VPN RV320, du Wireless-N WAP321, et les Commutateurs de gamme Sx300

Objectif

Dans un environnement professionnel toujours changeant, votre réseau de petite entreprise doit être puissant, flexible, accessible, et fortement fiable, particulièrement quand la croissance est une haute priorité. Puisque les périphériques sans fil sont devenus abordables, la commodité, et sont facile à utiliser, leur utilisation a été exponentiellement s'est développée ces dernières années. L'authentification permet aux périphériques de réseau pour vérifier et garantir la légitimité d'un utilisateur et pour protéger le réseau contre des utilisateurs non autorisés. La connexion sans fil peut offrir à la capacité et à l'option de la mobilité de l'utilisateur quand il est difficile se déployer des réseaux câblés. Certains des avantages des réseaux Sans fil sont : Coûtez efficace et facile-à-le déployez, évolutivité, et Disponibilité des ressources en réseaux. Est de nos jours important pour déployer une infrastructure réseau Sans fil sécurisée et maniable.

Cisco RV320 conjuguent routeur VPN BLÊME de gigabit avec une interface utilisateur intuitive te permet d'être en service en quelques minutes. La fourniture fiable, fortement la Connectivité d'accès sécurisé pour vous et vos employés qui est si transparent vous ne sauront pas que c'est là. Le Point d'accès de Sélectionable-bande de Wireless-N de Cisco WAP321 avec l'installation unique est un lisse, abordable, et facile-à-déploie le périphérique qui fournit la connexion sans fil rapide et fortement sécurisée. Il prend en charge des connexions à haut débit avec l'interface de RÉSEAU LOCAL de Gigabit Ethernet pour des applications exigeantes. Jette un pont sur des lan câblée ensemble sans fil, le facilitant pour que les petites entreprises développent leurs réseaux.

Ce conseil intelligent fournit des conseils pas à pas pour la configuration exigée pour activer l'accès Sans fil dans un réseau de Cisco Small Business, y compris le Routage inter-VLAN, le multiple SSID, et les paramètres de sécurité sans fil sur le routeur, le commutateur, et les Points d'accès.

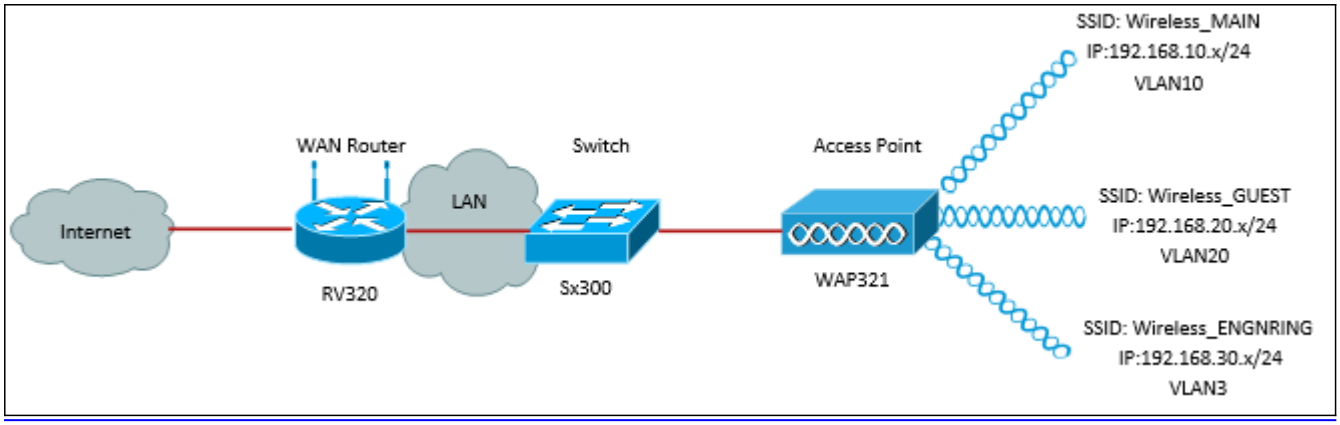
Périphérique applicable

- Routeur VPN RV320
- Point d'accès du Wireless-N WAP321
- Commutateur de gamme Sx300

Version de logiciel

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

Topologie du réseau



L'image ci-dessus illustre une implémentation d'échantillon pour l'accès Sans fil utilisant le multiple SSID avec un Cisco Small Business WAP, le commutateur et le routeur. Le WAP se connecte au commutateur et emploie l'interface de joncteur réseau pour transporter des paquets de VLAN multiple. Le commutateur se connecte au routeur WAN par l'interface de joncteur réseau et le routeur WAN effectue le Routage inter-VLAN. Le routeur WAN se connecte à l'Internet. Tous les périphériques sans fil se connectent au WAP.

Fonctionnalités principales

La combinaison de la fonctionnalité offerte de Routage inter-VLAN par le routeur de Cisco rv avec la fonctionnalité offerte d'isolation de la radio SSID par un Point d'accès de petite entreprise fournit une solution simple et sécurisée pour l'accès Sans fil sur n'importe quel réseau existant de Cisco Small Business.

Routage inter-VLAN

Les périphériques de réseau dans différents VLAN ne peuvent pas communiquer avec chacun sans routeur pour conduire le trafic entre les VLAN. Dans un réseau de petite entreprise, le routeur effectue le Routage inter-VLAN pour les réseaux de câble et Sans fil. Quand le Routage inter-VLAN est désactivé pour une particularité VLAN, les hôtes sur ce VLAN ne pourront pas communiquer avec des hôtes ou des périphériques sur un autre VLAN.

Isolation Sans fil SSID

Il y a deux types d'isolation Sans fil SSID. Quand l'isolation Sans fil (dans le SSID) est activée, les hôtes sur le même SSID ne pourront pas se voir. Quand l'isolation Sans fil (entre le SSID) est activée, le trafic sur un SSID n'est expédié à aucun autre SSID.

802.1x d'IEEE

La norme de 802.1x d'IEEE spécifie des méthodes utilisées pour implémenter le contrôle d'accès basé sur port de réseaux qui est utilisé pour fournir l'accès au réseau authentifié aux réseaux Ethernet. l'authentification basée sur port est un processus qui permet seulement à des échanges de créance pour traverser le réseau jusqu'à ce que l'utilisateur connecté au port soit authentifié. Le port s'appelle un port incontrôlé pendant le temps les échanges de qualifications. Le port s'appelle un port commandé après que l'authentification soit terminée. Ceci est basé sur deux ports virtuels existant dans un port physique simple.

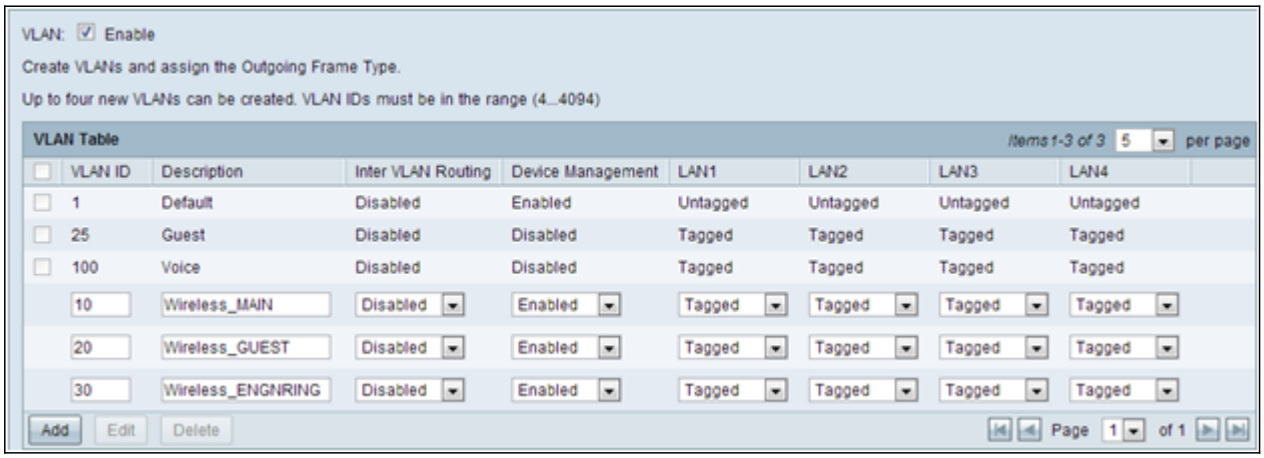
Ceci emploie les caractéristiques physiques de l'infrastructure LAN commutée pour authentifier des périphériques reliés à un port LAN. Access au port peut être refusé si la

procédure d'authentification échoue. Cette norme a été initialement conçue pour des réseaux d'Ethernets câblés, toutefois elle a été adaptée pour l'usage sur des réseaux locaux de radio de 802.11.

Configuration RV320

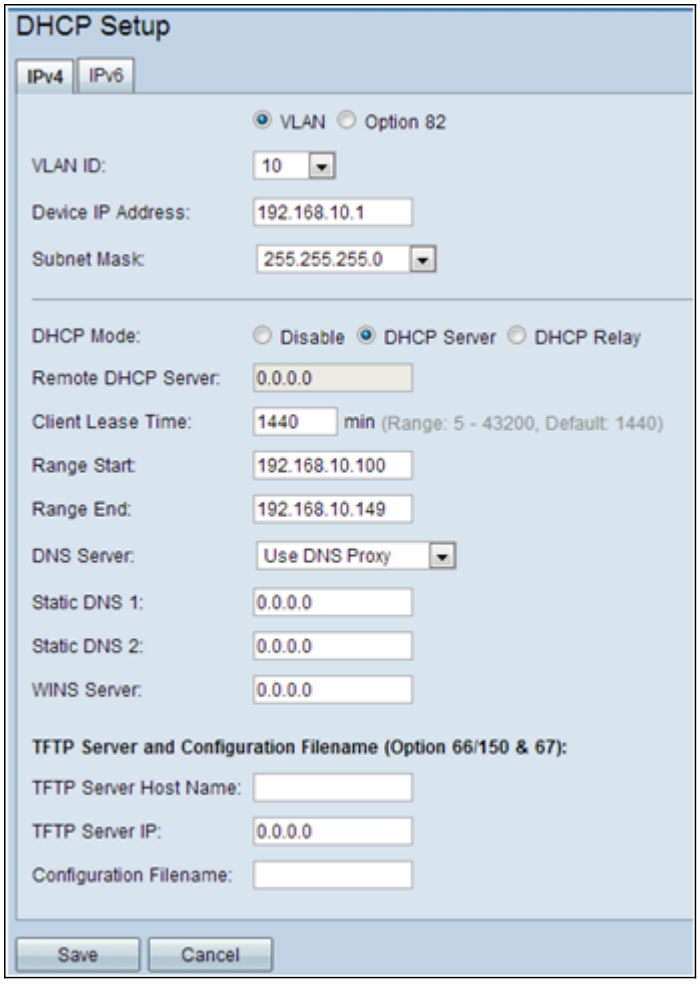
Dans ce scénario nous voulons que le RV320 agisse en tant que serveur DHCP pour le réseau, ainsi nous devrons placer cela haut aussi bien que configurer des VLAN distincts sur le périphérique. Pour commencer, se connecter dans le routeur se connecter à un des ports Ethernet et en allant à 192.168.1.1 (vous assumant n'ont pas déjà changé l'adresse IP du routeur).

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **gestion de ports > l'appartenance à un VLAN**. Une nouvelle page s'ouvre :



Étape 2. Nous créons 3 VLAN distincts pour représenter différents publics cibles. Cliquez sur Add pour ajouter une nouvelle ligne et pour éditer l'ID DE VLAN et la description. Vous devrez également s'assurer que le VLAN est placé à étiqueter sur toutes les interfaces sur lesquelles ils devront voyager.

Étape 3. Ouvrez une session à l'utilitaire de configuration Web et choisissez le **menu DHCP > l'installation DHCP**. La page d'*installation DHCP* s'ouvre :

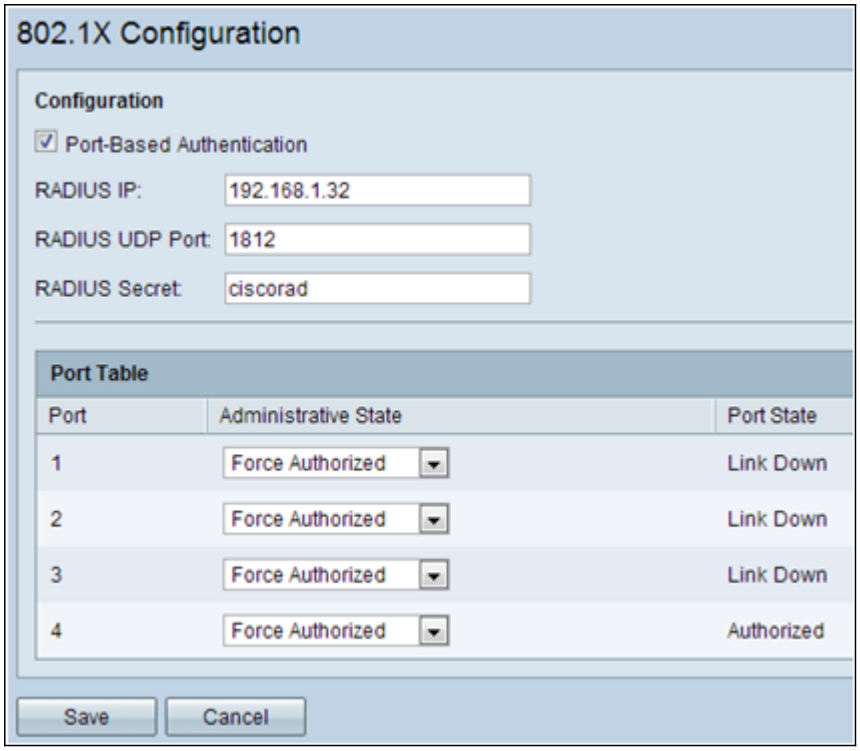


Étape 4. Dans la case de baisse d'ID DE VLAN, sélectionnez le VLAN que vous installez le pool d'adresses pour (dans cet exemple VLAN 10, 20, et 30).

Étape 5. Configurez l'adresse IP de périphérique pour ce VLAN, et placez la plage d'adresses IP. Vous pouvez également activer ou désactiver le proxy de DN ici si vous souhaitez, et ce dépendra du réseau. Dans cet exemple, le proxy de DN fonctionnera pour expédier des demandes de DN.

Étape 6. Cliquez sur la sauvegarde et répétez cette étape pour chaque VLAN.

Étape 7. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **configuration de gestion de ports > de 802.1x**. La page de *configuration de 802.1X* s'ouvre :



Étape 8. Activez l'authentification basée sur port et configurez l'adresse IP du serveur.

Le secret de RADIUS est la clé d'authentification utilisée pour communiquer avec le serveur.

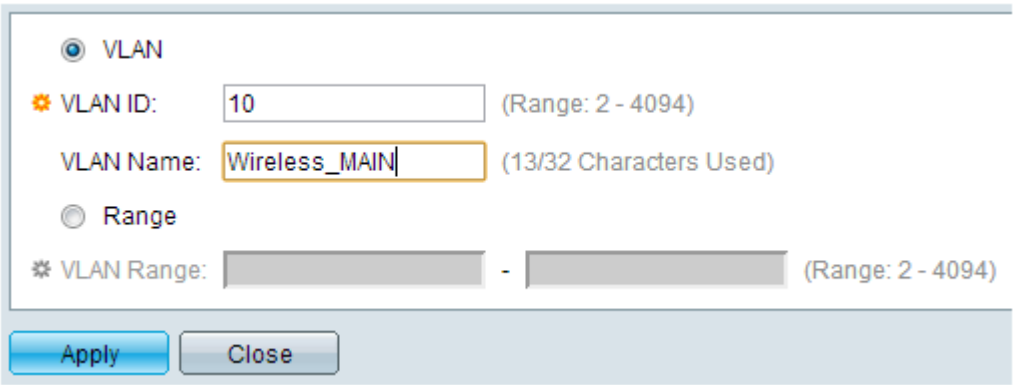
Étape 9. Choisissez quels ports utiliseront cette authentification et cliqueront sur la **sauvegarde**.

Configuration Sx300

Le commutateur SG300-10MP fonctionne comme intermédiaire entre le routeur et le WAP321 afin de simuler un environnement de réseau réaliste. La configuration sur le commutateur est comme suit.

Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **Gestion VLAN > créent le VLAN**. Une nouvelle page s'ouvre :

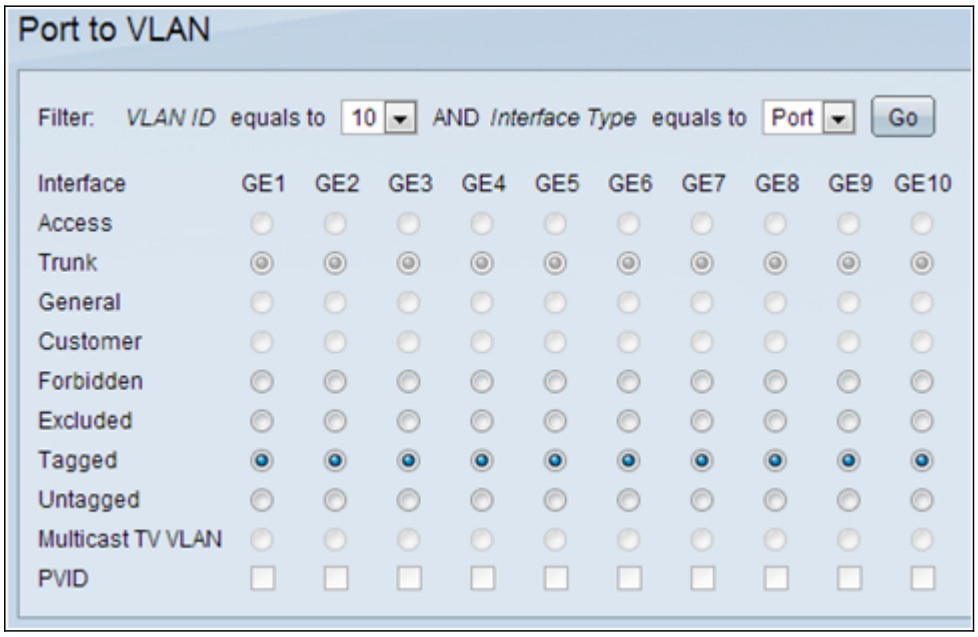
Étape 2. Cliquez sur Add. Une nouvelle fenêtre apparaît.



Étape 3. Écrivez l'ID DE VLAN et le nom VLAN (utilisez les mêmes que la description de la section I). Cliquez sur Apply, et puis répétez cette étape pour VLAN 20 et 30.

Étape 4. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **Gestion**

VLAN > le port au VLAN. Une nouvelle page s'ouvre :



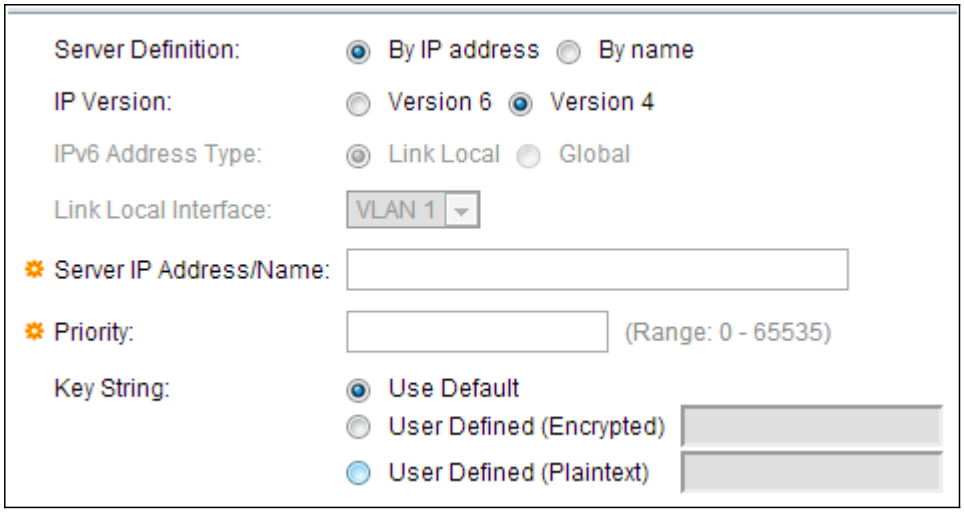
Étape 5. En haut de la page réglée les « égaux d'ID DE VLAN à » au VLAN vous ajoutez (dans ce cas, VLAN 10) et cliquent sur Go alors du côté droit. Ceci mettra à jour la page avec les configurations pour ce VLAN.

Étape 6. Changez la configuration sur chaque port de sorte que le VLAN 10 « soit maintenant étiqueté » au lieu de « exclu. » Répétez cette étape pour VLAN 20 et 30.

Étape 7. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **Sécurité > le Radius**. La page de *RADIUS* s'ouvre :

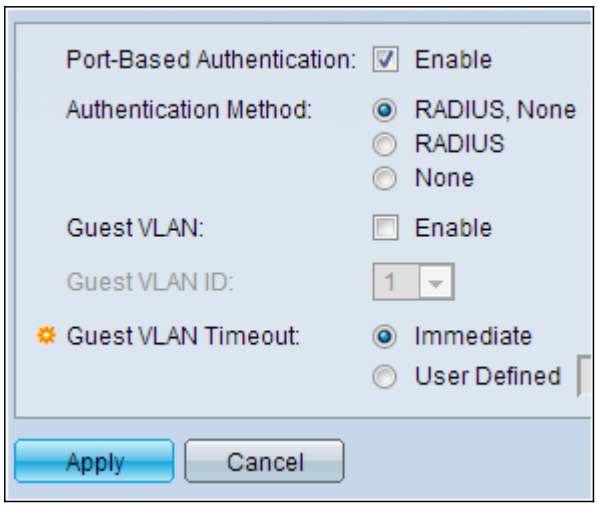
Étape 8. Choisissez la méthode de contrôle d'accès à utiliser par le serveur de RADIUS, contrôle d'accès de Gestion ou authentification basée sur port. Choisissez le contrôle d'accès basé par port et cliquez sur Apply.

Étape 9. Cliquez sur Add au bas de page pour ajouter un nouveau serveur pour authentifier à.



Étape 10. Dans la fenêtre qui apparaît vous configurerez l'adresse IP du serveur, dans ce cas 192.168.1.32. Vous devrez fixer une priorité pour le serveur, mais puisque dans cet exemple nous avons seulement un serveur pour authentifier à la priorité n'importe pas. C'est important si vous avez de plusieurs serveurs de RADIUS à choisir de. Configurez la clé d'authentification et le reste des configurations peut être laissé en tant que par défaut.

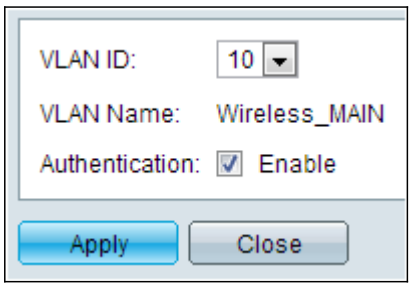
Étape 11. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **Sécurité > le 802.1X > le Properties**. Une nouvelle page s'ouvre :



Étape 12. Vérifiez l'**enable** pour activer l'authentification de 802.1x et pour choisir la méthode d'authentification. Dans ce cas nous utilisons un serveur de RADIUS ainsi choisissez la première ou deuxième option.

Étape 13. Cliquez sur **Apply**.

Étape 14. Choisissez un des VLAN et cliquez sur Edit. Une nouvelle fenêtre apparaît.



Étape 15. vérifiez l'**enable** pour permettre l'authentification sur ce VLAN et pour cliquer sur

Apply. Répétition pour chaque VLAN.

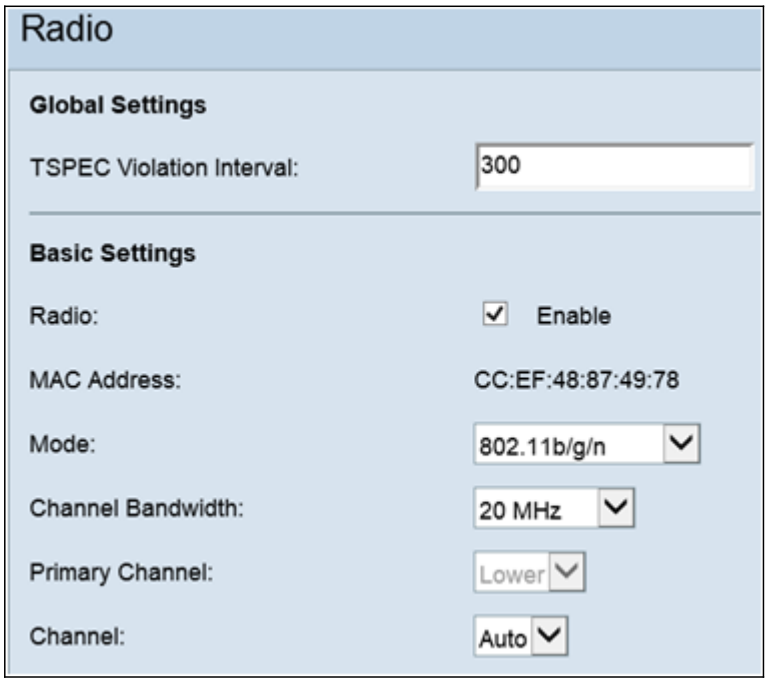
Configuration WAP321

Les Points d'accès virtuels (VAPs) segmentent le RÉSEAU LOCAL Sans fil dans les plusieurs domaines d'émission qui sont l'équivalent de radio des VLAN Ethernet. VAPs simulent des plusieurs points d'accès dans un périphérique physique WAP. Jusqu'à quatre VAPs sont pris en charge sur le WAP121 et jusqu'à huit VAPs sont pris en charge sur le WAP321.

Chaque VAP peut être indépendamment activé ou désactivé, excepté VAP0. VAP0 est l'interface par radio physique et les restes ont activé tant que la radio est activée. Pour désactiver l'exécution de VAP0, la radio elle-même doit être désactivée.

Chaque VAP est identifié par un Identifiant SSID (Service Set Identifier) utilisateur-configuré. Plusieurs VAPs ne peut pas avoir le même nom SSID. Des diffusions SSID peuvent être activées ou désactivées indépendamment sur chaque VAP. La diffusion SSID est activée par défaut.

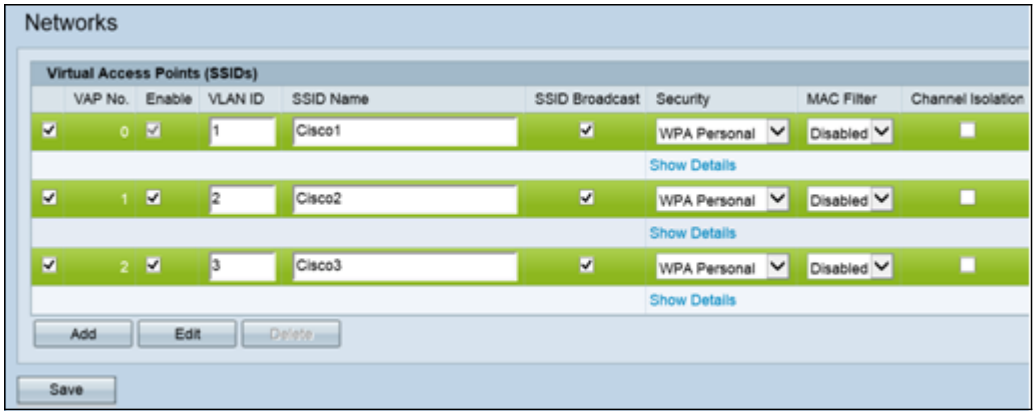
Étape 1. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **radio > la radio**. La page *par radio* s'ouvre :



Étape 2. Cliquez sur la case d'**enable** pour activer la radio Sans fil.

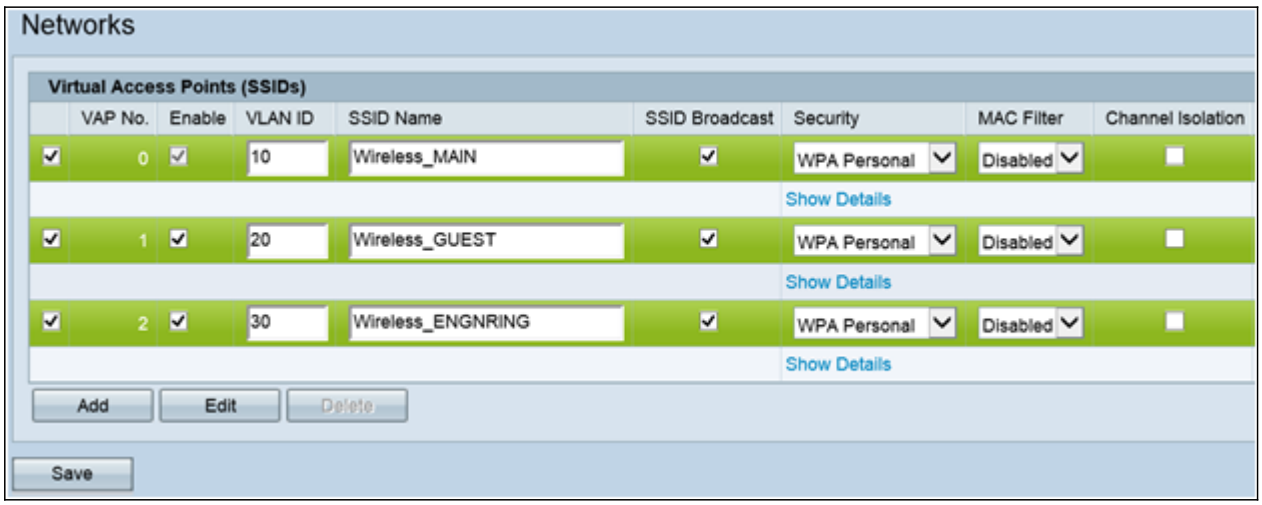
Étape 3. **Sauvegarde de** clic. La radio sera alors activée.

Étape 4. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **radio > les réseaux**. La page de *réseau* s'ouvre :



Note: Le SSID par défaut pour VAP0 est ciscosb. Chaque VAP supplémentaire créé a un nom du blanc SSID. Le SSID pour tout le VAPs peut être configuré à d'autres valeurs.

Étape 5. Cliquez sur les boutons de coche du côté gauche pour éditer le SSID :



Note: Tous les SSID peuvent être édités immédiatement en vérifiant le champ vers le gauche.

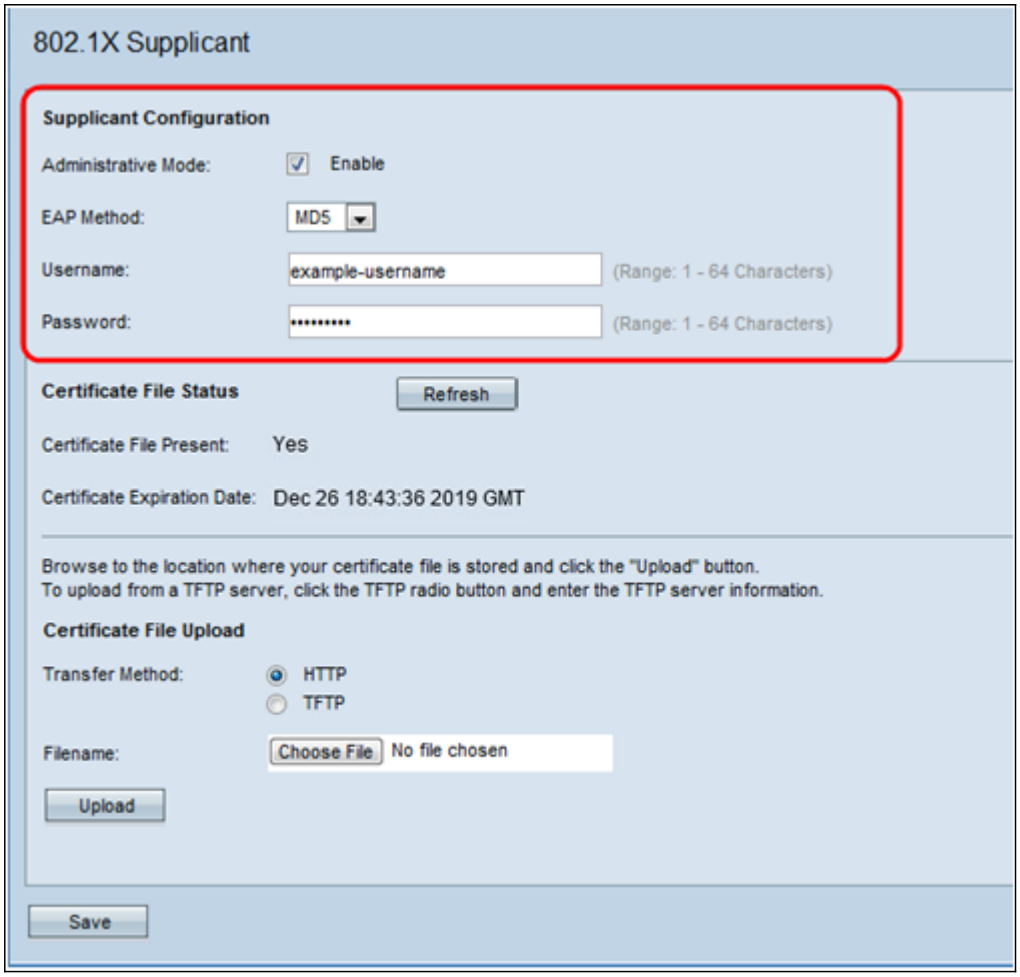
Étape 6. Cliquez sur le bouton de sauvegarde une fois que le SSID ont été écrits.

Chaque VAP est associé avec un VLAN, qui est identifié par un ID DE VLAN (VID). Un VID peut être n'importe quelle valeur de 1 à 4094, inclus. Le WAP121 prend en charge cinq VLAN actifs (quatre pour le WLAN plus un VLAN de gestion). Le WAP321 prend en charge neuf VLAN actifs (huit pour le WLAN plus un VLAN de gestion).

Par défaut, le VID assigné à l'utilitaire de configuration pour le périphérique WAP est 1, qui est également le VID non-marqué par défaut. Si la Gestion VID est identique que le VID assigné à un VAP, alors les clients WLAN associés avec cette particularité VAP peuvent gérer le périphérique WAP. Si nécessaire, une liste de contrôle d'accès (ACL) peut être créée pour désactiver la gestion des clients WLAN.

Étape 7. Écrivez la valeur requise l'ID DE VLAN dans la case d'ID DE VLAN, et cliquez sur le bouton de sauvegarde une fois que les IDs de VLAN ont été écrits.

Étape 8. Ouvrez une session à l'utilitaire de configuration Web et choisissez le **suppliant de sécurité des systèmes > de 802.1X**. La page de *suppliant de 802.1X* s'ouvre :



Étape 9. **Enable de** contrôle dans le domaine d'Administrative Mode pour permettre au périphérique d'agir en tant que suppliant dans l'authentification de 802.1X.

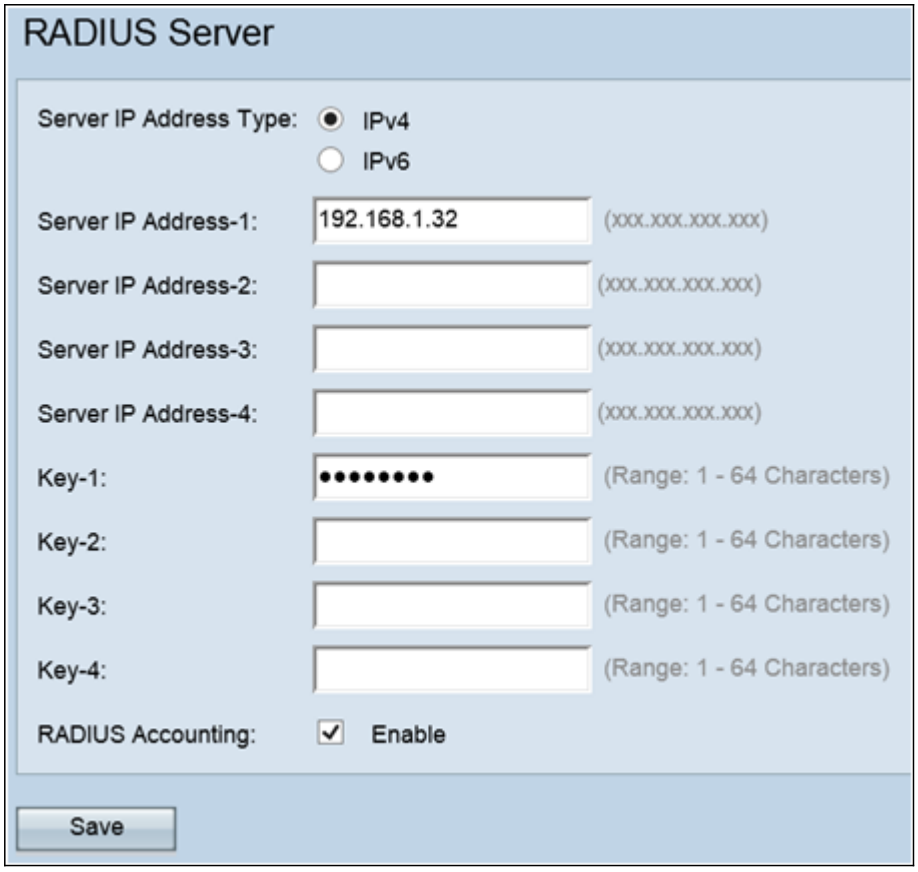
Étape 10. Choisissez le type approprié de méthode de Protocole EAP (Extensible Authentication Protocol) de la liste déroulante dans le domaine de méthode d'EAP.

Étape 11. Écrivez le nom d'utilisateur et mot de passe que le Point d'accès l'utilise pour obtenir l'authentification de l'authentificateur de 802.1X dans les domaines de nom d'utilisateur et mot de passe. La longueur du nom d'utilisateur et mot de passe doit être de 1 à 64 caractères alphanumériques et de symbole. Ceci devrait déjà être configuré sur le serveur d'authentification.

Étape 12. **Sauvegarde de** clic pour sauvegarder les configurations.

Note: La région d'état de fichier du certificat affiche si le fichier du certificat est présent ou pas. Le certificat ssl est un certificat digitalement signé par une autorité de certification qui permet au navigateur Web pour avoir une communication protégée avec le web server. Pour gérer et configurer le certificat ssl référez-vous à la *Gestion de certificat de Protocole SSL (Secure Socket Layer) d'*article *sur les Points d'accès WAP121 et WAP321 de Cisco*.

Étape 13. Ouvrez une session à l'utilitaire de configuration Web et choisissez la **Sécurité > le serveur de RADIUS**. La page de *serveur de RADIUS* s'ouvre :



Étape 14. Entrez les paramètres, et cliquez sur le bouton de sauvegarde une fois que les paramètres de serveur de Radius ont été entrés.