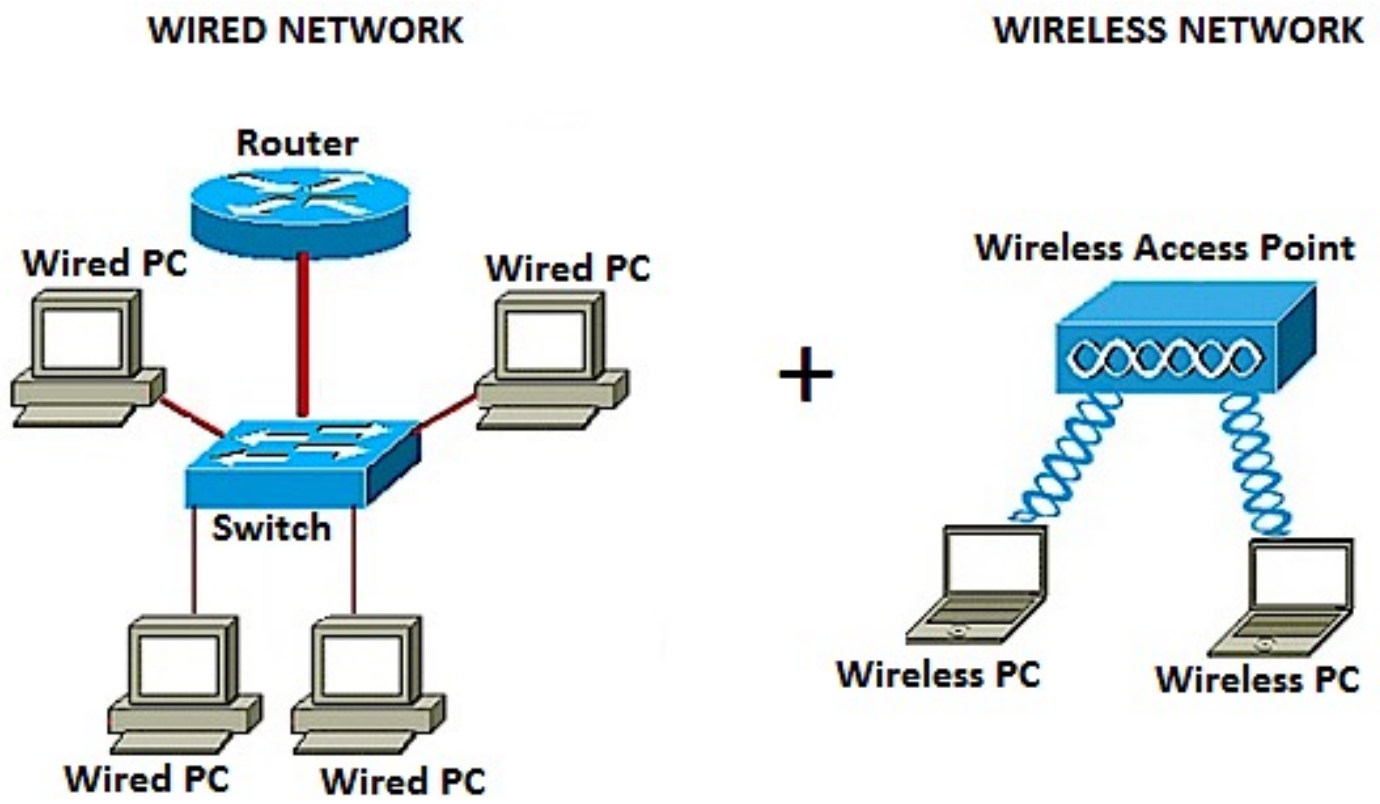
Ajouter un réseau sans fil à un réseau câblé existant à l'aide d'un point d'accès sans fil (WAP)

Objectif

R. Un point d’accès sans il (WAP) désigne un dispositif de réseautage qui permet à d’autres appareils Wi-Fi de se connecter à un réseau câblé. L’ajout d’un WAP à votre réseau filaire existant est utile pour prendre en charge les périphériques qui sont uniquement capables d’établir une connexion sans fil. Cela revient à créer un autre réseau uniquement pour les périphériques sans fil, mais à faire partie de votre réseau câblé existant, comme illustré dans le schéma ci-dessous.



Dans le schéma de réseau ci-dessus, la partie gauche présente un réseau câblé existant. Il se compose de quatre ordinateurs câblés connectés à un commutateur, qui est connecté à un routeur. Dans la partie droite, un réseau sans fil montre deux ordinateurs sans fil connectés à un WAP.

L’objectif de cet article est de vous montrer comment ajouter un réseau sans fil à votre réseau filaire existant à l’aide d’un point d’accès sans fil.

Périphériques pertinents

- Gamme WAP100
- Gamme WAP300
- Gamme WAP500

Version du logiciel

- 1.0.6.5 - WAP121, WAP321
- 1.0.2.8 : WAP131, WAP351
- 1.0.1.7 : WAP150, WAP361
- 1.3.0.3 : WAP371
- 1.2.1.3 : WAP551, WAP561
- 1.0.0.17 - WAP571, WAP571E

Ajouter un réseau sans fil à un réseau câblé existant

Configuration du réseau sans fil

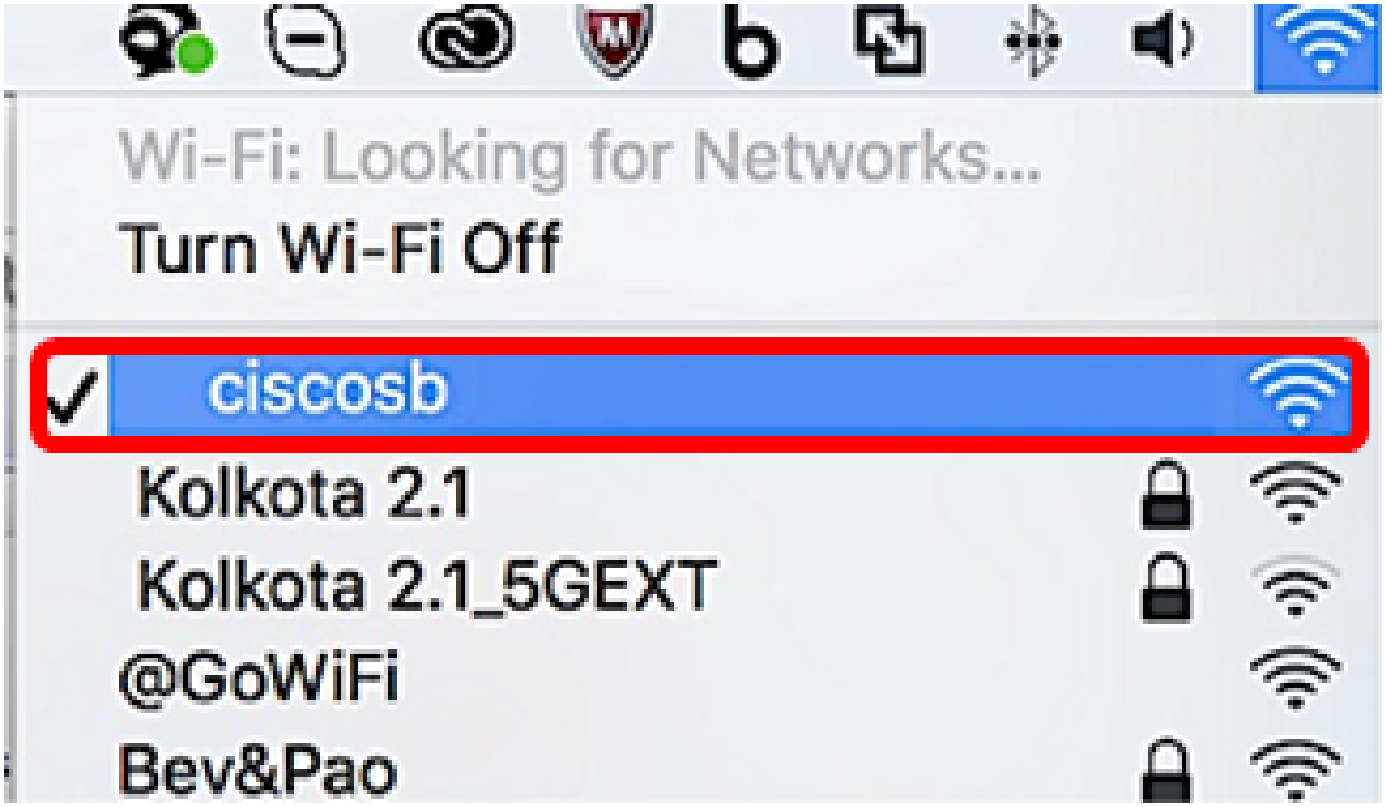
Remarque : les images peuvent varier en fonction du modèle exact de votre WAP. Les images utilisées dans cet article proviennent du WAP361.

Étape 1. Connectez le WAP à votre routeur ou à votre commutateur à l'aide du câble Ethernet fourni.

Remarque : si votre WAP ne dispose pas de la fonctionnalité Power over Ethernet (PoE), connectez l'adaptateur secteur au WAP et branchez-le sur la prise de courant.

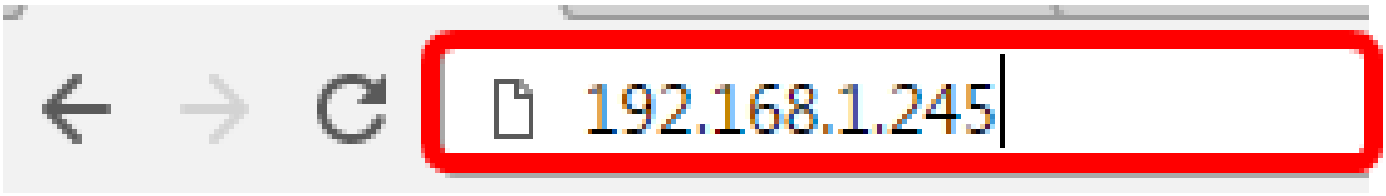
Étape 2. Connectez votre ordinateur sans fil au réseau sans fil que le WAP diffuse.

Remarque : l'identifiant SSID (Service Set Identifier) ou le nom de réseau sans fil par défaut du point d'accès Cisco est ciscosb.



Étape 3. Sur l'ordinateur sans fil, accédez à l'utilitaire Web du WAP en lançant un navigateur Web et en saisissant l'adresse IP du WAP dans la barre d'adresse.

Remarque : si vous ne connaissez pas l'adresse IP de votre WAP, vous pouvez utiliser l'outil de découverte Cisco FindIT ou l'outil de gestion de réseau Cisco FindIT si ces applications sont installées sur votre réseau. Ces applications vous aideront à vérifier les adresses IP et d'autres informations du point d'accès et d'autres périphériques Cisco de votre réseau. Pour en savoir plus, cliquez ici.

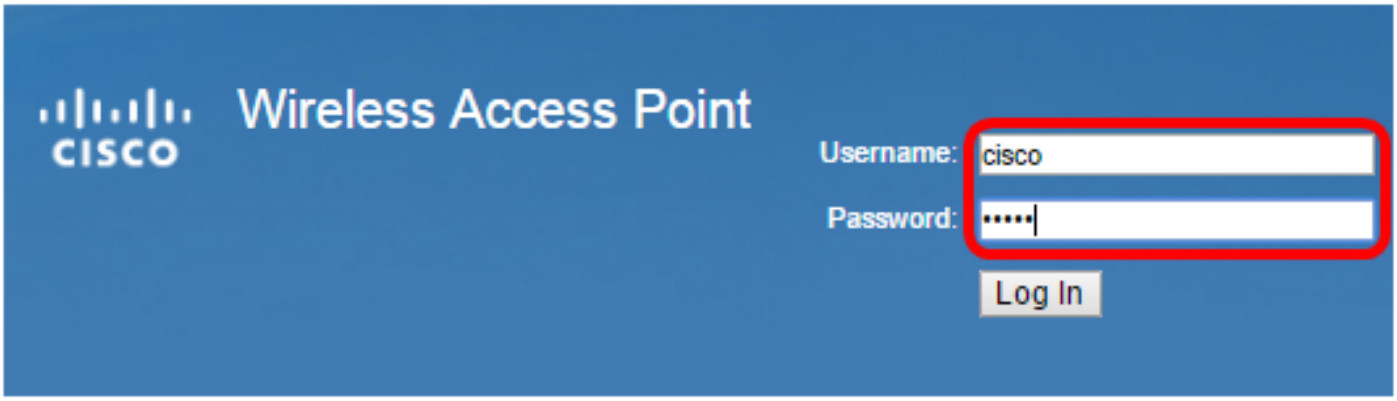


Remarque : dans l'image ci-dessus, 192.168.1.245 est utilisé comme exemple d'adresse IP. Il s'agit de l'adresse IP par défaut des points d'accès Cisco.

Étape 4. Dans la fenêtre d'authentification, entrez le nom d'utilisateur et le mot de passe du WAP dans les champs Username et Password, respectivement.

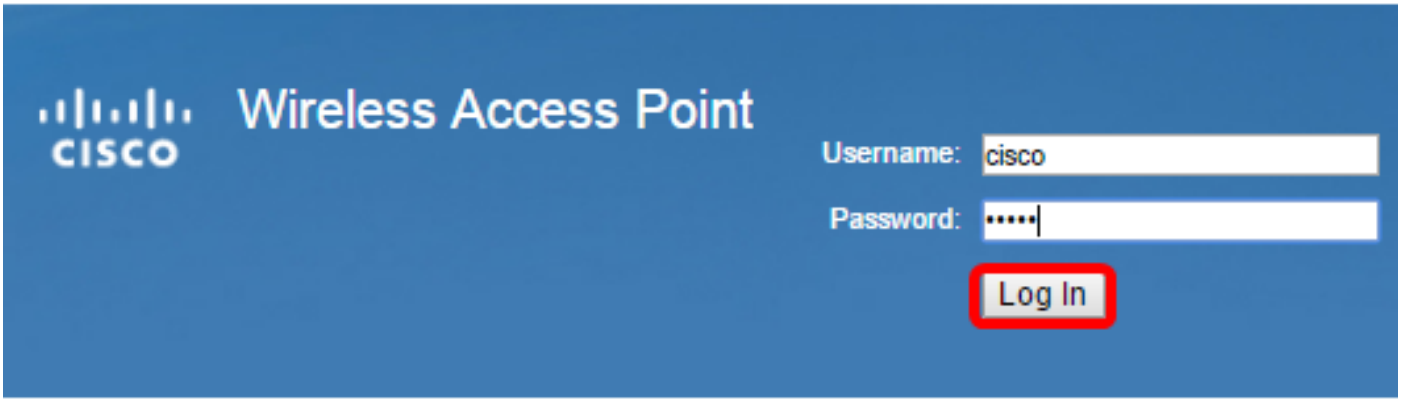
Remarque : vous pouvez configurer jusqu'à cinq utilisateurs pour chaque point d'accès que vous allez ajouter au réseau. Ces utilisateurs sont autorisés à accéder à l'utilitaire Web via leurs clés

d'authentification, mais un seul de ces utilisateurs peut disposer du niveau de privilège Lecture/Écriture. Vous pouvez également créer un nom d'utilisateur et un mot de passe différents pour chaque utilisateur. Pour en savoir plus, cliquez ici.

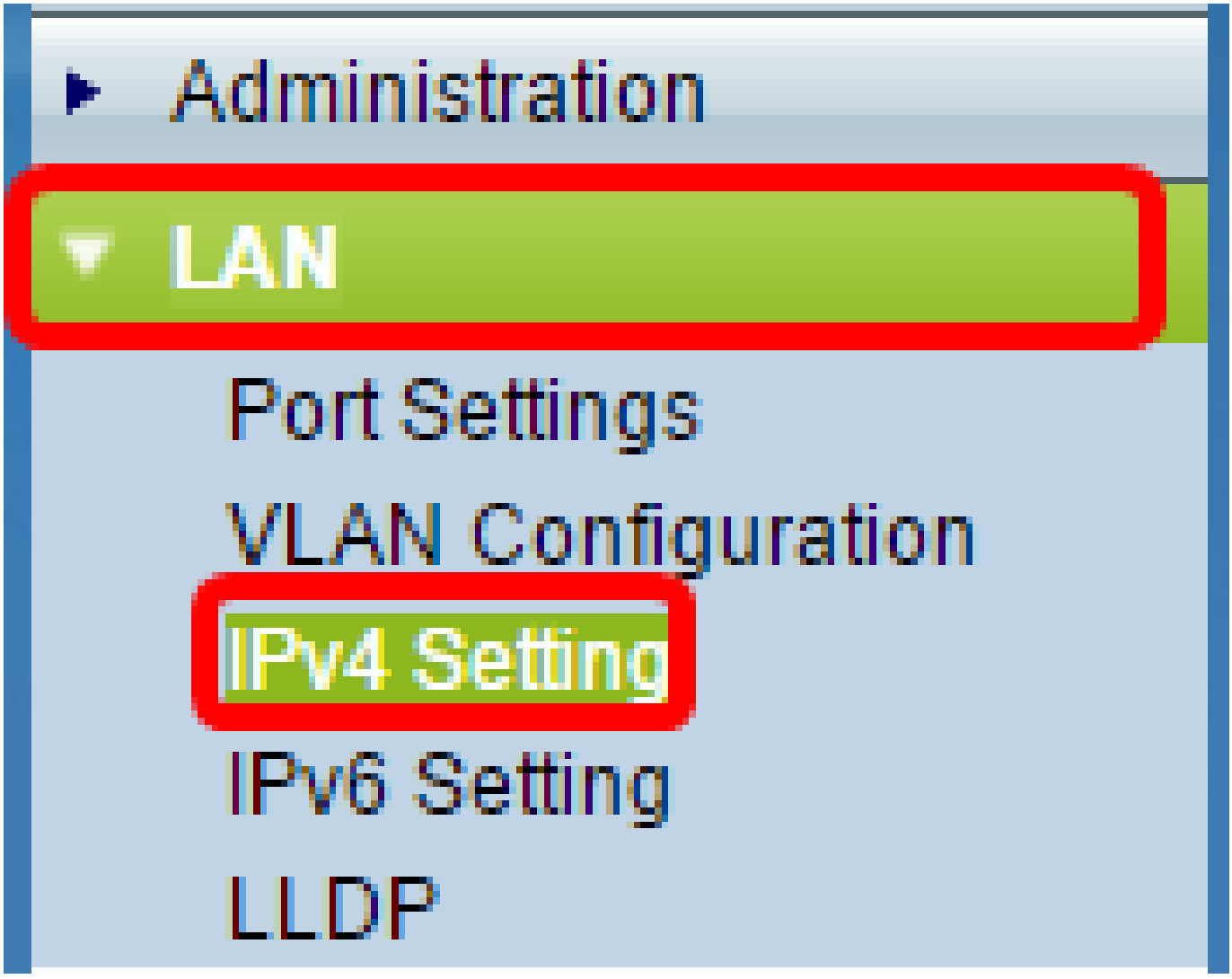


Remarque : le nom d'utilisateur et le mot de passe par défaut de l'utilisateur par défaut des points d'accès Cisco sont cisco/cisco.

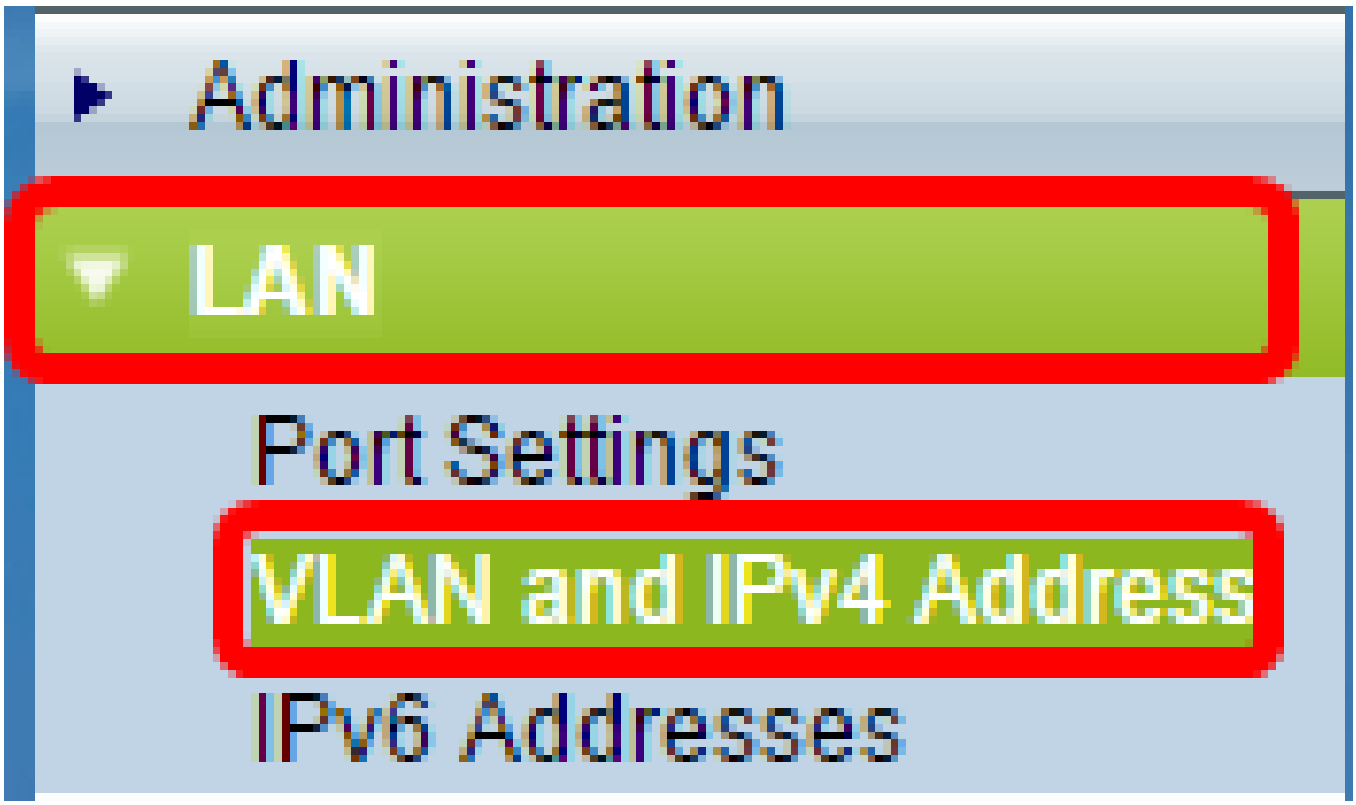
Étape 5. Cliquez sur Log In.



Étape 6. Dans la zone de navigation, choisissez LAN > IPv4 Setting.



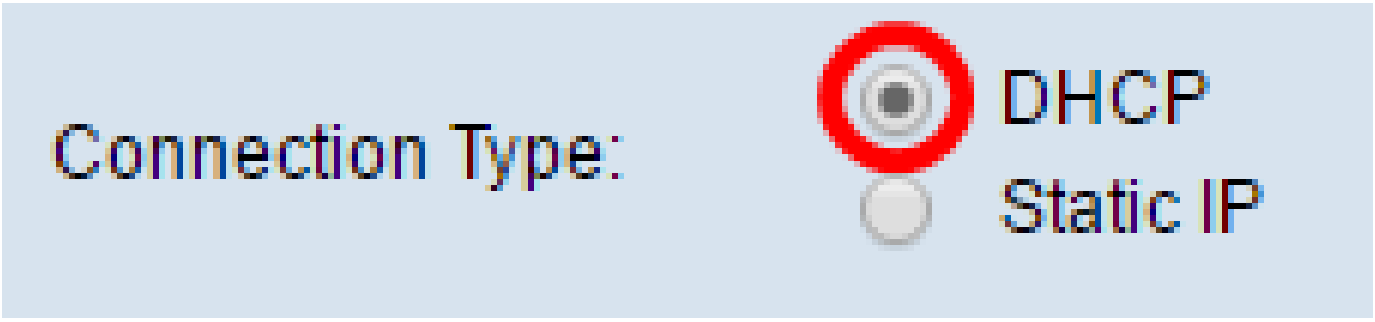
Remarque : si vous utilisez le WAP121, le WAP321, le WAP371, le WAP551 ou le WAP561, choisissez LAN > VLAN and IPv4 Address.



Remarque : si vous souhaitez utiliser l'adressage IPv6 à la place, cliquez ici pour obtenir des instructions.

Étape 7. Sélectionnez une case d'option pour choisir le type de connexion.

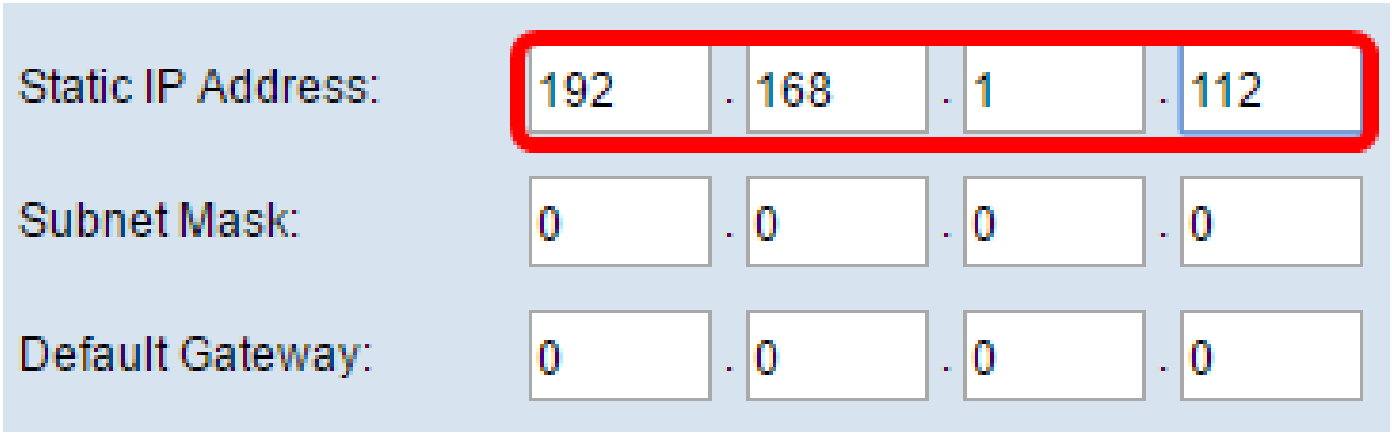
- DHCP : le point d'accès obtient son adresse IP d'un serveur DHCP (Dynamic Host Configuration Protocol) sur le réseau.
- Static IP : vous serez le seul à attribuer manuellement l'adresse IPv4 au WAP.



Remarque : dans cet exemple, DHCP est sélectionné. Voici la configuration par défaut . Si vous avez effectué cette étape, passez à l'étape 12.

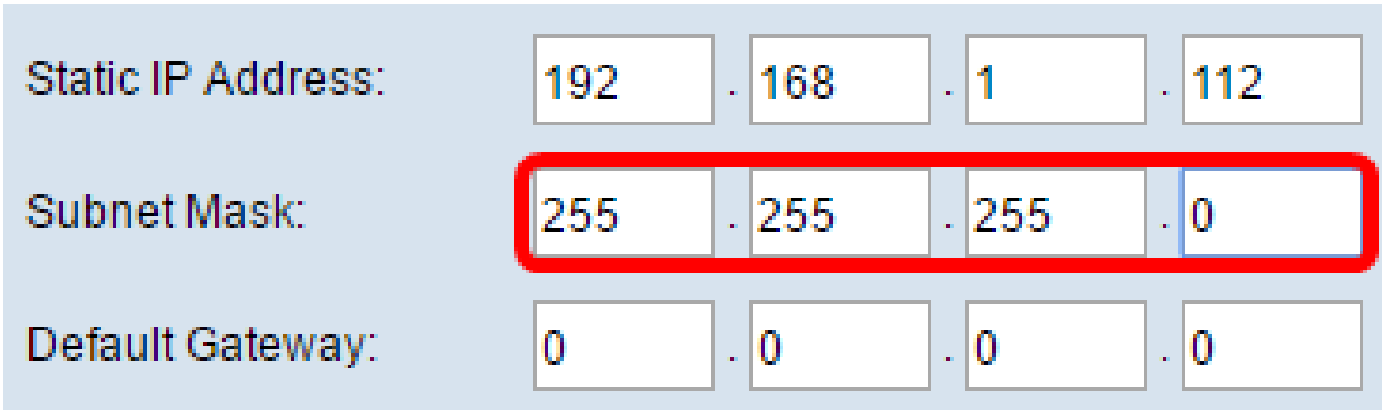
Étape 8. (Facultatif) Si vous avez choisi Static IP à l'étape précédente, saisissez l'adresse IP statique que vous souhaitez attribuer au WAP dans le champ Static IP Address. Assurez-vous que

l'adresse IP que vous attribuez se trouve dans la même plage que votre réseau.



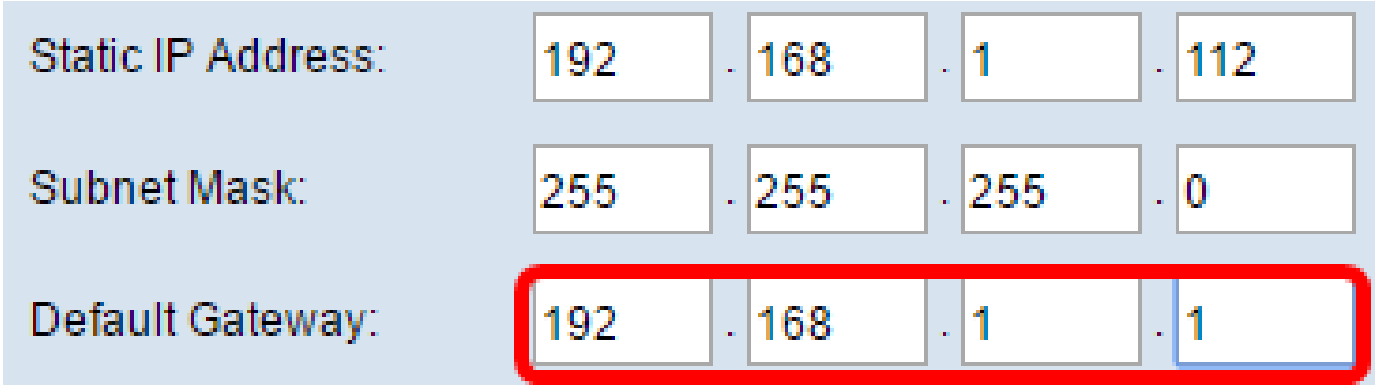
Remarque : dans cet exemple, l'adresse IP utilisée est 192.168.1.112.

Étape 9. (Facultatif) Entrez le masque de sous-réseau dans le champ Subnet Mask.



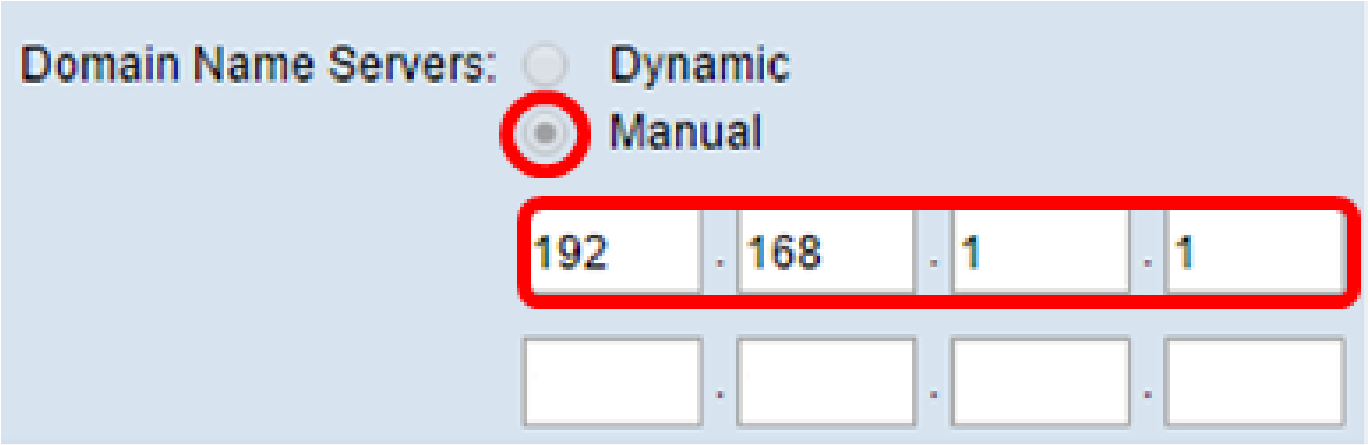
Remarque : dans cet exemple, 255.255.255.0 est utilisé.

Étape 10. Saisissez l'adresse IP du routeur dans le champ Default Gateway.



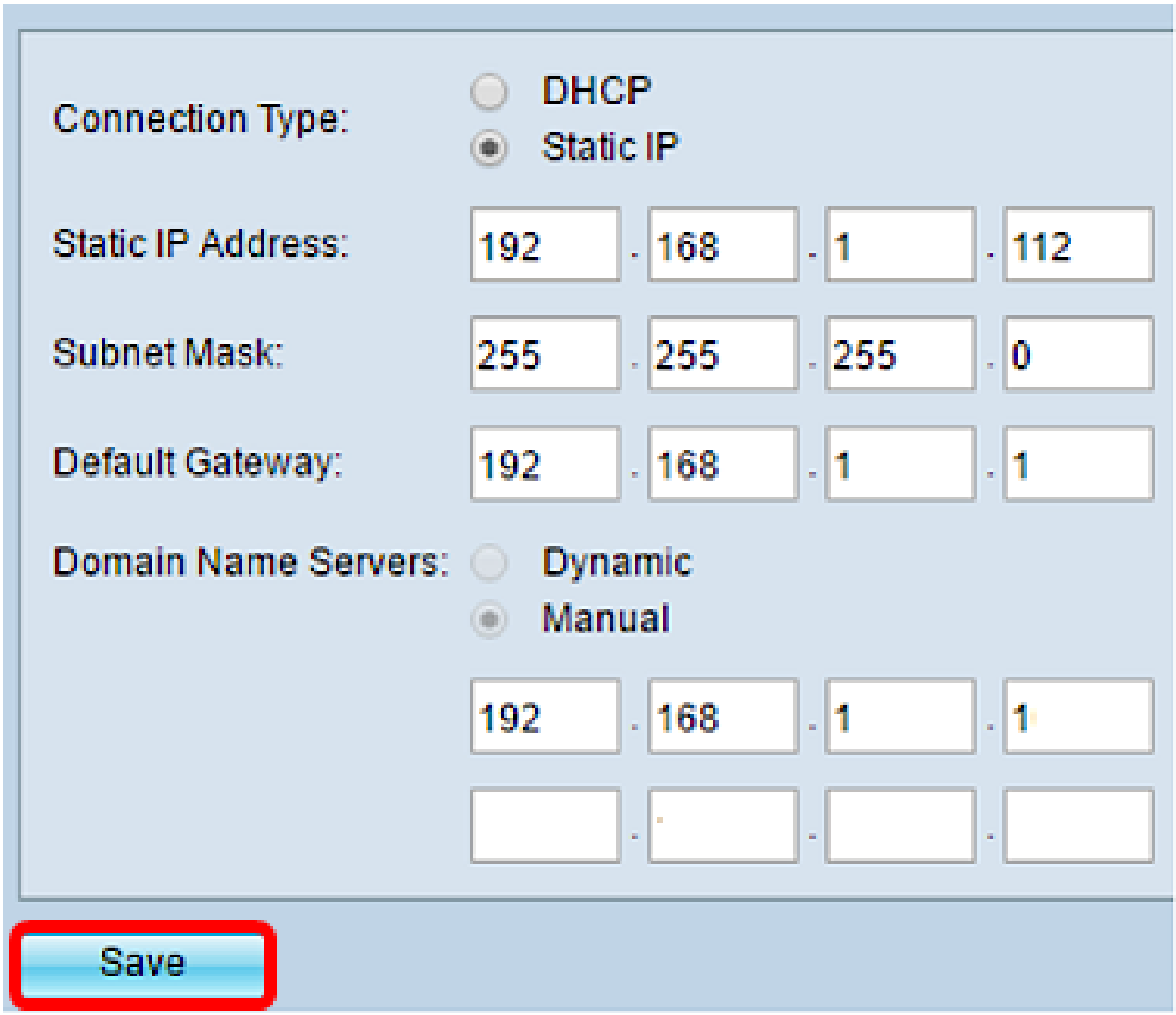
Remarque : dans cet exemple, 192.168.1.1 est utilisé comme passerelle par défaut.

Étape 11. Dans la zone DNS (Domain Name Servers), la case d'option Manual (Manuel) est automatiquement sélectionnée lorsque le type de connexion est défini sur Static IP (IP statique). Vous pouvez saisir jusqu'à deux adresses DNS dans les champs prévus à cet effet.



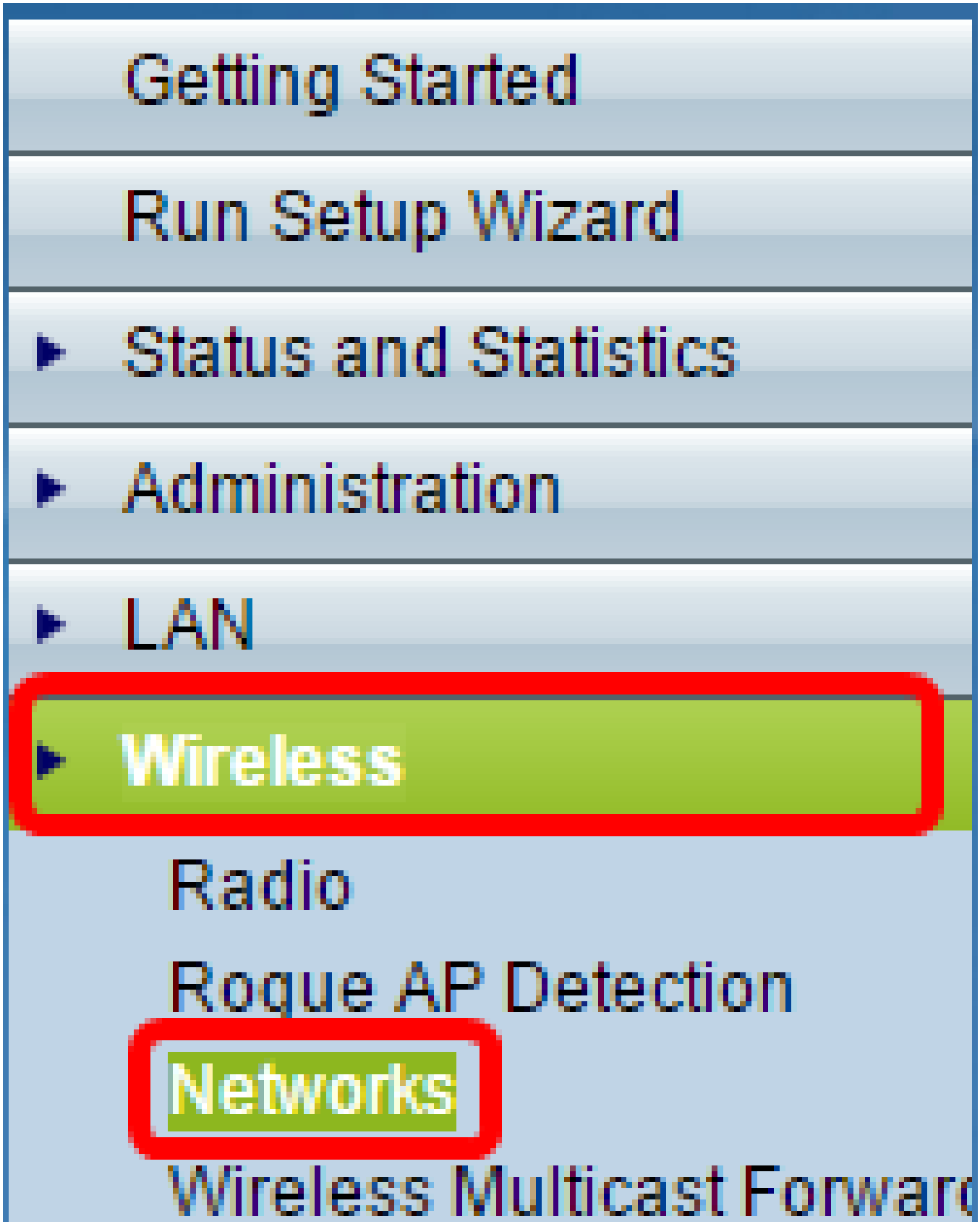
Remarque : dans cet exemple, 192.168.1.1 est utilisé.

Étape 12. Cliquez sur Save.



Configuration des paramètres sans fil

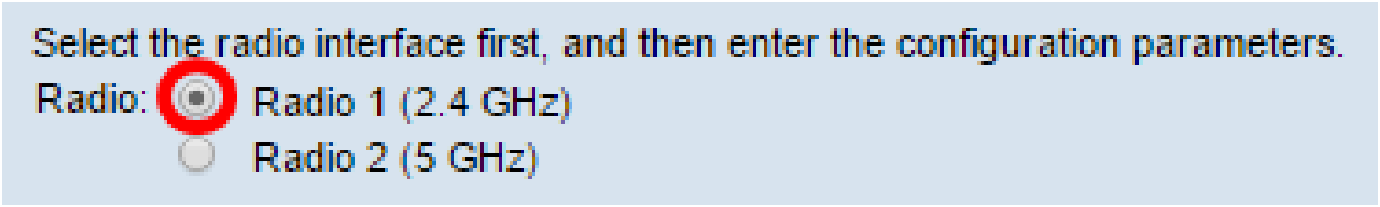
Étape 1. Choisissez Wireless > Networks.



Étape 2. (Facultatif) Si vous utilisez un point d'accès bibande, cliquez sur une case d'option pour choisir l'interface radio que vous souhaitez configurer.

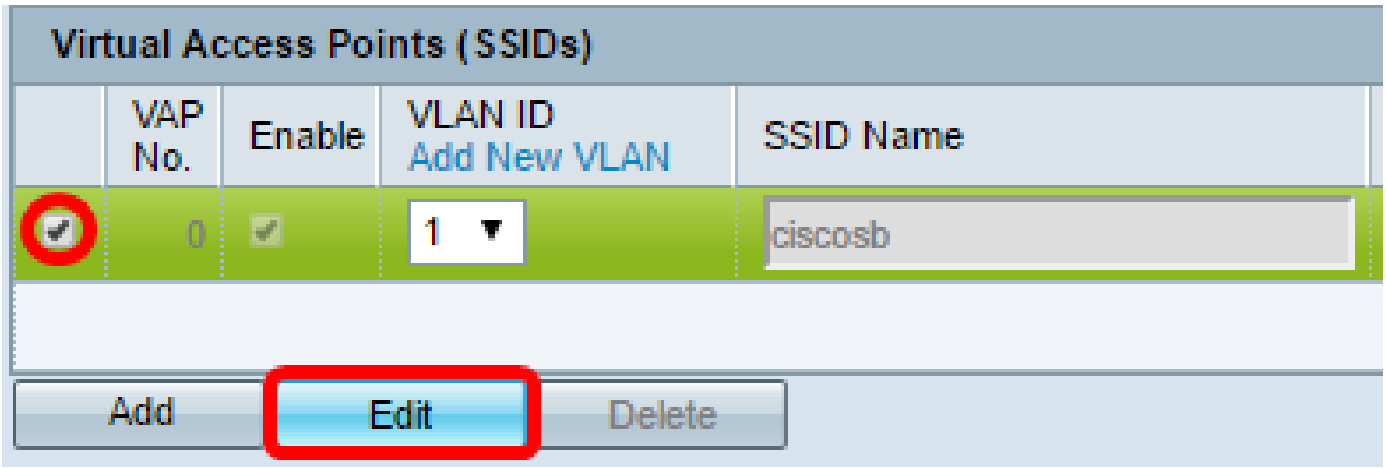
- Radio 1 (2,4 GHz) : pour les clients sans fil fonctionnant sur la fréquence 2,4 GHz.

- Radio 2 (5 GHz) : pour les clients sans fil fonctionnant sur la fréquence 5 GHz.



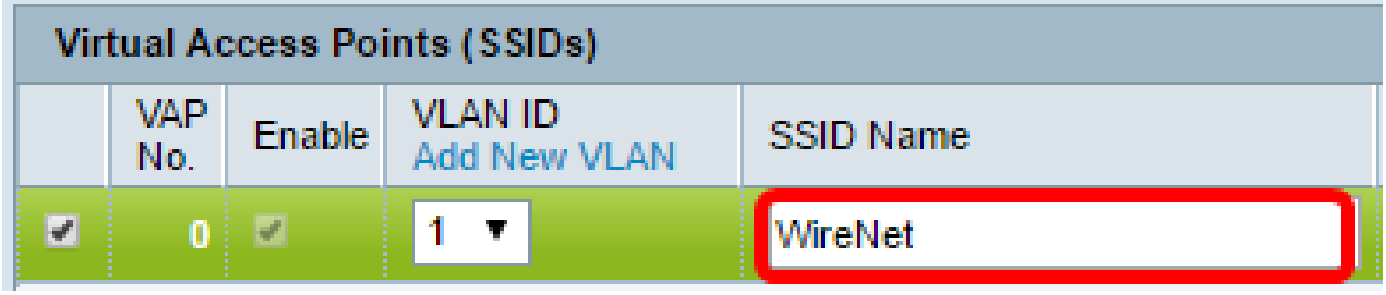
Remarque : dans cet exemple, Radio 1 (2,4 GHz) est sélectionné.

Étape 3. Dans la zone Virtual Access Points (SSID), cochez la case en regard du point d'accès virtuel (VAP) par défaut et cliquez sur le bouton Edit en dessous.



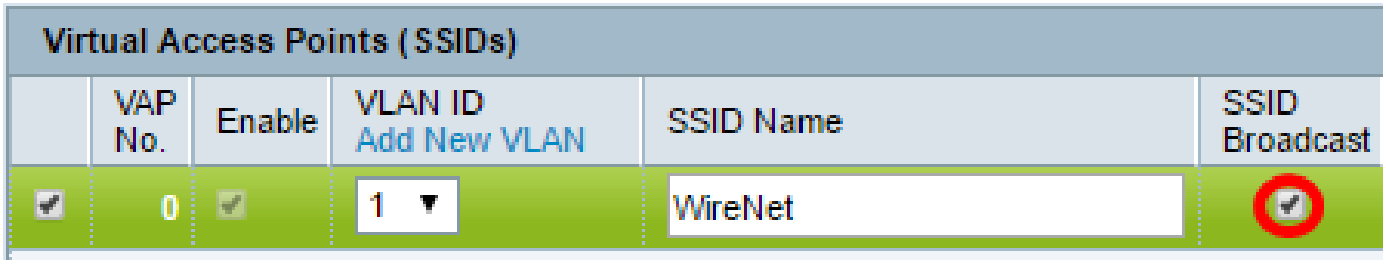
Remarque : vous pouvez ajouter ou créer plusieurs VAP sur votre WAP en fonction du modèle exact de votre périphérique en cliquant sur le bouton Ajouter. Pour le WAP361, sept VAP supplémentaires peuvent être créés.

Étape 4. Sous SSID Name, créez un nouveau nom pour votre réseau sans fil dans le champ prévu à cet effet.



Remarque : dans cet exemple, WireNet est utilisé.

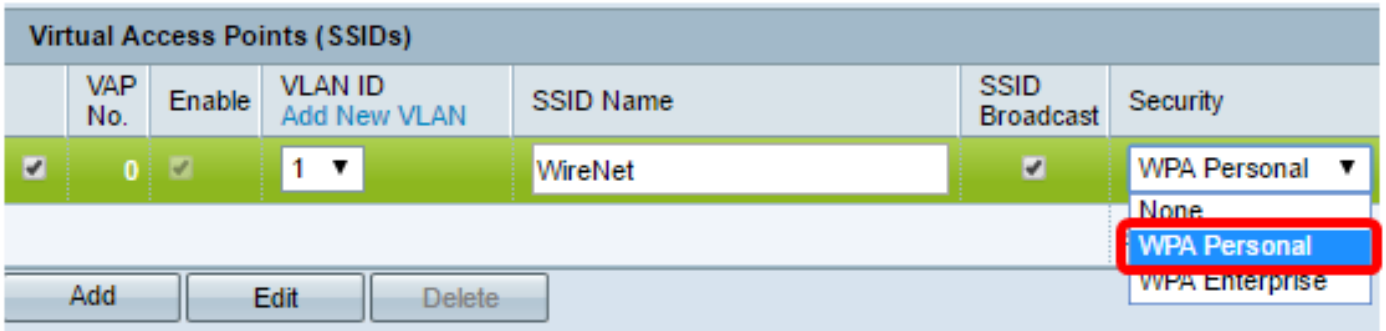
Étape 5. (Facultatif) Sous SSID Broadcast, cochez ou décochez la case en fonction de vos préférences. Cochez cette case pour permettre à votre réseau sans fil de diffuser son SSID ou d'être visible par tous les périphériques sans fil à sa portée. Décochez cette case pour la masquer sur tous les périphériques sans fil.



Remarque : dans cet exemple, la diffusion SSID est vérifiée.

Étape 6. Sous Security (Sécurité), cliquez sur le menu déroulant pour choisir le type de sécurité que vous souhaitez configurer sur le réseau sans fil. Les options sont les suivantes :

- None (Aucun) : cette option définit la sécurité sur l'ouverture et permet à tous les périphériques sans fil de se connecter à votre réseau sans fil sans qu'un mot de passe ou une authentification vous soit demandé.
- WPA Personal (WPA personnel) : le protocole WPA (Wi-Fi Protected Access) est un protocole de sécurité conçu pour améliorer les fonctions de sécurité du protocole WEP (Wired Equivalent Privacy). WPA utilise des clés 256 bits plus élevées et améliore le cryptage des données et l'authentification des utilisateurs. Ce mode de sécurité vous permet d'utiliser soit l'algorithme TKIP (Temporal Key Integrity Protocol), soit l'algorithme AES (Advanced Encryption Security) le plus récent, de niveau supérieur, si le périphérique est plus récent et le prend en charge avec WPA. Toutefois, les deux options mettent en oeuvre des normes de sécurité plus strictes.
- WPA Enterprise : en mode Enterprise, le mode WPA (Wi-Fi Protected Access) est utilisé avec l'authentification RADIUS (Remote Authentication Dial-In User Service) du serveur.

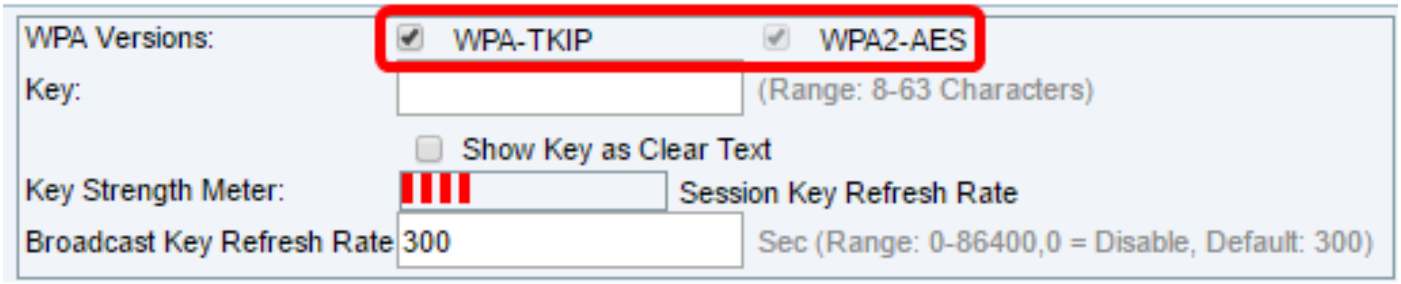


Remarque : dans cet exemple, WPA Personal (WPA personnel) est sélectionné. La fenêtre Détails de sécurité s'affiche alors.

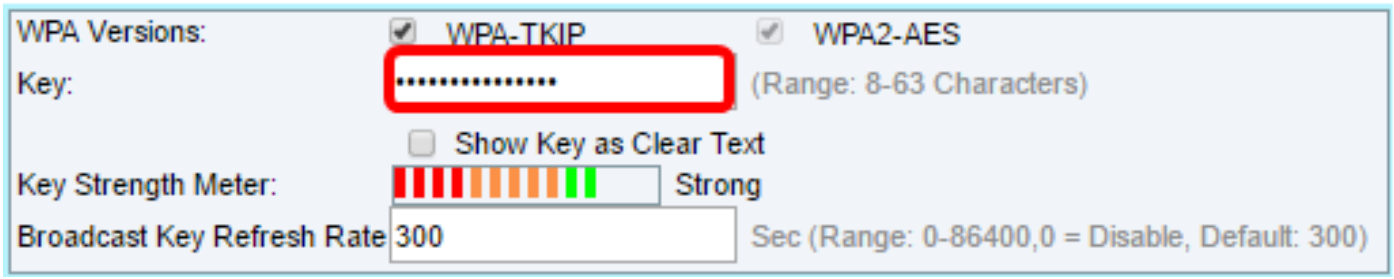
Étape 7. Sélectionnez les types de stations client que vous souhaitez prendre en charge en cochant les cases de la zone Versions WPA.

- WPA-TKIP : cette option permet aux clients sans fil qui prennent uniquement en charge les protocoles de sécurité WPA et TKIP d'origine de se connecter au réseau.
- WPA2-AES : cette version WPA offre la meilleure sécurité selon la norme IEEE 802.11i. Conformément à la dernière exigence de la Wi-Fi Alliance, le WAP doit prendre en charge ce mode tout le temps.

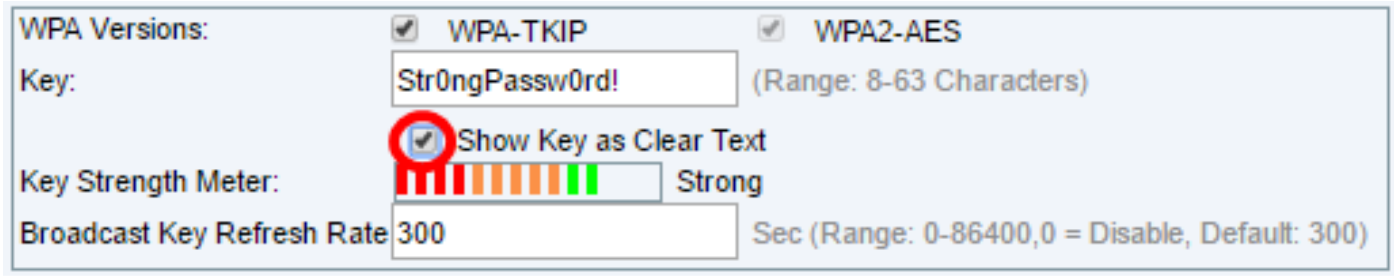
Remarque : si le réseau comporte plusieurs clients, cochez les deux cases. Ce paramètre permet aux stations clientes WPA et WPA2 de s'associer et de s'authentifier, mais il utilise le WPA2 plus robuste pour les clients qui le prennent en charge. Cette configuration WPA permet davantage d'interopérabilité au lieu d'une certaine sécurité.



Étape 8. Dans le champ Key, saisissez un mot de passe comprenant entre 8 et 63 caractères. Chaque périphérique sans fil qui tente de se connecter à ce réseau sans fil est invité à fournir cette clé d'authentification.

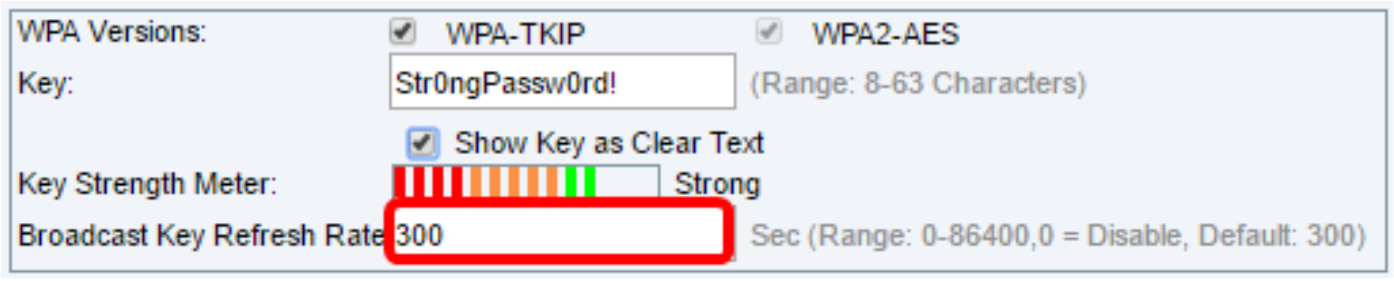


Étape 9. (Facultatif) Cochez la case Afficher la clé en texte clair pour afficher le mot de passe que vous avez créé.



Remarque : la zone Key Strength Meter (Indicateur de puissance de la clé) affiche des barres colorées en fonction de la puissance de la clé que vous avez créée. Dans cet exemple, Str0ngPassword0rd ! est utilisé comme clé d'authentification.

Étape 10. Dans le champ Broadcast Key Refresh Rate, saisissez une valeur comprise entre 0 et 86 400 secondes. Il s'agit de l'intervalle auquel la clé de diffusion (groupe) est actualisée pour les clients associés à ce VAP.

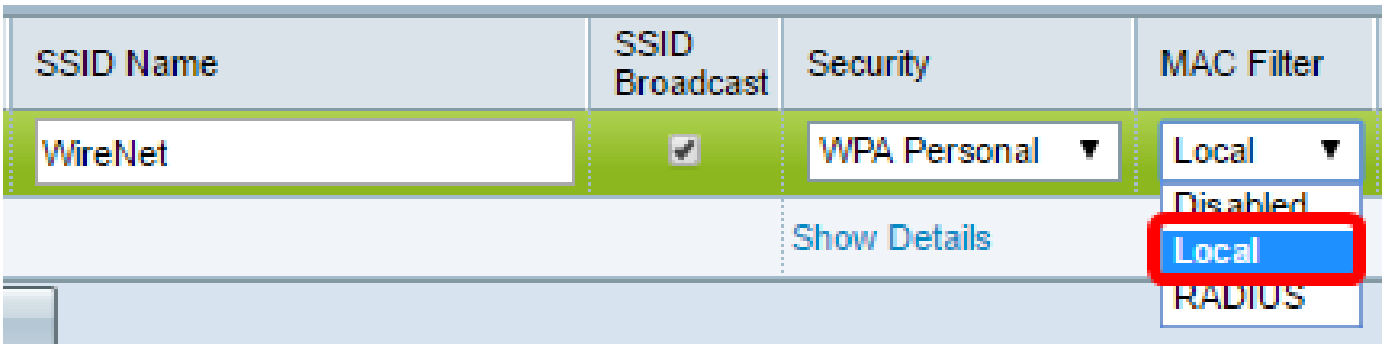


Remarque : dans cet exemple, 300 secondes sont utilisées. C'est la valeur par défaut.

Étape 11. (Facultatif) Sous MAC Filter (Filtre MAC), cliquez sur la liste déroulante pour désactiver MAC Filter (Filtre MAC) ou pour spécifier si les stations qui peuvent accéder à ce VAP sont limitées à une liste globale d'adresses MAC configurée. Les options sont les suivantes :

- Disabled : n'utilise pas le filtrage MAC.
- Local : utilise la liste d'authentification MAC que vous configurez sur la page MAC Filtering.
- RADIUS : utilise la liste d'authentification MAC sur un serveur RADIUS externe.

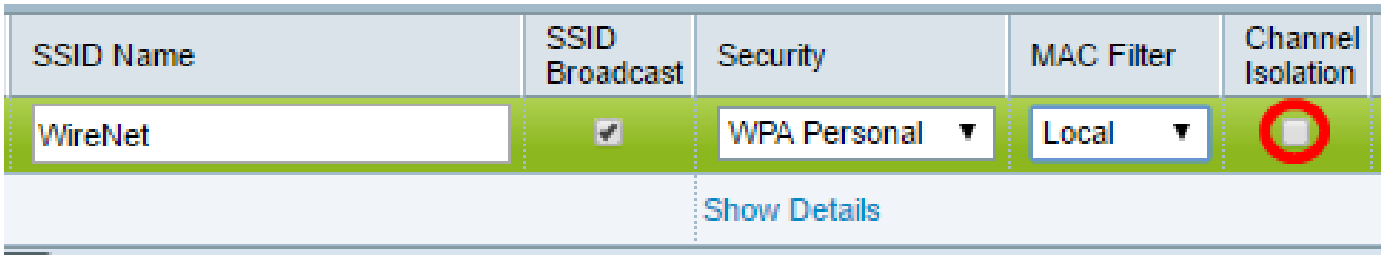
Remarque : pour savoir comment configurer le filtrage MAC, cliquez ici.



Remarque : dans cet exemple, Local est sélectionné.

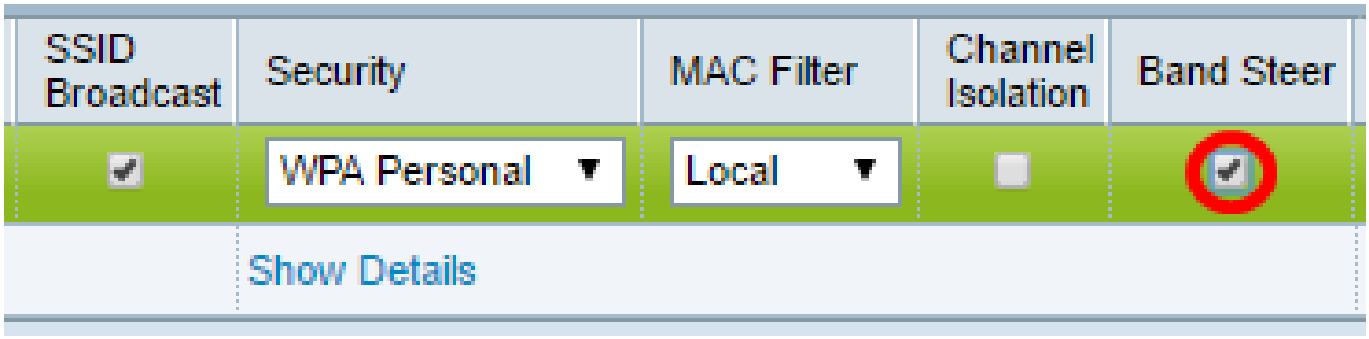
Étape 12. (Facultatif) Cochez ou décochez la case sous Isolation de canal pour l'activer ou la désactiver selon vos préférences. Lorsqu'il est activé, le WAP bloque la communication entre les

clients sans fil sur le même VAP. Le WAP autorise toujours le trafic de données entre ses clients sans fil et les périphériques câblés sur le réseau, via une liaison WDS (Wireless Distribution System) et avec d'autres clients sans fil associés à un autre VAP, mais pas entre les clients sans fil. Lorsqu'ils sont désactivés, les clients sans fil peuvent normalement communiquer entre eux en envoyant du trafic via le WAP.



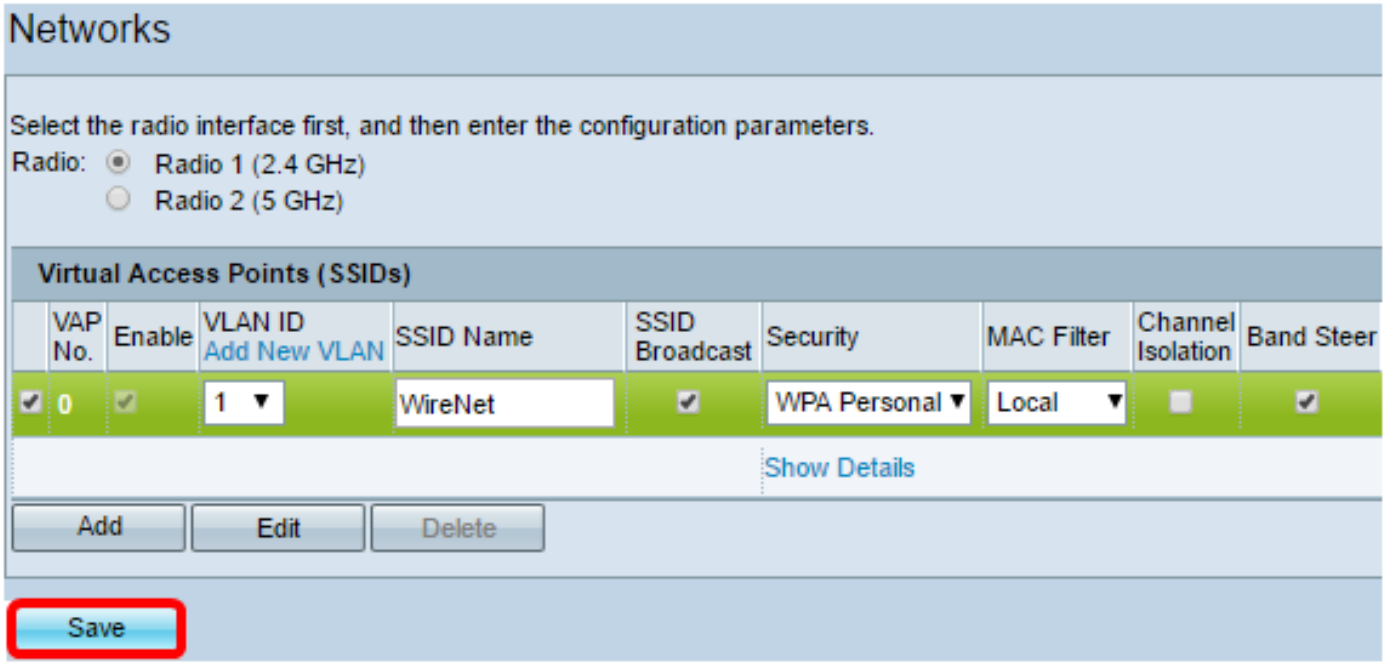
Remarque : dans cet exemple, l'isolation de canal est désactivée. Voici la configuration par défaut .

Étape 13. (Facultatif) Cochez ou décochez la case située sous Band Steer pour l’activer ou la désactiver selon vos préférences. Cette fonctionnalité est réservée aux WAP bibande uniquement. L'activation de l'orientation de bande utilise efficacement la bande 5 GHz en orientant les clients bibande pris en charge de la bande 2,4 GHz vers la bande 5 GHz lorsque les deux radios sont activées.

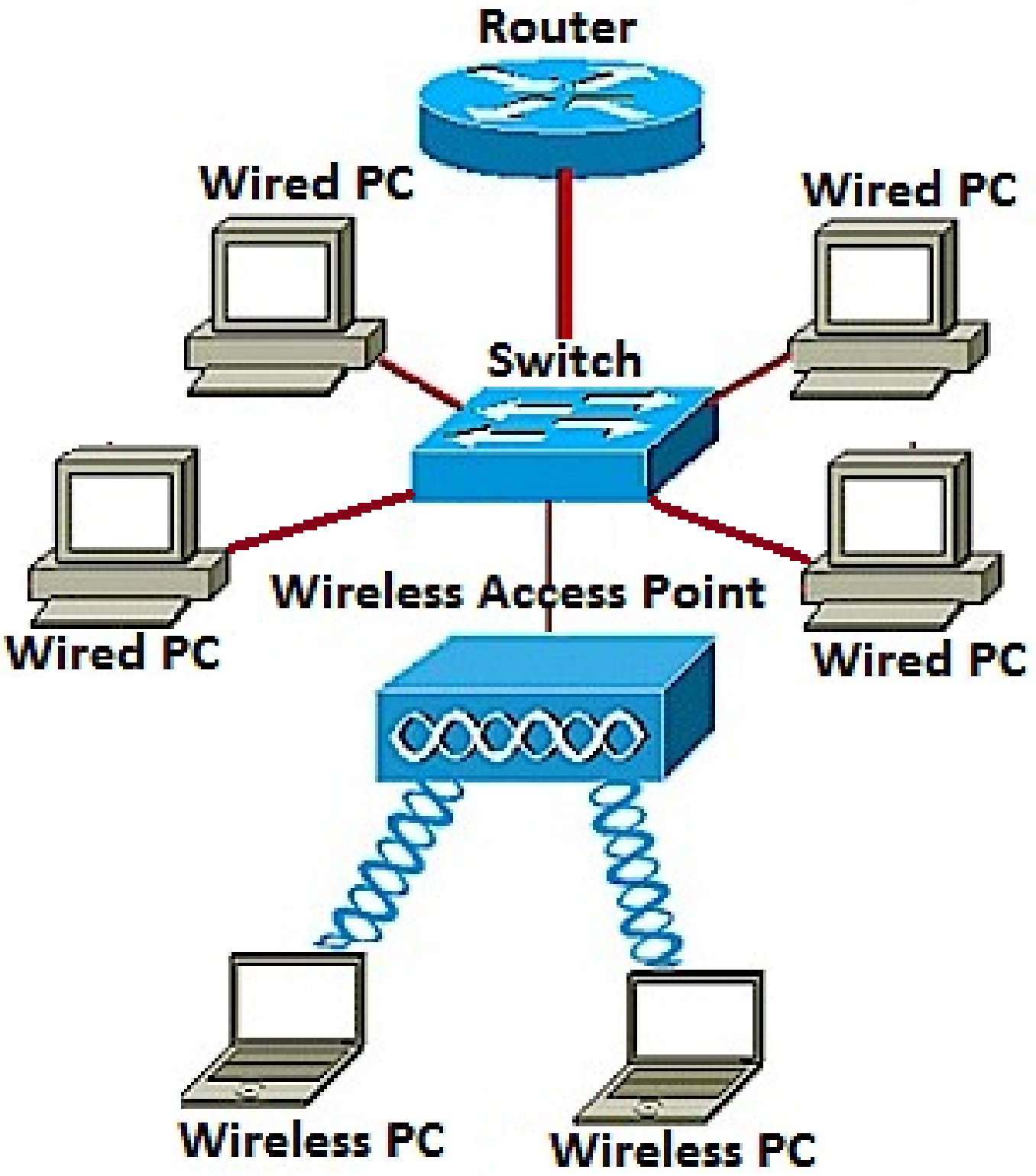


Remarque : dans cet exemple, le mode de gestion de bande est activé.

Étape 14. Cliquez sur Save.



Vous devez maintenant avoir ajouté un réseau sans fil à votre réseau câblé existant à l'aide d'un point d'accès sans fil, comme illustré dans le schéma ci-dessous.


Router
Wired PC
Wired PC
Switch
Wired PC
Wireless Access Point
Wired PC
Wireless PC
Wireless PC

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.